Tampereen yliopisto

Vesa Palomäki

INHIMILLINEN RAJAPINTA KYBERHYÖKKÄYKSISSÄ

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Marraskuu 2023

TIIVISTELMÄ

Vesa Palomäki: Inhimillinen rajapinta kyberhyökkäyksissä
Kandidaattitutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan tutkinto-ohjelma
Marraskuu 2023

Kyberrikollisuus on tilastojen mukaan kasvava ongelma sekä hyökkäysten määrässä että rahallisessa arvossa mitattuna. Internetin alkuajoista lähtenyt kilpajuoksu hakkerien ja tietoturvaratkaisujen välillä jatkuu edelleen. Teknisen tietoturvan huima kehitys on kuitenkin johtanut siihen, että rikollisten kohteeksi on kasvavassa määrin noussut laitteita ja ohjelmistoja käyttävä ihminen. Myös tiedeyhteisö ja tilastot tukevat käsitystä, että ihminen on tietoturvan heikoin lenkki.

Tämä tutkielma on kirjallisuuskatsaus, jossa tutkimuksen lähdemateriaalina on käytetty tieteellisiä artikkeleita, konferenssijulkaisuja ja kirjoja. Lähdemateriaaliksi on valikoitu sekä teoreettista että käytännön näkökulmaa ja tietämystä lain molemmilta puolilta. Päätavoitteena on aiempien tutkimusten pohjalta selvittää, mitä ihmiseen kohdistuviin kyberhyökkäyksiin sisältyy ja mitkä ovat ne tekijät, jotka vaikuttavat hyökkäyksien onnistumiseen. Fokus on tuossa inhimillisessä rajapinnassa kyberrikollisen ja hyökkäyksen kohteen välissä. Päätavoitteet on saavutettu tutkimalla käyttäjän manipulaatio- ja tietojenkalasteluhyökkäyksiä vaiheittain läpi. Apuna on käytetty kolmea tutkimuksen aikana löytynyttä mallia: ontologinen malli käyttäjän manipulaatioon, järjestelmällisen käyttäjän manipulaatio -hyökkäyksen malli ja tietojenkalastelun elinkaaren malli.

Tutkimuksessa löytyi kaksi ihmiseen kohdistuvaa hyökkäysmuotoa: käyttäjän manipulaatio ja tietojenkalastelu. Molemmissa hyökkäysmuodoissa rikollinen yrittää manipuloida kohteensa tekemään inhimillisen virheen, jonka avulla rikollinen saa luvattoman pääsyn salaisiin tietoihin. Manipulaation onnistuminen on hyökkäyksen tärkein osa. Tämän tutkimuksen mukaan kaksi keskeisintä manipuloinnin työkalua ovat suostuttelukeinot ja peitetarina. Hyökkäys on tehokkaimmillaan, kun suostuttelukeinot, peitetarina ja hyökkäyksen tavoite ovat linjassa toistensa kanssa ja pohjautuvat hyökkäyssuunnitelmaan, joka on tehty riittävän tiedonkeruun perusteella.

Avainsanat: Käyttäjän manipulaatio, tietojenkalastelu, kyberhyökkäys.

SISÄLLYSLUETTELO

KÄSITTEET

APWG	Anti-Phishing Working Group
BKT	Bruttokansantuote
Kohde	Hyökkäyksen kohde
Kyberrikollinen	Tietoverkkoja apuna käyttävä rikollinen
Kyberrikos	Tietoverkkosidonnainen rikos
Phishing	Tietojenkalastelu sähköpostilla
Rikollinen	Kyberrikollinen (tämän tutkielman yhteydessä)
Smishing	Tietojenkalastelu tekstiviestillä
Social Engineering	Käyttäjän manipulaatio
Spear Phishing	Kohdistettu tietojenkalastelu
Tunnistetiedot	Käyttäjätunnus ja salasana, SoTu
Vishing	Tietojenkalastelu äänipuhelulla
Whaling	Kohdistettu tietojenkalastelu korkean profiilin kohteeseen

1. JOHDANTO

Internet on yksi suurimmista askeleista ihmisen kehityksen varrella. Internetin alkuajoista on vielä sen verran vähän aikaa, että suuri osa väestöstä ei ole oppinut sitä täysin sisäistämään tai käyttämään, eikä myöskään varautumaan internetin mukana tuleviin vaaroihin. Siitä huolimatta monet tärkeät tahot kuten pankit ja julkisen sektorin laitokset ovat uudistaneet tieto- ja kommunikaatiokanaviaan sekä palveluitaan uuden teknologian piiriin. Tämän seurauksena myös haavoittuvaisempi osa väestöstä on joutunut pakon edessä liittymään osaksi nykypäivän tietoverkkoa.

Kaiken positiivisen kehityksen ja mahdollisuuksien lisäksi Internet on avannut uusia keinoja myös rikollisiin toimiin. Samaan aikaan kun yritykset parantavat kyberturvallisuuttaan ja kouluttavat työntekijöitään, myös rikolliset kehittävät uusia ja tehokkaampia keinoja kyberhyökkäyksille. Laitteistojen ja ohjelmistojen tietoturva on kehittynyt huimasti Internetin alkuajoista. Tämä kehitys on jatkuva prosessi, joten vaatimukset tietoturvan läpäisemiseen kasvavat jatkuvasti. Tämän seurauksena helpommaksi murtautumiskohteeksi on osoittautunut näitä laitteita käyttävä ihminen.

