SAFE MODE

Izsiljevalski virus:
Obramba in ukrepanje v primeru okužbe

UVOD

V zadnjih letih je področje kibernetskega kriminala doseglo nove višave. Napadalci so začeli delovati na način, ko neposredna kraja podatkov ali denarja ni več glavni vir dohodkov. Namesto da bi naše podatke ukradli, jih zdaj zašifrirajo in nato od nas zahtevajo odkupnino za povrnitev dostopa do njih. Najmočnejše orožje pri služenju ogromnih količin denarja predstavlja prav ena največjih pridobitev današnjega časa - šifriranje podatkov. Prvotno idejo, ki je služila za zaščito pomembnih podatkov in sistemov nepridipravi uporabljajo v svoji izvedbi - ***izsiljevalskem virusu***.

KAJ JE TO IZSILJEVALSKI VIRUS?

Izsiljevalski virus se pojavlja v različnih oblikah, bistvo njegovega delovanja pa je v tem, da zaklene datoteke na napravi in lastniku onemogoči dostop do njih. V zameno za dostop do podatkov zahteva plačilo odkupnine v obliki kripto valut, kot je npr. ***Bitcoin (BTC)***. Plačilo odkupnine je navadno časovno omejeno, po izteku tega časa pa se odkupnina lahko poveča.
Po prejetem plačilo napadalec (po navadi) žrtvi posreduje digitalni ključ, s katerim lahko odklene svoje, sicer močno šifrirane, datoteke.

KDO JE LAHKO TARČA?

Tarče smo vsi, saj napadalci ne ciljajo na določeno skupino posameznikov ampak ***masovno pošiljajo škodljivo programsko kodo*** preko elektronske pošte, lažnih spletnih strani, okuženih USB ključkov, itd.

KAJ SE LAHKO ZGODI V PRIMERU OKUŽBE?

V najboljšem primeru je lahko okužen samo en računalnik, če le ta ni priklopljen na mrežo. Na tej napravi nam je ***onemogočen dostop*** do določenih, šifriranih, datotek. V okoljih, kjer je več naprav povezanih v mrežo, je velika nevarnost, da se virus razširi po njej in okuži tudi ostale naprave. Povzročena je lahko velika gospodarska škoda. Posebej ranljiva sta zdravstveni sektor in kritična infrastruktura, saj lahko virus onemogoči dostop do datotek, ki so potrebne za delovanje življenjsko pomembnih sistemov.

KAJ SO TO KRIPTO VALUTE - BITCOIN?

Bitcoin je oblika kripto valute, ki ne obstajajo v fizični ampak izključno v digitalni obliki. Shranjeni so v digitalnih denarnicah, ki so ***anonimne***. Plačilo z Bitcoin-i je možno kadarkoli iz kjerkoli in kamorkoli po svetu, popolnoma anonimno. Iz tega razloga napadalci pri plačilu odkupnine zahtevajo uporabo omenjene kripto valute, saj jih organi pregona tako ne morejo izslediti. Vrednost Bitcoin-a stalno variira, v letu 2016 pa se vrednost giblje med $600 in $700.

TOR (omrežje za anonimnost)

Omrežje katerega kratica pomeni “The Onion Router”, ima tudi svoj spletni brskalnik. Oba sta zasnovana z namenom, da zagotovita ***anonimnost internetnemu prenosu podatkov***. Ves prenos podatkov po omrežju je šifriran in onemogoča določanje izvorne in končne lokacije prenosa podatkov. Uporabljajo ga posamezniki, ki želijo med brskanjem po internetu ostati anonimni. Priročen je tudi za napadalce, ki preko njega ***komunicirajo z svojimi žrtvami***, brez strahu, da bi jih izsledili.

KAKO VEMO, DA SMO OKUŽENI?

Simptomi, ki kažejo na to, da je vaša naprava okužena z izsiljevalskim virusom so očitni. Najpogosteje se zgodi, da:

- ne morete več odpirati običajnih datotek;
- se na vašem ozadju zaslona prikaže sporočilo z navodili, kako izvesti plačilo in pridobiti nazaj svoje podatke;
- se odpre okno izsiljevalskega programa, ki ga ne morete zapreti;
- se v vseh mapah prikažejo datoteke v različnih formatih, v katerih so navodila kako pridobiti svoje podatke nazaj;
- nas program opozori na odštevanje ure, ki kaže čas za plačilo določene odkupnine, saj se po izteku ure kupnina poveča.

