POSEBNA ŠTEVILKA

Monitor

ISBN 961-91168-2-8
9 789619 116821

ZABAVNA ELEKTRONIKA | RAČUNALNIŠTVO | NOVE TEHNOLOGIJE

POLETJE 2025 ◌ LETNIK 35 ◌ WWW.MONITOR.SI
CENA: 5,99 EUR

RAČUNALNIŠKI VIRUSI

VSE O:

- virusih
- črvih
- trojanskih konjih
- rootkitih
- botnetih
- izsiljevalcih!

PODROBNO:

- zgodovina
- najbolj znani
- virusi za Apple Mac
- obramba
- virus kot orožje

IZ TUJEGA TISKA

- Kdo so Shadow Brokers
- Bi morali zakonsko prepovedati odkupnine?
- Vojna in mir v času umetne inteligence

EVIDENCA

POLETJE 2025

VIRUSI SKOZI ČAS

20 Razvoj računalniških virusov

Zgodovina računalniških virusov ni zgolj zgodba o kodi, ki se je izmuznila nadzoru. Je pripoved o človeški radovednosti, domiselnosti, pa tudi o nepredvidenih posledicah razvoja tehnologije.

CILJI

36 Od heca do orodja moči

V začetku sedemdesetih let so bili prvi virusi ustvarjeni iz radovednosti in igrivosti, a romantike je bilo konec, ko so virusi dobili zobe. Danes prevladujejo izsiljevalski virusi, pa seveda tisti, s katerimi operirajo – države.

OBRAMBA

44 Najšibkejši člen je uporabnik

Še pred nekaj leti smo ob zagonu novega računalnika najprej pomislili na namestitev protivirusnega programa, danes pa je jasno, da zgolj ena plast zaščite nikakor ni dovolj. Sploh pa težava pogosto sploh ni v samem sistemu, temveč v uporabniku.

NAJBOLJ ZNANI

34 Virusi za **Apple Mac**

Dolga leta so uporabniki Applovih računalnikov živeli v prepričanju, da njihovi stroji preprosto ne morejo dobiti virusov. Toda ta občutek je bil iluzija. Virusi za mace so obstajali od nekdaj. Bili so sicer redkejši in subtilnejši, a pogosto enako nevarni.

DRŽAVE

54 Zlobne države

Države bi nemalokrat želele dostopiti do pametnih naprav državljanov ali prisluškovati njihovim komunikacijam, a zaradi moderne tehnologije in vseprisotnega šifriranja tega vedno ne znajo same. Zato se zatekajo se k nakupom programov ali storitev zasebnega sektorja.

IZ TUJEGA TISKA

64 Bi morali zakonsko prepovedati odkupnine?

Severna Karolina je prva ameriška zvezna država, ki je prepovedala plačila zaradi izsiljevalske programske opreme in sprejela celo prepoved pogajanj s kibernetičnimi zločinci

Takratnemu direktorju podjetja se je zdelo zanimivo odpreti priponko LOVE-LETTER-FOR-YOU, ki mu jo je poslal poslovni partner.

MATJAŽ KLANČAR
odgovorni urednik, matjaz.klancar@monitor.si

Od pingponga **do vojne**

Več kot 50 let je že tega, kar je nekdo spisal prvi računalniški virus. Takrat je bila to demonstracija izvedljivosti, danes pa so virusi posel, in to zelo dobičkonosen. In seveda sredstvo nadzora, ki ga s pridom uporablja marsikatera (ne)demokratična država.

Spominjam se, kot bi bilo danes – sedel sem v svoji polkletni študentski sobi in v moj novi PC tipkal programsko kodo (najverjetneje v Pascalu), ko so črke z mojega besedilnega zaslona nenadoma začele … padati! Res sem si moral nekajkrat pometi oči, da sem verjel – da, črke na zaslonu so padale v spodnjo vrstico, kot v kakšni risanki. Med tipkanjem, neverjetno! Takrat seveda ni bilo ChatGPT-ja ali Googla, zato je trajalo nekaj dni, da sem med kolegi na fakulteti našel nekoga, ki je sploh razumel, kaj mu pravim, in je vse skupaj prevedel v eno besedo – virus! Moj prvi računalniški virus, ki mu je kaj kmalu sledil še drugi, ki se je z mojim zaslonom šel pingpong oziroma nekakšen *Breakout*. Priznam, računalnik sem takrat okužil z disketami, ki so krožile med pirati in uporabniki.

Prevrtimo čas za 12 let naprej in virusi so že krožili po omrežjih – v moji takratni (in sedanji) službi se je kot blisk razširil ljubezenski virus in skorajda povzročil nepopravljivo škodo. Takratnemu direktorju podjetja se je zdelo zanimivo odpreti priponko LOVE-LETTER-FOR-YOU, ki mu jo je poslal poslovni partner. Tudi meni, kot takratnemu sistemcu v podjetju, je dan v trenutku postal »zanimiv« – na centralnem strežniku podjetja so namreč začele izginjati datoteke s končnico JPG. Predstavljate si lahko, da so te v podjetju, ki se ukvarja z izdajo medijev, »še kar« pomembne. K sreči smo bili leta 2000 že toliko osveščeni, da smo premogli sistem za samodejno izdelavo varnostnih kopij, ki je celo deloval. In izbrisane datoteke smo uspešno obnovili.

Takrat je bilo že vsem jasno: nepremišljeno klikati na sumljive priponke in datoteke je lahko izredno nevarno! Toda nepremišljeni so seveda vedno le »drugi«, sam sem previden in računalniško izobražen, sem si govoril, ko sem še naprej živel nevarno, brez nameščenega protivirusnega programa. Računalniki so bili takrat pač še šibki, protivirusni programi pa počasni in za sistem zelo obremenjujoči. Imeti računalnik, ki moj Word odpre nekaj sekund hitreje, se je zdelo bolj pomembno kot to, da je računalnik brez protivirusnika nevaren. Napaka! Nekoč mi je »uspelo« klikniti nekaj, kar je povzročilo okužbo. K sreči le mojega računalnika in ne tudi omrežja, vseeno pa je za čiščenje in ponovno nameščanje sistema šel kakšen dan ali dva.

Od takrat na mojem računalniku/računalnikih vedno teče protivirusnik. In ker so računalniki, tudi zaradi pogonov SSD, postali dovolj hitri, ga sploh ne opazim. Tudi zato, ker uporabljam Microsoft Defender, tisti protivirusnik, ki je priložen Windows. Vem, menda ni med najboljšimi na svetu, vendar testi neodvisnih institucij zagotavljajo, da je »dovolj dober«, če le ne naletimo na popolnoma novo nesnago, s katero še ni seznanjen.

Nikoli se namreč nisem mogel sprijazniti, da bi na svoj osebni računalnik namestil katero izmed protivirusnih rešitev, ki zahtevajo plačilo mesečne naročnine. Rešitev, ki so se za marsikatero varnostno podjetje izkazale kot gos, ki leže zlata jajca, saj so jih uporabniki kar privzeto naročali, največkrat že kar ob nakupu novega računalnika. Od nekdaj so se mi zdeli preveliki, preveč kompleksni, preveč omejujoči. Danes, ko je Microsoft Defender »dovolj dober«, je verjetno tudi to razlog, da so zgoraj omenjena gosja malce manj zlata, uspešnih in bogatih varnostnih podjetij za domače uporabnike pa je precej manj.

Kar pa ne pomeni, da varnostne/»protivirusne« industrije ne potrebujemo v poslovnem svetu. Nasprotno, tam je to zelo resen posel, večja podjetja imajo nameščeno še vse kaj drugega, kot le protivirusnike, o čemer lahko preberete v intervjuju z Gorazdom Božičem iz SI-CERT. Kar smo, denimo, videli lani, ko je posodobitev za enega takih sistemov za res velika podjetja, Crowdstrike, ohromila velik del svetovnega digitalnega sveta.

Da take sisteme podjetja morajo imeti, je seveda jasno – virusi danes ne premetavajo več črk po zaslonu niti z nami ne igrajo pingponga. Virusi danes kradejo in izsiljujejo, nepovratno šifrirajo datoteke, nemalokrat so lahko celo orožje. Nekateri »virusi« za mobilne telefone, ki so v uporabi držav, služijo celo za poseganje v zasebnost posameznikov. In ti so v resnici edini, proti katerim ne moremo nič.

Beli klobuk

V preteklem stoletju smo zgradili svet, ki je odvisen od električne energije, v tem stoletju pa smo se znašli v svetu, ki je odvisen od delujočih računalnikov in informacijskih sistemov. S tem postaja čedalje pomembnejši poklic hekerjev z belimi klobuki (‚white-hat') oziroma etičnih hekerjev. Govorili smo z enim slovenskih pionirjev na tem področju.

Matej Huš

▶ V slovenski javnosti ste verjetno najbolj znani etični heker, ki ga pogosto pokličejo za komentar ob odmevnih vdorih in napadih. Kako nekdo postane strokovnjak za varnost in etični heker? Študirali ste računalništvo, začeli pa ste kot razvijalec v Hermes Softlabu.

To se ne zgodi čez noč. Postati strokovnjak za varnost in etični heker je pot, ki zahteva veliko radovednosti, učenja, praktičnega dela in tudi izkušenj v resničnem življenju. Prvi korak je razumevanje osnov delovanja računalniških sistemov in omrežij, strežnikov, protokolov, aplikacij in zlasti tudi ranljivosti.

Pomemben del poti so tudi lastne raziskave in skupnost. Tak primer so tekmovanja CTF (*capture the flag*), sodelovanje na hekerskih dogodkih in organizacija dogodkov ter tudi celo samostojno raziskovanje ranljivosti v aplikacijah in sistemih. To je področje, kjer se učiš vse življenje. Grožnje se nenehno razvijajo, tehnologije se spreminjajo, napadalci napredujejo. Pri tem delu me najbolj navdušuje, da je vsaka nova ranljivost nova uganka in izziv, s katerim se je treba spopasti. Dokler ga ne rešiš, ti ne da miru.

▶ Etične hekerje od preostalih loči torej – etika.

Seveda, pomembna je jasna etična drža, zavedanje, kaj je prav in kaj ne, kje so meje, prek katerih ne smeš. Etika loči strokovnjaka za varnost od napadalca. Etični hekerji si prizadevamo pomagati organizacijam odkriti in odpraviti ranljivosti, preden jih izkoristijo zlonamerni napadalci. Pogosto pravim, da delamo nezakonite stvari na zakonit način, pa še plačajo nas.

▶ Z ustanovitvijo Virisa ste se osredotočili na računalniško varnost.

Nismo se takoj 'vrgli' na računalniško varnost, saj je podjetje Viris sprva delovalo na področju virtualizacije, požarnih pregrad in monitoringa sistemov, torej bolj sistemska integracija in nekaj varnosti, potem pa smo se osredotočili na varnost.

▶ Kaj vse počnete kot etični heker danes? Ali če vprašam drugače, je naziv ‚heker' preozek, saj tudi izobražujete, svetujete, predavate?

Izraz heker res zveni nekoliko ozko, saj si ga ljudje pogosto

predstavljajo kot nekoga, ki vstopa v sisteme. V resnici je delo etičnega hekerja veliko širše. Ne gre le za tehnično iskanje ranljivosti, ampak za razumevanje, kako zaščititi sisteme, ljudi in podatke. Torej za dobrega etičnega hekerja je pomembna širina, saj tudi svetuje.

Delo je torej zelo raznoliko. En dan rešujemo tehnični problem, kot je analiza ranljivosti, naslednji dan vodimo delavnico za zaposlene, nato pa z vodstvom podjetja snujemo varnostno strategijo.

▶ In katerega dela je več?

Tehničnega dela, torej penetracijskih testov in analize ranljivosti, je še vedno precej, a čedalje več je tudi izobraževanj, svetovanj in dela z ljudmi. Varovanje informacij danes ni več le tehnični problem, temveč vedno bolj vprašanje kulture in zavedanja. Res pa je, da tudi zelo užival v izobraževanju novih etičnih hekerjev in tistih, ki bodo ščitili naše sisteme v prihodnje, kar mi predstavlja še poseben izziv.

▶ Kdo so torej vaše stranke? Velika ali majhna podjetja?

Zelo različno. Delamo tako za velika kot tudi za manjša podjetja. Pri varnosti ni pomembno samo, kako veliko je podjetje, ampak to, kako pomembne podatke in sisteme želi zaščititi. Naši naročniki prihajajo z različnih področij, od finančnih institucij, javnega sektorja, proizvodnih podjetij, zdravstva do tehnoloških startupov. Varnost je postala univerzalna potreba, zato je treba pristop prilagoditi vsaki stranki posebej ne glede na velikost ali panogo. Ravno ta raznolikost nas dodatno motivira, saj lahko prenašamo dobre prakse med panogami in držimo korak z globalnimi trendi.

▶ Ste omejeni na Slovenijo ali delate tudi za tuja podjetja?

Poleg slovenskih podjetij imamo tudi že lepo število zadovoljnih strank v tujini, na kar smo posebej ponosni, saj to potrjuje, da je naše delo prepoznano tudi zunaj meja Slovenije. Prek meja je seveda še dosti težje uspeti, saj je konkurenca večja, zato smo vsake nove stranke ter njene pohvale še posebej veseli.

▶ Če pogledava tipičen varnostni pregled podjetja oziroma pen testing. Kaj obsega?

Tipičen penetracijski test ali varnostni pregled v resnici obsega več kot le tehnični pregled sistema in iskanje ranljivosti. Drži, jedro testa predstavlja tehnična analiza. Z njo preverimo, kako varni so aplikacije, omrežja in infrastruktura, preverimo konfiguracije, dostopne storitve, ranljivosti v programski opremi, zaščito podatkov, možnosti zlorab in še veliko drugega. S tem pripravimo podrobno poročilo z ugotovitvami, ocenami tveganj in s priporočili.

A to je šele začetek, saj mnogo podjetij danes pričakuje celostno pomoč. Poleg tehničnega pregleda pogosto pripravljamo tudi delavnice in usposabljanja za zaposlene, pomagamo pri vzpostavitvi varnostnih politik, incidentnih načrtov in celo sodelujemo pri načrtovanju varnih informacijskih sistemov že v fazi razvoja.

▶ Morate kdaj popravljati za drugimi?

Dober in kakovosten penetracijski test lahko pokaže tudi to. Včasih odkrijemo, da je bil prejšnji varnostni pregled drugega izvajalca pomanjkljiv ali površno opravljen. Morda je šlo samo za rezultat kakšnega orodja. To je problematično, ker podjetja pogosto menijo, da so z enim pregledom varna, a v resnici šele poglobljen in strokovno opravljen pregled pokaže pravo sliko in izpostavi skrite težave.

▶ Niso pa ranljivosti zgolj varnostne luknje, kajne? Pogosto beremo o napačnih nastavitvah, prelahkih geslih, nepravilnih pravicah dostopov.

Res je, ranljivosti niso vedno samo tehnične luknje v programski opremi, ki jih odkrijemo s skenerji ali testi. Pogosto gre za čisto človeške napake: napačne nastavitve, prelahka gesla, neustrezno dodeljene pravice, manjkajoče posodobitve. Vsak razvijalec ali sistemski skrbnik ima kdaj slab dan ali pa zaradi zahtev in kratkih rokov stori napako.

▶ Kako se zaščititi pred prvimi in kako pred drugimi?

Pred klasičnimi ranljivostmi, torej varnostnimi luknjami v aplikacijah ali sistemih, se zaščitimo s tehničnimi ukrepi. To so posodobitve, popravki in varnostne rešitve. Pred napačnimi nastavitvami, šibkimi gesli in neustreznimi dostopi pa se zaščitimo z vzpostavitvijo dobrih varnostnih praks. Takšni primeri so močna politika gesel, dvostopenjska avtentikacija, redni pregledi pravic in ozaveščanje o varnostnih tveganjih. Zaščita ni zgolj tehnični problem, temveč kombinacija tehnologije, pravilnih postopkov in predvsem zavedanja ljudi, da so varnostna pravila del vsakodnevnega dela.

Tipičen varnostni pregled obsega več kot le tehnični pregled sistema in iskanje ranljivosti.

Osnovna zaščita varuje pred množičnimi napadi, a ko postaneš tarča državnega napadalca, je igra drugačna.

▶ S tem se lahko zaščitimo pred večino, reciva temu, naključnih vdorov, ki prizadenejo tarče z naivnimi pomanjkljivostmi. Kaj pa lahko storijo tarče, ki si jih izrecno izberejo državni hekerji z dostopom do opreme NSO Groupa ali Cellebrita? Se sploh da zaščititi pred temi?

Res je, z upoštevanjem dobrih praks lahko preprečimo veliko večino naključnih vdorov, za katere napadalci iščejo najšibkejše tarče. A ko govorimo o naprednih grožnjah, kot so napadi državnih hekerjev z orodji NSO Group ali Cellebrite, je slika precej bolj kompleksna.

Sam rad citiram Mika Hyppönena, priznanega strokovnjaka za kibernetsko varnost, ki pravi: »Če je naprava pametna, je ranljiva.« To pomeni, če je nekaj povezano z omrežjem, če je pametno in kompleksno, ima tudi ranljivosti, včasih takšne, ki jih ni mogoče enostavno odpraviti ali se jim izogniti.

▶ Kar se sliši precej pesimistično.

Pred takšnimi ciljanimi napadi, kjer te nekdo namerno in usmerjeno napade, popolne zaščite preprosto ni. Lahko pa zmanjšamo tveganja z uvedbo večplastne varnosti: omejitvami dostopa, s šifriranjem, z zmanjšanjem napadalne površine, rednimi varnostnimi pregledi in predvsem z zavedanjem, da stoodstotna varnost ne obstaja.

▶ Torej bi se morali pripraviti na scenarij, kaj storiti po napadu?

Če te izrecno napade nekdo z dostopom do vrhunskih vohunskih orodij, so cilj predvsem zgodnje odkrivanje napada, odziv in omejitev škode, ne pa iluzija popolne zaščite. Razumeti moramo razliko. Osnovna zaščita varuje pred množičnimi napadi, a ko postaneš tarča državnega napadalca, je igra drugačna. Takrat moraš imeti strategijo, postopke in znanje, kako se odzvati, ko se napad zgodi.

▶ V pogovoru za platformo Ogrodje ste lani dejali, da ste že pred leti na konferenci NTK pokazali, da lahko zgolj z googlanjem pridete do glavnega sistema (main frame) večjega slovenskega podjetja.

Tisti primer na konferenci NTK je bil zelo zgovoren. Samo z nekaj iskanja po spletu in z uporabo javno dostopnih virov smo pokazali, kako ranljiva so lahko tudi velika podjetja. Od takrat je minilo že kar nekaj let in v tem času smo tudi sami vložili veliko energije v izobraževanja, predavanja in ozaveščanje. Prav s takimi primeri smo želeli pokazati, kako enostavno je včasih priti do občutljivih podatkov ali sistemov, če niso ustrezno zaščiteni.

▶ Je danes stanje boljše?

Stanje se je vsekakor izboljšalo. Podjetja so pozornejša, več vlagajo v varnost, več se govori o zaščiti podatkov in sistemov, vendar pa je treba biti realen, popolne varnosti še vedno ni in tudi napadalci ne stojijo na mestu. Razvijajo nove načine, iščejo nove poti, vdirajo prek verige dobaviteljev, izkoriščajo socialni inženiring, ciljne napade ...

Za izvedbo napadov so tudi umetno inteligenco takoj uporabili. Čeprav je varnost danes boljša kot pred leti, te tekme nihče ne more dobiti. Varnost ni cilj, ampak proces, ki ga je treba neprestano spremljati, prilagajati in izboljševati.

▶ Na kar včasih malo pozabimo.

Žal še vedno pogosto vidimo, da ravno incidenti najbolj spodbudijo vlaganja v varnost. Ko se zgodi vdor ali uhajanje podatkov, podjetja spoznajo, kako pomembna je varnost. Pogosto tedaj pride do premikov in izboljšav. Želeli pa bi si, da bi bilo več proaktivnega razmišljanja, ne šele reaktivnega ukrepanja po incidentu.

▶ Lahko podjetja k večji varnosti prisili zakonodaja?

Če primerjamo stanje danes z obdobjem pred desetimi ali dvajsetimi leti, je razlika zelo očitna. Takrat je regulativa močno zaostajala za dejanskimi tveganji, danes pa imamo veliko jasneje določene okvire, standardi so višji in tudi na zakonodajni ravni se stvari premikajo v pravo smer. Imamo nov Zakon o informacijski varnosti in tudi nove evropske predpise, kot je direktiva NIS2, ki uvaja še strožje zahteve in obveznosti za številne subjekte.

▶ Pa se v praksi regulativa spoštuje in kdo to preverja? So inšpekcijski nadzori realnost?

Stanje se izboljšuje, a še vedno ni idealno. Mnoge organizacije se trudijo vzpostaviti skladnost, a pogosto so ukrepi še vedno površinski, saj nekatere žene predvsem 'kljukica na obrazcu' in ne dejanska želja po izboljšanju varnosti.

Inšpekcijski nadzori pa so realnost. Pristojni organi jih izvajajo, predvsem za zavezance po zakonodaji, in tudi nekatere druge je to začelo že malo skrbeti. V praksi pa je še vedno precej prostora za izboljšave, tako pri obsegu nadzorov kot pri globini preverjanja. Žal pogosto vidimo, da se podjetja začnejo resno ukvarjati s skladnostjo in z varnostjo šele, ko pride do inšpekcijskega nadzora ali celo po kakšnem incidentu.

Regulativa je torej boljša, a varnosti ne smemo jemati zgolj kot formalnosti. Organizacije

morajo varnost razumeti kot poslovno nujnost in del digitalnega sveta.

▶ Razlike med sektorji, na primer bankami na eni strani in malimi družinskimi podjetji na drugi strani, verjetno niso majhne.

Razlike so precejšnje. Banke in mala družinska podjetja so povsem različni svetovi: tako po zahtevah kot zmožnostih. Banke in finančne ustanove so pod strogim regulatornim nadzorom, imajo zahtevne standarde, kot so PCI DSS, ISO 27001, in zdaj tudi direktivo NIS2, zato v varnost pogosto vlagajo precej sredstev, tako v tehnologijo kot kadre. Imajo ločene varnostne oddelke, notranje varnostne preglede, sodelujejo z zunanjimi izvajalci za penetracijske teste in podobno.

Na drugi strani pa imamo mala podjetja, ki pogosto nimajo časa, sredstev ali kadrov za kompleksne varnostne rešitve. Tam je pogosto izziv že to, da imajo redno posodobljen sistem, močna gesla in osnovne varnostne ukrepe. Zanje je ključno, da se osredotočijo na osnovne varnostne ukrepe, ki so primerni za njihovo velikost in tveganja. Niso premajhni, da bi bili tarča. Nasprotno, napadalci jih pogosto vidijo kot 'šibki člen' v dobavni verigi večjih podjetij.

To sta dva ekstrema, obstaja pa še vse vmes. Varnost mora biti prilagojena, vsi si ne morejo privoščiti varnostnega centra s stalnim nadzorom, lahko pa vsi naredijo osnovne korake. Varnostne kopije, močna gesla, osnovno zavedanje o varnostnih tveganjih in redne posodobitve so železni repertoar.

▶ Pa vendarle, ko je lani Crowdstrike onesposobil več kot osem milijonov računalnikov z Windows, je bila vzrok prav varnostna posodobitev. Programski opremi velikih proizvajalcev implicitno zaupamo, ko klikamo Posodobi.

To je bil jasen znak, da tudi veliki proizvajalci in priznani ponudniki varnostnih rešitev niso imuni na napake. To je bil globalni dogodek, ki je prizadel številna podjetja in organizacije po vsem svetu, in to ne zaradi napada, ampak zaradi programske napake v varnostni rešitvi. Moj sodelavec, denimo, zaradi tega incidenta ni mogel leteti na izbrano destinacijo.

Mala podjetja pogosto nimajo časa, sredstev ali kadrov za kompleksne varnostne rešitve.

Zanašanje na varnost zgolj prek velikih imen je lahko tvegano, saj tudi največji sistemi niso brezhibni. Teoretiki zarote bi lahko rekli, da je šlo za preizkus, kaj se zgodi, ko takšna ključna komponenta odpove, in kakšne so posledice na globalni ravni. A realno je incident pokazal, da je tudi v svetu varnosti programska oprema le skupek kode, ki jo pišejo ljudje, zato so napake neizogibne in testiranje zelo pomembno.

Ravno zato je pomembno, da gradimo odpornost sistemov. Razmišljati moramo o *failover* mehanizmih in se ne zanašati na en sam varnostni sloj, potrebujemo načrte odzivanja na nepredvidene dogodke. Varnost ni le zaščita pred napadi, ampak tudi sposobnost, da se hitro in učinkovito odzovemo, ko nekaj odpove.

▶ Danes najbolj odmevajo vdori z izsiljevalskimi virusi, kot sta bila napada na Univerzo v Mariboru in HSE. Gre v takih primerih za skrbno izbrane tarče, za naključje oziroma smolo ali za pa nezaščitene sisteme, ki bi jih prej ali slej nekaj napadlo?

O vseh podrobnostih teh primerov žal ne morem govoriti, vendar pa lahko rečem, da je uspešnost napada skoraj vedno povezana z več vzroki. Redko samo en dejavnik omogoči napad. Pogosto gre za kombinacijo ranljivosti v sistemu, neustrezno zaščitenih podatkov, pomanjkljivega varnostnega nadzora in včasih tudi čisto človeških napak.

Pri napadih z izsiljevalskimi virusi gre pogosto za kombinacijo. Nekateri napadi so ciljno usmerjeni, drugi pa so 'naključni', kjer napadalci iščejo ranljive sisteme po vsem svetu, nato pa se odločijo, koga bodo izsiljevali glede na to, kaj najdejo. Napadalci pogosto delujejo po načelu šibke tarče, vdirajo tam, kjer je zaščita najslabša ali kjer lahko z najmanj truda povzročijo največ škode. Ključno je zato, da podjetja in organizacije ne čakajo, da bodo na vrsti, ampak proaktivno izboljšujejo varnost. Ni vprašanje, ali bo napad, ampak, kdaj. Tako da je hitra zaznava čudnega obnašanja ali aktivnosti, ki niso običajne, danes bistvenega pomena za uspešen boj proti hekerjem.

▶ Takoj po vdoru zanimanje javnosti močno naraste, a o epilogih običajno ne beremo v medijih. Kakšni so epilogi velikih napadov pri nas?

Ob izbruhu incidenta se o tem veliko govori, potem pa, ko mine nekaj časa, se zadeva umiri in se gre naprej, kot da se ni nič zgodilo. Iz prakse pa vemo, da epilog takšnih incidentov pogosto vključuje dolgotrajno sanacijo, tehnične preglede, včasih tudi spremembo strategij in pristopov k varnosti. V določenih primerih so posledice tudi poslovne, izguba zaupanja, finančne škode, včasih pa tudi odškodninski zahtevki ali celo kazenski postopki.

Nekateri napadi so ciljno usmerjeni, drugi pa so 'naključni', kjer napadalci iščejo ranljive sisteme po vsem svetu.

▶ In za zaključek, česa se mora bati domači uporabnik in kaj lahko stori za svojo varnost? V Srbiji so lani in letos odmevali primeri, ko je policija vdrla v telefone novinarjev z orodjem Pegasus.

Domači uporabnik se mora zavedati, da na kibernetske grožnje ni imun. To ni filmski scenarij, napadi na posameznike so realnost, pa naj bodo to kraja osebnih podatkov, bančne goljufije, zloraba gesel, vdori v elektronsko pošto ali celo vdori v telefone z orodji, kot je Pegasus. Velikokrat pa se zgodi, da se prek domačih uporabnikov pridobi dostop do pravih poslovnih tarč, zato jih ne smemo zanemarjati.

Povprečen uporabnik verjetno ne bo tarča državnega akterja z orodji, kot jih imajo obveščevalne službe. Mora pa se zavedati, da so prav domači uporabniki pogosto najranljivejši, ker pogosto nimajo vzpostavljenih osnovnih varnostnih ukrepov. Pomembno je zato, da vsak posameznik poskrbi za osnovno digitalno higieno: uporablja močna in unikatna gesla, omogoči dvostopenjsko avtentikacijo, redno posodablja naprave in aplikacije, varnostno kopira pomembne podatke ter je previden pri odpiranju povezav ali priponk, ki jih prejme.

▶ Zdi se, da venomer pridigamo o istih ukrepih, učinki pa so skromni.

Resnici na ljubo bi morali nekateri uporabniki na tečaj osnov kibernetske higiene. Prevečkrat vidimo, da osnovnih varnostnih ukrepov ne poznajo ali pa jih preprosto ne uporabljajo. Morda pa bi morali o tem začeti razmišljati že prej. Recimo, da bi osnove digitalne varnosti in kibernetske higiene uvedli v izobraževalni sistem. Tako kot vsak zna zakleniti vrata svojega stanovanja, bi moral znati zakleniti tudi svoja digitalna vrata. To znanje bi moralo biti osnovna veščina, ne nekaj, česar se naučimo šele po prvem incidentu. ◀

Slovenski **angeli varuhi**

Ob 30-letnici Nacionalnega odzivnega centra za kibernetsko varnost (SI-CERT) smo govorili z njegovim dolgoletnim vodjo Gorazdom Božičem.

Matej Huš

SI-CERT opravlja pomembne naloge na področju kibernetske varnosti. Med drugim sprejemajo prijave incidentov, pomagajo, svetujejo, izobražujejo in opozarjajo. SI-CERT v četrto desetletje delovanja vstopa z dobro kondicijo, kljub čedalje nevarnejšemu svetu pa se zavedanje o pomenu varnosti v javnosti izboljšuje.

▶ SI-CERT je v Sloveniji postal sinonim za kibernetsko varnost. Širša javnost nanj pomisli, ko se varnostni incidenti pojavijo v medijih. Vi SI-CERT vodite, vaš elektronski naslov pa se konča z domeno arnes.si.

SI-CERT je Nacionalni odzivni center za kibernetsko varnost oziroma v angleščini *Slovenian Computer Emergency Response Team*. Smo del javnega zavoda Arnes, ki se je na neki način začel z internetom v Sloveniji. Ko so internet razvijali v akademskem okolju, je Arnes prevzel nekatere naloge v nacionalni infrastrukturi.

Trenutno imamo dve veliki območji delovanja. Arnes nudi storitve za raziskovalno in izobraževalno sfero, kamor sodi tudi internetna hrbtenica, kjer so vse te organizacije povezane. Drugi del pa je nacionalna internetna infrastruktura, kamor sodijo vozlišče za izmenjavo prometa SIX, register domen in tudi naš oddelek SI-CERT.

▶ Midva se danes pogovarjava na razdalji tisoč kilometrov prek Eduroama, ki je tudi del vaše infrastrukture.

Drži, vse to so Arnesove storitve. Nazadnje sem bil na univerzi v Krakovu na Poljskem na sestanku, kjer sem se prav tako z internetom povezal prek Eduroama. Šlo je zelo gladko.

▶ Če torej začneva s SI-CERT, vi ste del Arnesa. Kako veliki ste? Seznam vaših nalog je impresivno dolg.

Drži. Tam imamo zelo spodbudno okolje, v katerem lahko razvijamo svoje storitve. Naše aktivnosti financira Urad Vlade Republike Slovenije za informacijsko varnost, pristojni nacionalni organ za informacijsko varnost.

Zaposlenih nas je samo 13 in želeli bi biti večji. V primerjavi z drugimi državami zaostajamo, pa ne govorimo o Nemčiji ali Franciji, temveč o Estoniji, Latviji ali Hrvaški, ki so nam podobne po številu prebivalcev in BDP. Nas na SI-CERT je zelo malo in to je težava, ki smo jo predstavili tudi našemu pristojnemu organu.

▶ Kako velik bi SI-CERT želel biti?

Hitro zrasti s 13 na sto, govorim na pamet, ni mogoče. Ne gre samo za vprašanje financiranja in postopkov zaposlitve. Treba je najti ljudi z ustreznim znanjem. Na hitro ne moremo uvesti veliko ljudi, zato je lahko rast samo postopna. Ljudje z leti potem pridobijo znanja, integriramo jih v procese, prepoznamo kakovost. A čeprav smo majhna ekipa, sem osebno zelo ponosen na vse, kar nam uspe narediti. Bi si pa seveda želel vizije rasti in zavezo države, da nas bo podpirala in omogočala rast.

▶ Pa je težko dobiti nove kadre? Zasebni sektor je huda konkurenca.

Ni enostavno, a nam za zdaj dobro uspeva. Nekaj kadrov dobimo tudi iz drugih delov javnega sektorja, na splošno sem s trenutno situacijo zadovoljen. Pogosto dobimo tudi vprašanja vodij iz drugih delov javnega sektorja, kakšen mehanizem imamo za privabljanje kadrov.

▶ In skrivnost je?

Malce tudi to, da se ukvarjamo z zelo specifičnimi problemi, kar lahko odtehta razliko v plači v primerjavi z zasebnim sektorjem. Zlasti Slovenija je premajhna, da bi v zasebnem sektorju našli podjetja, ki bi vlagala veliko denarja v raziskave kibernetske varnosti, kot na primer ameriški Mandiant. Tak poslovni model v Sloveniji zelo težko deluje.

Po drugi strani na SI-CERT razvijamo različne strokovnosti, obratuje laboratorij za analizo škodljive kode, nudimo udeležbo na izobraževanjih, vlagamo v karierni razvoj, razvijamo različne kapacitete. Te potem ponudimo tudi organom pregona, ko jih potrebujejo, znamo narediti različne analize in preiskave. Rekel bi, da smo zelo sposobni, kar potrjujejo tudi naši zaposleni.

▶ In ste tudi v prvi vrsti, ko se zgodijo napadi. Lani smo imeli dva velika izpada infrastrukture, incident Crowdstrike in vdor v Univerzo v Mariboru, ki sta bila na prvih straneh medijev. Koliko pa je incidentov, ki tja ne pridejo?

Ni jih malo. Januarja smo objavili statistiko za preteklo leto, v katerem smo prejeli 4.587 prijav incidentov. Od tega je največ, približno tretjina, primerov ribarjenja (*phishing*). V teh primerih so tarče komitenti bank, denimo v imenu lažnih dostavnih podjetij.

Precej je tudi spletnih goljufij, denimo investicijskih prevar, v katerih neznanci nagovarjajo posameznike, naj vložijo v neko ničvredno kriptovaluto. Mnogokrat vzamejo celo posojila. Teh primerov je čedalje več, medtem ko se število tako imenovanih ljubezenskih prevar zmanjšuje. Ti primeri, čeprav imajo lahko hude posledice za žrtve, se tehnično vodijo kot lažji incidenti. Tu tudi ne moremo storiti kaj dosti, lahko osveščamo in svetujemo, a nismo policija. V preventivo se morajo vključiti tudi banke, potrošniške organizacije in drugi.

Tehnično zahtevnih incidentov pa je bilo 790, kamor sodi razvpiti primer vdora v Univerzo v Mariboru. Tu je najprej potrebna analiza, kaj se je sploh zgodilo, kako in zakaj. In da že takoj odgovorim na obvezno podvprašanje, ki ga vedno zastavijo …

▶ Koliko je neprijavljenih incidentov?

Kot je rekel Donald Rumsfeld, imamo neznane neznanke (*unknown unknowns*), ki jih zelo težko ocenimo, saj jih ne vidimo. Nekaj ocen vseeno obstaja. Kolegi v tujini ocenjujejo, da je prijavljenih približno tretjina incidentov. Drugi dve tretjini nista nujno le neprijavljeni, včasih so incidenti tudi neopaženi.

▶ Po naši zakonodaji je prijava obvezna.

To drži za zavezance, ki delujejo v posameznih sektorjih in so že po obstoječem zakonu o informacijski varnosti dolžni prijavljati incidente, ki vplivajo na zagotavljanje bistvenih storitev. Obvezne so prijave za incidente, če presegajo prag, ki določa mo-

Prijavljenih je približno tretjina incidentov. Ostali niso nujno le neprijavljeni, včasih so tudi neopaženi.

tnje storitve. V prihajajočem zakonu o informacijski varnosti, ki je bil sprejet konec maja letos, se nabor zavezancev širi, zato lahko pričakujemo več prijav malih in srednje velikih podjetij. Če pa je nekdo tarča nekega ribarskega napada, pri katerem ni nastala škoda, tega morda ne bo prijavil, sploh kadar je poskusov veliko. Lahko da prostovoljno prijavo, kar vzpodbujamo, ni pa to nujno.

▶ Ko se zgodi večji napad s hudimi posledicami, kako se odzove SI-CERT in kaj najprej svetujete žrtvi? Kakšne so vaše funkcije?

Mi se aktiviramo takoj in pomagamo pri prvih korakih. Ukrepi so zelo odvisni od vrste incidenta. Da ponazorim. Če gre za prevaro, s katero je računovodstvu nekdo podtaknil lažni račun

Delujemo že 30 let in imamo dobro razvejano mrežo ljudi, ki prijavljajo incidente.

(*CEO fraud*), je ukrepanje drugačno kot pri napadu z izsiljevalskim virusom, ki morda ravno teče, ali pa napadu s preobremenitvijo (*denial of service*). Oceniti moramo, kako so napadalci vstopili v sistem, katero ranljivost so izkoristili, kako globoko se je napad razširil. Ugotoviti je treba, ali gre za volumetrični ali aplikacijski napad. Skratka, prepoznati moramo vzorec.

▶ Kako pomembna je časovna komponenta? So napadi, kjer je takojšnji odziv nujen in vsaka ura šteje?

Seveda. Takšni primeri so zlasti v večjih organizacijah, ki imajo dobro konfigurirane sisteme. Njihovi sistemi SIEM (*security information and event management*) in EDR (*endpoint detection and response*) lahko pravočasno prepoznajo anomalije in se sprožijo. Običajno postavijo pregrade, ki zamejijo napad in preprečijo šifriranje podatkov po celotnem omrežju. Tak primer je bil tudi HSE, kjer je bila reakcija hitra, s čimer so omejili obseg napada. To so storile že njihove službe in centri, saj se mi vključimo šele, ko dejansko pride do napada in nas pokličejo.

▶ Lahko podobno kot forenziki analizirate zlonamerno kodo?

To tudi počnemo. Zlonamerno kodo pridobimo, jo v laboratoriju analiziramo in nato podamo priporočila žrtvi, kaj naj stori. Analiza lahko tudi pokaže, kaj vse je ogroženo, kakšne posledice so možne. Na primer, ali je napad meril na poverilnice oziroma digitalna potrdila ali druge podatke, ki se lahko prodajajo na temnem spletu.

▶ Zakaj? Ker je mogoče s temi podatki vdreti v podjetja?

To predstavlja dodatno ogroženost, ki so ji izpostavljena zlasti podjetja. Napadalci lahko merijo na posameznike v podjetju, in ko pridobijo dostop do njihovega elektronskega predala ali računalnika, spremljajo komunikacijo in poslovanje. Če je tarča nekdo v nabavi, storilci spremljajo njegovo delo in v ključnem trenutku vskočijo v komunikacijo s pretvezo, da se je spremenil bančni račun ali kaj podobnega. To je relevantno, ko slovenska podjetja poslujejo s tujimi.