Tunnettu entinen kyberrikollinen Kevin Mitnick totesi 2002 Simonin kanssa julkaisemassa kirjassa, että yritys on voinut ostaa parhaan mahdollisen teknisen turvan ja yrityksen henkilökunta voi noudattaa kaikkia asiantuntijoiden suosittelemia turvallisuuskäytäntöjä, mutta silti yritys on täysin haavoittuvainen. Tuolla haavoittuvaisuudella hän tarkoittaa ihmistä. [1, luku 1]

Tutkimusyhteisössä vallitsee yksimielisyys siitä, että ihminen on tietojärjestelmän heikoin lenkki. Ghafir et al. ennustavat vuoden 2016 tutkimuksessaan, että inhimillisten haavoittuvuuksien hyödyntämisen käyttämällä tietojenkalastelun tekniikoita nähdään tulevaisuudessa olevan suurin uhka tietojärjestelmien turvallisuudelle. [2]

Chamorro-Premuzic puolestaan toteaa 2023 julkaistussa artikkelissaan, että suurin kyberturvallisuus uhka on inhimillinen virhe, joka kattaa yli 80 % kaikista tapauksista. Tämä siitä huolimatta, että tietoturvaan on kokonaisvaltaisesti panostettu viime vuosikymmenen aikana huimasti. Chamorro-Premuzic:n mukaan kyberrikollisuuden vaikutusten odotetaan nousevan tänä vuonna 10 biljoonaan euroon, joka ylittää Yhdysvaltoja ja Kiinaa lukuun ottamatta kaikkien maiden BKT:n. Hän myös toteaa, että luvun arvioidaan kaksinkertaistuvan seuraavan neljän vuoden aikana. [3]

Tämä tutkielma on suoritettu kirjallisuuskatsauksena, jossa on selvitetty, mitä tiedeyhteisö on tuonut esille aihepiiriin liittyen. Tutkielman päätavoitteena oli tutkia rajapintaa kyberrikollisen ja hyökkäyksen kohteen välillä ihmiseen kohdistuvassa kyberhyökkäyksessä. Tutkimus on keskittynyt tekijöihin, jotka vaikuttavat rikollisen toiminnan onnistumiseen tuon inhimillisen rajapinnan läpi. Aihetta tutkitaan rikollisen perspektiivistä.

Tutkimuksessa löytyi kaksi ihmiseen kohdistuvaa kyberhyökkäyksen muotoa: käyttäjän manipulaatio ja tietojenkalastelu. Tiedeyhteisössä näiden käsitteiden määritykset eivät ole täysin vakiintuneita. Varsinkin käyttäjän manipulaatiolle löytyi useita tulkintoja. Tämän tutkielman toisena tavoitteena oli luoda selkeät rajat näille käsitteille ja selkeyttää myös niiden suhdetta toisiinsa.

Tutkielman tavoitteet on saavutettu tutkimalla käyttäjän manipulaatio- ja tietojenkalasteluhyökkäyksien rakennetta ja vaiheita. Apuna on käytetty kolmea tutkimuksen aikana löytynyttä mallia: ontologinen malli käyttäjän manipulaatioon, järjestelmällisen käyttäjän manipulaatio -hyökkäyksen malli ja tietojenkalastelun elinkaaren malli.

Käyttäjän manipulaatiota ja tietojenkalastelua tapahtuu jatkuvasti laillisesti monessa eri muodossa. Tässä tutkielmassa on keskitytty ainoastaan rikolliseen toimintaan. Tietojenkalastelun yhteydessä työtä on rajattu tekijöihin, jotka vaikuttavat hyökkäyksen onnistumiseen inhimillisen rajapinnan läpi. Tutkielmaan sisältyy näin ollen käyttäjää manipuloiva tietojenkalastelu ja tutkielman ulkopuolelle jää teknisempi puoli tietojenkalastelusta kuten verkkosivupohjaiset huijaukset ja haittaohjelmat.

2. TUTKIMUSMENETELMÄT

Tämä tutkielma on tehty kirjallisuuskatsauksena. Tarkoituksena on ollut selvittää, mitä aikaisemmat tutkimukset ovat löytäneet aihealueesta. Tutkielman lähdemateriaalina on käytetty tieteellisiä artikkeleita, konferenssijulkaisuja ja kirjoja. Lähdemateriaalien hakeminen on suoritettu pääasiassa Tampereen yliopiston tarjoaman Andor -hakupalvelun avulla. Andorin avulla on löydetty seuraavat lähteet: [1], [2], [5], [6], [7], [9], [11] ja [13].

Hakuja on suoritettu seuraavilla parametreillä:

- Päähakusanat: ”Social Engineering”, Phishing.
- Rajaavia hakusanoja: Attack, Penetration, Defence, Protect*, Detect*, Prevent*, Security, Mitigation.
- Esimerkki hakulauseesta: (”Social Engineering” OR Phishing) AND (Defence OR Protect* OR Detect* OR Prevent* OR Security OR Mitigation).

Lisäksi hakuihin on käytetty seuraavia rajauksia: ”Saatavilla verkossa”, ”Vertaisarvioidut lehdet” ja Vuosi -rajausta. Kohtuuttoman suuria hakutulosten määriä on karsittu rajaavien hakusanojen lisäksi Vuosi -rajauksella. Ennen karsintaa on kuitenkin tarkastettu relevanteimmat hakutulokset.

Hakutulosten valikoinnissa on ensimmäisenä luettu hakutuloksen otsikko ja tiivistelmä. Jos lähde on näiden perusteella vaikuttanut lukemisen arvoiselta, on se valittu potentiaaliseksi lähteeksi. Potentiaaliset lähteet on säilytetty, kunnes ne ovat joko valikoituneet käytettäviksi lähteiksi tai niistä on luovuttu.

Hakujen lisäksi lähteitä on etsitty jo käytettäviksi lähteiksi valittujen lähteiden lähdeluetteloiden avulla. Jos samaan lähteeseen on viitattu useassa tutkimuksessa, on kyseinen lähde yritetty löytää lähempään tarkasteluun. Lähteet [4] ja [8] on löydetty tällä menettelyllä. Tilastollisen tiedon etsimiseen on käytetty Googlea. Tarkoituksena on ollut löytää mahdollisimman tuore ja luotettava lähde. Googlen avulla on löytynyt lähde [3].

Kaikki lähteet on tarkastettu julkaisufoorumissa. Luokituksen 2 saivat [1], [7], [9], [11] ja [13]. Luokituksen 1 saivat [6] ja [8]. Luokituksen 0 saivat [2] ja [5].

