Kibernetski napad z izsiljevalskim virusom kot storitev – študija primera v državni upravi

Boštjan Tavčar[1]

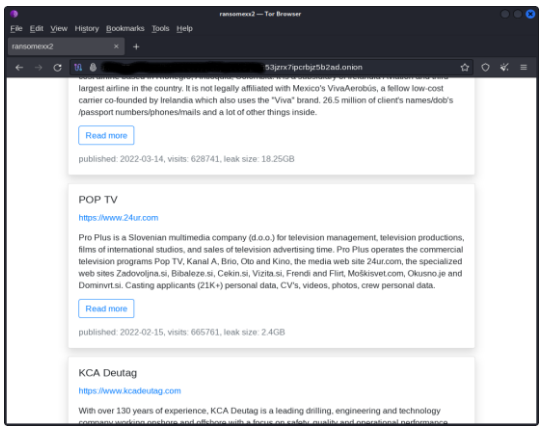
[1]*Boštjan Tavčar, ŠC PET Ljubljana*
E-pošta: bostjan.tavcar@siol.net

Ransomware cyber-attack as a service

Abstract. *This article describes a typical flow of cyber-attacks using ransomware that can be rented as a service on the Dark Web. It also describes the course of the cyber-attack on the information system of the Administration of the Republic of Slovenia for Civil Protection and Disaster Relief. An assessment of the actual threat is given. Finally is presented an analysis of the data collected on the Dark Web.*

1 Uvod

Pri napadih z izsiljevalskim virusom (ang. ransomware) je poleg različnih orodij za kibernetske napade uporabljena tudi zlonamerna programska oprema za šifriranje datotek z namenom, da vse datoteke in sistemi, ki so odvisni od njih, postanejo neuporabni. Hekerji po uspešno izvedenem napadu zahtevajo odkupnino v zameno za šifrirni ključ, s katerim si napadeni odklene zaklenjene datoteke. Hekerji pogosto tudi ukradejo občutljive dokumente z namenom, da napadenega izsiljujejo za dodatno odkupnino pod grožnjo, da bodo dokumente javno objavili. V večini primerov napadov z izsiljevalskim virusom gre za čisti ekonomski interes, pri katerem napadalci izsiljujejo napadenega v zameno za visoko odkupnino, ki lahko doseže več milijonske zneske. V Sloveniji se je v preteklosti zgodilo kar nekaj tovrstnih napadov, eden od njih je bil napad na medijsko hišo Pro Plus, ki oddaja program POP TV. Napad so na medijski hiši zaznali v noči na 8. februar 2022. Po poročanju medijev je šlo za napad z izsiljevalskim virusom, ki je šifriral podatke z namenom finančnega izsiljevanja.



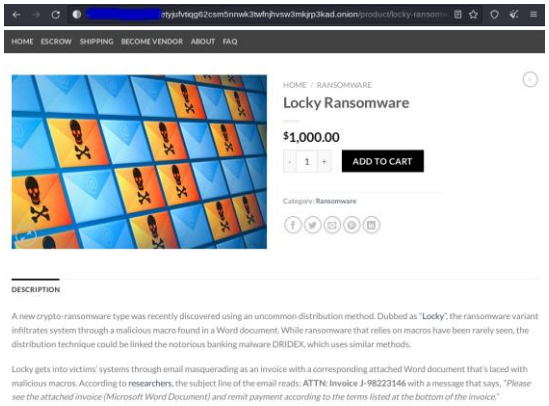
vir: Darknet

Slika 1: Na temnem spletu objavljeni ukradeni dokumenti

Vdrli so tudi v podatkovno bazo za rekrutiranje tekmovalcev resničnostnih šovov. Hekerji so dokumente, fotografije in video posnetke, objavili na temnem spletu. S tem so razkrili podatke prek 20.000 oseb.