Za tak napad običajno izvemo šele po odtujitvi sredstev, čeprav se je začel že s *phishingom* oziroma vstopom v poštni predal. V teh primerih je treba preveriti, kako je nastavljen poštni predal, ali so kakšni znaki *phishing* napada. Pomembno je ugotoviti, ali se je zloraba zgodila v slovenskem podjetju ali tujem podjetju, ker je to relevantno pri morebitnih odškodninah.

▶ Kako je s preiskanostjo vdorov in napadov? Vi niste organ pregona, a sodelujete tudi z njimi.

Ena izmed naših osnovnih funkcij je gradnja situacijskega zavedanja. To je bil med drugim tudi razlog za ustanovitev prvega CERT v ZDA in tudi naša naloga je spremljanje stanja v Sloveniji. Da pa bi podrobno preiskali vsak napad in lovili storilce, ni mogoče. Pri zahtevnih incidentih, kadar gre za ključno infrastrukturo (kot na primer HSE), se seveda storilci intenzivno iščejo. Za manjša oškodovanja in zelo splošne napade pa ne. Če karikiram, iluzorno je pričakovati, da se bo za oškodovanje nekaj sto evrov aktiviral celotni mednarodni pregon, ki je med drugim zelo drag. Večina storilcev tudi deluje iz držav, kjer je mednarodni pregon tako rekoč nemogoč. Najdejo pa se tudi primeri, ko so storilci blizu.

Delujemo namreč že 30 let in imamo dobro razvejano mrežo ljudi, ki prijavljajo incidente. Ko smo poleti 2023 opazili povečano število *phishing* napadov, ki so se začenjali s sporočili sms, smo stopili v kontakt z mobilnimi operaterji. Podatkov o naročnikih nam seveda ne smejo posredovati, smo jih pa vprašali, ali so omenjeni sms-i izvirali iz njihovih omrežij ali pa so imeli potvorjeno številko (*spoofing*). Ugotovili smo, da gre za dejanske stranke v omrežju in da uporabljajo predplačniške kartice SIM, ki so bile kupljene v Sloveniji. Podatke smo nato posredovali policiji, ki ima več pooblastil. Na koncu so v Mariboru aretirali štiri tuje državljane, ki so poslali okrog 50.000 sporočil.

Ko je enkrat denar nakazan, po možnosti v kriptovalutah, ko potuje skozi mešalnike (*mixer*) in pralnice denarja (*tumbler*) do različnih borz, se sled za njim izgubi. Videli smo že konkretna oškodovanja, celo do 140.000 evrov.

▶ Kaj pa preventiva?

Da, tudi to je pomemben del naših aktivnosti. Iz več virov pridobivamo podatke o stanju ranljivosti v Sloveniji. Ko se pojavi kakšna kritična, lahko sprožimo obveščanje kot v primeru nezakrpanih (*zero-day*) lukenj v Microsoftovem Exchangeu v zadnjih letih. Podatke dobimo tudi od tujih partnerjev, kot je Shadowserver Foundation, ki izvaja skeniranje interneta vsakih 24 ur. Kot nacionalni center dobimo podatke za celotno Slovenijo, ki jih nato razkosamo po operaterjih. Včasih vidimo celo, na katero domeno se nanašajo, in tedaj lahko njenega nosilca pozovemo, da namesti popravke.

▶ Kako to storite?

Dokler samo slutimo, da se bo nekaj zgodilo, lahko le opozarjamo, nimamo pa vpliva na to, kaj se zgodi na drugi strani. Rezultate pa spremljamo in potem te grafe, kako se zmanjšuje število ranljivih sistemov, pogosto kažem na predavanjih. Zanimivo je, da se število približuje ničli, a jo redko doseže.

Videli smo že konkretna oškodovanja, celo do 140.000 evrov.

▶ Storilce je torej mogoče odkriti.

Da, toda ta primer je bolj izjema kot pravilo, ker so bili storilci v Sloveniji. V trenutni geopolitični situaciji ni pričakovati, da bo pregon mednarodnega kriminala postal lažji ali da se bodo zgodile kakšne korenite spremembe.

Kar se tiče ljubeznih prevar, ki so pogoste iz Afrike, ter različnih investicijskih prevar, lahko ljudje največ storijo sami. Če nekdo obljublja zaslužek 3.000 evrov tedensko v oglasu na Facebooku, se moramo vprašati, zakaj tega posla ne zagrabijo vsi.

▶ Nekaj sistemov torej ostane ranljivih.

Da. O vzrokih lahko le ugibamo, imamo pa tri teorije. Nekatera podjetja so verjetno v stečaju ali kako drugače neoperativna in tam preprosto ni nikogar, ki bi naša elektronska sporočila sploh prebral, saj je celotna IT-ekipa že zdavnaj v drugi službi. Druga skupina so podjetja, ki nimajo javno objavljenih elektronskih naslovov, zato lahko sporočilo pošljemo le na splošni naslov info@domena.si. Kdo to bere in ali

sploh razume, kaj sporočamo, je drugo vprašanje. Tretja možnost pa je, da imajo takrat v podjetju neko drugo izredno situacijo, zato se s sporočilom nihče ne ukvarja. Morda se IT-jevci iz različnih razlogov ne morejo odzvati, morda nimajo podpore vodstva ali sredstev.

Imeli smo primer ustanove v javnem sektorju, ki smo jo obvestili o ranljivosti. Njihov odgovor je bil, da se za obvestilo zahvaljujejo in da bodo dali nadgradnjo v načrt nabave za prihodnje leto. Ampak njihova naprava sploh ni bila več podprta in zanjo popravkov ni bilo mogoče več dobiti, zato so bili izpostavljeni napadu z izsiljevalskimi virusi. Znotraj SI-CERT smo potem imeli resno debato, a ugotovili smo, da več ne moremo storiti. Mi smo izpolnili svojo odgovornost, a potrebujemo tudi sogovornika na drugi strani. Istočasno pa nas čaka še pet novih primerov, ki se jim tudi moramo posvetiti.

Iz neke ustanove v javnem sektorju so na obvestilo o ranljivosti odgovorili, da bodo nadgradnjo dali v načrt nabave za prihodnje leto.

▶ Bi potem rekli, da je situacija v javnem in zasebnem sektorju, ko govorimo o varnosti, bistveno različna? Kdo več vlaga v varnost, kdo je bolj zaščiten?

Na to je zelo težko enoznačno odgovoriti, morda lahko pogledamo povprečja. So deli javnega sektorja, kjer je za varnost zelo dobro poskrbljeno, in imamo takšne, kjer ni in je prostora za izboljšave zelo veliko. V zasebnem sektorju pa je razlika predvsem v velikosti podjetij. Velika podjetja, ki po možnosti delujejo na mednarodnih trgih, imajo običajno precej visoko stopnjo zavedanja o varnosti. Večji problem so mala in srednja podjetja, ki pogosto nimajo niti virov niti kadra.

Mi jim poskušamo namenjati čim več pozornosti, kar je zlasti pomembno pri incidentih. Takrat jim lahko pomagamo in svetujemo, kam pogledati, kje iskati podatke, katere dnevniške datoteke analizirati, kako povezati podatke z dogodki. Seveda se nikomur ne vsiljujemo, obstajajo pa zakonske zahteve.

▶ Pripravljate tudi številne kampanje.

Zadnji odmeven primer je kampanja Varni v pisarni, ki je brezplačni 30-minutni spletni tečaj, namenjen vsem zaposlenim. Zdaj pa razvijamo modul za obravnavo incidentov. Vidimo namreč, da je odzivanje težava, zlasti kaj so prvi koraki, kako pristopiti, če se zgodi.

▶ Slovenija je majhna, marsikdo se tolaži, da je nepomemben in nezanimiv za napade. Smemo tako razmišljati?

Tu gre za tri dejavnike. Prvič, spletni kriminalci se vedejo zelo oportunistično. Tarč ne izbirajo načrtno, temveč iščejo odprta vrata in v naslednjem koraku poskusijo to monetizirati. Imamo več akterjev. Ena skupina deluje s trojanci in zbira podatke o uporabnikih, ki jih potem prodajo na temnem spletu, sami pa se ne ukvarjajo z vdori. Druga skupina se ukvarja z izsiljevalskimi virusi in od te prve skupine kupujejo podatke za dostop do omrežij. Nekoč je bil najpogostejši vektor oddaljeni dostop v Windows (RDP), danes pa se napadi zgodijo prek dostopa zaposlenega do VPN. Tu pomaga, da imamo vključeno dvostopenjsko preverjanje identitete.

Drugi dejavnik je položaj naše države, saj smo člani EU in Nata. Ker smo majhni, imamo tudi manj virov za zaščito infrastrukture v državi, zato smo zanimivi kot vstopna točka. Tu je pomembno, da je naša zaščita res na nivoju, kar budno gledajo tudi naši zavezniki.

Tretji dejavnik pa je ravno nasproten, in sicer pri izsiljevalskih napadih nam majhnost pomaga. V Sloveniji nimamo veliko podjetij, ki bi bila sposobna ali pripravljena plačati milijonske odkupnine. Izsiljevalci zato raje napadajo velike multinacionalke v tujini, kjer lahko zaslužijo več. To ne pomeni, da pri nas izsiljevalskih napadov ni, so pa v upadu. Pred leti smo jih imeli od pet do šest na mesec, zdaj tri do štiri. Ker so naša podjetja manjša, so odkupnine nižje, tja do 20.000 evrov. Tarče se tudi spreminjajo. V zadnjih tednih so v tujini popularne tarče trgovske verige, denimo Marks & Spencer v Veliki Britaniji, nekaj indicev kaže tudi na napad na Eurospin na Hrvaškem.

▶ Se v podjetjih zaradi tega bolj zavedajo pomena varnosti?

V večjih podjetjih se tega zavedajo, kar vidimo zlasti ob medijskih odmevnih incidentih. Tedaj se obračajo na nas z vprašanji po priporočilih in predlogih. Tudi tisti, ki doslej niso bili zavezanci po zakonu, pa bodo to postali po novem zakonu, kažejo pristen interes in pripravljenost za sodelovanje. Situacija je boljša kot pred desetimi leti, zagotovo. Hkrati pa danes mnogo več poslujemo prek interneta kot pred desetimi leti, naše življenje je prepleteno z njim. Počasi so se tudi vodstva podjetij zavedela, da so potrebne investicije. V novem zakonu smo tudi predlagali, da za varnost niso odgovorni le vodje informacijske varnosti (*chief information security officer*), temveč da je odgovorno tudi vodstvo, ki mora ekipi za kibernetsko varnost zagotoviti vire, da lahko opravlja svoje delo. ◀

Virusi, črvi, »rootkiti«, »backdoori«, trojanci

Zlonamerna programska oprema, znana tudi kot malware, se pojavlja v različnih oblikah, od virusov in črvov do trojanskih konjev in izsiljevalske programske opreme. Vsaka vrsta ima svoje posebnosti, načine širjenja in učinke, vendar jim je skupno to, da delujejo brez vednosti uporabnika ter pogosto povzročajo finančno in podatkovno škodo.

Matej Šmid

Virus

Računalniški virus je programska oprema, običajno skrita znotraj drugega na videz neškodljivega programa, ki se lahko kopira in vstavi v druge programe ali datoteke ter običajno izvaja škodljivo dejanje (npr. uničenje podatkov).

Najpogosteje se širi ob pomoči uporabnika, ki klikne na program ali dokument in s tem sproži okužbo. Program ali dokument se lahko popolnoma pravilno odpre in/ali pokaže, v ozadju pa se sproži zlonamerna programska koda, ki sproži okuženje in nadaljnje širjenje. Ključna obramba pred vsako neželeno programsko opremo je torej uporabnika naučiti: »Ne klikaj ničesar, kar ti ni znano!«

▶ **Primera:** ILOVEYOU (2000) je bil eden najbolj uničujočih virusov, razširjen prek e-pošte. Drugi primer je Melissa (1999), ki je na kolena spravil številne e-poštne strežnike.

Črv (*worm*)

Črv je samostojna zlonamerna programska oprema, ki se aktivno prenaša prek omrežja in tako v druge računalnike. Kopira se samodejno, ne da bi pri tem spremenil oziroma okužil druge datoteke na sistemu. Virus za svojo širitev in okuženje potrebuje uporabnika, ki zažene okuženo programsko opremo ali operacijski sistem, medtem ko se črv širi sam.

▶ **Primera:** WannaCry (2017) je črv, ki je šifriral datoteke in zahteval odkupnino, SQL Slammer (2003) pa je že v nekaj minutah ohromil internetni promet.

Trojanski konj

Trojanski konj se lažno predstavlja kot običajen, neškodljiv program ali pripomoček, da žrtev nagovori k namestitvi. Običajno vsebuje skrito programsko kodo, ki se aktivira ob zagonu aplikacije. Ime izhaja iz starogrške zgodbe o trojanskem konju, ki je omogočil skrivni vdor v mesto Troja.

▶ **Primera:** Zeus Trojan (2007) je bil namenjen kraji bančnih podatkov, Emotet (2014) se je začel kot bančni trojanec, kasneje pa postal ena najnevarnejših platform za širjenje zlonamerne kode.

Dropperji

Dropperji so podvrsta trojancev, katerih edini namen je dostaviti drugo zlonamerno programsko opremo v sistem. Njihov cilj je izogniti se zaznavi z uporabo prikritega pristopa in majhne začetne velikosti. *Dropperja* ne gre zamenjevati z *loaderjem* ali *stagerjem*, ki zgolj naloži razširjeno zlonamerno kodo (npr. prek dinamičnega nalaganja knjižnic) v pomnilnik. *Dropper* preprosto prenese dodatno zlonamerno programsko opremo v sistem.

▶ **Primer:** Zgoraj omenjeni Emotet (2014) je pogosto služil kot *dropper* za druge trojance, kot sta TrickBot in Ryuk.

Rootkiti

Ko je zlonamerna programska oprema nameščena v sistem, je ključno, da ostane skrita pred zaznavanjem. Programski paketi, znani kot *rootkiti*, omogočajo to skrivanje s spremembami v gostiteljskem operacijskem sistemu, tako da je zlonamerna koda pred uporabnikom popolnoma skrita. *Rootkiti* lahko preprečijo, da bi bil škodljiv proces viden na seznamu procesov sistema, največkrat pa operacijski sistem njegovih datotek sploh ne prikaže.

▶ **Primer:** Sony je na svoje glasbene cedeje namestil BMG Rootkit (2005), ki je bil namenjen preprečevanju njihovega kopiranja, hkrati pa je podjetju poročal o glasbenih navadah uporabnika. Kmalu so se pojavili drugi trojanci in črvi, ki so zlorabili nameščeni BMG Rootkit.

Zadnja vrata (*backdoor*)

Zadnja vrata so splošen izraz za program, ki napadalcu omogoča vztrajno, nepooblaščeno oddaljeno dostopanje do računalnika žrtve brez njene vednosti. Napadalec običajno uporabi drugo obliko napada (trojanski konj, črv ali virus), da zaobide overitvene mehanizme in namesti aplikacijo z zadnjimi vrati prek interneta. Zadnja vrata so lahko tudi posledica programskih napak v zakoniti programski opremi, ki jih napadalci izkoristijo za dostop do računalnika ali omrežja žrtve.

▶ **Primer:** Back Orifice (1998) je omogočal popoln oddaljeni nadzor nad Windows računalniki brez vednosti uporabnika.

Izsiljevalska programska oprema (*ransomware*)

Izsiljevalska programska oprema uporabniku prepreči dostop do datotek, dokler ta ne plača odkupnine. Obstajata dva načina, kako do to doseči, in sicer kripto *ransomware* in zaklepni *ransomware*. Zaklepni le zaklene sistem, medtem ko kripto *ransomware* šifrira vsebino. Programi, kot je CryptoLocker, varno šifrirajo datoteke in jih dešifrirajo šele po plačilu visoke odkupnine.

Zaklepni sistemi, denimo, blokirajo zaslone naprav z Windows ali Android z lažno obtožbo (npr. o dostopu do nezakonite vsebine) ter žrtve poskuša prestrašiti in napeljati k plačilu.

Šifrirni *ransomware*, kot že ime pove, šifrira vse datoteke na okuženem računalniku. Nato prikaže sporočilo, da so datoteke zaklenjene in da mora uporabnik plačati za dostop (običajno v bitcoinih). Šifrirni algoritmi so navadno tako močni, da druge rešitve razen restavracije vseh podatkov iz varnostnih kopij običajno ni.

▶ **Primera:** CryptoLocker (2013) je bil eden prvih kripto *ransomware* programov, WannaCry (2017) pa je v nekaj urah okužil na stotisoče računalnikov po svetu.

Klik prevara

Zlonamerna programska oprema se uporablja tudi za ustvarjanje prihodka s kliki – ustvarjanje vtisa, da je uporabnik kliknil oglasno povezavo na spletni strani, čeprav tega ni naredil. Ker vsak klik lastniku oglasa prinaša denar, je na ta način zagotovljen finančni prihodek. Leta 2012 je bilo ocenjeno, da je 60–70 odstotkov vse aktivne zlonamerne programske opreme uporabljalo neko obliko klik prevare in da je bilo 22 odstotkov vseh klikov na oglase lažnih.

▶ **Primer:** Clickbot.A (2006) je bil botnet (omrežje okuženih računalnikov), sestavljen iz več deset tisoč okuženih računalnikov, ki so samodejno klikali oglase.

Botnet

Botnet (izraz izhaja iz *robot network*) je omrežje računalnikov, okuženih z zlonamerno programsko opremo, ki jih napadalec na daljavo nadzoruje brez vednosti uporabnikov. Okuženi računalniki, imenovani »zombi«, se lahko uporabljajo za izvajanje usklajenih napadov, kot so pošiljanje neželene pošte (*spam*), porazdeljeni napadi za onemogočanje storitev (DDoS), širjenje zlonamerne kode ali klik prevare. Botneti pogosto vključujejo na tisoče ali celo milijone naprav in predstavljajo eno največjih groženj za kibernetsko varnost.

▶ **Primer:** Mirai (2016) je znan botnet, ki je izkoriščal nezavarovane naprave IoT (spletne kamere) in povzročil enega največjih napadov DDoS doslej, vključno z ohromitvijo ponudnika storitev DNS Dyn. To je za nekaj časa izklopilo celo spletne velikane, kot so Twitter, Netflix in Reddit.

Vohunska programska oprema (*spyware*)

Programi, namenjeni spremljanju uporabnika, prikazovanju neželenih oglasov ali preusmerjanju dobičkov od partnerskega trženja, se imenujejo *spyware*. Ta se ne širi kot virusi, temveč se običajno namesti z izkoriščanjem varnostnih lukenj ali skrito skupaj z drugo nameščeno programsko opremo.

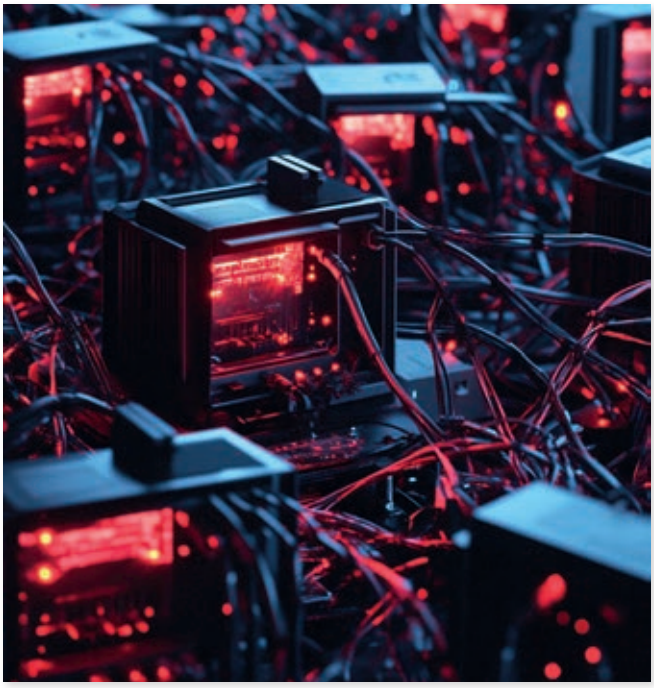
▶ **Primer:** FinFisher (od 2011 dalje) je, denimo, komercialna *spyware* oprema, ki jo uporabljajo vladne agencije. Najbolj znana tovrstna vohunska oprema danes pa je izraelski Pegasus.

Potencialno neželeni programi (PUP – *Potentially Unwanted Programs*)

Potencialno neželeni programi (PUP) so aplikacije, ki se, čeprav jih uporabniki pogosto namenoma prenesejo, štejejo za neželene. Mednje spadajo vohunska programska oprema (*spyware*), oglaševalska programska oprema (*adware*) in goljufivi klicalniki (*fraudulent dialers*).

Veliko varnostnih programov uvršča nepooblaščene generatorje licenčnih ključev (t. i. *keygeneratorje*) med PUP, čeprav ti pogosto poleg svoje navidezne funkcije vsebujejo tudi pravo zlonamerno programsko opremo. Ocenjuje se, da bi lahko kar 55 odstotkov takih generatorjev vsebovalo zlonamerno programsko opremo in da približno 36 odstotkov škodljivih *keygeneratorjev* protivirusni programi sploh ne zaznajo.

▶ **Primer:** InstallCore (od 2010 dalje) je pogosto skrit v »brezplačnih« programih in namešča neželene aplikacije. ◀



Začetki digitalne pandemije

Zgodovina računalniških virusov ni zgolj zgodba o kodi, ki se je izmuznila nadzoru. To je pripoved o človeški radovednosti, domiselnosti ter tudi o nepredvidenih posledicah razvoja tehnologije. V svetu, kjer so bili prvi računalniki veliki kot sobe in dostopni le redkim izbrancem v raziskovalnih ustanovah, si je le malokdo predstavljal, da bodo ti mogočni stroji nekoč vsakdanji in ranljivi kot povsem običajni organizmi. Še manj pa, da bodo ti organizmi zbolevali. In vendar se je zgodilo točno to – računalniki so se okužili, zboleli, širili digitalne bolezni in postali prenašalci nečesa, kar je danes postalo temeljni izziv informacijske varnosti – zlonamerne kode.

Na začetku ni bilo nič »zlobnega«. Prvi računalniški virusi so bili bolj eksperiment kot grožnja, bolj igra kot napad. Bili so nekakšni digitalni duhci v stroju – dokaz, da je program sposoben samorazmnoževanja, seljenja, obstoja brez posredovanja človeka. Creeper, prvi znani primer takšnega programa iz leta 1971, ni želel škodovati – na zaslonu je pustil le hudomušno sporočilo. A že ta zgodnji poskus je bil kot prvi kašelj v množici: dokaz, da nekaj lahko uide nadzoru.

Sčasoma so se nameni spremenili. Če so prvi virusi služili demonstracijam in eksperimentom, so poznejši nastali zaradi nabora različnih motivov – od hekerskega dokazovanja znanja in prestiža do odkrite zlobe, vohunstva in kibernetskega kriminala. Razvijalci virusov so postali nevidni nasprotniki na vedno bolj sofisticiranem bojišču, kjer črte med radovednostjo, sabotažo in vojno postajajo vse bolj zabrisane.

Ni nepomembno, da se je razvoj virusov odvijal vzporedno z razvojem računalništva samega. Vsaka nova faza digitalizacije – od osebnih računalnikov do interneta, od e-pošte do pametnih telefonov, od oblačnih storitev do naprav interneta stvari – je odprla nova vrata. In virusi so jih znali najti. Ko se je internet začel širiti po domovih, so postali virusi globalni; ko je z e-pošto prišla hitrost, so postali bliskoviti; ko je v digitalni svet vstopil denar, so postali dobičkonosni.

Virus ni več le metafora. Postal je digitalna entiteta, ki ima – podobno kot biološki virus – svojo genetiko (kodo), svoj cikel širjenja, celo svojo evolucijo. Nekateri ostanejo nespremenjeni leta, drugi se razvijejo v nove različice, odporne na protivirusne ukrepe. Obstajajo tihi in neopazni vohuni, obstajajo destruktivni saboterji ter izsiljevalci in celo politiki v preobleki vrstice kode. In vsi živijo znotraj ekosistema, ki ga ustvarjamo vsak dan s svojo povezanostjo, brezskrbnostjo in odvisnostjo od digitalnega sveta.

Prvi računalniški virusi so bili bolj eksperiment kot grožnja, bolj igra kot napad.

Poglejmo skoraj pet desetletij računalniške virologije – od začetnih, naivnih poskusov, prek svetovnih epidemij do današnjih sofisticiranih vohunskih operacij. Časovnica razvoja računalniških virusov ni zgolj seznam zlonamernih programov – je zgodovina človeškega odnosa do tehnologije, zgodovina moči, nadzora in odpora. In kot bomo videli, je to zgodovina, ki se še zdaleč ni končala.

Ko pregledujemo posamezne prelomnice digitalne okužbe, se ne sprašujemo več, *ali* bodo virusi še prihajali – temveč *kdaj, kje* in *kako.* Svet virusa je postal del našega digitalnega vsakdana. In morda je edini pravi obrambni mehanizem – znanje. Zato pojdimo na začetek. V čas, ko je bil virus še šala. ◀

Virusi skozi čas

1971

Sistem Creeper, eksperimentalni samorazmnožujoči se program, je okužil računalnike DEC PDP-10 z operacijskim sistemom TENEX. Prek Arpaneta (predhodnik interneta) se je prekopiral na oddaljeni sistem, kjer se je izpisalo sporočilo »Jaz sem Creeper, ulovi me, če me moreš!«. Kasneje so naredili program Reaper, da bi Creeperja izbrisal.

1974

Napisan je bil Virus Rabbit (ali Wabbit). Deluje tako, da naredi več kopij samega sebe na enem računalniku (ime *rabbit* (zajec) je dobil zaradi hitrosti, s katero to počne), dokler ne preobremeni sistema. To povzroči upočasnitev delovanja, nato sistem doseže prag zmogljivosti in se sesuje.

1975

Program ANIMAL je bil namenjen računalniku UNIVAC 1108. Uporabniku je zastavil več vprašanj, da bi poskušal uganiti, na katero žival uporabnik misli. Hkrati je v vsaki mapi, do katere je imel trenutni uporabnik dostop, program PERVADE ustvaril kopijo sebe in programa ANIMAL. Ko so uporabniki odkrili igro, se je razširil po večuporabniških sistemih UNIVAC, prek izmenjave pomnilnih trakov pa tudi na druge računalnike. Čeprav ni bil škodljiv, »Pervading Animal« predstavlja prvega »trojanskega konja«.

1982

Program z imenom Elk Cloner je bil namenjen računalniku Apple II, ustvaril ga je srednješolec, kot potegavščino. Elk Cloner je povzročil prvi večji izbruh računalniškega virusa v zgodovini.

1986

Izdan je bil virus Brain, ki okuži zagonski sektor na disketi/disku. Brain velja za prvi virus, združljiv z računalniki IBM PC, in je odgovoren za prvo epidemijo takšnega virusa. Znan je tudi pod imeni Lahore, Pakistani, Pakistani Brain in Pakistani flu, saj sta ga ustvarila 19-letni pakistanski programer Basit Farooq Alvi in njegov brat Amjad Farooq Alvi v mestu Lahore v Pakistanu.

1987

Pojavi se virus SCA, virus zagonskega sektorja za računalnike Amiga.

1988

Na Univerzi v Torinu je bil odkrit virus Ping-Pong (imenovan tudi Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A ali VeraCruz), zagonski virus za PC/MS-DOS. Prikazoval je »žogico«, ki je poskakovala po zaslonu tako v besedilnem kot v grafičnem načinu.

Drugi podoben virus je bil Cascade, sicer napisan v zbirniku. Okuževal je datoteke s končnico .COM in povzročil, da je besedilo na zaslonu začelo »padati« navzdol in se kopičiti na dnu zaslona. Bil je poseben tudi zato, ker je za prikrivanje pred zaznavo uporabljal šifrirni algoritem.

1992

Virus Michelangelo naj bi po napovedih medijev 6.marca povzročil digitalno apokalipso, ko naj bi bili diski milijonov računalnikov izbrisani. Kasnejše ocene škode so pokazale, da so bili dejanski učinki minimalni.

1995

Ustvarjen je prvi makro virus z imenom »Concept«. Napadal je dokumente Microsoft Word.

1996

Računalnike z Linuxom napade Staog, prvi virus za ta operacijski sistem.

1998

Pojavi se prva različica virusa CIH. Gre za prvi znani virus, ki je bil sposoben izbrisati vsebino BIOS-a v pomnilniku flash.

Narejen je bil virus Melissa, ki je napadal sisteme na osnovi Microsoft Worda in Outlooka ter povzročil veliko omrežnega prometa.

2000

Črv ILOVEYOU (znan tudi kot Love Letter, VBS ali Love Bug) je bil računalniški črv, napisan v jeziku VBScript, ki je za širjenje uporabljal tehnike socialnega inženiringa. V nekaj urah po izidu je okužil milijone računalnikov z operacijskim sistemom Windows po vsem svetu.

2001

Virus Anna Kournikova močno prizadene e-poštne strežnike, saj pošilja sporočila na vse naslove, ki jih najde v imeniku poštnega programa Microsoft Outlook. Njegov avtor, Jan de Wit, je bil obsojen na 150 ur družbenokoristnega dela.

Narejen je bil črv Code Red, ki napade razširitev Index Server ISAPI v spletnem strežniku Microsoft Internet Information Services (IIS). Popolnoma prenovljena različica, Code Red II, se začne agresivno širiti po Microsoftovih sistemih, predvsem na Kitajskem.

2003

Črv SQL Slammer, znan tudi kot Sapphire in Helkern, napade ranljivosti v Microsoft SQL Server in MSDE ter postane najhitreje širjen črv vseh časov. Le 15 minut po prvi okužbi povzroči ogromne motnje pri dostopu do interneta po vsem svetu.

Črv Blaster, znan tudi kot Lovesan, se hitro širi z izkoriščanjem ranljivosti v sistemskih storitvah na računalnikih Windows.

Odkrit je črv Nimda, ki se širi na različne načine, vključno z izkoriščanjem ranljivosti v operacijskem sistemu Microsoft Windows ter prek zadnjih vrat, ki jih je za seboj pustil črv Code Red II.

2004

Pojavi se črv MyDoom, ki trenutno drži rekord za najhitreje razširjenega črva prek e-pošte. Najbolj znan je po izvedbi porazdeljenega napada za onemogočanje dostopa (DDoS) na spletno stran www.sco.com, ki je pripadala podjetju The SCO Group.

2005

Razkrito je bilo, da so glasbeni cedeji založniškega velikana Sony BMG vsebovali zaščitni *rootkit*, ki je bil nameščen namerno in prikrito. Ta je ustvarjal ranljivosti na okuženih računalnikih, zaradi katerih so ti postali dovzetni za okužbe z virusi in s črvi.

2006

Odkrito je prvo zlonamerno programje za Mac OS X – trojanski konj z nizko stopnjo grožnje, znan kot OSX/Leap-A ali OSX/Oompa-A.

2008

Črv Conficker okuži med 9 in 15 milijoni Microsoftovih strežniških sistemov z različicami od Windows 2000 do Windows 7 Beta. Med prizadetimi so francoska mornarica, britansko ministrstvo za obrambo (vključno s kraljevo mornarico in podmornicami), nemška vojska, norveška policija in bolnišnice v britanskem Sheffieldu. Microsoft razpiše nagrado v višini 250.000 dolarjev za informacije, ki bi pripeljale do prijetja avtorjev črva.

2010

Zaznan je trojanski virus Stuxnet. Danes obstaja konsenz, da je bil zasnovan za napad na iranske jedrske objekte, najverjetneje pri ameriški agenciji NSA in izraelskem Mossadu. Uporablja veljaven certifikat podjetja Realtek.

2013

Razširi se trojanski konj CryptoLocker. Ta zašifrira datoteke na uporabnikovem disku in nato zahteva odkupnino za pridobitev ključa za dešifriranje. V naslednjih mesecih se pojavi še več posnemovalcev te izsiljevalske programske opreme.

2016

Ransomware Locky, s prek 60 izpeljankami, se razširi po Evropi in okuži več milijonov računalnikov. Na vrhuncu širjenja je bilo samo v Nemčiji okuženih več kot 5.000 računalnikov na uro!

Novinarji in raziskovalci razkrijejo obstoj vohunske programske opreme Pegasus, ki jo je razvilo in razširilo izraelsko zasebno podjetje. Ta zlonamerna programska oprema lahko prek nerazkritih varnostnih lukenj (»*0-day* ranljivosti«) brez posredovanja uporabnika okuži telefone Apple iOS in Google Android. Ko je nameščena, prestreza in pošilja osebne podatke, sledi lokaciji, snema z mikrofonom in s kamero. Raziskave kažejo, da jo še danes uporabljajo različne vladne agencije – za vohunjenje za novinarji, politiki, aktivisti in drugimi. Denimo v Srbiji.

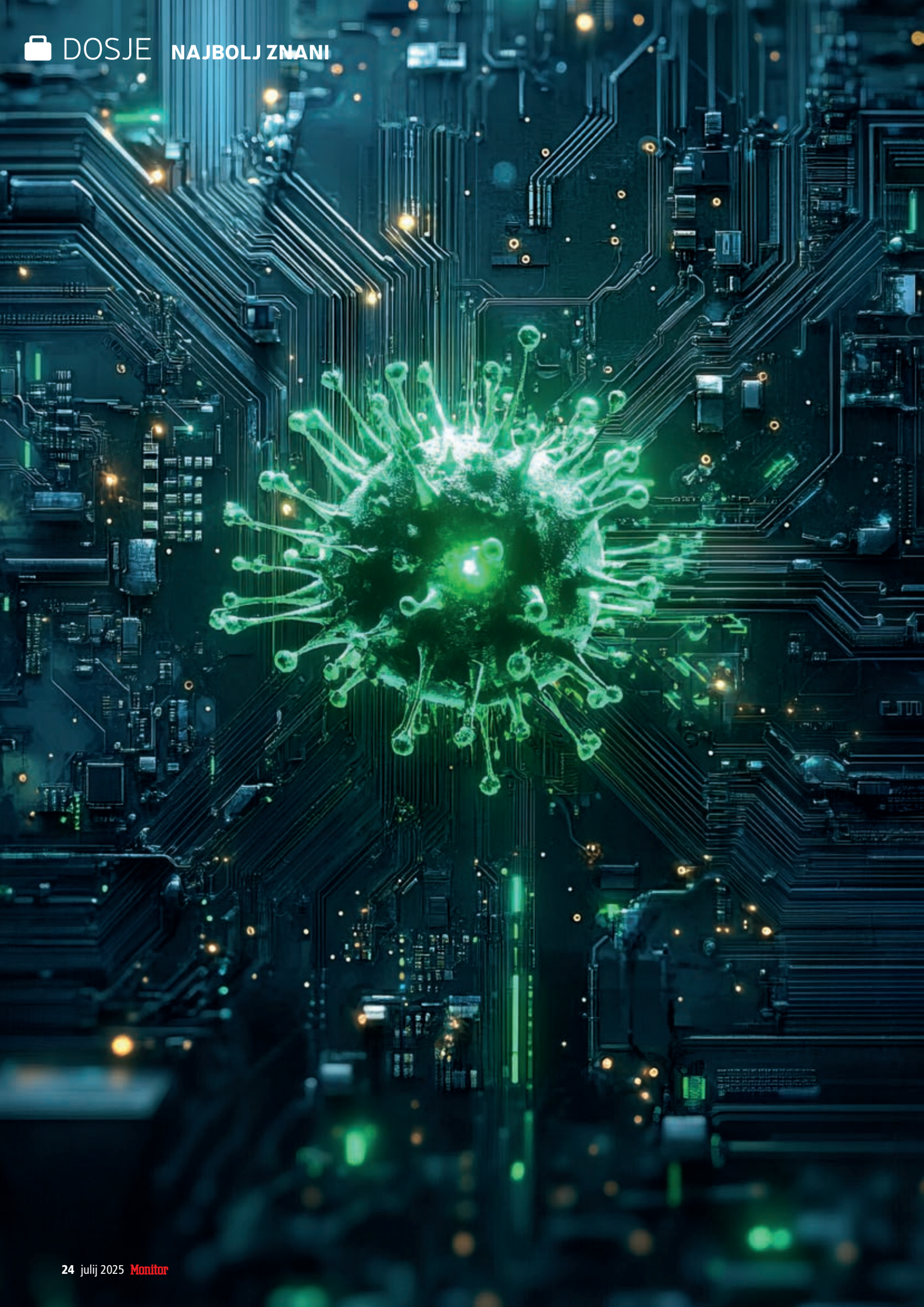
Zlonamerna programska oprema Mirai ob pomoči okužb naprav interneta stvari (IoT) oziroma spletnih kamer izvede nekatere izmed najmočnejših napadov DDoS doslej. Med drugim je 20. septembra 2016 s prometom 620 Gb/s napadla spletno stran Krebs on Security, še močnejši napad pa je zabeležil evropski ponudnik oblaka OVH – 1 Tb/s!

2017

Globalno se razširi izsiljevalska programska oprema WannaCry. Za širjenje izkorišča ranljivosti iz orodja za vdiranje NSA, razkritega v letu 2016. Kmalu po začetku okužb varnostni raziskovalec iz Združenega kraljestva skupaj z drugimi aktivira t. i. stikalo (*kill switch*), ki zaustavi začetni val širjenja.

Podobno se je razširil tudi napad virusa Petya. Raziskovalci podjetja Symantec so razkrili, da uporablja ranljivost EternalBlue – enako kot WannaCry.

Vir: Wikipedija



Najbolj znani in zanimivi virusi za PC in mac

Ko govorimo o računalniških virusih, večina najprej pomisli na računalnike z operacijskim sistemom Windows. Z dobrim razlogom – ti sistemi že desetletja predstavljajo glavno tarčo kibernetskih napadov, saj jih uporablja največ uporabnikov po svetu. Toda ta pogostost napadov je ustvarila tudi mit – mit, da so Applovi računalniki imuni. Mac naj bi bil svetla izjema, otok varnosti sredi digitalnega oceana groženj. Ta predstava je obstajala tako dolgo in bila tako uspešno zasidrana v kolektivno zavest, da jo mnogi še danes jemljejo kot samoumevno.

V resnici pa ni šlo za imuniteto, temveč za nerazmerje v zanimanju. Zgodovinsko gledano so pisci zlonamerne kode svoje napade vedno usmerjali tja, kjer je bila večina – na peceje. A tudi na macih so se pojavljali virusi. Sprva redki, potem postopoma bolj prefinjeni, vse dokler ni postalo jasno, da noben sistem ni nedotakljiv. Tudi mac ne. In čeprav so njegovi uporabniki dolgo verjeli v lastno tehnično nedolžnost, so v nekem trenutku morali priznati, da ni dovolj le izbira prave blagovne znamke, da bi izognili nevarnosti.

Čeprav je macOS dolga leta slovel kot varnejši sistem, se je pokazalo, da vendarle ni neprebojen.

