Optimized, te dodaje, da globalna prisutnost, tržišna povezanost i vodeći tehnološki položaj na području usmjerivača velikih snaga, distribuiranih proizvodnih sustava i automatizacije proizvodnje tvrtke ABB, daju tvrtki Hydrogen Optimized pristup tržištima i mogućnosti za postizanje svojih ciljeva. Prema ocjenama, objavljenim u lipanjskom izvještaju društva za DNV, do 2050. godine će globalni kapacitet elektrolizatora doseći vrijednost 3.100 gigawata, pri čemu najavljuju, da će do polovice ovog stoljeća dobivanje zelenog vodika s pomoću električne energije biti prevladavajuća metoda, koja će doseći 72 posto čitave proizvodnje.

Sredstva investicije tvrtke ABB u tvrtku Key DH Technologies, koju vodi ABB Technology Ventures, biti će iskorištena za daljnji razvoj intelektualnog vlasništva tvrtke Hydrogen Optimized, izgradnju korporativnih kapaciteta za povećanje opsega poslovanja i uvođenje automatizirane proizvodnje i robotike, što će ubrzati proizvodnju elektrolizera razreda veličine gigawata.

› ***www.abb.com***
› ***www.keydht.com***
› ***www.hydrogenoptimized.com***

» Na pragu internetskog svjetskog rata

Esad Jakupović

Rat u Ukrajini kao i druge geopolitičke napetosti se prenose i na polje kibernetske sigurnosti. Hakerske grupe, podupirane, a vjerojatno i angažirane od strane upletenih zemalja, dobivaju snažne resurse za svoje kibernetske operacije i napade. Kako države raspolažu s neusporedivo većim tehnološkim resursima, takva suradnja može imati nepopravljive posljedice na području kibernetske sigurnosti u svijetu općenito.

Vojna intervencija Rusije u Ukrajini utjecati će na buduće ratove, a dosadašnji kibernetski napadi između zemalja povezani s ratom služiti će kao priručnik za izvođenje povremenih stvarnih (kinetičkih) i kibernetskih bitki, procjenjuje portal IT pro. Rat u Ukrajini je prijeloman, ne samo zbog njenog opsega, jer su uključene dvije velike zemlje, već i zbog dvostruke fronte. To je naime prvi rat, koji se vodi i kinetički (na tlu, s puškama i topništvom), kao i kibernetski (u kibernetskom prostoru, na internetu). Rusko-ukrajinski rat predstavlja novu prekretnicu u ratovanju, kod kojeg se svakoga dana usklađuju novi kibernetski napadi i uključuju se nove potporne grupe na obje strane.

» *Rat na dvije fronte: rusko-ukrajinski rat je prvi, koji se vodi i kinetički i kibernetski.*

» *Nova prekretnica u ratovanju: u rusko-ukrajinskom ratu se svakog dana usklađuju novi kibernetski napadi te se uključuju nove grupe za podršku na obje strane. (foto: Shutterstock)*

Brisači na stotinama strojeva

Stručnjaci za kibernetsku sigurnost upozoravaju, da su već više mjeseci, prije nego li je Rusija službeno oglasila početak invazije na Ukrajinu, primjećivali znakove nadolazećeg rata. A sada upozoravaju, da nema nikakvih indikatora, koji bi najavljivali približavanje njegovog kraja. S tijekom sadašnjeg kibernetskog rata se povećava strah, da bi u budućnosti on mogao postati uzorom za stvarno smrtonosni kibernetski rat. U prvim mjesecima rata protiv Ukrajine, u velikoj mjeri su bili primjenjivani tzv. brisači, destruk-

tivna zlonamjerna programska oprema za uništavanje. Jedan od najnovijih i najučinkovitijih kibernetskih napada, koji je Rusija izvela tijekom rata, bila je primjena zlonamjernih brisača, koje su stručnjaci za sigurnost kasnije nazvali Hermetic Wiper.

Tvrtka za sigurnosnu programsku opremu ESET je otkrila podatke, koji ukazuju, da su brisači u danima nakon prvog otkrivanja bili instalirani na stotine strojeva u Ukrajini. ESET prema primijećenim uzorcima zlonamjerne programske opreme procjenjuje, da je ona moguće bila stvorena u prosincu 2021. godine, prije početka rata, te da je Rusija moguće planirala napad već više mjeseci prije toga. Daljnja istraživanja tvrtke ESET su otkrila, da su napadači u računalima žrtve u potpunosti preuzeli kontrolu nad serverom Active Directory. Čini se da je zlonamjerna programska oprema bila sakrivena u preuzetom pravilniku domene. Analize Cisco Talosa, jedne od najvećih grupa za upravljanje kibernetskim opasnostima, utvrdila je, da Hermetic Wiper počinje djelovanje s prebrojavanjem fizičkih drivea sustava i oštećivanjem prvih 512 bajta sa ciljem uništavanja glavnog zapisa drivea.

