USAID
OD AMERIČKOG NARODA

BOSNA I HERCEGOVINA PROJEKAT ASISTENCIJE ENERGETSKOM SEKTORU

IZVJEŠTAJ O ANALIZI NAPADA NA INFORMACIONI SISTEM SARAJEVOGASA

JANUAR 2023. GODINE
Ova publikacija je napravljena za pregled od strane Američke agencije za međunarodni razvoj. Pripremljeno od strane DT Global.

BOSNA I HERCEGOVINA PROJEKAT ASISTENCIJE ENERGETSKOM SEKTORU

IZVJEŠTAJ O ANALIZI NAPADA NA INFORMACIONI SISTEM SARAJEVOGASA

JANUAR 2023. GODINE

Ugovor broj:
72016819C00002

Pripremljeno za:
USAID BiH Ured za ekonomski razvoj Bosne i Hercegovine

Pripremio:
DT Global

SADRŽAJ

1 UVOD

KJKP „Sarajevogas“ d.o.o. Sarajevo pretrpio je napad na svoj informacioni sistem. Kao posljedica napada, usluge informacionog sistema nisu bile dostupne. Funkcionisanje sistema ponovo je uspostavljeno akcijama IT uposlenika.

USAID Projekat asistencije energetskom sektoru pripremio je analizu događaja na temelju dostupnih podataka. Analiza ima za cilj da se pouke iz ovog slučaja podijele sa učesnicima u energetskom sektoru.

Dana 31.10.2022. godine održan je sastanak u prostorijama Sarajevogasa između predstavnika Sarajevogasa, predstavnika USAID-a i predstavnika USAID Projekta asistencije energetskom sektoru. Na tom sastanku prikupljene su osnovne informacije o napadu i dogovoren naredni detaljni sastanak. Drugi sastanak održan je 16.11.2022. godine u prostorijama Sarajevogasa. Tokom sastanka su uposlenici IT službe Sarajevogasa iznijeli dodatne tehničke detalje o napadu. Tom prilikom je omogućen uvid u kopije datoteka koje su bile izmijenjene tokom napada. Na osnovu informacija prikupljenih tokom ova dva sastanka i uvida u kopije datoteka, te korištenjem stručnih znanja i dostupnih informacija o sličnim napadima sačinjena je analiza događaja.

Ovaj dokument ima za cilj analizirati konkretan napad ali i navesti na potencijalne nedostatke u sistemu informacione zaštite u energetskom sektoru, uz poseban osvrt na potrebu koordiniranog i sistemskog pristupa u poboljšanju sigurnosti informacionih sistema u sektoru energetike u BiH.

USAID Projekat asistencije energetskom sektoru ranije je napravio izvještaj o koracima potrebnim za ostvarivanje sigurnosti mrežnih i informacionih sistema u energetskom sektoru u BiH, kao i smjernice za transponovanje NIS direktive u skladu sa propisima cyber sigurnosti regulative Energetske zajednice i Europske Unije. Hitna implementacija ovih mjera i smjernica je od velike važnosti za kvalitetnu i sveobuhvatnu zaštitu informacionih sistema organizacija koje djeluju u energetskom sektoru u BiH.

2 IT STRUKTURA SARAJEVOGAS-A

Kantonalno javno komunalno preduzeće “Sarajevogas” d.o.o. Sarajevo bavi se distribucijom i trgovinom gasom putem distribucijske mreže. Osim toga, preduzeće se bavi projektovanjem, izgradnjom i održavanjem distributivnih gasnih mreža i priključaka. Kompanija opslužuje cca 65.000 aktivnih kupaca prirodnog gasa koji su podijeljeni u sljedeće kategorije: domaćinstava, mala privreda, velika privreda, KJKP “Toplane-Sarajevo” d.o.o. Sarajevo i Poseban kupac (“Sarajevo-gas” a.d. Istočno Sarajevo) za kojeg kompanija samo transportuje gas. Sarajevogas održava i upravlja sa cca 1.128 km niskotlačne distributivne gasne mreže sa pripadajućim servisnim priključcima.

IT infrastruktura Sarajevogasa sastoji se od mrežne opreme i veza, servera, korisničkih računara i dodatne opreme. Pojedini serveri u Sarajevogasu nisu odvojeni fizički računari. Umjesto toga koristi se virtualizacija. Virtualizacija omogućava da se na jednom fizičkom računaru (hardveru) istovremeno pokrene više (virtualnih) operativnih sistema. Svaki od ovih operativnih sistema ponaša se kao da je instaliran na svom vlastitom hardveru. Ovi operativni sistemi nazivaju se virtualne mašine. Ovakav način instalacije operativnih sistema i korištenja hardvera je vrlo efikasan i fleksibilan. Iz ovog razloga većina servera u savremenim okruženjima su pokrenuti kao virtualne mašine. Sarajevogas je u sklopu

modernizacije svog IT sistema prešao u potpunosti na virtualne servere. To im je olakšalo upravljanje serverima i smanjilo troškove. Činjenica su serveri Sarajevogasa dio virtualizacijske platforme je bitna za opis napada, jer je napad izvršen upravo na ovu platformu. Iz tog razloga dat je opis rada ove platforme u nastavku.