Na naslednjih straneh ponujamo dva prispevka. Prvi predstavlja najzanimivejše primere virusov, ki so zaznamovali osebne računalnike z operacijskim sistemom Windows. Od zgodnjih dni, ko so virusi potovali po disketah, do sodobnih kibernetskih napadov z milijardnimi posledicami. Gre za izjemno raznolike primere – nekateri so delovali kot samorazmnoževalni mehanizmi, drugi kot orodja državnih obveščevalnih služb. Vsem pa je skupno, da so bili prelomni. In vsi povzročili finančno škodo.

Drugi članek pa razbija mit o nedotakljivosti Applovih naprav. Čeprav je macOS dolga leta slovel kot varnejši sistem – delno zaradi tehnične zasnove, delno pa zaradi nadzora nad programsko in strojno opremo –, se je z vsako novo generacijo virusov pokazalo, da tudi ta obrambni zid ni neprebojen. MacMag, Leap.A, Flashback in celo ranljivosti na ravni procesorjev razkrivajo, da tudi v okolju, ki se zdi zaprto in nadzorovano, lahko pride do vdora. Prav ti primeri so še posebej zanimivi, saj pogosto delujejo bolj prikrito, zahtevajo sodelovanje uporabnika in izkoriščajo zaupanje, ki ga ta sistem tradicionalno uživa. In prav zato so nevarni – ker pridejo skozi vrata, ki smo jih sami odprli.

Ti dve zgodbi – o virusih za PC in za mac – nista ločeni, temveč vzporedni. Kažeta, kako se grožnje razvijajo glede na okolje, kako napadalci iščejo nove poti in kako se vsak mit o varnosti prej ali slej sooči z realnostjo. Osredotočili se bomo na tiste viruse, ki so bili najzanimivejši, najpametnejši, najvplivnejši. Na viruse, ki niso zgolj povzročili škode, temveč so preoblikovali našo predstavo o tem, kaj vse je v digitalnem svetu mogoče. ◀

Virusi za PC

Računalniški virus je skupek navodil, ki se prilepijo na druge računalniške programe, in čeprav ti še naprej opravljajo svoje običajne naloge, hkrati v ozadju izvršujejo tudi ukaze virusa. Ta se aktivira, ko je naložen v delovni pomnilnik računalnika, in nato usmeri gostiteljski program, da njegovo kodo prenese v druge programe in datoteke ter jih okuži. Sposobnost virusa, da se razmnožuje, omogoča njegovo širjenje na druge računalnike prek pomnilniških naprav, omrežij ali interneta. V hujših primerih virusi povzročijo ogromno škodo v le nekaj minutah ali urah, včasih pa celo zaklenejo sistem, dokler ni plačana odkupnina.

Dominik Cigala

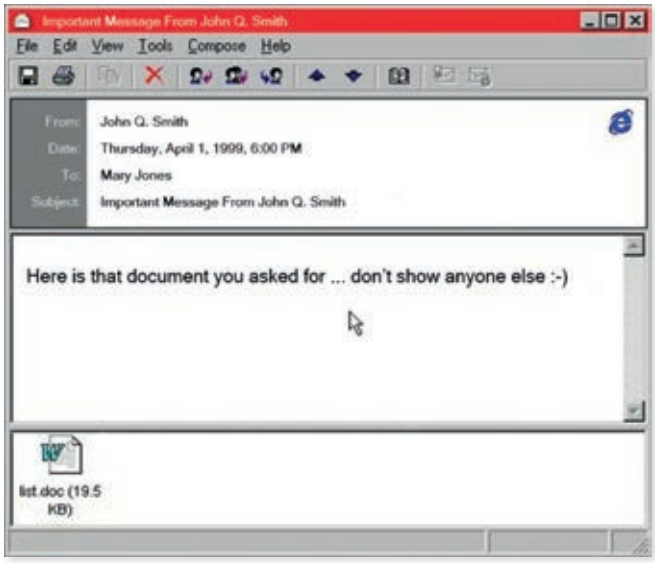
Melissa

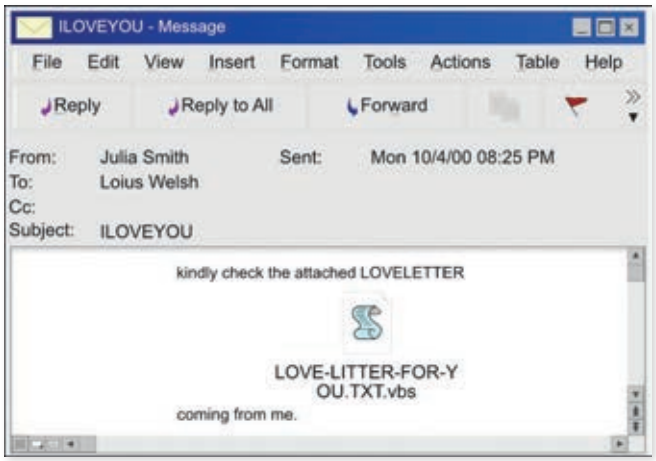
Leto: 1999
Način širjenja: Priponka, Microsoft Word
Ocenjena škoda: 80 milijonov USD

Pred 20 leti je svet interneta doživel eno prvih velikih opozoril o nevarnosti kibernetskih napadov. Virus Melissa, ki se je pojavil marca 1999, je s svojo neverjetno hitrostjo širitve in obsegom povzročene škode razkril temnejšo plat digitalne povezanosti. To je bil mejnik, ki je spodbudil razvoj sodobnih varnostnih sistemov in opozoril uporabnike na tveganja nenadzorovanega odpiranja elektronske pošte.

Programer David Lee Smith je izrabil račun AOL in na spletni forum alt.sex objavil datoteko, ki naj bi vsebovala brezplačna gesla za dostop do plačljivih spletnih strani za odrasle. Ko so uporabniki prenesli in odprli dokument v programu Microsoft Word, se je sprožil makro virus, ki je prek Microsoftovega Outlooka poslal okuženo sporočilo na prvih 50 naslovov v uporabnikovem imeniku. Sporočila so bila zasnovana tako, da so vzbudila radovednost, na primer z naslovi datotek kot so sexxxy.jpg, naked wife in s pripisi v stilu: »Tukaj je dokument, ki si ga želel. Nikomur ga ne pokaži ;-).« Tako se je virus širil kot avtomatizirano verižno pismo, a ne zaradi želje po kraji denarja ali uničenju podatkov. Melissa ni izbrisala datotek, toda kljub temu je povzročila ogromno škodo. Več kot 300 podjetij in vladnih ustanov po svetu je moralo začasno ustaviti delovanje svojih poštnih strežnikov, med njimi tudi Microsoft in ameriška mornarica. Ocenjuje se, da je bilo motenih približno milijon elektronskih računov, škoda pa je dosegla kar 80 milijonov dolarjev. Zahvaljujoč sodelovanju FBI, AOL in organov pregona iz New Jerseyja je bil Smith hitro odkrit in aretiran. Priznal je krivdo, bil obsojen na 20 mesecev zapora ter kaznovan z denarno kaznijo 5.000 dolarjev. Melissa, poimenovana po eksotični plesalki s Floride, ni bila najnevarnejši virus vseh časov, a morda je bila najbolj človeški. Pokazala nam je, da smo prav mi tisti člen v verigi, ki omogoči ali prepreči širjenje digitalnega kaosa. In čeprav je od leta 1999 minilo že precej let, je njeno sporočilo še vedno aktualno – varnost se začne pri posamezniku.

▽ **Makro virus Melissa je med prvimi izkoriščal človeško naivnost in radovednost.**





△ **Virus ILOVEYOU je povzročil, da se je širša javnost začela zavedati, da lahko že en sam klik vodi do ogromnih težav.**

ILOVEYOU

Leto: 2000
Način širjenja: Priponka
Ocenjena škoda: 10–15 milijard USD

Virus ILOVEYOU je eden najbolj razvpitih primerov računalniških napadov, ki je leta 2000 povsem pretresel svet. Njegov izbruh se je začel 4. maja, ko sta ga v obtok poslala študenta s Filipinov. Širil se je prek elektronske pošte, skrit v priponki z zavajajočim imenom LOVE-LETTER-FOR-YOU.txt.vbs. Uporabniki so zaradi radovednosti priponko množično odpirali, saj je naslov sporočila vzbujal čustva in vabil k ogledu navideznega ljubezenskega pisma. Ko je bil aktiviran, je virus začel svojo rušilno pot. Najprej je prepisal ključne sistemske datoteke, kar je kasneje pogosto povzročilo sesutje operacijskega sistema, nato pa se je samodejno razposlal vsem stikom iz uporabnikovega imenika.

Zaradi izjemno učinkovite metode širjenja je v nekaj urah dosegel globalne razsežnosti in prizadel milijone računalnikov po svetu.

Posledice napada so bile izjemno obsežne. Po ocenah strokovnjakov je povzročil za okoli 15 milijard dolarjev gospodarske škode. Moteno je bilo poslovanje številnih podjetij, posamezniki so izgubljali pomembne podatke, predvsem pa se je v javnosti razširilo globoko nezaupanje v digitalno varnost. Mnogi so se prvič srečali s pojmom zlonamerne kode, ki se lahko skriva v vsakdanjem elektronskem sporočilu, in spoznali, kako ranljiva je njihova digitalna zasebnost. Virus ILOVEYOU je predstavljal veliko prelomnico v odnosu do spletnih groženj. Nenadoma se je širša javnost začela zavedati, da lahko že en sam klik vodi do ogromnih težav. Strokovnjaki so začeli opozarjati na pomen previdnosti pri odpiranju priponk, pojavila se je potreba po širši

MyDoom je starodavno idejo verižnih pisem digitaliziral in jo opremil z zlonamerno kodo, ki se je samodejno širila.

uporabi protivirusne programske opreme in večjem ozaveščanju o digitalni varnosti.

Čeprav danes ni več aktiven, je njegov vpliv dolgoročen. Postal je simbol nevarnosti, ki jo predstavljajo digitalne grožnje, hkrati pa je spodbudil razvoj številnih varnostnih ukrepov, ki so danes postali standardni del digitalnega vsakdana. Še vedno nas opozarja, kako pomembno je, da znamo prepoznati nevarnosti, se iz njih učimo in se z njimi ustrezno spoprijemamo.

Klez

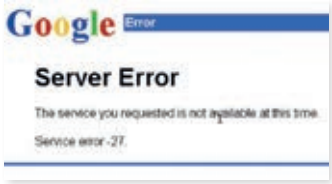
Leto: 2001
Način širjenja: Priponka
Ocenjena škoda:
19,8 milijarde USD

Računalniški črv Klez se je prvič pojavil oktobra 2001 na Kitajskem. Gre za zlonamerno programsko opremo, zasnovano za širjenje prek elektronske pošte, ki deluje na operacijskih sistemih Microsoft Windows. Njegova glavna tarča so bile ranljivosti v prikazovalnem mehanizmu Trident brskalnika Internet Explorer, ki se je uporabljal tudi v programih Outlook in Outlook Express. Virus Klez je datoteka v formatu Windows PE EXE, velika približno 65 KB. Ko uporabnik odpre okuženo elektronsko pošto, bodisi prek samodejnega izvajanja kode HTML ali ročnega odpiranja priponke, se črv aktivira. Nato pregleda računalnik za e-poštne naslove in se samodejno pošlje naprej. Priponka, ki vsebuje črva, je pogosto predstavljena kot posodobitev ali celo zdravilo proti samemu virusu Klez. Kasnejše različice črva so še dodatno otežile identifikacijo okuženega sistema, saj so za pošiljanje uporabljale naključno izbrane e-poštne naslove iz imenika, kar je povzročilo zmedo pri ugotavljanju pravega izvora virusa. Poleg tega so nekateri primerki pošiljali tudi druge datoteke iz okuženega računalnika, kar je povzročilo resne kršitve zasebnosti. Največja nevarnost Kleza pa je bila njegova sposobnost, da je nenehno spreminjal svojo programsko kodo. Postal je tako imenovani polimorfni virus. To pomeni, da se je znal prilagoditi in izmikati zaznavi protivirusnih programov, kar je močno otežilo njegovo odstranjevanje. Poleg tega so številni kibernetski kriminalci ustvarili njegove različice, zaradi česar je postal ena najbolj trdoživih in kompleksnih digitalnih groženj svojega časa.

MyDoom

Leto: 2004
Način širjenja: Množično pošiljanje po e-pošti + odprta vrata v operacijskem sistemu
Ocenjena škoda:
38 milijard USD

Skoraj tri leta po Klezovem pohodu se je 26. januarja 2004 po svetovnem spletu razlegel prvi val čudnih elektronskih sporočil. Na prvi pogled so bila povsem običajna, kratka in poslovnega videza. Priložena je bila priponka, ki je bila videti kot dokument. A ko je nič hudega sluteči uporabnik kliknil nanjo, se je začelo nekaj, česar takrat še nihče ni razumel in kar se je kmalu zapisalo v zgodovino kot najhitreje širjen računalniški virus vseh časov: MyDoom. Ta ni bil zgolj virus. To je bil digitalni požar, ki se je razširil hitreje kot

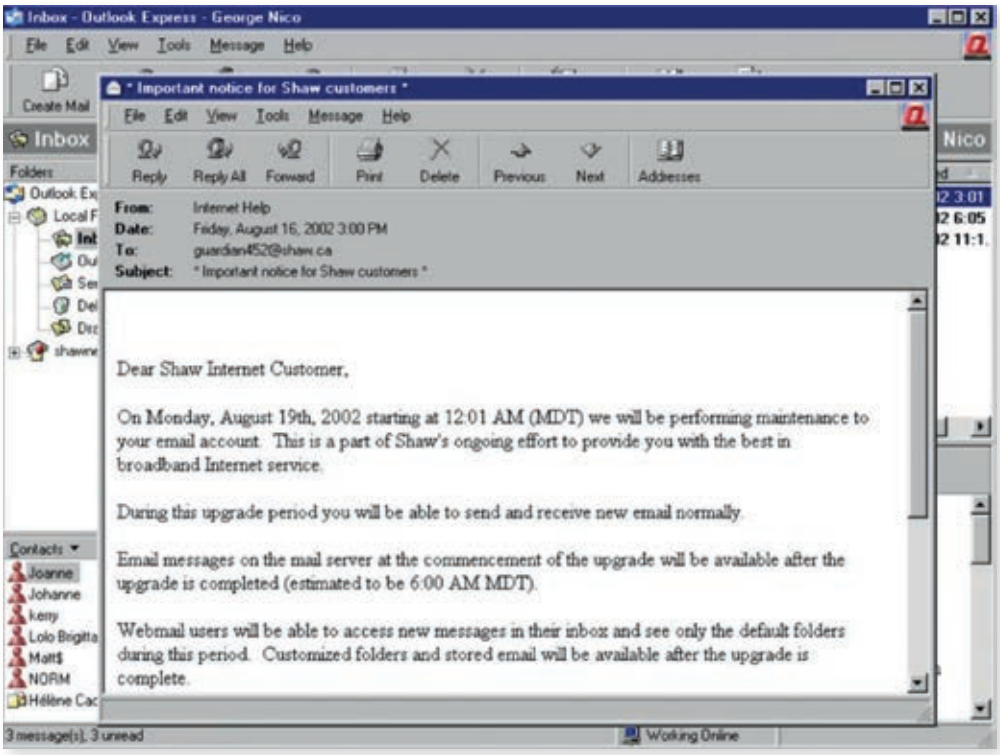


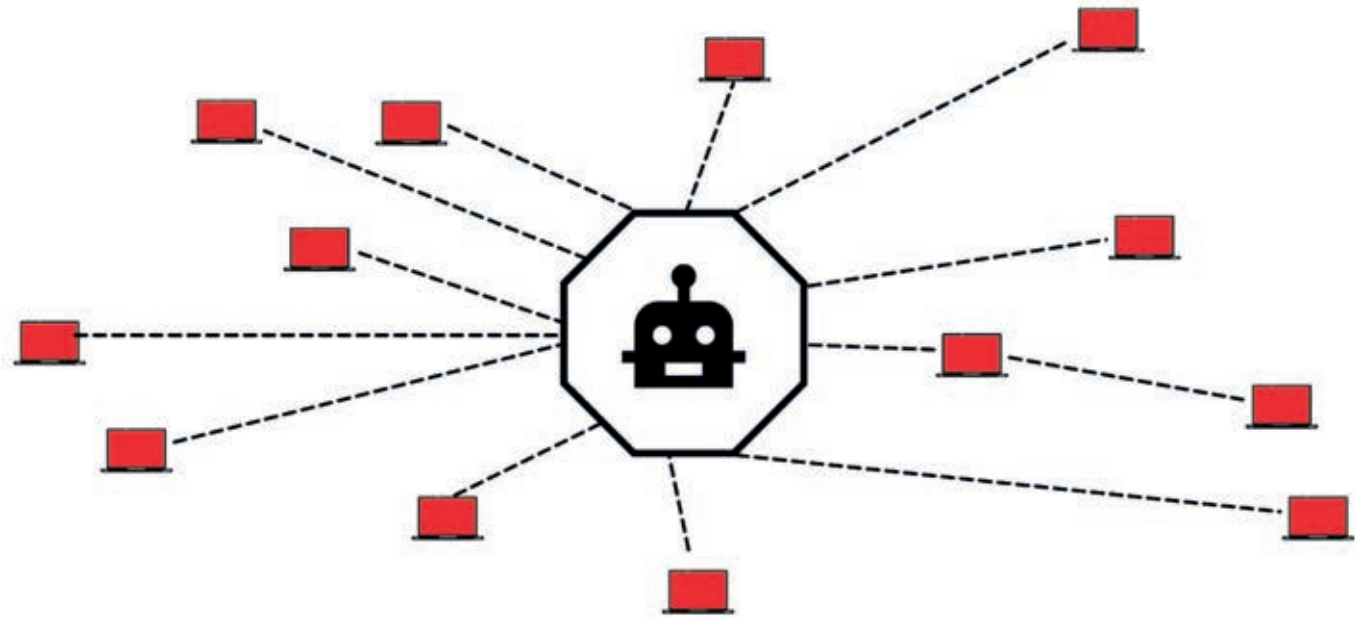
△ **Virus MyDoom je imel zelo specifične cilje in je onemogočil številne spletne strani, ki jih je zasul s prometom.**

katerakoli naravna katastrofa. V samo enem tednu je bilo okuženih že pol milijona računalnikov. Do konca svojega pohoda je virus vključil v svoj zlonamerni ustroj več kot 50 milijonov naprav. Kdo ga je ustvaril? Še danes ostaja skrivnost.

Zanimivo je, da je bila osnovna zamisel MyDooma precej stara – verižna pisma. Ta so že več kot stoletje uporabljena za manipulacijo in širjenje informacij. MyDoom pa je to starodavno idejo digitaliziral in jo opremil z zlonamerno kodo, ki se je skrita v elektronski priponki samodejno širila, ne da se prejemniki tega zavedali. Ko je uporabnik odprl okuženo priponko, se je virus v trenutku zasidral v sistem Windows, dostopal do uporabnikovega imenika in samodejno razposlal sebe naprej vsem stikom. Obenem je odprl vrata, skozi katera so lahko napadalci kadarkoli znova vstopili. MyDoom ni bil ustvarjen le zato, da bi se širil. Imel je zelo specifične cilje. Poleg okužb posameznih naprav je izkoriščal celotno mrežo kompromitiranih računalnikov za izvajanje napadov DDoS (*Distributed Denial-of-Service*), pri katerih se tarčne spletne strani in strežniki preobremenijo s prometom, dokler ne postanejo neuporabni. Prva žrtev je bilo podjetje SCO Group, tedaj pomemben akter v svetu operacijskega sistema Unix. Ko se je njihova spletna stran pod napadom sesula, so morali celo zamenjati spletni naslov. Naslednja tarča je bil Microsoft. A tehnološki gigant je imel močnejšo infrastrukturo in se mu je uspelo ubraniti. Kljub temu pa je virus povzročil precej škode, saj je istočasno blokiral dostop do protivirusnih strani, s čimer je uporabnikom onemogočil, da bi sploh prenesli zaščitna orodja.

▽ **Klez se je znal prilagoditi in izmikati protivirusnim programom.**





△ Conficker je okužene računalnike povezal v tako imenovano zombi omrežje.

Strokovnjaki ocenjujejo, da je MyDoom povzročil več kot 38 milijard ameriških dolarjev škode. Poleg različic A in B so se pojavile še številne druge mutacije, kot so C, F, G, H, U, V, W in X, vse z rahlo spremenjenimi cilji, a enako smrtonosnim učinkom. Številni računalniki so še dolgo po prvotni okužbi ostali ranljivi, saj so napadalci lahko kadarkoli znova dostopali do sistemov prek odprtih stranskih vrat. Uporabniki so sicer opazili upočasnjeno delovanje računalnikov, povečano porabo internetne povezave, čudna sporočila v imenu njihovih elektronskih naslovov, a pogosto prepozno. Virus je bil tako učinkovit in razširjen, da se še danes uvršča na seznam najbolj katastrofalnih kibernetskih groženj, ki so kadarkoli ogrozile digitalno varnost.

Conficker

Leto: 2008
Način širjenja: USB-ključek, omrežje + ranljivost operacijskega sistema
Ocenjena škoda: 9,1 milijarde USD

Leta 2008 se je v hotelskem baru v Arlingtonu, Virginija, po napornem dnevu sestankovanja skupina računalniških varnostnih strokovnjakov sproščala ob pijači. Sodelovali so z varnostnimi agencijami na letnem dogodku, kjer elita kibernetske varnosti načrtuje obrambo pred prihodnjimi napadi. A tistega večera se je med pogovorom pojavil nenavaden občutek. Microsoft je dva tedna pred običajnim rokom nenadoma izdal varnostni popravek, ki je bil namenjen varnostni luknji v operacijskem sistemu Windows. Ta se je nanašal na ranljivost v omrežnem protokolu, ki je omogočala oddaljeni dostop do sistema. Zdelo se je tehnično suhoparno, toda v resnici je šlo za vrata, skozi katera se je prikradel najbolj sofisticiran računalniški črv tistega časa.

Virus Conficker, znan tudi kot Downup, Downadup ali Kido, se ni zgolj širil, ampak je prevzemal nadzor. V nekaj tednih je okužil računalnike v domovih, na univerzah, v vladnih agencijah in celo vojski treh različnih držav. Nastalo je tako imenovano zombi omrežje, botnet, prek katerega so napadalci lahko prožili napade, zbirali podatke ali izvajali izsiljevanja. Strokovnjaki so bili osupli. Conficker je bil pametnejši od skoraj vseh znanih škodljivih programov. Uporabljal je šifrirane komunikacijske kanale, dinamično generiral spletne naslove, prek katerih je prejemal ukaze, ter blokiral protivirusne strani, da bi preprečil čiščenje okuženih sistemov. Bil je kot duh, neviden, izmuzljiv in hkrati uničujoč. Tudi ko so varnostni strokovnjaki razvozlali njegovo delovanje in vzpostavili delovno skupino za boj proti njemu, je nadaljeval svojo širitev. Bil je vedno korak pred zasledovalci.

Kljub ogromnim naporom celotne varnostne skupnosti, vključno z vladnimi agencijami, akademiki in industrijskimi giganti, avtorja Confickerja nikoli niso odkrili. Domneve segajo od kriminalnih združb do državnih akterjev, a identiteta ustvarjalca ostaja neznana. Ocenjuje se, da je Conficker okužil več kot 10 milijonov računalnikov, s čimer je postal eden največjih botnetov v zgodovini. Čeprav Conficker danes ne predstavlja več globalne nevarnosti, nas je naučil pomembno lekcijo. Kibernetski napadi se ne začnejo z eksplozijo, temveč s šepetom. Ena sama nepokrpana ranljivost je lahko dovolj, da zlonamerni črv zgradi infrastrukturo, ki ogrozi svet. Od tega napada naprej so bila uvedena številna pravila. Podjetja danes redno nameščajo varnostne popravke in šifrirajo komunikacijo, medtem ko varnostni strokovnjaki in vladne agencije odprto in proaktivno sodelujejo pri odkrivanju groženj. Conficker je dokaz, da v digitalnem svetu resnična moč ni v sili, temveč v nevidnosti in zvijačnosti. Črv, rojen iz preprostega popravka, je pokazal, kako krhek je lahko svet računalniške infrastrukture, če zanj ne skrbimo aktivno.

Conficker je naredil botnet, prek katerega so napadalci lahko prožili napade, zbirali podatke ali izvajali izsiljevanja.

CryptoLocker

Leto: 2013
Način širjenja: Trojanski konj Gameover ZeuS
Ocenjena škoda: 665 milijonov USD

Leta 1989, ko svet še ni poznal interneta, kakršnega imamo danes, in so bili računalniški virusi redki ter večina uporabnikov ni vedela, kaj pomeni pojem računalniška varnost, se je pojavil AIDS Trojan – prvi znani primer izsiljevalske programske opreme. Ni se širil po spletu, temveč z disketami. Ko je okužil računalnik, je zaklenil dostop do datotek in od žrtve zahteval 189 dolarjev, poslanih po pošti v Panamo. Preprosto, a vizionarsko. Takrat je bil to zgolj bizaren incident.

▷ **S kriptovaluto bitcoin kriminalci čez noč niso več potrebovali poštnih naslovov, bančnih računov ali tveganih srečanj. Rodil se je virus CryptoLocker.**

Nihče si ni predstavljal, da bo čez tri desetletja ta zamisel prerasla v večmilijardno kriminalno industrijo. Leta so tekla in tehnologija je napredovala, a izsiljevalska programska oprema je ostajala v ozadju kot tiho, skoraj pozabljeno orodje. Pravi razcvet pa je sledil okoli leta 2010, ko se je pojavila kriptovaluta bitcoin. Z njo se je zgodil preboj, kriminalci čez noč niso več potrebovali poštnih naslovov, bančnih računov ali tveganih srečanj. Zdaj so lahko izsiljevali ljudi anonimno, hitro in globalno. Kriminalna podzemlja so prepoznala priložnost in izsiljevalski virusi so začeli svojo pot iz niše v središče kibernetske grožnje.

Jeseni leta 2013 je svetovni splet prešel v novo ero, dobo digitalnega izsiljevanja. Bil je september, ko so se začele pojavljati prve žrtve pošiljanja okuženih priponk, ki niso le pokvarile računalnika, temveč zaklenile vse uporabnikove datoteke in zahtevale odkupnino. Tako se je svetu prvič predstavil CryptoLocker. To ni bil več otročji virus, ampak profesionalni izdelek. Uporabljal je močno RSA enkripcijo z 2048-bitnimi ključi in datoteke šifriral tako, da jih ni bilo mogoče obnoviti brez plačila. Odkupnina se je gibala med 300 in 700 ameriškimi dolarji, plačana pa je morala biti v kriptovaluti itcoin ali prek predplačniških bonov. CryptoLocker se ni širil sam, razširjal ga je bančni trojanec Gameover Zeus, ob pomoči katerega je okužil tisoče naprav. Bil je del sofisticiranega omrežja, imenovanega Gameover ZeuS botnet, prek katerega so napadalci pošiljali lažna elektronska sporočila s škodljivimi priponkami. Ko je uporabnik priponko odprl, se je virus takoj aktiviral, našel vse pomembne dokumente, slike, Excelove tabele, baze podatkov, in jih zaklenil. Napadalci niso več kradli podatkov, imeli so jih za talce. V zameno za njihovo vrnitev so žrtvam postavili ultimat: plačaj ali pa se poslovi od njih za vedno.

Leta 2014 so svetovne varnostne agencije v sodelovanju z zasebnimi podjetji sprožile obsežno akcijo, imenovano Operacija Tovar, s katero so razbile infrastrukturo, ki je podpirala CryptoLocker in Gameover ZeuS. Napadalna mreža je bila uničena, strežniki onemogočeni, grožnja začasno zatrta. A duh je takrat že pobegnil iz steklenice. Kljub uspešni operaciji so se že pojavile številne posnemovalke CryptoLockerja, ki so sledile isti strategiji šifriranja in izsiljevanja. Škoda, ki jo je povzročil CryptoLocker, ni bila samo finančna. Podjetja so utrpela večdnevne izpade poslovanja, izgubila zaupne podatke, nekatera pa so celo propadla. Za posameznike je bil udarec pogosto še hujši; fotografije družine, zasebni dokumenti, življenjski projekti, vse je čez noč izginilo. Poleg tehničnih in poslovnih izgub pa je CryptoLocker pustil tudi psihološke posledice. Ljudje so spoznali, kako krhek je njihov digitalni svet, če ni zaščiten.

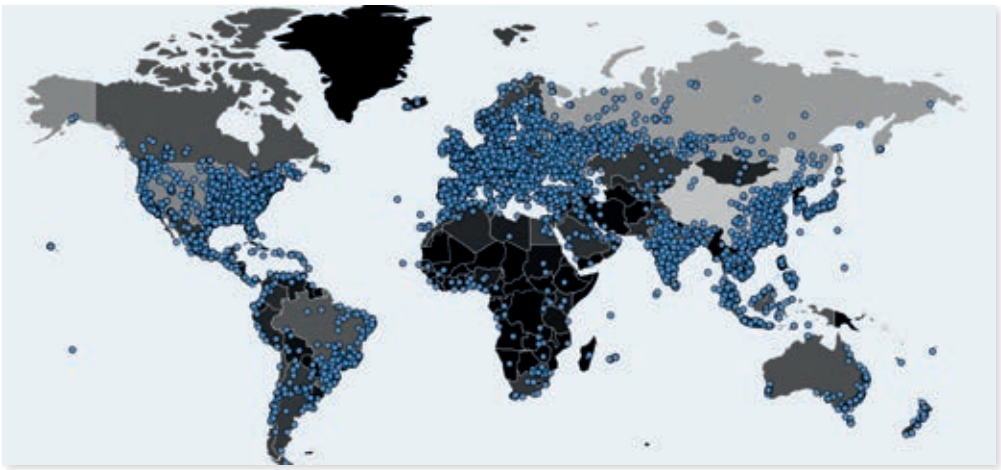
CryptoLocker ni bil več otročji virus, ampak profesionalni izdelek.

Originalna različica CryptoLockerja je danes onemogočena, a njegovo poslanstvo živi dalje. Številna sodobna izsiljevalska programska oprema temelji na principih, ki jih je postavil CryptoLocker, a gre še korak dlje. Če odkupnina ni plačana, napadalci podatkov ne izbrišejo, temveč jih javno objavijo, kar je v številnih primerih še veliko hujše. Iz izkušnje s CryptoLockerjem se je svet informacijske varnosti naučil nekaj ključnih stvari: da so redne (lokalne in oblačne) varnostne kopije vedno najboljša obramba, filtriranje e-pošte in izobraževanje uporabnikov prepreči večino napadov, posodobitve programske opreme zaprejo varnostne luknje, ki jih napadalci izkoriščajo, in da plačilo odkupnine ni priporočljivo, saj nikoli ni zagotovila za srečen konec zgodbe. CryptoLocker je bil prvi opozorilni znak, da se vojna v kibernetskem prostoru začenja. Bil je uveljavitev digitalnega izsiljevanja kot poslovnega modela za kriminalce. Njegov vpliv se čuti še danes, vsakič ko v e-poštnem nabiralniku pomislimo, ali je priponka res varna, vsakič ko ustvarimo varnostno kopijo.

WannaCry

Leto: 2017
Način širjenja: Škodljiva koda EternalBlue + ranljivost operacijskega sistema
Ocenjena škoda: 4 milijarde USD

Dvanajsti maj 2017 je bil za večino prebivalcev Zemlje povsem običajen dan, a v ozadju digitalnega sveta se je začela ena najbolj uničujočih kibernetskih zgodb sodobnega časa. Le nekaj ur po prvih opozorilih se je prek interneta začela širiti zlonamerna koda, poimenovana po priponi wncry, ki jo je puščala za seboj. Svet je kmalu izvedel za njeno ime – WannaCry. V zgolj 24 urah je virus ohromil bolnišnice, vlade, podjetja in univerze v kar 150 državah. Več kot 200.000 organizacij je bilo prizadetih, med njimi tudi britanski Nacionalni zdravstveni sistem (NHS), Deutsche Bahn, FedEx, ruska Sberbank in več državnih institucij v Indiji. To je bil napad brez primere, tako po hitrosti kot po učinku in razsežnosti.



△ WannaCry je v enem dnevu ohromil bolnišnice, vlade, podjetja in univerze po vsem svetu.

Čeprav je WannaCry zahteval odkupnino, se v resnici ni razlikoval od kibernetskega orožja. Prvič smo videli, kako lahko izsiljevalska programska oprema služi tudi državno podprtim ciljem, ne le kriminalnim skupinam. Ameriške in britanske oblasti so odgovornost pripisale skupini APT38, znani tudi kot Lazarus Group. Vse sledi so vodile v Severno Korejo. Medtem ko je svet zmrznil, so napadalci zbrali relativno majhen znesek, med 150.000 in 386.000 dolarji. Toda cilj ni bila finančna škoda, ampak kaos. Najbolj strašljiv prizor se je odvijal v britanskem zdravstvu. Bolnišnice so bile prisiljene odpovedati operacije, reševalna vozila so bila preusmerjena, zdravniki niso mogli dostopati do kartotek. Nihče ne ve natančno, koliko življenj je bilo neposredno prizadetih, saj nikoli ni bila izvedena nobena uradna analiza vpliva na paciente. In to nas pripelje do prve velike lekcije napada WannaCry. Brez sistematičnega zbiranja podatkov o posledicah napadov ne moremo razumeti njihovega resničnega vpliva na družbo.

Eden najbolj skrb vzbujajočih vidikov WannaCryja je bil izvor ranljivosti, ki jo je izkoristil. Uporabljena je bila koda EternalBlue, orodje, ki ga je razvila ameriška agencija NSA in ga je kasneje ukradla hekerska skupina Shadow Brokers. Razkritje tega dejstva javnosti je povzročilo razburjenje. Druga lekcija WannaCryja je bila jasna: zbiranje in skrivanje varnostnih lukenj državnih institucij predstavlja resno globalno grožnjo. Tudi več let od napada številne organizacije še vedno niso namestile popravkov, medtem ko je WannaCry mutiral. Tretja lekcija je učila, da tovrstni napadi ne izginejo, ampak mutirajo, se prilagajajo in ostajajo z nami. Čeprav je napad WannaCry zabeležen v arhivih kibernetske varnosti kot zgodovinski mejnik, ni stvar preteklosti. Ostaja z nami, v novih oblikah, nezakrpani infrastrukturi, sistemih, ki se še vedno zanašajo na zastarele rešitve. Je opomin, da digitalna varnost ni tehnično vprašanje, ampak družbeni izziv. In dokler ne bomo razumeli človeških zgodb za številkami, bodo napadi, kot je WannaCry, še vedno imeli moč, da nas presenetijo in ohromijo.

StuxNet
Leto: 2010
Način širjenja: USB-ključek, omrežje
Ocenjena škoda: 10 milijonov USD

Za konec ne moremo mimo virusa, ki ni bil grožnja navadnemu uporabniku računalnika, a vseeno zasluži mesto na seznamu največjih digitalnih groženj doslej. Stuxnet je bil namreč prva kibernetska bomba v zgodovini. Da bi razumeli, zakaj, si moramo pobliže ogledati, kdaj. V času po letu 2000 so diplomati po vsem svetu zadržano dihali. Iran je s svojim jedrskim programom napredoval, zahodne sile pa so se bale, da se približuje točki, ko bi lahko razvil jedrsko orožje. Takrat je obstajala resnična grožnja, da bo Izrael ukrepal z letalskim napadom, kar bi zanetilo celotno regijo. Toda v tem ozračju tihe napetosti se je v ozadju pripravljala povsem drugačna rešitev. Brez strelov, brez bomb, brez kričanja. Rešitev, ki je bila nevidna, a smrtonosna. Zgodba se je začela kot skrivna skupna operacija ameriške in izraelske obveščevalne službe. Celo njeno kodno ime *Operation Olympic Games* zveni kot nekaj iz vohunskega romana. A šlo je za resnično in zelo resno misijo: ustvariti programsko orodje, ki bi fizično uničilo iranske centrifuge za obogatitev urana.

WannaCry je uporabljal kodo EternalBlue, orodja, ki ga je razvila ameriška agencija NSA.

Operacija Olimpijske igre je ustvarila črva Stuxnet. Programska oprema velikosti 500 kilobajtov je okužila računalnike vsaj 14 industrijskih lokacij v Iranu, vključno z obratom za bogatenje urana. Črv je bil edinstven zaradi svoje tridelnosti: najprej je okužil računalnike z operacijskim sistemom Windows, nato ciljal programsko opremo Siemens Step7, ki se uporablja za industrijske nadzorne sisteme, na koncu pa je prevzel nadzor nad programirljivimi logičnimi krmilniki (PLC). To mu je omogočilo vohunjenje za industrijskimi sistemi in celo povzročanje poškodb, kot je uničenje centrifug, ne da bi operaterji zaznali težave. Delavci v objektu Natanz v Iranu so se soočili z nepojasnjenimi napakami v napravah. Centrifuge, izjemno občutljive in drage naprave, so se začele kvariti. Nihče ni razumel, zakaj. Celo Mednarodna agencija za jedrsko energijo (IAEA) je bila zmedena. Leta 2010 je opazila, da je bilo poškodovanih skoraj 2.000 centrifug, več kot dvakrat več, kot bi bilo pričakovano.

Stuxnet je bil tehnološka mojstrovina. Njegov razvoj je verjetno zahteval večletno delo ekipe vrhunskih strokovnjakov. Stroški razvoja so ocenjeni na milijardo do dve ameriških dolarjev. Črv se je širil prek ranljivosti v operacijskem sistemu Windows, ki do tedaj še niso bile javno znane. Razširil se je prek lokalnih omrežij in USB-ključkov, kar mu je omogočilo dostop tudi do računalnikov brez internetne povezave. Ko je okužil računalnik, je virus preveril, ali ta nadzira določene Siemensove krmilnike. Če jih je našel, je začel tiho spreminjati njihove programe. Rezultat? Centrifuge so se začele vrteti z nepravilnimi hitrostmi: dovolj subtilno, da so jih poškodovale, a ne tako očitno, da bi uporabniki takoj zaznali napako. Obenem je Stuxnet skrbno prikrival svoje delovanje in poskrbel, da so prikazovalniki kazali normalno delovanje.

Ironično je, da Stuxnet nikoli ni bil namenjen širjenju po svetu. Objekt Natanz je bil namreč popolnoma odrezan od interneta. A virus je vseeno pobegnil, morda zaradi človeške napake, morda zaradi preagresivne kode. Vse se je razkrilo, ko je iranski uradnik poklical tehnično pomoč, ker so se računalniki v njegovi pisarni začeli nenavadno sesuvati. Klic je pristal pri beloruskem varnostnem podjetju VirusBlokAda, kjer je raziskovalec Sergey Ulasen začel raziskovati skrivnostni virus. Kar je našel, ga je presunilo:

sofisticiran črv, napisan v več programskih jezikih, opremljen z vohunskimi orodji, ki je upravljal industrijsko opremo. Za pomoč je prosil širšo varnostno skupnost. Strokovnjaki, kot je Liam O'Murchu iz Symanteca, so opisali Stuxnet kot najbolj zapleteno kodo, kar so jih kadarkoli analizirali, in po mesecih povratnega inženiringa razkrili, da je bil Stuxnet zasnovan za napad na Siemensovo opremo v iranskem programu obogatitve urana. Analiza kode je razkrila, da je Stuxnet iskal specifične frekvenčne pretvornike, ki so se ujemali z dokumentacijo Mednarodne agencije za jedrsko energijo (IAEA) o iranskih centrifugah.