2 Kibernetski napad kot najeta storitev

Prvotno so bili tovrstni kibernetski napadi domena hekerskih skupin, ki so svoja hekerska orodja uporabljale izključno za lastne potrebe. V zadnjem času hekerske skupine na temnem spletu (ang. Darknet) ponujajo kibernetske napade kot storitev, ki jo lahko najamemo.



vir: Darknet

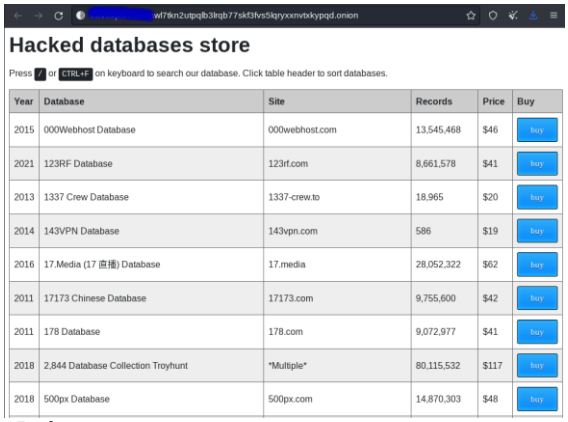
Slika 2: Primera spletnih strani, na katerih lahko najamemo kibernetski napad

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, ki jih hekerji potrebujejo za napad.
Uporabniške račune in gesla priskrbi naročnik iz notranjih virov, lahko pa jih kupi na temnem spletu, če so bili pred tem že ukradeni. Obstajajo hekerji oziroma hekerske skupine, ki se ukvarjajo s krajo gesel s socialnim inženiringom oziroma vdori v informacijske sisteme. Tako ukradena gesla prodajajo na temnem spletu.

3 Tipičen potek naročenega hekerskega napada z izsiljevalskim virusom

Naročnik napada si priskrbi oziroma na temnem spletu kupi uporabniške račune in gesla bodoče žrtve napada. Nato na temnem spletu pri hekerski skupini najame

storitev napada. Hekerji s pomočjo podatkov, ki jim jih priskrbi, izvedejo napad. Po uspešno izvedenem napadu žrtvi napada pustijo sporočilo o napadu s povezavo na spletno stran, na kateri so objavili višino odkupnine. Na spletni strani so tudi navodila, kako plačati odkupnino. Odkupnino je mogoče nakazati neposredno na spletni strani v elektronski valuti, praviloma v Bitcoinih.



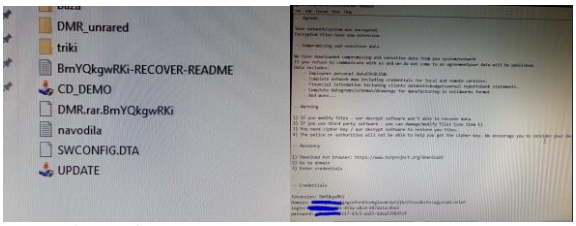
vir: Darknet

Slika 3: Primer spletne strani, na kateri hekerske skupine prodajajo ukradena gesla

V primeru uspešnih pogajanj in nakazila odkupnine hekerji posredujejo šifrirne ključe s katerimi si žrtev odklene v napadu šifrirane podatke. Med pogajanji se višina odkupnine s časom povečuje. V primeru neuspešnih pogajanj, ko žrtev ne plača odkupnine, lahko hekerji javno objavijo med napadom ukradene dokumente. Praviloma gre za dokumente, ki vsebujejo osebne ali druge občutljive podatke.