Primer okna, ki se nam odpre v primeru okužbe:

Vidna je ura, ki odšteva čas, na voljo za plačilo, navodila kako izvesti plačilo in razlaga, kaj se je z našo napravo pravzaprav zgodilo.

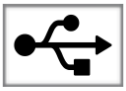
Pojavna okna se razlikujejo glede na različico virusa. Primer se nanaša na t.i. TeslaCrypt, ki je v času pisanja ena izmed zadnjih in tudi bolj sofisticiranih različic izsiljevalskega virusa.

KAKO SE LAHKO OKUŽIMO?

Preko elektronske pošte: Najbolj običajen scenarij vsebuje elektronsko sporočilo s pripeto datoteko, ki na prvi pogled deluje neškodljiva. Napadalci pogosto dodajo več končnic na koncu imena datoteke in s tem poskušajo zakriti pravi tip dokumenta. Če uporabnik ne preveri izvora elektronskega sporočila in odpre pripeto datoteko lahko to vodi do okužbe z izsiljevalskim virusom. Elektronsko sporočilo je lahko tudi brez priložene datoteke in namesto tega vsebuje povezavo, na katero naj bi kliknili. Pomembno je, da vedno preverimo kam povezava vodi, saj lahko ob kliku sprožimo nalaganje virusa na našo napravo.

Z obiskom sumljive spletne strani: Veliko okužb se zgodi tudi z obiskom sumljivih spletnih strani. Tehniko imenujemo drive-by-download. Napadalci izkoriščajo varnostne luknje zastarelih spletnih brskalnikov in ostale ne-posodobljene programske opreme. Ko uporabnik obišče tovrstno spletno stran, poseben program preveri za možnimi ranljivostmi in jih v nadaljevanju izkoristi za namestitev izsiljevalskega virusa.

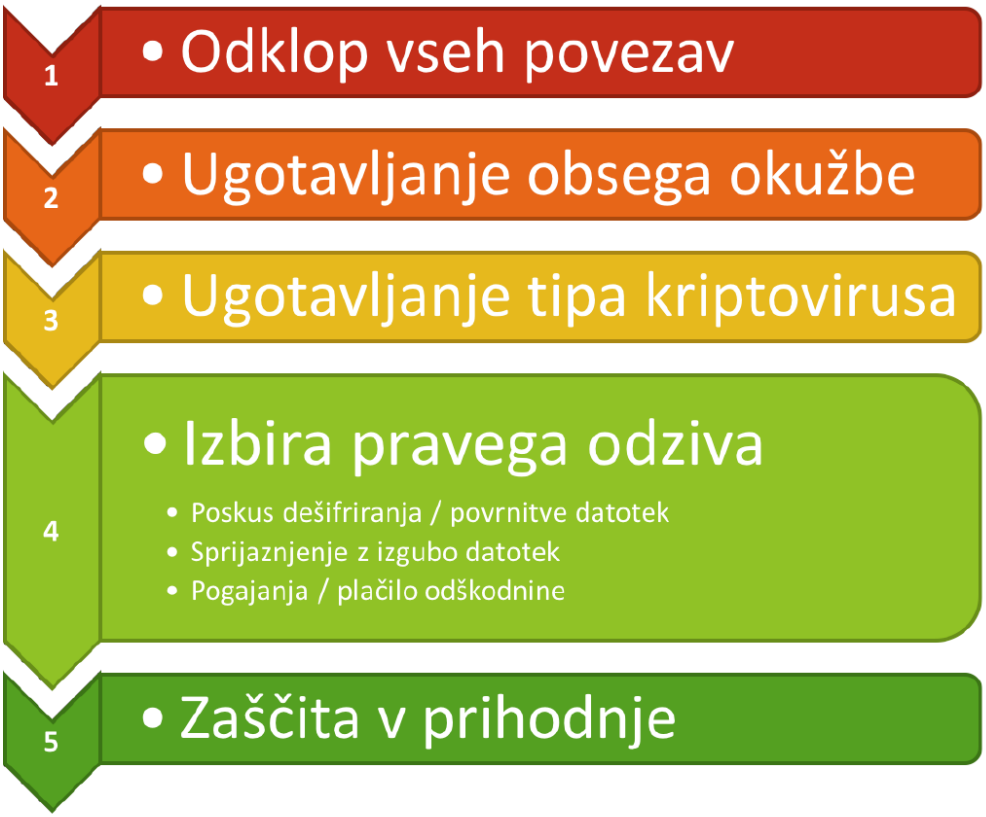
Z nalaganjem zastonjske in piratske vsebine: Napadalci lahko zlonamerno programsko kodo zapakirajo v nek drug izdelek (npr. program za urejanje PDF dokumentov) in ga zastonj ponudijo na spletu. Ob nameščanju tovrstnih programov nepoznanih proizvajalcev je potrebna dodatna pazljivost in velja dodatno preveriti avtorja programa. Posebno pozornost je potrebno nameniti tudi v primeru nameščanja piratskih vsebin na naše naprave. Virus se najpogosteje skriva v raznih računalniških igrah ali programski opremi, vsebini za odrasle, ohranjevalnikih zaslona, itd. Ko se virus namesti na našo napravo, se lahko skrije in začne delovati šele čez nekaj časa (npr. nekaj tednov).