» *Podrška upletenih zemalja: hakerske grupe vjerojatno dobivaju snažne resurse upletenih zemalja za svoje kibernetske operacije i napade.*

Bolje uništiti nego li obnavljati

Na taj način se onemogućuje pravilno djelovanje računala, čak i ako zlonamjerna programska oprema djelomično ne uspije obaviti svoj zadatak. Program zatim analizira pojedine particije i onemogućuje Volume Shadow Copy Service te instalira različite destruktivne mehanizme, ovisno o vrsti drivea (FAT ili NTFS). Cilj napada su bile i različite sistemske datoteke, koje su zatim čekale, da se svi usporeni procesi završe i da se ponovo pokrene stroj te s time dovrši postupak brisanja. Sigurnosna tvrtka Check Point procjenjuje, da je zlonamjerna programska oprema za brisanje jedan od ključnih sigurnosnih trendova u 2022. godini. U nekim slučajevima se pokazalo, da se više isplati računala uništiti, nego li ih popravljati.

Uz to je Kibernetsko zapovjedništvo SAD (US Cyber Command, USCC) upozorilo na 20 novih vrsta zlonamjerne programske opreme, koje su ciljale na sustave u Ukrajini, i koje nadopunjuju velik broj DDoS napada (distribuirane paralize usluge), pokušaja ribarenja i druge taktike, koje su primijenjene protiv Ukrajine. Povećana razmjena obavještajnih podataka između Ukrajine i SAD te napora obiju strana na području kibernetske sigurnosti su doveli do otkrića vala zlonamjerne programske opreme. Od straha, da Rusija možda koristi sadašnji napad kao sredstvo oblikovanja »plana« uspješnog kibernetskog rata, US CC savjetuje, da »savezničke nacije smatraju svaku analizu strategije Rusije kao važnu za sprječavanje prevladavanja napadačkih nacija u budućim bitkama«.

Prelijevanje po čitavoj Europi

Ribarenje (lažno predstavljanje) je prema mišljenju US CC središnji stup kibernetske ofenzive Rusije tijekom napada i uz to je platforma, preko koje ta zemlja nastoji zaraziti ciljeve sa zlonamjernom programskom opremom. Kibernetska sigurnosna tvrtka Mandiant je nedavno otkrila, da su određene vrste zlonamjerne programske opreme, koje su otkrili Ukrajina i US CC, često prodrle preko napada ribarenja. Mandiant smatra, da te operacije vode dvije grupe za napade – UNC1151 vjerojatno povezana s vladom Bjelorusije, i UNC2589, povezana s vladom Rusije. Stručnjaci za sigurnost iz zemalja saveznica su već na početku konflikta upozoravali, da kibernetski napadi mogu postati toliko snažni, da će se posljedice osjetiti i izvan Ukrajine. Te prognoze su se ostvarile na početku godine, nakon napada Rusije na Viasat, koji se odvijao svega nekoliko sati prije službenog početka rata i prelio se u druge dijelove Europe.

Pojedinci su imali probleme s internetom i doživljavali su ispade

› Rat protiv obrazovanja

Rat je zahvatio milijune ljudi te im je uskratila najosnovnije potrebe, uključujući obrazovanje. Prema podacima ukrajinskog ministarstva za školstvo, od početka napada bilo je oštećeno ili uništeno više od 1800 škola i sveučilišta. Obje strane su primjenjivale škole kao vojne baze ili za skladištenje oružja. Obrazovanje je temeljno za učenike i studente tijekom rata, jer pored obrazovanja, škole i sveučilišta mogu osigurati siguran prostor, vratiti im barem dio osjećaja normalnog života te ih povezati sa resursima za pomoć, kao što su obroci i usluge duševnog zdravlja. Na sreću je 3,7 milijuna ukrajinske djece unatoč zatvaranju škola moglo pristupati internetu i učiti na daljinu. To je smanjilo praznine u edukaciji, iako je dugoročni utjecaj rata na kvalitetu i pristup obrazovanju vrlo ozbiljan. Obnove škola će zahtijevati mnogo vremena i sredstava, a brojni učenici i učitelji će doživjeti stres i traume, koje otežavaju učenje i poučavanje.