3. KÄYTTÄJÄN MANIPULAATIO

3.1 Termin historiaa ja määritelmä

Tämän tutkielman keskeisin käsite on englanninkielinen termi *social engineering*, joka on yleisesti suomennettu muotoon käyttäjän tai henkilön manipulaatio. Käsitettä on käytetty tässä tutkielmassa muodossa käyttäjän manipulaatio.

Käyttäjän manipulaatio terminä alkoi yleistyä 1990-luvulla. Englanninkielistä termiä on käytetty ensimmäistä kertaa jo 1980-luvun lopulla tietoturvallisuuden aihealueella. Silti vielä v.1998 David Harvey on todennut tutkielmassaan, että käyttäjän manipulaatio -termiä käytetään suureen määrään eri aktiviteettejä, mikä tekee termistä parhaimmillaan hämmentävän [4, s. 4]. Harveyn mukaan termin määritelmä on kuitenkin tarkoituksellisesti laaja, mikä antaa paremman mahdollisuuden “taudin” hallintaan “oireiden” sijaan [4, s. 5]. Taudilla hän tarkoitti manipulaation valtaan joutumista ja oireilla onnistuneen hyökkäyksen haittoja.

Käyttäjän manipulaatio -termille on tehty lukuisia määritelmiä. Alla on kaksi esimerkki määritystä 20 vuoden aikavälillä (Mitncik ja Simon 2002, Sonowal 2022). Ensimmäinen määritys on käytännönläheisempi ja jälkimmäinen puolestaan teoreettisempi.

Mitnickin ja Simonin mukaan käyttäjän manipulaatiossa käytetään vaikutusvaltaa ja suostuttelua pettääkseen ihmisiä vakuuttamalla heidät siitä, että käyttäjän manipuloija on joku, jota hän ei ole. Tämän seurauksena käyttäjän manipuloija pystyy hyödyntämään ihmisiä saadakseen tietoa teknologian avulla tai ilman sitä. [1]

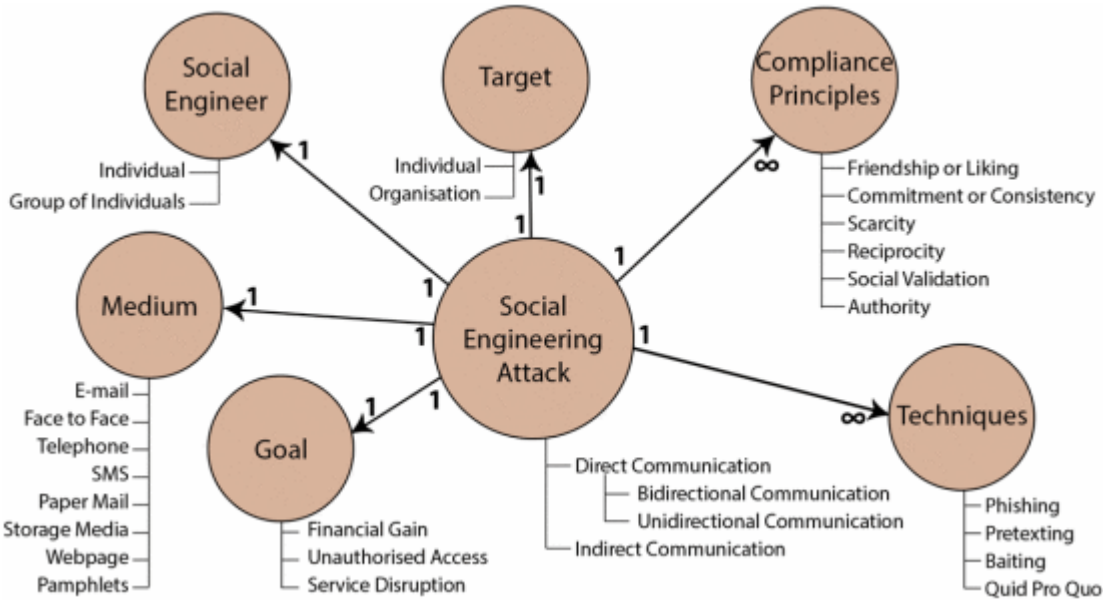
Mitnickin ja Simonin määritelmä kuvaa hyvin Mitnickin käytännönläheistä suhdettaan asiaan entisenä kyberrikollisena. Tärkeä aspekti, jonka Mitnick ja Simon ovat tuoneet kirjassaan korostetusti esille, luottamuksen rakentaminen ja hyödyntäminen, on jätetty rivien väliin. Heidän mukaansa luottamuksen rakentaminen kohteeseen on avain onnistumiseen käyttäjän manipulaatiossa [1, luku 2].

Sonowal määrittelee käyttäjän manipulaation olevan petoksen muoto, joka hyödyntää inhimillistä virhettä luvattoman pääsyn saamiseksi [5, luku 2]. Määritelmä on kuin suora sanakirjakuvaus termistä. Sonowalin määrityksessä ei ole mitään virheellistä, mutta se jättää paljon lukijan tietämyksen varaan. Määrityksessä tulee kuitenkin esiin tärkeimmät asiat: petoksen muoto, inhimillinen virhe ja luvaton pääsy.

3.2 Ontologinen malli käyttäjän manipulaatioon

Mouton et al. loivat tutkimuksessaan ontologisen mallin hahmottamaan käyttäjän manipulaatio -hyökkäyksiä (kuva 1). Tämä malli sisältää kaikki keskeiset käsitteet kuvaamaan mitä tahansa käyttäjän manipulaatio -hyökkäystä. Mallin avulla on mahdollista luoda hyökkäysvektori, jota voidaan käyttää esimerkiksi järjestelmällisen käyttäjän manipulaatio -hyökkäyksen suunnitteluvaiheessa [6]. Tämä on osoitus siitä, kuinka Moutonin tutkimukset kommunikoivat keskenään.