Z nepoznanimi pomnilni mediji: V skoraj vsaki organizaciji se na dnevni ravni uporablja različne pomnilne medije (USB ključki, zunanji diski, spominske kartice, itd.). Ker smo uporabe pomnilnih medijev navajeni, naše naprave pa jih prepoznajo kot zaupanja vredne, ti predstavljajo visoko tveganje. V primeru, da npr. USB ključek najdete na hodniku vaše organizacije ali pa ga dobite kot promocijski material ga ne vstavljajte v službene računalnike. V primeru, da je neznani pomnilni medij okužen z virusom, lahko s tem povzročite veliko škodo.

"Napadalci pri izvedbi napada na uporabnika v večini primerov (več kot 80%) uporabljajo socialni inženiring. To pomeni, da s prevaro pridobijo zaupanja tarče in nato to zaupanje izkoristijo oziroma tarčo preslepijo."

KAJ STORITI V PRIMERU OKUŽBE?



1. **Odklop vseh povezav**: Ko ugotovite, da ste se okužili z izsiljevalskim virusom nemudoma izključite napravo iz omrežja. Izključite mrežni kabel, lahko tudi napajanje, Wi-Fi, Bluetooth, skratka vse kar omogoča povezljivost med napravami.
2. **Ugotavljanje obsega okužbe**: Obseg okužbe nam pove kolikšna škoda je narejena in nakaže kateri so smiselni nadaljnji ukrepi.
3. **Ugotavljanje tipa kriptovirusa**: Z identifikacijo virusa lahko posledično izvemo katere datoteke cilja, kako se širi in če gre za starejšo različico, lahko zanj obstaja že rešitev, ki nam omogoča povrnitev naših podatkov brez plačila odkupnine.
4. **Izbira pravega odziva**: Glede na nastalo škodo in pomembnost podatkov, ki so bili zaklenjeni se odločimo za najbolj smiseln odziv.
5. **Zaščita v prihodnje**: Naj nam bo neprijetna izkušnja z izsiljevalskim virusom opozorilo za naprej. Odslej moramo za našo varnost narediti več. Področja, ki jih moramo pokriti so: redno nadgrajevanje programske opreme, izdelava varnostnih kopij in delo na človeškem faktorju (se pravi nas samih). Če se je okužba zgodila v organizacijskem okolju, je pomembno, da organizacija zagotovi ustrezna izobraževanja za vse zaposlene, da bi v bodoče lahko bolje ščitili svoje premoženje. Na mestu so občasni simulirani napadi s pomočjo strokovnjakov, saj na realnih primerih zaposleni lahko največ naučijo. Vsak posameznik, ki dela z informacijsko komunikacijsko tehnologijo, se mora zavedati pretečih groženj in ukrepov, da se pred njimi obvaruje.

