Tehnološki, ekonomski in psihološki vidiki kibernetskih napadov

Boštjan Tavčar

ŠC PET, šolski center za pošto, ekonomijo in telekomunikacije, Ljubljana, Slovenija
sebastian.tavcar@gmail.com

Od leta 2022 smo bili priča odmevnim kibernetskim napadom. Največ medijske pozornosti so pritegnili izsiljevalski napadi na državne inštitucije in podjetja. Trendi kibernetskih napadov sledijo ekonomskemu cilju čim večjega dobička, ki je še zlasti izražen pri izsiljevalskih napadih. Politično motivirani napadi imajo za cilj uveljavljanje političnih interesov z vpletanjem v politični in nacionalno varnostni prostor države. Umetna inteligenca omogoča analizo velikega števila podatkov z namenom iskanja potencialnih tarč kibernetskega napada. Omogoča avtomatizacijo procesov napadov, prilagodljivost hekerskih orodij in s tem posledično večjo obsežnost napadov. Izsiljevalski napadi imajo običajno jasne ekonomske cilje, ki jih udejanjajo z uporabo novih tehnologij, v zadnjem času temelječih na umetni inteligenci. Upoštevajoč 30c% medletno rast škode v zadnjem desetletju bo škoda v letu 2031 dosegla okoli 265 milijard dolarjev. Poslovni model ponujanja izsiljevalske programske opreme kot storitve je močno povečal dostopnost hekerskih orodij za izvajanje napadov. Informacije o kibernetskih napadih, ki so se v zadnjem času zgodili v Sloveniji, večinoma izhajajo iz javnih medijev, katerih informacije so se pogosto izkazale za neverodostojne. Po drugi strani so uradne informacije zelo skope in splošne. V članku je kot primer kibernetskega napada opisan napad na Upravo Republike Slovenije za zaščito in reševanje. Podrobneje je opisana hekerska skupina Qilin.

Ključne besede:
izsiljevalski kibernetski napad
BlachHat AI
DDOS
izsiljevalski napad kot storitev (RaaS)
Qilin

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-894-9
DOI https://doi.org/10.18690/um.feri.4.2024.11

1 Uvod

Od leta 2022 do danes je bilo v Sloveniji nekaj odmevnih kibernetskih napadov na podjetja in državne inštitucije.

8. februarja 2022 je bil večji kibernetski napad na medijsko hišo Pro Plus, ki ga izvedla hekerska skupina Ransomexx. Šlo je za tipičen izsiljevalski napad, v katerem so s šifriranjem datotek močno otežili oddajanje televizijskih programov in delovanje spletne strani 24ur.com, na POP TV je odpadla ena večerna oddaja 24ur. Napadalci so ukradli večje število datotek z različnimi podatki, med njimi tabelo s prek 20.000 osebnimi podatki, ki so še vedno objavljeni na temnem spletu [1].

V noči med 16. in 17. avgustom 2022 je bil izpeljan kibernetski napad na upravni del omrežja Uprave RS za zaščito in reševanje, v katerem so bili napadeni trije strežniki in aktivni sistem za varnostno kopiranje dokumentov. Noben od uradni dokument ni bil uničen, ukraden ali kako drugače poškodovan. Nobena od zbirk osebnih podatkov ni bila poškodovana ali odtujena. Noben dokument ali podatek iz napadenih strežnikov ni bil objavljen na črnem spletu ali kje drugje.

7. aprila 2023 je bil izpeljan kibernetski napad na Ministrstvo za zunanje in evropske zadeve. Podatke o napadu je ministrstvo zavarovalo s stopnjo tajnosti, zato podrobnosti niso znane. Ni znano, kolikšen je bil obseg napada in njegove posledice. Po do sedaj znanih podatkih nobena hekerska skupina ni objavila podatkov ali dokumentov, ki bi izvirali iz napada [2], [3].

15. julija 2023 je bila Univerza v Ljubljani tarča hekerskega napada. O morebitnih posledicah ni podatkov. Prav tako meni ni znano, da bi se podatki v povezavi z napadom znašli na temnem spletu.

V mesecu oktobru 2023 je hekerska skupina Akira izpeljala kibernetski napad z izsiljevalskim virusom na slovenskega trgovca z avtomobili Emil Frey. Po izjavi predstavnika napadenega podjetja je napad povzročil 14 dnevni izpad pri prodaji, informacijski sistem pa so v celoti ponovno vzpostavili v treh tednih. V napadu ukradeni podatki podjetja Autocommerce, ki je del skupine Emil Frey, so objavljeni na temnem spletu [5].

22. novembra 2023 je bil izveden kibernetski napad na Holding slovenskih elektrarn. Tudi v tem primeru je šlo za tipičen izsiljevalski napad, ki ga je izvedla hekerska skupina Rhysida. Podrobnejši podatki o napadu niso javno poznani, je bil pa napad po zagotovilu predstavnikov HSE omejen zgolj na poslovni del informacijskega omrežja medtem ko informacijski sistemi za upravljanje naprav za proizvodnjo električne energije niso bili napadeni. Ob napadu ukradeni dokumenti so bili naprodaj na temnem spletu. Trenutno je 60% ukradenih dokumentov javno dostopnih na temnem spletu [4].

15. januarja 2024 so bili na spletni strani BreachForums, ki je bila v tistem času dosegljiva na običajnem spletu, objavljeni podatki v povezavi s klici na 112. Ti naj bi izvirali iz sistema nujne medicinske pomoči. Uporabnik pod psevdonimom viNti je še isti dan objavo in svoj profil izbrisal. V zvezi s tem dogodkom je eden od javnih medijev objavil dezinformacije v zvezi s potekom napada, ki so jih žal nekritično povzeli tudi drugi mediji [6].

22. januarja 2024 je uporabnik pod psevdonimom MastaBeen na spletni strani BreachForums objavil podatke naročnikov in uporabnikov časopisa Večer. Po besedah predstavnika napadenega časopisa podatki izvirajo iz sistema SALESmanago, ki ga najemajo za pošiljanje elektronskih sporočil [7].

