jamk.fi

Kohdeyrityksen phishing-testaus

Tuomas Siikamäki

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Siikamäki, Tuomas	Opinnäytetyö, AMK	Kuukausi Vuosi
	Sivumäärä 49	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Kohdeyrityksen phishing-testaus

Tutkinto-ohjelma

Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)

Esa Salmikangas, Jani Immonen

Toimeksiantaja(t)

Anonyymi yritys

Tiivistelmä

Opinnäytteessä tehtiin tietojenkalastelustestaus anonyymille suomalaiselle IT-alan yritykselle. Tietojenkalastelu on tapa ohittaa tekniset suojamekanismit hyväksikäyttäen ihmisen heikkouksia, hyödyntäen psykologisia ja teknisiä keinoja. Tehtävänä oli selvittää yrityksen organisaatio, henkilöstö ja verkossa olevat laitteet hyödyntäen avoimia lähteitä. Selvityksessä paljastuneiden tietojen perusteella yritykseen tehtäisiin mahdollisimman realistinen tietojenkalastelu-testaus. Rajoituksiksi sovittiin kalasteluviestien lähettäminen työntekijäksi esittäytymällä, ei oikeita haittaohjelmia, luvan kysyminen ennen toimia, eikä ketään tulisi nolata.

Tutkimus avoimista lähteistä ja tekninen valmistelu kesti noin kuukauden ja itse tietojenkalastelu toteutettiin kolmella sähköpostilla, jotka lähetettiin noin viikon sisällä. Sähköpostit lähetettiin toimitusjohtajan ja tietoturvapäällikön nimissä, lähes oikeita vastaavista sähköpostiosoitteista.

Toimitusjohtajan nimissä lähetetyissä kahdessa sähköpostissa liitetiedoston avaamisella kuvattiin haitallista liitetiedostoa, jonka avaaminen saastuttaisi tietojärjestelmät. Tietoturvapäällikön nimissä lähetetyssä viestissä kohteita pyydettiin kirjautumaan linkin takaa löytyvälle kalastelusivustolle, joka tallensi käyttäjänimen ja IP-osoitteen. Avaamisista ja tietojenkalastelusta eteenpäin raportoinnista kerättiin statistiikkaa lokitiedoista ja kyselyllä.

Viestit jäivät aluksi kiinni yrityksen tietoturvatuotteisiin, mutta testausta jatkettiin henkilöstöön ja viestit sallittiin. Testauksesta saadut tulokset noudattelivat julkisia testaustuloksia. >60 % viestin vastaajista avasi sähköpostissa olleen liitetiedoston ja 9 % yritti kirjautua kalastelusivustolle. Tehokkain tapa estää tietojenkalastelu on koulutus.

Avainsanat (asiasanat)

Tietojenkalastelu, Testaus, APT, Huijaus

Muut tiedot (Salassa pidettävät liitteet)

Liitteet 1-5 ovat salassa pidettäviä, ja ne on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.

jamk.fi

Description

Author(s)	Type of publication	Date
Siikamäki, Tuomas	Bachelor's thesis	May 2020
		Language of publication: Finnish
	Number of pages: 49	Permission for web publication: x

Title of publication

Phishing testing for a company

Degree programme

Information and Communication Technology

Supervisor(s)

Salmikangas, Esa & Immonen, Jani

Assigned by

Anonymous company

Abstract

The purpose of the thesis was to create a phishing test to a Finnish IT company. Phishing is way to pass technical security mechanics of information systems by exploiting humans' weaknesses using psychological and technical means. The objective was to gather information from employees, organization and IT infrastructure from open sources and then conduct a realistic phishing attack. The restrictions were not to impersonate anyone outside the company, not to use real malware, ask for a permission before acting and no one should be embarrassed by the test.

Information gathering and preparing for the attack took approximately a month, and phishing was conducted using three emails sent with the name of the CEO and CISO from altered domain name.

The two emails sent in the name of the impersonated to CEO had an attachment that played a malicious role. Opening the email meant compromising IT systems. The email from the CISO contained a URL to a phishing site that steals credentials. Statistics were collected from log files and phishing reports were made. Afterwards there was a poll about the test to its targets.

The company's security software caught the emails as phishing or spam; however, the emails were whitelisted so that the employees could be tested. The obtained statistics were common to a phishing test. >60 % of the employees opened attached document and 9 % entered their credentials to the phishing site. The best way to lower these numbers is to educate, test and repeat.

Keywords/tags (subjects)

Phishing, Smishing, APT, Online scam

Miscellaneous (Confidential information)

Attachments 1 to 5 that include assignee company's information are classified and removed from the public thesis. A reason for the classification is the Act on the Openness of Government Activities (621/1999) 24 § part 17. Classification time is fifteen (15) years and it ends 25.5.2035

Sisältö

Kuviot

1 Johdanto

1.1 Johdatus petoksiin

Ensimmäinen raportoitu petosyritys sijoittuu antiikin Kreikkaan 300 vuotta ennen ajanlaskun alkua, jolloin Hegestratos-niminen kauppias yritti vakuutuspetosta vakuuttaen laivansa ja rahtinsa. Tuolloin laivalastin vakuudeksi annettiin laivan ja rahdin arvo lainana kauppiaalle. Mikäli lasti tuli ehjänä perille, maksettiin laina takaisin korkoineen, ja mikäli lainaa ei maksettu, otettiin laiva ja sen rahti hallintaan. Hegestratos yritti myydä rahtina olleen maissin ja pitää lainan. Hän jäi kuitenkin kiinni upottaessaan laivaansa miehistönsä avustuksella ja hukkui yrittäessään paeta jahtaajiaan. (Cunningham 2015.)

Digitaalisen vallankumouksen myötä ihmisten, yritysten ja valtioiden viestintä ja talousasiat ovat siirtyneet verkkoon tuoden Hegestratosin kaltaiset huijarit mukanaan. Nykypäivänä huijareita löytyy yksittäisistä henkilöistä, rikollisorganisaatioista ja valtiollisista toimijoista motivaation vaihdellessa laajalla skaalalla taloudellisesta hyödystä vakoiluun ja sabotaasiin. Historiaa ja nykypäivää yhdistävät samat psykologiset seikat, joita huijarit hyödyntävät häikäilemättömästi uhrinsa luottamuksen saavuttamiseksi, sillä teknisen tietoturvan kehittyessä kovaa vauhtia on ketjun heikoin lenkki ihminen.

Internet on tuonut tullessaan myös ongelman petosten torjuntaan vahvan ja helpon anonymisoinnin vuoksi. Tämän lisäksi hyökkääjä voi sijaita fyysisesti eri maassa kuin kohde, mikä edelleen hankaloittaa virkavallan toimia rikosten torjunnassa ja selvittämisessä. Isot rikollisorganisaatiot ja valtiolliset toimijat käyttävät operaatioissaan huomattavia resursseja motivaatioidensa täyttämiseen ja lähestyvät kohteitaan yleensä kohdennetuilla kalasteluviesteillä, joiden muotoiluun on käytetty hyväksi vallalla olevia trendejä, kohteesta löydettyjä tietoja tai molempia. Vuonna 2018

päivittäin lähetettiin keskimäärin 281.1 miljardia sähköpostiviestiä (Number of sent and received e-mails per day worldwide from 2017 to 2023 2020), ja se onkin ollut pitkään käytetyin väylä tietojenkalastelulle.

1.2 Tausta, tehtävänkuvaus ja analyysimenetelmä

Opinnäytetyössä tehtiin tietojenkalastelutestaus suomalaiseen IT-yritykseen hyökkääjän silmin, eli ennalta tietämättä mitään kohteen verkkoinfrastruktuurista, organisaatiosta ja henkilöstöstä. Tavoitteena oli selvittää avoimia tietoaineistoja käyttäen ja kartoittaa yrityksen kyky puolustautua tietojenkalasteluhyökkäystä vastaan ilman taloudellisia haittavaikutuksia. Hyökkäyksessä mallinnettiin käytetyimpiä tunnettuja hyökkäysmetodeja, joita on käytetty osana kohdistettuja haittaohjelmahyökkäyksiä. Saatuja tuloksia analysoitiin kerätyn statistiikan perusteella kvantitatiivisen analyysin menetelmin ja verrattiin muihin alan tutkimuksiin. Kvantitatiivisilla menetelmillä tarkoitetaan täsmällistä matemaattista tilastointia, joka perustuu lukumääriin ja prosenttiosuuksiin (Heikkilä 2014). Kohdehenkilöstölle tehtiin testauksen jälkeinen kysely ja yritykselle jäi vertailukelpoinen tulos tuleviin testauksiin. Kysely sisälsi kysymyksiä, joista saatiin lukumääriä ja avoimesti kirjoitettuja vastauksia. Kyselyn tuloksia analysoitiin kvantitatiivisesti, sekä avoimien vastauksien osalta kvalitatiivisesti. Kvalitatiivisella analyysilla selvitetään tutkittavaa ilmiötä tutkittavan henkilön näkökulmasta (Heikkilä 2014). Kysely tuki lokitiedoista saatuja tietoja ja auttoi ymmärtämään ihmisen käyttäytymistä pelkkiä lokitietoja syvällisemmin.

1.3 Kohdeyritys

Opinnäytetyön tilannut kohdeyritys on alle sata henkeä työllistävä suomalainen IT-yritys. Yrityksessä työskentelee pääosin IT-alan ammattilaisia ja myyjiä. Yritys halusi, että liitetiedostot salataan ja nimi peitetään opinnäytetyön myötä mahdollisesti paljastuvien kiusallisten tulosten vuoksi.

2 Huijarit ennen ja nyt

Huijareita on ollut todistetusti jo antiikin Kreikan ajoilta, mutta huijareiden kulta-aika sijoittui 1800-luvun lopusta 1900-luvun alkuun. Tuolloisia huijareita voidaan pitää nykyaikaisten sosiaalisten manipuloijien esi-isinä. Historioitsija Karen Halttusen mukaan 1860-luvulla poliisi arvioi lähes yhden kymmenestä newyorkilaisesta ammattirikollisesta olevan huijareita, englanniksi heidät tunnettiin nimellä confidence man. Yhtenä tuon ajan käytetyimmästä huijauksesta oli The Glim Dropper. Siinä uhrille kaupiteltiin arvotonta tavaraa kuten esimerkiksi väärennettyjä koruja alennettuun hintaan, jolloin uhri luulee tekevänsä voittoa kaupassa. (Conheady 2014, 7-8).

Nykypäivänä huijarit pyrkivät saamaan uhreiltaan tietoa tai rahaa käyttäen apunaan sähköisiä viestimiä tietojenkalasteluun. Tietojenkalastelijat muokkaavat keinojansa maailmalla liikkuvien trendien ja tapahtumien mukaan. 2020 maaliskuussa tietojenkalasteluviesteissä nousevana teemana oli COVID-19-epidemian hyödyntäminen kohteiden ollessa terveydenhoitolaitokset, työläiset ja vasta työttömäksi jääneet (Phishing Activity Trends Report 1st Quarter 2020 2020).

Vuonna 2019 havaituista kalastelusivustoista 75 % käyttää SSL-suojausta (Phishing Activity Trends Report 1st Quarter 2020 2020). SSL-suojaus näkyy useissa selaimissa lukkona osoitekentän vasemmassa laidassa, ja sen puuttuminen antaa käyttäjälle huomautuksen tietojen salaamattomuudesta, mikä on painostanut sivustojen ylläpitäjiä ja heidän perässään kalastelijoita ottamaan SSL-suojauksen käyttöön.