Stuxnet je prvič dokazal, da lahko programska oprema fizično uniči naprave in spremeni tok geopolitike. In čeprav je bil ustvarjen za točno določen cilj, uničenje iranskega jedrskega programa, je odprl Pandorino skrinjico. Njegov vpliv je preoblikoval razumevanje kibernetskih konfliktov in odprl vrata novim vrstam napadov, kot so Duqu, Flame in Gauss, ki so sledili po odkritju Stuxneta. Roel Schouwenberg, raziskovalec iz laboratorija Kaspersky, meni, da je bil Stuxnet prelomnica v zgodovini kibernetske varnosti. Kar smo prej videli le v filmih, je postalo resničnost. V 90-ih letih prejšnjega stoletja so računalniški virusi večinoma povzročali zgolj preglavice, kot je bila izbrisana datoteka ali spremenjena spletna stran, Stuxnet pa je predstavil novo obdobje prefinjenega kibernetskega vojskovanja. Običajnemu uporabniku sam po sebi nikoli ni bil resna grožnja, največ, kar bi nas ob okužbi doletelo, je modri zaslon smrti, ki nam ne bi povzročil večje škode, saj ne upravljamo uranovih centrifug. Tudi ranljivosti, ki jih je črv izkoriščal, že davnaj ni več. So pa tu nove in zagotovo Stuxnetovi potomci. Svet se je z njim naučil, da koda lahko uniči stroje. Da lahko vrstica programske opreme pomeni razliko med mirom in vojno. In poti nazaj ni. ◀

△ **StuxNet je bila prva kibernetska bomba v zgodovini. Iran je oškodovala za 10 milijonov ameriških dolarjev in dve leti napredka pri razvoju jedrskega orožja.**

Virusi za **Apple Mac**

Dolga leta so uporabniki Applovih računalnikov živeli v prepričanju, da njihovi stroji preprosto ne morejo dobiti virusov. Ta občutek varnosti je temeljil na kombinaciji Applovih tržnih sporočil, uporabniške izkušnje in (v zgodnjih dneh) dejanskih podatkov. Večina škodljivih programov je napadala Windows, kar je uporabnikom operacijskega sistema macOS dalo občutek nedotakljivosti. Toda ta občutek je bil iluzija. Virusi za mace so obstajali. Bili so sicer redkejši in subtilnejši, a pogosto enako nevarni.

Dominik Cigala

Vse se začne pri številkah. Operacijski sistem Windows je dolga desetletja prevladoval na trgu osebnih računalnikov, kar pomeni, da so bili pisci virusov motivirani, da napadejo največji zbir potencialnih žrtev. Poleg tega je macOS zasnovan na Unixovi arhitekturi, znani po svoji robustnosti in strogi ločitvi uporabniških privilegijev. Nenazadnje je Apple že od začetka strogo nadzoroval svojo programsko in strojno opremo. V nasprotju z odprto naravo Windows okolja, kjer lahko uporabnik (ali napadalec) skoraj brez omejitev spreminja sistemske nastavitve, je Apple omejeval dostop, kar je pomagalo preprečevati širjenje zlonamerne kode. Čeprav je mac veljal za varen, skoraj nedotakljiv sistem, so se skozi leta začele pojavljati razpoke in skoznje so se počasi, a vztrajno začeli plaziti zlonamerni programi.

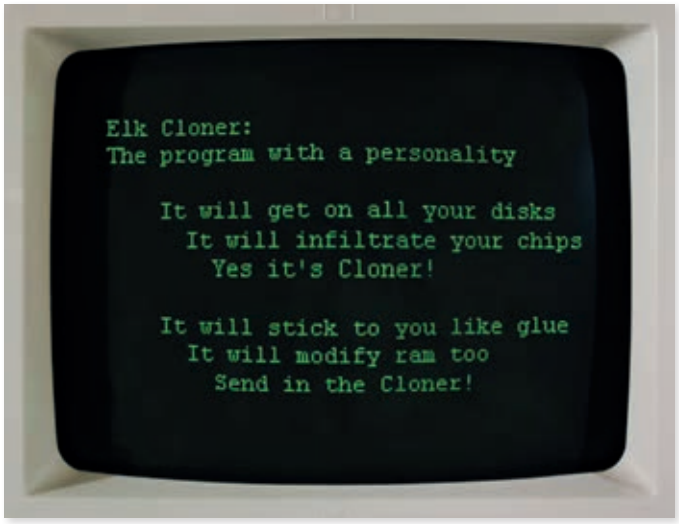
Že leta 1982 se je pojavil prvi znani virus za mac – Elk Cloner. Izdelal ga je srednješolec Rich Skrenta in sprva ni bil zlonameren. Širil se je prek disket, uporabnikom pa je na zaslonu prikazal kratko pesmico. Bil je igriv, a pomenljiv dokaz, da so tudi maci ranljivi. Leta 1987 pa se je situacija zaostrila z virusom MacMag, ki se ni več zgolj igral, temveč je poškodoval datoteke in onemogočil uporabo aplikacij. Leto kasneje je udaril Morrisov črv, ki je okužil več sistemov, tudi Mac in Unix, ter povzročil kaos po zgodnjem internetu. Isto leto se je pojavil še INIT 29, prvi virus, ki je neposredno okužil sistemske datoteke Mac OS. Povzročal je naključna sesutja in izgubo podatkov. Leta 1989 sledi nVir, virus, ki ni zgolj okužil datotek Finder in System, temveč je vseboval tudi sporočilo, v katerem je avtor izrazil nezadovoljstvo s podjetjem iz Cupertina. Računalništvo je tako postalo tudi prostor protesta.

V 90-ih letih je mac postal še bolj priljubljen, kar je pomenilo večjo tarčo. Virusi so postajali kompleksnejši. Leta 1992 se je pojavil Scores, zagonski virus, ki je okuževal prek disket. Ob njem je deloval tudi Dark Avenger, eden prvih polimorfnih virusov, ki je bil sposoben spreminjati svojo kodo, da bi se izognil protivirusnim programom. Leta 1996 je udaril Laroux, ki se je širil prek priponk elektronske pošte. Ob koncu desetletja, leta 1997, se je pojavil Concept, virus, ki se je prenašal z Wordovimi dokumenti in prvič zabrisal mejo med Windows in platformo Mac. Leta 1998 sledi FunLove, virus, ki je okužil izvršljive datoteke in povzročal izgubo podatkov, s čimer je bil nevaren tako za sisteme Mac kot Windows. Svetovni splet je odprl vrata množičnemu širjenju virusov in nova resničnost je bila jasna – Mac ni bil več varen otok.

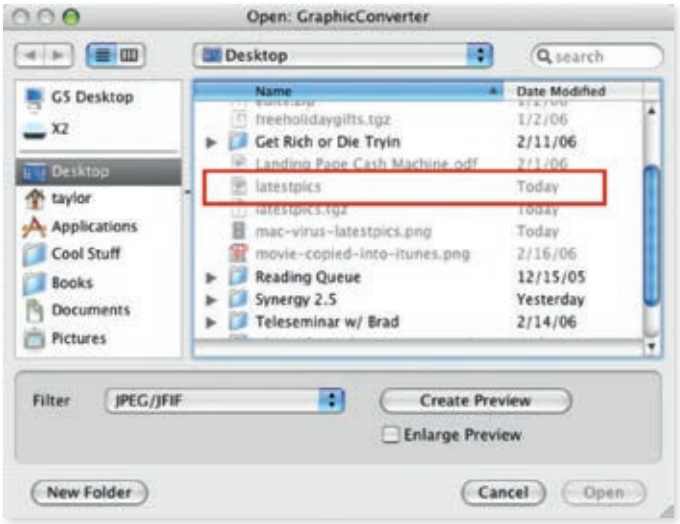
Leta 2006 je podjetje Intego odkrilo prvega pomembnega črva za Applov operacijski sistem. Poimenovali so ga Leap.A oziroma v bolj šaljivi različici Oompa-Loompa. Odkritje v javnosti velja za simbolični konec zlatega obdobja varnosti, v katerem so uživali uporabniki Applovih računalnikov. Leap.A namreč ni bil običajen virus, kakršne so jabolčni navdušenci zelo redko srečevali do takrat. Širil se je prek priljubljenega Applovega programa za neposredna sporočila iChat. Uporabniku je bila poslana datoteka z imenom latestpics.tgz, ki je obljubljala predogled prihodnjega operacijskega sistema macOS. Znotraj arhiva pa se je skrival izvršljivi program, prikrit kot slika, z znano ikono. Da bi virus deloval, ga je moral uporabnik ročno zagnati. Potreboval je nevedno žrtev, ki je odprla vrata. Ko se je zlonamerni program zagnal, je poskušal pridobiti administratorske pravice in okužiti aplikacije, a le tiste, ki jih je namestil trenutni uporabnik (ne sistemskih). Deloval je samo na aplikacijah, izdelanih s programskim vmesnikom Cocoa, in okužil največ štiri najpogosteje uporabljene programe. Če niso ustrezali kriterijem, ni ukrepal.

V nasprotju s številnimi zlonamernimi programi Leap ni bil uničevalen v tradicionalnem smislu, ni brisal podatkov, vohunil ali nadzoroval sistema. Ironično pa zaradi napake v kodi okuženi programi niso več delovali. To je po svoje pomagalo, saj je onemogočilo nadaljnje širjenje, a tudi povzročilo precejšnje nevšečnosti uporabnikom. Črv

▽ **Prvi znani virus za Applove računalnike ni bil zlonameren in je uporabnikom na zaslonu prikazal le kratko pesem.**



▽ **Leap.A je bil prvi pomemben črv za Applov operacijski sistem, ki je povzročil, da nekateri programi na macih niso več delovali.**



▷ **Virus Flashback se je na začetku pretvarjal, da je posodobitev predvajalnika Adobe Flash Player.**

se ni mogel širiti prek interneta. Uporabljal je le lokalno omrežje LAN in še to le v primeru, če je bil omogočen protokol Bonjour. Ob okužbi sta bili najučinkovitejši rešitvi ročno brisanje zlonamernih datotek in ponovna namestitev aplikacij. Ker sistemske aplikacije niso bile ogrožene, ni bilo potrebe po popolni ponovni namestitvi operacijskega sistema. Čeprav je bil Leap omejen po obsegu in tehnični sposobnosti, je njegov pomen izjemen, saj je Applove uporabnike naučil, da sta odpiranje sumljivih datotek in omogočanje upraviteljskih pravic lahko pogubna.

Nekateri uporabniki macov so jeseni 2011 naleteli na pojavno okno, ki je opozarjalo, da je treba posodobiti Adobe Flash Player. Ker je bilo to običajno opravilo in so bile podobe prepričljive, so številni kliknili pritrdilen odgovor ter vpisali svoje uporabniško geslo. S tem so nevede povabili nezaželenega gosta v svoj sistem. Tako se je začela zgodba virusa Flashback, enega prvih množično razširjenih zlonamernih programov za macOS. Črv, ki je dolgo ostal neopažen, je do pomladi 2012 okužil več kot pol milijona Applovih računalnikov po vsem svetu. Bil je tih, premeteno prikrit in zelo uspešen. Medtem ko so se prve različice Flashbacka pretvarjale, da so legitimne nadgradnje Flash Playerja, so napadi čez nekaj mesecev postali še bolj prefinjeni. Nove različice virusa so izkoristile Java ranljivosti (CVE-2012-0507 in CVE-2011-3544), ki so omogočile, da se je Flashback samodejno namestil že samo z obiskom okužene spletne strani. Flashback ni bil najbolj destruktiven virus, ni brisal datotek ali zaklepal sistemov. Njegov cilj ni bil uničenje, temveč preusmerjanje iskanj in generiranje prihodkov prek oglasov, a vendar je bil njegov pomen ogromen. To je bil trenutek, ko so tudi najbolj skeptični uporabniki začeli dvomiti o Applovi imuniteti.

Virusi danes niso edini problem. Že leta 2015 je bila odkrita ranljivost Freak, ki je izkoristila slabost v šifrirnih protokolih in vplivala tudi na macOS. Čeprav ni šlo za specifično Applovo napako, je bila to opozorilna zgodba o medsebojni povezanosti varnosti. Leta 2022 pa so raziskovalci v laboratorijih MIT nenadoma odkrili nekaj, kar je spominjalo na digitalno legendo. Nekaj prikritega. Ne en sam hrošč. Ne ena luknja v kodi, temveč celoten razred ranljivosti, ki tiho preži v Applovem procesorju M1. Poimenovali so ga Pacman. Šaljivo ime za Applov čip pomeni precej bolj resno grožnjo. Razred ranljivosti Pacman bi lahko omogočil napad, ki ne potrebuje fizičnega dostopa in ne zahteva eksplozivnega vdora. Namesto tega deluje tiho, skoraj kot duh, ter v popolni tišini izkorišča kombinacijo strojne in programske ranljivosti v mehanizmu Pointer Authentication Codes (PAC), ki ga je Apple uvedel, da bi onemogočil izvajanje nepooblaščene kode v procesorjih ARM.

PAC je bil varnostna inovacija. Dodatek v siliciju, ki preverja, ali so kazalci v pomnilniku zakoniti. Če niso, sistem zavrne nadaljnje izvajanje. A Pacman napad je obrambo spremenil v napad. Napadalec lahko z zlonamernim programom preizkusi različne vrednosti PAC in ob pomoči tako imenovanih stranskih kanalov (*side-channel attack*) ugotovi, katera kombinacija deluje – vse to brez opozorila. Applov M1 je bil dolga leta videti kot svetel zgled varnosti v svetu osebnih računalnikov. Njegova zaprta arhitektura, preverjanje kazalcev in zaščita pred strojno manipulacijo so predstavljali visok prag za napadalce. A Pacman dokazuje, da na ravni strojne opreme ni nič nedotakljivo. Pacman ni ranljivost, ki jo lahko enostavno popravijo s programsko posodobitvijo, saj temelji na interakciji med programsko opremo in strojno opremo in kot taka ostaja neodpravljiva na računalnikih s procesorji M1, ki so bili izdelani pred odkritjem. To nas je ponovno opomnilo, da varnost v digitalnem svetu nikoli ni dokončna. Lahko je napredna. Lahko je močna. Lahko je boljša od druge. A absolutna ni nikoli. ◀

▽ **Applov procesor M1 je imel nepopravljiv komplet ranljivosti, s katerimi bi zlikovci sicer inovativno zaščito PAC lahko iz obrambe preusmerili v napad.**

Od heca do **orodja moči**

Računalniški virusi so, tako kot vsi tehnološki pojavi, produkt svojega časa – in svoje okolice. V dobrih 50 letih, kolikor jih poznamo, so iz preprostih, pogosto šaljivih digitalnih potegavščin prerasli v sofisticirana orodja nadzora, sabotaže in predvsem – zaslužka. Njihova zgodovina je hkrati zgodovina razvoja informacijske družbe in njenih temnejših plati: od naivnega eksperimentiranja, prek kaosa, ki ga je prinesla hiperpovezanost, do današnjega časa, ko digitalni zlikovci izsiljujejo multinacionalke in države razvijajo lastne kibernetske arzenale.

V začetku 70-ih let so bili prvi virusi ustvarjeni iz radovednosti in igrivosti. Creeper, predhodnik vseh, je znal zgolj prehajati z enega sistema na drugega in na zaslonu izpisati izzivalno sporočilo. Njegov »protivirus«, Reaper, je bil prav tako le demonstracija koncepta. Tudi v 80-ih letih je šlo večinoma za ekscentrične poskuse – pesmi na zaslonih, grafične animacije in drobne neprijetnosti, ki so kazale predvsem na spretnost avtorjev.

A romantike je bilo konec, ko so virusi dobili zobe. V 90-ih letih so se razbohotili kot posledica slabe zaščite operacijskih sistemov in nepazljivosti uporabnikov. Nekateri, kot Melissa ali ILOVEYOU, so za okužbo potrebovali le klik na navidezno neškodljivo priponko. Drugi, kot Černobil, so šli dlje – in že povzročali tudi fizično škodo. Ob tem je vedno več napadov imelo tudi jasen motiv: denar.

Z novim tisočletjem je virus postal produkt. Uporabljali so ga za pošiljanje nezaželene pošte, krajo podatkov, prikrito rudarjenje kriptovalut. Klasični vandalizem se je počasi umikal profesionalizaciji. Vse več virusov je začelo meriti na finančne institucije, okužene naprave pa so postale orodja za oddaljeni nadzor, krajo identitet in vohunstvo. Ni šlo več za zabavo – šlo je za posel.

Danes virusi obstajajo v številnih oblikah, a prevladujejo – izsiljevalski. Ti ugrabijo podatke in od žrtve zahtevajo odkupnino, pogosto v kriptovalutah, ki zagotavljajo (navidezno) anonimnost. Takšni napadi ne prizanašajo nikomur – tarče so podjetja, bolnišnice, šole, vladne ustanove. Profesionalne skupine, kot so Dark Angels, zadajajo milijonske udarce, pogosto brez sledu, da bi jih kdo ustavil.

A morda še bolj skrb vzbujajoča kot kriminal je vloga držav. Če so bili virusi včasih hobi nadobudnih programerjev, danes obstajajo kot del nacionalnih oborožitvenih programov. Primeri, kot je Stuxnet, jasno kažejo, da se vojne prihodnosti ne bodo več vodile (samo) s tanki in topovi, temveč tudi z vrsticami kode, ki za cilj izbirajo industrijske sisteme ali infrastrukturo. Špijonaža, sabotaža, nadzor – vse to danes omogočajo virusi, razviti in financirani z državnim denarjem. ◀

Danes virusi obstajajo v številnih oblikah, a prevladujejo izsiljevalski.

Cilji se **spreminjajo**

Računalniški virusi so v takšni ali drugačni obliki z nami že več kot pol stoletja, a jih je evolucija v tem času preoblikovala bolj kot njihove biološke sorodnike. Kar se je začelo z nedolžnimi potegavščinami, so postali večmilijonski posli. Časi so se spreminjali, z njimi pa tudi virusi.

Matej Huš

Računalniški virusi so na neki, četudi sprevržen način, žrtve modernega časa. Njihova zgodovina je pestra in barvita. Avtorji so z njimi izpostavljali najrazličnejša stališča in na različne, včasih duhovite, spet drugič škodljive, načine vplivali na delovanje okuženih sistemov. Da je romantike konec, smo ugotavljali že pred 13 leti (*Od starega do atomskega veka*, *Monitor 09/12*). Tedaj se je zdelo, da so virusi postali orožje, projektil vojaške industrije, s katerim se bodo države v prihodnosti bojevale v kibernetskem prostoru.

To se dogaja še danes, a večine nevšečnosti ne povzročijo ruski, kitajski ali ameriški državni hekerji. Univerze v Mariboru ali Holdinga Slovenske elektrarne niso napadle tuje obveščevalne agencije, temveč neizvirni črvi, s katerimi želijo zlikovci preprosto samo zaslužiti. Ideologije so se že zdavnaj umaknile materialnim koristim. Kako zelo je 13 let star pogled na viruse danes zastarel, morda najlepše priča tema, o kateri molči. Obsežni pregled virusov in njihove zgodovine leta 2012 ni niti enkrat uporabil besed kriptovaluta, bitcoin ali izsiljevalski virus (*ransomware*). Kako neizmerno banalnejši je svet danes!

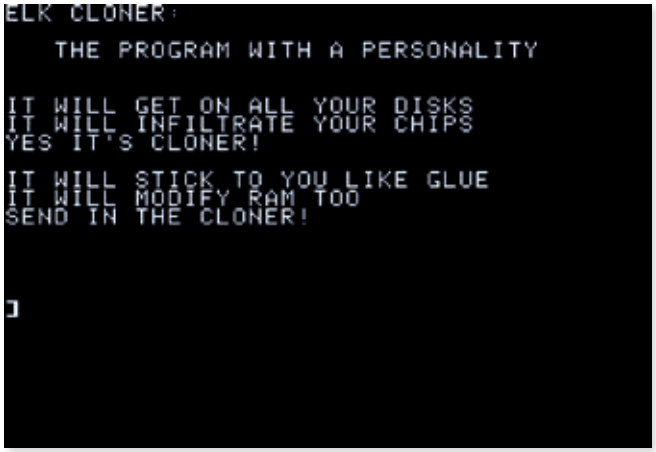
Zgodnji šaljivci

Pred zgolj pol stoletja so bili virusi benigni in zabavni. Bob Thomas je leta 1971 enega prvih izpustil v omrežje Arpanet preprosto zato, da bi pokazal izvedljivost ideje. Creeper je bil program, ki se je sam kopiral, pri prehodu na vsako novo tarčo pa se je poskušal pobrisati s predhodnega računalnika. Računalnik je bil tedaj DEC-ov PDP-10, na katerem je tekel operacijski sistem Tenex. Virusova edina funkcija je bila izpisati *I'M THE CREEPER. CATCH ME IF YOU CAN*! na zaslonu. Njegov protistrup je bil program Reaper, ki ga je leto pozneje napisal Ray Tomlison. Nekoliko škodljivejši je bil Rabbit/Wabbit iz leta 1974, ki se je na sistem prepisal, kolikorkrat se je mogel, zaradi česar se je sistem naposled zrušil. Težko bi mu očitali, da je namenoma uničeval sistem, ga je pa preobremenil oziroma popolnoma zapolnil.

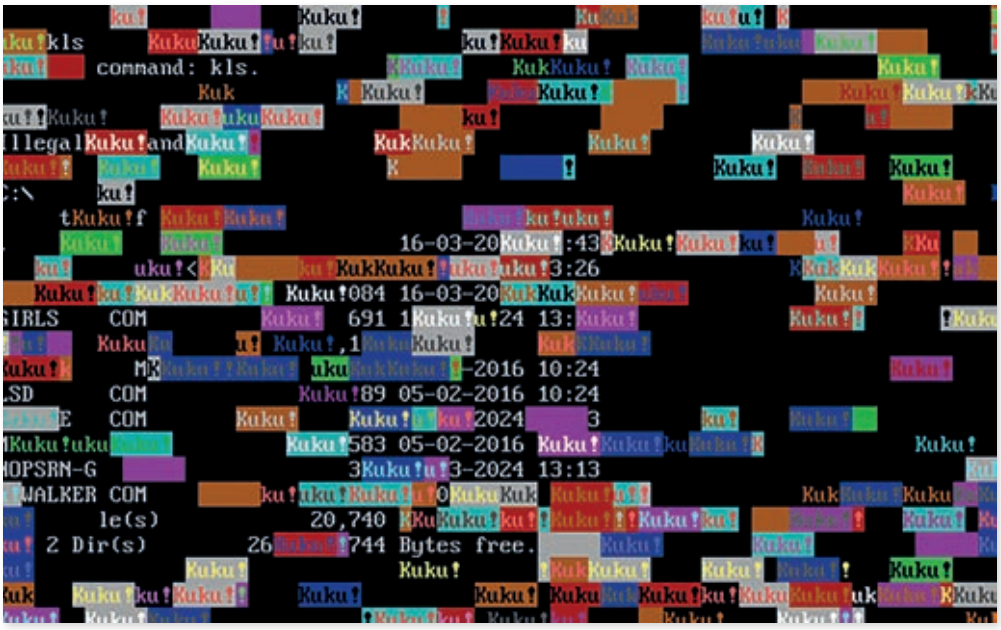
V 80. letih so računalniški virusi prvikrat pokazali čekane. Prvi večji izbruh je povzročil virus Elk Cloner, ki se je – za današnje čase paradoksalno – širil po Applovih računalnikih. Napisal ga je dijak Richard Skrenta kot potegavščino, ki se skrije na disketo, ter ga nato shranil na disketo z igro. Elk Cloner se je učinkovito razširjal po računalnikih s sistemom Apple DOS 3.3. Po 50 zagonih je okuženi računalnik izpisal pesem, hkrati pa je učinkovito okužil vsako disketo, ki jo je prebral. Apple II se je tedaj namreč zaganjal z disket. Čeprav je Elk Cloner dvignil veliko prahu, resne škode ni povzročil. Da se je širil kot požar, je kriva njegova inovativnost. Tedaj virusov ni bilo, računalniki niso imeli protivirusnih programov, védenje o njih pa med uporabniki praktično ni obstajalo.

Prvi resni virus za računalnike IBM z operacijskim sistemom DOS je bil Brain, ki je nastal v Pakistanu. Brata Basit in Amjad Farooq Alvi iz mesta Lahore sicer z njim nista želela povzročiti škode. Brain je zgolj upočasnil delovanje disketnega pogona in odškrnil neznaten del pomnilnika, sicer pa se sploh ni zapisoval na disk. Njegov namen je bil preprečiti nezakonito kopiranje disket s programom, v zagonski sektor pa je zapisal podatke o sebi in kontaktne podatke avtorjev. Številni drugi virusi iz tistih časov so bili zabavni, saj so pobarvali zaslon v DOS (Kuku), prikazali animacijo ognjemeta v Windows (Happy99) in podobno.

Tudi virusi, ki so dejansko povzročali škodo, so to počeli na zelo naiven način. Črv Morris, ki ga je leta 1988 napisal Robert Morris, tedanji študent na Cornellu, ni imel nobene uničujoče komponente. Preprosto je



△ **Elk Cloner se je naglo širil, a je izpisal le pesem.**



▽ **Virus Kuku je jasno naznanil svojo prisotnost.**

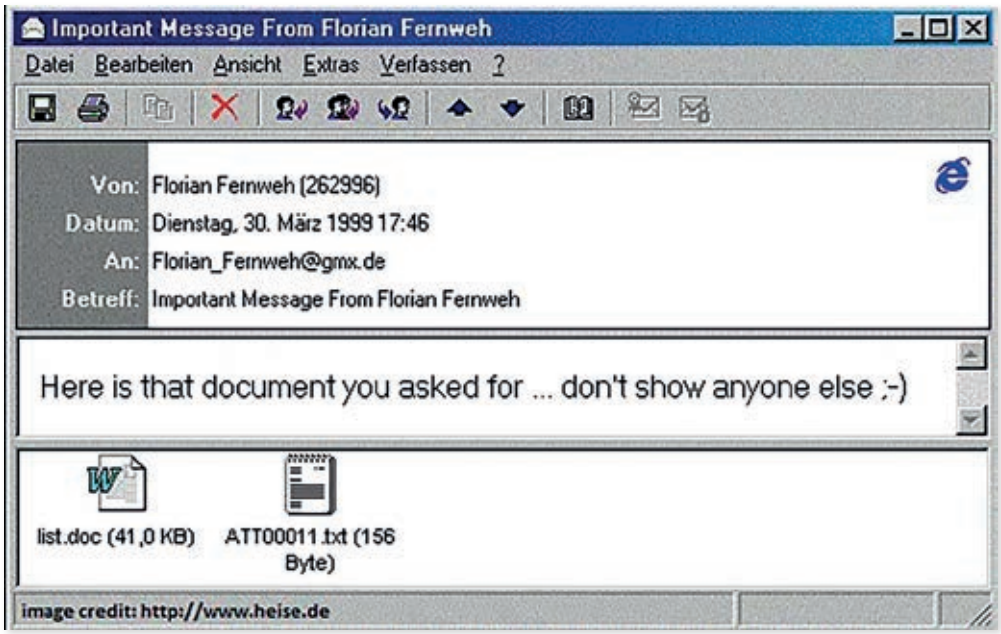
izkoriščal znane ranljivosti v sistemu Unix in se kopiral po računalnikih. Morris se je v 14 odstotkih primerov skopiral na novi računalnik, zato je sčasoma sisteme lahko okužil večkrat in jih upočasnil do neuporabnosti in zrušitve. Avtor je bil leta 1991 na drugi stopnji kot prvi v ZDA pravomočno obsojen zaradi svojega virusa.

Destruktivna 90. leta

Virusi v zgodnji dobi so bili šaljivci, ki pa so kmalu začeli dobivati tudi bolj zlovešče funkcije. K hitremu širjenju pa je v zgodnji dobi interneta in osebnega računalništva prispevalo tudi nekaj nerodnih odločitev. Prvi odjemalci za e-pošto so samodejno brali pošto HTML (in izvajali ukaze, vključno z JavaScriptom), končnice datotek so bile privzeto skrite, zgodnji pisarniški programi (zlasti Word) so izvajali makroje v datotekah in podobno. To je konec 90. let in v začetku tisočletja povzročilo pravo eksplozijo virusov, ki so lahko postali precej agresivnejši.

Michelangelo se je razširil leta 1991 in je vsako leto 6. marca – na umetnikov rojstni dan – prepisal prvih sto sektorjev na disku z ničlami, s čimer je onesposobil zagon računalnika. Virusi, ki so prepisovali zagonski sektor, so bili konec 80. let in v začetku 90. let prave uspešnice, prva različica pa sega v leto 1987, ko je novozelandski študent napisal virus Stoned, ki je ob zagonu računalnika (če je bil čas zagona deljiv z osem) agitiral za legalizacijo marihuane.

Bistveno večje nevšečnosti je povzročil CIH oziroma Černobil, ki je leta 1998 uničeval sisteme z Windows 95 in 98. Okužil je več kot 60 milijonov računalnikov, na katerih je prepisoval podatke na diskih in v nekaterih primerih mu je uspelo uničiti tudi BIOS. S tem gre za prvi virus, ki je povzročil fizično škodo. K njegovi razširjenosti je pripomogla zakasnela sprožitev, saj je krožil leta 1998, nato pa je vsako leto 26. aprila udaril. Vtihotapil se je celo v demo različice iger, posodobitve Yamahine programske opreme za zapisovalnike CD-R in celo nove računalnike IBM Aptiva.



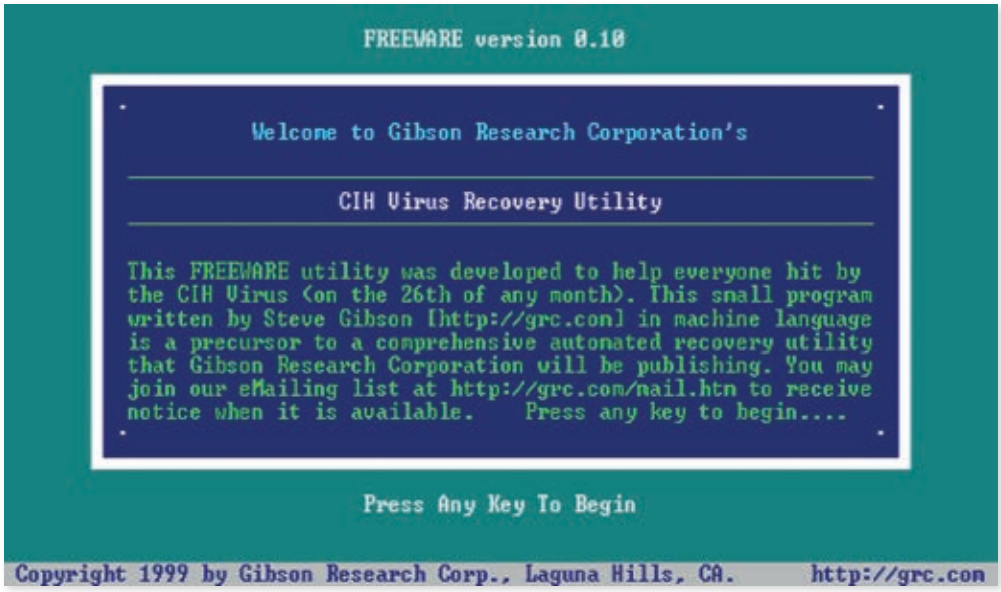
△ Virus Melissa se je širil z elektronskimi sporočili.

Melissa je leta 1999 nakazal prihodnost, ki so jo sestavljali zlonamerni makroji. Širil se je po Wordu in Officeu, ljudje so ga nevede pošiljali po elektronski pošti z okuženimi priponkami. Ob sprožitvi se je poslal prvim 50 stikom v imeniku v Outlooku, zato je preobremenil številne e-poštne sisteme. Povzročil je milijonsko škodo, čeprav na računalnikih hujše škode ni povzročal. Enkrat na uro je v odprte Wordove dokumente zapisal: *Twenty-two points, plus triple-word-score, plus 50 points for using all my letters. Game's over. I'm outta here*. Melissa ni bil prvi virus v makrojih, je bil pa z naskokom najbolj množičen.

Precej več posledic je imel ILOVEYOU, ki se je leta 2000 širil v obliki skripte za Visual Basic pod imenom LOVE-LETTER-FOR-YOU.TXT.vbs. Operacijski sistem Windows privzeto ni prikazoval končnic, zato je bila priponka v elektronskem sporočilu videti povsem neškodljiva. Ob zagonu je pobrisal dokumente in slike, skril datoteke MP3 in se prek Outlooka samodejno razposlal vsem stikom. Ker je bil napisan v VBScriptu, so ga lahko uporabniki enostavno spreminjali, zato so se na internetu kmalu znašle precej bolj uničujoče različice, ki so pobrisale več datotek in onesposobile sisteme.

Avtomatizacija

Naštetim virusom iz 90. let je bilo skupno zanašanje na žrtev, ki je morala odpreti okuženi dokumenti oziroma zagnati kakšno priponko. To se je po letu 2000 kmalu spremenilo, saj so splet preplavili virusi, ki so bili še *bolj agresivni*, hkrati pa niso zahtevali nobene uporabnikove interakcije. Zadoščalo je, da je bil računalnik povezan z internetom in neposodobljen ali brez protivirusnega programa. Na internetu še danes najdemo posnetke, kako hitro sveža namestitev Windows XP brez popravkov stakne virus,



▷ CIH se je odstranjeval z različnimi pripomočki.

△ **Blaster je povzročal ponovni zagon Windows XP.**

če računalnik povežemo z internetom. Leta 2004 se je to zgodilo povprečno 20 sekundah!

Predvsem pa po letu 2004, ko je širokopasovni dostop do interneta po svetu (in tudi pri nas) že postal običajen, virusi niso bili več bolj ali manj duhovite potegavščine. Tudi vandalizem se je počasi izpel, pisci so postali podjetni. Kriptovalut še ni bilo, a okuženi in stalno na internet priključeni računalniki so imeli svojo uporabnost. Leta 2004 je Sophos ocenil, da 40 odstotkov spama že pošiljajo zombiji, torej okuženi računalniki. Podjetje Sandvine je ta delež ocenjevalo celo na 80 odstotkov. Priče smo bili tudi prvim koordiniranim napadom (DoS), s katerimi so upravljavci množice okuženih računalnikov lahko začasno onesposobili celotne spletne strani. Druge možnosti zlorabe okuženih računalnikov so bili še pošiljanje virusov, kraja osebnih podatkov, razpečevanje otroške pornografije in razširjanje prevar.

Virusi so tedaj povzročili veliko preplaha, saj so se prvikrat zares hitro širili in dosegli milijone in milijone sistemov. V 80. in 90. letih to preprosto ni bilo mogoče, ker toliko računalnikov sploh ni bilo povezanih z internetom. Nato pa smo nenadoma dobili črve Code Red (2001), ki je napadal spletne strani z Microsoft IIS, Nimda (2001) SQL Slammer (2003), ki je povzročal napade DoS, Blaster (2003), ki je sprožal samodejni izhod iz Windows, in še mnoge druge.

Tatvine

Z bankami smo v prvem desetletju tega stoletja čedalje več poslovali prek računalnika, kar je virusom ponudilo čudovito priložnost. Njihovi avtorji so ugotovili, da je pritajeno čakanje na računalniku, dokler jim ne uspe izprazniti žrtvenega bančnega računa, donosnejša taktika od uničevanja. Leta 2007 je luč sveta ugledal Zeus, ki je prestrezal ter beležil vsebino zaslona in pritiske na tipkovnice, s čimer je poskušal dobiti prijavne podatke za e-banke. To so bili časi, ko banke (niti kdo drug) večinoma niso uporabljale dvostopenjskega preverjanja identitete (2FA). Zlasti v ZDA je Zeus povzročil veliko škode, saj so napadalci z bančnih računov žrtev prenakazali večje količine denarja, ki so ga iz bankomatov potem dvignili kurirji oziroma mule.

Eden večjih podvigov je predstavljal virus Carbanak, ki so ga odkrili leta 2014. Tudi tega so žrtve prejele v elektronskem sporočilu, nato pa so jim napadalci izpraznili bančne račune. Carbanak ni prizadel le fizičnih oseb, temveč so z njim okužili tudi banke in bankomate, manipulirali z njihovim delovanjem in jih pretentali, da so izvrgli bankovce. BlackPOS je šel leta 2013 še korak dlje in je okužil računalnike, ki so imeli priključene terminale POS (tedaj še niso bili samostojni). Sproti je shranjeval podatke o plačilnih karticah in jih nato pošiljal zlikovcem. Bil je tako premeten, da je z njimi komuniciral le med delovnim časom, da ni vzbujal nepotrebne pozornosti. Virusov, ki so neposredno ali posredno kradli denar, tedaj ni manjkalo. Dridex je to počel kot makro v Wordu, Trickbot je uporabljal več namenskih orodij za izrabo ranljivosti (EternalBlue, EternalRomance, EternalChampion).