Čak i kada se vrate obrazovanju, djeca na područjima, koje je zahvatio rat, biti će najmanje dva puta više odsutni od onih u drugim krajevima. Posljedice na obrazovanje se, nažalost, ne događaju samo u Ukrajini. Učenje trpi po čitavom svijetu, jer je oružano nasilje nad učenicima, učiteljima i obrazovnim ustanovama u porastu. Konkretno se u 2020. i 2021. godini u prosjeku dogodilo šest napada na obrazovanje svakoga dana, kako navodi novi izvještaj Globalne koalicije za zaštitu obrazovanja od napada (GCPEA). U tom devetogodišnjem razdoblju su identificirali više od 5.000 primjera napada ili vojnih primjena škole, u kojima je bilo ozlijeđeno ili umrlo više od 9.000 studenata, učitelja i profesora. Za zaštitu obrazovanja u Ukrajini i drugdje moguće je usvojiti više ključnih koraka, počevši s time, da sukobljene strane moraju prestati napadati škole i sveučilišta ili primjenjivati eksplozivno oružje u njihovoj blizini.

Sukobljene strane bi morale izbjegavati i okupacije škola i sveučilišta te njihove primjene u vojne svrhe. Vlade bi morale usvojiti i provoditi Deklaraciju o sigurnim školama, koji je usvojila GCPEA. Rusija nije podržala deklaraciju, dok ju je Ukrajina usvojila 2019. godine i zatim pripremila potrebne mjere za ispunjavanje obaveza deklaracije tijekom konflikta, kao što je uvođenje učenja na daljinu i sakupljanje podataka o napadima na obrazovne objekte. Vlade, Ujedinjeni narodi te nacionalne i međunarodne organizacije bi morale poduprijeti napore za sakupljanje pouzdanih dokaza i napadima na škole i sveučilišta, kao i na studente i osoblje, osigurati pomoć žrtvama napada te nastojati, da se odgovornim osobama sudi na pravednim nacionalnim i međunarodnim sudovima. Na kraju je potrebno povećati financiranje i usmjeriti ga u obnovu škola i sveučilišta, uništenih u napadima, odmah čim to bude sigurno.

po čitavom kontinentu, a u susjednim zemljama su zabilježeni problemi s vjetroelektranama. To je bio prvi veći napad u ratu i onaj, koji je na kraju obilježio sljedeće mjesece šokantnog ratovanja – prvi primjer rata, koji se odvijao i kinetički, kao i u kibernetskom prostoru. »Lažne zastave, pogrešno dodjeljivanje, ometane komunikacije i manipulacija društvenim medijima su ključni elementi ruskih scenarija informacijskog rata,« ocjenjuje tvrtka Sophos, specijalizirana za programsku i strojnu sigurnosnu opremu. »Rusija ne može brinuti za stalno skrivanje svojih djelovanja na terenu ili bilo gdje, stoga mora jednostavno uzrokovati dovoljno zakašnjenja, zbunjenosti i protuslovlja, kako bi s drugim istodobnim operacijama postigla svoje ciljeve.«

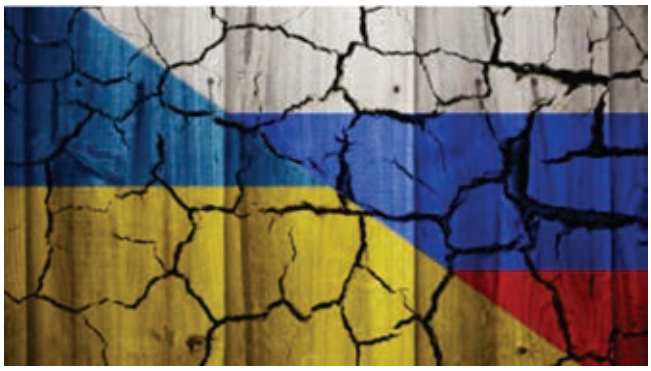
Microsoft identificira ranjivost

Microsoft je u lipnju objavio rezultate produbljenog istraživanja dotadašnjih kibernetskih iskustava dobivenih rijekom rata u Ukrajini. Zaključci su temeljeni obzirom na uvid u zlonamjerne digitalne aktivnosti Rusije i na novim detaljima o sofisticiranim i opsežnim operacijama utjecaja na inozemstvo povezane s ratom. Microsoft je imao jedinstven položaj praćenja digitalne situacije u Ukrajini od početka ruskog napada 24. veljače, zapravo još i

» *Strategija kibernetskog rata: prema ocjeni Microsofta Rusija izvodi kibernetske napade unutar Ukrajine, prodore u mreže i špijuniranje izvan Ukrajine te operacije kibernetskog utjecaja u svijetu.*

prije Predsjednik tvrtke, Bred Smith, ne u ožujku, uz financiranje humanitarnih napora za tehničku pomoć, naložio primjenu Microsoftove platforme RiskIQ za identificiranje ranjivosti kibernetske sigurnosti u ukrajinskom vladinom sustavu. Društvo je ukrajinskoj vladi dostavilo »popis nepopravljenih grupnih ranjivosti i izloženosti (CVE), koji napadačima mogu omogućiti prodor«.