Vuonna 2019 tietojenkalastelu kasvoi globaalisti 65 % ja 90 % tietomurroista johtui tietojen kalastelusta. Arviolta 1.5 miljoonaa kalastelusivustoa luodaan kuukausittain, ja yrityksistä 76 % raportoi joutuneensa tietojenkalasteluhyökkäyksen kohteeksi vuonna 2019. (Phishing and Email Fraud Statistics 2019.)

Keskimääräinen tietomurron hinta oli 3.92 miljoonaa dollaria jakautuen seuraavasti (Cost of a Data BreachReport 2019 2020):

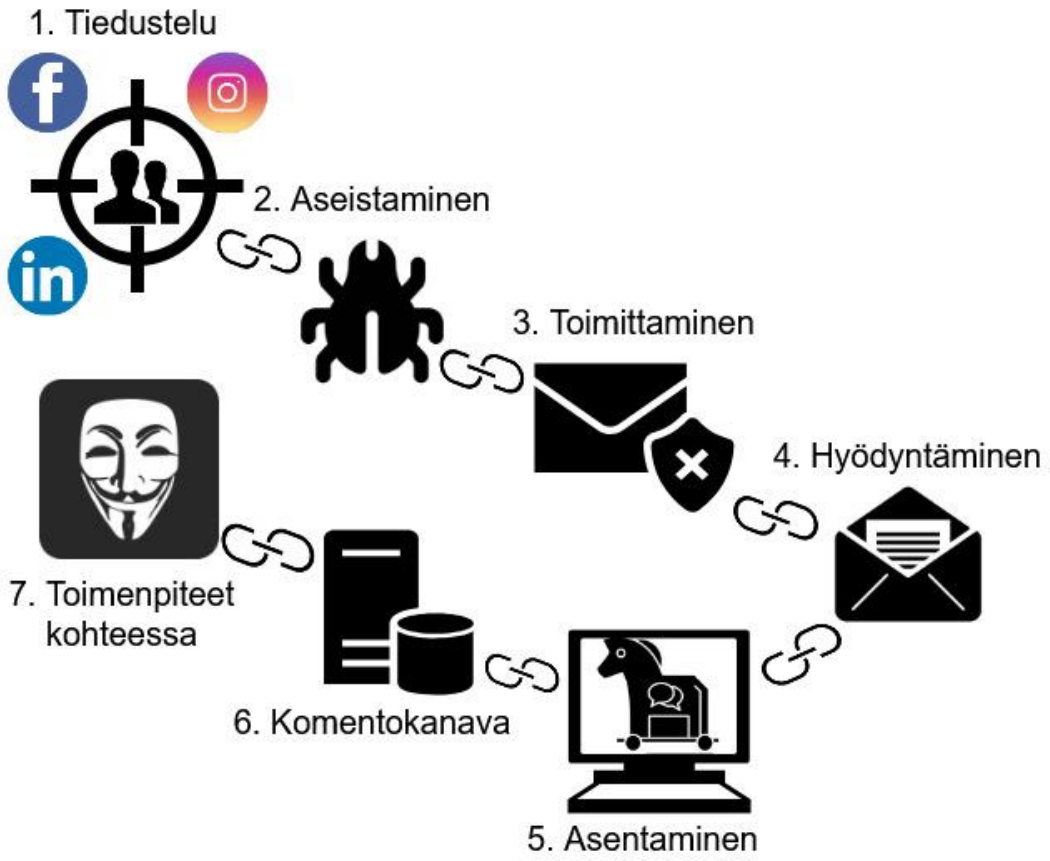
- 1.42 m$ menetettyä liiketoimintaa koostuen menetetystä myynnistä, mainehaitasta ja järjestelmien seisokeista.
- 1.07 m$ tietomurron jälkeiset toiminnat sisältävät lakitoimet, tuotealennukset, uusien tilien luonti, tukipalvelut ja sakot.
- 0.21 m$ ilmoituskulut johtuvat viranomaisille, sekä tietomurtojen kohteeksi joutuneille ilmoittamisesta.
- 1.22 m$ havaitsemisen kulut koostuvat murron analysoinnista, auditoinneista ja kriisiryhmästä.

3 Kohdistettu haittaohjelmahyökkäys

Tässä luvussa tarkastellaan tyypillistä toimintatapaa kohdistetuissa haittaohjelmahyökkäyksissä ja sitä, miten tietojenkalastelua hyödynnetään osana operaatioita. Kohdistettu haittaohjelmahyökkäys tunnetaan myös termillä APT (Advanced Persistent Threat). Termiä on käytetty kuvaamaan kehittyneitä, usein valtiollisia toimijoita, jotka pyrkivät pitkäjänteiseen toimintaan kohteessaan tavoitteidensa saavuttamiseksi. Hyökkääjillä on käytössään poikkeuksellisen kattavat taidot sekä huomattavat resurssit, joita se voi hyödyntää tavoitteidensa saavuttamiseksi. Hyökkääjä voi hyödyntää operaatioissaan useita hyökkäysvektoreita saadakseen jalansijan kohteen tietojärjestelmään. (Pols 2017.). Tietojenkalastelua voidaan pitää yhtenä hyökkäysvektorina kuten myös fyysistä pääsyä kohteeseen, jolla hyökkääjä pääsee käsiksi kohdetietojärjestelmään.

Vuonna 2019 kohdistetuissa haittaohjelmahyökkäyksissä mediaani hyökkäyksen paljastumiselle tietojärjestelmissä oli 56 päivää. Vuonna 2011 mediaani oli vielä 416 päivää. Vuonna 2019 kahdessatoista prosentissa tapauksista hyökkääjän paljastumiseen kului yli 700 päivää (M-Trends 2020).

Amerikkalaisen Lockheed Martinin laatiman Cyber kill chainin perusteella kohdistetut haittaohjelmahyökkäykset voidaan jakaa ketjumaisesti seitsemään eri vaiheeseen, joista jokaisen täytyy toteutua hyökkäyksen onnistumiseksi (ks. kuvio 1). Ketju on tehty havainnollistamaan hyökkääjän eteneminen operaationsa aikana, jolloin siltä puolustautuminen on helpompaa (Pols 2017). Yhdenkin vaiheen estäminen rikkoo ketjun ja estää hyökkääjän toimenpiteet kohdetietojärjestelmässä.



Kuvio 1 Lockheed martin. Cyber kill chain

3.1 Tiedustelu

Valmisteltaessa hyökkäystä tiedustelun tavoitteena on kartoittaa kohdeorganisaatio, henkilöt, toimintatavat ja tekninen laitteisto. Kartoittamiseen hyökkääjä voi käyttää muun muassa avoimia tietolähteitä (Open source intelligence), rekistereitä tai tietomurroissa vuodettuja tietoja. Valtiolliset toimijat voivat hyödyntää eri tiedustelulajien keräämiä tietoja kuten kuvaus-, henkilö- ja signaalitiedustelua (Johansen 2017).

Tiedustelu-vaihe tunnetaan englanniksi nimellä Recon ja se voidaan jakaa passiiviseen ja aktiiviseen tiedusteluun. Passiivinen tiedustelu ei näy kohteen tietojärjestelmissä. Sen lähteinä voidaan käyttää mm. hakukoneita, rekistereitä ja siihen tarkoitettuja ohjelmistoja. Aktiivisilla keinoilla ollaan yhteydessä kohteeseen. Näillä keinoilla voidaan vahvistaa sähköpostiosoitteiden toimivuus, hankkia kalasteluviestille uskottavuutta sähköpostin vaihdolla henkilön kanssa, jona esiinnytään myöhemmin tai käydä paikan päällä keräämässä tietoa kohteen tietojärjestelmistä ja henkilöstöstä mm. sosiaalisen manipuloinnin keinoin. Aktiivinen vaihe voi sisältää myös kohdejärjestelmiin tehtyjä haavoittuvuusskannauksia. (Bunda 2020; Pols 2017.) Haavoittuvuusskannauksella tarkoitetaan tietojärjestelmään tehtyä hakua, jolla siitä etsitään tietoturvapoikkeamia.

3.2 Aseistaminen

Aseistamisella tarkoitetaan etäkäytettävän troijalaisen ja haavoittuvuuden yhdistäminen toimitettavaan hyötykuormaan. Kasvavana trendinä on käyttää toimisto-ohjelmistojen tiedostoja kuten Microsoft Office -asiakirjoja ja PDF-tiedostoja. Tyypillisesti käytetään automatisoitua työkalua (weaponizer). (Hutchins, Cloppert, Amin 2011).

3.3 Toimittaminen

Toimitusvaiheessa välitetään hyötykuorma uhrin tietojärjestelmään usein hyödyntämällä ihmisen toimintatapoja. Hyökkääjä lähestyy yksittäistä tai useaa kohdetta sähköisellä viestimellä, tekeytyen legitiimiksi henkilöksi hyödyntäen viestin sisällössä tiedusteluluvaiheessa kerättyjä tietoja. Uhrin toimintaa pyritään ohjaamaan käyttämällä psykologisia keinoja tavoitteena saada hänet toimimaan halutulla tavalla. Psykologisia keinoja voivat olla muun muassa Auktoriteetin käyttö tuomaan henkistä painetta tai perusteltu pyynnön kiireellisyys. (Conheady 2014. 206.)

Kuvion 1 kohdassa 3 kuvattu toimittamien voidaan toteuttaa useilla eri keinoilla joita voivat esimerkiksi olla yksi tai useamman yhdistelmä seuraavissa kappaleissa kuvatuista metodeista. Metodeja yhdistämällä voidaan lisätä viestien luotettavuutta yhdistämällä esimerkiksi tekstiviestihuijaus kohdistettuun verkkourkintaan. Näitä keinoja yhdistelemällä saadaan hyökkääjän kannalta parempia tuloksia. (Pontus 2019.)

Tietojen kalastelu (Phishing) on verkkorikollisuuden muoto, jossa hyökkääjät lähettävät tekaistuja sähköposteja, jotka näyttävät tulevan luotettavasta lähteestä. Sähköpostien tarkoitus on huijata vastaanottajaa klikkaamaan haitallista linkkiä ja saada käyttäjä syöttämään luottamuksellisia tietoja valesivustolle, joka tallentaa kalastellut tiedot hyökkääjän tietokantaan. Sähköpostit voivat sisältää myös haitallisia liitetiedostoja, jotka avautuessaan saastuttavat tietokoneen haittaohjelmalla. (The Ultimate guide to Phishing. N.d.).

Aiemmin ihmiset toimivat useammin hyökkääjän haluamalla tavalla, mutta tietoisuuden kasvaessa verkkorikollisuuteen liittyen on hyökkäyksistä tullut monimutkaisempia ja hienostuneempia, jotta hyökkääjä pääsee tavoitetilaansa (The Ultimate guide to Phishing. N.d.).

Kohdistettu verkkourkinta (Spear phishing) on yksittäiseen henkilöön tai pieneen joukkoon kohdistettu hyökkäys, joka tapahtuu pääosiltaan kuten tietojenkalastelu-hyökkäys, mutta viestit ovat kohdennettua. Hyökkäyksessä hyödynnetään muun muassa sosiaalisesta mediasta ja yrityksen verkkosivuilta löytyviä tietoja, joita käytetään hyväksi personoloidun viestin kirjoittamisessa. (The Ultimate guide to Phishing. N.d.)