Softver koji omogućava virtualizaciju naziva se hipervizor. To je poseban softver koji se instalira direktno na hardver i stvara virtualni sloj između hardvera i operativnog sistema. On je namijenjen za upravljanje i upotrebu virtualnih mašina. Postoji više prozvođača softvera za virtualizaciju. Sarajevo gas koristi softver proizvođača VMware. To je proizvođač koji ima najveći dio tržišta virtualizacije. Hipervizor kompanije VMware koji koristi Sarajevogas naziva se ESXi. Radi lakšeg upravljanja većim brojem virtualnih mašina VMware ima dodatni softver koji se naziva vCenter Server. To je softver za upravljanje serverima. On omogućava automatizaciju uspostavljanja virtualnih mašina i olakšava upravljanje njima. Komplet softvera hipervizora, ESXi i softvera za upravljanje virtualnim mašinama, vCenter Server, čini virtualizacijsku platformu. Naziv VMware virtualizacijske platforme je vSphere.

Da bi se neka virtualna mašina, odnosno server sa njegovim operativnim sistemima, instaliranim aplikacijama i podacima pokrenuo, ESXi hipervizor učitava njenu konfiguraciju iz datoteka koje predstavljaju virtuelnu mašinu koju treba pokrenuti. U tim datotekama su pohranjene sve postavke operativnih sistema i virtualnog hardvera, kao i svi podaci koji se nalaze na trajnoj memoriji koju operativni sistem koristi pri svom radu. Ti podaci uključuju i instalirane aplikacije. Uobičajeno je da se sve datoteke za jednu virtualnu mašinu pohranjuju u jedan folder. Svaka virtualna mašina ima svoj folder sa datotekama. Datoteke virtualnih mašina se na VMware virtualizacijskoj platformi vSphere pohranjuju na poseban datotečni sistem VMFS (*Virtual Machine File System*). VMFS je datotečni sistem prilagođen pohranjivanju datoteka koje predstavljaju virtualne mašine. Datotečni sistem je način pohranjivanja datoteka na disk. VMFS je različit od datotečnih sistema koje savremeni operativni sistemi uglavnom koriste, NTFS (Windows) i ext4 (Linux).

Neispravnost datoteka koje predstavljaju virtualne mašine dovodi do nemogućnosti pokretanja virtualnih mašina. To se očituje kao nedostupnost servera sa svim njihovim uslugama.

3 OPIS NAPADA

Dana 31.08.2022. godine uposlenici Sarajevogasa koji su korisnici informacionog sistema primjetili su da informacioni sistem ne radi. Niti jedna od usluga nije bila dostupna. Ispravan rad svih poslovnih procesa koji se oslanjaju na informacioni sistem bio je onemogućen. [1]

Uposlenici IT službe pokušali su provjeriti stanje servera. Nije im bilo moguće pristupiti serverima preko računarske mreže. Niti jedan od servera sa kojim su pokušali uspostaviti vezu nije bio dostupan. Umjesto očekivane forme za unos pristupnih podataka za administraciju servera dobivali su poruke o nedostupnosti servera. Izvršen je neposredan uvid u stanje virtualizacijske platforme. Ustanovljen je razlog nedostupnosti servera. Sve datoteke koje predstavljaju virtualne mašine, servere sa kojim su se pokušali povezati, bile su izmijenjene. Zbog ovih izmjena ESXi hipervizor nije mogao pokrenuti virtualne mašine. Nemogućnost pokretanja virtualnih mašina onemogućila je pokretanje servera sa svim uslugama informacionog sistema koje oni pružaju. Pored ovoga, rezervne kopije (backup) podataka Sarajevogasa koje je pravio Veem softver bile su obrisane.

Ovakav način napada i onemogućavanja rada informacionog sistema nije nešto što se obično dešava prilikom napada. Obično se napad izvodi na usluge dostupne vanjskim i unutrašnjim korisnicima. Te usluge se, u Sarajevogasu i u većini organizacija u energetskom sektoru, pružaju kroz virtualne servere. Uspješan klasični napad utiče samo na podatke na uspješno napadnutom serveru. Napadač dođe do podataka kojim ne bi smio imati pristup, izmjeni podatke koje ne bi smio mijenjati ili podatke učini nedostupnim ovlaštenim korisnicima. Takav napad pogađa jedan server ili računar. Moguće je da se napad proširi na druge servere ili računare, ali za to je potrebno da napadač zaobilazi odbrane svakog novog računara koji napada.

Analizirani napad u Sarajevogasu izvršen je na virtualizacijsku platformu. To je relativno novi oblik napada. Takav napad je vrlo poguban jer onemogućavanje rada virtualizacijske platforme onemogućava rad svih (virtualnih) servera koji su pokrenuti na toj platformi. Napadač odjednom može zaustaviti kompletan rad informacione infrastrukture organizacije. To je upravo ono što se desilo.