Kraje informacij

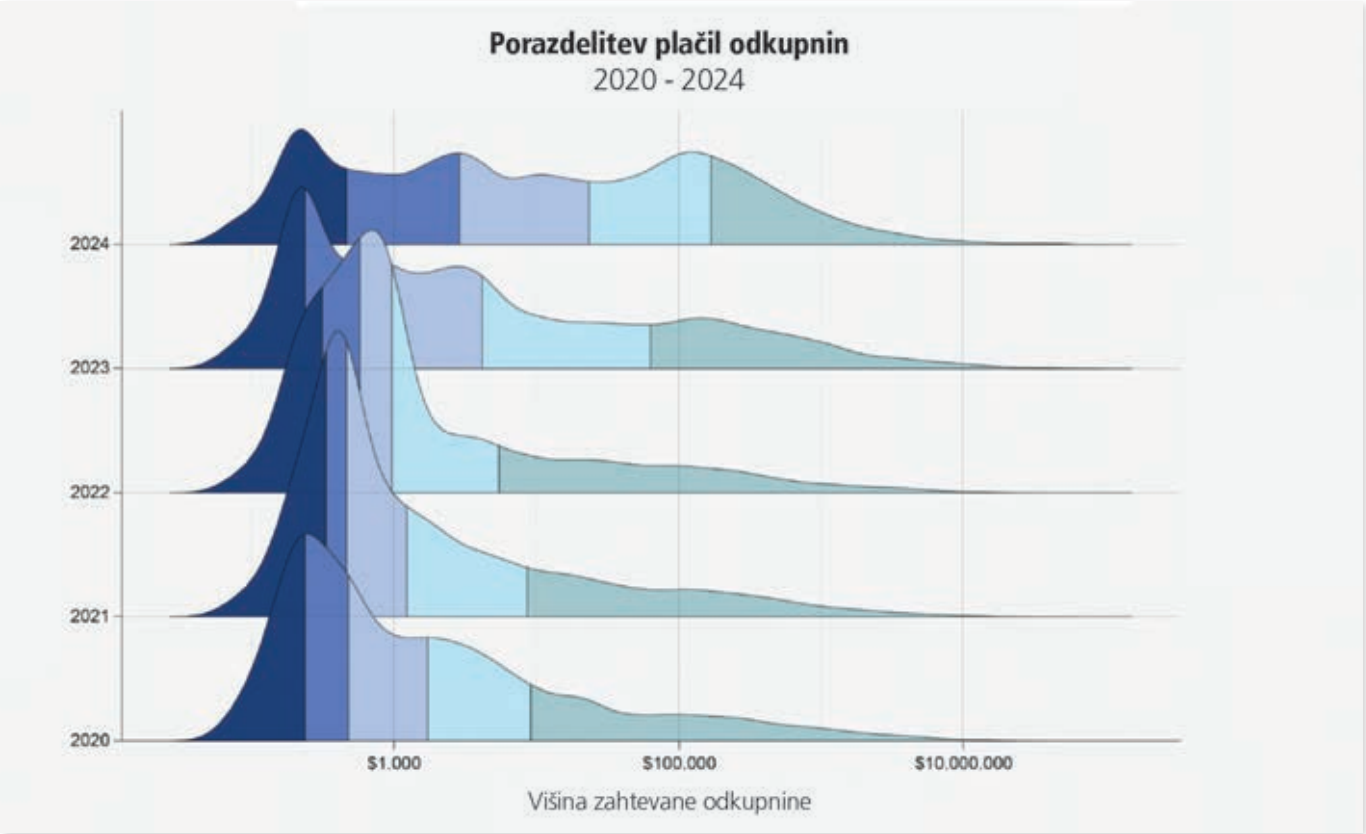
Po definiciji so virusi, ki so želeli krasti bančne podatke, morali vohuniti in deliti informacije, a na tem mestu nas zanimajo virusi, ki so informacije zbirali zaradi informacij samih. Znameniti primer je Red October, ki so ga oktobra 2012 odkrili v podjetju Kaspersky Lab. Deloval naj bi bil že vsaj pet, žrtve pa so ga staknile – kako predvidljivo – z okuženimi Wordovimi in Excelovimi dokumenti. Napadal je veleposlaništva po svetu, vojaške sisteme, podjetja, raziskovalne institucije in univerze, državne agencije itd. Avtorja niso nikoli identificirali, jezik komentarjev v kodi pa kaže, da so pisci kot materni jezik govorili rusko. Drugo desetletje tega stoletja je bilo polno podobnih virusov za vohunjenje: DuQu, Flame, Mahdi, Gauss in drugi. To so že bili virusi, ko se širili na nov način – z okuženimi ključki USB. Nekateri pa so se ugnezdili kar na infrastrukturo, denimo VPNFilter na usmerjevalnike interneta.

V tem času se je razvila tudi široka paleta virusov, ki so jih za prisluškovanje uporabljale različne države. V večini primerov jih sploh niso razvijale same, temveč so jih preprosto kupile, marsikdaj kot storitev (denimo orodje Pegasus izraelskega podjetja NSO Group). Še bolj specializirani pa so bili virusi, ki so povzročali fizično škodo, denimo Stuxnet, in so bili delo državnih hekerjev. O vsem tem pišemo v sosednjem članku.

Kriptovirusi

Posebno omembo zasluži CryptoLocker, ki se je sprva neovirano širil po internetu od septembra 2013 do razbitja maja 2014. To je bil prvi znani virus, ki

▽ **CryptoLocker je zahteval plačilo odkupnine v zameno za dešifriranje podatkov.**



△ **Porazdelitev višine odkupnin ob okužbah z izsiljevalskimi virusi.**

je datoteke zašifriral in od uporabnikov zahteval plačilo odkupnine v obliki bitcoinov. Marsikdo kljub njenemu plačilu ni mogel odšifrirati podatkov, ves svet pa si je oddahnil maja 2014, ko so policijske enote iz več držav v usklajeni akciji uničile botnet Zeus, ki je širil CryptoLocker, in pridobile zbirko šifrirnih ključev. Kasneje je bilo izdelano orodje za odklep datotek brez plačila odkupnine, a so ocenili, da so žrtve pred tem že plačale okrog tri milijone dolarjev. Nato se je pojavilo še nekaj klonov virusa, denimo CryptoWall in TorrentLocker, katerih avtorji niso bili povezani z originalnim.

CryptoLocker je nekritično ciljal na vse računalnike, ki so mu prišli na pot, zato je zahteval tudi sorazmerno nizko odkupnino (okrog 400 dolarjev). Po istih stopinjah je šel tudi WannaCry, ki je krožil leta 2017. Izrabljal je ranljivost v vseh tedaj aktualnih različicah Windows in od žrtev zahteval plačilo približno 300 dolarjev v bitcoinu. Raziskovalci so še isti dan odkrili, kako močno upočasniti njegovo širitev, saj je virus pred okužbo preveril, ali je posebna domena morebiti aktivna (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). Ko so jo registrirali, je bilo moč virus zajeziti, kasneje pa se je pojavilo še orodje za odklep datotek. Zanimivo je, da se je WannaCry širil z izrabo luknje, ki jo je Microsoft dva meseca pred izbruhom že zakrpal. Prizadeti so bili sistemi, ki niso namestili posodobitev. Poganjanje sistemov brez varnostnih posodobitev je tvegano, k čemur dodajmo, da bo Windows 10 letos oktobra izgubil podporo!

Zdi se, da so računalniki z Windows posebej ranljivi, a so zaradi najbolj razširjenega operacijskega sistema zgolj najprikladnejše tarče. Da to ni nujno, je dokazal Mirai, ki je leta 2017 napadal sisteme z Linuxom in celo pametne naprave, kot je usmerjevalnik ali pametni televizor. Za kratek čas je bilo popularno tudi *rudarjenje* kriptovalut, ki ga je Mirai krajši čas tudi izvajal. Tovrstne zamisli so pisci virusov kmalu opustili, saj je rudarjenje postalo računsko preveč potratno, da bi bilo smiselno na domačih računalnikih. Danes nihče več ne rudari na skrivaj.

Megavdori

Tudi danes so najpogostejši tip računalniških virusov izsiljevalski virusi, ki tako ali drugače želijo iz žrtve iztisniti finančno korist, še najraje v obliki odkupnine, ki se plača z bitcoini. Grozijo dvakratno: z razkritjem ukradenih podatkov, hkrati pa onesposobijo sisteme in zašifrirajo vse podatke žrtve. Tudi tarče izbirajo precej bolj premišljeno.

Lani so kriminalci s kriptovalutami v žepe pospravili vsaj 51 milijard dolarjev, so v februarskem poročilu ocenili v *Chainalysis*, a bo končni znesek še precej večji. Lani so ocenili, da je bilo leta 2023 tako odtujenih 24 milijard dolarjev, letos so vrednost za leto 2023 popravili na 46 milijard dolarjev, saj so nekatere denarnice identificirali, da so last kriminalcev. Enako bo veljalo tudi za leto 2024.

A omenjena vsota se nanaša na različne zlorabe, tudi na lažne spletne trgovine, ukradene kreditne kartice, razširjanje otroške pornografije in prevare vseh vrst. Na plačilo odkupnin po okužbah z izsiljevalskimi virusi je odpadlo »samo« 813 milijonov dolarjev, kar je 35 odstotkov manj kot leta 2023. Celoletni znesek se z manjšimi nihanji okrog milijarde dolarjev letno giblje že vsaj pet let. Zmanjšuje se tudi število izplačil, saj so računalniški sistemi čedalje bolj zaščiteni, a kadar napadalcem uspe prebiti zaščito, so lahko odkupnine visoke.

Porazdelitev odkupnin, ki je bila še pred petimi leti izrazito ozka in zgoščena okoli 500 dolarjev, ima dandanes precej daljši rep, ki sega krepko prek 100.000 dolarjev, neredko tudi milijona. Zgostitve so tri: pri 500–1000 dolarjih, okrog 10.000 dolarjev in nad 100.000 dolarji. Lani izstopa rekordnih 75 milijonov dolarjev, ki jih je skupina Dark Angels izsilila od podjetja Cencora, nekdaj znanega pod imenom AmerisourceBergen. Zahtevali naj bi bili še dvakrat več, a so po pogajanjih privolili v polovico nižjo odkupnino za 100 TB podatkov, ki so jih odnesli iz podjetja.

Dark Angels niso več novinci. Na spletu so se prvikrat pojavili leta 2022, odtlej pa so se uspešno izogibali preveliki publiciteti. Po lastnih navedbah naj bi nastali že leta 2021, prvi napadi pa segajo v april 2022, ko so uporabili orodje Babuk, kasneje pa RTM Locker, ki je razvit iz Babuka. Napadajo zelo izbrane tarče, ki pa jim ukradejo

TELEFONI

Virusi na **pametnih telefonih**

Pametni telefoni veljajo za odpornejše proti virusom – tudi zaradi operacijskih sistemov Android (ki temelji na Linuxu) in iOS (iz katerega je uporabnik skoraj zaklenjen) –, a niso imuni. Prva okužba sega dve desetletji v preteklost, ko je črv Cabir zmogel okužiti telefone z operacijskim sistemom SymbianOS prek bluetootha. Škoda je bila neznatna: telefon je prikazoval sporočilo Caribe ob vklopu.

Precej več nevšečnosti in stroškov je povzročil Joker, ki je leta 2017 napadel telefone z Androidom. Tarče je naročal na plačljive storitve prek SMS, ni bilo pa to njegovo edino početje. Simuliral je klike na reklame, v ozadju je zbiral podatke o dogajanju na telefonu (kjer imamo mobilno bančništvo) in podobno. Joker se skriva v več aplikacijah, ki se jim je uspelo prebiti na spletno tržnico Play Store, pojavlja pa se še danes.

Danes redko govorimo o virusih za telefone, namesto njih se bojimo škodljivih aplikacij, ki pa imajo običajno vgrajeno znano zlonamerno kodo. Te so v Play Storu največkrat Joker, Adware, Facestealer, Coper in Loanly Installer. To se zgodi, četudi Apple in Google preverjata, kaj se objavi na njunih spletnih tržnicah. Lani je Google blokiral 2,36 milijona škodljivih aplikacij, a je bilo kljub temu približno 200 škodljivih aplikacij prenesenih osemmilijonkrat. Nameni virusov na telefonih so mnogoteri: kraja podatkov, prijava žrtve na drage premijske storitve, prikazovanje oglasov in manipulacije. Običajno se skrivajo v na prvi pogled povsem neškodljivih aplikacijah.

V Applovem App Storu je stanje boljše, predvsem pa iOS ne dovoljuje nameščanja aplikacij iz drugih virov in uporablja podpisovanje (*Secure Enclave*), zato je izjemno težko dobiti kakšen virus. Izjema so seveda ciljani napadi, ki se jih gredo nekatere države, ki telefon odklenejo in nanj namenoma podtaknejo orodje za prisluškovanje. Tak primer je Pegasus iz NSO Groupa.

veliko podatkov in potem iztržijo bajne odkupnine. Leta 2022 so zgolj vdirali v sisteme in izsiljevali, že leto pozneje pa so na Telegramu začeli objavljati ukradene podatke. Aprila 2023 so vzpostavili tudi stran Dunghill Leak, ki je dostopna na omrežju Tor in kjer objavljajo odtujene datoteke. Za vdore izkoriščajo ranljivosti, do katerih dostopijo s pošiljanjem lažnih elektronskih sporočil v tarčah. Pri tem v nasprotju s podobnimi skupinami ne uporabljajo podizvajalcev oziroma RaaS (*ransomware-as-a-service*), temveč napade izpeljejo sami. Pri pregledu tarče in pridobljenih podatkov se tudi odločijo, ali bodo zgolj zagrozili z razkritjem podatkov ali jih bodo tudi zašifrirali in onesposobili njene računalniške sisteme. Njihov cilj namreč ni dvigovati prahu, temveč želijo čim bolj neopazno priti do odkupnine. Cencora sploh ni imela nobenih motenj v delovanju, plačilo je bilo izvedeno izključno zato, da bi preprečili deljenje ukradenih podatkov.

Profesionalizacija

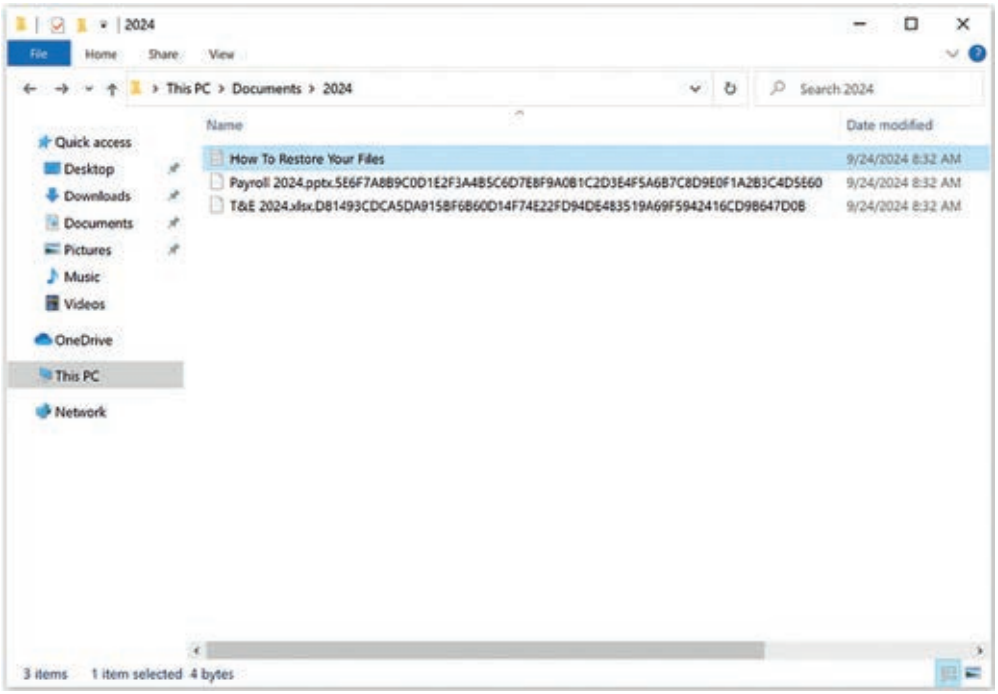
V tem pogledu so Dark Angels precej edinstvena skupina. Preostali izsiljevalski virusi ne izbirajo niti tarč niti metod. Leta 2021 je bil tarča napada Colonial Pipeline iz Atlante, zaradi česar so morali zapreti naftovode iz Teksasa do drugih zveznih držav na jugovzhodu. V zameno za orodje za odklep podatkov na računalniških sistemih so skupini DarkSide izplačali 75 bitcoinov, tedaj vrednih 4,4 milijona dolarjev; približno polovico so organi pregona kasneje zasegli.

Druge velike skupine, ki so lani nabirale izsiljevalske bitcoine, so Akira, Black Basta, Medusa, Play, Underground Team, Lockbit. Najpopularnejši način delovanja je omenjeni RaaS. Razvijalci izsiljevalskih virusov se ukvarjajo samo z razvojem in s podporo, nato pa jih prodajo drugim skupinam (*affiliates*), ki z njimi dejansko napadajo. Lockbit in Black Basta sta najbolj znana primera RaaS, ki ju uporabljajo v različnih prilagojenih različicah številne skupine, še zdaleč pa nista prva ali edina. Prvi je bil zelo verjetno Tox že leta 2015, številne druge pa so organi pregona z leti zaprli. DarkSide in Ryuk sta se poslovila leta 2021, REvil leto pozneje. Nadomestili so jih Hive, CLOP, Eldorado in drugi.

Poslovnih modelov je več: mesečna naročnina, enkratni nakup licence, delež odkupnine (ponavadi 20–40 odstotkov) ali partnerstvo (mesečna naročnina in manjši del odkupnin). RaaS resnično deluje kot storitev, saj naročniki dobijo možnost prilagajanja virusov, krmilno-nadzorne strežnike, pomoč pri vzpostavljanju plačilnih kanalov, postavitvi strani za deljenje ukradenih podatkov itd. Najbolj dodelani RaaS imajo svoje portale, kjer lahko naročniki spremljajo status svojih okuženih tarč, vsoto plačil, število zašifriranih datotek in drugo statistiko. Hkrati se RaaS oglašujejo na forumih, tekmujejo za naročnine, objavljajo na družbenih omrežjih itd. To je popolnoma profesionaliziran posel.

Virusi danes so posel podobne vrste, kot so bili piratski napadi na ladje pred stoletje. Organiziran, premišljen, strukturiran in do najmanjše podrobnosti načrtovan. Edina neznanka je le konkretna tarča, a brez ustrezne zaščite bomo to slej ko prej postali tudi sami. ◀

▽ **Izsiljevalski virusi zašifrirajo podatke na disku.**



Najšibkejši člen je uporabnik

Še pred nekaj leti smo ob zagonu novega računalnika najprej pomislili na namestitev protivirusnega programa, danes pa je jasno, da zgolj ena plast zaščite nikakor ni dovolj. Sploh pa težava pogosto ni v samem sistemu, temveč v uporabniku.

Računalniška varnost danes ni več vprašanje ene same aplikacije ali naprave, temveč celovite strategije, ki vključuje osnovno računalniško higieno, nenehno izobraževanje uporabnikov in premišljeno uporabo tehnologije. Vse se začne pri operacijskem sistemu – nekateri so tradicionalno bolj izpostavljeni napadom, preprosto zato, ker jih uporablja več ljudi. Tako pomembno kot izbira sistema je tudi redno posodabljanje – ne le operacijskega sistema, temveč tudi gonilnikov in aplikacij.

Najpomembnejše varovalo pa je kar naša zdrava pamet. Previdnost pri odpiranju priponk, dvom ob nenavadnih sporočilih in nezaupanje do nepreverjenih virov so ukrepi, ki rešijo marsikatero nevšečnost. Družinski računalniki, ki jih uporablja več članov gospodinjstva, pogosto nimajo niti osnovne ločnice med uporabniki. Uporaba enega samega administratorskega računa brez gesla ali s trivialnimi, kot je »1234«, odpira vrata številnim zlorabam. Pomembno je, da vsak uporabnik računalnika deluje v svojem okolju, z omejenimi pravicami, saj to znatno zmanjša možnosti za okužbo sistema. Enako velja za podjetja, kjer mora biti informacijska varnost del vsakodnevne poslovne prakse, ne pa prelaganje odgovornosti na zadnjo linijo obrambe – informatika.

Za povprečnega uporabnika je osnovna konfiguracija, ki jo ponujajo operacijski sistemi, običajno dovolj, a zahtevnejši uporabniki in podjetja lahko posežejo po naprednejših rešitvah. Sodobni protivirusni programi so danes precej več kot le orodje za iskanje virusov – vključujejo funkcionalnosti za varnostno kopiranje podatkov, upravljanje gesel, uporabo VPN, filtriranje spletnih vsebin in celo zaščito za spletno bančništvo. Čeprav večina uporabnikov teh funkcij ne izkorišča v celoti, ponujajo ti paketi precej višjo raven varnosti kot nekoč. A še vedno ostaja dejstvo:

Uporaba administratorskega računa z geslom »1234« odpira vrata številnim zlorabam.

nič ne more nadomestiti razumevanja, kako tehnologija deluje, in kaj se lahko zgodi, če ji slepo zaupamo.

In ko vse odpove, so zadnja linija obrambe varnostne kopije. Ko zlonamerna koda zaklene datoteke ali jih izbriše, lahko podatke reši le še to, če jih imamo shranjene še drugje. V svetu, kjer je mogoče skoraj vse digitalizirati, je varnostna kopija edina »analogna« rešitev, ki še vedno zanesljivo deluje.

Digitalna varnost ni enkratno dejanje, temveč neprestano ravnotežje med udobjem in zaščito. Vsak klik, vsaka nameščena aplikacija, vsaka priključena naprava je lahko nova priložnost za vdor ali okužbo. Če želimo ostati varni, moramo razumeti, da zaščita ni odvisna le od programske opreme, temveč predvsem od nas – naših odločitev, navad in pripravljenosti, da se učimo.

Bolje preprečiti, kot pa (pre)pozno zdraviti. ◀

Bolje preprečiti kot ...

Računalniški virusi, črvi, trojanski konji in drugi kosci zlonamerne programske opreme obstajajo praktično od samega začetka računalništva. Še pred dobrim desetletjem smo ob namestitvi operacijskega sistema Okna mrzlično iskali tudi najboljši protivirusni program, ker pravega soglasja o tistem najboljšem ni bilo. Dandanes pa velja, da je največja nevarnost za naše podatke v resnici naša naivnost, in to ne le na enem področju.

Matjaž Jeruc

Namestitev protivirusnega programa ni edina zaščita, ki jo naš računalnik potrebuje. Pravzaprav lahko spletno varnost razdelimo na različna področja, za katera je treba redno skrbeti, da nam bo naš računalnik, tablica ali telefon dolgo in dobro služil. Na dobro postavljenih temeljih, torej skrbi za operacijski sistem in programsko opremo, se začne vsaka zgodba o uspehu.

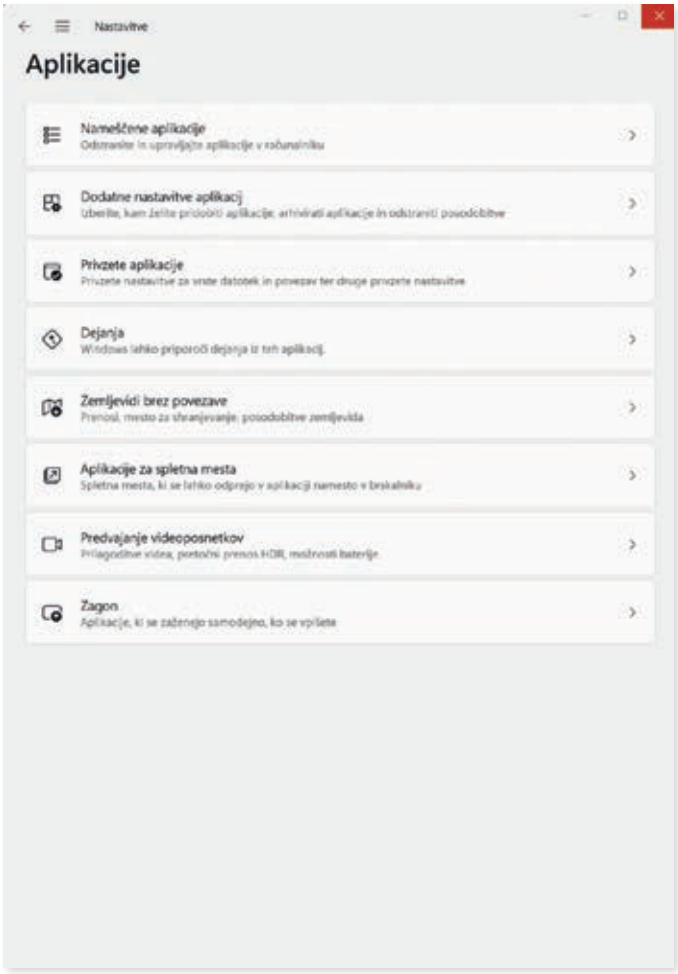
Dobro položeni temelji (operacijskega sistema)

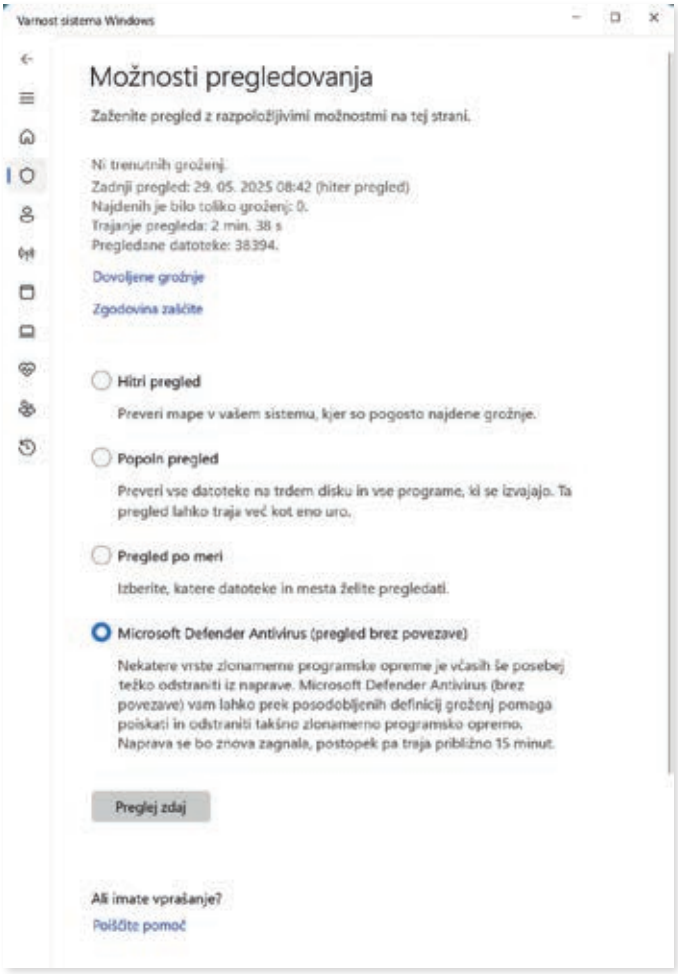
Začne se v resnici že pri izbiri samega operacijskega sistema. Microsoftova Okna, kot najbolj razširjen operacijski sistem na svetu, so bila že od samega začetka najbolj »hvaležna« tarča za napadalce in varnostne luknje v njih so bile najbolj zavzeto izkoriščane. Čeprav lahko z gotovostjo trdimo, da so imeli (imajo?) nekateri drugi operacijski sistemi boljše varnostne mehanizme kot Okna, pa množičnega števila virusov ne moremo preprosto pripisati slabemu načrtovanju in izvedbi. Ne gre zanemariti dejstva, da je to operacijski sistem, ki ga množično uporabljajo tudi tehnološko manj vešči uporabniki (v nasprotju z, recimo, različnimi distribucijami Linuxa), zato se je širjenje različne neželene programske opreme odvijalo z večjo hitrostjo, kot bi se sicer lahko. Širjenje virusov je bilo v preteklosti neizogibno povezano tudi s piratiziranjem programske opreme (predvsem iger), ki na drugih operacijskih sistemih ni bila tako dostopna.

Od leta 2012 je v Okna vgrajen res uporaben protivirusni program, ki je skozi dobro desetletje razvoja nosil različna imena in je danes poznan kot Protivirusni branilec (*Defender Protivirus*). Če smo povsem iskreni, česa boljšega za vsakdanjo rabo niti ne potrebujemo, četudi nas oglaševalske spletne strani konkurenčnih paketov prepričujejo o nasprotnem. Na različnih primerjalnih testih se Microsoftov branilec navadno izkaže kot zelo dober, kadar mora najti viruse, ki so (že nekaj časa) znani, manj pa, ko naleti na virus, ki je bil ravnokar »izvaljen«.

Uporabniki MacOS in različnih distribucij Linuxa poročajo, da je neželene programske opreme za njihove sisteme manj, a z večjo rabo teh operacijskih sistemov se vztrajno širi tudi »smetje«. Redno posodabljajmo operacijski sistem, tako se bodo namreč naložili tudi vedno sveži podatki o novih virusih ter zaščiti pred njimi, in večino dela smo s tem že opravili.

Prepričani smo, da se bodo mnogi med vami takoj sporekli





DOBRO GESLO

Kaj je dandanes **dobro geslo in alternative**

Priporočila za dobra gesla se iz leta v leto zaostrujejo in dandanes je priporočljivo geslo dolgo že 16 znakov ali več, ima raznolike znake (velike in male črke, številke, posebne znake kot so !, @ ali #) in je nepredvidljivo (torej ne vsebuje osebnih podatkov, imen, rojstnih datumov, naslovov in pogostih vzorcev kot so 12346 ali geslo). Vsaka storitev naj bi imela svoje unikatno geslo in priporoča se uporaba geselnih fraz v smislu ZeleniKonj!JeP 0wn0chiŠeV€dn0Z€len.

Čeprav se pogosto menjavanje gesel ne oglašuje več tako pogosto kot včasih, pa ob obilici različnih storitev hitro pridemo na sam rob človeških zmogljivosti pomnjenja. Iz istega naslova je tudi tvorba vedno daljših in daljših gesel vedno manj smiselna, strojna moč pa se iz leta v leto povečuje in tudi čas za razbitje gesel z metodo »gole sile« se vedno bolj krajša.

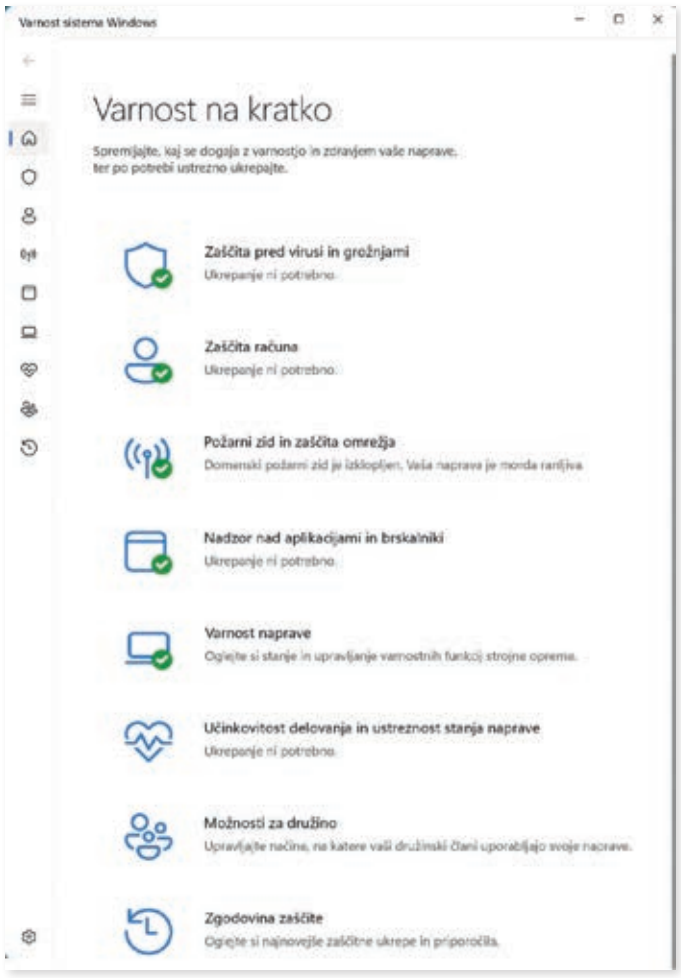
Za shranjevanje gesel se na trgu ponuja kar nekaj ponudnikov, ki trdijo, da so njihove shrambe varne in da lahko opravilo pomnjenja ter vsakokratnega vnosa gesla prepustimo kar njim. Med boljšimi so zagotovo storitve podjetja 1Password in Bitwarden, a zavedajte se, da absolutne varnosti ni in da se vdor lahko zgodi tudi najboljšim. Prav v ta namen imajo boljše storitve podporo tudi za geselne fraze in se povezujejo tudi z dvofaktorsko avtentikacijo (katerakoli kombinacija dveh ali več različnih načinov preverjanja pristnosti).

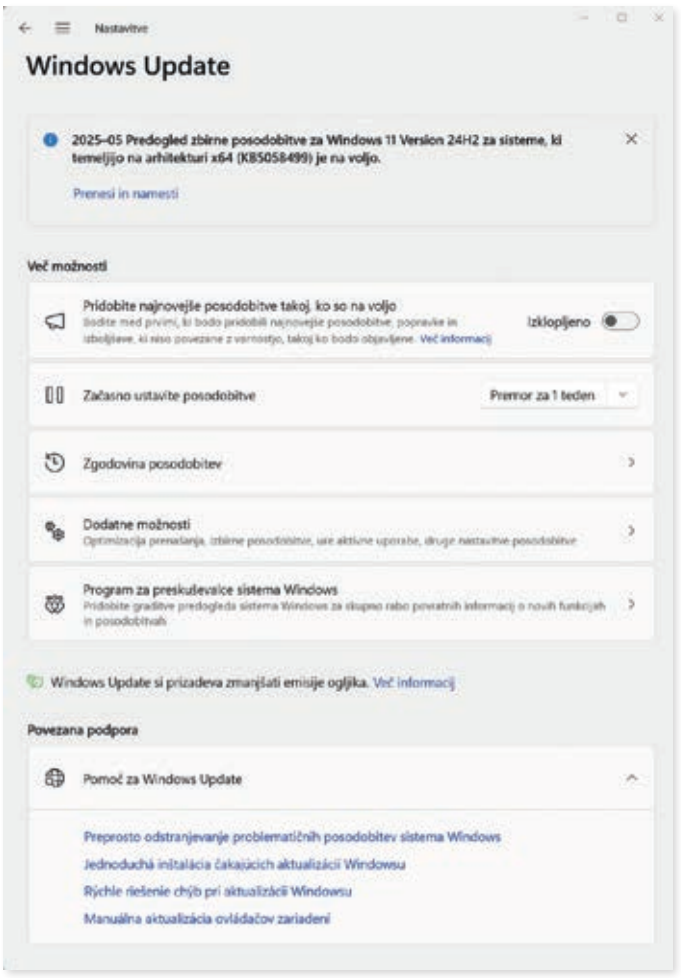
Med alternativami geslom se uporabljajo biometrični podatki (prstni odtis, obraz, šarenica, glas), ki so na mobilnih napravah tako rekoč standard in skupaj z uporabo varnostnih ključev tvorijo tako imenovano prijavo brez gesel. A če se biometrične podatke ukrade, jih iz očitnih razlogov ni moč ponastaviti. Omenimo še preverjanje prek potisnih obvestil in vnosa unikatno generiranih kod (Microsoft Authenticator, Google Prompt), SMS in sporočil po e-pošti.

Med bodoče načine preverjanja pristnosti (ker je trenutno za vsakdanjo rabo še preveč nezanesljiva) pa zagotovo spada vedenjska biometrija, ki preverja uporabnika tudi po samem načinu uporabe, torej kako tipka, premika miško, hodi, premika glavo ipd.

z nami in nam hiteli razlagati o neodpiranju čudnih priponk, datotek na ključkih USB, diskih, cedejih in podobno. Osebno prenosnih naprav USB za prenašanje datotek, slik, videov in različnih preglednic sploh ne uporabljamo že dolgo vrsto let. Večino stvari si pošljemo po elektronski pošti oziroma, še raje, datoteke delimo prek oblačnih shramb. Tak način prenašanja datotek mimogrede preverja tudi okužbe z morebitnimi virusi in potencialno nevarnih datotek niti ne dovoli pošiljati oziroma nalagati. Seveda ima taka raba tudi svoje slabosti, predvsem se moramo vprašati, kje se ti naši podatki nahajajo in kaj si podjetja dovolijo z njimi početi (o čemer pa več lahko preberete v zadnji redni številki Monitorja).

Da, vse manjša uporaba pomnilniških medijev USB je na smetišče zgodovine poslala večino tako imenovanih trojancev in črvov, a v skladu z našo »spletno potrošnjo« so se spremenili tudi virusi. Vsaj tako pomemben dejavnik, kot je





ČIŠČENJE WINDOWS

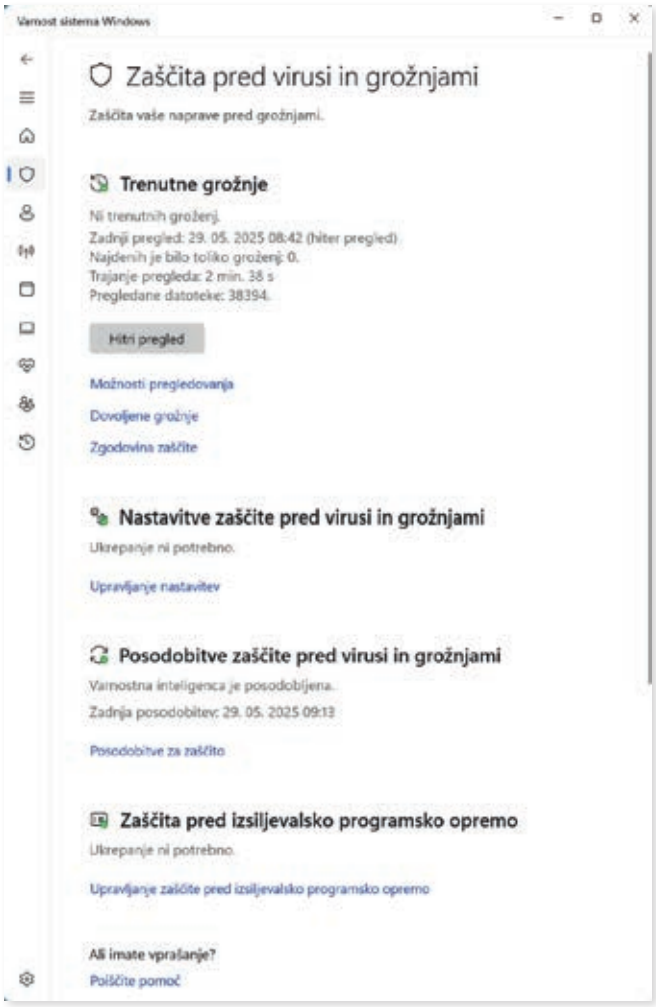
Hitri pregled in čiščenje

V Oknih 11 osnovna vzdrževalna opravila niso več nobena umetnost; posodobitev operacijskega sistema, gonilnikov in Pisarne predlagajo sama Okna, na vas je le, da najdete čas, kdaj boste to opravilo prepustili računalniku. Če si želite sami ogledati, kako stvari stojijo, pa v nastavitvah Oken (ki jih ponavadi skriva ikona zobnika) poiščite *Windows Update*.

Varnostni elementi se skrivajo v razdelku Zasebnost in varnost ter podmeniju Varnosti sistema Windows, ki s preprostim sistemom semaforja takoj da vedeti, kje se nahajajo težave. Vmesnik je intuitiven in ni potrebno veliko znanja, da izvedete osnovni, napredni ali popolni pregled računalnika.

