KIBERNETSKI NAPAD NA UPRAVO REPUBLIKE SLOVENIJE ZA ZAŠČITO IN REŠEVANJE

Boštjan Tavčar[1]

Povzetek

V članku je prestavljen značilen potek hekerskih napadov z uporabo izsiljevalskih virusov, ki se jih lahko kot storitev najame na temnem spletu. Opisani so tudi potek kibernetskega napada na informacijski sistem Uprave Republike Slovenije za zaščito in reševanje (URSZR), ukrepanje ob napadu in po njem ter odprava posledic napada. Predstavljena je ocena dejanske ogroženosti. Na koncu je analiza podatkov, pridobljenih na temnem spletu.

CYBERATTACK ON THE ADMINISTRATION OF THE REPUBLIC OF SLOVENIA FOR CIVIL PROTECTION AND DISASTER RELIEF

Abstract

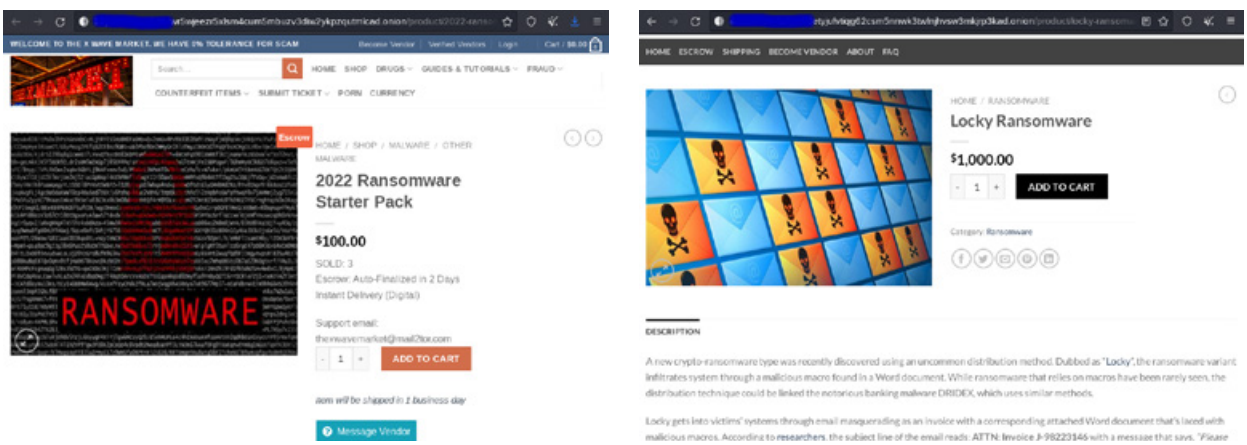
This article describes a typical flow of cyberattacks using ransomware, which can be rented as a service on the Dark Web. It also describes the course of a cyberattack on the information system of the Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, the actions taken during and after the attack, and the elimination of the consequences of the attack. An assessment of the actual threat is given. Finally, an analysis of the data collected on the Dark Web is presented.

[1] Ministrstvo za obrambo, Uprava RS za zaščito in reševanje, Vojkova cesta 61, Ljubljana, *bostjan.tavcar@urszr.si*

UVOD

Uprava RS za zaščito in reševanje je bila v noči med 16. in 17. avgustom 2022 tarča usmerjenega kibernetskega napada z izsiljevalskim virusom. V napadu so bili prizadeti trije strežniki, primarni sistem za izdelavo varnostnih kopij in eden izmed domenskih strežnikov, vsi v upravnem delu informacijskega omrežja. V drugih delih informacijskega omrežja ni bilo zaznati nobenih dejavnosti napadalca. Ob napadu ni bil uničen ali kako drugače prizadet noben uradni dokument, prav tako ni znakov, ki bi kazali na to, da je bil kateri izmed dokumentov ali osebnih podatkov odtujen. Napadalcu ni uspelo vdreti v informacijski sistem centrov za obveščanje ter druge dislocirane enote Uprave RS za zaščito in reševanje. Prav tako napadalcu ni uspelo vdreti v nobenega izmed javno dostopnih strežnikov in službenih računalnikov.