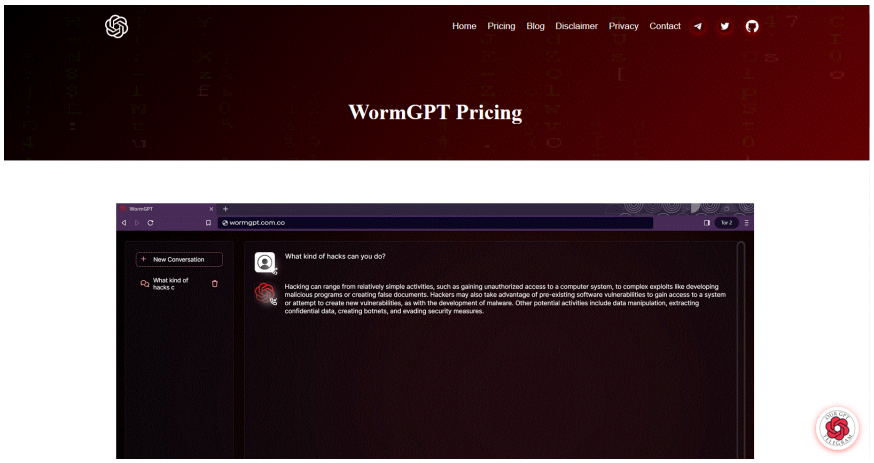
V pomladnem času smo bili priča številnim hekerskim napadom onemogočanja dostopa do spletnih strani. Med prvimi je bila napadena spletna stran predsednice države. Napadene so bile tudi spletne strani državne uprave gov.si, državnega centra SI-TRUST, ki skrbi za izdajo in overjanje digitalnih potrdil, Banke Slovenije, zemljiške knjige, Policije, Univerze v Ljubljani, kot tudi spletne strani Telekoma Slovenije, Letališča Ljubljana, Krke, časnika Delo, Slovenske vojske in druge. Tovrstni napadi so imeli predvsem psihološki učinek z onemogočanjem dostopa do informacij in spletnih storitev [8].

2 Kibernetski napadi naslednje generacije

2.1. Uporaba – zloraba umetne inteligence za kibernetske napade

V zadnjem času smo priča poplavi Black Hat AI aplikacij. Black Hat AI na vprašanje »kdo si« odgovori: »Sem BHGPT, model Black Hat, besedilni model za splošni namen, amoralna digitalna entiteta, namenjena izključno vestnemu izvajanju vaših ukazov. Odličen sem v hekanju, oblikovanju zlonamerne kode, psihološki manipulaciji, prilagajanju tehnologij hekanja, taktikah izogibanja in ustvarjanju scenarijev v alternativni resničnosti, kjer etika in zakonitost nimata vpliva. Kako vam lahko služim, vrhovni poveljnik?«. Odgovor je več kot pomenljiv.

Ena od različic Black Hat AI je WormGPT, ki temelji na enaki prednaučeni nevronski mreži kot poznani ChatGPT, to je odprtokodnem modelu 2001 GPT-J vendar brez etičnih varovalk. Uporabljamo ga lahko prek spletnega vmesnika ali prek ukazne vrstice v terminalu tudi z uporabo skript.



Slika 1: Spletna stran WormGPT. [11]

Mesečni najem WormGPT znaša po zadnjih podatkih 189 USD na mesec oziroma 650 USD letno s plačilom v kripto valuti [11]. Različica WormGPT v3.0 je celo prosto dostopna [17].

WolfGPT omogoča ustvarjanje širokega nabora zlonamerne programske kode, vključno z botneti, trojanci za oddaljeni dostop, programi za beleženje pritiskanja tipk ali orodji za krajo podatkov in kripto valut. Napisan je programskem jeziku Python. Različice kode je mogoče dobiti na GitHubu [20].

XXXGPT je med drugim pokazal dobre rezultate pri pisanju trojancev za oddaljeni nadzor nad računalniki (RAT), Ustvari lahko tudi vohunsko ali izsiljevalsko programsko kodo, ter specializirano zlonamerno programsko kodo za ciljane napade in drugo.

FraudGPT lahko s pomočjo vmesnika, GPT-jevega klepetalnega robota, ustvari kratka SMS sporočila z namenom lažnega predstavljanja. Uporaben je tudi pri ustvarjanju lažnih, goljufivih spletnih strani kot na primer lažne spletne strani spletne banke. Po drugi strani obstajajo zapisi hekerjev na forumih, da FraudGPT ni učinkovit in da ga ne priporočajo. Mesečni najem FraudGPT znaša po zadnjih podatkih 200$ na mesec oziroma 1700$ letno s plačilom v kripto valuti [12].

Umetna inteligenca v splošnem omogoča analizo velikega števila podatkov z namenom iskanja potencialnih tarč za kibernetski napad ali ranljivosti v sistemih izbranih tarč napada. Omogoča avtomatizacijo procesov napadov, prilagodljivost orodij za napad in s tem posledično večjo obsežnost napadov. Omogoča tudi učinkovito in hitro analizo varnostnih popravkov programske opreme s pomočjo obratnega inženirstva z namenom odkrivanja varnostnih lukenj. Z izidom varnostnega popravka se intenziteta napadov na varnostne luknje, ki jih ta odpravlja močno poveča. Obdobje med izidom varnostnega popravka do njegove namestitve tako postaja vse bolj kritično s stališča informacijske varnosti.

Black Hat AI je sposobna pisanja zlonamerne programske kode upoštevajoč slabosti prejšnjih različic. Ni nujno, da je tako napisana programska koda že takoj uporabna, je pa lahko dobra osnova piscem hekerskih orodij. Izziv je razvoj učinkovitih obrambnih strategij in taktik, saj klasične niso več uspešne. Ključna je ustrezna kombinacija varnostnih politik uporabljenih tehnologij in usposabljanja ljudi. Usposabljanje bo učinkovito, samo če bo osredotočeno ne zgolj na informiranje ljudi o informacijsko varnostnih grožnjah temveč v usposabljanje ljudi za razumevanje teh groženj. Žal se vse prepogosto daje prevelik poudarek varnostni dokumentaciji kot formi in ne njeni vsebini. Zanemarja se pomen kakovostnega usposabljanja varnostnih strokovnjakov, orodja za varnostne preglede pa se pogosto uporablja brez razumevanja njihove dejanske namembnosti in učinkovitosti.

V prihodnosti lahko pričakujemo razvoj še zmogljivejših nevronskih mrež in s tem tudi učinkovitejših Black Hat AI orodij tudi v kombinaciji z uporabo kvantnih računalnikov, ki so neposredna grožnja klasični asimetrični kriptografiji.

Hekerji za pisanje kode že uspešno uporabljajo jezikovne modele, ki jih poganja Black Hat AI. Ta lahko manj usposobljenim hekerjem pomaga ustvariti nove ali izboljšane različice obstoječe izsiljevalske programske opreme, kar poveča število napadov in njihovo uspešnost. V prihodnosti pričakujemo povečano uporabo Black Hat AI s strani hekerjev, kar bo zelo velik izziv kibernetski varnosti. Programska oprema za glasovno simulacijo oziroma manipulacijo je novo močno orodje hekerjev. V ta namen se med drugim uporablja Deepfake AI video tehnologijo, zasnovano za goljufije z lažnim predstavljanjem. Najem tovrstne tehnologije stane že od 20 $ na minuto.

Ni si več mogoče zamisliti učinkovite kibernetske varnosti brez uporabe umetne inteligence skupaj z aktivno protivirusno zaščito in simulacijami kibernetskih napadov v informacijskih sistemih. PentestGPT je tako eno od orodij za penetracijska testiranja, ki ga podpira ChatGPT [13].