3.1. RANSOMWARE

Napad spada u kategoriju koja se naziva *ransomware*. To je napad u kojem napadač šifrira datoteke na napadnutom računaru/serveru. Kada je datoteka šifrirana njen originalni sadržaj je izmijenjen i postao je nečitak. Da bi se sadržaj vratio u izvorno stanje, potrebno je uraditi dešifriranje. Nakon dešifriranja sadržaj datoteke je vraćen u izvorno stanje i datoteka se može normalno koristiti. Za dešifriranje datoteka napadač traži novčanu naknadu.

Šifriranje i dešifriranje su matematičke transformacije sa dodatnim parametrom koji se naziva ključ. Kada se neki sadržaj šifrira to se radi uz izbor nekog ključa. Ključ je niz bita. Da bi se sadržaj mogao dešifrirati potrebno je imati odgovarajući ključ. Ono što sprečava dešifriranje je nepoznavanje ključa. To je i jedan od razloga za naziv ključ jer „zaključava/otključava“ sadržaj.

Sadržaj šifriranih datoteka, kod *ransomware* napada, postaje nedostupan žrtvi napada. Nedostupnost sadržaja znači različite stvari za različite vrste datoteka. Za datoteke sa podacima, poput teksta (npr. Word) ili tabela (npr. Excel), to znači da podaci iz datoteka postaju nečitki i ne mogu se prikazati u svom originalnom obliku. Za datoteke sa programima ili konfiguracijama nedostupnost sadržaja znači

[1] Tokom razgovora sa Sarajevogasom nisu navedene usluge koje njihov informacioni sistem pruža. Iz tog razloga nije moguće navesti konkretne poslovne procese. S obzirom na stepen informatizacije može se pretpostaviti da su to minimalno svi administrativni i finansijski procesi.

da se programi koje su originalne datoteke predstavljale ili konfigurisane ne mogu biti pokrenuti. Ukratko, šifrirane datoteke postaju neupotrebljive za svoju originalnu namjenu. Napadači obično ostave obavještenje u kojem kažu da su šifrirali datoteke i upute korisnika kako da napadačima izvrši uplatu radi povrata podataka. Nakon uplate bi žrtva trebala od napadača dobiti ključ za dešifriranje. Naziv *ransomware* dolazi od ove ucjene i zahtjeva za otkupninom (eng. *ransom*) da bi se povratilo oteto, u ovom slučaju podaci.

3.2. IZMJENJENA EKSTENZIJA FAJLOVA

U slučaju napada na Sarajevogas virtualnu infrastrukturu, u svakom od foldera sa datotekama virtualnih mašina sve datoteke sa ekstenzijama (slova iza tačke u imenu) .vmx (konfiguracija VM), .vmxf (dodatna konfiguracija VM),.vmdk (virtualni disk), .log (zapisi), .vmsd (podaci o sačuvanim stanjima VM), .vswp (*swap* datoteka VM) i .hlog (zapisi vCenter) su bile šifrirane i dobile su dodatnu ekstenziju ._d0nut. Tako je, na primjer, originalna VM konfiguracijska datoteka „Eracun.vmx“ šifrirana i postala „Eracun.vmx._d0nut“. Naziv ekstenzije nema nikakvo tehničko značenje. To je proizvoljno izabran niz znakova od strane autora softvera čijom upotrebom se izvodi *ransomware* napad. Naziv ekstenzije uglavnom je različit za svaki konkretan *ransomware* napad. Napadi i dobivaju nazive po ekstenzijama koje koriste. Kao posljedica šifriranja ovih datoteka virtualnih mašina nije bilo moguće pokrenuti te virtualne mašine. To znači da serveri, koji su bili pokretni kao virtualne mašine, i usluge koji oni pružaju nisu bili dostupni korisnicima. Ukratko, informacioni sistem nije uopšte radio.

Jedine datoteke koje nisu bile šifrirane su datoteke sa .nvram ekstenzijom (BIOS ili EFI konfiguracija VM). Njihovo šifriranje nije bilo neophodno za postizanje cilja napadača, a to je bilo onemogućavanje pokretanja virtuelnih mašina.

3.3. PORUKA NAPADAČA

U svakom od foldera pojavila se identična datoteka READ.MD s objašnjenjem na koji način Sarajevogas može povratiti svoje podatke. Tekst iz datoteke glasi (na engleskom):

/
So what happened?

All files are encrypted with Integrated Encryption Scheme.
The file structure was not damaged. You have been assigned a unique identifier.
After infection, you have 96 hours to declare decryption.

After the expiration of 96 hours, decryption cost will be automatically increased.
Now you should send us message with your personal ID, which is at the bottom of the message.
We hope that you understand the importance of the work we have done.

Before paying you can send us 2 files for free decryption.
The total size of files must be less than 2Mb.
Files should not contain valuable information (databases, backups, large excel sheets, etc..).

Attention! If you want to RECOVER YOUR DATA without problems - NEVER!!! :
reboot, disconnect hard drives or take any action unless you know WHAT YOU ARE DOING!!!
Otherwise, we cannot be 100% sure that the decryptor will work correctly.