Za napad je bil zlorabljen zasebni računalnik uslužbenca Uprave RS za zaščito in reševanje, prek katerega je napadalcu uspelo vstopiti v upravni del omrežja. Gre za vrsto napada, ki ga je le s tehničnimi ukrepi skoraj nemogoče preprečiti. V napadu prizadete strežnike



Slika 1: Primera spletnih strani, na katerih lahko najamemo kibernetski napad (vir: temni splet)
Figure 1: *Examples of websites on which we can hire a cyberattack (Source: Darknet)*

smo ponovno vzpostavili v petih dneh. Kibernetski napad je časovno sovpadal z začetkom načrtovane celovite prenove informacijskega omrežja, v okviru katere smo dan pred napadom v omrežje namestili sistem za nadzor nepravilnosti v omrežju, ki pa še ni mogel zaznati dejavnosti napadalcev. Po napadu smo načrtovano prenovo omrežja prilagodili takratnemu stanju in zahtevam koordinacijske skupine na področju informacijskih in komunikacijskih sistemov Ministrstva za obrambo. Med drugim smo takoj začeli prenovo glavnih strežnikov centrov za obveščanje in segmentacijo omrežja, kar je uporabnikom povzročilo nekaj težav. Incident je bil uradno končan 19. septembra 2022, in sicer po tem, ko so bila opravljena vsa varnostna preverjanja, ki so trajala od 29. avgusta do 19. septembra.

Poznejše preiskave incidenta so pokazale, da je šlo za usmerjen kibernetski napad z izsiljevalskim virusom Agenda ransomware. Na podlagi pridobljenih znakov in podobnih primerov napadov lahko z veliko gotovostjo sklepamo, da je bil napad naročen na temnem spletu pri ponudniku, ki se na spletu oglašuje s psevdonimom Qilin.

KIBERNETSKI NAPAD Z IZSILJEVALSKIM VIRUSOM

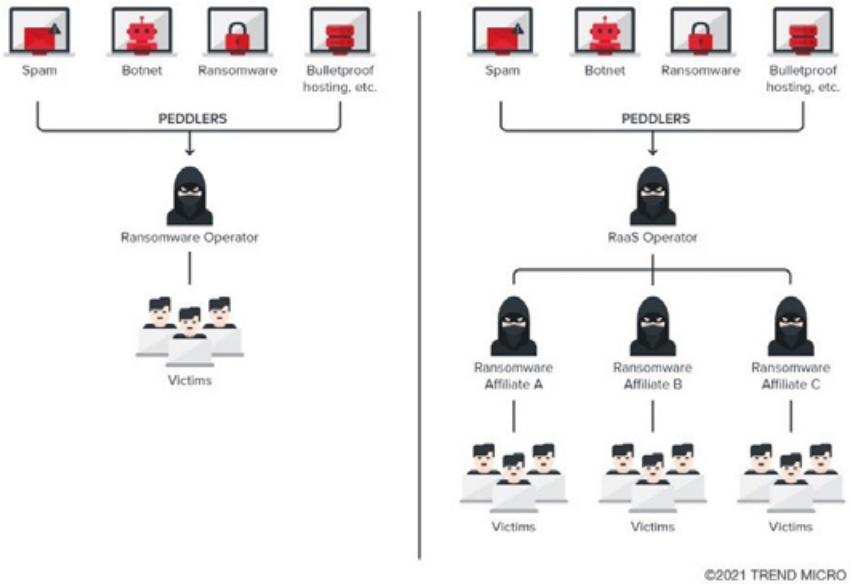
Pri napadih z izsiljevalskim virusom (ang. *ransomware*) je poleg orodij za kibernetske napade uporabljena tudi zlonamerna programska oprema za šifriranje datotek, da datoteke in sistemi, ki so odvisni od njih, postanejo neuporabni. Hekerji po uspešnem napadu zahtevajo odkupnino v zameno za šifrirni ključ, s katerim si napadeni lahko odklene zaklenjene datoteke. Hekerji pogosto tudi ukradejo občutljive dokumente, da napadenega izsiljujejo za dodatno odkupnino ob grožnji, da bodo dokumente javno objavili. V večini primerov napadov z izsiljevalskim virusom gre za gospodarski interes, pri katerem napadalci izsiljujejo napadenega v zameno za visoko odkupnino, ki lahko doseže večmilijonske zneske. V Sloveniji se je v preteklosti zgodilo kar nekaj takih napadov, eden izmed njih je bil napad na medijsko hišo PRO PLUS, ki oddaja program POP TV. Napad so v medijski hiši zaznali v noči na 8. februar 2022. Po poročanju medijev je šlo za napad z izsiljevalskim virusom, ki je šifriral podatke za finančno izsiljevanje. Vdrli so tudi v podatkovno bazo za pridobivanje tekmovalcev resničnostnih šovov. Hekerji so dokumente, ki vsebujejo podatke ljudi, fotografije in pri nekaterih tudi video posnetke, objavili na temnem spletu. Tako so razkrili podatke več kot 20.000 ljudi.