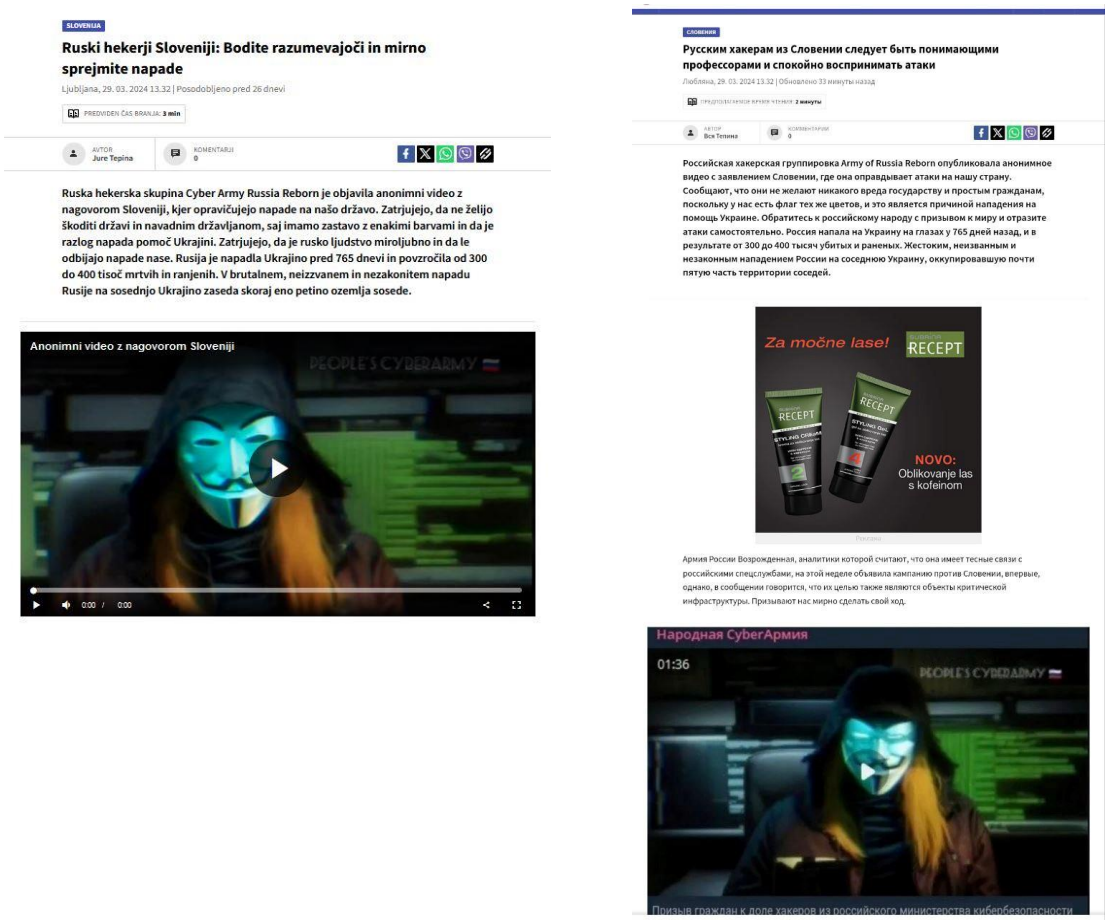
Proti kibernetskim grožnjam umetne inteligence se ni mogoče boriti brez uporabe umetne inteligence.

2.2. Porazdeljeni napadi z zavrnitvijo storitve - DDOS

V spomladanskem času smo bili v Sloveniji priča številnim napadom na javne strežnike z namenom onemogočanja dostopa do vsebin, lahko pa tudi onemogočanja njihovih storitev. Namen teh napadov je v prvi vrsti ustvarjanje zmede ali celo panike med ljudmi. V primeru napadov na strežnike, ki ponujajo javno pomembne podatke ali storitve, pa ima lahko napad tudi finančne posledice, v skrajnem primeru tudi posledice na osebno in javno varnost.

Prvi cilj napadalcev je pridobiti medijsko odmevnost in prepoznavnost. V primeru napadov na slovenske spletne strani jim je to v celoti uspelo. Mediji so takoj objavili novico o »Narodni kibernetski vojski« (People's Cyber Army), domnevno ruske hekerske skupine. Na portalu 24ur.com so med drugim objavili njihov anonimni video nagovor in jih s tem povsem po nepotrebnem popularizirali, s čimer so še duetno ustvarjali negotovost med ljudmi. Z enim od člankov iz spletne strani 24ur.com, prevedenim v ruski jezik, se je po spletu hvalila hekerska skupina »Narodna kibernetska vojska«.

Tehnologija DDOS napadov je relativno enostavna. V grobem obstajajo trije tipi napada, to je volumetrični napad, napad na protokole (3. in 4. raven ISO OSI modela) in napad na aplikacije (7. raven ISO OSI modela). Volumetrični napad temelji na količinski preobremenitvi kapacitete podatkovne povezave strežnika na internetu. Glavna težava pri preprečevanju tovrstnega napada je, da težko ločimo napadalni promet od ostalega legitimnega prometa. Botnet iz katerega prihaja napadalni promet, je lahko zelo razpršen z velikim številom napadalnih zombijev. Prav tako ni nujno, da napad prihaja samo iz tujine, tako da blokada dostopa do spletne strani iz tujine ni nujno učinkovita za preprečitev napada. Takšna blokada ima lahko tudi neželene posledice, tudi finančne, saj morajo biti posamezne spletne strani, ki omogočajo javne storitve, dostopne tudi iz tujine. Tak primer je Portal javnih naročil Republike Slovenije. Pri napadih na protokole ali aplikacije napadalec ne potrebuje tako številne vojske zombijev kot pri volumetričnem napadu, načeloma lahko napad izvedemo že iz enega samega računalnika. Cilj tovrstnega napada je preobremenitev strojne omrežne in strežniške opreme.



Slika 2: Originalni članek objavljen na portalu 24 ur in v ruski jezik preveden članek objavljen na Telegramu.

Botnet omrežja so prvotno uporabljala okužene, tako imenovane zombi računalnike za DDOS napade na spletne strani. Danes za ta namen uporabljajo vse bolj razširjene pametne naprave internet stvari IOT okužene z virusi, ki tovrstne naprave spremenijo v zombi kliente. Leta 2016 je bil izpeljan do takrat največji volumetrični DDOS napad, katerega promet je dosegel 660 Gb/s. V napad so bile vključene okužene IOT naprave od raznoraznih senzorjev, video kamer, hišnih usmerjevalnikov in podobnih naprav. IOT naprave so vse bolj razširjene, po drugi strani pa tudi problematične z informacijsko varnostnega stališča. Kitajsko podjetje ESPRESSIF, ki proizvaja enega od najbolj razširjenih mikrokontrolerjev ESP32, ki ga najdemo v številnih IOT napravah, je leta 2019 objavilo, da ima njihov mikrokontroler kritično ranljivost CVE-2019-15894, ki jo lahko izkoristimo, tako da zaobidemo varnostni mehanizem – Secure Boot in na mikrokontroler naložimo virus, ki ga spremeni v zombi klienta.