Microsoftovi sigurnosni stručnjaci su bili među prvima, koji su



» *Početak dan prije invazije: Microsoft je utvrdio, da je Rusija primijenila uništavajuće kibernetsko oružje protiv ukrajinskih računala 23. veljače. (foto Shutterstock)*

već u siječnju, prije invazije, otkrili napade zlonamjerne programske opreme, koji su srušili oko 70 internetskih stranica ukrajinske vlade. Tvrtka je u Microsoft 365 ugradila zaštitu za novo otkrivenu destruktivnu zlonamjernu programsku opremu. Predsjednik Microsofta je u uvodu izvještaja napisao, da je »prvi pucanj Rusije protiv Ukrajine bio uništavajuće kibernetsko oružje protiv ukrajinskih računala nazvano Foxblade primijenjeno 23. veljače, dakle prije početka rata«. Smith je rekao, da ruska strategija kibernetskog rata uključuje »tri odvojena i donekle koordinirana djelovanja« – uništavajuće kibernetske napade unutar Ukrajine, prodore u mreže i špijuniranje izvan Ukrajine te operacije kibernetskog utjecaja, usmjerene na ljude po čitavom svijetu«.

Ciljanje na kritične strukture

Prema ocjeni tvrtke Symantec jedna od najaktivnijih kibernetskih grupa povezanih s Rusijom je Shuckworm (mošusni crv), koja već dulje vrijeme ukrajinskim organizacijama šalje zlonamjernu programsku opremu za prenošenje podataka i druge špijunske alate. Symantecov Threat Hunter Team, koji je dio Broadcom Software, procjenjuje, da su nove aktivnosti većinom nastavak napada, o kojima je u srpnju izvijestio Odzivni centar za kibernetsku sigurnost Ukrajine (CERT-UA). Symantec pojašnjava, da je Shuckworm (ili Gamaredon tj. Armageddon, kako se još naziva) grupa, koja se gotovo isključivo usredotočuje na Ukrajinu, a njihova zlonamjerna programska oprema je sposobna snimati zvuk s pomoću mikrofona u sustavu, preuzeti snimke zaslona, bilježiti tipkanje na tipkovnici te preuzimati i izvoditi datoteke .exe i .dll.

Ukrajinski centar procjenjuje, da se učestalost ruskih kibernetskih napada utrostručila neposredno prije početka rata, a od početka rata su agresivno ciljali na kritične infrastrukture. Mnogi stručnjaci u svijetu su na početku rusko-ukrajinskog rata procjenji-

vali, da će ruske kibernetske operacije brzo blokirati informacijske sustave u Ukrajini, no to se nije dogodilo. Ukrajinski ministar za digitalnu preobrazbu Mihail Fedorov glavni razlog ruskog neuspjeha vidi u razlici između sustava dviju zemalja, jer je, prema njegovom mišljenju, ruski sustav centraliziran i monopoliziran, s time i korumpiran, što s nastavkom rata postaje sve očitije. Fedorov ističe, da se Ukrajina na ruski napad pripremala od 2014. godine. Između ostalog, opremila se s više od 10.000 terminala Starlink, koji omogućuju povezanost zemlje i tijekom bombardiranja i granatiranja.

Osposobljavanje ukrajinske obrane

Starlink je internetska satelitska mreža tvrtke SpaceX Elona Muska, u kojoj je do danas u niskoj orbiti postavljeno više od 3000 malih satelita iz masovne proizvodnje. Mreža nudi satelitski internet u 40 zemalja, u kojima je od lipnja ove godine sakupila više od 500 tisuća naručitelja. Nabava Starlink terminala je dio opremanja zemlje, povezanog sa suradnjom, osposobljavanjem i vježbama s NATO savezom, koji su Ukrajinu načinili bitno otpornijom na kibernetske napade. Ukrajinski dužnosnici ističu, da bi bilo pogrešno podcjenjivati napredne operacije Rusije u njihovoj zemlji, kao što bi također bilo pogrešno precjenjivati ruske kibernetske mogućnosti. Stručnjaci neprekidno procjenjuju ruske potencijale na tom području te primjećuju djelovanje grupa, kao što su Sandworm, Fancy Bear i Gamaredon, koje su i dalje aktivne i opasne.