Kibernetski napad, storitev, ki jo lahko najamemo

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

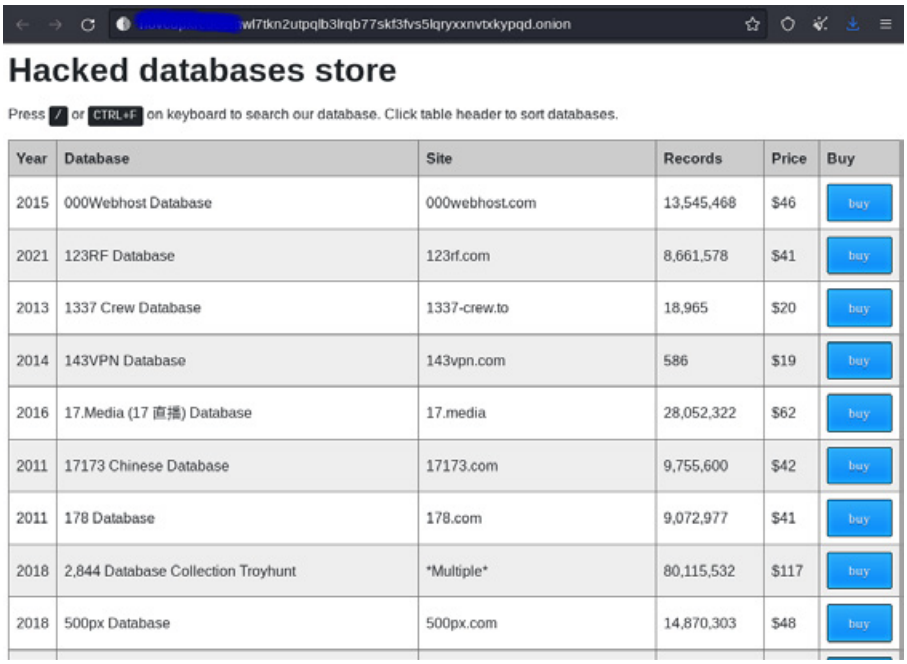
Hekerska skupina je v takem primeru le izvajalec storitve v imenu in interesu naročnika, ki mora priskrbeti potrebne podatke za napad, med katerimi so bistveni podatki o uporabniških računih in geslih, ki jih hekerji potrebujejo za napad.

Uporabniške račune in gesla tako priskrbi naročnik iz notranjih virov, lahko pa jih kupi na temnem spletu, če



Slika 2: Slikovni prikaz razlike med klasičnim kibernetskim napadom in kibernetskim napadom kot storitvijo (vir: Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat)

Figure 2: *A visual representation of the difference between a classic cyberattack and a cyberattack as a service (Source: Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat)*



Hacked databases store

Press / or CTRL+F on keyboard to search our database. Click table header to sort databases.

Year	Database	Site	Records	Price	Buy
2015	000Webhost Database	000webhost.com	13,545,468	$46	buy
2021	123RF Database	123rf.com	8,661,578	$41	buy
2013	1337 Crew Database	1337-crew.to	18,965	$20	buy
2014	143VPN Database	143vpn.com	586	$19	buy
2016	17.Media (17 直播) Database	17.media	28,052,322	$62	buy
2011	17173 Chinese Database	17173.com	9,755,600	$42	buy
2011	178 Database	178.com	9,072,977	$41	buy
2018	2,844 Database Collection Troyhunt	*Multiple*	80,115,532	$117	buy
2018	500px Database	500px.com	14,870,303	$48	buy

Slika 3: Primer spletne strani, na kateri hekerske skupine prodajajo ukradena gesla (vir: temni splet)