!!!THIS IS ESPECIALLY RELATED TO ESXI!!!

If you will try to use any third-party software for restoring your data or antivirus solutions:
this can lead to complete damage to all files and their irrecoverable loss.
Any changes in encrypted files may entail damage of the private key and the loss of all data.

Your personal id: A62A229AB534F137
Username and password are identical to above.

Since we are using SSL encryption as well as .onion, the certificate is not properly signed.
So in order to get into the chat, you need to confirm the insecure connection exception.
Or just use our embeded APP (Windows version only for now). Thank you for understanding.

You can download TOX here:
https://tox.chat/download.html

You can also write to the chat located in TOR network at:
https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion

You can download TOR browser here:
https://www.torproject.org/download/

our TOX below:
D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F061520IA519F7EAB2E2

We hope you carefully read this message and already know what to do.
**/*
D

Prevod ovog teksta je:

/
Pa šta se desilo?

Sve datoteke su šifrirane Integrisanom Šemom Šifriranja.
Struktura datoteke nije oštećena. Dodijeljen vam je jedinstveni identifikator.
Nakon infekcije, imate 96 sati da prijavite dešifriranje.

Nakon isteka roka od 96 sati, troškovi dešifriranja će se automatski povećati.
Sada bi trebalo da nam pošaljete poruku sa svojim ličnim ID, koji se nalazi na dnu poruke.
Nadamo se da shvatate važnost posla koji smo uradili.

Prije nego što platite, možete nam poslati 2 datoteke za besplatno dešifriranje.
Ukupna veličina datoteka mora biti manja od 2Mb.
Datoteke ne bi trebalo da sadrže vrijedne informacije (baze podataka, rezervne kopije, veliki Excel listovi, itd.).

Pažnja! Ukoliko želite da VRATITE SVOJE PODATKE bez problema - NIKAD!!! : ne restartujte, ne odvajajte hard diskove ili preduzimajte bilo kakvu akciju osim ako ne ZNATE ŠTA RADITE!!!

U suprotnom, ne možemo biti 100% sigurni da će dešifrator ispravno funkcionisati.

!!!OVO SE POSEBNO ODNOSI NA ESXI!!!

Ako pokušate da koristite bilo koji softver treće strane za vraćanje podataka ili antivirusno rešenje:
ovo može dovesti do potpunog oštećenja svih datoteka i njihovog nepovratnog gubitka.
Svaka promjena u šifriranim datotekama može da dovede do oštećenja privatnog ključa i gubitka svih podataka.

Vaš lični ID: A62A229AB534F137
Korisničko ime i lozinka su identični sa prethodnim.

Pošto koristimo SSL enkripciju kao i .onion, certifikat nije pravilno potpisan.
Dakle, da biste ušli u chat, morate potvrditi izuzetak za nesigurnu vezu. Ili samo koristite našu ugrađenu APP (Windows verzija samo za sada). Hvala na razumijevanju.

TOX mozete preuzeti sa:
https://tox.chat/download.html

Takođe možete pisati na chat koji se nalazi u TOR mreži na:
https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion

TOR browser možete preuzeti sa:
https://www.torproject.org/download/

naš TOX je ispod:
D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F06152O1A519F7EAB2E2
Nadamo se da ste pažljivo pročitali ovu poruku i da već znate šta da radite.
**/*
D

Poruka ima neke posebnosti u odnosu na uobičajene poruke ove vrste. Prva posebnost je da nema nikakvih podataka o iznosu novca koji je potrebno platiti, kao ni Bitcoin, ili neke druge adrese, na koju treba uplatiti. Od žrtve se traži da uspostavi komunikaciju sa napadačem putem TOX aplikacije za sigurno dopisivanje (*chat*). To je aplikacija poput Viber ili WhatsApp, ali bez centralnog servera pod nadzorom kompanije koja je autor aplikacije. Umjesto toga koristi *peer-to*-peer sistem povezivanja. Cilj je da se smanji mogućnost nadgledanja i kontrole učesnika i sadržaja dopisivanja. Naveden je i TOX identifikator napadača. Ova informacija može pomoći da se pronađu druge žrtve istog napadača i poveže više napada. Poruka navodi i lični ID žrtve. I ovaj ID može biti provjeren u potrazi za sličnim napadima. U poruci se posebno spominje ESXi hipervizor. To može značiti da je pravljena namjenski za napade na VMware virtualizacijsku platformu.

Pored ovog, uobičajenog, rezultata *ransomware* napada na virtualizacijsku infrastrukturu, napadači su dodatno otežali oporavak od posljedica napada na način da su obrisali rezervne kopije (*backup*) podataka Sarajevogasa koje su napravljene korištenjem Veem softvera. To su bile kopije svih podataka koje je Sarajevogas čuvao. Njihova namjena je bila upravo da se može oporaviti od događaja u kom su originalni podaci izgubljeni. Ovim su napadači željeli povećati svoje šanse za naplatu. Pojava da napadači brišu rezervne kopije u sklopu, a obično neposredno prije napada nije viđena prvi put, ali je relativno novijeg datuma. Prve ovakve pojave registrovane su 2020. godine. Da bi bilo moguće obrisati rezervne kopije napadači su morali imati prava korisnika koji upravlja ovim kopijama. To znači da su napadači pristupali sistemu pod prijavom administratora sistema, tj. na neki način su došli do prijavnih podataka ili su iskoristili propust u nekom softveru koji pokreće administrator sistema.