SEZNAM UKREPOV V PRIMERU IZSILJEVALSKEGA VIRUSA

1. korak: Izklopite vse povezave!
   - ☐ Izklopite računalnik iz mreže.
   - ☐ Izklopite vse brezžične povezave (Wi-Fi, Bluetooth, NFC,…).

2. korak: Ugotovite obseg okužbe, poiščite zaklenjene datoteke
   - ☐ na različnih diskih na vašem računalniku in datotekah v skupni rabi,
   - ☐ datoteke v skupni rabi ostalih računalnikov,
   - ☐ na mrežnih napravah za shranjevanje dokumentov,
   - ☐ na zunanjih trdih diskih,
   - ☐ na USB ključkih, spominskih karticah, priklopljenih telefonih, kamerah, itd.,
   - ☐ storitvah za hrambo podatkov v oblaku (DropBox, iCloud, Google Drive, …).

3. korak: Ugotovite tip izsiljevalskega virusa
   - ☐ Izsiljevalskih virusov je več vrst, in nastopajo pod različnimi imeni (TeslaCrypt, Locky, CryptoWall, itd.).

4. korak: Izberite pravi odziv (s pomočjo korakov 2 in 3)
   - ☐ Povrnite svoje datoteke iz varnostnih kopij.
   - ☐ Poskušajte odkleniti vaše datoteke.
   - ☐ Ne nič naredite, če škoda ni velika.
   - ☐ Pogajajte se za nižjo odkupnino in jo plačajte.
   - ☐ Pokličite strokovnjake, ki vam bodo pri povrnitvi podatkov pomagali.

5. korak: Zaščitita v prihodnje:
   - ☐ Implementirajte ukrepe, ki vas bodo v prihodnosti varovali pred okužbo z izsiljevalskim virusom (kontinuirano izobraževanje na področju varovanja informacij).

UKREPI ZA PREPREČEVANJE OKUŽBE S KRIPTOVIRUSOM

1. Tretja linija obrambe: Varnostne kopije

- ☐ Vpeljite programske ali strojne rešitve za izdelavo kvalitetnih varnostnih kopij.
- ☐ Definirajte informacijsko premoženje organizacije, da boste vedno varnostno kopirali ključne podatke, ki jih potrebujete za poslovanje.
- ☐ Varnostne kopije zaščitite, jih posodabljajte in poskrbite, da bodo dostopne, ko bo to potrebno.
- ☐ Redno testirajte postopek povrnitve podatkov iz varnostnih kopij in v primeru pojave težave, le te odpravite.

2. Druga linija obrambe: Posodobitve programske opreme

- ☐ Zagotovite uporabo požarnega zidu.
- ☐ Vpeljite programsko opremo, ki vas bo ščitila pred poskusi kraje osebnih podatkov in neželeni elektronski pošti.
- ☐ Poskrbite, da vsi v vaši organizaciji uporabljajo posodobljene protivirusne programe in ostalo zaščito za delo z spletnimi storitvami.
- ☐ Onemogočite nameščanje neavtorizirane programske opreme na računalnikih vaših zaposlenih, v domačih okoljih pa bodite previdni pri nameščanju zastonjskih in piratskih programov.
- ☐ Redno posodabljajte tudi ostalo programsko opremo, saj se čez čas lahko ugotovi določene ranljivosti in se za njih izda popravek.

3. Prva linija obrambe: Uporabniki

- ☐ Vpeljite učinkovito izobraževanje uporabnikov, ki bo uporabnikom redno posredovalo potrebna znanja za obrambo pred pretečimi grožnjami.
- ☐ Sami ali s pomočjo zunanjih strokovnjakov redno izvajajte simulirane napade na področju socialnega inženiringa, lažnih spletnih strani in sumljive elektronske pošte (saj so to najpogostejši načini okužbe z zlonamerno programsko kodo).

Kontaktni podatki:

info@safe-mode.net

080 1235

https://www.safe-mode.net

Izvedbeni partnerji:

ZUPO.SI GLOBALNA INFORMACIJSKA DRUŽBA D.O.O.

EVIDENTIUM DETEKTIVSKE IN VARNOSTNE REŠITVE D.O.O.

40 let Univerza v Mariboru

Fakulteta za varnostne vede