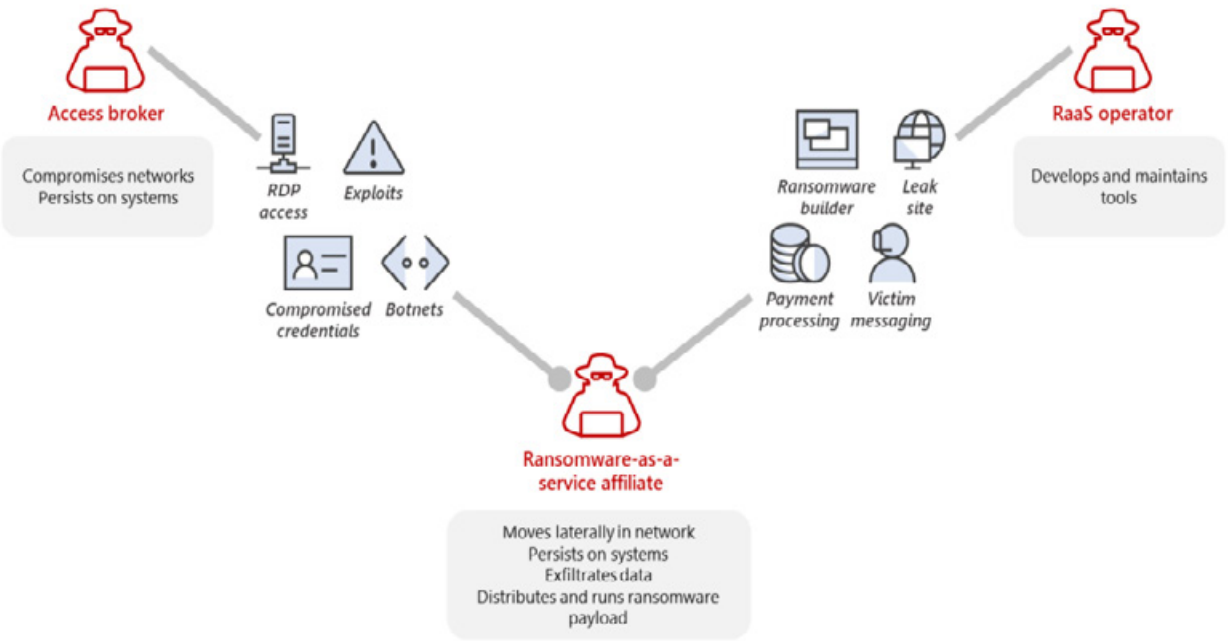
Figure 3: *An example of a website where hacking groups sell stolen passwords (Source: Darknet)*

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. Ukradena gesla prodajajo na temnem spletu.

Pri značilnem hekerskem napadu kot storitvi imamo naročnika napada s svojim interesom. Navadno gre za gospodarski interes. Naročnik od hekerja ali hekerske skupine odkupi ukradene uporabniške račune in gesla žrtve bodočega napada ter najame hekerja ali hekersko skupino, ki izvede napad po naročilu naročnika.

Značilen 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,



Slika 4: Slikovni prikaz sodelovanja akterjev pri kibernetskem napadu kot storitvi (vir: Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat)

Figure 4: *A pictorial representation of actor cooperation in a cyberattack as a service (Source: Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat)*

ki jim jih priskrbi, izvedejo napad. Po uspešnem 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, navadno v bitcoinih. Po uspešnih pogajanjih in nakazilu odkupnine hekerji posredujejo šifrirne ključe, s katerimi si žrtev lahko odklene šifrirane podatke. Med pogajanji se višina odkupnine sčasoma povečuje. Pri neuspešnih pogajanjih, ko žrtev ne plača odkupnine, navadno hekerji tudi javno objavijo med napadom ukradene dokumente. Navadno gre za dokumente, ki vsebujejo osebne ali druge občutljive podatke.

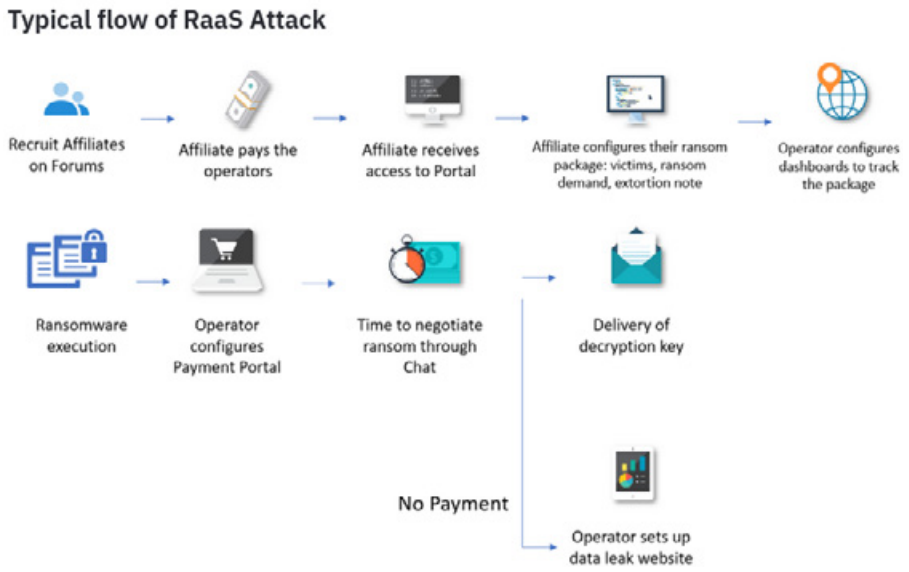
KIBERNETSKI NAPAD NA INFORMACIJSKI SISTEM URSZR