4 OTKLANJANJE POSLJEDICA NAPADA

Osnovna negativna posljedica napada bila je nedostupnost usluga informacionog sistema Sarajevogasa. To znači da su svi poslovni procesi za čije obavljanje je neophodan informacioni sistem bili zaustavljeni. Upravljanje sistemom snabdijevanja plinom se ne radi kroz informacioni sistem, pa ta funkcionalnost nije bila ugrožena. Ipak, zaustavljanje nekih poslovnih procesa dovodi do materijalnih troškova. Ovi troškovi se u nekoj mjeri mogu izračunati. Pored materijalnih gubitaka postoje i nemjerljiva šteta po ugled kompanije. Iz ovog razloga, prvi cilj je bio omogućiti rad informacionog sistema i nastavak normalnog rada kompanije.

Potrebno je osvrnuti se na budućnost u kojoj će se i upravljanje sistemom snabdijevanja plinom raditi kroz informacioni sistem. U toj skoroj budućnosti ovakav napad bi za posljedicu mogao imati potpuni prekid snabdijevanja plinom. To bi, pogotovo u zimskom periodu, moglo imati katastrofalne posljedice koje bi uključivale i opasnost po živote ljudi.

Oporavak izmjenjenih ili obrisanih datoteka vrši se iz rezervnih kopija (*backup*). U ovom slučaju brzi povrat datoteka virtualnih mašina direktno iz lako dostupnih rezervnih kopija putem Veem softvera nije bio moguć. Te datoteke su, dijelom i zbog njihove lake dostupnosti, bile obrisane tokom napada. U skladu sa dobrim praksama Sarajevogas je imao dodatne kopije datoteka koje nisu direktno dostupne za povrat, ali su time teže dostupne i napadačima. Ove kopije su, što je uobičajeno za ovakve druge kopije, bile na magnetnim trakama.

Magnetne trake za čuvanje podataka su slične magnetnim trakama korištenim u muzičkim i video kasetama. Na njih se može pohraniti velika količina podataka, ali se tim podacima mora pristupati redom. To znači da je potrebno premotati traku do pozicije na kojoj se neki podatak nalazi. Radi poređenja, podacima na hard diskovima se pristupa direktno bez potrebe da se nešto premotava. Zbog načina pisanja i čitanja proces čuvanja i oporavka podataka sa traka je mnogo sporiji nego što je to slučaj za hard diskove. Za čitanje i pisanje magnetnih traka koriste se posebni uređaji. Trake se ubacuju u ovaj uređaj kad se na njih nešto zapisuje ili sa njih čita. Kada se ne koriste trake se nalaze

van uređaja. Iako je kapacitet traka veliki, količine podataka čije se kopije se danas prave su tolike da je potrebno imati veći broj traka. Ovo trake čini relativno nepraktičnim, ali sa druge strane prilično sigurnim načinom čuvanja rezervnih kopija. Da bi se ove kopije obrisale ili izmijenile napadač bi morao imati fizički pristup trakama. Naravno, fizička zaštita traka od oštećenja ili krađe je neophodna.

Kako je napad na Sarajevogas bio samo putem informacionog sistema podaci na trakama nisu bili ugroženi. To je omogućilo uposlenicima IT službe Sarajevogasa da uspješno povrate ispravne kopije svih datoteka virtuelnih mašina. Oni su, pored ovoga, uredili i reinstalaciju virtualizacijskog VMware softvera koji koriste. Taj korak je napravljen da bi se eliminisala mogućnost da je neki softver napadača još prisutan u virtualizacijskoj platformi koju Sarajevogas koristi. Reinstalirani softveri za virtualizaciju i ispravne kopije virtuelnih mašina omogućile su pokretanje ovih virtuelnih mašina. Time su pokrenuti svi serveri informacionog sistema Sarajevogasa sa svim svojim uslugama. Sve usluge informacionog sistema su postale dostupne. Svi poslovni procesi ovisni o njima su se mogli obavljati.

Potrebno je napomenuti da prilikom povrata datoteka iz njihovih rezervnih kopija uvijek dođe do određenog gubitka podataka. Dio podataka koji je nastao od trenutka pravljenja kopija, sa kojih je rađen oporavak, do trenutka kad se desi događaj zbog kog je potrebno izvršiti povrat bude izgubljen. Koliko podataka će biti izgubljeno zavisi od učestalosti pravljenja kopija i intenziteta generisanja novih podataka. Za slučaj Sarajevogasa ovi podaci nisu bili dostupni.