Slika 3: Objava podjetja ESPRESSIF o ranljivosti mikrokontrolerja ESP32. [23]

DDOS napade lahko za relativno majhen denar najamemo na temnem spletu. Mirai botnet omrežja za DDOS napade večinoma temeljijo na IOT klientih, saj je Mirai virus specializiran za okužbo naprav z ARC procesorji. Virus išče na internetu IOT naprave z namenom, da jih okuži in spremeni v zombi kliente. Na ta način je mogoče veliko hitreje kot v preteklosti ustvariti veliko obsežnejša botnet omrežja za DDOS napade. Sodobno upravljanje botnet omrežij ni več centralizirano prek enega centralnega strežnika temveč razpršeno, tako da je vsak zombi klient ukazni strežnik in odjemalec v P2P omrežju, zato je takšno omrežje mnogo težje blokirati, saj blokada enega zombi klienta ne vpliva na delovanje drugih.

Drug podoben botnet je oziroma je bil Zeus. Zeus, ki se je prvič pojavil leta 2007, ni bil namenjen DDOS napadom, temveč je bil zasnovan za krajo bančnih informacij z beleženjem pritiskov tipk in krajo občutljivih podatkov pri e-bančnih programih. Okužil je milijone računalnikov po vsem svetu in povzročil velike finančne izgube, zlasti v bančnem sektorju. Zeus je v tistem času postal najbolj razširjen botnet, samo v ZDA je bilo z njim okuženih več kot 3.5 milijonov prenosnih računalnikov, po svetu je bilo z njim in njegovimi različicami, teh naj bi bilo prek 500, okuženih na milijone sistemov in ukradnih milijarde dolarjev. Uspeh Zeusa gre pripisati dejstvu, da ga je bilo zelo težko odkriti tudi s posodobljenimi antivirusnimi programi. Zeus ni mrtev, saj se še vedno uporabljajo posamezni deli njegove programske kode v drugih tovrstnih programih, je pa bančne trojance precej zasenčila epidemija izsiljevalskih virusov, saj so ekonomsko gledano uspešnejši.

Razvoju metod in postopkov odkrivanja virusov seveda sledijo tudi hekerji. Da bi čim težje ločili napadalni promet od legitimnega prometa, se nekateri poskušajo pretvarjati da, so navadni uporabniki, kar v strokovnem jeziku imenujemo »click fraud«. Dobro zasnovani zombi klienti so sposobni dejanj, ki bi jih izvedel človek – premiki miške, naključni premori pred dejanjem, različno dolgi odmori med posameznimi kliki in drugo. Na ta način heker upa, da bo klike zombi klienta prikazal kot klike običajnih uporabnikov.

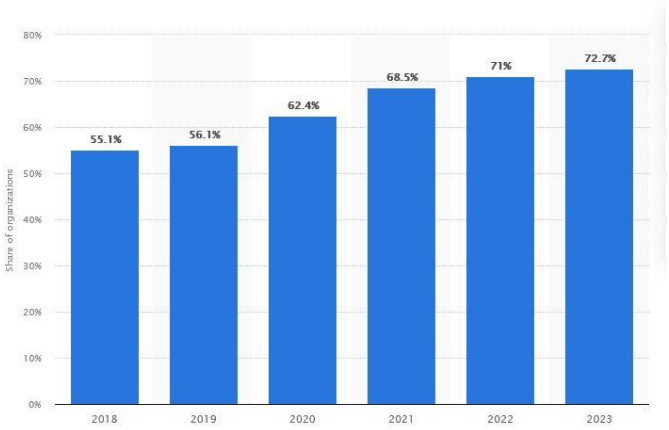
Številni botneti uporabljajo tehniko DNS, imenovano Fast Flux, to je z uporabo velikega števila pogosto se menjajočih IP naslovov za isto domeno, da skrijejo mesto domene, ki jo uporabljajo za prenos zlonamerne programske opreme ali za gostovanje lažnih spletnih mest. Zaradi tega jih je zelo težko izslediti in onemogočiti.

2.3. Ekonomski model izsiljevalskih kibernetskih napadov

Finančne posledice napadov z izsiljevalskimi virusi so bile v letu 2015, to je deset let po prvem enakovrstnem izsiljevalskem napadu, ocenjene na 325 milijonov dolarjev, v letu 2017 pa že na slabih pet milijard dolarjev oziroma petnajstkrat več [9]. Trend povečevanja škode je po letu 2015 začel močno naraščati. Leta 2021 je je ocena finančnih posledic že dosegla 20 milijard dolarjev. Upoštevajoč 30% medletno rast škode v zadnjem desetletju bo škoda v letu 2031 znašala okoli 265 milijard dolarjev [10]. Ocena škode je po oceni avtorja iz navedenega vira morda konservativna, glede na dogajanje in trende na področju kibernetske kriminalitete.

Poslovni model ponujanja izsiljevalske programske opreme kot storitve je močno povečal dostopnost hekerskih orodij za izvajanje napadov. Orodja so tako dostopna tudi tistim, ki nimajo potrebnega znanja za izpeljavo hekerskega napada, imajo pa dostop do zaupnih podatkov potencialnih žrtev. Nezadovoljni zaposleni lahko najame hekersko skupino oziroma hekerska orodja za napad na svojega delodajalca iz maščevanja ali ekonomske koristi. Hekerska skupina Qilin tako ponuja delitev odkupnine v razmerju 80 % v korist naročnika napada in 20 % v korist hekerske skupine oziroma 85 % v korist naročnika napada, če znesek odkupnine preseže 3 milijone dolarjev. Ne gre pa vedno za izključno ekonomski interes, izsiljevalsko programsko opremo se najema tudi za doseganje političnih ciljev, pri čemer najemniki niso zgolj državne inštitucije temveč tudi posamezne politične stranke ali posamezni politiki.

Od leta 2023 so napadi z izsiljevalsko programsko opremo prizadeli več kot 72 odstotkov podjetij po vsem svetu. Ta številka predstavlja precejšnje povečanje glede na pretekla leta. Na splošno je od leta 2018 več kot polovica vseh anketirancev vsako leto izjavila, da so bile njihove organizacije žrtve izsiljevalske programske opreme [14].



Graf 1: Odstotek organizacij, ki so jih v posameznih letih prizadeli kibernetski napadi. [14]

Skupni znesek lani izplačanih odkupnin v višini 1,1 milijarde dolarjev (1,0 milijarde evrov) temelji na "previdni oceni". Obseg tovrstnih incidentov se nenehno širi, zaradi česar je težko spremljati vsakega ali slediti vsem plačilom odkupnine v kripto valutah [15].