Mouton et al. eivät ole täysin avanneet kaikkia kuvassa 1 olevia käsitteitä. Ainakin käsitteiden viestintäväline (Medium), tavoite (Goal) ja tekniikat (Techniques) alle on mahdollista lisätä vaihtoehtoja. Nämä seikat eivät ole kuitenkaan tämän tutkielman kannalta tärkeitä, ja esimerkiksi kaikkien mahdollisten käyttäjän manipulaatio -hyökkäyksien tavoitteiden määrittäminen on haastavaa. Mallista käydään alla läpi keskeisin sisältö tälle tutkielmalle.



Kuva 1. Mouton et al. ontologinen malli käyttäjän manipulaatioon [7, luku 4].

Käyttäjän manipulaatio -hyökkäyksen voi Mouton et al. mukaan jakaa suoraan ja epäsuoraan kommunikaatioon (direct & indirect communication) [7, luku 4]. Epäsuoraa kommunikaatiota käytetään tässä yhteydessä tietojenkalasteluun, jossa kyberrikollinen käyttää jotain kolmatta osapuolta kuten sosiaalista mediaa tai keskustelufoorumia apunaan huijauksessa esimerkiksi johdattamaan kohteensa luomilleen valenettisivuille ja jää

odottamaan hyökkäyksen tuloksia. Suora kommunikaatio voi olla yksi- tai kaksisuuntaista (unidirectional & bidirectional communication) [7, luku 4]. Yksisuuntainen kommunikaatio on esimerkiksi sähköposti tai tekstiviesti, johon ei odoteta vastausta tai siihen ei reagoida tai anneta mahdollisuutta. Kaksisuuntaisessa kommunikaatiossa käyttäjän manipulaatio on korostetusti esillä. Siinä voidaan käyttää kaikkia suostuttelukeinoja ja hyökkäystekniikoita hyväksi. Sähköposti on yleisin kommunikaatioväline, mutta ääritapauksissa viestitään jopa kasvokkain.

Kommunikaatiotapojen merkitys tämän tutkielman kannalta on helpottaa hahmottamaan käyttäjän manipulaatio- ja tietojenkalasteluhyökkäyksien välisiä eroavaisuuksia. Tietojenkalasteluhyökkäyksien luonne tukee passiivisempia kommunikaatiotapoja, mutta niissä voidaan käyttää kaksisuuntaista kommunikaatiota tehostekeinona. Esimerkiksi kohde voidaan yrittää vakuuttaa kaksisuuntaisella kommunikaatiolla varsinaisena hyökkäyksenä toimivan sähköpostin tai tekstiviestin luotettavuudesta. Käyttäjän manipulaatiohyökkäyksissä asia on lähes päinvastainen. Hyökkäyksen valmistelussa voidaan käyttää tietojenkalastelua hyväksi tiedonkeruuvaiheessa, mutta varsinaisessa hyökkäyksessä kommunikaatio on aina kaksisuuntaista.

Suostuttelukeinot (Compliance Principles) kuuluvat keskeisimpiin asioihin, jotka vaikuttavat käyttäjän manipulaatio -hyökkäyksen onnistumiseen. Hyvin suunnitellussa hyökkäyksessä tehokkaimmat suostuttelukeinot kohteen manipuloimiseksi pyritään selvittämään ennen hyökkäyksen alkua. Alla on esitetty aiempien tutkimusten perusteella löydetyt tärkeimmät suostuttelukeinot tämän tutkielman viitekehyksessä. Lisäksi on kerrottu hieman historiallista taustaa niiden määrittämisestä.

Toisen maailmansodan aikainen propaganda sai sodan jälkeen yhteiskuntatieteilijät tutkimaan tapoja, joilla voidaan vaikuttaa toisen henkilön asenteisiin tai toimintaan. Cialdini on ollut pitkään mukana näissä tutkimuksissa, ja hän on julkaissut niiden pohjalta 6 merkittävintä suostuttelukeinoa, joilla voidaan vaikuttaa positiivisen vastauksen luomiseen. Ne ovat auktoriteetti, mieltymys, niukkuus, sosiaalinen hyväksyntä, vastavuoroisuus ja yhtenäisyys. [8]

Cialdinin tuomia suostuttelukeinoja ei ole laadittu lähtökohtaisesti nykymaailman tietoturvan näkökulmasta, mutta käyttäjän manipulaatiossa on pitkälti kyse yleismaailmallisesta psykologisesta manipulaatiosta, joten hänen esittelemänsä suostuttelukeinot ovat täysin valideja myös tässä viitekehyksessä. Varsinkin järjestelmällisessä käyttäjän manipulaatiossa, jossa rikollinen yrittää luoda kohteensa kanssa luottamussuhdetta.

Hadnagy viittaa myös kirjassaan Cialdinin tutkimustuloksiin. Hän käsittelee kirjassaan Cialdinin esittelemiä suostuttelukeinoja käyttäjän manipulaation perspektiivistä:

- Auktoriteetti: Kohde ei kyseenalaista pyyntöä (tai komentoa), jos hän uskoo pyynnön esittäjällä olevan valtuudet tehdä kyseinen pyyntö. [9, luku 6]
- Mieltymys: Jos kohteelle pystyy antamaan miellyttävän kuvan itsestään, helpottaa se hyökkäyksen onnistumista. Esimerkiksi yhteinen mielenkiinnon kohde auttaa luomaan mieltymystä. Hadnagyn mukaan tärkeintä on aitous. Teeskentelyn ylläpitämien on vaikeaa. Jos siitä jää kiinni, tilannetta on sen jälkeen vaikea korjata. Kehuminen ei automaattisesti onnistu. Sen pitää olla ansaittua ja sopia tilanteeseen. [9, luku 6]
- Niukkuus: Niukkuus lisää tavaroiden tai palveluiden arvoa. Kohteella on taipumus suostua pyyntöön, jos hän uskoo, että hänen haluamansa tavara on vähissä ja muut kilpailevat siitä. Niukkuuden ajava voima on kiire ja pelko siitä, että tavara on saatavilla vain lyhyen aikaa. [9, luku 6]
- Sosiaalinen hyväksyntä: Kohde hyväksyy helpommin pyynnön, jos pyyntö on linjassa sen kanssa, mitä muut tekevät tai hyväksyvät. Hadnagyn mukaan kaikilla ihmisillä on samanlaisuuden halu. [9, luku 6]
- Vastavuoroisuus: Ihmisillä on taipumus vastavuoroisuuteen. Vastavuoroisuuden tunne tulee myös tilanteissa, joissa avun saaja ei ole sitä pyytänyt. Ennen vastapalvelun pyytämistä on tärkeää antaa kohteelle aikaa kehittää tunne, että hän on vastapalvelun velkaa. [9, luku 6]
- Yhtenäisyys: Ihmisillä on taipumus pysyä kannassaan, jos he ovat tehneet julkisen sitoumuksen tai kannatuksen jonkun asian puolesta. Jos kohde suostuu pieneen pyyntöön, hän todennäköisesti suostuu sen jälkeen myös isompaan pyyntöön, jos se on johdonmukainen ensimmäisen pyynnön kanssa. Hadnagyn mukaan vastavuoroisuuden ja yhtenäisyyden onnistunut yhdistely käyttäjän manipulaatio hyökkäyksessä on kuin pysäyttämätön voima. [9, luku 6]