Bitno je naglasiti da su u ovom slučaju slučaju ispoštovane sve procedure zaštite u skladu sa pravilima struke, a koje predviđaju uspostavljanje višestrukih rezervnih kopija. Također, bitno je da su ove kopije bile ispravne i oporavak sa njih je bio moguć, što ne mora uvijek biti slučaj.

5 ANALIZA NAPADA

5.1. NAPADAČ – „DONUT LEAKS“

Na osnovu prikupljenih podataka izvršena je pretraga za sličnim napadima. Po ekstenziji „.d0nut“ koju dobiju šifrirane datoteke ovaj *ransomware* je nazvan „d0nut *ransomware*“. Prvi zabilježeni napadi ovim *ransomware* su iz druge polovine 2022. godine. Pored ekstenzije ovi napadi su imali identičnu ili vrlo sličnu poruku od napadača. Isti TOX *chat* identifikator D340414145 9BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F0615201A519F7EAB2E2i TOR adresa za *chat* https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion pojavljuju se u svim porukama. Ovi identifikatori su povezani sa napadačkom grupom „donut leaks“. Nije poznato odakle je ova grupa. Ona je odgovorna za bar 10 napada. Tri od 10 kompanija su javno objavile da su napadnute, it o:

1. Sheppard Robson, arhitektonsku firmu u Velikoj Britaniji 24.7.2022.
2. Sando, globalna građevinska kompanija 7.2022.
3. DESFA, grčka kompanija za prirodni gas 20.8.2022.

Ostale žrtve nisu se javno oglasile, pa njihova imena nisu javna. Minimalni broj žrtava je utvrđen na osnovu web adrese dostupne putem, anonimnog, TOR web preglednika. Na toj adresi grupa „donut leaks“ je objavila dio podataka koje su preuzeli iz napadnutih kompanija. Broj kompanija čiji podaci su bili dostupni je bio 10. Cilj ove objave podataka bio je da se žrtve osramote i prisile za plaćanje otkupnine. Ovo objavljivanje je vezano i sa imenom grupe „leaks“ jer ukazuje da oni „procure“ podatke kompanije u javnost. Zanimljivo je da su za napad na DESFA odgovornost preuzela i napadačka grupa Ragnar Locker, a za napad na Sando odgovornost je preuzela grupa Hive Ransomware. Smatra se da je Donut Leaks originalno izvela napad , ali da je dio podataka iz nekih od

napada dospio do drugih grupa, moguće od članova koji su promijenili grupe. Isti TOX *chat* identifikator pojavio se i u napadima sa HelloXD *ransomware* iz novembra 2021, vezanim za grupu x4k. Detaljan opis tog *ransomware* dala je Unit 42 sigurnosne kompanije PaloAlto[2]. Najbolji opis rada grupe Donut Leaks objavio je BleepingComputer u svoja dva članka od 23.8.2022.[3] i 22.11.2022.[4]

5.2. SPECIFIČNOSTI NAPADA NA SARAJEVOGAS

Specifičnost napada na Sarajevogas ogleda se u tome što je, za razliku od napada na druge kompanije izvršene istim *ransomware* (d0nut), od strane iste grupe (Donut Leaks), u ovom slučaju izvršen napad na virtualizacijsku platformu. U svim drugim slučajevima ovog ransomware napada, napad je izvršen direktno na računare/servere, a ne na virtualizacijsku platformu. Kako je ranije napomenuto, napad na virtualizacijsku platformu ima mnogo veće posljedice nego napad na neki pojedinačni server ili računar. U slučaju napada na pojedini server samo taj server postaje nedostupan. U slučaju napada na virtualizacijsku platformu svi serveri postaju nedostupni.

Razlog za napada na virtualizacijsku platformu može biti što su slučaju Sarajevogasa isti napadači uspjeli doći do pristupa virtualizacijskoj platformi, pa su tu izvršili napad. Nadalje, Sarajevogas nije dobilo obavijest o mogućem objavljivanju njihovih podataka radi dodatnog pritiska da izvrše uplatu. Ipak isti podaci za kontakt ukazuju da se radi o istom organizatoru napada.

Nije bilo moguće utvrditi kako su napadači uspjeli pokrenuti svoj zlonamjerni softver za šifriranje datoteka. Nije bilo moguće utvrditi kako su se uspjeli pristupiti Veem rezervnim kopijama podataka i obrisati ih. Za ovo je bilo neophodno da na sistem budu prijavljeni kao administratori. Nije bilo moguće utvrditi kako su napadači došli do pristupnih podataka za prijavu kao administrator sistema. Na pregledanim personalnim računarima u Sarajevogasu nisu pronađenih znakovi zaraze zlonamjenim softverima. Prilikom oporavka podataka iz rezervnih kopija i reinstalacije VMware virtualizacijskog softvera te oporavka svih potencijalno zaraženih računara u Sarajevogasu prepisani su tragovi koji su možda mogli ukazati na izvor i put napada. Ova situacija se često dešava prilikom napada. Organizacija želi da što prije povrati funkcionalnosti. To znači poduzimanje koraka za uklanjanje napada. Sa druge strane organizacije, a posebno agencije za sprovođenje zakona, žele da prikupe tragove koji će im pomoći da ustanove kako je do napada došlo i odakle je došao. Prilikom izrada planova reakcije na incidente neophodno je imati u vidu oba aspekta i napraviti odgovarajući plan.