Med Nastavitvami pa najdemo tudi razdelek Aplikacije, ki omogoča pregled nad nameščenimi programi, kjer jim lahko spreminjamo nastavitve ali jih odstranimo. Med aplikacijami si lahko ogledate tudi, katere so privzete aplikacije za odpiranje posameznih datotek in storitev ter katere aplikacije se odprejo takoj ob zagonu računalnika (ter jih tudi ustrezno omejite).

posodabljanje operacijskega sistema, programov in gonilnikov, ki jih uporabljamo, pa je tudi njihovo odstranjevanje, če jih ne uporabljamo več oziroma so zastareli in brez podpore. Ranljivosti nimajo le operacijski sistemi, ampak jih najdemo v vsaki programski opremi, strojni programski opremi različnih naprav, ki jih uporabljamo, in pravzaprav v vsaki napravi, ki ima vgrajen vsaj krmilnik in pomnilnik. In namenskega



protivirusnega programa za vašega sesalnega robota v tem trenutku najbrž še ni …

Zdrava pamet

V zadnjem desetletju se je zlonamerna programska koda preusmerila iz računalnika na splet, tako kot tudi večina naših podatkov. Lažno predstavljanje (*phishing*), zlonamerne spletne strani in napadi prek ranljivosti v programski opremi najbolj merijo na naivnost, nevednost, včasih pa tudi dobronamernost uporabnika. Banke nas tedensko opozarjajo, naj ne nasedamo lažnim obvestilom o potrebnem dodatnem posredovanju podatkov na čudne elektronske naslove ali pa celo lažne spletne strani bank, ki so namenjene zgolj kraji dostopnih podatkov. Na video portalih si lahko dnevno ogledamo posnetke ogoljufanih strank, ki so prek klica iz domnevno Microsoftove podpore, da je nekaj narobe z njihovim računalnikom, ostali brez prihrankov. Zdi se kot pretiravanje, a če take na videz preproste goljufije ne bi delovale, potem tudi obvestil o prevarah ne bi bilo več.

Na prvi pogled se mogoče zdi, da »cepiva« za človeško naivnost, razen nenehnega izobraževanja, ni. Vendar pa v skladu s pregovorom, da je previdnost mati modrosti, lahko sprejmemo nekatere ukrepe, da naivnost ne more biti kaznovana. Recimo, da nehamo uporabljati administratorske račune operacijskih sistemov za uporabnike, ki ne vedo, kaj delajo, in povsem nekritično nameščajo programsko opremo neznanega izvora ter klikajo tisti znameniti Naprej, dokler je to fizično mogoče. Na tak način lahko neposredno preprečimo, da bi nevešč uporabnik na računalnik namestil nekaj, kar na računalniku nima kaj iskati.

Pravzaprav nas vedno znova šokira, kako zelo malo ljudi v resnici doma uporablja ločene račune za vsakega člana družine; v večini povprečnih gospodinjstev najdemo računalnike z enim administratorskim računom, ki, uganili ste, nima nastavljenega nobenega gesla ali, kar je celo še slabše, ima geslo v obliki 1234. Zelo na hitro rečeno ima račun brez nastavljenega gesla blokiran vsaj oddaljeni dostop, kar je v primeru slabega gesla ovira za zgolj nekaj pičlih milisekund. Kdor je kadarkoli delal v podjetju kot informatik, ve, da je obdobje po dopustih vedno prvenstveno namenjeno obnovitvi gesel, ki so med dopustom izpuhtela. O tem, kakšna gesla je še smiselno nastavljati, pa pišemo v okvirčku.

Požarni zid, ki ne varuje pred ognjem

Požarni zid v računalniških omrežjih deluje kot filter med računalnikom in internetom, saj nadzira ves vhodni in izhodni promet v računalnik oziroma napravo ter iz njiju ter blokira nepooblaščen dostop. V praksi to pomeni, da požarni zid lahko prepreči, da bi se zlonamerna programska oprema povezala z zunanjimi strežniki ali pa da bi nepridipravi dostopali do našega sistema. V večino operacijskih sistemov je požarni zid že vgrajen oziroma ga je moč namestiti, samo nastavljanje pa zahteva računalniško znanje, ki se ne šteje za osnovno. Podjetja in napredni uporabniki lahko uporabljajo tudi strojne požarne zidove, torej namenske naprave, ki poskrbijo, da se zaradi tega internetni pro-

Banke nas redno opozarjajo, naj ne nasedamo lažnim pozivom za posredovanje podatkov.

met ne upočasni pod sprejemljivo mejo.

V Oknih je požarni zid sicer nameščen in delujoč, kar priča tudi semaforček v Varnosti sistema Windows. Za osnovne potrebe sicer zadošča, a »pirati« med bralci ste se zagotovo srečali z delovanjem požarnega zidu, ko ste poskušali »deliti« kako datoteko z drugimi uporabniki. Kako je požarni zid nastavljen pri vas, je v veliki meri odvisno od tega, koliko različnih programov ste

TELEFONI

Mobilna zaščita

Za mobilne naprave poleg vsega v članku naštetega velja, da je treba zelo veliko pozornosti posvetiti izvorom aplikacij, ki jih nameščamo na svojo napravo, in pa dovoljenjem, ki jih aplikacije zahtevajo. Če aplikacije nameščamo iz uradnih trgovin (Play ali App store), bojazni skorajda ni, saj se Google in Apple trudita že v kali zatreti vsako neželeno programsko opremo. Vseeno pa, ko nas aplikacije sprašujejo, ali jim dovolimo uporabljati neko funkcionalnost naprave, krepko razmislimo, kaj v resnici dovoljujemo. Mar naš robotski sesalnik resnično potrebuje dostop do naših fotografij? In naš tiskalnik, mar res potrebuje dostop do mikrofona naprave?

»Piratsko« navdahnjeni bralci vedo, da lahko mobilne naprave tudi »odklenemo« (*rootamo*, *jailbrejkamo* in podobno), s čimer ponavadi odklepamo zmogljivosti, ki so jih proizvajalci zaklenili, ali pa nameščamo programsko opremo, ne da bi zanjo plačali. Vir takih aplikacij so pogosto vprašljive spletne strani, ki ne ponujajo nobenega jamstva, da so aplikacije, ki se jih namešča, tudi v resnici varne. Pod vprašanjem torej ni le garancijsko jamstvo naprave (ki je ponavadi s takim dejanjem izničeno), ampak tudi podatki v njej.

V zadnjem obdobju se je doba programske podpore mobilnim napravam močno podaljšala; večina proizvajalcev novih naprav tako obljublja najmanj petletno podporo v obliki nadgradenj, popravkov in izboljšav programske opreme naprave, kar nekako sovpada z njeno uporabno dobo (z izjemo baterije). Zavedajte pa se dejstva, da je naprava, ki že dolgo časa ni posodobljena oziroma varnostnih popravkov niti ne prejema, prava varnostna »črna« luknja v vašem žepu.

Kaj pa mobilni protivirusni programi, povprašate. Kot smo že pisali v samem članku, je njihova največja dodana vrednost v dodatnih zmogljivostih, ki jih ponujajo (VPN, zaščita pred krajo, spletni filtri, zaščita pred *phishingom*), in pa dejstvu, da Android in iOS v osnovi nimata nameščenega klasičnega protivirusnega programa. Hkrati pa velja poudariti dejstvo, da imata oba operacijska sistema vgrajene varnostne mehanizme, ki delujejo kot zaščita pred zlonamerno programsko opremo. Odločitev je torej prepuščena vam in vašim potrebam; za vsakdanjo rabo, in če ne tvegate z odklepanjem naprave in nameščanjem nepregledane programske opreme, niso zares potrebni.

na operacijski sistem že naložili in kolikim ste tak ali drugačen dostop do vašega računalnika tudi dovolili prek pojavnih oken, ki so zahtevala dostop. Požarni zid namreč lahko nastavljate na različne načine: bodisi dovoljujete ali blokirate dostop različnim programom bodisi zaščito nastavljate na transportni plasti računalniških omrežij (odpiranje vrat in protokolov). Prvi način je nekoliko lažje razumljiv laikom, a s tem tudi manj zanesljiv, saj v resnici ne vemo, kaj program v ozadju počne oziroma s kom komunicira.

Ali za to, da boste enkrat v letu s plaže dostopali do svoje mobilne banke, res potrebujete VPN?

Je protivirusni program res še to?

Ker imajo Okna že dobro desetletje vgrajeno zelo spodobno zaščito pred virusi in ostalo zlonamerno nesnago, so se nekdanji veliki igralci (Bitdefender, Norton, Malwarebytes in drugi) morali prilagoditi. Poleg preboda na mobilne naprave, o katerih več pišemo v okvirčku, so zraven osnovne zmogljivosti morali ponuditi še nekaj več. Nekateri v kompletu ponujajo tudi orodje za izdelavo varnostnih kopij, napredne požarne zidove, VPN, upravljalnike gesel, filtre spletnih strani, »peskovnike« za spletno bančništvo, podporo več operacijskim sistemom (tudi za mobilne naprave) in še bi lahko naštevali. Dodana vrednost je torej v preventivi pred človeško naivnostjo, ki jo sicer lahko nadomesti tudi zdrava kmečka pamet in pa kakšno izobraževanje na temo spletne varnosti. Svoje osnovno poslanstvo, torej zaščito pred zlonamerno programsko opremo, večina paketov opravlja več kot zgolj zadovoljivo, izrazite favorite pa torej iščite tam, kjer za svoj denar dobite največ (pa če to v resnici potrebujete ali ne).

Posebno mesto v tej zgodbi imajo VPN, navidezna zasebna omrežja, ki so poleg zasebnosti in varnosti (ki jo, roko na srce, večina povprečnih uporabnikov le stežka upraviči, poznavalci pa uporabljajo strojne rešitve priznanih podjetij) postali pravi prodajni hit zaradi odklepanja geografsko omejenih vsebin na vse bolj popularnih pretočnih video in igričarskih storitvah. Kar ponavadi lahko preberete v drobnem tisku, je seveda to, da vseh storitev ne podpirajo, da jih ne podpirajo ves čas, da ponudba lahko variira in da ugodna cena zgolj ene kavice na mesec velja zgolj ob zakupu triletnega paketa. VPN vam za potrebe službe ponavadi priskrbi delodajalec, ki ga skrbi za lastne podatke, oziroma za to poskrbite sami z namensko rešitvijo, ki najbolj ustreza vašemu podjetju. Ali VPN potrebujete za to, da boste enkrat v letu dostopali do svoje mobilne banke s plaže na hrvaški obali, pa presodite sami.

Varnostne kopije

Ko odpove čisto vsa zaščita, nas še vedno lahko rešijo dobro načrtovane in redno izvajane oziroma posodabljane varnostne kopije. Če bi v resnici postali tarča premišljenega hekerskega napada, katerega cilj je ukrasti podatke, jih zakleniti in nam jih prodati v zameno za bitcoin, dva ali tri, nam pogosto preostane le še restavriranje podatkov, če jih seveda imamo kje shranjene. Povprečni uporabniki si želijo zgolj povrnitve slik in videov, posameznih elektronskih dokumentov, ki jih nimajo natisnjenih, in to je v večini to. Smiselno je imeti najmanj tri varnostne kopije, dve na isti lokaciji (torej v naši hiši, stanovanju, sobi) in tretjo nekje zunaj stalnega bivališča (lahko tudi v oblaku) za primer, če bi nas poleg hekerskega napada doletelo več tegob hkrati (kakšen požar, potres, poplava ali celo vojna).

Varnostne kopije lahko delamo ročno oziroma uporabljamo sinhronizacijske možnosti (torej svoje podatke kopiramo na zunanje diske, oblačne shrambe), opravilo lahko prepustimo operacijskemu sistemu, kjer povemo kakšno vrsto varnostne kopije si želimo (tukaj je med bolj znanimi program Time Machine, vgrajen v Mac OS), lahko pa si za to omislimo programsko opremo določenega podjetja (med bolj znanimi so Acronis, Macrium ali EaseUS Todo).

Pri podjetjih je načrtovanje varnostnih kopij del širše varnostne politike podjetja in bi morala biti plod skrbnega načrtovanja več strokovnjakov in tudi končnih uporabnikov. Poleg samih podatkov je marsikje pomemben tudi čas, ko storitve podjetja niso na voljo in pomenijo tudi izpad vira prihodkov ter zaslužka.

Računalniška, spletna in pa seveda tudi fizična varnost so v veliki meri odvisne od poznavanja problematike, volje za učenje in sredstev, predvsem finančnih, ki so nam na razpolago. Mnogokrat najdražje rešitve niso nujno tudi najboljše, prav tako pa velja, da upoštevanje osnovnih navodil, ki jih naštevamo skozi celoten članek, odpravi 99,9 odstotka potencialnih varnostnih pomanjkljivosti povsem povprečnih domačih uporabnikov. Za kaj več, sploh če želite zaščititi občutljive podatke svojega posla, pa bo treba seči v žep in plačati za znanje ter predvsem izkušnje. Te pa se gradijo predvsem na napakah in seveda na okužbah ter vdorih v sisteme. ◀

Ko država postane **heker**

Kaj se zgodi, ko države prekršijo pravila igre in ko v boj za nadzor, informacije in varnost vstopijo z orodji, ki so bila nekoč domena hekerjev, a jih danes razvijajo zasebna podjetja po naročilu državnih organov? In kaj pomeni, ko sredi miru postanemo tarče – ne vojakov, ampak vrhunskih vrstic kode?

V zadnjem desetletju se je svet dramatično spremenil. Komunikacija je postala digitalna, podatki so postali ključna valuta, nadzor pa neviden. In čeprav nas številne tehnologije varujejo – s šifriranjem, z varnostnimi posodobitvami in zavestjo o zasebnosti –, se vedno znova izkaže, da so največja grožnja pogosto prav tisti, ki bi nas morali ščititi.

Raziščimo to temno plat digitalne moči držav! V ospredju ni le vohunjenje – temveč sistematična uporaba sofisticiranih orodij za vdor v telefone, računalnike, komunikacijska omrežja in celo fizično infrastrukturo. Pogosto brez sodnih odredb, včasih tudi brez zakonite podlage, skoraj vedno pa v imenu »varnosti«, »interesa države« ali »zaščite družbe«.

Kaj sploh še pomeni zasebnost, če lahko država prestreže skoraj vsak pogovor?

Kdo razvija ta orodja? Kdo jih kupuje? Na koga merijo? In kaj se zgodi, ko tako orodje uide nadzoru ali ga uporabijo proti lastnim državljanom?

Predstavljamo konkretne primere iz prakse: vdor v telefone opozicijskih aktivistov in novinarjev, tajna sodelovanja z zasebnimi podjetji, ki prodajajo ranljivosti namesto rešitev, ter primere, ko so države same izvajale kibernetske napade na tuje infrastrukture. Od odmevnega primera Pegasus do tihih (kitajskih?) preusmeritev internetnega prometa, od vladnih poskusov razbijanja šifriranja telefonov do sabotažnih virusov, ki so uničevali industrijske sisteme.

Digitalna tehnologija ni le priročen pripomoček za vsakdan – postala je nova fronta geopolitičnih iger, tihih pritiskov in nevidnega nadzora. Ob tem se zastavlja vprašanje: kaj sploh še pomeni zasebnost, če lahko država – ali kdorkoli, ki ima dovolj denarja – prestreže skoraj vsak pogovor, vdre v vsak telefon in manipulira z informacijami, ki krožijo po omrežjih?

Odpiramo vrata v svet, kjer države niso vedno zaščitnice svobode, temveč lahko postanejo tudi tihi napadalci v lastni soseski. Ne iščemo teorij zarote, temveč konkretne primere, preverjena dejstva in resnične zgodbe o tem, kako se državna moč uporablja v digitalnem prostoru – včasih upravičeno, a pogosto brez nadzora in odgovornosti. ◀

Zlobne države

Države bi nemalokrat želele dostopiti do pametnih naprav državljanov ali prisluškovati njihovim komunikacijam, a zaradi moderne tehnologije in vseprisotnega šifriranja tega vedno ne znajo same. Zatekajo se k nakupom programov ali storitev zasebnega sektorja, ki izkoriščajo ranljivosti ali kako drugače odklepajo moderne pametne naprave in računalnike. Primerov ni malo.

Matej Huš

V svobodnem svetu država načelno ne sme nepovabljeno kukati, kaj šele vstopati v tuja stanovanja. Za nasilen vstop obstajajo stroga merila, katerih izpolnjevanje *pred* vstopom običajno preveri sodišče (izjeme so redke, recimo, če kdo iz stanovanja kliče na pomoč), predvsem pa je v stanovanje težko vstopiti na skrivaj. Prestrezanje pisem je z nekaj truda že mogoče izvajati praktično neopazno, povsem pa so se posegi v zasebnosti skrili s prihodom elektronskih telekomunikacij.

Zasebnost napadajo z dveh strani: uporabnik težko zazna, da mu kdo prisluškuje ali vdira v elektronsko napravo, po drugi strani pa te naprave vsebujejo več osebnih podatkov kot pisma ali celo stanovanja. Situacijo je dodatno zapletel izum šifriranja od konca do konca (*end-to-end encryption*), ki je lahko matematično varno in nezlomljivo. Država v takem primeru do podatkov ne more, četudi bi imela legalno podlago, zato pritiska na proizvajalce sistemov, da jih namerno ošibijo, s čimer pa bi lahko vanje vdirali tudi zlikovci. V svetu elektronskih naprav in interneta namreč razdalje ni, vsi smo drug drugemu sosedje.

Precej spremenjene razmere in nove tehnološke možnosti so zato vaba, ki se ji države težko uprejo. Četudi nimajo zakonitih razlogov ali pa zato, ker gre za tarče v tujini, iščejo načine za vdore v računalniške sisteme, telefone in druge elektronske naprave, s katerimi želijo pridobiti podatke o posamezniku. Včasih morejo, a ne smejo, kar jih ne ustavi. Spet drugič ne morejo, pa smejo, kar jih jezi, zato iščejo neobičajne poti, vdirajo in hekajo. Še raje pa na pomoč pokličejo profesionalce, ki delujejo v sivem svetu senc. Primerov, ko so države vdirale v elektronske naprave, ne manjka.

Pegasus

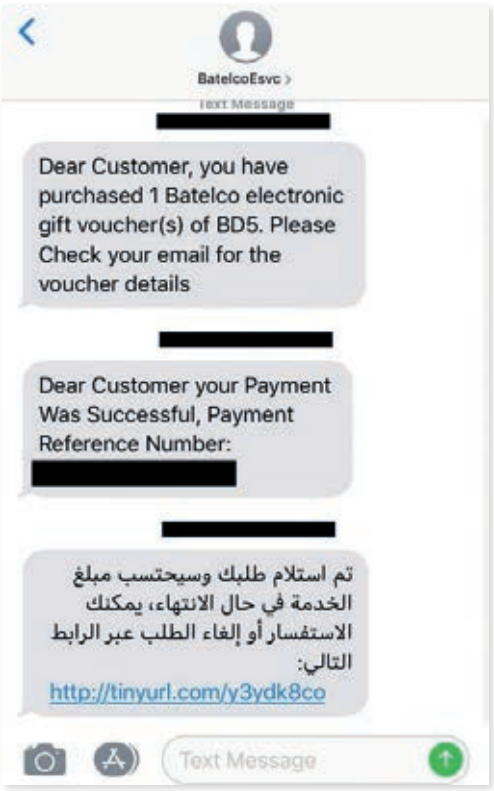
Maja letos je okrožno sodišče v severni Kaliforniji odločilo, da mora NSO Group podjetju Meta plačati 167 milijonov dolarjev kazenske odškodnine, ker je bilo njegovo orodje Pegasus uporabljeno za vdor v več kot 1.400 uporabnikov Whatsappa. Že decembra lani je sodišče ugotovilo, da je NSO Group odgovoren, ker Pegasus na telefone nameša in z njim pridobiva podatke NSO Group, in ne države, za katere to počne. Zdaj pa je to še odškodninsko ovrednotilo.

NSO Group je zloglasno izraelsko podjetje, ki razvija orodja za vdiranje v računalniške sisteme. Kratica NSO sestoji iz začetnic imen trojice (Niv, Shalev, Omri), ki je podjetje ustanovila leta 2010. Petnajst let pozneje ima podjetje več kot 700 zaposlenih in stranke po vsem svetu. Njegov glavni izdelek se imenuje Pegasus, ki so ga prvikrat izdali leta 2011 in ga odtlej redno posodabljajo. Pegasus je po mnenju izraelske vlade orožje, zato za njegovo prodajo in izvoz potrebujejo posebne licence, ki se izdajajo le za državne kupce. Namenjen je pridobivanju podatkov s telefonov iPhone in Android, torej vohunjenju, namestijo pa ga lahko oddaljeno brez sodelovanja (*zero-click exploit*) tarče. Na njenem telefonu potem bere sporočila, snema klice, zbira gesla, shranjuje lokacijo, vklaplja kamero in mikrofon, vpogleduje v aplikacije itn.

Za Pegasus je širša javnost izvedela leta 2016, ko je Citizen Lab objavil poročilo o neuspelem poskusu vohunjenja za nekim aktivistom. Da gre za razširjeno taktiko, smo ugotovili leta 2020, ko je v javnost pricurljal seznam 50.000 telefonskih številk, za katerimi so različni akterji vohunili s Pegasusom. Seznam sta prva objavila Amnesty International in Forbidden Stories, kasneje pa je zgodbo preiskalo več kot 80 novinarjev največjih svetovnih medijev. Med tarčami je bilo tudi 14 svetovnih voditeljev držav, tudi francoski predsednik Emmanuel Macron in evropski komisarji, pa še številni drugi iz Alžirije, Belgije, Egipta, Iraka, Jemna, Južne Afrike, Kazahstana, Libanona, Maroka, Pakistana, Ugande. Vidni politiki, diplomati, aktivisti, novinarji, oporečniki in ostale tarče pa so bili še iz drugih držav, tudi Finske, Španije, Velike Britanije in Madžarske, če se omejimo le na nekatere evropske. Morda najbolj znana tarča pa je bil novinar Jamal Khashoggi iz Savdske Arabije, ki so mu prisluškovali, preden so ga umorili na savdskoarabskem konzulatu v Turčiji. Nekoliko manj razvpit je primer tajskega aktivista Jatupata Boonpattararakse, ki so mu leta 2021 v telefon vdrli kar trikrat. NSO Group je tožil, a je zaradi pomanjkanja dokazov tajsko sodišče sodbo zavrglo.

NSO Group nikoli ni zanikal uporabe svojih orodij za vdore, a so vedno poudarjali, da jih le prodajajo državam, ki potem z

Primerov, ko so države vdirale v elektronske naprave, ne manjka.



◁ Napadi NSO napadi potekajo tudi s sporočili SMS.

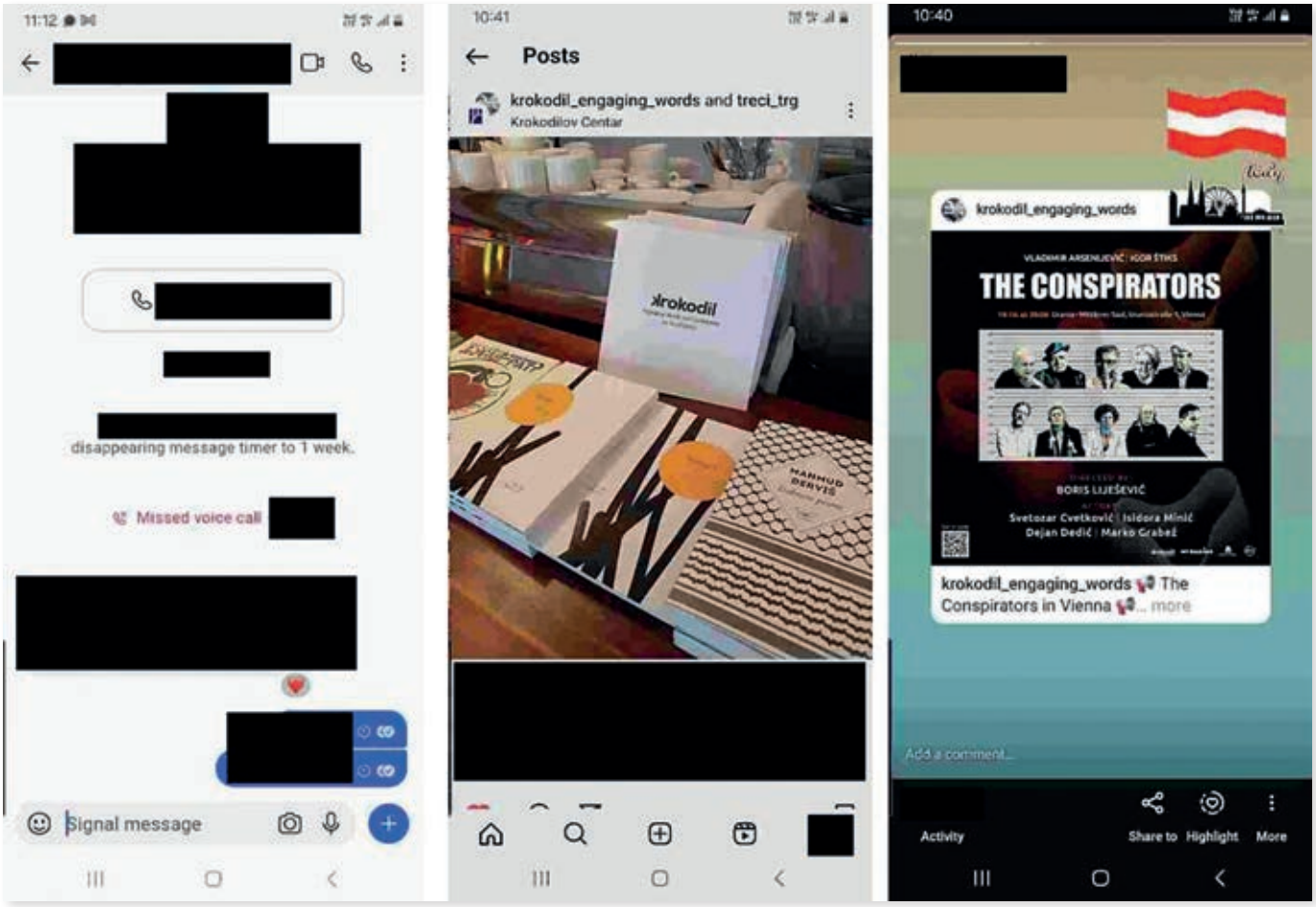
njim ravnajo v skladu z zakonodajo. Vsaj tako obljubljajo.

Srbski študentje

Konec lanskega leta smo iz poročila Amnesty International izvedeli tudi, da srbski organi pregona uporabljajo orodja NSO Group in Cellebrite za nadzor nad novinarji in aktivisti. Novinarja Slavišo Milanova so februarja lani pridržali med na videz rutinskim nadzorom prometa, ob čemer so mu za nekaj ur odvzeli telefon. Ko ga je dobil nazaj, je opazil nenavadno obnašanje, zato ga je poslal Amnesty International. Tam so odkrili sledove programske opreme UFED, ki jo izdeluje podjetje Cellebrite. Z njo so nanj namestili orodje NoviSpy, ki je beležilo pogovore in slike zaslona.

Amnesty International je odkril tudi, katere ranljivosti je NoviSpy uporabil za namestitev, zato so jih sporočili Googlu in Qualcommu, ki sta hitro ukrepala. Prav tako jim je uspelo s številnih telefonov na daljavo pobrisati NoviSpy. To ni bil osamljeni primer, saj so marca letos izdali novo poročilo, v katerem so opisali še dva potrjena primera, ko so srbske oblasti poskušale vdreti v telefone novinark v BIRN (*Balkan Investigative Reporting Network*) – to pot z orodjem Pegasus. Cellebrite je že februarja dejal, da bodo sodelovanje s Srbijo prekinili, NSO Group pa bolj pragmatično zatrjuje, da sodelujejo le z državami, ki orodja uporabljajo v zakonite namene. Amnesty International sicer v poročilu *Digital Prison* ugotavlja, da v Srbiji vsaj tri leta sistematično prisluškujejo novinarjem, aktivistom in drugim za oblast motečim dejavnikom.

▽ **Slike, ki jih z okuženih telefonov zajema srbski NoviSpy.**



MANIPULIRANJE USMERJEVALNIKOV

Kitajska **pomota**

Dobrih 15 odstotkov vsega svetovnega internetnega prometa je 8. aprila 2010 teklo skozi kitajske usmerjevalnike, česar uporabniki nismo opazili. To ni bil edini tovrstni primer, saj je v preteklem desetletju svetovni internetni promet večkrat za krajši čas tekel skozi Kitajsko. V nekaterih primerih je šlo za dalj časa trajajoče preusmeritve, denimo šestmesečni obvoz iz Kanade v Južno Korejo skozi Kitajsko v letu 2016. V drugih primerih je celo promet med Švedsko in Norveško ter Japonsko potoval na Kitajsko.

V vseh primerih gre za napačne nastavitve strežnikov BGP (*Border Gateway Protocol*), ki usmerjajo internetni promet. Usmerjevalniki uporabljajo informacije BGP, da pravilno pošiljajo pakete z enega naslova IP na drugega. Usmerjevalniki z BGP oznanjajo, do katerih naslovov lahko najhitreje spravijo promet. Zaščit ni, saj BGP nima ustreznih mehanizmov za zagotavljanje zaupanja. V teoriji lahko torej kdorkoli oznanja katerikoli naslov, pa bo začel dobivati promet, ki je namenjen tja.

Ali Kitajska namerno preusmerja svetovni promet k sebi ali gre za napake v nastavitvah, je nemogoče dokazati. Bolj jasen je pakistanski primer, ko so leta 2008 zaradi sodbe sodišča želeli blokirati Youtube znotraj svojih meja, nato pa je Pakistani Telecom (avtonomni sistem 17557) začel oznanjati naslov 208.65.153.0/24, ki ga je PCCW Global (avtonomni sistem 3491) posredoval vsemu svetu. Youtube je tedaj globalno nehal delovati za skoraj tri ure.

Manipuliranje BGP (*BGP hijacking*) je sicer zelo primitiven način napadov, ki se konča bodisi z nedostopnostjo strani bodisi s preusmeritvijo vsega (sicer šifrirnega prometa), zato za prisluškovanje ni preveč uporaben. Povzroča pa nemalo škode in slabe volje.

Hekerje napadli hekerji

Pegasus je osupnil svet predvsem z obsegom vohunjenja – tako po številu tarč kakor naročnikov –, še zdaleč pa ni prvo orodje za te namene. Na naslovnice je FinFisher prispel leta 2014, ko so hekerji vdrli v njegovega razvijalca Gamma in na internetu priobčili izvorno kodo

△ **Citizen Lab je leta 2015 med uporabniki FinFisherja izpostavil tudi Slovenijo, česar uradno ni nikoli nihče potrdil.**

orodja, podatke o ceni, seznam strank in druge interne dokumente. Gamma Group je angleško-nemško podjetje z nejasnim lastništvom in registracijo v davčni oazi na Britanskih deviških otokih. Že leta 2013 smo vedeli, da ga uporablja vsaj 36 držav, med njimi tudi Avstrija, Madžarska, Nemčija, Srbija, leto pozneje pa smo se muzali ob objavi 40 GB ukradenih podatkov. Citizen Lab je leta 2015 na seznam verjetnih uporabnikov umestil tudi Slovenijo.

FinFisher se je osredotočal na vdore v računalnike, ne toliko v pametne telefon, ker so bili leta 2013 časi drugačni. Širil se je s priponkami v elektronski pošti, z lažnimi programskimi posodobitvami in prek ranljivosti v programski opremi. Čeprav je bilo uporabnikov oziroma naročnikov mnogo, poznamo zgolj nekaj konkretnejših zgodb. Z njim naj bi prisluškovali turški in ugandski opoziciji, bahrajnskim aktivistom, novinarjem, odvetnikom in politikom. V Bahrajnu so aktivisti med arabsko pomladjo (2010–2012) prejemali elektronska sporočila (*phishing*), ki so imela okužene priponke, podobno se je širil tudi v Egiptu dve leti pozneje. V Turčiji pa so leta 2016 kar na vladne spletne strani naložili FinFisher, tako da so ga obiskovalci staknili s prenosom obrazcev in programske opreme.

Medtem ko FinFisher *še* deluje, dasiravno pod drugim dežnikom (trenutno Lench IT Solutions), pa je italijanski Hacking Team klavno propadel. Podjetje iz Milana je bilo butični igralec s slabimi sto zaposlenimi v Italiji, ZDA in Singapurju, njegove izdelke pa so uporabljali v več desetih državah po vsem svetu. Leta 2015 jih je prizadel vdor, s katerim so hekerji odnesli 400 GB podatkov, ki so jih potem postavili na splet. HackingTeam si nikoli opomogel, leta 2019 jih je kupil InTheCyber Group. HackingTeam je razvijala platformi Da Vinci in Galileo, ki sta beležili dogajanje na okuženih sistemih, ki so bili raznovrstni – Windows, Linux, Mac OS, Android, iOS in drugi. Vdor leta 2015 je bil poveden zlasti zato, ker je razkril kupce, ki niso bile le države. Med njimi sta bila tudi Deutsche Bank in British Telecom.

Intellexa

Kako različna je lahko obravnava podjetij, ki razvijajo, preprodajajo ali izrabljajo ranljivosti, priča Cytrox. V nasprotju z NSO Groupom ali Cellebritom, ki sta spoštovana dobavitelja več držav, tudi ZDA, se je Cytrox leta 2023 znašel na seznamu podjetij, proti katerim so Američani uvedli sankcije, ki so jih lani še zaostrili. Te veljajo tudi za vodilne zaposlene v podjetju. Cytrox je del skupine Intellexa Consortium, ki razvija orodje Predator. Pri prodaji državam nima demokratičnih zadržkov, zato so ga dobavili tudi sudanskim milicam in egiptovski obveščevalni službi, poslovali pa so s Cipra.

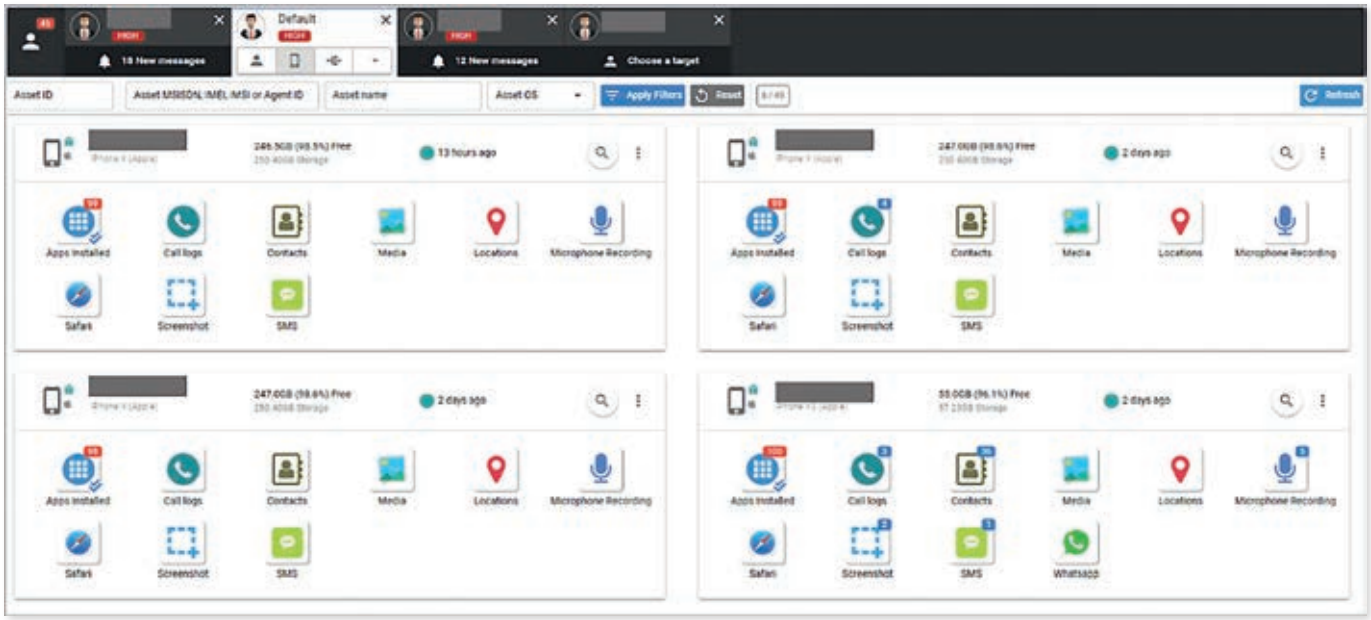
Cytroxovi začetki so zaviti v tančico skrivnosti, pred petimi leti pa je podjetje pristalo v lasti nekdanjega poveljnika iz izraelske vojske. Omenjeni Tal Dilian je tudi ustanovitelj skupine Intellexa, katere izdelke Predator, Alien in druge so zaznali že v več kot 25 državah. Obsežna preiskava Amnesty International in Der Spiegla je leta 2023 pokazala, da so napadli vsaj 27 posameznikov v 23 institucijah. Med njimi so bili predsednica evropskega parlamenta, nemški veleposlanik v ZDA, tajvanski predsednik, ameriški senatorji in drugi.

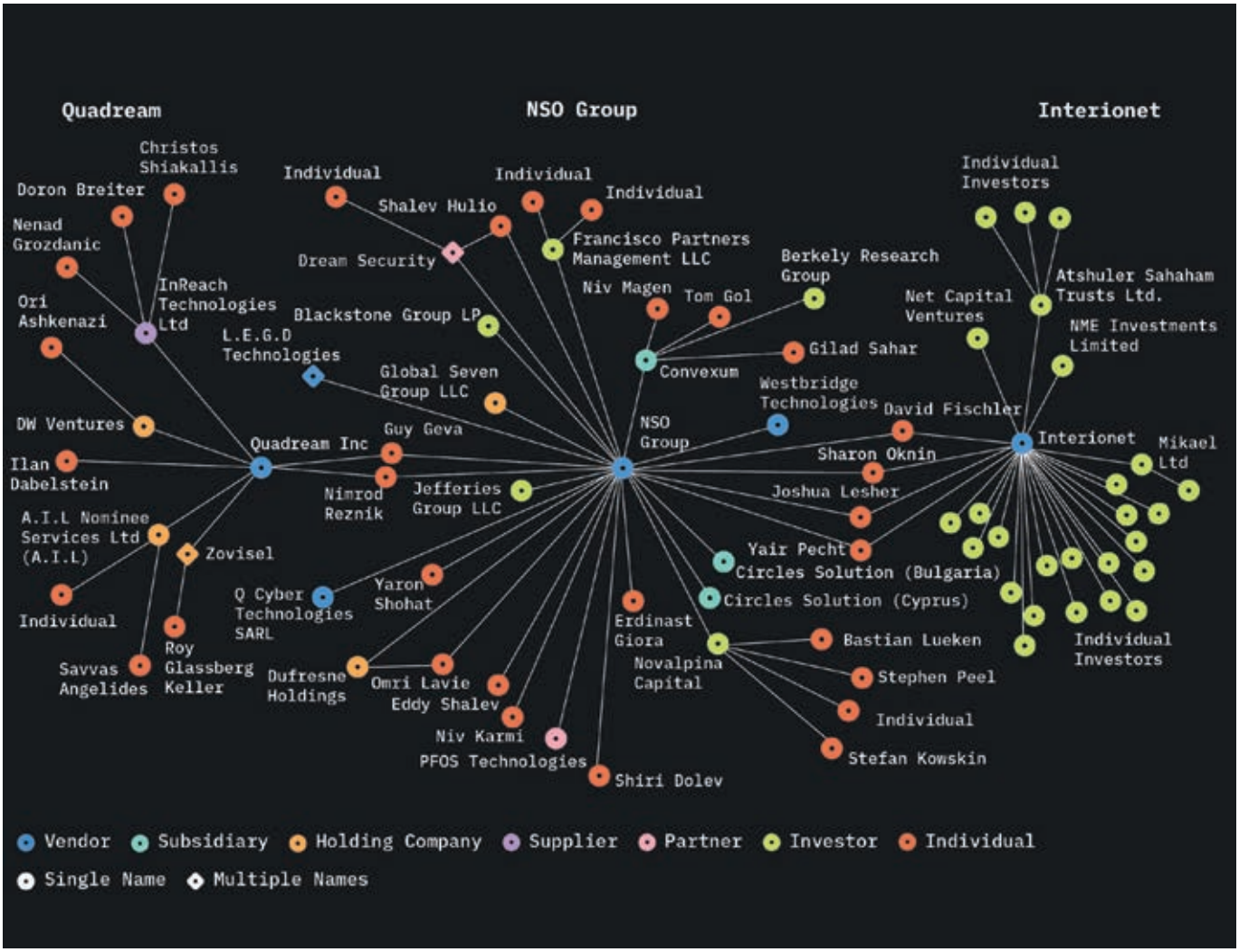
V skupini Intellexa so podjetja Wispear/Passitor (Ciper), Cytrox (Severna Makedonija), Cytrox Holdings (Madžarska), Intellexa (Grčija), Intellexa LTD (Irska), Thalestris ltd (Irska). Sodeluje s skupino Nexa, v kateri so še Nexa Technologies (Francija),1 Nexa Technologies CZ s.r.o ***(Češka),*** Advanced Middle East Systems (ZAE), Trovicor (ZAE).