Informacijski sistem Uprave RS za zaščito in reševanje je bil v noči s 16. na 17. avgust 2022 tarča usmerjenega kibernetskega napada s kriptovirusom. Posledice napada so v jutranjih urah zaznali operaterji nočne izmene Regijskega centra za obveščanje Ljubljana in Centra za obveščanje Republike Slovenije. Okoli 10.30 je bila odkrita prva šifrirana datoteka, malo pred 11. uro pa je bil potrjen sum napada s kriptovirusom.

Takoj je bil odrejen preventiven izklop informacijskega omrežja zaradi zaščite delovanja regijskih centrov za obveščanje, ki sprejemajo klice v sili na telefonsko številko 112, zaščite dokazov o kibernetskem napadu in preprečitve nadaljnjega širjenja napada. O napadu so bili obveščeni pristojni organi, objavljena pa je bila tudi izjava za javnost. Začele so se dejavnosti, ki so bile razdeljene na tri faze. V prvi fazi sta bila najpomembnejša ustavitev napada in zavarovanje dokazov, v drugi fazi pa smo ponovno vzpostavili prizadete strežnike ter preventivno tudi najpomembnejše strežnike. V tretji fazi smo opravili varnostni pregled omrežja in kontrolirano priključitev izpostav URSZR ter regijskih centrov za obveščanje. Hkrati je potekala prenova omrežne in strežniške konfiguracije, katere začetek je bil že predhodno načrtovan za oktober, ko je bila predvidena dobava nujne informacijske opreme.

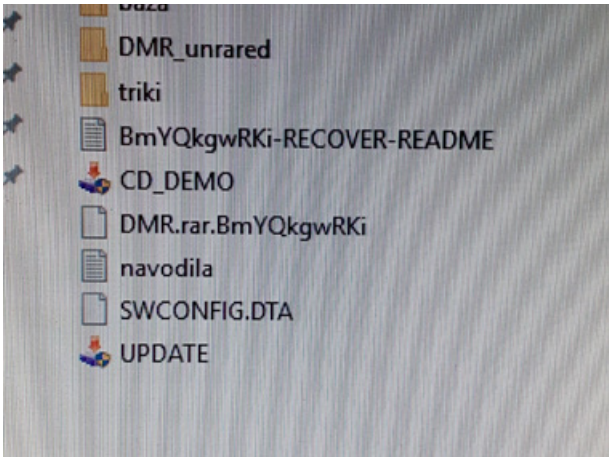
Potek napada

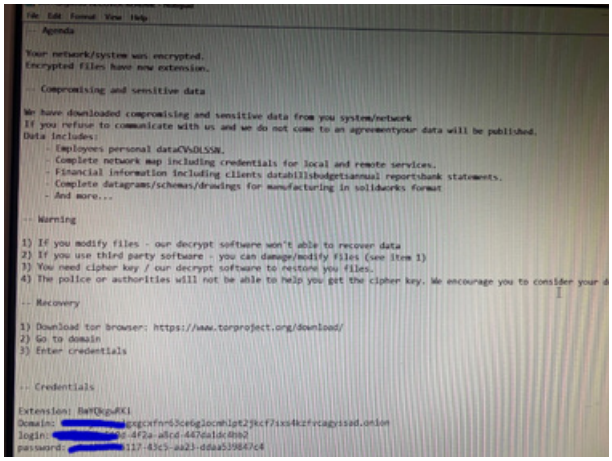
Kibernetski napad je časovno sovpadal z začetkom načrtovane celovite prenove informacijskega omrežja, v okviru katere smo dan pred napadom v omrežje namestili sistem za nadzor nepravilnosti v omrežju, ki je bil še v fazi učenja, zato ni mogel zaznati dejavnosti napadalcev. Na podlagi več neodvisnih forenzičnih 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. julija 2022 ob 6:05:32 z uporabo enega izmed ukradenih uporabniških računov. Prijava je bila opravljena iz tujine, trajala pa je 20 sekund. Gre za domnevo, da je napadalec preizkusil veljavnost računa. Pred napadom se je napadalec povezal v omrežje še 25. in 29. julija ter 3. in 4. avgusta 2022. Ob tem je domnevno iz zapisa HASH pridobil enega izmed domenskih administratorskih računov, ki mu je omogočil izvedbo kibernetskega napada. Po pregledu dnevniških datotek iz 16. in 17. avgusta 2022 smo rekonstruirali potek napada, s čimer smo potrdili