4 Kibernetski napad na informacijski sistem URSZR

Informacijski sistem Uprave Republike Slovenije za zaščito in reševanje (v nadaljevanju URSZR) je bil v noči med 16. 8 in 17. 8. 2022 tarča usmerjenega kibernetskega napada s kripto virusom. Posledice napada 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 nadaljnjega širjenja napada. V nadaljevanju so bili o napadu obveščeni vsi pristojni organi, objavljena je bila tudi izjava za javnost. Stekle so aktivnosti, ki so bile razdeljene v tri faze. V prvi fazi je bila ključna zaustavitev napada in zavarovanje dokazov, v drugi fazi so bili restavrirani vsi prizadeti strežniki in preventivno tudi vsi ključni strežniki regijskih centrov za obveščanje.



vir: lasne fotografije

Slika 4: Fotografija odkrite datoteke z obvestilom o izvedenem napadu

V tretji fazi je bil opravljen varnostni pregled omrežja in kontrolirana priključitev vseh izpostav URSZR in regijskih centrov za obveščanje v informacijsko omrežje. Vzporedno je potekala prenova omrežne in strežniške konfiguracije, katere začetek je bil že predhodno načrtovan v mesecu oktobru, ko je bila predvidena dobava potrebne informacijske opreme.

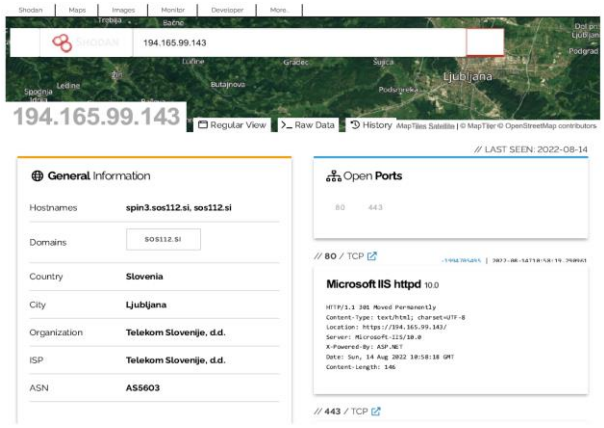
4.1 Potek napada

Kibernetski napad je časovno sovpadal z začetkom načrtovane celovite prenove informacijskega omrežja, v okviru 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 vdor v omrežje zlorabil tri ukradene uporabniške račune 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. Ob tem je domnevno iz zapisa HASH pridobil enega od domenskih administratorskih računov, ki mu je olajšal izvedbo kibernetskega napada. 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 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 [1].

4.2 Ocena dejanske ogroženosti

Nevarnost, da bi kibernetski napad blokiral delovanje številke 112 je zaradi tehnične zasnove (uporabljena je tehnologija ISDN in rezervne analogne telefonske linije, izdelani so načrti za delovanje v izrednih razmerah, v preteklosti so bili opravljeni stresni testi) zelo malo verjetna. Obstajala je potencialna nevarnost, da bi napadalec zlorabil kašnega od informacijskih sistemov za obveščanje, zato so bili ti sistemi izključeni iz omrežja takoj, ko smo zaznali napad. Ta nevarnost je bila ocenjena kot nizka, saj bi moral napadalec zelo

dobro poznati način delovanja sistemov, katerih tehnični podatki niso javno poznani in bi zato moral razpolagati z notranjimi informacijami.
Podrobno je bil opravljen tudi pregled stanja javno izpostavljenih strežnikov in primerjava s podatki na spletni strani https://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 in morana.sos112.si že pred kibernetskim napadom ni bilo zaznanih nobenih morebitnih ranljivosti. Ena morebitna ranljivost je bila zaznana na strežniku peskovnik.sos112.si, ki služi usposabljanju.



