jamk.fi

Tutkimustyö

Tunkeutumis- ja puolustamismenetelmät

Tuukka Bordi M2296, TTV18S1
Timo Lehosvuo M3426, TTV18S1

Harjoitustyö, Jarmo Nevala
Maaliskuu 2021
Liikenteen ja tekniikan ala
Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisällys

1. Psykoterapiakeskus Vastaamon tietomurron aikajanakuvaus 2

2. APT –Advanced Persistent Threat: APT 6

2.1. Organisaatiokuvaus 6

2.2. APT 32:n käyttämät työkalut 7

2.3. APT 32:n kill chain 7

2.4. Puolustusmenetelmät 9

2.5. Puolustus- ja hyökkäystaidot 11

3. Pohdinta 11

Lähteet 12

1. Psykoterapiakeskus Vastaamon tietomurron aikajanakuvaus

Nro	Lähde	Päiväys	Kuvaus	Linkki
1.	Yle	Marraskuu 2018	Verkkorikollinen murtautuu Vastaamon järjestelmiin. Vastaamon koko potilastietokanta varastetaan.	https://www.is.fi/digitoday/tietoturva/art-2000006697806.html
2.	IS	Maaliskuu 2019	Toinen tietomurto Vastaamon järjestelmiin.	https://www.is.fi/digitoday/tietoturva/art-2000006700584.html
3.	Yle	28.9.2020	Vastaamon henkilöstö sai ensimmäisen kiristysviestin.	https://yle.fi/uutiset/3-11642774
4.	HS	29.9.2020.	Vastaamo teki rikosilmoituksen tietomurrosta ja kiristyksestä.	https://www.hs.fi/kotimaa/art-2000006699117.html
5.	IS	30.9.2020	Nixu aloitti yhteistyön Vastaamon kanssa.	https://www.is.fi/digitoday/tietoturva/art-2000006700950.html

6.	HS	21.10.2020	Tapaus tulee julkisuuteen, kun tietomurtaja julkaisi Vastaamon asiakkaiden tietoja ja vaati Vastaamolta noin 450 000 euroa vastaavaa summaa digivaluutta bitcoineina.	https://www.hs.fi/kotimaa/art-2000006699117.html
7.	IS	21.1.2020	Kiristäjä alkoi julkaista potilastietoja netissä.	https://www.is.fi/digitoday/tietoturva/art-2000006700584.html
8.	Yle	22.10.202	Valvira ilmoittaa, että se selvittää terapiakeskus Vastaamon tietomurtoa.	https://yle.fi/uutiset/3-11607115
9.	IS	23.10.2020	Kiristäjä lataa koko potilastietokannan sivuilleen Tor-verkossa.	https://www.is.fi/digitoday/tietoturva/art-2000006700584.html
10.	Tietosuojavaltuutetun toimisto	23.10.2020	Apulaistietosuojavaltuutettu määräsi Psykoterapiakeskus Vastaamon ilmoittamaan tietomurron kohteeksi joutuneille asiakkailleen henkilökohtaisesti.	https://tietosuoja.fi/-/apulaistietosuojavaltuutettu-maarasi-psykoterapiakeskus-vastaamon-ilmoittamaan-tietomurron-kohteeksi-joutuneille-asiakkailleen-henkilokohtaisesti

11.	HS	24.10.2020	Kiristäjä alkaa kiristämään tietomurron uhreja.	https://www.hs.fi/kotimaa/art-2000006698803.html
12.	IS	26.10.2020	Vastaamo päättää irtisanoa toimitusjohtajansa; Vastaamon omistava Intera Partnersin holding-yhtiö PTK Midco Oy aloittaa toimitusjohtajaa kohtaan siviilioikeudelliset toimet.	https://www.is.fi/digitoday/tietoturva/art-2000006700336.html
13.	Yle	29.10.2020	Kiristäjä siirtelee saamien kiristyslunnaita bitcoin-lompakosta toiseen	https://yle.fi/uutiset/3-11616210
14.	Yle	9.11.2020	Vastaamon hallituksen puheenjohtaja vaihtuu. Myös rivijäsenissä tapahtuu muutoksia. Uuden hallituksen tarkoituksena on selvittää yhtiökokousta varten vaihtoehtoisia malleja liiketoiminnan jatkamiselle.	https://yle.fi/uutiset/3-11638020
15.	MTV	15.11.2020	Valkohattuhakkerit ovat päässeet tietomurtajan jäljille. Verkossa esiintyvä ransom_man kertoo tietokannan salasanan olleen root:root.	https://www.mtvuutiset.fi/artikkeli/vastaamo-kiristajaa-jahtaavat-muutkin-kuin-poliisi-mtv-uutiset-vieraili-valkohattuhakkerin-

