Harjoitustehtävä 08.Tietoturvaraportti

Opiskelijan nimi: Jenny
Opiskelijanumero:
Raportin nimi: Sophos threat report
Milloin raportti on julkaistu: 2022
Mistä latasit raportin: https://www.sophos.com/en-us/content/security-threat-report

1 Toimeksianto

Etsi internetistä mahdollisimman uusi tietoturvaan liittyvä raportti ja laadi siitä 2-3 sivun mittainen tiivistelmä. Lisää loppuun pohdinta osio, missä mietit raportin asioita omasta näkökulmasta sekä yritysnäkökulmasta. Voit kirjoittaa raportin suomeksi tai englanniksi (kielioppiin en takerru. olennaisinta on, että ymmärrän mitä tarkoitat). Muista merkitä raporttiin dokumentin nimi sekä osoite, mistä raportti on ladattavissa.

Hakusanat: Security report, Threat report, Internet security threat report (useimmat virustorjuntayhtiöt julkaisevat näitä vuosittain)

Palauta tiedosto Moodleen (palautuskansio 08-Tietoturvaraportti) **PDF** muodossa ja nimeä tiedosto omilla tiedoilla **opiskelijanumero_sukunimi_etunimi.pdf**

PISTEYTYS
Tehtävästä on mahdollisuus saada 10 pistettä ja pisteytyksessä huomioin seuraavat kohdat

- Dokumentissa käytetty mallipohjaa ja muotoiluja.
- Tiivistelmä raportista
- Pohdinta yritysnäkökulmasta
- Pohdinta omasta näkökulmasta
- Vapaasana kohdan ajatukset

2 Tiivistelmä raportista

Uudet uhat, kohteena linux ja LoT laitteet.

Kyberuhat ovat kokoajan muuttuva alue. Sophosin raportin mukaan, heidän tietoturvalaitteensa on havainneet malwareita windowsin käyttöjärjestelmissä lisääntyneessä määrin.
Sophos on toteuttanut useita yhteistyöhankkeita eri yrityksen sekä toimijoiden kanssa, jossa on havaittu, että haittaohjelmat ovat olleen kohdistettuna suoraan linux pohjaisiin käyttöjärjestelmiin, vuoden 2021 aikana.

Kiristyshaittaohjelmien hyökkääjät eivät ole unohtaneet linux palvelimia, jonka seurauksena vuoden 2021 aikana on havaittu kiristyshaittaohjelma nimeltä RansomEXX. Kiristyshaittaohjelman tarkoitus on kopioida linuxin rajapintaa hyökätessään windows käyttöjärjestelmää kohden.

Linux mailmassa kiristyshaittaohjelma nimeltä DarkRadiation havaittiin vuonna 2021, joka käytti pääasiana bash scriptejä. Bash scriptit ovat samanlaisia, kuin windows puolella oleva PowerShell.

DarkRadiation haittaohjelman kohteena oli yleensä Debian tai Red hat linux distrot. Haittaohjelma tarkoitus oli seurata käyttäjän liikkeitä, eli vakoilla. Sekä cryptate kaikki tärkeät tiedostot laitteelta.

DarkRadiationin pääasialliset kohteet olivat yritykset jotka myivät palveluita logistiikan tai laivateollisuudessa. Myös vuoden 2021 lopulla, havaittiin haittaohjelma myös yrityksessä joka myivät leipomotuotteita kuluttajille.

Lot laitteissa, jossa oli käytössä linux ja sen sisällä käytössä oleva ominaisuus nimeltä busybox olivat myös kohteena. Lot laitteet yleensä jäivät rauhaan kiristyshaittaohjelmasta, mutta sensijaan näihin ujutettiin yleensä cryptomainer, Eli virtuaalivaluutan laskentatyökalu. Myös joskus reitittimet olivat kohteina, jossa oli kyseinen ominaisuus otettu käyttöön valmistajan/kuluttajan puolelta.

Myös zombie haittaohjelmia havaittiin lot laitteissa, yleensä nämä saastutettiin käyttämällä oletussalasanoja sekä tietoja. Ei niinkään hyökätty muulla tavoilla.

Lot laitteissa on huono tietoturva, jonka seurauksena laitteistot ovat yleensä helppo kohde hyökkääjille. Käyttäjät eivät muuta salasanoja, eikä muitakaan oletustietoja.
Myös valmistajat eivät niinkään kiinnitä lot laitteiden tietoturvaan vuoden 2022 aikana, trendi tulee jatkumaan.

Kiristyshaittaohjelmien korkeat lunnasvaatimukset, ovat enimmäkseen rasittaneet Pohjois-Amerikkaa sekä Euroopan alueita.
Suurien lunnasvaatimuksien vuoksi monilla yrityksillä, sekä mailla ei ole varaa maksaa edes. Vaikkakin se ei ole järkevää muutenkaan, mutta tämä mahdollisuus on suoraan pois suljettu summien takia.

Yleensä tämä hyökkäykset kohdistuvat maista, joista ei saada tarpeeksi tietoa rikollisten kiinnijäämiseksi. Näin ollen viranomaiset eivät kykene antamaan sanktiota hyökkääjän tahoille tai niiden mahdollistajiin.