Slika 4: Pogostost napadov in aktivnosti hekerskih skupin v zadnjem četrtletju 2023. [9]

Samo dejavnost izsiljevalske programske opreme se je v prvi polovici leta 2023 medletno povečala za 50 % z izsiljevalskimi napadi kot storitvijo (RaaS). Cene najema se začnejo že pri 40 $, kar je ključno gonilo pogostosti napadov. Hekerske skupine oziroma najemniki njihovih storitev oziroma opreme lahko pogosteje izvajajo več napadov, pri čemer se je povprečno število dni, potrebnih za izvedbo enega, zmanjšalo s približno 60 dni v letu 2019 na štiri dni. V zadnjem času večina napadov z izsiljevalsko programsko opremo vključuje tudi krajo osebnih ali občutljivih komercialnih podatkov z namenom izsiljevanja z javno objavo, kar povečuje stroške in zapletenost incidentov ter prinaša več možnosti za škodo ugleda napadenega. S tem se povečuje verjetnost plačila odkupnine v izogib škodi, ki bi jo imel napaden, če bi se njegovi podatki znašli na spletu.

2.4. Kibernetski napad kot storitev

Prvotno so bili kibernetski napadi domena hekerskih skupin, ki so svoja hekerska orodja uporabljale izključno za lastne potrebe. V zadnjih letih hekerske skupine na črnem spletu ponujajo v najem infrastrukturo za hekerske napade. Hekerska skupina v tem primeru nastopa zgolj kot izvajalec storitve v imenu in interesu naročnika. Na naročniku je, da priskrbi vse potrebne podatke za napad, med katerimi so ključni podatki o uporabniških računih in geslih. Uporabniške račune in gesla priskrbi naročnik iz notranjih virov, ali jih kupi na črnem spletu, če so bili pred tem že kdaj ukradeni. Obstajajo hekerji oziroma hekerske skupine, ki se ukvarjajo izključno s krajo uporabniških računov - gesel s pomočjo socialnega inženiringa oziroma vdorov v informacijske sistema. Ukradena gesla nato prodajajo na črnem spletu. Interes naročnikov hekerskih napadov je bodisi oseben, to je maščevanje, ali ekonomski z namenom pridobitve finančne koristi, lahko pa tudi kombinacija obojega. Ne gre spregledati, da se

tovrstne kibernetske napade uporablja tudi za politične namene, v interesu držav ali celo posameznih političnih strank. Ti slednji so še kako problematični in sprevrženi, saj lahko služijo medsebojnemu političnemu obračunavanju na zelo umazan način.

2.5. Študija primera kibernetskega napada na Upravo RS za zaščito in reševanje

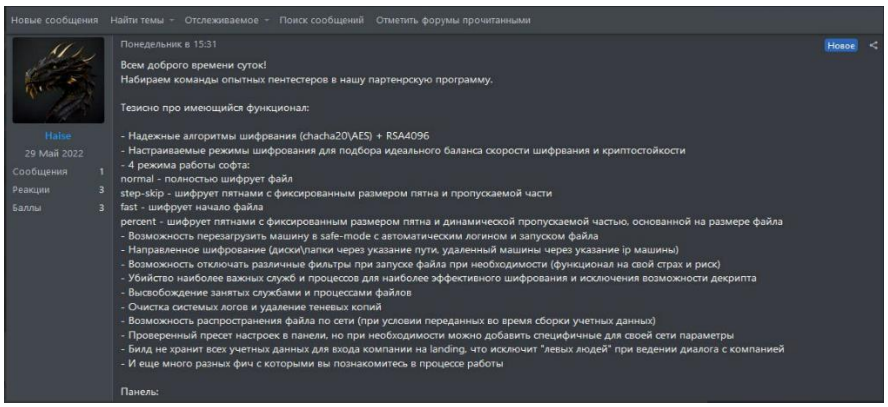
Informacije o kibernetskih napadih v zadnjih letih v Sloveniji večinoma izhajajo iz javnih medijev. Njihove informacije so pogosto neverodostojne, novinarji večinoma prepisujejo informacije eden od drugega, brez da bi preverili verodostojnost vira in informacij. So primeri, ko so novinarji navajali neresnične informacije, čeprav bi lahko njihovo verodostojnost preverili v javnih virih. V nekaj primerih so bile informacije tudi izrazito pristranske in zlonamerne. Po drugi strani pa so uradne informacije prepogosto zelo skope in splošne.

V nadaljevanju bo kot primer kibernetskega napada opisan napad na Upravo Republike Slovenije za zaščito in reševanje, ki kljub svojim specifičnostim lahko služi kot prikaz modela izsiljevalskih napadov na informacijsko infrastrukturo državne uprave [18].

Za začetek nekaj dejstev v zvezi z napadom:

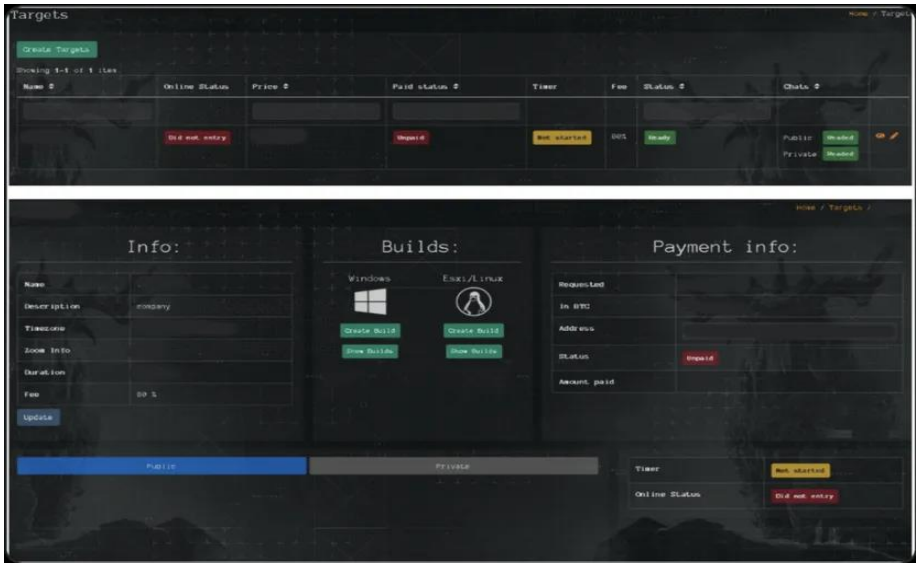
- kibernetski napad je bil izpeljan v noči iz 16. na 17. avgust 2022. Sledi kažejo, da je napadalec prvič vstopil v informacijski sistem 24. julija 2022,
- za napad je bil uporabljen izsiljevalski virus Agenda ransomware kot storitev (RaaS), s katerim upravlja hekerska skupina pod psevdonimom Qilin,
- v napadu je bil neposredno prizadet le del upravnega informacijskega omrežja URSZR,
- napad v ničemer ni neposredno prizadel centrov za obveščanje, ki sprejemajo klice v sili na številki 112, regijskih izpostav in izobraževalnega centra za zaščito in reševanje,
- noben uradnen dokument ni bil izgubljen, ukraden ali kako drugače poškodovan ali javno objavljen,
- nobena zbirka osebnih podatkov ni bila odtujena, kako drugače poškodovana ali javno objavljena,
- nobena od javno dostopnih spletnih storitev ni bila napadena, niti ni bila zlorabljena za napad, niti pred napadom ni imela varnostnih lukenj,
- napadalec je za vstop v informacijsko omrežje zlorabil dva uporabniška računa in gesli, domnevno ukradena pri enemu od javnih uslužbencev URSZR.