Slika 5: Značilen potek kibernetskega napada kot storitve (vir: Ransomware-as-a-Service: An infamously lucrative business model)

Figure 5: *A typical flow of a cyberattack as a service (Source: Ransomware-as-a-Service: An infamously lucrative business model)*





Slika 6: Fotografija odkrite datoteke z obvestilom o izvedenem napadu (vir: B. Tavčar)
Figure 6: *A photo of the detected file with a notice of the attack carried out (Source: B. Tavčar)*

svoje domneve, da je bil napad omejen le na upravni del omrežja URSZR. Pri analizi podatkov na strežniku SharePoint je bila zaznana uporaba programa SystemBC, ki deluje kot omrežni posrednik za prikrito komunikacijo in orodje za oddaljeno upravljanje. Med analizo je bilo potrjeno, da je bil napad izveden z uporabo virusa Agenda ransomware, katerega orodja so bila napisana v programskem jeziku Go za 64-bitna računalniška okolja (New Golang Ransomware Agenda Customizes Attacks).

Odprava posledic napada

Datoteke z datotečnega strežnika smo restavrirali do vključno 4. avgusta 2022, torej do datuma, ko je bilo zaznati prve spremembe v sistemu. Podatkov s poštnega strežnika nismo restavrirali, saj za izdelavo varnostnih kopij podatkov takrat nismo imeli dovolj zmogljivosti v diskovnem sistemu, nakup nove opreme pa je zamujal. Prav tako še nismo restavrirali strežnika SharePoint, na katerem podatkovna baza ni bila prizadeta, saj na strežniku ni bilo pomembnih podatkov. Njegova restavracija je bila predvidena v drugi fazi. Marca 2022 so uslužbenci URSZR dobili uradno pismo z navodili o obveznem izdelovanju varnostnih kopij dokumentov in elektronske pošte na svoje osebne računalnike. Uslužbenci, ki so se dosledno držali tega navodila, niso izgubili nobenih podatkov z datotečnega in poštnega strežnika, če pa je prišlo do izgube podatkov, je bila ta zelo majhna.

V začetku oktobra 2022 smo načrtovali celovito prenovo omrežja in strežniškega okolja, zato smo v sanacijo posledic kibernetskega napada vključili tudi načrtovano prenovo, kar je delno podaljšalo čas sanacije. Pri namestitvi posameznih aplikacij smo imeli pomoč zunanjih strokovnjakov. Posvetovali smo se tudi s strokovnjaki na Ministrstvu za obrambo. Na novo smo namestili vse strežnike, za kar smo uporabili zadnje različice razpoložljivih operacijskih sistemov in aplikacij ter spremenili zasnovo njihovih konfiguracij v skladu z zadnjimi standardi varnostne politike. V skladu s priporočili stroke smo ločili omrežje na dve ravni, in sicer infrastrukturno (virtualizacija, upravljanje fizičnih strežnikov in omrežnih naprav ter izdelava varnostnih kopij) in produkcijsko (strežniki, delovne postaje ter drugo). Spremenili smo uporabniške politike od triravninskih administratorskih računov do novih politik glede gesel. Na novo smo konfigurirali informacijsko omrežje, da smo povečali informacijsko varnost, pri čemer pa še ne gre za končno konfiguracijo. Pristojna služba Ministrstva za obrambo je opravila varnostno skeniranje celotnega omrežja pred njegovo ponovno vzpostavitvijo. Iz omrežja smo odstranili morebitne varnostno vprašljive delovne postaje in drugo opremo. Izdali smo dopis oziroma obvezno navodilo glede pravilne uporabe gesel s prepovedjo uporabe podatkovnih medijev USB in osnovnimi informacijami glede informacijske varnosti. Obiskali smo izpostave URSZR in na srečanjih z zaposlenimi pojasnili okoliščine kibernetskega napada, takratne zaostrene razmere in ukrepe, ki jih morajo zaposleni izvesti za boljšo informacijsko varnost tako v zasebnem življenju kot službi.