Vuonna 2017 tapahtuneista verkkohyökkäyksistä 65 %:ssa ensisijaisena hyökkäysvektorina oli kohdistettu verkkourkinta ja tärkeimpänä motivaationaan tiedon kerääminen. Tiedetään, että 23 % hyökkääjistä hyödynsi haavoittuvuuksia, jotka eivät ole tietoturvayhtiöden tai ohjelmistokehittäjien tiedossa eli niin sanottuja nollapäivähaavoittuvuuksia (Internet Security Threat Report 2019). Nollapäivähaavoittuvuudella tarkoitetaan tietoturvaan liittyvää heikkoutta ohjelmistossa, laitteistossa tai laiteohjelmistossa eikä siihen ole vielä korjausta tai havainnointikeinoa (Brien Posey, Sharon Shea. 2019).

Valastelu (Whaling) tai valaanpyynti tarkoittaa kohdistettua verkkourkintaa, jossa kohteena on merkittävät henkilöt kuten esimerkiksi hallituksen jäsenet tai toimitusjohtaja (Whaling phishing attacks. N.d).

Klooni kalastelu (Clone Phishing) on variaatio kohdistetusta verkkourkinnasta, jossa hyökkääjä lähettää uhrille muunnellun kopion hänen aiemmin saadusta viestistä. Viestiä on helppo erehtyä luulemaan aidoksi vastaavan jo kerran nähtyään. (Phishing attack. N.d.)

Tekstiviestihuijaus (Smishing) on tietojen kalastelua, joka hyödyntää tekstiviestejä. Tavoitteena on saada kohde antamaan arvokasta tietoa kuten PIN-koodi, luottokorttitiedot, sosiaaliturvatunnus tai avaamaan haitallinen linkki. Yleisesti ihmiset suhtautuvat epäilevästi sähköposteihin, mutta luottavat tekstiviesteihin. (What is smishing? N.d.)

Markkinointiin suunnitelluilla palveluilla kuten Sinch, voidaan lähettää teksti-, WhatsApp- tai multimediaviestejä yhdelle tai usealle käyttäjille ajastetusti siten, että lähettäjän numeron tilalla lukee tekstiä. Mikäli lähettäjänimeksi valitaan jokin kohdepuhelimessa jo oleva yhteistieto, menee lähetetty viesti viestiketjun viimeisimmäksi tehden siitä erittäin luotettavan oloisen.

Vuoden 2020 keväällä Suomessa käytettiin edellä mainittuja keinoja. Postin nimissä lähetettiin huijausviesti, joka liittyi lähetettyyn tai vastaanotettuun pakettiin. Viestissä kerrotaan muutaman euron maksusta ja ohjataan linkin maksamaan se huijaussivustolle, joka kerää luottokorttitiedot. (Postin nimissä liikkeellä huijausviestejä. 2020.)

Soittopyyntöurkinta (Vishing) tapahtuu puhelimen tai muun puheyhteyden välityksellä siten, että hyökkääjä tekeytyy toiseksi henkilöksi ja pyytää tunnuksia palveluihin tai kysyy muuta hyökkäystä tukevaa informaatiota, kuten tietokoneen käyttöjärjestelmän versiota tai virustorjuntaohjelmistoa.

3.4 Hyödyntäminen

Kun hyötykuorma on toimitettu uhrin järjestelmään, ajetaan kohdejärjestelmässä hyökkääjän koodia hyödyntäen käyttöjärjestelmässä tai ohjelmistossa olevia haavoittuvuuksia. Tällä voidaan tarkoittaa myös uhrin hyödyntämistä tai saada käyttöjärjestelmä ajamaan koodi automaattisesti. (Hutchins ym. 2011.)

3.5 Asentaminen

Etäkäytettävän troijalaisen tai takaportin asentaminen uhrin kohdejärjestelmään luo hyökkääjälle pysyvyyden järjestelmässä. (Hutchins ym. 2011.) Pysyvyys tarkoittaa sitä, että haittaohjelma säilyy kohdejärjestelmässä, vaikka se käynnistettäisiin uudelleen. Pysyvyys voidaan toteuttaa lisäämällä esimerkiksi rekisteriarvo, joka käynnistää haittaohjelman käyttöjärjestelmän käynnistyksen yhteydessä. (Karppinen 2014.)

3.6 Komentokanava

Kohdistetuissa verkkohyökkäyksissä käytettävät haittaohjelmat vaativat yleensä manuaalisia toimenpiteitä ja komentokanava mahdollistaa hyökkääjälle keinon kommunikoida etäkäytettävän troijalaisen kanssa. (Hutchins ym. 2011.). Kommunikaatioliikenne komentokanavalle pyritään piilottamaan uhrilta. Se voidaan tehdä esimerkiksi lisäämällä viestiliikenne normaalin verkkoliikenteen sisään tai lisäämällä siihen ylimääräisiä osia. (Data Obfuscation 2017.)

3.7 Toimenpiteet kohteessa

Kuuden edellisen vaiheen jälkeen hyökkääjä on päässyt kohdejärjestelmään ja voi aloittaa tiedon keräämisen, mikä on yleensä tällaisen operaation tarkoitus. Ennen tiedon kotiuttamista hyökkääjä salaa tiedostot. Hyökkääjän tavoitteena voi olla myös siirtyminen kohteen tietoverkossa lateraalisesti toisiin järjestelmiin, vaikuttaa tiedon eheyteen, luottamuksellisuuteen, saatavuuteen tai lamauttaa kohdeverkko. (Bunda 2020; Hutchins ym. 2011.)

4 Hyökkäys kohdeyritykseen

4.1 Tavoite ja rajaukset

Opinnäytetyön tavoitteena oli selvittää avoimista lähteistä kohdeyrityksen henkilöstö, verkossa olevat laitteet ja palvelimet sekä niissä mahdollisesti olevat haavoittuvuudet. Toisena tavoitteena oli suorittaa mahdollisimman realistisesti tietojenkalastelua tekeytymällä työntekijäksi ja selvittää kohdeyrityksen työntekijöiden valveutuneisuus tietojenkalasteluviesteihin liittyen. Hyökkäyksessä hyödynnettäisiin vain avoimista lähteistä löytyvää tietoa ja toimittaisiin niin sanotusti blackbox-tyylisesti, ilman sisäpiiritietoa. Yrityksen työntekijöille ei ilmoitettu meneillään olevasta testauksesta. Tekemällä tietojenkalastelutestausta kertomatta siitä kohteille, saa yritys selvän kuvan sen hetkisestä kyvystään puolustautua tosimaailman kalasteluhyökkäyksiä vastaan. Mikäli kalastelutestauksesta kerrottaisiin testattaville, painottuisi testaus koulutukselliseen aspektiin ja työntekijät pysyisivät varuillaan myös todellisia uhkia vastaan. (Hadnagy 2015.)

Hyökkäyksen aikana kerättiin statistiikkaa kohdehenkilöiden käyttäytymisestä sosiaalisessa mediassa, sekä tietojenkalasteluhyökkäyksen aikana. Hyökkäyksen jälkeen kohdehenkilöille toteutettiin kysely, jossa selvitettiin heidän kykyä havainnoida ja raportoida tietojenkalasteluhyökkäystä. Samalla selvitettiin syitä, mitkä paljastivat viestien olleen epäluotettavasta lähteestä.

Työn rajauksiksi sovittiin seuraavaa:

- Kalasteluviestien lähetys piti suorittaa tekeytymällä kohdeyrityksen työntekijäksi, jotta vältytään asiakkaiden mukaan sotkeutumiselta.
- Ennen kalasteluviestien lähettämistä pyydetään lupa tietoturvapäälliköltä.
- Sähköpostiosoitteiden ja puhelinnumeroiden oikeellisuus tarkistetaan ennen toimia.
- Kalastelluista käyttäjätunnuksista ei tallenneta salasanaa.
- Ei haittaohjelmia yritysverkkoon.
- Ketään ei nolata.

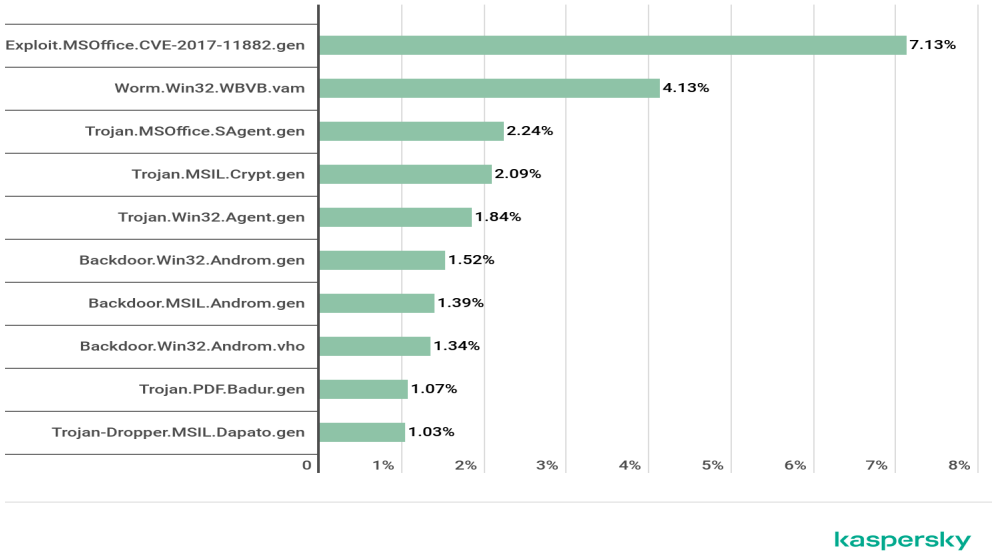
Hyökkäys toteutettiin luvussa kolme esitetyn Lockheed Martinin Cyber Kill Chainin (ks. kuvio 1) vaiheet 1–4 toteuttaen. Hyökkäys aloitettiin kohteen tiedustelulla jaotellen se henkilöstöön, organisaatioon ja tekniseen laitteistoon. Aseistamista kuvasti liitetiedoston teko, verkkotunnuksien osto, sähköpostitilien valmistelu ja myöhemmässä vaiheessa tietojenkalastelusivuston luonti. Toimittamista kuvasti sähköpostiviestit sisältäen liitetiedoston ja myöhemmässä vaiheessa linkin tietojenkalastelusivulle. Hyödyntämisessä käytettiin hyväksi Word-dokumenttia ja huonosti konfiguroitua verkkosivua, joka löytyi tiedusteluvaiheessa.

Toimitusvektoreiksi valittiin Venäjän sotilastiedustelu GRU:n alaisen hakkeriryhmä APT28:n toimintatavat, jotta testauksesta saataisiin kohdeyritykselle mahdollisimman realistiset tulokset ja samalla oppisin itse valtiollisen tason toimintatavat tietojenkalastelussa siinä määrin, kuin se olisi mahdollista opinnäytettä tehtäessä.

APT28:n toimitusvektorit olivat vuosien 2007–2016 välisenä aikana sähköpostiviestejä, joilla huijattiin käyttäjä linkin kautta väärennettyyn webmail-kirjautumisikkunaan, jolla saatiin käyttäjän sähköpostitunnukset (Kuvio 1, kohta 3. Toimitus). Tunnuksia voitiin edelleen käyttää kohdennettuihin tietojenkalasteluviesteihin tai ladata

sähköpostitilillä olleet viestit. Toinen menetelmä perustui kohteen tietokoneen saastuttamiseen sähköpostilla lähetettyyn haitalliseen liitetiedostoon tai linkkiin, joka johtaa haitalliselle sivulle. (Bunda 2020, 90.)