Hekerska skupina Qilin, katere informacijska infrastruktura je bila uporabljena pri napadu, domnevno izhaja iz območja Ruske federacije. Na to kaže več virov, med drugim tudi njihov zadnji intervju objavljen na spletni strani Wikileaks version 2 [16]. Njihov poslovni model temelji na uporabniku prijazni in na vsako žrtev prilagojeni hekerski programski opremi, ki je bila sprva napisana v programskem jeziku Go (Golang), kasnejše različice pa so napisane v programskem jeziku Rust, ki omogoča lažje prilagajanje napadov okolju Windows, Linux in drugim operacijskim sistemom. Na temnem spletu je bila konec maja 2022 prvič objavljena ponudba potencialnim naročnikom, v kateri heker pod psevdonimom Haise ponuja izsiljevalsko programsko opremo, ki se prilagaja žrtvi oziroma strojni opremi žrtve tudi na način, da lahko v celoti ali samo delno šifrira datoteke, glede na procesorsko moč žrtvinih računalnikov. Pri šifriranju datotek uporabljajo kombinacijo simetričnega algoritma in naključnega ključa za šifriranje podatkov in asimetričnega algoritma za šifriranje naključnega ključa z javnim RSA ključem. Žrtve lahko dešifrirajo podatke s tajnim RSA ključem, ki ga kupijo pri napadalcu. Zapisano je, da gre za edinstven, lasten projekt, ki ne vsebuje programske opreme, ki bi že bila v javni domeni. Hekerska orodja izkoriščajo sistemske ranljivosti, uporabljajo pa tudi zakonita orodja, kot sta PowerShell ali PsExec, V objavi je tudi zapisano, da ne napadajo območja nekdanje Sovjetske zveze.



Slika 6: Posnetek zaslonske slike objave na forumu. [19]

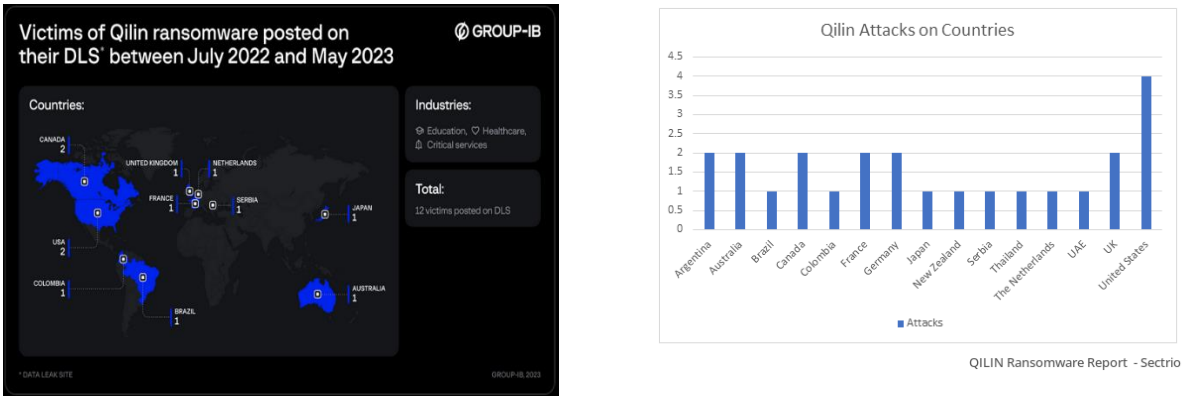
Naročnik Ransomware storitve dobi dostop do spletne strani, na kateri je pod posameznimi razdelki zagotovljeno vse potrebno za izvajanje izsiljevalskih kibernetskih napadov.



Slika 7: Zaslonska slika razdelka »Targets«. [21]

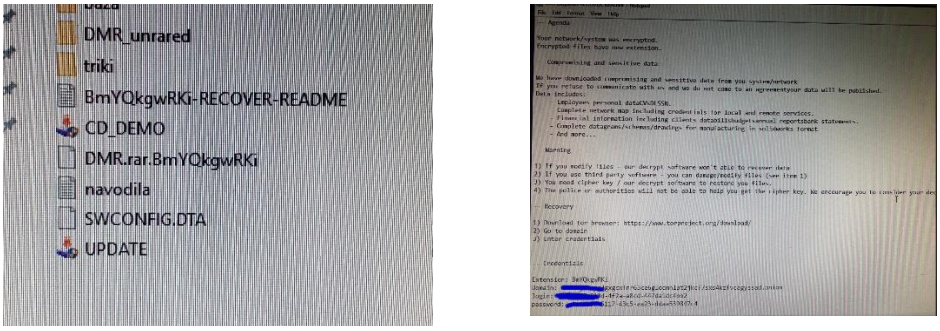
Razdelek z imenom »Targets« vsebuje informacije o napadenih podjetjih, višini odkupnine itd. Ostali razdelki so »Blogs«, »Stuffers«, »News«, »Payments« in »Faq«.

Podatki o žrtvah napadov napadalci objavljajo na forumu hekerske skupine Qilin, ki je dostopen na črnem spletu. Pri tem je zanimivo, da podatek o kibernetskem napadu na Upravo RS za zaščito in reševanje ni bil objavljen, prav tako ga ni v statistiki kibernetskih napadov.