Myös Mitnickin kirjassa viitataan Cialdinin tuloksiin ja Mitnickin käsitys asioista on linjassa Hadnagyn kanssa – vain hieman suppeammin esiteltynä. Hadnagyn tietämys pohjautuu Mitnickin tavoin käytännönläheisyyteen. Hän ei ole Mitnickin tavoin hankkinut osaamistaan rikollisin toimin, vaan hänen työnkuvaansa kuuluu käyttäjän manipulaatio - hyökkäysten suunnittelu ja toteutus yritysasiakkaiden henkilökunnan testaamiseksi. Tällainen käytännön testaama tieto on pääasiallisesti aina arvokkaampaa tietoturvan aihealueella kuin teoreettinen tieto, jota esimerkiksi Moutonin tutkimustyöt edustavat eri työtovereiden kanssa.

Tietojenkalasteluhyökkäys on luonteeltaan aggressiivisempi kuin käyttäjän manipulaatio -hyökkäys. Tietojenkalasteluhyökkäyksessä rikollinen yrittää pääsääntöisesti yhdellä viestillä manipuloida kohteensa tunnetilan valtaan, jossa virheen tekemisen mahdollisuus kasvaa. Aikaikkuna onnistuneelle manipuloinnille on verrattain lyhyt, sillä viestin aiheuttama tunnetila heikkenee ajan myötä. Sonowal on Andersonin artikkelia mukaillen todennut, että viisi yleisintä suostuttelukeinoa tietojenkalasteluhyökkäyksissä ovat ahneus, kiire, uteliaisuus, pelko ja halu auttaa [10, katso 5, luku 2]. Cialdinin suostuttelukeinoista niukkuus on ainoa, joka on luonteeltaan pääasiallisesti tietojenkalasteluun soveltuva. Siinä yhdistyvät kiire, pelko ja mahdollisesti ahneus. Kaikki suostuttelukeinot toimivat yksinään, mutta yhdistelemällä niitä on mahdollista saada aikaan tehokkaampia hyökkäyksiä.

Tekniikoista (Techniques) tämän tutkielman perspektiivissä tärkeimmät ovat peitetarina (Pretexting) ja tietojenkalastelu (Phishing). Tietojenkalastelu on toinen tutkielman pääkäsitteistä, jota käsitellään tarkemmin luvussa 4. Käyttäjän manipulaatio -hyökkäyksen yhteydessä tietojenkalastelua käytetään tiedonkeruun apuvälineenä.

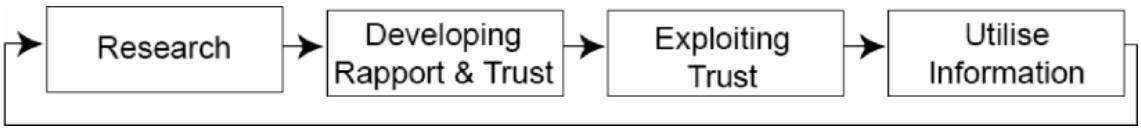
Watsonin et al. mukaan peitetarina on hyökkäyksen keino, jossa käyttäjän manipuloija yrittää luoda skenaarion, jonka avulla hän pystyy vakuuttamaan kohteensa antamaan haluttuja tietoja. Tärkeimpinä asioina ovat peitetarinan ja -roolin uskottavuus. [11, luku 3]

Tietojenkalastelussa peitetarina on kiinteä osa hyökkäystä. Esimerkiksi imitoitavat valenettisivut määrittävät peitetarinaa. Käyttäjän manipulaatiohyökkäyksissä peitetarina muodostetaan tiedonkeruun perusteella. Samalla voidaan määrittää myös peitetarinaan sopivat suostuttelukeinot. Hadnagyn mukaan peitetarinan tulee olla suoraan linjassa tavoitteen kanssa, jolloin tavoitetietojen kysymisestä tulee luontevampaa [9, luku 4].

3.3 Järjestelmällinen käyttäjän manipulaatio -hyökkäys

Järjestelmällisempään käyttäjän manipulaatio -hyökkäykseen löytyy aiemmista tutkimuksista useita eri malleja, joista ensimmäinen on tehty jo 1990-luvulla. Tunnetuin malli, johon useat muut tutkimukset viittaavat, on tekstimuodossa Mitnickin ja Simonin 2002 ilmestyneessä kirjassa käytännön esimerkein esitettynä. Mitnickin ja Simonin kirja kuvailee jokaista vaihetta konkreettisesti ja käytännönläheisesti. Entisenä kyberrikollisena Mitnickillä on kokemusta ja tietoa, jota muuten kuin tekemällä on vaikea saada. Kirjan yhteenvedossa keskeisimmät asiat on referoitu taulukoksi.

Mouton et al. loivat Mitnickin ja Simonin kirjaa mukaillen alla olevan käyttäjän manipulaatio -hyökkäyksen mallin (kuva 2). Heidän tarkoituksenansa oli käyttää Mitnickin ja Simonin tutkimustulosta lähtökohtana omaan jatkotutkimukseensa.