Vuonna 2017 paljastuneessa nollapäivähaavoittuvuudessa CVE-2017-11882 uhrin kone kyettiin saastuttamaan, mikäli hän avasi sähköpostin liitteenä olleen Word-dokumentin ilman, että hän avaa sen muokkaustilaan. Hyödyntämällä haavoittuvuutta hyökkääjä pystyi ajamaan koodia kohdekoneelle kirjautuneen käyttäjän oikeuksilla. (CVE-2017-11882. 2017; Malware campaign uses Microsoft Word without macros. 2018). Haavoittuvuuksia luetoidaan edellä nähdyn CVE-numeron mukaisesti. Ensimäinen osa kertoo havainnointi vuoden ja toinen järjestysnumeron. Vaikka kyseessä on jo vanha ja päivityksellä korjattu haavoittuvuus, se oli tietoturvayhtiö Kasperskyn mukaan eniten käytetty sähköpostin liitetiedostoissa oleva haavoittuvuus 2019 syksyn aikana (Kuvio 2.). Se, onko APT28 käyttänyt kyseistä nollapäivähaavoittuvuutta operaatioissaan, ei ole tiedossa.



Kuvio 2 Kaspersky, haittaohjelmat sähköpostien liitetiedostoissa Q3/2019 (Spam and phishing in Q3 2019. 2019).

Hyökkäyksessä simuloitiin CVE-2017-11882:n tai vastaavan haavoittuvuuden hyödyntämistä Word-dokumentilla. Kalastelijan lähettämä avattu liitetiedosto merkitsisi kohdejärjestelmän saastumista. APT28:n käyttämä käyttäjätunnusten kalastelu toteutettiin vpn-portaaliin.

4.2 Henkilöstöön ja organisaatioon kohdistuva tiedustelu

Kohdeyrityksen henkilöstöstä ja henkilöistä, joita epäiltiin kohdeyrityksen henkilöstöksi, aloitettiin keräämään Excel-taulukkoa (ks. liite 2). Taulukkoon kirjattiin titteli, nimi, sähköpostiosoite, puhelinnumero, fax, yrityksen osoitteet ja kolme saraketta lähteille.

Kohteen omilta verkkosivuilta löytyi useita sähköpostitunnuksia, viisi henkilökohtaista ja neljä geneerisempää osoitteita, kuten myynti@kohdeyritys.fi tai helpdesk@kohdeyritys.fi.

Hakukoneista käytössä olivat google, bing ja duckduckgo. Hakutuloksia pelkällä yrityksen nimellä löytyi maltillinen määrä, joten ne käytiin läpi mahdollisten uusien yhteystietojen kannalta. Tällä menetelmällä tietojenkalastelussa hyödynnettäviä yhteystietoja löytyi muutamia.

Etsimiseen voidaan käyttää myös ns. google dorksia, eli käyttää googlen edistyneempiä hakuehtoja. Exploit databasen verkkosivuilla on listattuna kirjoitushetkellä 5624 hakuehtoa, joita voi hyödyntää tiedusteluvaiheessa niin henkilötietojen kuin haavoittuvuuksienkin haussa. (Google Hacking Database 2003.)

Hakuehdolla: *filetype:pdf yrityksennimi* etsitään pdf-tiedostoja, joissa mainitaan yrityksen nimi. Hakuehdolla löytyi kaksi pdf-tiedostoa, joiden muotoilua hyödynnettiin myöhemmin uskottavan liitetiedoston luonnissa. Tiedostojen metatiedoista ei paljastunut uusia nimiä. Muita haettuja tiedostomuotoja olivat txt, doc, docx, cfg, db, dat.

inurl:file "yrityksennimi" -haulla löytyi dokumentti, jossa mainittiin asiakkuussuhde. Tätä voitaisiin hyödyntää tietojenkalasteluhyökkäyksessä tekeytymällä asiakkaaksi ja tietysti esiintymällä yrityksen työntekijänä asiakkaan suuntaan, mutta se oli rajattu pois hyökkäyskeinoista.

Kuvahaulla löytyneistä yritykseen liittyvistä kuvista ei löytynyt hyökkäykseen relevanttia tietoa, eikä metatietoa kuten kuvan omistajaa.

Rekistereistä patentti ja rekisterihallituksen maksullisesta rekisteristä varmistui yrityksen toimitusjohtaja, tilintarkastaja ja varatilintarkastaja. Toimitusjohtaja ja tietorturvapäälikkö olivat tietoisia hyökkäyksestä ja yrityksen ulkopuolisina tilintarkastajat olivat rajattu pois hyökkäyksen kohteista.

Instagramista löytyy kohteen yritystili. Tilistä ja siihen liittyvistä hashtageista listattiin kaikki tykkäykset ja seuraukset.

Facebookista löytyy kohteen yritystili. Tilistä, siihen liittyvistä kuvista ja julkaisuista listattiin kaikki tykkäykset ja seuraukset.

LinkedIn:ssa oli yli 50 % yrityksen henkilöstöstä. Heidän some-käyttäytymistä testattiin lähettämällä connect-pyyntö valeprofiililla, jolla oli suomalainen nimi, ei kuvaa ja status IT-opiskelija JAMK:ssa. Pyynnön hyväksyi vain 15 % kohdeyrityksen LinkedIn käyttäjistä, mikä vaikutti matalalle osuudelle verrattuna muiden LinkedIn -käyttäjien

käyttäytymiseen. Tämä kertoi normaalia korkeammasta tietoturvaosaamisesta kohdeyrityksessä valeprofiileihin liittyen.

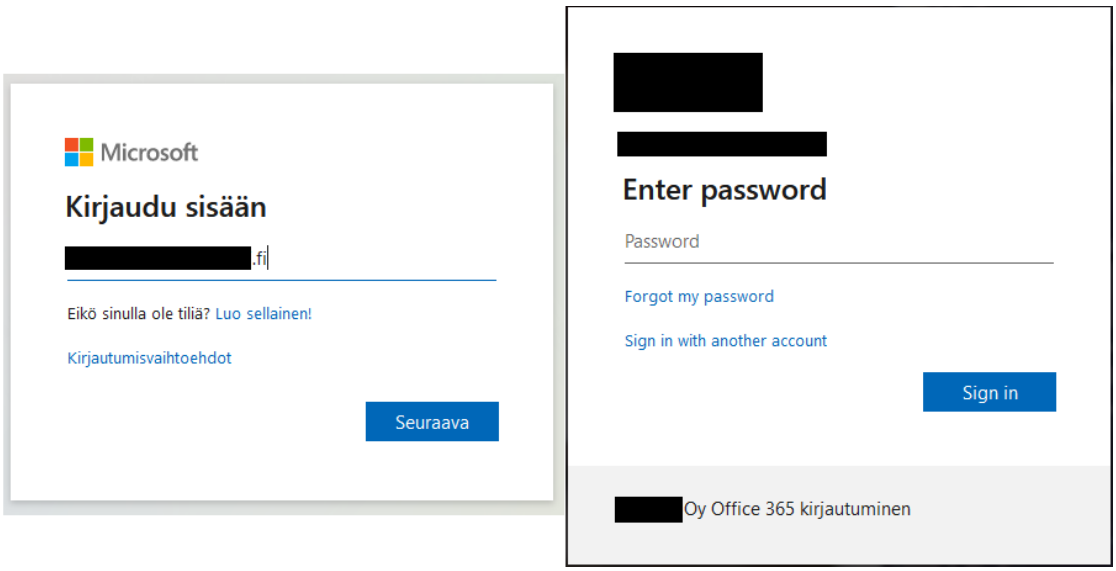
Vaikuttavana seikkana voidaan tosin pitää testauksen aggressiivista tapaa tehdä connect-pyyntöjä lähes ainoastaan kohdeyrityksen työntekijöille, sekä henkilöstön WhatsApp-ryhmässä ilmi noussutta hämmennystä profiilia kohtaan.

Steam. Kohdeyritykseltä löytyi aktiivinen e-sports -joukkue, mutta Steam-tunnuksista ei pystytytty päättelemään yksittäisiä henkilöitä eikä sähköpostiosoitteita.

Sähköpostitilit. Avoimista tietolähteistä kerätty listaus epäillyistä työntekijöistä, tykkääjistä ja seuraajista sisälsi etunimi-sukunimi yhdistelmiä, sekä @-alkuisia nimimerkkejä, joista osan oikean nimen pystyi päättelemään. Kohdeyrityksessä työskentelevät henkilöt pystyttiin vahvistamaan oikeiksi tarkastamalla, löytyykö heiltä etunimi.sukunimi@kohdeyritys.fi -sähköpostiosoite. Sähköpostiosoitteiden nimeämiskäytäntö selvisi yrityksen omilta sivuilta löytyneistä sähköpostiosoitteista.

Maltegon Verify email address exists [SMTP] -kyselyllä pystytään tarkastamaan sähköpostiosoitteiden olemassaolo, mutta se osoittautui epäluotettavaksi testattavien osoitteiden lukumäärän ollessa suuri. Kyselyyn tuli usein vääriä negatiivisia tuloksia, mikä todennäköisesti johtui sähköpostipalvelimen roskapostisuotimista.

Yrityksen kotisivuilta löytyi uutinen Microsoft Dynamics 365:n käyttöönotosta, josta oli helppo päätellä heidän käyttävän myös Microsoftin sähköpostitilejä ja sama ilmeni MX-tietueesta, joka oli muotoa *yrityksennimi-fi.mail.protect.outlook.com*. Microsoft Office 365 -sivustolla kirjautuminen toimii kaksivaiheisesti siten, että ensiksi syötetään sähköpostitili ja seuraavassa ikkunassa salasana (ks. kuvio 3).



Kuvio 3 Office 365 -kirjautuminen

Edellä mainittua kirjautumistapaa pystytään hyödyntämään, kun kartoitetaan yrityksen henkilöstöä, sillä kirjautumisikkunasta ei pääse etenemään väärällä sähköpostiosoitteella. Huomattava seikka oli myös se, että Microsoftin sallii yritykset kirjautua usealla kymmenellä sähköpostiosoitteella. Palveluita suunniteltaessa olisikin otettava edellä mainitun kaltaiset tapaukset huomioon ja tehdä kirjautumisikkunat siten, että käyttäjänimi ja salasana tulee laittaa samaan ikkunaan, eikä väärin täytettäessä kerrota oliko käyttäjänimi vai salasana väärin.

Haveibeenpwned -verkkosivusto kerää tietokantaa eri tietomurroissa vuotaneista sähköpostiosoitteista. Syöttämällä sivustolle sähköpostiosoite selviää, missä tietomurrossa sähköpostitili on ollut ja mitä tietoja on mahdollisesti vuotanut. Yleensä tallaisia tietoja ovat sähköposti, salasana ja käyttäjätunnus. Osaa tietomurtojen kohteena olleista tietokannoista myydään ja jaetaan anonyymeissä verkoissa, jolloin tietomurron aikainen salasana on muiden nähtävillä. Tästä syystä jokaisessa palvelussa tulisi olla eri salasana.

Avoimista lähteistä kerätty listaus sisälsi muutaman vuodetun sähköpostiosoite-salasana-yhdistelmän, joista yksi oli helpdeskin eli tukipalveluiden sähköpostiosoite ja loput henkilökohtaisia työsähköposteja. Yrityksen edustajia kehotettiin vaihtamaan vuodettujen tilien salasanat.

Hyökkääjä voi myös hyödyntää haveibeenpwned -tietokantoja käytettyjen ohjelmistojen ja verkkosivustojen kartoittamisessa, joita voidaan hyödyntää kalasteluviestien valmistelussa ja hyödynnettävien haavoittuvuuksien valinnassa.