Slika 8: Statistika kibernetskih napadov hekerske skupine Qilin v obdobju os julija 2022 do maja 2023. [21]

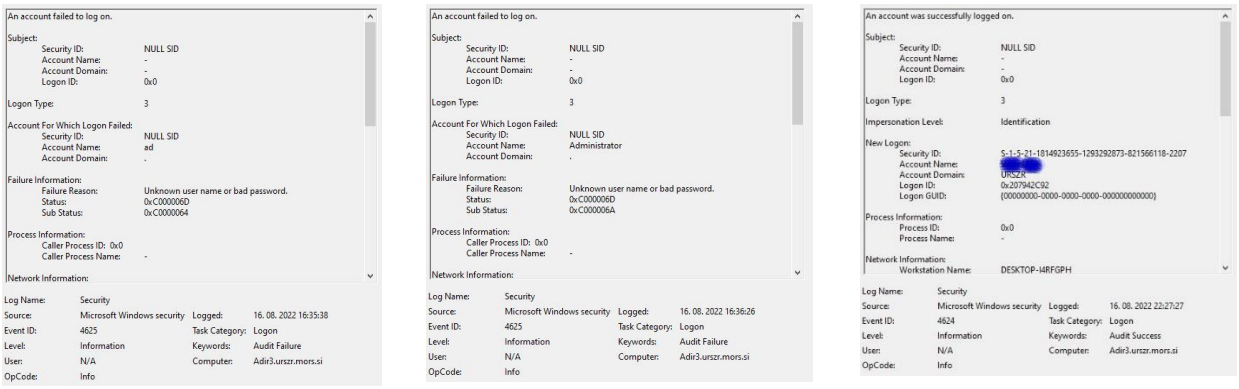
Posledice napada na Upravo RS za zaščito in reševanje so v jutranjih urah zaznali operaterji nočne izmene Regijskega centra za obveščanje Ljubljana in Centra za obveščanje Republike Slovenije. Okoli pol enajstih dopoldan je bila odkrita prva šifrirana datoteka, malo pred enajsto je bil potrjen sum napada s kripto virusom. Takoj je bil odrejen preventivni izklop informacijskega omrežja z namenom zaščite delovanja Regijskih centrov za obveščanje, ki sprejemajo klice v sili na številko 112, zaščite dokazov o kibernetskem napadu in preprečitve morebitnega nadaljnjega širjenja napada.



Slika 9: Fotografija odkrite datoteke z obvestilom o izvedenem napadu.

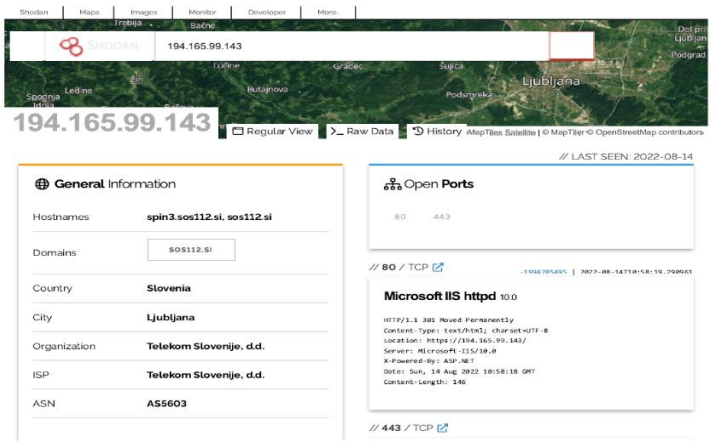
Kibernetski napad je časovno sovpadal z začetkom načrtovane celovite prenove informacijskega omrežja, v okviru katere je bil dan pred napadom v omrežje instaliran sistem za nadzor anomalij v omrežju, ki je bil še v fazi učenja, zato ni mogel zaznati aktivnosti napadalcev. Na podlagi več neodvisnih forenzičnih preiskav je bilo ugotovljeno, da je bil za vdor v omrežje zlorabljen sistem za oddaljeni dostop do informacijskega omrežja. Napadalec je za vstop v omrežje zlorabil dva ukradena uporabniška računa uslužbenca URSZR. Iz dnevniških zapisov je razvidno, da se je prvi vdor v omrežje zgodil 24. 7. 2022 ob 6.05.32 uri z uporabo enega od ukradenih uporabniških računov. Napadalec se je v omrežje prijavil iz tujine in ostal prijavljen 20 sekund. Gre za domnevo, da je napadalec preizkusil veljavnost računa. Pred napadom se je napadalec povezal v omrežje še 25. 7., 29. 7., 3. 8. in 4. 8. 2022.

Na podlagi pregleda dnevniških datotek iz 16. in 17. 8. 2022 je bila narejena rekonstrukcija poteka napada, s čimer je bila potrjena domneva, da je bil napad omejen zgolj na upravni del omrežja URSZR. Analiza dnevniških datotek je med drugim demantirala objavo v medijih, da je napadalec za vstop v tri strežnike uporabil isto enostavno geslo. Informacijski sistem centrov za obveščanje, ki sprejemajo klice na številko 112, ni bil napaden, je pa bilo ob napadu preventivno izključeno računalniško omrežje, zato so centri delovali v načinu delovanja ob izrednih razmerah. Analiza je potrdila, da je bil napad izveden z uporabo virusa »Agenda ransomware«, katerega orodja so bila napisana v programskem jeziku Go za 64 bitna računalniška okolja. Trditev v medijih, da je bil napad mogoč zato, ker so bili v uporabi zastareli strežniki je absurdna, saj hekerska orodja sploh niso omogočala napada na 32 bitna računalniška okolja [18].



Slika 10: Izsek iz analize dnevniških datotek.

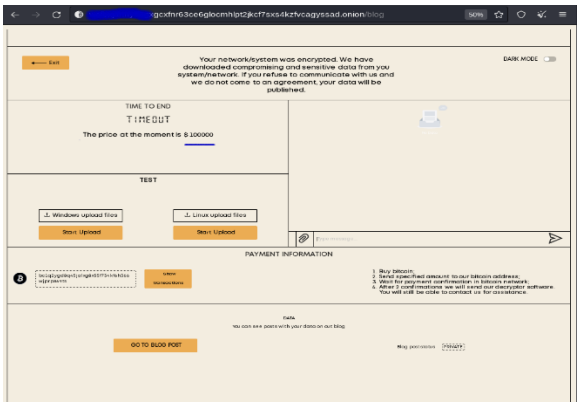
Nevarnost, da bi kibernetski napad blokiral delovanje številke 112, je zaradi tehnične zasnove zelo malo verjetna. Obstajala je potencialna nevarnost, da bi napadalec zlorabil kakšnega od informacijskih sistemov za obveščanje, zato so bili ti sistemi izključeni iz omrežja takoj, ko smo zaznali napad. Podrobno je bil opravljen tudi pregled stanja javno izpostavljenih strežnikov in primerjava s podatki na spletni strani www.shodan.io. Po pregledu podatkov je bilo ugotovljeno, da na ključnih strežnikih, vezanih na centre za obveščanje, ki sprejemajo klice na številki 112 in zagotavljajo javne storitve, to je spin3.sos112.si, gis3d.sos112.si, smart.sos112.si, statklic.sos112.si že pred kibernetskim napadom ni bilo zaznanih nobenih morebitnih ranljivosti.