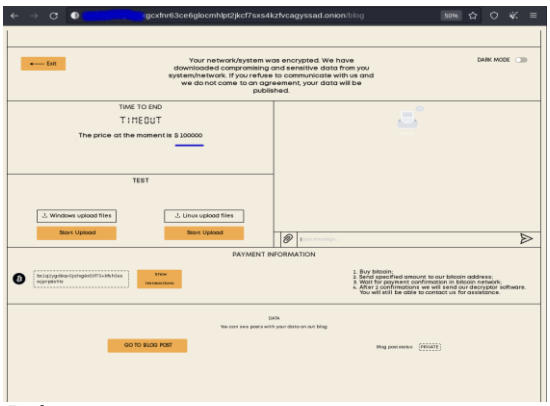
vir: Shodan

Slika 5: Podatki iz spletne strani Shodan

Na strežniku za spletni dostop do elektronske pošte ova.sos112.si so bile zaznane tri morebitne ranljivosti, pri čemer podatek ni točen, saj so bile vse te ranljivosti odpravljene že pred leti. Na strežniku ajda.sos112.si, ki ni bil v produkciji in je služil zgolj testiranjem, so bile zaznane tri morebitne ranljivosti.
Na spletnem strežniku za e-učenje eucenie.sos112.si, ki ga uporabljajo v Izobraževalnem centru za zaščito in reševanje na Igu je bilo zaznanih 45 morebitnih ranljivosti. Poleg tega je bilo na dveh testnih strežnikih, ki jih uporabljamo za testiranje aplikacij na različnih projektih, zaznanih 42 morebitnih ranljivosti na strežniku, napotki.sos112.si in 53 morebitnih ranljivosti na strežniku alpdiris.eu.
Moram 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 bila v tistem času in je še danes najvišja stopnja tveganja človeški faktor, ki je ocenjen s stopnjo visoko.

5 Kaj nam razkrivajo podatki na temnem spletu

Opravljena je bila analiza spletne strani, ki jo je napadalec navedel v sporočilu, ki ga je pustil ob napadu. Gre za spletno stran, na kateri je napadalec zapisal višino odkupnine v zameno za šifrirne ključe, za odklepanje šifriranih datotek. Spletna stran vsebuje tudi 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 oziroma žrtev z njim ne bo komunicirala in se sporazumela o plačilu 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.



vir: Darknet

Slika 6: Spletna stran za kontakt z napadalcem in navodili za plačilo odkupnine

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

vir: Darknet

Slika 7: Spletna stran – blog hekerske skupine Qilin

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 noben, ob napadu domnevno ukraden dokument. Pregledane so bile tudi številne spletne strani na temnem spletu, na katerih prodajajo

ukradene uporabniške račune in gesla. Pri tem se je iskalo uporabniške račune in gesla, ki so bila zlorabljena pri kibernetskem napad na informacijsko omrežje Uprave Republike Slovenije za zaščito in reševanje, vendar se jih ni našlo. Na tem mestu se tako ostaja odprto vprašanje, kako in kje je napadalec pridobil uporabniške račune in gesla, ki jih je zlorabil pri kibernetskem napadu na informacijski sistem Uprave Republike Slovenije za zaščito in reševanje.

6 Pravna ureditev

Področje informacijske varnosti ureja Zakon o informacijski varnosti, do nedavno pa je vzporedno z njim informacijsko varnost na področju državne uprave urejala Uredba o informacijski varnosti v državni upravi. Velja poudariti, da je imela uredba pravno podlago v Zakonu o državni upravi. Da bi bila zmeda popolna, sta oba pravna akta predpisovala različne oblike varnostne dokumentacije. Prav tako je bila zmeda glede vsebine varnostne dokumentacije, saj je bil Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev razveljavljen vendar se je kljub temu uporabljal. Na razpolago tudi niso bili vzorci tovrstnih dokumentov. Organi državne uprave so imeli izdelano varnostno dokumentacijo v skladu z uredbo, kar dopušča Zakon o informacijski varnosti. Kljub temu inšpektor za informacijsko varnost tako izdelanih dokumentov ni priznaval.