Five Eyes, obavještajni savez, koji uključuje Australiju, Kanadu, Novi Zeland, Ujedinjeno kraljevstvo i SAD, daje naslutiti kako njihove obavještajne agencije osiguravaju osposobljavanje i podršku ukrajinskoj kibernetskoj obrani i dijele obavještajne podatke o prijetnjama. Drugi izvori izvještavaju, da je razmjena informacija »dvosmjerna«, jer Ukrajina, između ostalog, ima organizirano masovno sakupljanje obavještajnih podataka, u kojem obični ljudi izvještavaju o kretanjima ruskih vojnih jedinica. Fedorov posebno ističe, kako se Ukrajina uspjela obraniti i u kibernetskom prostoru, kao i u propagandnom ratu zbog činjenice, da je ostala povezana na internet. Povezanost na Internet je uspjela ne samo zbog terminala povezanih sa satelitskom mrežom Starlink, već i zbog decentraliziranosti mreže ponuditelja internetskih usluga.

Tajni kibernetski rat

Ministar Fedorov pojašnjava, da bi za obnovu kilometara kabelskih veza između gradova nakon teških bitaka bilo potrebno nekoliko mjeseci, a s pomoću jednog Starlink satelita i terminala, to je moguće učiniti u nekoliko dana. Dodaje, da terminale Starlink primjenjuju prije svega za povezivanje u tzv. slijepim točkama za tradicionalno pokrivanje, dok se trude zaštititi zemaljske i mobilne veze ili ih ažurno obnavljati. Fedorov između ostalog ističe, da je za Ukrajinu ostati na internetu jasan strateški cilj. Da je toga svjesna Rusija, potvrđuje činjenica, da su pojedini terminali bili očigledno više ciljano bombardirani i uništeni, no time nije bio ugrožen čitav sustav. Kako god, za zemlju je iznimno važno, da je podnijela agresivne pokušaje, da se na njenom terenu onemogući djelovanje interneta te energetskih i financijskih sustava.

Kibernetski incidenti zapravo imaju središnju ulogu u rusko-ukrajinskom ratu, ocjenjuje Cynthia Brumfield, IKT-analitičarka i stručnjakinja za kibernetsku sigurnost. Unatoč tome se nije dogodio »kibernetski rat velikih razmjera, kao što su neki poznavatelji najavljivali barem kao mogućnost. Postoji više teorija, koje pojašnjavaju, zašto Rusija nije pokrenula uništavajući kibernetski napad na Ukrajinu, iako je za to sposobna. Razloga je više, od uvjerenja da Rusija najteže kibernetsko oružje čuva za gorak kraj, do ocjene, da je previše brine vjerojatnost uništavajućeg zapadnog odgovora. Najvjerojatnije smo danas na sredini toga, što Thomas Rid, profesor strateških studija u Školi za napredne međunarodne studije Sveučilišta Johns Hopkins, naziva tajnim kibernetskim ratom. Digitalni rat se odvija u sjeni, smatra Rid, pri čemu je cilj očitijih kibernetskih napada preusmjeravanje pozornosti s incidenata, koje ne bismo smjeli vidjeti.

» Kamera, koja vidi što želi

Jernej Kovač

Istraživači sa Sveučilišta Kalifornija u Los Angelesu UCLA su predstavili kameru, razvijenu s umjetnom inteligencijom. Njena posebnost je, da u svoj objektiv prihvaća samo predmete iz okoline, koji zanimaju korisnika. Druge objekte zanemari. Dizajneri su pojasnili, da za druge objekte (p) ostaje slijepa, jer omogućuje specifično slikanje ciljnih predmeta s trenutnim optičkim brisanjem predmeta drugih razreda.

U posljednjem desetljeću su se digitalne kamere na široko uvele u različitim aspektima našeg društva i masovno se primjenjuju u mobilnim telefonima, sigurnosnim nadzorima, autonomnim vozilima i pri prepoznavanju lica. S tim kamerama se stvaraju ogromne količine slikovnih podataka, što rezultira sve većom zabrinutošću obzirom na zaštitu privatnosti.

Neke postojeće metode te dvojbe rješavaju primjenom algoritama za prikrivanje osjetljivih informacija iz dobivenih slika, kao što su zamagljivanje slike ili šifriranje. No kod takvih metoda i dalje postoji rizik od izloženosti osjetljivih podataka, jer su neobrađene slike snimljene i prije digitalne obrade, s kojom se osjetljive informacije mogu sakriti ili šifrirati. Pored toga, izračunavanje tih