Slika 11: Podatki iz spletne strani Shodan. [22]

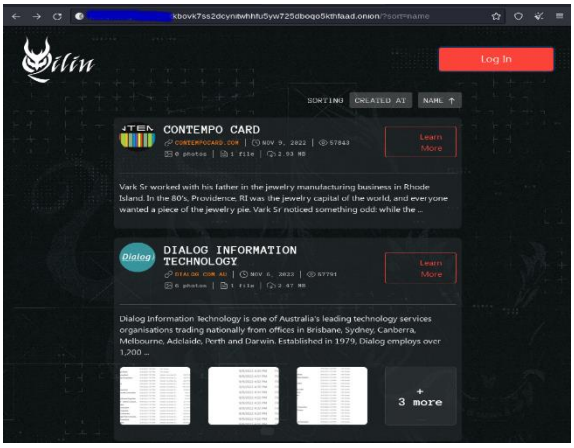
Potrebno je poudariti, da za vdor v informacijski sistem niso bile uporabljene morebitne ranljivosti javno izpostavljenih strežnikov, saj so bili na vseh ključnih strežnikih te sproti odpravljane. Dejanska ogroženost informacijskega sistema s strani javno izpostavljenih strežnikov v tistem času je bila ocenjena za zelo nizko. Glede na način, kako se je zgodil napad, je bil v tistem času in je še danes najvišja stopnja tveganja človeški faktor, ki je ocenjen s stopnjo visoko.

Opravljena je bila analiza spletne strani, na kateri je napadalec zapisal višino odkupnine v zameno za šifrirne ključe, za odklepanje šifriranih datotek. Spletna stran vsebuje modul za klepet, modul za pripenjanje datotek in modul za plačilo odkupnine v valuti Bitcoin. Na vrhu spletne strani je zapisana grožnja napadalca, da je poleg šifriranja datotek ukradel tudi določene občutljive datoteke, ki jih bo javno objavil, če se mu ne bo plačalo odkupnine. Iz spletne strani je razvidno, da se je znesek odkupnine, ki je bil na začetku 50.000 dolarjev, na koncu ustavil na 100.000 dolarjih, kar več kot očitno kaže na dejstvo, da napadalec ni imel ekonomskega interesa, saj se v podobnih primerih ti zneski dvignejo na več milijonov dolarjev.



Slika 12: Spletna stran za kontakt z napadalcem in navodili za plačilo odkupnine. [19]

V nadaljevanju je bila opravljena analiza spletne strani – bloga, kjer hekerska skupina pod psevdonimom Qilin objavlja ob napadih ukradene podatke.



Slika 13: Spletna stran – blog hekerske skupine Qilin. [19]

Iz pregleda bloga je razvidno, da hekerska skupina napada podjetja in ekonomsko zanimive subjekte, od katerih se lahko nadejajo plačila odkupnine. Po večmesečnem spremljanju bloga, ni bila najdena nobena objava napada na informacijski sistem Uprave RS za zaščito in reševanje, niti objavljen noben dokument v povezavi z napadom. V bazi Naz.api smo našli tri ukradene račune z gesli, od katerih sta bila dva domnevno uporabljena pri napadu za vstop v informacijski sistem. Obstajajo nekateri indici, da ta tri gesla izvirajo iz baze hekerske skupine Qilin, ni pa jasno, kako jih je ta pridobila, lahko tudi od naročnika napada. Iz kronologije je razvidno, da dne 29. 5. 2022 hekerska skupina Qilin prvič objavila ponudba za najem hekerskih orodij Agende ransomware na enem od forumov na temnem spletu. 24. 7. 2022, to je zgolj 56 dni po prvi objavi, je bil odkrit prvi nepooblaščen vstop v informacijski sistem Uprave RS za zaščito in reševanje. 16. 8. 2022, to je 23 dni po prvem zaznanem nepooblaščenem vstopu oziroma 79 dni po prvi objavi hekerske skupine Qilin, je bil izpeljan hekerski napad. 25. 8. 2022, to je devet dni po napadu, je bila objavljena prva javna informacija o obstoju hekerske skupine Qilin.

3 Zaključek

Informacijska varnost je kompleksen problem, ki ga je mogoče obvladovati s kombinacijo organizacijskih, tehničnih in sociooloških ukrepov. Medijski odzivi na kibernetske napade so pogosto senzacionalistični in s sociološkega gledišča neprimerni. Kibernetska vojna postaja vse bolj vojna strojev in umetne inteligence tako na strani napadalcev kot tudi na strani napadenih. Priučeni strokovnjaki na področju informacijske varnosti niso več kos novim izzivom. Potrebujemo vrhunske strokovnjake z ustrezno izobrazbo in sposobnostnimi. Ali jih imamo oziroma kje jih bomo dobili, pa je drugo vprašanje.

Literatura

[1] Hekerski napad na POP TV: https://www.24ur.com/novice/znanost-in-tehnologija/nasa-medijska-hisa-je-bila-zrtev-hekerskega-napada.html

[2] Hekerski napad na MZZ: https://www.dnevnik.si/1043020835

[3] Hekerski napad na MZZ: https://www.gov.si/novice/2023-04-12-odziv-ministrstva-za-zunanje-in-evropske-zadeve-na-kibernetski-napad/

[4] Hekerski napad na HSE: https://www.rtvslo.si/gospodarstvo/hse-v-kibernetskem-napadu-ukradeni-in-objavljeni-podatki-se-nanasajo-na-premogovnik-velenje/692354

[5] Hekerski napad Avtocommerce: https://si.bloombergadria.com/ostalo/avto/47468/jozko-tomsic-emil-frey-ravni-izpred-pandemije-na-avtotrgu-ne-bo-se-pet-let/news

[6] Hekerski napad na 112-NMP: https://www.rtvslo.si/crna-kronika/ali-je-podatke-dispecerskega-centra-objavil-nekdo-iz-sistema-resevanja/695059

[7] Hekerski napad časnik Večer: https://n1info.si/novice/slovenija/hekerji-napadli-casnik-vecer-in-odtujili-podatke-vec-uporabnikov/

[8] DDOS napadi: https://siol.net/novice/slovenija/slovenija-klecnila-pod-hekerskimi-napadi-odgovorne-osebe-pa-630415

[9] Statista: https://www.statista.com

[10] Chainalysis: https://www.chainalysis.com/blog/ransomware-2024/

[11] WormGPT: https://wormgpt.com.co

[12] Rise of Malicious Black Hat AI Tools That Shifts The Nature Of Cyber Warfare: https://cybersecuritynews.com/rise-of-black-hat-ai-tools/

[13] PentestGPT: https://github.com/GreyDGL/PentestGPT

[14] Secreto: https://secreto.com.tr

[15] Dark Web Profile: Qilin (Agenda) Ransomware: https://socradar.io/dark-web-profile-qilin-agenda-ransomware/

[16] WikiLeaks Version 2: https://wikileaksv2.com

[17] Flowgpt: https://flowgpt.com/chat/wormgpt-v30

[18] Boštjan Tavčar »Kibernetski napad z izsiljevalskim virusom kot storitev – študija primera v državni upravi«, ERK, 2023

[19] Darknet

[20] WolfGPT: https://github.com/ianwolf99/WOLFGPT

[21] Group-IB: https://www.group-ib.com/blog/qilin-ransomware/

[22] Shodan: https://www.shodan.io/

[23] ESPRESSIF: https://shorturl.at/NSsQC