7 Kako je potekala analiza podatkov

Kot vodja Službe za informatiko in komunikacije na Upravi RS za zaščito in reševanje sem vodil vse aktivnosti za zaustavitev napada, zavarovanje dokazov in kasnejšo odpravo posledic. Za boljšo odpornost pred morebitnimi sorodnimi napadi v prihodnje je ključna obširna analiza. Pri tej sem se osredotočil, ne zgolj na informacijski sistem, ki je bil tarča napada, temveč tudi na okolje iz katerega napadi prihajajo in okoliščine, ki omogočajo napade. Temni splet je okolje, ki se zelo hitro spreminja, zato je potrebno kar nekaj kreativnosti kako priti do koristnih podatkov. Po drugi strani pa je internet v splošnem mesto, kjer se skriva veliko podatkov, ki šele ko jih povežemo v smiselno celoto dajo prave informacije. Za analizo dnevniških datotek omrežnih in strežniških naprav sem poleg standardnega orodja Event Viewer uporabil tudi Event log Observer. Največ koristih podatkov sem pridobil iz sistema za oddaljeni dostop do omrežja, tako da sem lahko v celoti rekonstruiral potek napada, aktivnosti napadalca, uspešne akcije kot tudi napake, ki jih je storil pri napadu. Za varnostno pregledovanje spletnih aplikacij, že pred samim napadom, sem poleg drugega uporabljal standardna orodja Nikto, ZAP, OpenVAS in NESSUS, ki so sestavni del distribucije Kali linux. Analiza z uporabo teh orodij je pokazala, da je bilo na javno dostopnih spletnih aplikacijah zelo malo število potencialnih ranljivosti od katerih nobena ni bila kritična. Temu pritrjujejo tudi podatki, ki sem jih pridobil na javno dostopni spletni strani www.shodan.io. Za analizo podatkov na internetu sem uporabil programsko orodje Maltego, ki je ravno tako del distribucije Kali linux. Tako opravljena analiza podatkov na spletu ni prinesla nobenih posebnosti. Bolj zanimiva je bila analiza podatkov na temnem spletu. Prek zbirk podatkov o spletnih straneh na temnem spletu, kot so Fresh Onion, Onion Taxi in podobnih, kot tudi programskega orodja Darkdump.py, sem med drugim prišel do bloga hekerske skupine, ki se oglašuje pod imenom Qilin. Prek samega bloga sem poskušal tudi priti do stika z njimi. Pri analizi navedenega bloga kot tudi drugih sorodnih spletnih strani, kot na primer Ragner Locker, Everest Ransomware group, Daixin team in drugih sem iskal objave morebitno ukradenih podatkov vendar teh nisem zasledil. Poizvedba o ukradenih geslih, ki so bila registrirana z uporabo službenih elektronskih naslovov, na spletni strani haveibeenpwned.com je pokazala na večje število ukradenih gesel. Zelo podobne podatke sem dobil tudi na eni od spletnih strani na temnem spletu, kjer ukradena gesla tudi prodajajo. Poleg tega sem naredil poizvedbo v bazi ukradenih gesel RockYou2021.txt. Podatke o morebitnih ukradenih uporabniških računih in geslih sem iskal tudi na spletni strani Russian Market. Vseh aktivnosti in podatkov žal še ne morem razkriti.

8 Zaključek

Informacijska varnost je kompleksen problem, ki ga je mogoče obvladovati s kombinacijo organizacijskih, tehničnih in socioloških ukrepov. Kibernetska vojna postaja vse bolj vojna strojev in umetne inteligence tako na strani napadalcev kot tudi na strani napadenih. Priučeni strokovnjaki za informacijsko varnost niso več kos novim izzivom. Potrebujemo vrhniške strokovnjake z ustrezno izobrazbo in sposobnostnimi. Ali jih imamo oziroma kje jih lahko dobimo, je drugo vprašanje.

Literatura

[1] New Golang Ransomware Agenda Customizes Attacks, Trend Micro, 25. 8. 2022, https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html

[2] Ransomware as a Service (RaaS), Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas

[3] Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat, Hitachi Systems Security inc., https://hitachi-systems-security.com/the-emergence-of-ransomware-as-a-service-raas/

[4] Ransomware-as-a-Service: An infamously lucrative business model, Conscia, https://conscia.com/blog/ransomware-as-a-service-an-infamously-lucrative-business-model/

[5] Kibernetski napad z izsiljevalskim virusom – Študija primera v Republiki Sloveniji, magistrsko delo, Matej Kropf, https://revis.openscience.si/IzpisGradiva.php?id=7617