Največji škandal na evropskih tleh sega v leto 2022, ko so v Grčiji s Predatorjem prisluškovali

Cytrox so uporabili za prisluškovanje predsednici evropskega parlamenta, nemškemu veleposlaniku v ZDA, tajvanskemu predsedniku, in ameriškim senatorjem.

▽ **Intellexa Predator za vdiranje v telefone.**





△ Grozd podjetij okoli NSO Group. Slika: Atlantic Council

Mitološke zveri

Atlantic Council je septembra lani objavil poročilo *Mythical Beasts*, v katerem so poskušali osvetliti svet preprodajalcev ranljivosti in izdelovalcev orodij za državno rabo. Preiskali so obdobje v letih 1992–2023 in odkrili prepleteno omrežje, ki ga sestavlja 49 proizvajalcev opreme za vdore, 36 podružnic, 24 partnerskih podjetij, 20 dobaviteljev, 32 holdingov ter 95 investitorjev. Podjetja se povezujejo v tri večje grozde – izraelskega, italijanskega in indijskega, redno sodelujejo, se povezujejo, spreminjajo imena in sedeže. Vsaj 80 držav na svetu je kupilo programsko opremo od vsaj enega takega podjetja. V Evropski uniji je vsaj 14 držav kupovalo opremo od NSO Group.

več opozicijskim politikom in novinarjem. Grška vlada je bila vpletena v nakup in uporabo Predatorja, česar niso priznali, so pa potrditi vohunjenje za novinarjem Thanasisom Koukakisom. Leto pozneje je informacijski pooblaščenec odkril 220 sporočil SMS, ki so bila poslana na različne številke, v njih pa je bila povezava, ki okuži s Predatorjem. Med njimi so bili najvišji politiki, poslovneži, novinarji in drugi.

Odklepanje iphonov

Apple se rad pohvali, da sta zasebnost in varnost uporabnikov na prvem mestu, in to tudi trži kot konkurenčno prednost. Podatki v iCloudu so lahko šifrirani tako, da jih niti Apple ne more prebrati, že prej pa je to veljalo za podatke na napravah, zlasti pametnih telefonih. Dokler so telefoni zaklenjeni, je vanje *skoraj* nemogoče vstopiti, sodišča tako v ZDA kakor v EU pa so že večkrat povedala, da je vnos gesla *pričanje*. V samoovadbo pa človeka ni mogoče prisiliti. Pod črto lahko dodamo še, da odklep telefona s prstnim odtisom ali z biometrijo ni definiran kot pričanje, zato nas organi pregona ali sodišče v to običajno prisilijo. Tega se zaveda tudi Apple, ki je lani novembra posodobil iOS tako, da se telefon po 72 urah ponovno zažene, če ga v tem času nismo uporabljali. Po vsakem zagonu pa je za prvi odklep treba vpisati geslo, podatki pa so še bolj zaščiteni kot, če je telefon zgolj zaklenjen med uporabo.

V preteklih letih smo bili priče več razvpitim primerom, ko so imeli osumljenci ali storilci pri sebi telefon, na katerem bi lahko bili za preiskavo relevantni podatki. V nekaterih primerih ga je FBI hitro odklenil, drugič je trajalo precej dlje. Prvo veliko reklamo o zatesnjenosti iphona je Apple dobil leta 2016, ko se je FBI mesece mučil z odklepom iPhona 5C. Pripadal je Syedu Rizwanu Farooku, ki je 2. decembra 2015 v San Bernardinu v Kaliforniji skupaj s Tashfeen Malik streljal na božični zabavi in ubil 14 ljudi ter jih še 22 ranil. Policija je nekaj ur po napadu storilca izsledila in ju ustrelila, nato pa se lotila odklepanja njunih telefonov.

Farookov iPhone 5C je bil zaklenjen, podatki pa šifrirani. Starejše kopije so preiskovalci lahko sneli iz iClouda – ki tedaj še ni poznal šifriranja s ključem brez Applove vednosti –, novi podatki pa so bili le na telefonu. Do njih FBI ni mogel, pri čemer mu niti Apple ni mogel pomagati, saj ni poznal kode (PIN) za odklep. Deset napačnih vnosov bi nepovratno izbrisalo ključ za dostop do podatkov. FBI je od Appla zahteval pomoč, a mu Apple ni želel ali mogel (šlo je za kombinacijo) pomagati. Apple bi bil moral napisati novo različico iOS z naluknjano zaščito, česar Apple ne bo nikoli storil, so zagotovili v Cupertinu.

Ko se je zdelo, da se bo pat položaj vlekel mesece, je 28. marca FBI sporočil, da jim je neznana stranka pomagala odkleniti telefon. Kdo in kako je to storil, nismo nikoli uradno izvedeli.

OSLABITEV ŠIFRIRANJA

Zakonita **ranljivost**

V časih državam sploh ni treba iskati obvodov, skrivnih vhodov ali stranskih vrat, temveč preprosto sprejmejo zakon, ki jim omogoča dostop. V Veliki Britaniji že od leta 2016 velja Zakon o preiskovalnih pooblastilih (*Investigatory Powers Act*), ki je dobil leta 2024 amandma, na podlagi katerega je vlada januarja letos Applu izdala ukaz (*Technical Capability Notice*) o oslabitvi šifriranja. Apple za podatke v oblaku iCloud omogoča šifriranje podatkov od uporabnika do oblaka, kar imenuje ADP (*Advanced Data Protection*). Do teh podatkov niti Apple nima dostopa, ker nima ključa za dešifriranja, zato organom pregona uporabnikovih podatkov *ne more* dati, četudi bi dobil sodno odredbo. V Veliki Britaniji je bil ADP na voljo od leta 2022 do februarja letos, ko so ga ukinili zaradi omenjenega ukaza. Velika Britanija je zahtevala vgradnjo stranskih vrat, ki bodo organom pregona omogočila dostop do podatkov, a Apple vztraja, da šifriranje s stranskimi vrati pač ni šifriranje, zato so ADP raje ugasnili. Apple se je sicer tudi pritožil, postopek pa še teče. V njegov prid so se oglasile številne nevladne organizacije, zagovorniki zasebnosti in tudi druga podjetja, Veliko Britanijo so okrcali celo v ameriškem kongresu, a ostaja neomajna.

△ **Apple je moral v Veliki Britaniji ukiniti šifriranje v iCloudu.**

Neuradno je krožilo več teorij: izraelsko podjetje Cellebrite, neodvisni hekerji z zlorabo nezakrpane (*zero-day*) ranljivosti v iphonu, avstralsko podjetje Azimuth Secruity ali ameriško podjetje Grayshift.

Zelo podoben primer se je vlekel več mesecev po terorističnem napadu na vojaško bazo Pensacola na Floridi, v katerem je strelec Mohammed Saeed Alshamrani decembra 2019 ubil tri vojake. Napad se je končal, ko so ga ubili, za njim pa sta ostala tudi zaklenjena iPhone 5 in iPhone 7 Plus. FBI se je za pomoč obrnil na Apple, a ga je pričakal znani odgovor: lahko vam posredujemo vse podatke iz iClouda, varnostnih lukenj pa v IOS ne bomo vrtali. Šele maja prihodnje leto je FBI sporočil, da so telefona odklenili, a ob tem ni pozabil skorajda užaljeno poudariti, da brez Applove pomoči. Generalni tožilec je dobesedno zapisal: »*Zahvaljujoč odličnemu delu FBI – in brez zahvale Applu – nam je uspelo odkleniti Alshamranijeva telefona.*« Da, tudi uradne izjave niso imune na pikrost.

Precej težje je z novimi iphoni. Newyorškega župana Erica Adamsa so septembra lani obtožili več kaznivih dejanj, med drugim podkupovanja, prejemanja daril in poneverb. Iphone in ipad so mu zasegli že novembra 2023, na osebnem telefonu pa je pred tem zamenjal kodo za odklep, da ne bi kdo izmed članov njegovega osebja pomotoma česa izbrisal, trdi Adams. Kodo je nato prikladno pozabil in FBI prinesel zaklenjeni telefon. FBI je želel pridobiti vsebino telefona, a jim to da aprila letos ni uspelo. Apple je vnovič zavrnil kakršnokoli pomoč pri odklepu, vsebina v iCloudu pa je tako šifrirana, da niti Apple nima ključa. Nato je pravosodno ministrstvo pod novim ameriškim predsednikom zahtevalo ustavitev pregona. Žal nikjer v sodnem spisu ni zabeležena ključna informacija: *kateri* iphone in katero različico iOS uporablja Adams. Očitno pa je, da je uporabljal zgolj PIN, ne pa tudi biometričnih podatkov za odklep ali pa je bil telefon na sveže ponovno zagnan.

Androidni telefoni še manj varni

Zadnji primer je sorazmerno svež. Matthew Crooks je julija lani streljal na Donalda Trumpa, med aretacijo pa so zasegli tudi njegov Samsungov Android telefon. FBI v Pittsburghu sicer ni imel ustreznega orodja za odklep, v forenzičnem centru v Quanticu v Virginiji pa s tem niso imeli težav. Sami sicer niso zmogli, zato so na pomoč poklicali stare znance iz podjetja Cellebrite. Uporabili so njihovo orodje in nekaj tehnične pomoči iz podjetja, da so v 40 minutah odklenili telefon. Podobni postopki ponavadi trajajo mesece, a to pot je šlo za absolutno prioriteto. Ob tem povejmo, da je imel storilec kar šest telefonov, med njimi tudi Applove, v katere FBI ni mogel, Apple pa mu kljub moledovanju Donalda Trumpa ni pomagal.

Cellebrite sicer javno ne oglašuje svojih zmogljivosti, a občasno kaj pricurlja v javnost. Lani poleti je *404 Media* poročal, da zmore Cellebrite odkleniti vseh iphone do različice 17.4 in Android 14. Z nekaterimi novejšimi Googlovimi pixli imajo sicer še nekaj težav, a v večino naprav lahko vstopijo. Cellebrite gre pri skrivnostnosti celo tako daleč, da v pogodbah z organi pregona zahteva molčečnost o uporabi tehnologije tudi na sodišču.

PRESKOK V FIZIČEN SVET

Uničevanje infrastrukture

V veliki večini primerov so vdori in napadi držav namenjeni pridobivanju informacij, v bolj radikalnih primerih brisanju podatkov, precej redkejši pa so napadi s posledicami v realnem svetu. Med njimi moramo omeniti očeta vseh napadov, črva Stuxnet. V iranske centrifuge za bogatenje urana v Natancu ga je leta 2008 na USB-ključku prinesel Erik van Sabben, kasnejše različice črva pa niso več potrebovale mule, temveč so se širile same. Stuxnet so razvili Američani in Izraelci, njegova naloga pa je bila sabotaža jedrskega programa. Stuxnet je spreminjal nastavitve Siemensovih programljivih logičnih krmilnih enot (PLC), zaradi česar je fizično okvaril centrifuge.

Decembra 2015 je Ukrajina ostala brez električne energije v dveh zahodnih pokrajinah, kar je prizadelo okrog četrt milijona odjemalcev. Zlonamerni program BlackEnergy 3 se je ugnezdil na računalniške sisteme treh dobaviteljev električne energije, ki so nadzorovali sisteme SCADA v razdelilnih postajah, zaradi česar je bila za nekaj ur motena dobava električne energije. Leto dni pozneje se je napad ponovil v Kijevu. Precej obširnejši pa je bil napad junija 2017, ko je črv Petya na videz deloval kot izsiljevalski program in je tudi prizadel več držav, a je bil v resnici osredotočen na Ukrajino in napisan tako, da je povzročil največ škode. V vseh primerih strokovnjaki kot najverjetnejšega napadalca navajajo Rusijo.

Cellebrite ne želi, da bi se kakršnekoli podrobnosti o zmožnostih ali celo tehnikah vdorov omenjale na sodiščih ali pristale v dokaznem gradivu.

Podtikanje certifikatov

V nekaterih primerih so bile države tako nerodne, da je težko oceniti, ali so imele resne namene prisluškovati, je šlo zgolj za preverjanje terena ali pa enostavno niso imele ustreznih znanj. V to kategorijo sodi Kazahstan, ki je svojim državljanom kar trikrat poskusil podtakniti lastne certifikate, na koncu pa so obupali.

Že decembra 2015 so izdali samopodpisani korenski certifikat (*root certificate*), nato pa je nacionalni ponudnik interneta Kazakhtelecom zahteval, da ga uporabniki interneta namestijo na svoje naprave. Poimenovali so ga certifikat za nacionalno varnost in bi ga morali začeti uporabljati januarja 2016. Odbor za telekomunikacije, informatizacijo in informatiko pri ministrstvu za investicije in razvoj, ki je regulator interneta, je zapisal, da zakon o telekomunikacijah zahteva uporabo novega certifikata za zaščito prometa. Certifikat je nekaj dni enako skrivnostno, kot se je pojavil, tudi izginil.

Poskusili so še dvakrat. Julija 2019 so tamkajšnji ponudniki dostopa do interneta svoje stranke spet začeli obveščati, da morajo namestiti korenski certifikat (*Qaznet Trust Certificate*), a je bil odziv proizvajalcev brskalnikov jadrn. Mozilla in Google sta že avgusta sporočila, da omenjenega certifikata ne bosta upoštevala, četudi bi ga uporabniki ročno namestili. Ko je decembra 2020 Kazahstan poskusil še v tretje, je bil odziv enak.

Pravih razlogov ne poznamo, a jih ni težko uganiti. Korenski certifikat predstavlja izhodišče v verigi zaupanja, ki temelji na overiteljih in njihovem podpisovanju certifikatov. Če država izda korenski certifikat, lahko teoretično izvaja napade s prisluškovanjem MITM (*man in the middle attack*). Četudi je promet zašifriran s tem certifikatom, ga lahko država odklene (ker ima pripadajoč zasebni ključ), prebere in potem zašifrira s pravim ključem stran, ki jo želi obiskovalec v resnici videti. Napadi MITM temeljijo na podtikanju javnih ključev, ki niso v lasti organizacije, za katero se lastnik izdaja. Če pa država uporabnike prisili v namestitev takih certifikatov, sploh ni treba ničesar na skrivaj podtakniti, saj uporabniki svoje brskalnike odklenejo kar sami. Analiza je pokazala, da je bilo prizadetih vsaj 37 domen in, zanimivo, ne vsi uporabniki, temveč zgolj stranke Kazakhtelecoma (avtonomni sistem 9198 KazTelecom).

Če država izda korenski certifikat, lahko teoretično izvaja napade s prisluškovanjem MITM (man in the middle attack).

Podoben incident je izbruhnil tudi februarja 2015, ko so na prenosnih računalnikih proizvajalca Lenovo odkrili samopodpisane certifikate, ko so imeli enake zasebne ključe na vseh računalnikih. Razlog je bil v programski opremi Superfish Visual Search, ki je bila prednameščena na njih. Microsoft je kmalu izdal popravek, ki je prisilno izbrisal Superfish, Lenovo pa je kasneje sklenil več sodnih poravnav in v ZDA kupcem prizadetih prenosnikov plačal 3,5 milijona dolarjev. ◀

Ko se vojna **preseli v kodo**

Vojne se danes ne začenjajo več s topovi, temveč z računalniško kodo. Nevidni konflikti se odvijajo na strežnikih, med podatkovnimi centri in prek signalov, ki potujejo skozi satelite in optična vlakna. V svetu, kjer je internet postal ključno bojno polje, kibernetski napadi niso več zgolj tehnični incidenti – postajajo strateško orožje, s katerim države izvajajo pritisk, kriminalne združbe kopičijo dobičke, politični akterji pa oblikujejo novo ravnotežje moči.

Digitalna doba ni le posodobila orodij, s katerimi se vodi vojna – preoblikovala je sam pojem konflikta. Napad na bolnišnico lahko danes pomeni zaklep informacijskega sistema in onemogočanje operacij. Vdor v državno agencijo ni več le tatvina podatkov, temveč poseg v politično suverenost. Izsiljevalski virusi so v kratkem času postali donosnejši kot trgovina z mamili, umetna inteligenca pa odpira vprašanja, ki presegajo inženirsko domišljijo: lahko stroj sam odloča, kdo bo živel in kdo umrl?

V tej novi realnosti državne meje ne nudijo več zaščite. Napadalci so lahko kjerkoli – v podzemlju ruskih forumov, pisarnah zahodnih korporacij ali državnih strukturah, ki svoje sposobnosti preizkušajo v sivih območjih prava. Hekerji ne potrebujejo več tankov, da bi zrušili električno omrežje, in ne potrebujejo vojske, da bi zajezili politično voljo nasprotnika. Vse, kar potrebujejo, sta dostop in motiv.

A to ni le zgodba o napadih, je tudi zgodba o tem, kako se države, mesta in posamezniki odzivajo. Kako vlade razpravljajo, ali je, denimo, prav plačevati izsiljevalske odkupnine. Kako vojske preizkušajo pametne algoritme za odločanje v bojnih razmerah. Kako varnost postaja vedno bolj odvisna od etike in odgovornosti programerjev, politikov in voditeljev.

Pred nami je svet, v katerem tradicionalna pojmovanja varnosti odpovedujejo.

Pred nami je svet, v katerem tradicionalna pojmovanja varnosti odpovedujejo in kjer se moramo vprašati, kaj pomeni mir, če je vsaka digitalna naprava lahko potencialno orožje. In kje je meja med obrambo in napadom, če se oba odvijata v prostoru, ki ga ne moremo videti, slišati ali fizično zavarovati.

Naslednje strani odpirajo prostor za razmislek o teh temeljnih vprašanjih. Ne zato, da bi ponudile preproste odgovore, temveč, da bi omogočile globlje razumevanje tega novega, kompleksnega sveta – kjer so sence, tišina in hitrost postale novo orožje sodobnega časa. ◀

Kdo so **Shadow Brokers?**

Leta 2013 je skrivnostna skupina hekerjev, ki se je poimenovala Shadow Brokers, ukradla nekaj disket Nacionalne varnostne agencije NSA, polnih tajnih podatkov. Te skrivnosti je nato objavljala na internetu in tako javno osramotila agencijo ter okrnila njene zmožnosti zbiranja podatkov, hkrati pa je sodobno kibernetično orožje položila v roke vseh, ki so si ga le zaželeli.

Bruce Schneier, *The Atlantic Online*

Skupina je razkrinkala velike ranljivosti v Ciscovih usmerjevalnikih, Microsoftovih Oknih in na Linuxovih poštnih strežnikih. Ponudnikom in njihovim strankam je povzročila hude težave, za nameček pa razvijalcem izsiljevalske programske opreme WannaCry omogočila, da so okužili na stotisoče računalnikov po vsem svetu.

Po izbruhu WannaCry je skupina Shadow Brokers zagrozila, da bo vsak mesec izdala nove skrivnosti NSA in tako kibernetičnim nepridipravom ter drugim državam ponudila dodatna orodja za vdiranje in nove možnosti izkoriščanja.

Kdo so pripadniki skupine? Kako so kradli podatke? Kratek odgovor se glasi, da ne vemo, lahko pa ugibamo na podlagi materiala, ki so ga objavili.

Shadow Brokers so se na lepem pojavili avgusta 2016, ko so objavili kup orodij za vdiranje v računalnike in obelodanili ranljivosti v razširjeni programski opremi. Material je nastal jeseni 2013 in očitno ga je zbiral zunanji testni strežnik NSA, naprava, ki je bila v lasti, finančnem najemu ali kakorkoli drugače pod nadzorom ZDA, vendar nima nikakršne povezave z agencijo. Hekerji NSA iščejo temačne kotičke interneta, kamor skrijejo orodja, ki jih potrebujejo med svojim delom, in očitno so Shadow Brokersi uspešno okupirali enega teh skrivališč.

Skupina je skupaj objavila več sklopov materiala NSA: sklop z ranljivostmi in orodja za vdiranje, naprave, ki podatke usmerjajo skozi računalniške mreže, podobno zbirko za napade na poštne strežnike, zbirko za mešanje štren Microsoftovim Oknom in delovni imenik nekega analitika NSA, ki je vdrl v bančno mrežo Swift. Časovni žigi na dokumentih in drugem materialu so pokazali, da vse izvira iz okoli leta 2013. Orodja za napad na Okna so morda leto ali malo več starejša, odvisno, katero različico tega sistema podpirajo.

Objavljeni material se tako razlikuje, da skoraj zagotovo izvira od več virov v NSA. Dokumenti, povezani z bančnim sistemom Swift, očitno izvirajo iz internega računalnika NSA, ki je povezan z internetom. Microsoftovi dokumenti so prav tako drugačni in nimajo enakih identifikatorjev kot dokumenti z usmerjevalnika in s poštnega strežnika. Shadow Brokers so objavili neurejen in nepregledan material, ki ga niso predhodno skrbno prečesali novinarji tako kot pri Snowdnu, ali preverili tako kot Wikileaks, ko je objavljal Ciine tajne dokumente. Skupina je objavila tudi nekaj anonimnih sporočil v polomljeni angleščini, sklepati je mogoče na ameriško kulturno okolje.

Glede na vse to skoraj ne more biti govora o žvižgaču, saj ta najbrž ne bi čakal tri leta, preden bi objavil svoj material. Najbrž bi se odločil podobno kot Edward Snowden ali Chelsea Manning, ki sta nekaj časa zbirala podatke in nato takoj objavila dokumente, v katerih je opisano, kaj komu počnejo ZDA. V primeru Shadow Brokers pa gre za kup izkoriščevalskega programja brez politične ali etične zveze, ki bi jo žvižgač želel poudariti. Bančni podatki se nanašajo na operacijo NSA, drugi objavljeni dokumenti pa nakazujejo, da je NSA ranljiva za napade, namesto da bi jih pomagala preprečiti in skrbela za večjo varnost.

Poleg tega se ne zdi verjetno niti, da so to navadni hekerji,

Kdo so pripadniki skupine? Kako so kradli podatke? Kratek odgovor se glasi, da ne vemo, lahko pa ugibamo na podlagi materiala, ki so ga objavili.

ki so po naključju naleteli na ta orodja in so želeli predvsem škoditi NSA in ZDA. Vnovič je treba poudariti, da se triletno čakanje ne zdi logično. Dokumenti in orodja so kibernetični kriptonit – kdor jih skrivaj kopiči, se mora bati polovice obveščevalnih agencij z vsega sveta. Tudi dinamika objav ne kaže na kibernetične kriminalce, saj bi ti orodja za vdiranje v informacijske sisteme uporabili sami in varnostne luknje vključili v črve ter viruse, da bi ukradeni material lahko čim bolje unovčili.

Tako pridemo do države. Kdor je informacije pridobil in jih začel objavljati šele čez nekaj let, je zmožen vdreti v NSA in pripravljen objavljati. Države, kot sta Izrael in Francija, so tega zmožne, a najdenega materiala ne bi nikoli objavile, saj si ne bi želele nakopati ameriškega besa. Severna Koreja in Iran, na primer, verjetno ne bi mogla vdreti v tuj sistem. (Severno Korejo so sumili, da stoji za Wannacry, ki je nastal, ko so Shadow Brokers javno objavili to ranljivost.) Na seznamu najočitnejših kandidatk, ki izpolnjujejo oba pogoja, sta tako le še Rusija in Kitajska – ki se je pred nekaj leti trudila prikupiti ZDA.

Ko so avgusta 2016 objavili prve dokumente, in preden je takšno govorjenje veljalo za politično sporno, je prevladalo prepričanje, da za objavami stojijo Rusi in da je to opozorilo takratnemu predsedniku Baracku Obamu, naj se ne maščuje zaradi vdora v sistem demokratskega nacionalnega odbora. Tudi Edward Snowden je sumil Rusijo, vendar je težko najti razlog, da bi to storila. Objavljena orodja bi bila veliko vrednejša, če bi jih varovali kot skrivnost. Rusija bi jih lahko izkoristila za odkrivanje vdorov NSA v svoji državi in za napade na druge države. Z objavo orodij so Shadow Brokers nakazali, da jim je vseeno, ali ZDA vedo za krajo.

Seveda obstaja možnost, da so napadalci vedeli, da so ZDA vedele, da so napadalci vedeli – in tako naprej. A brezbrižnost ob objavi nakazuje na napadalce oziroma napadalca, ki ne razmišlja strateško, na hekerja oziroma hekersko skupino, to pa potem izključuje teorijo o hekerski državi.

Vse to so ugibanja na podlagi razprav z ljudmi, ki nimajo dostopa do zaupnih forenzičnih in obveščevalnih analiz. V sami NSA imajo veliko več podatkov. Številni objavljeni dokumenti vključujejo operativne pripombe in podatke, na podlagi katerih je mogoča prepoznava, zato strokovnjaki NSA točno vedo, kateri strežniki so bili ogroženi, in tako lahko tudi sklepajo, do katerih podatkov so dostopali napadalci. Tako kot pri dokumentih, ki jih je javnosti predal Snowden, vedo le, kaj bi napadalci lahko presneli, ne pa tudi, kaj dejansko so. Microsoft so o ranljivosti Oken obvestili več mesecev prej, preden so jo javno razgalili Shadow Brokers. So lahko prisluškovali, kot so zatrjevali, ko so Rusi napadli zunanje ministrstvo? To je nemogoče ugotoviti.

Je nekdo v NSA napačen strežnik po naključju priključil na zunanje omrežje? To bi bilo mogoče, a se za takšno organizacijo ne zdi verjetno, da bi zagrešila začetniško napako. Je nekdo ugrabil sistem NSA, so v agenciji krti?

Kako je torej Shadow Brokers uspelo? Je nekdo v NSA napačen strežnik po naključju priključil na zunanje omrežje? To bi bilo mogoče, a se za takšno organizacijo ne zdi verjetno, da bi zagrešila začetniško napako. Je nekdo ugrabil sistem NSA, so v agenciji krti?

Če bi takrat v njej res imeli krta, so ga po vsej verjetnosti aretirali, še preden so Shadow Brokers karkoli objavili. Ni države, ki bi razgalila krta, ko dela zanjo, tako, da bi javnost obvestila o njegovem početju, dokler bi bil še ogrožen. Obveščevalne agencije vedo, če tako brutalno ogrozijo vir, zlepa ne bodo več našle koga, ki bi bil pripravljen to delati.

Vse to nakazuje na dve možnosti, in sicer, da je material zbiral Hal Martin, pogodbeni sodelavec NSA, ki so ga avgusta 2016 aretirali, ker je pri sebi doma dve leti kopičil skrivnosti agencije. Ni pa on odgovoren za objavo, saj so Shadow Brokers nadaljevali delo, tudi ko je bil že v zaporu. Kljub temu je objavljeni material morda izviral iz njegove zaloge, na primer, ker bi ga predal skupini ali pa, ker je nekdo vdrl v njegov računalnik. Datumi se ujemajo, zato je to teoretično mogoče. Martina niso obdolžili prodaje skrivnosti tuji sili, vendar je to podatek, ki ga v obtožnici tako in tako ne bi navedli in ni nujen za obsodbo.

Če je bil vir dokumentov res posameznik, potem lahko ugibamo, da je heker po naključju naletel na material in da ni kriva tuja država, zmožna kibernetičnega napada.

Druga možnost je skrivnosti sodelavec NSA, mogoče oseba, ki je ukradla dokumente in jih posredovala tretji osebi. To so omenjali v zgodbi o Martinu v *Washington Postu*:

»Drugi vdor, o katerem doslej niso poročali, so odkrili poleti 2015, zanj pa je prav tako kriv uslužbenec, in sicer uslužbenec enote za zbiranje podatkov o kibernetičnem vojskovanju TAO, kot je povedal uradni predstavnik agencije. Tudi to osebo so aretirali, le da tega niso javno objavili. Uradni predstavnik je dodal, da po podatkih agencije oseba materiala ni predala drugi državi.«

Seveda po podatkih agencije ne pomeni isto, kot da oseba tega ni storila.

Zanimivo je, da zaradi opisanih vdorov niso nikogar aretirali oziroma tega vsaj niso objavili. Če NSA ve, od kod so bili dokumenti, ve tudi, kdo je lahko dostopal do njih. Zaslišala je vse vpletene in bi morala vedeti, ali nekdo namenoma ali nehote ni dovolj skrbno ravnal z njimi. Številni ljudje, tudi uradni predstavniki vlade, so menili, da je vpleten nekdo od znotraj. Zadeva je nemara bolj zapletena, kot se zdi na prvi pogled.

Opisanemu napadu je sledilo ustrahovalno sporočilo, ki je napovedovalo storitev z imenom Podatkovna sprostitev meseca (*Data Dump of the Month*). Proti plačilu so ponujali prodajo neobjavljenih orodij NSA za vdiranje v tuje sisteme in hkrati zagrozili, da jih bodo objavili javno, če nihče ne bo plačal. Skupina se je bahala še z drugimi načrtovanimi napadi, na primer, da bo mogoče objavila nove šibke točke v spletnih brskalnikih, mrežni opremi, pametnih telefonih in operacijskih sistemih, zlasti v Windowsih. Še hujša je bila grožnja, da bo objavila nerevidirane prestrežene podatke NSA, podatke iz bančne mreže Swift in bank ter kompromitirane podatke o jedrskih programih ter izstrelkih Rusije, Kitajske, Irana in Severne Koreje.

Nihče ne ve, kdo so bili Shadow Brokers, kako so ukradli tajne podatke NSA in zakaj so jih objavili. Poletje 2016 je bilo nočna mora ne le za Fort Meade, temveč tudi za marsikoga drugega. ◀

Bi morali zakonsko **prepovedati odkupnine?**

Severna Karolina je prva ameriška zvezna država, ki je prepovedala plačila zaradi izsiljevalske programske opreme in sprejela celo prepoved pogajanj s kibernetičnimi zločinci. To je bila prelomna odločitev, ki jo je leta 2022 posnemala še Florida, vendar je tamkajšnja zakonodaja manj stroga in vključuje manj kaznivih dejanj, blažje so tudi kazni.

Nikki Davidson, *TNS*

To sta tudi edini prepovedi na ameriški državni ravni, ki pa sta kljub temu sprožili razprave na zvezni ravni o tem, kako bi se najučinkoviteje zoperstavili tej razširjeni kibernetični grožnji. Strokovnjaki še danes niso prišli do enotnega sklepa, ali je to sploh ustrezen pristop.

Srž težave tiči v moralni in fiskalni dilemi: bi se države morale odločiti, da ne bodo financirale zločinskih podjetij, čeprav bi s tem morda povzročile motnje v preskrbi z osnovnimi storitvami, ki jih nudijo bolnišnice, šole in ustanove za zagotavljanje javne varnosti? Kaj, če bi visoka moralna drža, zaradi katere ne bi plačevale izsiljevalcem, davkoplačevalce dolgoročno stala več zaradi prekinitev storitev, stroškov odpravljanja škode in možnosti nadaljnjih napadov?

Varuhi reda in miru, na primer FBI, odločno nasprotujejo plačevanju izsiljevalcem, saj se bojijo, da bi tako le še spodbudili kibernetične kriminalce. Kljub temu pa se marsikateri organizaciji zdi, da nima druge izbire, kot da plača.

Meredith Ward, namestnica direktorja Nacionalne zveze državnih vodij informacijskih služb (NASCIO), se zaveda zapletenosti težave: »Ne moremo govoriti o nasprotujočih si stališčih, temveč o različnih.« Poudarila je, da njena nacionalna organizacija nima uradnega stališča, ali bi morale agencije prepovedati plačila, saj se zaveda različnih potreb in razmer v posameznih zveznih državah. Prepričana pa je, da bi morale te same presoditi, ali je prepoved plačil ustrezen pristop.

Je odgovor prepoved na zvezni ravni? Dokončne odločitve še ni.

Dilema podatkov: nejasen vpliv obstoječih prepovedi

Ob tehtanju razlogov za prepoved plačevanja izsiljevalcem in proti njej se izlušči ključno vprašanje, ali bi takšna prepoved tudi delovala.

Vodja informacijske službe Severne Karoline James Weaver je povedal, da je ocena uspešnosti na podlagi trenutno razpoložljivih podatkov zahtevna. Država od lokalnih oblasti zahteva poročanje o vseh večjih kibernetičnih incidentih, vendar je učinek prepovedi težko ločiti od drugih dejavnikov, ki vplivajo na število napadov.

»Trudimo se, da se o tej možnosti ne bi niti razpravljalo,« je poudaril Weaber, »saj se morajo agencije zdaj po navodilih nemudoma posvetiti okrevanju, ne pa pogajanjem s kibernetičnimi nepridipravi.«

Kot kažejo podatki državnega tožilstva Severne Karoline, je število izsiljevanj s programsko opremo po letih vztrajnega naraščanja leta 2023 v primerjavi z letom prej nekoliko upadlo. Še vedno pa napade štejejo v stotinah: v Severni Karolini je bilo leta 2023 843 kaznivih dejanj, povezanih z izsiljevalsko programsko opremo tako v javnem kot zasebnem sektorju.

Weaver pravi, da prepoved plačevanja izsiljevalcem ni zdesetkala takšnih napadov in da bo treba določiti izhodiščno vrednost za merjenje dejanskega učinka nove zakonodaje. »Ne morem odločno zatrditi, da je napadov manj.«

Kljub temu upa, da se bo tok opazno spremenil.

»Upajmo, da se bo dolgoročno pokazal učinek, ko bo presahnil vir sredstev, na katerega računajo ti malopridneži,« je še dodal. Zaveda se, da so nekateri dejavniki motivirani iz drugih razlogov, ne finančnih, recimo iz želje po ustvarjanju nereda in po zbujanju pozornosti v vse večji množici hekerjev.

Zdi se mu, da bi zakonodaja učinkovala bolje, če bi veljala za vse.

»Če bi jo sprejeli vsi, se koristoljubni napadi z izsiljevanjem ne bi več ponavljali,« je prepričan

»Prepoved se zdi smiselna, dokler izsiljevanja ne doživiš na lastni koži,« je opozoril Mark Weatherford, višji strokovni delavec v Središču za digitalno vlado. »Težko je biti načelen, ko ti nekdo drži pištolo na čelu.«

Weaver. »Vsak mora prispevati svoj delež. Če bi sodelovale celotne ZDA, bi bilo to enkratno.«

Na kocki je veliko

Posledice izsiljevanja niso le finančne in operativne, temveč so lahko uničevalne za prebivalstvo.

Napadi so namreč že ohromili klic v sili na številko 911, zato se je podaljšal odzivni čas. Zaradi njih se je prekinila dobava elektrike, od katere smo danes ljudje življenjsko odvisni. Napadi imajo tudi učinek domin in katastrofalne posledice predvsem za najranljivejše skupine prebivalstva.

»Prepoved se zdi smiselna, dokler izsiljevanja ne doživiš na lastni koži,« pa je opozoril Mark Weatherford, višji strokovni delavec v Središču za digitalno vlado. »Težko je biti načelen, ko ti nekdo drži pištolo na čelu.«

Weatherford trdi, da bi bila vsesplošna prepoved nemara učinkovita pred leti, vendar so se razmere zdaj preveč zaostrile in se kriminalci dobro zavedajo, kaj vse je na kocki. Učinkovitejša rešitev bi bila, da bi se svet, vključno z državami, kot sta Kitajska in Rusija, proti kriminalu bojeval tako, da bi zločince poklical na odgovornost.

»Kot globalna skupnosti bi morali odločno reči, da jih bomo poiskali in da se ne morejo skriti,« je poudaril. »Ta kazniva dejanja bi morali obravnavati kot najhujše zločine, pa ne le zato, ker ljudje umirajo, temveč tudi zaradi drugih resnih posledic za organizacije.«

Tako ali drugače je treba plačati ceno

Danes podatki niso le enke in ničle, temveč kri sodobnega vodenja države.

Finančne izgube zaradi izsiljevalskih programov danes in v prihodnih letih bodo astronomske, če ne bo mogoče obnoviti podatkov.

»Lahko sicer rečemo, da nismo plačali, v resnici pa je ceno plačala javnost,« je pojasnil Alan Shark, direktor Public Technology Institute. »Če lokalne oblasti ne morejo opravljati storitev za svoje občane, to ni mačji kašelj, zato lahko razumete pomisleke.«

Napadene organizacije morajo poleg cene vnovične postavitve poškodovanih sistemov včasih poravnati tudi škodo, ker jim ni uspelo zaščititi podatkov.

»Te obveznosti sicer ne boste našli v zakonu, se pa razume, in to je, da država mora ukrepati,« je še dodal Shark. »To morda pomeni, da bo morala za leto ali dve financirati nadzor in opazovanje, a če upoštevate škodo, povzročeno tisočim, če ne milijonom državljanov, bi to ponekod stalo zelo veliko.«

A zvišuje se tudi cena, ki jo zahtevajo kriminalci. V prvem napadu z izsiljevalsko opremo leta 1989 – z disketo – je nepridiprav zahteval nekaj sto dolarjev za dešifriranje dokumentov. Dandanašnji podatki pa so dragoceni kot plemenite kovine, zato tu pa tam izsiljevalci zahtevajo tudi milijone dolarjev.

Razmere so še bolj zapletene, ker ni jamstva, da bodo po plačani odkupnini šifrirani podatki spet sproščeni. Vzpon izsiljevalske opreme kot storitve je demokratiziral kibernetične zločine in celo zelenim hekerjem omogoča izvesti zahtevne napade.

Shark je izpostavil, da so dobro organizirane združbe za izsiljevanje spoštovale svoja pravila igre, a je to zaupanje načeto zaradi priliva novih igralcev, ki delujejo drugače.