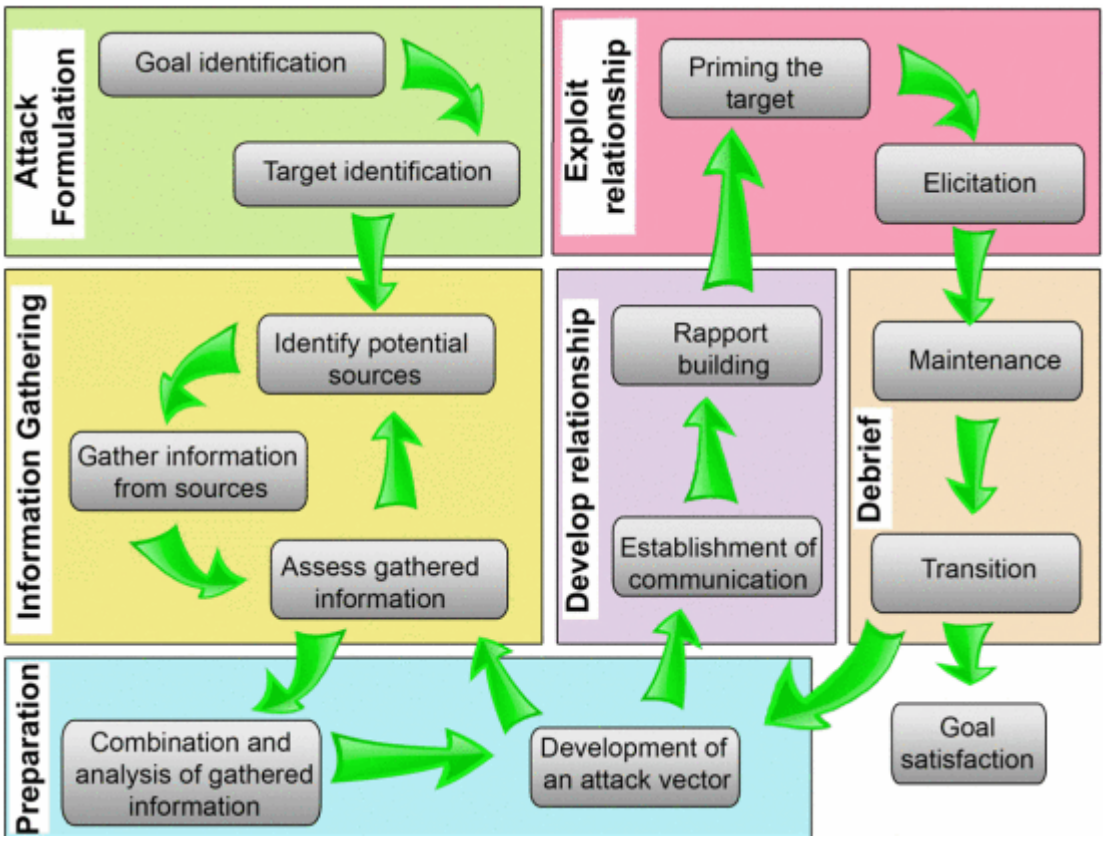


Kuva 2. Perustuu Mitnickin ja Simonin käyttäjän manipulaatio -hyökkäyksen vaiheisiin, joista Mouton et al. ovat luoneet yllä olevan graafisen mallin [1, katso 6].

Mitnickin ja Simonin käyttäjän manipulaatio -hyökkäyksen vaiheet Moutonin et al. mukaan:

- Tiedonkeruu (Research): Tarkoitus on hakea tietoa kohteesta. Rikollisen tulee tietää kohteesta mahdollisimman paljon ennen hyökkäyksen aloittamista. [1, katso 6]
- Luottamuksen kehittäminen kohteeseen (Developing Rapport & Trust): Suhdetta ja luottamusta voidaan kehittää esimerkiksi käyttämällä sisäpiiritietoa, siteeraamalla kohteen tuntemia henkilöitä, osoittamalla avun tarvetta, esittämällä väärää identiteettiä tai toimimalla arvovaltaisessa roolissa. Luottamuksen kasvattaminen parantaa varsinaisen hyökkäyksen onnistumismahdollisuuksia. [1, katso 6]
- Luottamuksen hyödyntäminen (Exploiting Trust): Kasvatettuaan luottamussuhdetta kohteeseensa, alkaa varsinainen hyökkäys. Hyökkäys voi olla esimerkiksi tiedon-, palvelun- tai avunpyyntö. Tässä vaiheessa rikollinen pyrkii saamaan kohteeltaan haluamansa. [1, katso 6]
- Tiedon käyttö (Utilise Information): Rikollinen käyttää saamiaan tietoja tavoitteensa täyttämiseen, joka voi olla lopullinen päämäärä tai osa seuraavaa tiedonkeruu vaihetta. [1, katso 6]

Mouton et al. eivät jättäneet työtään vain yllä olevan mallin hahmottamiseen ja tulkitsemiseen. He kokivat, että Mitnickin ja Simonin malli ei ollut tarpeeksi yksityiskohtainen ja se jätti liikaa tulkitsemisen varaa. Joten he päättivät jalostaa Mitnickin ja Simonin mallin pohjalta oman yksityiskohtaisemman mallin järjestelmälliselle käyttäjän manipulaatio -hyökkäykselle (kuva 3).



Kuva 3. Mouton et al. järjestelmällinen käyttäjän manipulaatio -hyökkäys [6].