Tulokset. Kohdeyrityksen henkilöstöstä pystyttiin kartoittamaan 65 % avoimia tietolähteitä hyödyntäen ja siihen pystyttiin kohdistamaan tietojenkalastelua tarvittavalla laajuudella tilastollisesta näkökulmasta. Työn rajaukset estivät syvällisen henkilöstön profiloinnin, jolloin olisi todennäköisesti löydetty muutamia osumia. Esimerkiksi vertaamalla sosiaalisista medioista vahvistettujen työntekijöiden yhteisiä kavereita. Testin päätyttyä kohdehenkilöille järjestetyssä kyselyssä vastaajista lähes kolmannes yllättyi siitä, että heidät pystyttiin yhdistämään yrityksen työntekijöiksi avoimia lähteitä hyödyntäen.

4.3 Tekniseen laitteistoon kohdistuva tiedustelu

Teknisen laitteiston kartoittamisella hyökkääjä pyrkii saamaan käsityksen kohteensa verkkoinfrastruktuurista ja sitä kautta valitsemaan itselleen järkevimmän ja usein helpoimman kohteen. Yleisesti yrityksillä on julkiseen käyttöön tarkoitetut sivut kuten yrityksennimi.fi ja mahdollisesti vekkokauppa.yrityksennimi.fi. Näiden ulkopuolelle jäävät erilaiset aliverkkotunnukset, joilla voidaan hoitaa esimerkiksi tukipalveluita, vpn-kirjautumisia tai kassajärjestelmiä, jotka hyökkääjä haluaa kartoittaa. Hyökkääjä voi valita kohteekseen epäloogiselta tuntuvan kohteen ja käyttää sitä lateraaliseen liikkumiseen yritysverkossa. Puolustautumisen kannalta tulisi kartoittaa ja miettiä hyökkääjälle helpoimmat kohteet ja vahvistaa niiden tietoturvaa.

Kaikki tekniseen laitteiseen kohdistuva tiedustelu tehtiin hyödyntäen seuraavissa kappaleissa olevia tapoja. Löydetyistä palvelimista ja verkkotunnuksista täytettiin excel-tiedostoa, (ks. liite 3) johon kirjattiin seuraavat tiedot: ASN, IP-osoite, avoimet portit, maa, organisaatio, palveluntarjoaja, tiedonkeruupäivä, DNS-nimi, tyyppi ja haavoittuvuudet. Edellä mainitut ASN, IP-osoite, portit ja DNS-nimi ovat tietoliikenneprotokollia, joilla verkossa olevat laitteet kommunikoivat keskenään (Clark 2003). Jotta opinnäytteen tilaaja pysyisi anonyyminä, esimerkeissä käytetään kohdeyritys.fi osoitetta.

Google Dorks haulla *site:https://kohdeyritsyritys.fi -inurl:www* listattiin kohdeyrits.fi -sivustot ilman www. alkuosaa. Tällaisia sivuja ovat yleensä aliverkkotunnukset, kuten verkkokauppa.kohdeyritys.fi. Sivustoilla voi kuitenkin olla verkkotunnuksia, jotka jäävät edellä mainitun haun ulkopuolelle; esimerkiksi www.verkkokauppa. kohdeyritys.fi.

Riddler on F-Securen kehittämä web-crawler, jonka avulla on helppo selvittää yrityksen internetiin avoinna olevaa infrastruktuuria (Riddler N.d). Hakutermillä *pld:kohdeyritys.fi* listattiin sen löytämiä aliverkkotunnuksia. Luomalla tunnukset palvelussa näytetyt tulokset kasvavat yli kymmeneen.

Shodan on hakukone kuten google tai bing, mutta se on tehty verkkolaitteiden etsintään. Shodan kerää jatkuvasti dataa koko IP-osoiteavaruudesta useista porteista ja palvelinten banner-tiedoista. Kerättyä dataa haetaan hakuehdoilla kuten: *http.title:"kohdeyritys"*, joka näyttää kaikki ip-osoitteet joiden takaa löytyy verkkosivu, jonka välilehden otsikkona näkyy kohdeyritys. Shodan listaa myös havaitut haavoittuvuudet. (What is Shodan? N.d.)

Sertifikaatti- ja domain tiedot eivät tarjonneet hyökkäykseen relevanttia tietoa.

DNS historiatiedoista löytyi paljon käytöstä poistettuja aliverkkotunnuksia kuten *mail.kohdeyritys.fi*.

Robots.txt on tekstitiedosto, jolla kerrotaan hakukoneille sivuista, joita niiden ei haluta indeksoivan. Robots.txt löytyy selaimella https://www.kohdeyritys.fi/robots.txt. (About robot.txt N.d.). Siellä voidaan listata esimerkiksi tulevia verkkosivuja, joita ei haluta vielä hakukoneiden avulla löytävän. Tiedosto voi tarjota hyökkääjälle hyödyllistä informaatiota. Työtä tehdessä eräälle aliverkkotunnukselle tehty robots.txt katselu päätyi Apachen virheilmoitukseen tiedoston puuttumisesta. Virheilmoitus sisälsi asennetun Apachen version ja käyttöjärjestelmän. Kyseinen Apachen versio sisälsi useita haavoittuvuuksia.

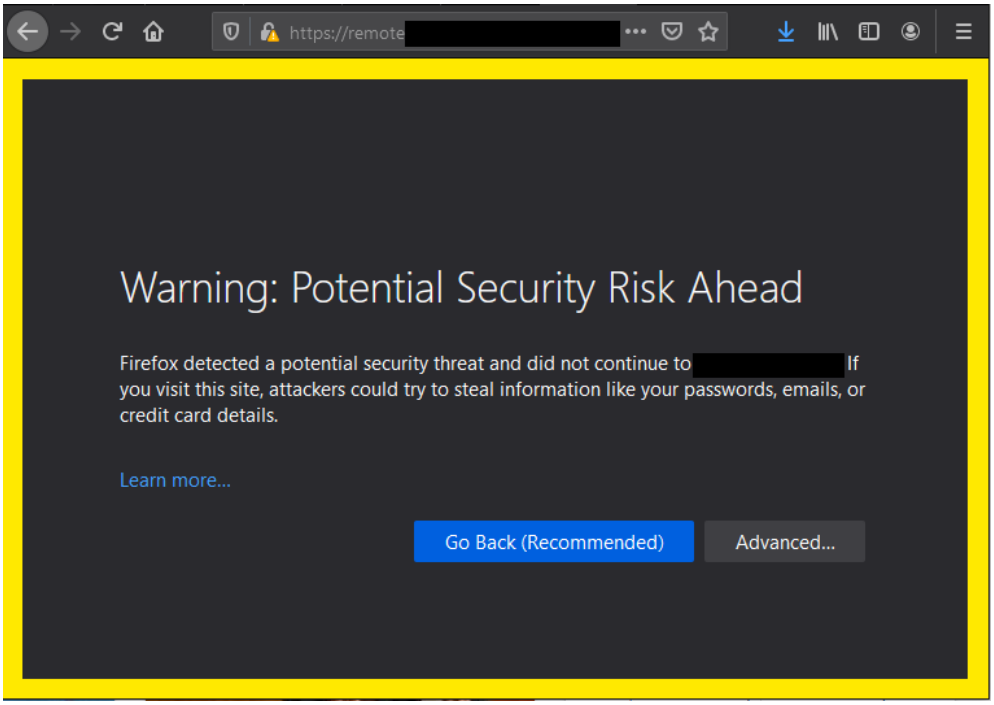
Maltego on työkalu, jolla voidaan hakea tietoa muun muassa verkkotunnuksista, sähköpostiosoitteista ja ip-osoitteista. Tulokset näytetään visuaalisesti erillisinä entiteetteinä ja entiteettien väliset relaatiot visualisoidaan linkeillä. Hakuja kutsutaan transformeiksi ja useat palveluntarjoajat, kuten Shodan, mahdollistavat API-rajapinnan käytön Maltegossa. Maltego antoi Classic-lisenssin käyttööni opinnäytteen ajaksi ja siitä oli suuri hyöty.

Tulokset. Edellä mainittuja keinoja käyttäen yrityksen verkkoinfrastruktuurista paljastui kymmeniä verkkotunnuksia ja useista niistä haavoittuvuuksia ja vääriä konfiguraatioita. Havainnot tuotiin ilmi tietoturvapäällikölle pidetyssä PowerPoint -esityksessä ja yritykselle luovutettiin havainnoista koottu excel-taulukko (ks. liite 3), sekä Maltegolla piirretty verkkokuva (ks. liite 1).

4.4 Aseistaminen (Tekninen valmistelu)

Käyttäjätunnusten kalastelu toteutettiin hyödyntämällä avoimien lähteiden kautta löytynyttä kirjautumissivustoa kohdeyrityksen aliverkkotunnuksesta.

Aliverkkotunnuksen nimi: remote viittasi VPN-tunneliin. Sivustolla oli käytössä self-signed-sertifikaatti ja se oli ulkoasultaan yksinkertainen. Sivuston self-signed-sertifikaatin takia sivustolle mennessä selain varoittaa varmentamattomasta sertifikaatista (Kuva 4), jota voimme hyödyntää hyökkäyksessä kirjautujien tiedostaessa oikean sivun ongelmat.



Kuvio 4 Varoitus self-signed-sertifikaatista

Jotta kloonatusta kalastelusivusta ja sinne johtavasta linkistä tulisi uskottava, oli hankittava lähes identtinen verkkotunnus. Metodia kutsutaan Typosquatting:ksi. Siinä ostetaan verkkotunnus, joka muistuttaa ulkoasultaan alkuperäistä, mutta kirjoitetaan tahallaan väärin. Se voi olla kirjaimien li sijaan ll tai mil rnil. (What is typosquatting? N.d.) Esimerkiksi:

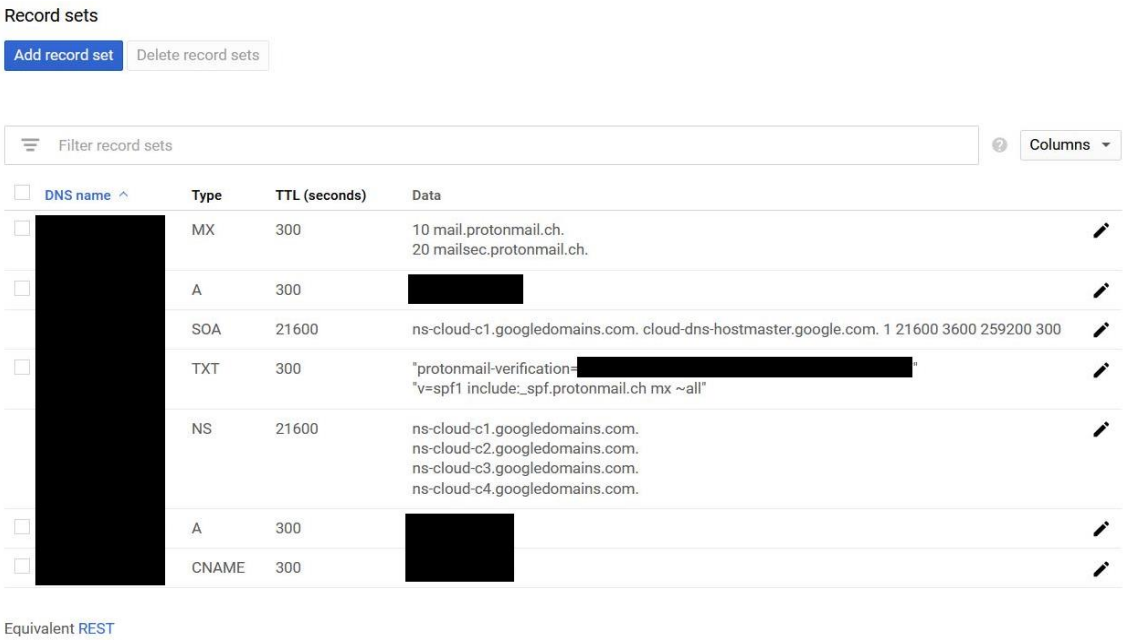
iltalehti.fi -> lltalehti.fi

mil.fi -> rnil.fi

Typosquattingiksi kutsutaan myös eri ylätasonverkkotunnuksen ostamista, jolloin verkkotunnuksen rakenne säilyy oikeana. (What is typosquatting? N.d.) Eri tahot myös varaavat ja kaupittelevat tällaisia verkkotunnuksia rahallisen motivaation ajamina, josta esimerkkinä voidaan pitää JAMK:n verkkosivuja, joiden .com päätteistä sivustoa myydään avoimesti sivustolla jamk.com alkuperäisen sivuston ollessa jamk.fi.