				tyohuoneessa-tietomurtaja-on-tehnyt-monia-virheita/7984488
16.	Kaupp alehti	26.1.2021	Vastaamon toimitusjohtaja ja hallituksen puheenjohtaja Heini Pirttijärvi irtisanoutui tehtävistään valmistuneen selvityksen jälkeen.	https://yle.fi/uutiset/3-11755889
17.	Yle	27.1.2021	Vastaamon uhrien tietoja ilmestyi jälleen Tor-verkkoon. Ainakin osa tiedoista on aitoja.	https://yle.fi/uutiset/3-11757676
18.	IS	15.2.2021	Vastaamo asetettiin konkurssiin.	https://www.is.fi/digitoday/art-2000007803843.html

19.	IS	24.3.2021	Helsingin käräjäoikeus määräsi Psykoterapiakeskus Vastaamon perustajan ja entisen toimitusjohtajan Ville Tapion sekä tämän vanhempien Nina Tapion ja Perttu Tapion omaisuutta takavarikkoon 9 667 000 euron edestä.	https://www.is.fi/digitoday/art-2000007879204.html

2. APT –Advanced Persistent Threat: APT

2.1. Organisaatiokuvaus

APT 32 -ryhmän (“OceanLotus”) organisaatiorakenteesta ei ollut tietoa saatavilla missään. Tiedossa kuitenkin on, että kyseessä on todennäköisesti vietnamilainen ryhmä (Carr 2017), joka on ollut aktiivinen vuodesta 2014 asti. Ryhmä kohdistaa toimiaan Aasian alueelle. Esimerkkimaita, joihin OceanLotus on kohdistanut toimia ovat Vietnam, Filippiinit, Laos ja Kambodža (APT32, SeaLotus, OceanLotus... 2017). Ryhmällä on vahva fokus myös oletetussa kotimaassaan (Adair & Lancaster 2020).

APT32 on lähiaikoina kohdentanut toimiaan yrityksiin, varsinkin teollisuus-, kuluttuja-, konsultointi- ja majoitusaloihin. (Advanced Persistent Threat Groups n.d.)

APT32 organisaationa käyttää tiettyjä hyökkäysmenetelmiä uhrejaan vastaan. Traditionaalisesti APT32 käyttää spear-phishing, eli sähköpostikalastelumenetelmää (Carr 2017). Kuitenkin viime aikoina APT32 on siirtynyt käyttämään myös infektoituneita verkkosivuja (Adair & Lancaster 2020, OceanLotus Infused Cobalt Strike to BMW and Hyundai to Control the System n.d).

2.2. APT 32:n käyttämät työkalut

OceanLotus käyttää monia työkaluja saavuttaakseen päämääriään. Osa työkaluista on täysin laillisia työkaluja, kun toiset ovat taas muokattu tai tehty hakkerointia varten (APT32, SeaLotus, OceanLotus... 2017.)

Cobalt Strike

Tunnetuin ja monipuolisin työkalu, jota OceanLotus käyttää lienee Cobalt Strike, joka käyttää monenlaisia tekniikoita operoidessaan koneella. Cobalt Strike on maksullinen sovellus, jota ei ole kehitetty pimeisiin tarkoituksiin, mutta rikolliset ovat alkaneet käyttää sitä omiin tarkoitusperiinsä (Cobalt Strike. N.d).

Cobalt Strike on suosittu rikollisten keskuudessa todennäköisesti sen beacon-toiminnallisuuden takia: beaconin avulla rikollinen voi esim. Ajaa komentoja uhrin koneella, siirtää tiedostoja uhrin koneelle, asentaa keyloggerin ja paljon muuta. (Cobalt Strike. N.d.)

Muita työkaluja

OceanLotus käyttää myös seuraavia haittaohjelmia: Denis**,** Goopy**,** KOMPROGO**,** OSX_OCEANLOTUS.D**,** PHOREAL**,** SOUNDBITE**,** WINDSHIELD (APT32, SeaLotus, OceanLotus… 2017).

Nämä kaikki voidaan luetella backdooreiksi, eli ohjelmiksi, jotka asentavat koneelle mekanismin, jonka kautta hyökkääjä voi ottaa siihen myöhemmin yhteyden.