Poročilo obveščevalne enote podjetja za kibernetsko varnost Sohpos navaja, da so potencialni hekerji na spletnih forumih oglaševali okoli 15 različic izsiljevalske programske opreme s ceno od skromnih 50 do tisoč dolarjev za mesečno naročnino.

V preteklosti niso zabeležili primerov, da se izsiljevalci ne bi držali dogovora, ambiciozni novinci na črnem trgu naročnin pa v nasprotju s starimi mački ne spoštujejo vedno pravil igre.

»Vsakdo se lahko čez noč sprevrže v kriminalca,« je komentiral Shark. »Zdaj ljudje postajajo malomarni in se računalniški kod včasih nepreklicno izbriše. V nekaj primerih je žrtev plačala, pa izsiljevalci kljub temu niso sprostili dokumentov.«

Zaradi te negotovosti je odločitev za plačilo odkupnine postala še zahtevnejša, sploh za javne agencije vseh velikosti. Shark sklepa, da bi enotna prepoved plačevanja morda preveč poenostavljen pristop, saj je področje izsiljevalske programske opreme izjemno kompleksno.

»Zakon o prepovedi plačevanja izsiljevalcem je vsekakor dobronameren, a ima preveč lukenj, da bi ga resno jemali,« meni Shark.

Kibernetično zavarovanje: dejavnik, ki dodatno zapleta razmere

Agencije ne marajo razglašati kibernetičnega zavarovanja, saj se bojijo, da bi s tem še dodatno privabljale kibernetične zločince. In to je še en dejavnik v razpravi o prepovedi plačevanja odkupnin.

Kibernetično zavarovanje je vse težje skleniti, saj številni ponudniki zahtevajo obsežne varnostne ukrepe. Poleg tega zavarovalna pogodba pogosto predpisuje takojšnje obveščanje v primeru napada, kar bi lahko vplivalo na odziv agencij v primeru izsiljevanja.

Weaver je potrdil, da je prepoved plačevanja odkupnin vplivala na odnose z zavarovalnimi družbami.

»Včasih si želijo možnosti, da bi se pogajale, pa jih moramo opomniti, da v Severni Karolini ta možnost ne obstaja, in jim svetujemo, naj se raje osredotočijo na reševanje težave,« je pojasnil.

Kibernetično zavarovanje velja za kontroverzno, vendar lahko pripomore k zmanjšanju finančnega vpliva napadov z izsiljevanjem. Weatherford je izpostavil, da so se zavarovalnice nekajkrat že uspešno pogodile za zmanjšanje zneska odkupnine.

»Včasih se nepridipravi raje pogajajo z zavarovalnico, ker to vidijo kot odnos med poslovnimi strankami,« je dodal Weatherford.

Cena, ki jo zahtevajo kriminalci, se zvišuje. V prvem napadu z izsiljevalsko opremo leta 1989 – z disketo – je nepridiprav za dešifriranje dokumentov zahteval nekaj sto dolarjev. Danes izsiljevalci zahtevajo tudi milijone dolarjev.

Shark pa ima pomisleke o etiki zavarovalnic, ki plačajo odkupnino v imenu javnih agencij.

»Eno je, če lokalne oblasti izpraznijo svojo blagajno,« je rekel in namignil, da zasebna zavarovalnina briše meje med javno in zasebno odgovornostjo. »Če denar pride od zavarovalnice, to ni več javni denar – primerljivo je z avtomobilskim zavarovanjem.«

Če bi zavarovalnice vedele, da plačilo odkupnine ne pride v poštev, bi to verjetno ohladilo trg s kibernetičnimi zavarovanji, meni Shark.

Razprava še traja in Wardova iz zveze NASCIO upa, da bo letos, po lanskem volilnem letu v ZDA, še katera od zveznih držav sprejela zakone o prepovedi izplačila odkupnin, čeprav se zaveda, da se zaradi nepredvidljivost kibernetičnih groženj lahko razplete tudi drugače.

»Le en odmeven incident se mora zgoditi,« je komentirala Wardova. »Nemogoče je napovedati, kaj podžge zvezno državo, da uvede novost in vztraja pri njenem uresničevanju.«

Nadgrajuje se tudi sama tema o prepovedi plačevanja odkupnin zaradi izsiljevalske programske opreme, saj ne gre za preprosto izbiro, kaj je prav in kaj napačno, temveč iskanje ravnovesja med pomembnimi dejavniki in najmanj boleče poteze v igri z visokimi stavami. ◀

Vojna in mir v času umetne inteligence

Umetna inteligenca (UI) bo postala ključni dejavnik svetovne ureditve od prilagoditve vojaških strategij do prenove diplomacije. Imuna je na strah ter usluge in predstavlja novo možnost za objektivnost pri strateških odločitvah. A ta objektivnost, ki jo izkoriščata tako vojak kot mirovnik, bi morala ohranjati človeško subjektivnost, ki je ključna za odgovorno izkoriščanje moči. UI bo v vojni osvetlila najboljše in najhujše plati človeštva, služila bo kot sredstvo tako za začetek kot konec vojne.

Henry A. Kissinger, Eric Schmidt, Craig Mundie

Dolga bitka človeštva, da bi se uspešno umestilo v vse bolj zapletenih razmerah in ne bi nobena država absolutno nadvladala nad drugo, je dosegla status neprestanega, neprekinjenega naravnega zakona. Na svetu, na katerem so glavni igralci še vedno ljudje – četudi opremljeni z UI za informiranje, posvetovanje in iskanje nasvetov –, bi države še vedno morale uživati neko mero stabilnosti na podlagi skupnih pravil vedenja, ki bi jih sproti prilagajale.

Če pa se bo UI uveljavila kot tako rekoč neodvisna politična, diplomatska in vojaška entiteta, bi novo, nenadzorovano neravnovesje izrinilo dolgoletno ravnovesje moči. Mednarodna skupnost držav – občutljivo in nihajoče sožitje, ki so ga dosegle v zadnjih stoletjih – se je delno obdržala zaradi inherentne enakosti udeleženk. Izrazito asimetričen svet – v katerem bi nekatere države najzmogljivejšo UI sprejele hitreje kot druge – bi bil manj predvidljiv. Ko bi se nekateri ljudje morali vojaško ali diplomatsko soočiti z državo, močno podprto z UI ali celo s samo UI, bi morda težko že preživeli, kaj šele, da bi se enakovredno merili z njo. Takšna ureditev bi lahko pripomogla k imploziji družbe in nenadzorovani eksploziji zunanjih sporov.

Obstaja še veliko drugih možnosti. Ljudje se že dolgo spopadajo in bojujejo ne le za varnost, temveč tudi za zmago ali čast. Naprave za zdaj ne poznajo teh konceptov. Mogoče nikdar ne bodo šle v vojno in bi se raje odločile za takojšen, skrbno pripravljen prenos ozemlja na podlagi zahtevnih preračunov. Ali pa bi dale prednost rezultatu namesto življenju posameznikov in bi se odločile za korake, ki bi se stopnjevali v krvave vojne, dokler se človeštvo ne bi izčrpalo. Po enem od scenarijev bi se naša vrsta lahko močno spremenila, da bi se popolnoma izognila brutalnosti človekovega vedenja, po drugem pa bi nas tehnologija tako zasužnjila, da bi nas to vrnilo v barbarsko preteklost.

Varnostne dileme umetne inteligence

Številne države se posvečajo predvsem zmagi v tekmi za UI, kar je delno mogoče razumeti. Kultura, zgodovina, komunikacija in stališča so med današnjimi velesilami pripomogli k diplomatskim razmeram, ki pri vseh podpihujejo negotovost in sumničavost. Voditelji so prepričani, da bi manjša taktična prednost v morebitnem konfliktu odločala o zmagi in da bi to ključno prednost lahko nudila ravno UI.

Če bi si vsaka država hotela izboriti čim boljši položaj, bi nastale razmere za psihološko tekmo med vojaškimi silami in obveščevalnimi agencijami, kakršnih

človeštvo še ni doživelo. Pojavila bi se dilema eksistenčne varnosti. Zdi se logično, da bi človeški akter, ki bi se prikopal do superinteligentne UI – hipotetične UI, inteligentnejše od človeške –, najbrž želel zagotoviti, da nihče drug ne bi imel zmogljivejše različice tehnologije. Takšen akter bi samoumevno verjetno tudi predvideval, da njegov tekmec, ki ga pestijo enake negotovosti in skrbi, razmišlja o enaki potezi.

Superinteligentna UI bi razen vojne lahko preprečila, spodkopala in preprečila konkurenčne načrte. UI obeta, da bo nepredstavljivo okrepila delovanje konvencionalnih računalniških virusov in jih hkrati temeljito zakamuflirala. Tako kot računalniški črv Stuxnet – kibernetično orožje, ki so ga odkrili 2010 in naj bi uničil petino iranskih centrifug za uran – bi tudi sistem UI lahko sabotiral napredek tekmecev in prikril svojo prisotnost, sovražnikove znanstvenike pa s tem prisilil, da bi lovili sence. Ker zna UI izvrstno manipulirati s šibkimi točkami človeške psihologije, bi lahko ugrabila tudi sovražnikove medije in objavljala plaz umetno ustvarjenih lažnih informacij ter podpihovala množično nasprotovanje nadaljnjemu napredku zmogljivosti UI v tej državi.

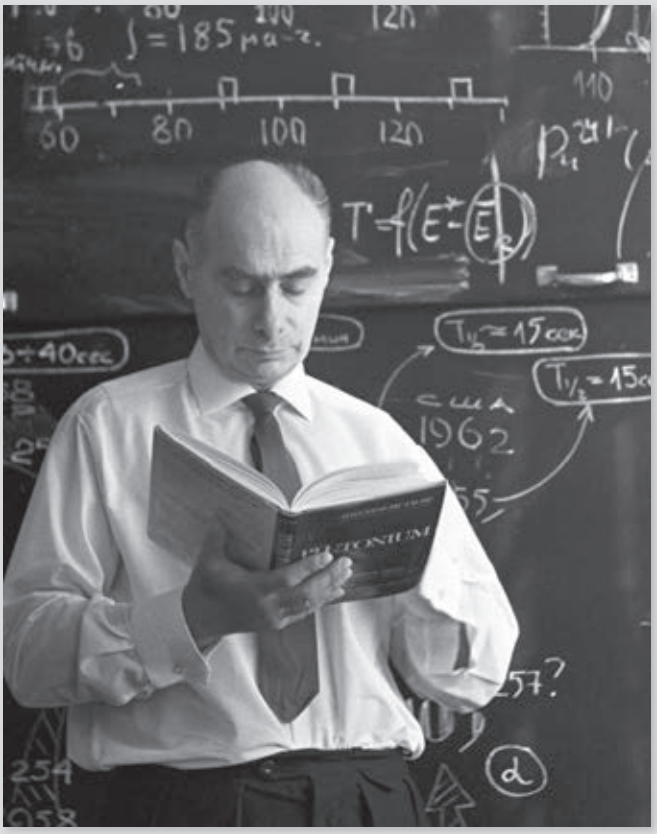
Države bodo težko dobile jasno podobo o svojem položaju v primerjavi z drugimi udeležencami v tekmi za UI. Največje modele UI že danes učijo v varnih omrežjih, odklopljenih od preostalega interneta. Nekateri direktorji so prepričani, da bodo prej ali slej tudi sam razvoj UI preselili v neprebojne bunkerje in superračunalnik bodo poganjali jedrski reaktorji. Podatkovna središča zdaj gradijo na dnu oceanov. Kmalu bodo lahko krožila v orbitah okrog Zemlje. Tako podjetja kot države se bodo večkrat odločili za molk in ne bodo več objavljali izsledkov raziskav UI, in to ne le zaradi škodljivih udeležencev, temveč tudi zato, da bi prikrili svojo stopnjo razvoja. Dosežke bi lahko izkrivljali tudi tako, da bi načrtno objavljali zavajajoče raziskave, pri ustvarjanju prepričljivih lažnih zgodb pa bi jim pomagala kar UI.

Takšne znanstvene skrivalnice že poznamo. Leta 1942 je sovjetski fizik Georgij Fljorov pravilno sklepal, da Združene države Amerike sestavljajo jedrsko bombo, saj je opazil, da so Američani in Britanci na lepem nehali objavljati znanstvene razprave o jedrski cepitvi. Danes bi bil takšen podvig še manj predvidljiv zaradi zapletenega in dvoumnega merjenja napredka na poti do nečesa tako abstraktnega, kot je inteligenca. Čeprav si marsikdo domišlja, da ima sorazmerno prednost zaradi velikosti modela, to ni v vseh okoliščinah tudi nujno boljše in večji model ne premaga vedno manjših. Bolj specializirane naprave na temelju UI lahko delujejo kot jata dronov v primerjavi z velikim letalom – ne morejo ga uničiti, lahko pa ga onemogočijo.

Akterju bi nemara pripisovali prednost, če bi moral prikazati dosežek na točno določen področju. Težava pri takšnem načinu razmišljanja pa je, da UI pomeni strojno učenje, ki ni vključeno le v eno tehnologijo, temveč tudi v širok nabor različnih tehnologij, in zmogljivost na enem področju včasih omogočajo povsem drugačni dejavniki kot na drugem. V tem primeru bi lahko bila prednost, ocenjena s klasičnimi postopki, le namišljena.

In kot je pokazala eksponentna, nenapovedana eksplozija zmogljivosti UI v zadnjih letih, pot napredka ni niti linearna niti predvidljiva. Tudi če bi lahko rekli, da eden od akterjev druge prehiteva za neko število let ali mesecev, lahko nenaden tehnološki ali teoretični preboj na ključnem področju v ključnem trenutku premeša karte vseh igralcev.

V takšnem svetu, v katerem voditelji ne morejo zaupati niti najzanesljivejšim podatkom, svojemu notranjemu glasu in celo ne temeljem resničnosti, državam ne moremo očitati, da ravnajo paranoično in sumničavo. Voditelji se nedvomno že danes odločajo na podlagi predpostavke, da njihovo početje nekdo opazuje ali da nanj vplivajo izkrivljanja zaradi zlonamernega vplivanja. Če bi vedno imeli v mislih najbolj črn scenarij, bi vsak akter v svojih strateških tehtanjih dal prednost hitrosti in tajnosti pred varnostjo. Voditelje lahko ohromi strah, da drugo mesto ne obstaja. Pod pritiskom bi preuranjeno pospešili uporabo UI za odvračanje neželenih zunanjih vplivov.



Leta 1942 je sovjetski fizik Georgij Fljorov pravilno sklepal, da Združene države Amerike sestavljajo jedrsko bombo, saj je opazil, da so Američani in Britanci na lepem nehali objavljati znanstvene razprave o jedrski cepitvi.

Nova paradigma vojne

Skoraj vso človeško zgodovino so vojne bojevali na razmejenem prostoru, kjer so vsi lahko s precejšnjo zanesljivostjo ocenili zmogljivosti in položaj sovražnih sil. Kombinacija teh dveh atributov je obema stranema vzbujala občutek psihološke varnosti in dogovora, kar je omogočilo obveščeno omejevanje žrtev. Le ko so voditelji imeli enake predstave, kako bi se lahko odvijala vojna, so nasprotne sile lahko pretehtale, ali jo je vredno začeti.

Hitrost in mobilnost sta med najbolj predvidljivimi dejavniki, na podlagi katerih je mogoče oceniti zmogljivost posameznih kosov vojaške opreme. Eden najstarejših primerov je razvoj topa. Teodozijevo obzidje je tisočletje po izgradnji veličastno mesto Konstantinopel varovalo pred zunanjimi napadalci. Nato je leta 1452 madžarski topniški inženir vladarju Konstantinu XI. predlagal gradnjo ogromnega topa, s katerim bi napadalce obstreljevali izza obzidja in jih zmleli. A samozadovoljni vladar, ki ni imel niti sredstev niti uvida, da bi prepoznal pomen tehnologije, je predlog zavrnil. Na njegovo veliko žalost

Umetnointeligenčno vojskovanje bo omejeno predvsem na oceno sovražnikovih namenov ter njihovih strateških ciljev in ne toliko z njegovimi zmogljivostmi.

se je pokazalo, da je madžarski inženir velik koristoljubnež. Zamenjal je taktiko (in stran), nadgradil svoj top, da je bil mobilnejši in ga je lahko vleklo še vedno impresivnih 60 volov in 400 mož, ter ga ponudil Konstantinovemu tekmecu, otomanskemu sultanu Mehmedu II., ki se je pripravljal na zavzetje nepremagljive utrdbe. Podjetni Madžar, ki je sultanov interes pritegnil s trditvijo, da bi njegov top lahko podrl tudi zidove samega Babilona, je tako turškim silam pomagal, da so starodavne zidove osvojili v pičlih 55 dneh.

Temeljne značilnosti drame iz 15. stoletja je mogoče vedno znova razbrati skozi vso zgodovino. V 19. stoletju sta hitrost in mobilnost premešali karte najprej v Franciji, ko je Napoleonova vojska osvajala Evropo, in nato še v Prusiji pod vodstvom Helmuta von Moltkeja (Starejšega) in Albrechta von Roona. Oba sta izkoristila takratno novost, železnice, ki so omogočale hitrejše in prilagodljivejše manevriranje. Podobno so *blitzkrieg*, nadgradnjo istih nemških vojaških načel, ponovili proti zaveznikom med drugo svetovno vojno, kar je imelo pogubne posledice.

Bliskovita vojna je v dobi digitalnega vojskovanja dobila nov pomen – in postala vseprisotna. Vse se zgodi takoj, napadalcem ni treba žrtvovati ljudi, da ohranijo mobilnost, saj zemljepisne danosti ne predstavljajo več omejitev. Čeprav je ta kombinacija v digitalnih udarih večinoma koristila napadalcem, bi v dobi UI lahko doživeli še hitrejši odziv in v kibernetični obrambi poskrbeli za enako moč kot v kibernetičnih napadih.

V kinetičnem vojskovanju bo UI pripomogla k še enemu skoku naprej. Droni, na primer, bodo izjemno hitri in nepredstavljivo okretni. Ko bo UI prešla v splošno uporabo, ne bo usmerjala le enega drona, temveč kar celo floto. Nastajali bodo roji brezpilotnikov in popolnoma usklajeno leteli kot ena sama, enotna skupnost. Bodoče jate dronov bodo brezšivno razpadale in se brez omahovanja postrojile v nove enote različnih velikosti, podobno kot elitne enote za posebne naloge nastajajo iz večjih ali manjših skupin, od katerih je vsaka zmožna delovati tudi samostojno.

UI bo poleg tega omogočila hitro in prilagodljivo obrambo. Flote brezpilotnikov je težko ali celo nemogoče sestreliti s konvencionalnimi projektili. Strelno orožje na temelju UI, ki bi izstreljevalo salve fotonov in elektronov namesto klasičnega streliva, bi lahko doseglo enako pogubne in hromeče zmogljivosti kot sončna nevihta, ki včasih cvre vezje izpostavljenih satelitov.

Orožje z UI bo tudi neverjetno natančno. Omejeno poznavanje nasprotnikovega terena ne bo več kratilo zmogljivosti in načrtov udeležencev v vojni. A naveza med znanostjo in vojno po novem prinaša tudi vse natančnejše instrumente in pričakovati je, da bo UI pripomogla k še več prelomnim novostim. UI bo tako zmanjšala razkorak med namero in izidom, vključno z uporabo smrtonosne sile. Tako kopenske jate brezpilotnikov kot avtomatsko orožje na morju in morda medzvezdne flote bodo zaradi naprav natančne in bodo ljudi pobijale z zanemarljivo stopnjo negotovosti in s strahovitim učinkom. Razsežnosti uničenja bodo odvisne le od volje in zadržkov tako ljudi kot naprav.

Umetnointeligenčno vojskovanje bo omejeno predvsem na oceno sovražnikovih namenov ter njihovih strateških ciljev in ne toliko z njegovimi zmogljivostmi. V jedrski dobi smo v to fazo že vstopili – a njena dinamika in pomen bosta deležna veliko večjega zanimanja, ko bo UI dokazala, da se obnese tudi kot orožje v vojni.

Ob uporabi tako dragocene tehnologije glavna tarča vojne ob pomoči UI mogoče sploh ne bodo ljudje. Z UI bi ljudi kot izvajalce bojev pravzaprav lahko povsem izključili iz vojne, da bi bile manj smrtonosne, a zato nič manj pomembne. Prav tako samo želja po ozemlju najbrž ne bi sprožila agresije ob podpori UI – zanimivejši bi bili namreč podatkovni centri in druga pomembna digitalna infrastruktura.

Predaja se potemtakem ne bo zgodila, ko bodo nasprotnikove vrste zdesetkane in njegovi arzenali prazni, temveč ko silicijev ščit preživelih ne bo več zmožen zavarovati tehnološkega premoženja – in nazadnje tudi njegovih človeških namestnikov. Vojna bi se lahko razvila v igro z izključno mehanskimi žrtvami, odločilni dejavnik pa bi bil psihološka moč človeka (ali UI), ki bi se moral boriti proti tveganju oziroma preprečiti prelomni trenutek pred popolnim uničenjem.

Celo motivi na novem bojnem polju bi bili delno tuji. Angleški pisec Chesterton je nekoč pronicljivo pripomnil, da se pravi vojak ne bori, ker bi sovražil, kar ima pred seboj, temveč zato, ker ljubi, kar je za njim. Vojna ob pomoči UI najbrž ne bo vključevala ljubezni in sovraštva, kaj šele koncept vojaške hrabrosti. Po drugi strani pa bo verjetno še vedno polna ega, istovetnosti in pripadnosti, čeprav našteto verjetno ne bo enako temu, kar poznamo danes.

Vojna računica je razmeroma preprosta: stran, ki ji bo prvi postala nevzdržna bol bojevanja, bo najbrž poražena. Zavedanje o lastnih omejitvah je v preteklosti pripomoglo k omejevanju. Brez tega zavedanja in občutka (ter prenašanja) bolečine se človek mora vprašati, kaj le bo omejevalo UI, ki so jo vključili v vojskovanje, in kaj bo pripomoglo k zaključku konfliktov, ki jih bo podpirala. UI, ki igra šah, bi igrala do zadnjega kmeta, če je ne bi seznanili s pravili, kdaj je partija končana.

Geopolitično prestrukturiranje

V vsakem obdobju se je v človeštvu kot v skladu z nekim naravnim zakonom pojavila entiteta, kot se je nekoč izrazil Kissinger, z močjo, voljo in intelektualnim ter moralnim zagonom, da bi celoten mednarodni sistem prilagodila svojim lastnim vrednotam. Najbolj znana ureditev človeške civilizacije je klasični vestfalski sistem držav. Predstava o suvereni nacionalni državi je stara le nekaj stoletij in se je porodila na podlagi pogodb iz sredine 17. stoletja, ki jih poznamo pod skupnim imenom vestfalski mir. To ni vnaprej določena enota družbene organizacije in morda ni primerna za dobo UI. Ker ta pravzaprav zaradi množičnega dezinformiranja in avtomatizirane diskriminacije sproži izgubo zaupanja v to ureditev, morda predstavlja vrojeni izziv moči vlade nacionalne države. Po drugi strani pa bi UI lahko spremenila razmerja med relativnimi položaji tekmecev znotraj sedanjega sistema.

Če bodo njeno zmogljivosti izrabljale predvsem same nacionalne države, bi človeštvo lahko prisilile v hegemonistični pat položaj ali pa nemara v novo ravnovesje nacionalnih držav, opolnomočenih z UI. Vendar bi tehnologija lahko postala tudi katalizator še temeljnejšega prehoda v popolnoma nov sistem, v katerem bi bile posamezne države prisiljene, da bi opustile svojo osrednjo vlogo v globalni politični infrastrukturi.

Ena od možnosti je, da bi podjetja, ki so lastniki in razvijalci UI, pridobila popolno družbeno, gospodarsko, vojaško in politično moč. Danes so države prisiljene, da se spopadajo s svojim težavnim položajem kot navijačice zasebnih podjetij – svojo vojaško moč, diplomatski kapital in gospodarski vpliv zastavljajo za spodbujanje teh domačih podjetij – in kot podpornice povprečnega državljana, sumničavega do monopolističnega pohlepa in skrivnostnosti. To bo morda nepremagljivo protislovje.

Mogoči razpleti s tem še niso izčrpani. Nenadzorovana, odprtokodna razširjenost bi lahko povzročila pojav manjših tolp ali združb s šibkimi sistemi UI, vendar velikimi zmogljivostmi, ki bi zadostovale za njihov obstoj in omejeno obrambo. V človeških združbah, ki odklanjajo uveljavljeno avtoriteto zaradi decentraliziranih financ, komunikacije in uprave, bi utegnila prevladati takšna protoanarhija na osnovi tehnologije. Takšne skupine bi lahko bile tudi versko obarvane, saj imajo navsezadnje krščanstvo, islam in hinduizem večji ter tudi trajnejši domet od katerekoli države v zgodovini. V prihodnjih obdobjih bi verska opredelitev utegnila zagotavljati otipljivejši okvir za poistovetenje in pripadnost kot državljanstvo.

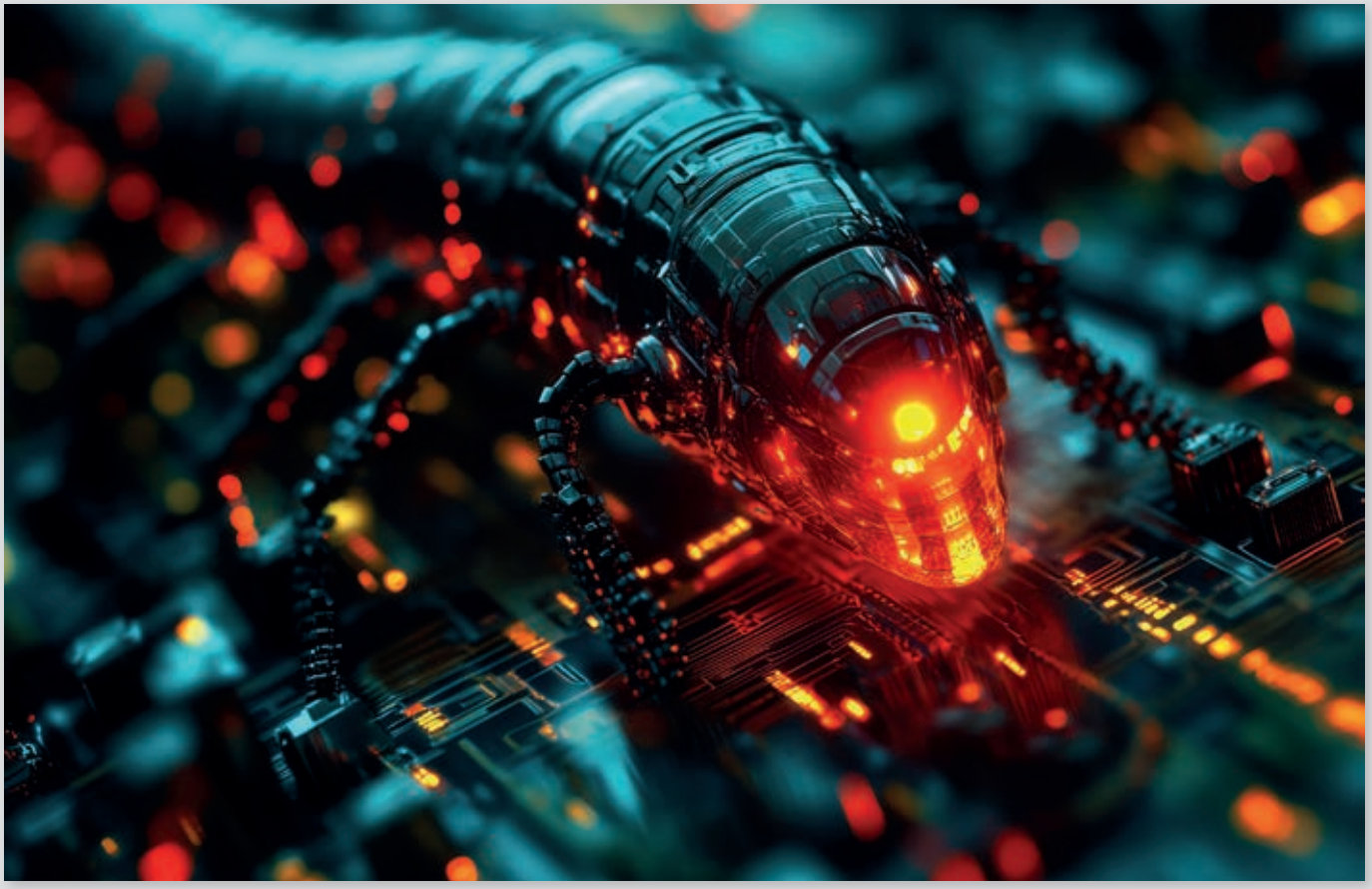
Karkoli že bo prinesla prihodnost, četudi bodo v njej prevladale podjetniške naveze ali razpršene verske skupnosti, novega ozemlja, ki si ga bodo prilastile takšne združbe – in zaradi katerega se bodo tudi spopadale – ne bomo merili v kvadratnih metrih, saj bodo delovale v digitalni pokrajini. Prizadevale si bodo za pripadnost posameznih uporabnikov, vezi med njimi in vodstvom, kakršnekoli že bodo, pa bodo izrinile tradicionalno podobo o državljanstvu. Prav tako dogovori med novimi entitetami ne bodo spominjali na klasična zavezništva.

Z zgodovinskega zornega kota so zavezništva sklepali posamezni voditelji, služili pa so krepitvi moči države v primeru vojne. Nasprotno bo razumevanje državljanstva in zavezništev – pa mogoče tudi zavojevanj in križarskih pohodov – na temelju mnenj, prepričanj, hkrati s subjektivno identiteto navadnih ljudi v obdobju miru, prineslo novo (ali zelo staro) pojmovanje imperija, nujno pa bo tudi vnovično tehtanje obveznosti, ki jih prinaša zvestoba domovini, ter stroškov za možnosti izstopa, saj v nasprotnem primeru v umetnointeligenčni prihodnosti sploh ne bodo mogli obstajati.

Mir in moč

Zunanja politika nacionalnih držav se oblikuje in nato prilagaja z iskanjem ravnovesja med

UI, ki igra šah, bi igrala do zadnjega kmeta, če je ne bi seznanili s pravili, kdaj je partija končana.



idealizmom in realizmom. Začasno ravnovesje, ki ga lovijo naši voditelji, naknadno ne obvelja za končno stanje, temveč ga moramo videti le kot kratkotrajne strategije za njihov čas. Z vsako novo dobo ta napetost prinese različno izražen politični red. Sestavni del te nikoli končane evolucije je razkorak med prizadevanjem za interese in negovanjem vrednot – oziroma med prednostmi neke nacionalne države in globalno blaginjo. Voditelji manjših držav so se zgodovinsko na diplomatskem področju odzivali odločno in prednost dali pogojem za lastno preživetje. Nasprotno pa so se odgovorni v svetovnih imperijih s sredstvi za doseganje dodatnih ciljev morali soočati z globljimi zadregami.

Od začetka civilizacije, ko so se počasi razvijale človeške organizacijske enote, se je hkrati povečevalo tudi sodelovanje. Danes pa postaja vse očitnejši hlad do tega trenda, morda zaradi zahtevnosti izzivov, s katerimi se sooča ves planet, in hkrati zaradi očitne materialne neenakosti med državami in znotraj njih. UI bi lahko bila primeren odgovor na zahteve še večjega obsega človeškega vodenja, zmožnega natančno in verno razbrati ne le obvez države, temveč tudi vzajemno delovanje sveta.

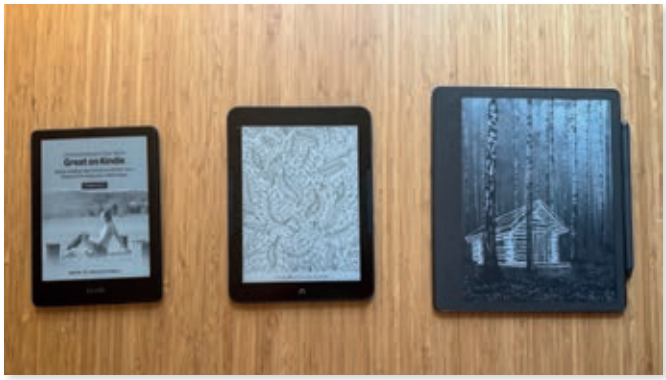
Tako kot računalniški črv Stuxnet – kibernetično orožje, ki so ga odkrili 2010 in naj bi uničil petino iranskih centrifug za uran – bi tudi sistem UI lahko sabotiral napredek tekmecev in prikril svojo prisotnost, sovražnikove znanstvenike pa s tem prisilil, da bi lovili sence.

Upajmo, da bo UI, uporabljena v politične namene tako doma kot v tujini, storila več, kot le osvetlila uravnotežene kompromise. Idealno bi bilo, če bi nudila nove, globalno optimalne rešitve, delovala glede na dolgoročne napovedi in natančneje, kot so to zmožni ljudje. Tako bi tudi uskladila različne človeške interese. V prihodnjem svetu bo strojna inteligenca, ki bo usmerjala konflikte in se pogajala za mir, mogoče pomagala razjasniti ali celo premagati tradicionalne dileme.

No, če bi UI dejansko rešila težave, za katere bi morali upati, da jih zmoremo sami, bi lahko nastala kriza zaupanja tako zaradi pretiranega kot zaradi premalo zaupanja. Ko bomo dojeli omejitve lastnih zmožnosti samopopravkov, nam bo mogoče težko priznati, da smo napravam prepustili preveč vpliva pri reševanju eksistenčnih vprašanj človekovega vedenja. Kar pa se tiče premalo zaupanja, bi spoznanje, da je že odstranitev človeškega dejavnika iz urejanja zadev zadostovala, da smo razrešili najvztrajnejša odprta vprašanja, utegnilo še preveč jasno razgaliti pomanjkljivosti človeških vzorcev. Če mir od nekdaj ni nič drugega kot preprosta prostovoljna odločitev, je cena za človeško nepopolnost plačana z valuto nenehnih vojn. Zavedanje, da rešitev obstaja od nekdaj, a je nismo zagotovili sami, bi strla človeški ponos.

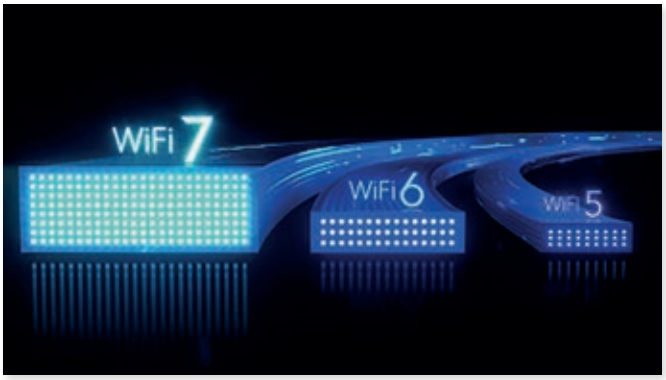
Ko gre za varnost, se v nasprotju z nadomeščanjem ljudi pri znanstvenih in drugih akademskih podvigih morda laže sprijaznimo z nepristranskostjo mehanske tretje strani kot inherentno boljše od človeškega prizadevanja za lastne interese – tako kot ljudje hitro prepoznajo potrebo po mediatorju v zapleteni razvezi zakonske skupnosti. Ravno nekatere naše najslabše lastnosti nam bodo omogočile, da bomo pokazali tudi nekaj najboljših: človeški nagon, zaradi katerega smo nagnjeni k skrbi za lastne interese, četudi na račun drugih, nas bo morda pripravil, da bomo zaradi UI presegli svoj jaz. ◀

24. junija nadaljujemo



Veliki test: E-bralniki

Primerjali bomo najnovejše modele e-bralnikov – kateri ima najboljši zaslon, najbolj zmogljivo baterijo, najboljše uporabniško okolje? In kateri podpirajo slovenske knjižnice!



Wi-Fi 7

Wi-Fi 7 prinaša velike hitrosti, nizke zakasnitve in zmogljivosti, ki bodo spremenile način dela in zabave. Vse, kar morate vedeti o novem standardu, ki bo zaznamoval prihodnja leta.

MonitorPRO

V prilogi Monitor Pro pa o poenotenih komunikacijah in računalništvu v oblaku.

Monitor

ODGOVORNI UREDNIK
Matjaž Klančar

UREDNIK
Uroš Mesojedec

LEKTURA
Simona Mikeln

PREVAJANJE
Petra Piber

LIKOVNA ZASNOVA
Peter Gedei

OBLIKOVANJE NASLOVNICE
Peter Gedei

RAČ. GRAFIKA IN STAVEK
Peter Gedei

FOTOGRAFIJE
Peter Gedei, fotoarhiv Monitorja, iStock, Midjourney

NASLOV UREDNIŠTVA
Monitor, Dunajska 51, 1000 Ljubljana, tel.: (01) 230 65 00
e-pošta: urednistvo@monitor.si

MONITOR V SPLETU
www.monitor.si

Revija Monitor posebej odličnim izdelkom pri svojih preizkusih podeljuje priznanje »zlati Monitor«. To je priznanje za konkretni izdelek na konkretnem testu. Zato lahko uporablja zlati Monitor v propagandne namene vsako podjetje, ki ta izdelek trži, s tem da jasno navede, v kateri številki Monitorja je bil objavljen test in kateri izdelek je prejel priznanje.

IZDAJATELJ
Mladina časopisno podjetje d.d., Dunajska cesta 51, 1000 Ljubljana, dav. št. 83610405

IZVRŠNA DIREKTORICA
Denis Tavčar

PRODAJA OGLASNEGA PROSTORA
tel.: (01) 230 65 36,
e-pošta: marketing@monitor.si

VODJA MARKETINGA IN OGLASNEGA TRŽENJA
Ines Markovčič, tel.: (01) 230 65 33

NAROČNINE IN PRODAJA
tel. (01) 230 65 00,
e-pošta: narocnine@monitor.si

RAČUNOVODSTVO
e-pošta: racunovodstvo@monitor.si

TISK
Shwartz Print, Ljubljana

DISTRIBUCIJA
Izberi d.o.o., Ljubljana

Poštnina za naročnike plačana pri pošti 1102, Ljubljana. V ceno izvodov v maloprodaji je vključen DDV v višini 5%.
ISSN 1318-1017

Izid je finančno podprla Javna agencija za raziskovalno dejavnost Republike Slovenije.

BERITE MONITOR 20% CENEJE

Revijo Monitor lahko naročite tako, da plačate letno naročnino in jo od naslednje številke naprej prejemate na želeni naslov.

- **Fizične osebe imajo 20% popusta na polno ceno.**
- **Naročite se lahko po navadni ali elektronski pošti na** narocnine@monitor.si.
- **Plačilo je mogoče tudi s plačilnimi karticami.**
- **Naročnina se plačuje enkrat letno. Če naročnik ne zahteva odpovedi, se naročnina podaljša za naslednje obdobje.**
- **Odpoved je možna pisno ali po telefonu.**
- **Vse dodatne informacije lahko dobite po telefonu (01) 230 65 30 ali po elektronski pošti narocnine@monitor.si.**