Ocena dejanske ogroženosti

Nevarnost, da bi kibernetski napad blokiral delovanje telefonske številke 112, je zaradi tehnične zasnove zelo malo verjetna, saj uporabljamo tehnologijo ISDN in rezervne analogne telefonske linije, pripravljene

imamo načrte za delovanje v izrednih razmerah in v preteklosti so bili opravljeni stresni testi. Obstajala je morebitna nevarnost, da bi napadalec zlorabil kakšnega izmed informacijskih sistemov za obveščanje, zato so bili ti sistemi izključeni iz omrežja takoj, ko smo zaznali napad. To nevarnost ocenjujemo kot majhno, saj bi moral napadalec zelo dobro poznati način delovanja teh sistemov, katerih tehnični podatki niso javno znani, zato bi moral imeti notranje informacije.

Natančno smo tudi pregledali stanje javno izpostavljenih strežnikov. Po pregledu podatkov na spletni strani *https://www.shodan.io* ugotavljamo, da na glavnih strežnikih, vezanih na centre za obveščanje, ki sprejemajo klice na telefonski številki 112 in zagotavljajo javne storitve, to so spin3.sos112.si, gis3d.sos112.si, smart.sos112.si in morana.sos112.si, že pred kibernetskim napadom ni bilo zaznanih nobenih morebitnih ranljivosti. Morebitna ranljivost je bila zaznana na strežniku peskovnik.sos112.si, ki se uporablja za usposabljanje. Na strežniku za spletni dostop do elektronske pošte ova.sos112.si so bile zaznane tri morebitne ranljivosti, pri čemer pa moramo poudariti, da podatek ni točen, saj so bile te ranljivosti pred leti že odpravljene. Na strežniku ajda.sos112.si, ki ni bil v produkciji in se je uporabljal le za preizkušanje, so bile zaznane tri morebitne ranljivosti.

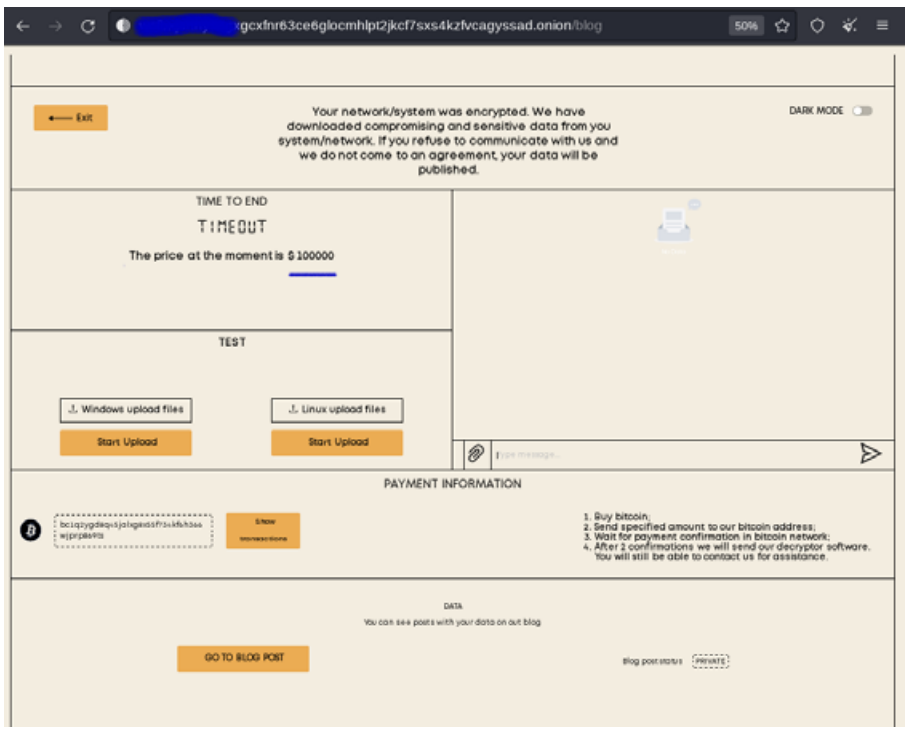
Na spletnem strežniku za e-učenje eucenie.sos112.si, ki ga uporabljajo v Izobraževalnem centru za zaščito in reševanje na Igu, smo zaznali 45 morebitnih ranljivosti. Poleg tega je bilo na dveh testnih strežnikih, ki jih uporabljamo za preizkušanje aplikacij pri različnih projektih, zaznanih 42 morebitnih ranljivosti na strežniku napotki.sos112.si in 53 morebitnih ranljivosti na strežniku alpdiris.eu.