OceanLotus käyttää tämän lisäksi apunaan **Mimikatz**-ohjelmaa. Mimikatzilla voi esimerkiksi elevoida käyttöoikeuksia ja varastaa Windowsin salasanojen hash-arvoja. Kokonaisuudessaan Mimikatz sisältää sellaisia työkaluja, jotka ovat ”post-exploit”, eli sellaisia, joita käytetään, kun järjestelmän sisään on jo päästy. (Mimikatz. n.d).

2.3. APT 32:n kill chain

Vaihe	Hyökkääjä	Puolustaja
Reconnaissance	Kohteesta tiedon kerääminen ja sähköpostiosoitteiden kerääminen phishing viestejä varten	Havaitseminen: Tuntemus olemassa olevista uhkista Estäminen: yrityksen sisäinen tiedonjakopolitiikka
Weaponization	Sähköpostien, liitteiden, koodin, haittaohjelmien ja Infektoituneiden nettisivujen tekeminen	Havaitseminen: Tuntemus olemassa olevista uhkista Estäminen:
Delivery	Sähköpostien lähettäminen ja nettisivujen julkaiseminen	Havaitseminen: Konekohtainen virustorjunta, sähköpostifiltteri Estäminen: automatisoitu antivirus-skannaus sähköposteille, proxy-pohjainen verkkosivusuojaus, organisaation sisäinen muutoksenhallinta, verkkosivujen whitelist
Exploitation	Sähköpostin liite avataan ja haitallinen koodi ajetaan Nettisivuilla kävijöistä kerätään tietoa scriptin avulla tai käyttäjä lataa haitallisen paketin, joka on naamioitu	Havaitseminen: Henkilökunnan kouluttaminen, Konekohtainen virustorjunta, konekohtainen IPS/IDS

	esim. Flash player päivitykseksi, joka ajaa koodia.	Estäminen: vahva salasana, päivitystenhallinta
Installation	Koodi lataa haittaohjelman järjestelmään (backdoor)	Havaitseminen: SIEM, Konekohtainen IDS Estäminen: käyttöoikeuksien separaatio, vahva salasana, kaksivaiheinen tunnistautuminen
Command & control	Hyökkääjä pääsee järjestelmään sisään ja aloittaa tutkimisen peitellen jälkiään	Havaitseminen: verkkopohjainen IDS, konekohtainen IDS Estäminen: palomuurin pääsynhallintasäännöt (ALS), verkon segmentointi
Actions on objectives	Hyökkääjä lataa järjestelmästä keräämänsä tiedot	Havaitseminen: konekohtainen virustorjunta Estäminen: Data-at-Rest Encryption

2.4. Puolustusmenetelmät

Puolustusmenetelmät

OceanLotuksen menetelmiin kuuluu phishing-sähköpostit (Carr 2017). Näitä vastaan

voi suojautua koulutuksella. Nykyaikana sähköpostihuijaukset ovat kehittyneet yhä sofistikoituneimmiksi, joten tietoisuuden nostaminen tästä on tärkeää. Toinen tärkeä asia phishing-huijauksilta suojautumiseen on se, että yrityksellä on tiukka tiedonjakopolitiikka. Mitä vähemmän hyökkääjät tietävät kohteestaan, sen vaikeampaa on suorittaa onnistunut phishaus.

Viimeiseksi sähköpostikalastelusta, sähköpostien automaattinen virusskannaus voi suojata näiltä uhkilta tehokkaasti.

OceanLotus käyttää hyökkäyksiinsä myös **infektoituneita verkkosivuja** (Adair. & Lancaster 2020), joten puolustajan virusturvan täytyy olla kunnossa. Lisäksi verkkoliikenteen seurauksen avulla voi selvittää, onko haittaohjelmia päätynyt omalle koneelle tai onko tapahtunut mitään muuta epäilyttävää (eli näiden ohjelmien osaamisella on hyötyä). Virusskannaus on myös hyödyllinen.

Infektoituneet verkkosivut voivat käyttää hyödykseen esimerkiksi iframe-elementtiä, jonka avulla hyökkääjä voi infektoida käyttäjän koneen, avata toisen (haitallisen) verkkosivun samaan selaimen välilehteen, suorittaa clickjackingiä ym. (Why are iframes considered dangerous and a security risk? 2014.) Infektoituneet verkkosivut voivat tehdä monia muitakin asioita.

Ennen verkkosivuvierailua puolustaja voi selvittää sivuston luotettavuuden kolmannen osapuolen sivustoilta. Näin epäilyttävä linkki jää käyttämättä.