Mouton et al. järjestelmällisen käyttäjän manipulaatio -hyökkäyksen vaiheet:

- Hyökkäyksen muotoilu (Attack Formulation): Ensimmäiseksi määritetään hyökkäyksen tavoite (Goal Identification) ja kohde (Target Identification). Kohteeksi valitaan helpoin mahdollinen, millä tavoite saadaan täytettyä. [6]
- Tiedonkeruu (Information Gathering): Tunnistetaan potentiaaliset tietolähteet (Identify potential sources). Tietolähteinä voivat olla esimerkiksi yrityksen kotisivut ja sosiaalinen media. Seuraavaksi kerätään mahdollisimman paljon tietoa määritellyistä tietolähteistä (Gather information from sources). Tärkeitä tietoja ovat esimerkiksi luvun 3.2 suostuttelukeinojen ja peitetarinan määritykseen tarvittavat tiedot. Tämän jälkeen arvioidaan riittääkö tieto hyökkäyksen läpivientiin (Assess gathered information). Jos ei riitä, palataan vaiheen alkuun. Tämä vaihe on erittäin tärkeä koko hyökkäyksen kannalta. Laadukas taustatieto parantaa mahdollisuuksia suhteen luomiseen ja luottamuksen kasvattamiseen. [6]
- Valmistautuminen (Preparation): Kerätty tieto organisoidaan ja sen perusteella laaditaan tarkempi hyökkäyssuunnitelma (Combination and analysis of gathered

information). Luvussa 3.2 esitetyn ontologisen mallin avulla luodaan hyökkäysvektori (Development of an attack vector), jossa jokaisella komponentilla on arvo. Suunnitelman tulee tässä vaiheessa sisältää peitetarina ja suostuttelukeinot, joiden avulla tavoite yritetään saavuttaa. [6]

- Suhteen kehittäminen (Develop relationship): Peitetarinaa käyttäen luodaan kommunikaatioyhteys kohteeseen (Establishment of communication). Tämän jälkeen aletaan kasvattamaan luottamussuhdetta peitetarinan ja suostuttelukeinojen avulla (Rapport building). Tämä vaihe voi olla aikaa vievä. Jos luottamusta ei pystytä luomaan, tavoitteen saavuttaminen on epätodennäköistä. Hyvin laadittu peitetarina yhteydenotolle helpottaa tavoitteen saavuttamista. [6]
- Suhteen hyödyntäminen (Exploit relationship): Lopulta ollaan vaiheessa, jossa kohdetta yritetään manipuloida tavoitteen saavuttamiseksi. Aikaisemman tiedonkeruun pohjalta valittujen suostuttelukeinojen avulla kohde yritetään ensin pohjustaa (Priming the target) sellaiseen tunne- tai olotilaan, että manipulointi olisi mahdollisimman tehokasta. Tämän jälkeen tehdään hyökkäys, jonka tarkoituksena on päästä tavoitteeseen (Elicitation). [6]
- Yhteenveto (Debrief): Viimeisessä vaiheessa kohde yritetään saada takaisin perusolotilaan (Maintenance). On tärkeää, ettei hän jää tunteeseen, että jotain on vialla. Perusolotilassa kohde todennäköisemmin ei ajattele tapahtumien kulkua uudestaan. Tässä vaiheessa rikollinen voi päättää, että lopputulos on riittävän hyvä ja lopettaa hyökkäyksen (Goal satisfaction). Vaihtoehtoisesti hän voi palata takaisin tiedonkeruu- tai valmistautumisvaiheeseen (Transition). [6]

Myös Mitnick ja Simon neuvovat kirjassaan, ettei koskaan kannata lopettaa keskustelua heti kun tavoite on saavutettu. Kannattaa vielä hetki keskustella ja mahdollisesti esittää pari ylimääräistä kysymystä, joiden jälkeen voi sanoa hyvästit. Jos kohde muistaa myöhemmin jotain esitetyistä kysymyksistä, ovat ne luultavasti pari viimeistä kysymystä. Loput yleensä unohdetaan. [1, luku 2]

Mitnickin kirja on täynnä kokemukseen pohjautuvia skenaarioita, joissa käyttäjän manipulaatiota toteutetaan erilaisissa ympäristöissä. Tieto on arvokasta, mutta sitä on vaikea käyttää tiedemaailman teoreettisessa käsitemaailmassa. Mouton et al. ovat luoneet tutkimuksillaan sillan kokemusten ja teorian välille ja heidän luomansa kuvan 3 malli on riittävän yksityiskohtainen kuvaamaan kaikkia Mitnickin kirjan skenaariota.

4. TIETOJENKALASTELU

4.1 Termin historiaa ja määritelmä

Englanninkielinen termi phishing on yleisesti suomennettu muotoon tietojenkalastelu, jota myös käytetään tässä tutkielmassa. Käännös ei ole täysin tarkka, mutta silti kuvaava. Phishing käsittää pääasiallisesti vain sähköpostilla tapahtuvan tietojenkalastelun. Esimerkiksi tekstiviesteillä tapahtuvaa tietojenkalastelua kutsutaan termillä smishing ja äänipuheluiden tapauksessa terminä on vishing. Suomenkielinen termi tietojenkalastelu kattaa yleisesti kaiken tietojenkalastelun kommunikaatiovälineestä riippumatta. Kommunikaatioväline voidaan erikseen mainita asian yhteydessä.

Sekä suomen- että englanninkielinen termi on juonnettu perinteisestä kalastuksesta. Syynä on yhtäläisyys molemmissa toiminnoissa. Kuten kalastuksessa myös tietojenkalastelussa houkuttimena käytetään syöttiä, jolla yritetään saada saalista. Tietojenkalastelussa madon tai vieheen sijasta syöttinä käytetään käyttäjän manipulaatiota ja saaliiksi yritetään saada esimerkiksi kohteen tunnistetiedot.