Jedan od mogućih puteva napada je udaljena konekcija prema mreži Sarajevogasa koju je koristila kompanija koja je radila na SCADA sistemu Sarajevogasa. Prema dobivenim informacijama od Sarajevogasa ta konekcija je omogućavala partnerskoj kompaniji neograničen daljinski pristup dijelu sistema Sarajevogas na kom su radili. Drugi mogući način na koji su napadači pristupili virtualizacijskoj platformi su konekcije koje su postojale sa nekih od računara IT uposlenika na ovoj platformi. Ove konekcije su omogućavale IT uposlenicima zaduženim za održavanje virtualizacijske platrforme da obavljaju ove zadatke sa svojih računara, bez potrebe za fizičkim pristupom serveru na kom je ova platforma pokrenuta. Ta praksa je uobičajen način upravljanja virtualizacijskom infrastrukturom. Napadači su mogli zaraziti računar nekog od IT uposlenika i preuzeti kontrolu nad njim. Veza tog računara sa virtualizacijskom platformom je onda iskorištena da se napadač poveže i šifrira datoteke. Međutim, ni na ovim računarima nisu pronađeni tragovi zlonamjernog softvera. To može značiti da nisu bili put napada ili da su napadači uklonili svoj softver po završenom napadu.

[2] https://unit42.paloaltonetworks.com/helloxd-ransomware/

[3] https://www.bleepingcomputer.com/news/security/new-donut-leaks-extortion-gang-linked-to-recent-ransomware-attacks/

[4] https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/

Putevi napada su obično prevara korisnika ili loše zaštićena konekcija prema unutrašnjoj mreži. Korisnici se prevare da unesu svoje pristupne podatke na neku lažnu stranicu ili da pokrenu softver iz priloga e-pošte ili sa neke navodno korisne stranice. Napadač ukradene pristupne podatke koristi da bi dobio pristup sistemu korisnika čije podatke ukrao. Na taj način napadač ostvari pristup resursima unutar organizacije koje želi napasti, u ovom slučaju šifrirati ili obrisati podatke.

Ako korisnik bude prevaren da pokrene softver koji mu je napadač podmetnuo, taj softver dobiva prava korisnika koji ga ke pokrenuo. Sa tim pravima softver može izvršiti šifriranje i brisanje ili omogućiti napadaču udaljeni pristup sistemu, kao kod ukradenih pristupnih podataka. Ako informacioni sistem organizacije ima aktivnu konekciju koja omogućava spoljnim saradnicima pristup radi održavanja ili unapređenja sistema, takav pristup može biti zloupotrebljen. Moguće je da pristupni podaci za sistem budu pogođeni ili ukradeni. Druga opcija je da napadači izvrše upad u sistem spoljnih saradnika i na taj način zloupotrebe konekciju koju ti saradnici imaju prema organizaciji koja je krajnji cilj napada.

6 ZAKLJUČCI I PREPORUKE

6.1. ENERGETSKI SEKTOR U BIH MOŽE BITI META

Najvažnija pouka je da se ovakvi napadi dešavaju i kod nas, u Bosni i Hercegovini. Žrtve napada su i kompanije u energetskom sektoru. Treba očekivati sve više ovakvih napada. Uz dolazak zime i moguće vrlo ograničene količine energije dostupne u Evropi energetske kompanije će biti sve privlačnije žrtve ovakvih ucjena. Treba biti spreman. To znači smanjiti rizik od toga da kompanije bude žrtva uspješnog napada i smanjiti moguće posljedice takvog napada.

Veoma je bitno da sve kompanije i organizacije koje djeluju u energetskom sektoru u BiH stave ovo pitanje na svoje agende, izvrše interne analize ranjivosti i aktivno rade na zaštiti svojih sistema i informacija.

6.2. USVAJANJE ZAKONSKOG OKVIRA I EDUKACIJA

Usvajanje neophodnog zakonskog okvira koji će urediti sve aspekte vezane za cyber bezbjednost u BiH je neophodno i predstavlja nužni preduslov sistemskog rješavanja ovih pitanja.

Pored svega spomenutog potrebno je da se kontinuirano diže svijest javnosti o ovome problemu i njegovoj prisutnosti, uz kontinuiranu edukaciju o razmjerima problema koji mogu nastati usljed cyber napada.