OceanLotus myös imitoi ”oikeita verkkosivuja” käyttämällä domain-nimiä, jotka näyttävät oikeilta (OceanLotus Infused Cobalt Strike to BMW and Hyundai to Control the System n.d). Tätäkin vastaan voi suojautua tarkastamalla verkkosivun luotettavuus etukäteen. Erityisesti sen tiedon tarkastaminen, kuka onko domain-nimi rekisteröity kyseiselle yritykselle paljastaa valesivut.

Ikinä ei pidä myös unohtaa vahvan salasana sekä kaksivaiheisen tunnistautumisen hyödyllisyyttä. Eritoten kaksivaiheinen tunnistautuminen estää monia tilien vaarantumisia.

Viimeisenä olisi aina hyvä pitää virustorjunta ja käyttöjärjestelmä päivitettynä, jotta uusimmat tietoturvapaikkaukset & virustunnisteet on asennettu koneelle.

2.5. Puolustus- ja hyökkäystaidot

Hyökkäystaidot

Hyökkääjä, kuten APT-ryhmä OceanLotus, tarvitsee monia taitoja toteuttaakseen hyökkäyksiään.

- Ohjelmointitaitoja haittaohjelmien tekoon
- Kohteena olevien käyttöjärjestelmien syvällistä tuntemista
- Käytössä olevien verkko(sivu)teknologioiden tuntemista
- Verkkoprotokollien ja domain-järjestelmän tuntemusta
- Taktista taitoa ja tuntemusta hyökkäyksen aikaisiin toimiin
- Tietoa haavoittuvuuksista ja osaamista niiden hyväksikäyttöön
- Social Engineering -taitoja phishing-menetelmien käyttöön, valedomainien ja niissä olevien verkkosivujen toteutukseen ja infektoituneiden valedokumenttien toteutukseen

Puolustustaidot

- Työntekijöiden kouluttaminen verkkosivujen vaaroista
- Työntekijöiden kouluttaminen sähköpostihuijauksista
- Työntekijöiden kouluttaminen virustorjuntaohjelmien käyttöön
- Lokien läpikäymistaidot ja taito tunnistaa sieltä epäilyttäviä asioita
- Tuntemusta haittaohjelmien toimintatavoista, jotta saastumisen merkkejä (Indicators of Compromise; IOC) voidaan havaita.
- Reverse Engineering taidoista voi olla hyötyä, jos haittaohjelman syvällinen analyysi on tärkeää. Näin voi paljastua tarkemmin, mitä haittaohjelma tekee.

3. Pohdinta

APT:sta oli kiinnostavaa tehdä tutkimusta. Sallittu maksimisivumäärä eli 10 tekstisivua tuli helposti täyteen. Mielestämme saimme oleelliset tiedot talteen, vaikka enemmänkin tietoa olisi ollut saatavilla. Kiitos mielenkiintoisesta tehtävästä!

Lähteet

Adair, S. & Lancaster, T. 2020. OceanLotus: Extending Cyber Espionage Operations Trough Fake Websites. Volexityn verkkosivut. Julkaistu 6.11.2020. Viitattu 26.3.2021. https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/.

Advanced Persistent Threat Groups. N.d. FireEyen verkkosivut. Viitattu 27.3.2021. https://www.fireeye.com/current-threats/apt-groups.html.

APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 | MITRE ATT&CK. 2017. Mitren verkkosivut. Julkaistu 14.12.2017. Viitattu 26.3.2021. https://attack.mitre.org/groups/G0050/.

Carr, N. 2017. Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. FireEyen verkkosivut. Julkaistu 14.5.2017. Viitattu 26.3.2021. https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

Cobalt Strike. N.d. Fraunhofer-tutkimuslaitoksen malwaretietokanta. Viitattu 27.3.2021. https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike.

Dholakiya P. 2021. What Is the Cyber Kill Chain and How It Can Protect Against Attacks. Viitattu 28.03.2021. https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks

Mimikatz. N.d. Artikkeli Offensive Securityn sivuilla. Viitattu 27.3.2021. https://www.offensive-security.com/metasploit-unleashed/mimikatz/.

OceanLotus Infused Cobalt Strike to BMW and Hyundai to Control the System. N.d. Verkkoartikkeli. Viitattu 27.3.2021. https://www.linuxhelp.com/news/oceanlotus-infused-cobalt-strike-to-bmw-and-hyundai-to-control-the-system.

Why are iframes considered dangerous and a security risk?. 2014. Kysymys StackOverFlow:n verkkosivuilla. Viitattu 27.3.2021. Why are iframes considered dangerous and a security risk.