Verkkotunnuksen osto tapahtui hintavertailun jälkeen hostingpalvelu.fi:stä. Tietojenkalastelusivujen teko toteutettiin TrustedSecin kehittämän Social Engineering Toolkitin Credential harvester -työkalulla. Sen avulla kopioidaan uhrille tuttu kirjautumis- tai lomakesivusto. Kun verkkosivun käyttäjä täyttää kirjautumis- tai lomaketiedot ja painaa kirjaudu- tai lähetä painiketta, lähettää käyttäjä täytetyt lomakekentät tietojen kalastajalle ja käyttäjä ohjautuu oikealle kirjautumis- tai lomake -sivustolle. Käyttäjälle tämä näkyy selainikkunan päivityksenä ja lomakekenttien tyhjentymisenä. Konfiguraatio on mahdollista toteuttaa myös siten, että käyttäjä ohjataan erikseen määritetylle verkkosivustolle. Koulutustarkoituksissa tällainen sivusto voisi informoida käyttäjän erehtyneen tietojenkalastelusivulle ja tarjoavan aiheeseen liittyvän koulutuspaketin. Credential harvester konfiguroitiin siten, että käyttäjän salasanaa ei tallennettu, eikä näytetty livenäkymässä.

Ensimmäinen version sivustosta luotiin paikallisesti Kali-linux virtuaalikoneella. Sähkökatkojen, mahdollisten laitevikojen ja dynaamisen ip-osoitteen takia käytetty kalastelusivu rakennettiin Google Cloud-pilvipalveluun. Pilveen tehtävälle koneelle varattiin staattinen ip-osoite ja se liitettiin ostettuun verkkotunnukseen hyödyntäen Googlen ilmaista DNS-palvelua (ks. kuvio 5). Kalin asentamisen sijaan työssä käytettiin Docker-konttia, jotta sivuston testaus olisi ketterämpää. Sivut olivat ulkoasultaan identtiset, mutta yksi ikoni ei latautunut kaikilla selaimilla tuntemattomasta syystä. Alkuperäiset sivustot käyttivät itse allekirjoitettua ssl-suojausta, mutta kalastelusivustolle tätä ei otettu käyttöön.



Kuvio 5 Cloud DNS

Sähköpostiosoitteet tuli lähettää tekeytymällä yrityksen työntekijäksi. Protonmail kuten Microsoftin Office 365 mahdollistavat sähköpostiosoitteen liittämisen omistamaasi verkkotunnukseen. Liittäminen tapahtuu lisäämällä DNS-tietoihin TXT- ja MX-tietueet (ks. kuvio 5). Yhtenä työn rajoitteena oli asiakkaaksi tekeytyminen, joten oli tekeydyttävä kohdeyrityksen työntekijäksi. Sähköpostiosoitteet luotiin toimitusjohtajan ja tietoturvapäällikön nimiin. Molemmat sähköpostiosoitteet löytyivät nyt yhden protonmail-käyttäjätunnuksen alta ja lähettäjää pystyttiin vaihtamaan alasveto-valikosta. Sähköpostin toimivuus testattiin lähettämällä viesti luodusta sähköpostisoitteesta toiseen luotuun sähköpostiosoitteeseen. Toimitusjohtajalle ja tietoturvapäällikölle lähetettiin sähköpostia koulun sähköpostiosoitteesta, jotta saatiin selville heidän viestiensä allekirjoituksen. Valitettavasti toimitusjohtaja vastasi täysin ilman allekirjoitusta ja oli tyydyttävä epäviralliseen tapaan laittamalla pelkkä *etunimi* allekirjoitukseksi kalasteluviestin uskottavuuden parantamiseksi.

Haitallinen liitetiedosto oli tunnusten kalastelun lisäksi toinen hyökkäysvektori. Rajoitukset estivät kuitenkin oikean haittaohjelman asentamisen yritysverkkoon, joten piti keksiä toinen tapa kerätä tilastoja tiedostoa editoineista työntekijöistä. Täksi tavaksi valikoitui lähettää heille täytettävä kysely etätöihin liittyen Word-dokumentin muodossa. Täytetty kysely varmistaisi kalasteluviestin toimivuuden. Dokumentissa hyödynnettiin tiedusteluvaiheessa löydettyjen pdf-tiedostojen muotoilua ja logon sijoittelua (ks. liite 4).

4.5 Toimittaminen

Sähköpostin lähetystä testattaessa yrityksen tietoturvapäällikön kanssa, todettiin teknisten kontrollien estävän kalasteluviestit johtuen lähes identtisestä verkkotunnuksesta. Sähköpostit saapuivat muihin, kuten koulun sähköpostiin normaalisti. Jotta voisimme testata henkilöstöä, sallimme sähköpostit luoduista sähköpostiosoitteista.

Ensimmäiseksi päätettiin toteuttaa haitallisen liitetiedoston lähettäminen, sillä se olisi todennäköisesti vähemmän huomiota herättävä ja sitä kautta tuleviin viesteihin ei suhtauduttaisiin yhtä kovalla varauksella. Sähköposti lähetettiin kaikille tiedusteluvaiheessa löytyneille työntekijöille. Sähköpostin muotoilussa ja lähetyksen ajankohdassa hyödynnettiin seuraavia psykologisia seikkoja, jotka lisäsivät viestin ja lähettäjän uskottavuutta sekä saivat aikaan kiireellisyyden tunteen:

- Auktoriteetin käyttö tuomaan henkistä painetta (Conheady 2014, 206). Lähettäjäksi vastaanottajalle näkyi ylin esimies.
- Ihmisen halua auttaa (Robin 2011, 33.). Pyyntö sisälsi kolme autettavaa: esimies, työyhteisö ja vastaanottaja.
- Perusteltu pyynnön kiireellisyys (Conheady 2014, 206.). Esimies toivoi vastauksen samana päivänä. Viestien lähetysajankohta oli vappuaattona 14:10 – 14:30.
- COVID-19-viruksen aiheuttama etätyön lisääntyminen loi luontevan syyn kyselylle
- Liitetiedostossa käytettiin yrityksen logoa, värejä ja muotoilua

30.4.2020 klo: 14:10 lähetetty viesti:

Terve,

Liitteenä kysely etätöihin liittyen. Täytätkö sen vielä tänään, niin saan Vapuksi luke-mista.

-Seppo

Viestin allekirjoitus on muutettu. Kyseessä oli kohdeyrityksen toimitusjohtaja etuni-mellä.

Kyselyn vastaukset jäivät kuitenkin matkalle virheellisen DNS-konfiguraation takia. Puuttuva MX-tietue esti vastausviestien tulon perille asti ja viestiin vastaajalle tämä näkyi myöhemmin virheilmoituksena. Listaamalla lokitiedoista sähköpostiin vastan-neet, tietoturvapäällikölle ja toimitusjohtajalle vastanneet tai kalastelusta ilmoitta-neet saimme kuitenkin luotettavaa statistiikkaa kohteiden toiminnasta hyökkäyksen aikana. (ks. kuvio 6).

Kuvio 6 30.4.2020 lähetetyn viestin statistiikka

Vian selvittyä päätettiin hyödyntää tilanne, sillä 28 % vastaanottajista eivät reagoineet ensimmäiseen viestiin. Muotoiltiin viesti, jossa vastaanottajalle jäisi mielikuva siitä, että hän voisi yhä vastata vappuaattona lähetettyyn viestiin esimiehen huomaamatta myöhästymistä.

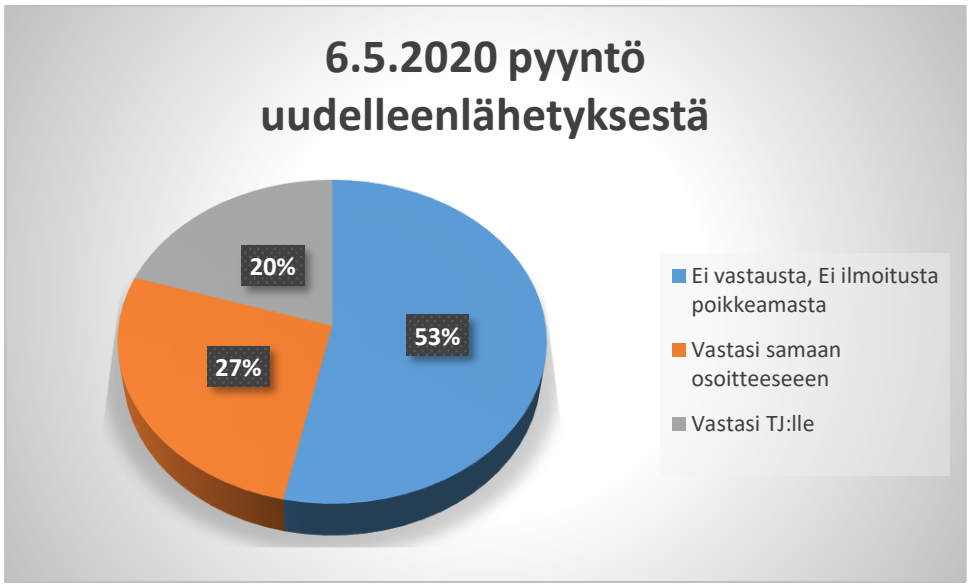
6.5.2020 lähetetty viesti

Terve,

Laitoin kyselyä tulemaan vappuaattona ja valitettavasti osa vastauksista on jäänyt matkalle Outlookin herjoista johtuen. Voisitko uudelleenlähettää torstaisen vaikkapa replynä tähän viestiin, niin katsotaan josko toimisi.

-Seppo (nimi muutettu)

Viesti lähetettiin vain henkilöille, jotka eivät olleet reagoineet aiempaan viestiin tai yrittivät uudelleen lähettää sen tekaistuun osoitteeseen, jotta työnteko keskeytyisi mahdollisimman vähän testauksen aikana. Yhdistämällä kahden sähköpostiviestin tulokset, varmistetusti noin 60 % vastaanottajista muokkasi viestin liitetiedostoa. Todellinen tulos on todennäköisesti hiukan korkeampi, sillä pieni osuus kohteista ei vastannut sähköpostiin, eikä ilmoittanut tietojenkalastelusta, mutta testauksen jälkeen tehdyssä kyselyssä osa kertoi avanneensa ja täyttäneensä kyselyn, mutta eivät lähettäneensä sitä eteenpäin.



Kuvio 7 6.5.2020 lähetetyn viestin statistiikka

Käyttäjätunnuksien kalastelu piti alun perin toteuttaa tekstiviestihuijauksella, mutta kolmen palveluntarjoajan estettyä toiminta epäiltynä tietojen kalasteluna, täytyi turvautua sähköpostilla tapahtuvaan kalasteluun. Muotoillun tekstiviestin sisältö oli lähes identtinen lähetettyyn sähköpostiin. Tekstiviestillä tapahtuvat yhteydenotot eivät ole yleisiä kohdeyrityksessä, mutta yleisesti niitä pidetään sähköposteja luotettavampina. Tekstiviestin vastaanottajalle lähettäjän nimenä olisi näkynyt tietoturvapäällikön etunimi ja sukunimen ensimmäinen kirjain.