6.3. POBOLJŠATI RAZMJENU INFORMACIJA U ENERGETSKOM SEKTORU

Druga lekcija je da su napadnute kompanije u situaciji da ne znaju kome se obratiti. Jedan kontakt su agencije za sprovođenje zakona. One se bave krivičnom odgovornošću napadača. Za tehničku pomoć i podršku kompanije se moraju obratiti privatnim firmama. To je uglavnom neophodan korak, ali mogu mu prethoditi drugi koji će dodatno pomoći. Dobro uspostavljena razmjena informacija između kompanija u energetskom sektoru omogućila bi učenje na iskustvima drugih. To može pripremiti kompanije za napade koji su se negdje već desili. Može olakšati zaustavljanje napada i otklanjanje njegovih posljedica. Drugo kompanije iz sektora mogu podijeliti i iskustva u angažovanju privatnih firmi za oporavak od napada. Jedan uobičajeni oblik takve saradnje je CSIRT za energetski

sektor. Trebalo bi raditi na njegovom formiranju. To u početku može biti manje formalna grupa uposlenika energetskih kompanije koji se bave sigurnošću informacija. Vremenom može postati pravi formalni CSIRT.

6.4. BACKUP JE NEOPHODAN

Za ovakve napada koji ugrožavaju dostupnost podataka najvažnija zaštita su rezervne kopije podataka (*backup*). Za pravljenje ovih kopija treba koristiti namjenski softver. Nezavisno od softvera treba se držati pravila 3-2-1[5]. To znači da treba imati tri kopije svih važnih datoteka. Jednu primarnu i dvije rezervne. Čuvati kopije na dvije različite vrste medija. Pohraniti jednu kopiju na fizički različitu lokaciju od lokacije izvornih podataka. Rezervne kopije ne štite samo od *ransomware* napada. One omogućavaju oporavak podataka i za sve druge slučajeve kada su podaci obrisani ili nedostupni usljed napada, greške legitimnih korisnika ili prirodne katastrofe.

6.5. ZAŠTITI VIRTUALIZACIJSKU PLATFORMU

Napadi na virtualizacijsku infrastrukturu će biti sve češći. Oni su vrlo efikasni za napadača jer jednim uspješnim napadom ugrožavaju kompletnu IT infrastrukturu organizacije. Kompanije u energetskom sektoru su uglavnom velike što znači i velika IT infrastruktura. Takva infrastruktura je danas uglavnom virtualizovana. Znači da meta ovih napada mogu biti kompanije u energetskom sektoru u BiH. Neophodno je da ove kompanije analiziraju i učvrste zaštitu svoje virtualne infrastrukture. Dosta odbrana je fokusirano na odbranu pojedinačnih usluga i/ili pojedinačnih servera. Te odbrane treba i dalje da postoje. Uz njih je potrebno imati i odbranu infrastrukture. Ta odbrane treba da uključuje tehničke, ali i fizičke mjere koje ograničavaju pristup infrastrukturi. Ovo se naziva odbrana po dubini ili slojevita odbrana i preporučeni je pristup izgradnji zaštita.

6.6. KORISTITI VIŠEFAKTORNO POTVRĐIVANJE IDENTITETA

Smanjivanje rizika od uspješnih napada postiže se i prekidanjem puteva napada. Prema statistikama[6][7] najčešći putevi napada su krađa pristupnih podataka i iskorištavanje nezakrpljenih sigurnosnih propusta u javno dostupnim uslugama. Ovi napadi se često izvode na partnere organizacije koja je krajnji cilj napada. Napadaju se partneri koji imaju pristup unutrašnjoj mreži organizacije. U skladu sa statistikama zaštite se trebaju i prioritetizirati. Krađa pristupnih podataka se dešava prevarom korisnika ili njihovim pogađanjem. Od prevara korisnika se štiti obukom korisnika. Od pogađanja pristupnih podataka se štiti razumnom politikom kompleksnosti ovih podataka. Za obje situacije dobra preporučena zaštita je korištenje višefaktornih metoda potvrđivanja identiteta prilikom prijava na sistem. To danas najčešće znači da korisnik pored lozinke unosi i dodatni broj koji mu generiše softver na telefonu. Ovakav način prijavljivanja bi morao biti obavezan za kritične sisteme poput virtualizacijske platforme.

6.7. REDOVNO AŽURIRATI OPERATIVNE SISTEME I SOFTVER

Redovnim ažuriranjem softvera otklanjaju se sigurnosni propusti koje napadači iskorištavaju. Ako postoje softveri koje nije moguće ažurirati, a to se dešava u energetskom sektoru zbog dugog vijeka

[5] Paul Ruggiero and Matthew A. Heckathorn, „Data Backup Options“, CISA/US-CERT, 2013.
[6] John Pescatore and Terry Hicks, „SANS 2022 Top New Attacks and Threat Report“, SANS, 2022.
[7] „Microsoft Digital Defense Report 2022“, Microsoft, 2022.

namjenskog hardvera i softvera, onda se moraju poduzeti druge mjere zaštite koje onemogućavanje iskorištavanje neažurnih softvera. Svi partneri kojim se omogućava daljinski pristup sistemu moraju dokazati da su poduzeli bar identične mjere zaštite kao i organizacij kojoj ime se omogućava pristup, prije davanja ovog pristupa.

Naravno, mjera može biti i više. Ovdje su radi primjenjivosti i konciznosti navedene one koje su prioritetne.

Američka agencija za međunarodni razvoj

www.usaid.gov