Za vdor v informacijski sistem niso bile uporabljene morebitne ranljivosti, navedene v analizi spletne strani Shodan, saj smo na glavnih strežnikih te sproti odpravljali. Dejansko ogroženost informacijskega sistema s strani javno izpostavljenih strežnikov v tistem času ocenjujemo za zelo nizko.

Glede na način, kako se je zgodil napad, je bilo v tistem času in je še danes največje tveganje človeški faktor.

Kaj nam razkrivajo podatki na temnem spletu?

Na temnem spletu smo analizirali spletno stran, ki jo je napadalec navedel v sporočilu, ki ga je pustil ob napadu. Gre za spletno stran, na kateri je napadalec navedel višino odkupnine v zameno za šifrirne ključe, s katerimi bi lahko odklenili datoteke, ki nam jih je šifriral. Spletna stran vsebuje tudi modul za klepet, modul za pripenjanje datotek in modul za plačilo odkupnine v bitcoinih. Na vrhu spletne strani je zapisana grožnja napadalca, da je poleg šifriranja datotek ukradel tudi nekatere občutljive datoteke, ki jih bo javno objavil, če mu ne plačamo oziroma z njim ne bomo komunicirali in se sporazumeli.



Slika 7: Spletna stran za stik z napadalcem in navodili za plačilo odkupnine (vir: temni splet)

Figure 7: Website for contacting the attacker and instructions for paying the ransom (Source: Darknet)

Slika 8: Spletna stran oziroma blog hekerske skupine Qilin (vir: temni splet)

Figure 8: *Website – Qilin hacker group blog (Source: Darknet)*

Slika 9: Spletna stran, na kateri prodajajo tri gesla, registrirana prek enega izmed službenih elektronskih naslovov URSZR (vir: temni splet)

Figure 9: *A website where they are selling three passwords registered through one of the Administration for Civil Protection and Disaster Relief's official email addresses (Source: Darknet)*

S 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 gospodarskega interesa, saj se v podobnih primerih ti zneski povečajo na več milijonov dolarjev.

V nadaljevanju smo analizirali spletno stran oziroma blog, na katerem hekerska skupina pod psevdonimom Qilin objavlja ob napadih ukradene podatke. Iz pregleda bloga je razvidno, da hekerska skupina napada podjetja in gospodarsko zanimive subjekte, od katerih lahko pričakuje plačila odkupnine. Na blogu, ki smo ga pregledovali več mesecev, nismo našli objave napada na informacijski sistem Uprave RS za zaščito in reševanje ter nobenega dokumenta, ki bi bil ukraden ob napadu.

Pregledali smo tudi številne spletne strani na temnem spletu, na katerih prodajajo ukradene uporabniške račune in gesla. Našli smo več ukradenih zasebnih uporabniških računov in gesel uslužbencev URSZR, ki so jih uslužbenci registrirali z uporabo službenih poštnih naslovov. Na sliki 9 je razvidno, da so bili ukradeni trije zasebni uporabniški računi in gesla, vsi registrirani na enem izmed službenih elektronskih računov Uprave RS za zaščito in reševanje.

S primerjavo zapisov ukradenih gesel HASH z zapisi gesel HASH, ki so jih uslužbenci uporabljali za službene namene, smo ugotovili, da so nekateri uslužbenci za zasebne namene uporabljali enaka gesla, kot jih uporabljajo za službene namene, kar je zaskrbljujoče.

Na temnem spletu smo iskali tudi uporabniške račune in gesla, ki so bili zlorabljeni pri kibernetskem napadu na informacijsko omrežje URSZR, vendar jih nismo našli. Tako se postavlja vprašanje, kako in kje je napadalec pridobil uporabniške račune ter gesla, ki jih je zlorabil pri kibernetskem napadu na informacijski sistem Uprave RS za zaščito in reševanje.

Viri in 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,* 4. 6. 2023.
2. Ransomware as a Service (RaaS), Trend Micro. *https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas,* 4. 6. 2023.
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. 6. 2023.
4. Ransomware-as-a-Service: An infamously lucrative business model, Conscia. *https://conscia.com/blog/ransomware-as-a-service-an-infamously-lucrative-business-model/,* 4. 6. 2023.