Kolmas sähköposti lähetettiin 7.5.2020 tietoturvapäällikön nimissä apua pyytäen.

Moro,

Tein muutoksia palomuuriin. Voisitko auttaa ja käydä testaamassa, kiitos.

remote.kohdeyritys.fi

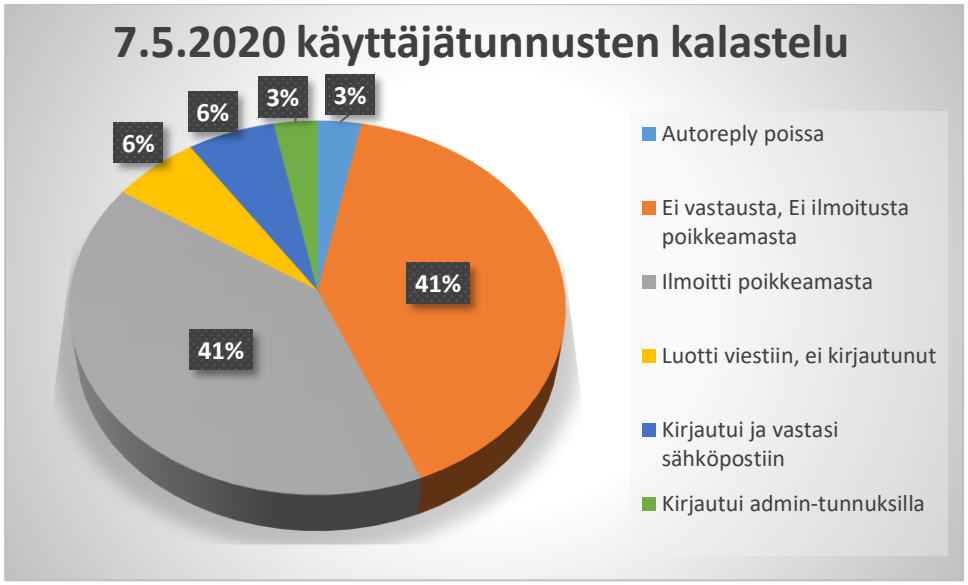
Tietoturvapäällikön allekirjoitus puhelinnumeroineen ja some-linkkeineen

Viestissä näkyvä remote.kohdeyritys.fi oli tekstiä, johon upotettu hyperlinkki johti credential harvesterilla aseistamisvaiheessa toteutetulle kalastelusivustolle *remote.kohdeyrtys.fi*. Sivustolle syötetyt käyttäjätunnukset ja ip-osoitteet näkyivät reaaliaikaisesti ja jäivät lokitiedostoon, josta alla n-merkein sensuroituna lyhyt ote.

> *84.248.nnn.nnn - - [07/May/2020 08:57:18] "GET / HTTP/1.1" 200 -*
> *directory traversal attempt detected from: 84.248.nnn.nnn*
> *84.248.nnn.nnn - - [07/May/2020 08:57:20] "GET /favicon.ico HTTP/1.1" 404*
> *[*] WE GOT A HIT! Printing the output:*
> *POSSIBLE USERNAME FIELD FOUND: fw_username=nnnn.nnnnnnn@nnnnnn.fi*
> *PARAM: fw_domain=nnnnnn.ad*
> *POSSIBLE USERNAME FIELD FOUND: submit=Login*
> *POSSIBLE USERNAME FIELD FOUND: action=sslvpn_web_logon*
> *POSSIBLE USERNAME FIELD FOUND: fw_logon_type=logon*

Kuviosta 8 selviää, että vain pieni osa syötti tunnuksensa sivustolle ja 6 % käyttäjistä ilmoitti oikealle tietoturvapäällikölle, ettei voi auttaa koska eivät omaa tunnuksia järjestelmään eli toisin sanoen he luottivat viestin sisältöön. On huomioitavaa, että sivustolle yritettiin kirjautua admin-tunnuksilla(järjestelmänvalvoja), joilla oikea hyökkääjä olisi saanut laajennetut käyttöoikeudet kohteeseen. Verrattaessa ensimmäiseen lähetettyyn viestiin on tietojen kalastelusta ilmoittaneiden osuus noussut

huomattavasti. Kappaleessa 5. Johtopäätökset käsitellään enemmän osiota: Ei vastausta, Ei ilmoitusta.



Kuvio 8 7.5.2020 lähetetyn viestin statistiikka

Tietojenkalastelusivusto oli päällä vuorokauden ja sulkemisen jälkeen. Osallistuneelle henkilöstölle jaettiin linkki Microsoft-Forms jälkikyselyyn, jota käsitellään viidennessä luvussa. Ostettu verkkotunnus, verkkokuva, tiedusteluvaiheen tulokset, Forms-kysely ja kalasteluviestien vastaukset etätöihin liittyen on luovutettu kohdeyritykselle.

4.6 Hyödyntäminen

Kun liitetiedosto avattiin kohdekoneelle, alettiin kohteelle ajamaan kuvainnollisesti hyökkääjän haittaohjelmaa. Tunnusten kohdalla tämä vaihe tarkoittaisi hyökkääjää hyödyntämässä kalasteltuja tunnuksia.

5 Testauksen tulokset

Testauksen yhtenä tavoitteena oli selvittää kohdeyrityksen verkkoinfrastruktuuri ja siinä mahdollisesti olevia haavoittuvuuksia. Yrityksen verkkoinfrastruktuurista paljastui kymmeniä verkkotunnuksia ja useista niistä haavoittuvuuksia ja vääriä konfiguraatioita. Osa verkossa olleista palveluista vaikutti unohtuneilta tai ylläpitämättömiltä. Niiden päivittäminen tai poistaminen verkosta on suositeltavaa yritykseen kohdistuvan hyökkäyspinta-alan pienentämiseksi.

Henkilöstön ja organisaation kartoitus avoimista lähteistä kattoi 65 % henkilöstöstä, joka oli riittävä määrä tietojenkalastelutestauksen toteuttamiselle. Kartoituksessa selvisi iso osa titteleistä ja organisaation rakenteesta. Kartoituksessa testattiin henkilöstön kykyä huomata valetilejä sosiaalisessa mediassa. 15 % LinkedIn:iä käyttävistä kohdeyrityksen työntekijöistä hyväksyi connect-pyynnön uskottavalta tililtä. Tämä kertoi organisaation hyvästä tietoisuudesta valetileihin liittyen.

Testin jälkeen osallistujille jaettiin linkki testauksen jälkikyselyyn, joka oli tehty Microsoft Forms ohjelmistolla (ks. liite 5). Kysely oli avoinna neljä vuorokautta ja siihen vastasi 53 % tietojenkalastelutestaukseen osallistuneista.

Yhdistämällä kahden ensimmäisen kalastelusähköpostiviestin tulokset, varmistetusti noin 60 % vastaanottajista muokkasi viestin liitetiedostoa. Todellinen tulos on todennäköisesti hiukan korkeampi, sillä pieni osuus kohteista ei vastannut sähköpostiin, eikä ilmoittanut tietojenkalastelusta. Testauksen jälkeen tehdyssä kyselyssä osa kertoi avanneensa ja täyttäneensä kyselyn, mutta eivät lähettäneensä sitä eteenpäin. Kyselyssä kysyttiin myös sitä, mikä herätti kalasteluviestin huomanneiden huomion. Suurimpina tekijöinä mainittiin väärä verkkotunnus, lähettäjän normaalista poikkeava allekirjoitus ja puuttuva profiilikuva.

Maailman suurin tietojenkalastelutestauksia tekevä yritys KnowBe4 kertoo 2018 vuoden vuosiraportissaan kohdeyritystä vastaavien yritysten PPP-luvuksi 30.68 %. Luvulla tarkoitetaan Phish-prone Percentagea, jolla kuvataan prosenttiosuutta työntekijöistä, jotka todennäköisesti ovat taipuvaisia sosiaaliselle manipuloinnille tai tietojenkalastelulle. (2018 Phishing by industry benchmarking report 2019.). Raportista ei selviä, tehdäänkö testaus koko henkilöstölle vai tämän opinnäytteen tapaisesti hyökkääjän silmin. Testauksesta saatu tulos poikkeaa huomattavasti KnowBe4:n keskimääräisestä. Tuloksia on kuitenkin mahdotonta vertailla luotettavasti, sillä testausta voidaan tehdä monilla eri tavoilla ja vaikeusasteilla.

Kolmas sähköposti, jolla kalasteltiin käyttäjätunnuksia, huomattiin edellisiä selvemmin tietojenkalasteluksi. Kalastelusta ilmoittaneiden määrä nousi 25 prosentista 41 prosenttiin. Viestiin luotti varmistetusti 15 % sähköpostin saaneista ja 9 % syötti tunnukset kalastelusivustolle. PhishingBoxin mukaan testauksissa on selvinnyt, että keskimäärin 12 % työntekijöistä avaa haitallisen linkin (Phishing Attack Test N. d.). Testissä saatu tulos on linjassa käyttäjätunnusten kalastelun osalta testausta tekevän yrityksen tulosten kanssa. Jälkikyselyn perusteella epäilykset heräsivät edellisten viestien tapaan väärästä verkkotunnuksesta, sekä väärästä henkilöstä kysymässä apua palomuurien kanssa.

Huomioitava seikka jälkikyselyssä oli, että kyselyyn vastanneista ensimmäisen viestin huomasi kalasteluksi 7 %, mutta ei ilmoittautunut asiasta eteenpäin. Toisen viestin kohdalla tulos oli 0 % ja kolmannen viestin kohdalla luku oli 50 %. Kalasteluviestit koskevat yleensä isompaa käyttäjäryhmää ja niistä olisi tärkeä ilmoittaa eteenpäin.

Jälkikyselyssä kysyttiin avointa palautetta, jossa vastaajat kertoivat suhtautuvansa jatkossa työsähköpostien avaamiseen suuremmalla varovaisuudella ja ensimmäisen viestin liitteenä ollutta kyselyä pidettiin aitona ja relevanttina maailmantilanteeseen nähden. Ilmapiiri vastauksissa oli positiivinen ja testausta pidettiin hyödyllisenä.

6 Pohdinta

Opinnäytteessä tavoitteena oli tehdä tietojenkalastelutestaus mahdollisimman realistisesti ilman lähtötietoja. Työn tilaajalle selviäisi yrityksen todellinen kyky vastata tietojenkalastelun uhkiin, jotka ovat yleensä vain osa isompaa operaatiota kuten kohdistettua haittaohjelmahyökkäystä. Työ toteutettiinkin mukailemalla kohdistetun haittaohjelmahyökkäyksen alkuvaiheita. Näkisin testauksen onnistuneen tulosten ollessa alan yritysten tulosten mukaisia tai parempia hyökkääjän näkökulmasta asiaa tarkastellen.

Henkilökohtaisena tavoitteena oli oppia tietenkin syvällisesti tietojenkalastelijoiden toimintatavat ja perusteet valtiollisten toimijoiden tavoista. Aihe on erittäin relevantti kyberturvallisuuteen liittyen, mutta sitä vain sivuttiin muutamalla opetussuunnitelman opintojaksolla. Kalasteluun liittyy myös psykologinen aspekti, jonka opiskelu oli erittäin mielenkiintoista. Työn valmistelu alkoi perehtymällä alan kirjallisuuteen muiden töiden ohessa noin vuosi ennen kohdeyrityksen valintaa. Opinnäytetyössä teoriassa opitut asiat saatiin siirrettyä käytännön toteutukseen, kalasteluhyökkäykseen. Julkisen raportin kirjoittamista hankaloitti kohdeyrityksen peittäminen, sillä esimerkiksi kuvia Shodanista ja Maltegosta ei voinut hyödyntää ja lukujen tilalla piti käyttää prosentteja.