Vuoden 2021 aikana, US(amerikka) raportoi että Venäjän hallinnoimalla cryptovalutta pörssillä, tiedettiin että 40% heidän cryptovalutoista olivat peräisin kyberhyökkääjiltä, erinlaisista kiristyshaittaohjelmien kamppanijoista.
Eräs kiristyshaittaohjelman hyökkääjä ryhmä välttyi heille langetetuista sanktioista, muuttamalla heidän kiristyshaittaohjelmaa niin ettei voinut enää yhdistää sitä heihin. Nimenmuutokset yms.

Kryptovaluutat joita yleensä halutaan kiristyshaittaohjelmien lunnaina, on hyvä tapa tuoda lisää haastetta kyberuhkien selvittelyyn. Kryptovaluuttojen käsittely kannattaa suorittaa maassa, jossa niiden käsittely on vähiten säännöstelty ja seurattu. Joissa ei saa sanktioita niiden käytöstä.

Kryptovaluutat ovat anonyymiä valuuttaa, sitä on tosi vaikea seurata mihin se lopulta päätyy. Yleensä tämä valuutta päätyy muuhun maahan, jossa se vaihdetaan mahdollisuuksien mukaan rahaan.

3 Pohdinta yritysnäkökulmasta

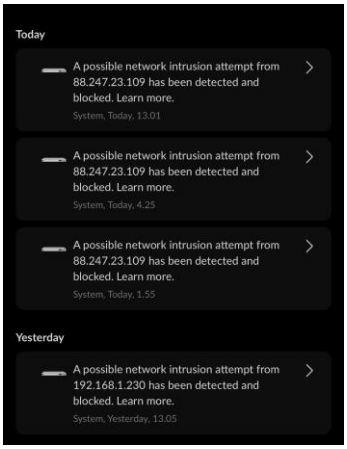
Yritysten tulee varautua erinlaisiin skenaarioihin mahdollisimman pian. Omasta mielestäni on parempi tehdä puolustus mahdollisimman hyväksi, mitä rahalla saa. Näin voidaan ennaltaehkäistä kiristyshaittaohjelmien lunnasvaatimuksia. Suomessa ei ole vielä havaittu ilmeisesti korkeita lunnaita, mutta se on varmasti ajankysymys kun kyseinen haittaohjelma pääsee yhteiskunnan kriittiseen osa-alueeseen. Jolloin lunnasvaatimukset varmasti on myös sen mukaiset.

Käyttäjät ovat yleensä ne heikoin lenkki tietoturvankanssa. Koulututa tulee järjestää säännöllisesti, ja mielellään myös kädestä pitäien. Mitä tapahtuu kun joku avaa sähköpostin kautta saapuneen liitetiedoston. Henkilökohtaisesti sellaiset tylsät luennot, jossain yrityksen toimistossa on tylsää. Työntekijät varmasti oppivat paremmin, kun pääsevät valvotussa ympäristässä oikeasti klikkailemaan erinlaisia linkkejä ja scenaarioita.

Joissain yrityksissä on käytössä myös erinlaisia lot laitteita. Niiden laitteiden tietoturvaa tulisi erityisesti tutkia, että onko ne laitteet heidän järjestelmässä se heikko lenkki.

4 Pohdinta omasta näkökulmasta

Olen pitänyt omat laitteeni asianmukaisessa kunnossa. Päivitykset asennan yleensä heti, jos työskentelyni sitä ei estä. Näin vältytään vahingoilta. Kotonani on nykyään käytössä ubiquiti järjestelmä, joka soveltuu pieneen tai keskisuureen yritykseen.
Laitteesta jää valtavasti logitietoja järjestelmään. On todella helppo huomata, että lähestulkoon jokapäivä joku kolkuttelee ovella ja yrittää tunkeutua sisään tavalla tai toisella. Myös ping kyselyt on estetty, mutta silti ovella koputellaan. (Liite havainnollistamaan hyökkäysyritykset.)



Vaikka olisi Kuinka hienot laitteet ja vehkeet omassa ympäristössä, eise estä hyökkääjän pääsyä sisälle verkkoon, jos itse olet säätänyt asetukset väärin. Vaikkakin yleensä näissä on minkälaisen palomuurit, tulee silti tietää mitä tekee. Pahimmassatapauksessa laitteellasi voi olla kiristyshaittaohjelma.

5 Vapaasana harjoitustehtävästä

Harjoitus ei itselleni aiheuttanut mitään toimenpiteitä, koska omat laitteistoni on omasta mielestäni kunossa sekä niiden asetukset.
Harjoituksessa tuli hyvin esiin, lukemalla raporttia että minkälaisia uhkia oli 2021 aikana sekä minkälaisia odotuksia vuodelle 2022 on.

Kyberhyökkäykset modernisoituvat kokoajan parempaan suuntaan, mikä tuo puolustuksenkannalta lisää haasteita. Tämä tietenkin kasvattaa ja kehittää meidän laitteistoa uuteen ulottuvuuteen.

Itse haluaisin nähdä, kuina AI koneoppiminen saadaan enemmäksi määrin mukaan hyökkäykseen sekä puolustukseen. Nyt olemassa olevat haittaohjelmat eivät käytä koneoppimista. Tulevaisuudessa, onko meillä sellainen skenaario jossa hyökkäys ja puolustus kilpailevat keskenään verkossa kumpi on parempi? Mitä tästä voisi seurata? Onko meillä kenties järjestelmä, jossa ei tarvita enää ihmistä?
On mielenkiintoista seurata mihin tämä kehittyy.