Kohdeyrityksessä tietoturvapoikkeamat ilmoitetaan vain tietoturvapäällikölle. Testissä ensimmäinen ilmoitus kalasteluviestistä tuli tietoturvapäällikölle noin kahdessa minuutissa. Hän ei kuitenkaan voi olla tavoitettavissa ympäri vuorokauden ja kun viestien kohteena saattaa olla laaja joukko, on nopeus varoittamistoimissa valttia. Mikäli ilmoitukset olisivat tulleet koko henkilöstölle, olisi testin tulos ollut todennäköisesti aivan eri luokkaa. Testaustuloksia lukeneena tietojenkalastelun epäonnistuminen on erittäin epätodennäköistä. Vaikka yritykseen kohdistunut kalasteluyritys

huomattaisiin nopeasti, tulisi tietojärjestelmissä aloittaa toimet mahdollisten tunkeutujien ja haittaohjelmien varalta.

Opinnäytteen tuloksia ei tule verrata muihin maailmalla tehtyihin testeihin, vaan pitää sitä niin sanottuna lähtötason testinä. Henkilöstöä tulisi kouluttaa ja järjestää uusia testauksia sykleittäin. Tulevat testaukset tulisi ulottaa koskemaan koko henkilöstöä, sillä myös tässä testissä löytymättömät henkilötiedot voivat päätyä hyökkääjän postituslistalle.

Osa kohdeyrityksen henkilöstöstä ei raportoinut tapauksia, vaikka huomasi ne kalasteluviesteiksi. On huomioitavaa, että kalasteluviesteistä tulisi ilmoittaa, vaikka epäilee vahvasti niiden olevan sisäistä koulutusta, jottei päädytä tilanteeseen, jossa oikea kalasteluviesti menee tarkkojen silmien läpi koulutusaiheisena kalasteluviestinä vaarantaen yrityssalaisuudet.

Edellä mainittua tilaa voi verrata englanniksi kutsuttuun *Boy who cries wolf* -hyökkäykseen, jossa brittiläisen Kolumbian yliopiston antropologian museon valvontakamerat sammuivat muutama tunti ennen murtoa ja vartijat saivat puhelun olla piittaamasta hälytyksistä. Sinä yönä museosta varastettiin kahden miljoonan dollarin arvosta taide-esineitä. (Conheady 2014, 6.)

Ajantasaiset päivitykset ja tietoturvaohjelmistot estävät suurilta osin haittaohjelmien uudelleenkäytön, mutta kalastelun estämiseksi tekniset ratkaisut toimivat vain osittain. Yrityksellä käytössä olleet tietoturvakontrollit estivät samankaltaisesta verkkotunnuksesta tulleet kalasteluviestit, mutta mikään ei estä edistynyttä hyökkääjää tekeytymästä asiakkaaksi yleisen sähköpostiosoitteen kuten gmail:n avulla. Yrityksille ja työntekijöille on suuri kynnys lähteä tarkastamaan sähköpostien oikeellisuutta. Ratkaisuna tähän voisi olla verkkosivuilta löytyvä yhteyskaavake, johon asiakas ohjattaisiin kuvaamaan ongelmat. Toinen mahdollinen keino olisi käyttää vahvaa

tunnistautumista kuten pankkitunnuksia, joilla asiakas pakotettaisiin kirjautumaan tiketöintijärjestelmään, sillä kalastelija haluaa pysyä anonyyminä.

Järjestettäessä tietojenkalastelutestausta tulee pohtia myös sen eettisyyttä. Tehtäessä testejä saadaan todennäköisesti suurempia joukkoja avaamaan sähköpostit, mikäli sisältö on kohdetta koskettavaa ja mahdollisesti shokeeraavaa. Tällainen voisi olla vaikkapa ilmoitus irtisanomisesta tai yt-neuvotteluista. Edellä mainitut viestit voivat kuitenkin aiheuttaa suurta henkistä kärsimystä ja viestien sisältöä tulisi tarkoin pohtia ja pyytää siitä yrityksen edustajan mielipide.

IT-alan yritysten henkilöstö koostuu karkeasti jaoteltuna johtavasta, kaupallisesta ja suorittavasta osasta. Yleisesti olettaen taitotaso tietoturvapoikkeamien havaitsemiseen on korkein suorittavalla tasolla, joka koostuu IT-alan ammattilaisista. Eniten näkyvillä olevat johtavat ja kaupalliset henkilöt ovatkin ensisijaisia kohteita hyökkääjille kohdistetuissa kalasteluviesteissä. Testaus tulisi järjestää eri vaikeustasoilla taitotasojen mukaisesti, jotta mahdollisimman monelle tulisi onnistumisen tunne, joka ruokkisi motivaatiota opiskella turvallisia toimintatapoja.

Lähteet

2018 Phishing by industry benchmarking report. 2019. KnownBe4 raportti tietojenkalastelutestauksesta. https://www.ciosummits.com/KnowBe4-Phishing-By-Industry-Benchmarking-Report.pdf

About robots.txt N.d. Artikkeli googlen verkkosivuilla. Viitattu 25.5.2020 https://support.google.com/webmasters/answer/6062608?hl=en

Bunda J. 2020. Pro-gradu. APT28, Tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007 – 2017. Jyväskylän yliopisto: Informaatioteknologian tiedekunta.

Brien Posey, Sharon Shea. 2019. Artikkeli Techtargetin verkkosivuilla. Viitattu 7.5.2020 https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

Clark, M. 2003. Data Networks, IP and the Internet: Protocols, Design and Operation. Sussex: Wiley.

Conheady, S. 2014. Social Engineering in IT Security. New York: Canveo publisher services.

Cost of a Data BreachReport 2019. 2020. IBM Securityn vuosiraportti tietomurroista. Viitattu 18.5.2020. https://databreachcalculator.mybluemix.net/executive-summary

Cunningham, I. 2015. Artikkeli petoksista YourMoneyn verkkosivuilla. Viitattu 15.5.2020 https://www.yourmoney.com/credit-cards-loans/a-history-of-fraud-through-the-ages-and-how-to-avoid-being-a-victim/

CVE-2017-11882. 2017. Konseptitodistus haavoittuvuuden käytöstä githubissa. Viitattu 20.5.2020. https://github.com/embedi/CVE-2017-11882

Data obfuscation. 2017. Artikkeli komentopalvelimen liikenteen piilottamisesta Mitren verkkosivuilla. Kirjoitettu 31.5.2017. Viitattu 25.5.2020. https://attack.mitre.org/techniques/T1001/

Dreeke, R. 2011. It's not all about me. The top then techniques for building quick rapport with anyone. USA: CPSIA

Google Hacking Database. 2003. Listaus Google dorks komennoista Exploit-db:n verkkosivuilla. Viitattu 25.5.2020. https://www.exploit-db.com/google-hacking-database

Hadnagy, C. 2015. Phishing dark waters: The offensive and defensive sides of malicious e-mails. Indiana: John Wiley & Sons.

Hadnagy, C. 2018. Social engineering, The science of human hacking. Indiana: John Wiley & Sons.

Heikkilä, T. 2014. Kvantitatiivinen tutkimus. Viitattu 24.5.2020 T. http://tilastollinentutkimus.fi/1.TUTKIMUSTUKI/KvantitatiivinenTutkimus.pdf

Hutchins E, Cloppert M, Amin R. 2011. Intelligence-Driven Computer Network DefenseInformed by Analysis of Adversary Campaigns andIntrusion Kill Chains.

Internet Security Threat Report, Symantec. 2019. Symantecin vuoden 2019 uhkaraportti. Viitattu 21.5.2020 https://docs.broadcom.com/doc/istr-24-2019-en

Johansen, G. 2017. Digital Forensics and Incident Response. Mumbai: Packt.

Karppinen, T. 2014. Pro gradu -tutkielma. Haittaohjelmat ja niiden analyysi. Jyväskylän yliopisto: Tietotekniikan laitos.

Malware campaign uses Microsoft Word without macros. Artikkeli SpamTitanin verkkosivuilla. Julkaistu 16.2.2018. Viitattu 7.5.2020. https://www.spamtitan.com/blog/malware-microsoft-word-without-macros/

M-Trends 2020. 2020. FireEyen erikoisraportti. Viitattu 21.5.2020 https://content.fireeye.com/m-trends/rpt-m-trends-2020

Number of sent and received e-mails per day worldwide from 2017 to 2023. 2020. Artikkeli lähetetyistä sähköposteista statistan verkkosivuilla. Viitattu 25.5.2020. https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

Phishing Activity Trends Report 1st Quarter 2020. 2020. Anti-phishing working group:n neljännesvuosiraportti tietojenkalastelusta. Viitattu 14.5.2020 https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

Phishing and Email Fraud Statistics 2019. Retrusterin verkkosivut. Viitattu 15.5.2020. https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

Phishing attack. N.d. Artikkeli Rapid7:n verkkosivuilla. Viitattu 17.5.2020. https://www.rapid7.com/fundamentals/phishing-attacks/

Phishing Attack Test. N.d. Artikkeli testauksesta phishingboxin verkkosivuilla. Viitattu 24.5.2020. https://www.phishingbox.com/phishing-attack-test

Pols, C. 2017.The Unified Kill Chain. Opinnäyte. Cyber Security Academy. https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Pontus. 2019. Tekstiviestit sähköpostiperustaisen tietojenkalastelun tehokeinona. Opinnäytetyö. https://www.theseus.fi/handle/10024/173291

Postin nimissä liikkeellä huijausviestejä. Postin verkkosivut. Julkaistu 23.3.2020. Päivitetty 23.4.2020. Viitattu 5.5.2020. https://www.posti.fi/private-news/tiedotteet/2020/20200323_huijausviestit_ohjeet.html

Riddler. N.d. Riddlerin infosivut. Viitattu 25.5.2020. https://riddler.io/about

Spam and phishing in Q3 2019. Osavuositilasto Securelistin verkkosivuilla. Julkaistu 23.10.2019. Viitattu 16.5.2020 https://securelist.com/spam-report-q3-2019/95177/

The Ultimate guide to Phishing. N.d. The Ultimate guide to Phishing. MetaCompliance. Viitattu 21.5.2020 https://www.metacompliance.com/resources/ultimate-guide-to-phishing/

Whaling phishing attacks. N.d. Artikkeli Rapid7:n verkkosivuilla. Viitattu 17.5.2020. https://www.rapid7.com/fundamentals/whaling-phishing-attacks/

What is Shodan? 2020. Artikkeli Shodanin verkkosivuilla. Viitattu https://help.shodan.io/the-basics/what-is-shodan

What is smishing? N.d. Artikkeli Nortonin verkkosivuilla. Viitattu 5.5.2020. https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

What is typosquatting? N.d. Artikkeli UpGuardingin verkkosivuilla. Viitattu 5.5.2020. https://www.upguard.com/blog/typosquatting

Liitteet

Liite 1. Verkkokuva

Liite on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.

Liite 2. Tiedustelun-tulokset

Liite on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.

Liite 3. Havaitut haavoittuvuudet

Liite on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.

Liite 4. Kysely.docx

Liite on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.

Liite 5. Testauksen jälkikysely

Liite on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon perusteena on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n kohta 17: yrityksen liike-tai ammattisalaisuus. Salassapitoaika on viisitoista (15) vuotta. Salassapito päättyy 25.5.2035.