APWG (Anti-Phishing Working Group) määrittelee tietojenkalastelun rikoksena, jossa käytetään käyttäjän manipulaatiota ja teknisiä keinoja tietojen varastamiseen kohteelta. Käyttäjän manipulaation keinoilla rikollinen yrittää saada kohteensa uskomaan, että hän on tekemisissä laillisen ja luotettavan osapuolen kanssa. Käyttämällä harhaanjohtavia sähköpostiosoitteita ja -viestejä, kohde pyritään ohjaamaan väärennetyille nettisivuille, joiden tarkoitus on kalastaa kohteelta rikollisen haluamat tiedot kuten tunnistetiedot. Vaihtoehtoisesti kohde yritetään saada lataamaan haittaohjelma järjestelmäänsä. [12]

Hadnagyn mukaan tietojenkalastelussa lähetetään haitallisia sähköpostiviestejä, jotka valheellisesti näyttävät olevan peräisin hyvämaineisista lähteistä. Tavoitteena on kerätä tunnistetietoja, toimittaa haittaohjelma kohteelle tai kerätä muita tietoja myöhempiä hyökkäyksiä varten. [9, luku 9]

Hadnagy viittaa määritelmänsä lopussa, että tietojenkalasteluhyökkäykset voivat olla iteratiivisia, jolloin edellisen hyökkäyksen tulosta käytetään hyväksi seuraavassa hyökkäyksessä. Tietojenkalastelu voi olla myös osa luvun 3.3 järjestelmällistä käyttäjän manipulaatio -hyökkäystä, jossa tietojenkalastelulla yritetään kerätä tietoa kohteesta.

Tämän tutkimuksen viitekehyksessä tietojenkalastelu on luvun 3.2 ontologisen mallin mukaan suora tai epäsuora pääsääntöisesti yksisuuntainen hyökkäys. Tietojenkalastelussa käytetyissä sähköposteissa tai tekstiviesteissä harvoin on mahdollisuutta vastata tai vastauksiin ei reagoida.

Kaksisuuntaisena kommunikaatiovälineenä äänipuhelut liitetään yleensä tietojenkalasteluun, mutta niiden luonne on tämän tutkimuksen mukaan enemmän käyttäjän manipulaatio -käsitteen mukainen. Äänipuhelua voidaan kuitenkin käyttää tietojenkalastelussa esimerkiksi tehostekeinona sähköposti- tai tekstiviestihyökkäykselle, jossa puhelulla pyritään vahvistamaan kyseisen viestin luotettavuutta. Äänipuheluissa ei kuitenkaan ole suoraa yhteyttä teknisiin aspekteihin, jotka erottavat tietojenkalasteluhyökkäykset käyttäjän manipulaatio -hyökkäyksistä. Kuten luvussa 3.2 mainittiin, äänipuheluissa käyttäjän manipulaatio on korostetusti esillä. Niillä on mahdollista manipuloida kohdetta reaaliaikaisesti peitetarinaa ja tilanteeseen sopivia suostuttelukeinoja apuna käyttäen. Kohteella on myös vähemmän aikaa reagoida ja analysoida puhelun sisältöä. Rikollinen on voinut suunnitella hyökkäystä pitkään, joten moneen kohteen reaktioon voi olla vastaus jo valmiina.

4.2 Käyttäjää manipuloiva tietojenkalastelu

Tietojenkalastelun tekninen puoli on laaja kenttä erilaisia keinoja, joilla rikollinen voi yrittää huijata kohdettaan. Esimerkiksi nettisivupohjaiset huijaukset tai erityyppiset haittaohjelmat ovat laajoja aihepiirejä, joista voisi tehdä erilliset tutkimukset. Nämä rajataan tästä tutkielmasta pois siitä huolimatta, että näissäkin käyttäjän manipulaatiota voi esiintyä.

Sonowalin mukaan käyttäjää manipuloivan tietojenkalastelun voi jakaa kolmeen kategoriaan: petollinen tietojenkalastelu (phishing), kohdennettu tietojenkalastelu (spear phishing) ja valaanpyynti (whaling) [5, luku 2].

Petollinen tietojenkalastelu on tietojenkalastelun perusmuoto. Petollisen tietojenkalastelun ominaispiirteitä ovat suuri määrä satunnaisia kohteita, alhainen onnistumisprosentti ja muihin tapoihin verrattuna alhaisin suunnitteluaika. [5, luku 2] Harjaantunut käyttäjä huomaa tällaiset huijausviestit helpolla. Kohteena ovatkin käyttäjät, joiden tietoturvan hallinta on mahdollisimman vähäistä. Hyökkäyksessä luotetaan määrään sisällön osuvuuden sijaan. Esimerkiksi jos petollinen tietojenkalasteluhyökkäys sisältää 100000 sähköpostiviestiä ja onnistumisprosentti on 1 %, saa rikollinen silti 1000:n ihmisen tunnistetiedot haltuunsa.

Kohdennetussa tietojenkalastelussa perusajatus ei muutu petollisesta tietojenkalastelusta, mutta siinä käytetään henkilökohtaisempaa lähestymistapaa hyökkäykseen. Satunnaisten kohteiden sijaan kohteeksi valitaan esimerkiksi tietty organisaatio tai jokin muu toisiinsa sidonnainen ryhmä ihmisiä kuten tietyn pankin asiakaskunta. Tarkoituksena on ensin kerätä tietoa kohderyhmästä ja sen jälkeen suunnitella hyökkäys kerättyjen tietojen avulla sopivaksi juuri tuolle kohderyhmälle. Suunnittelutyön ansiosta kohdennettujen tietojenkalasteluhyökkäysten onnistumisprosentti on yleensä huomattavasti suurempi petolliseen tietojenkalasteluun verrattuna. [5, luku 2] [11, luku 9] Kohdennettua tietojenkalastelua voidaan käyttää myös yksittäisiin ihmisiin. Esimerkiksi osana luvun 3.3 järjestelmällistä käyttäjän manipulaatio -hyökkäystä.

Valaanpyynti on kohdennetun tietojenkalastuksen muoto, jossa kohteena ovat korkean profiilin henkilöt. Tällaisia ovat esimerkiksi poliitikot, yritysten johtoportaiden edustajat ja varakkaat julkisuuden henkilöt. Erona kohdennettuun tietojenkalasteluun on, että korkean profiilin kohteiden tietoturva on vaikeampi murtaa. Varakkailla julkisuuden henkilöillä on yleensä palkattuna ammattihenkilö, joka vastaa heidän tietoturvastaan. Tämän takia taustatyön määrä kasvaa ja hyökkäys vie enemmän aikaa. [5, luku 2] Valaanpyynnin korkean profiilin kohteiden vuoksi rikollisen tavoitteena voi olla arkaluontoisen materiaalin saanti. Tällaisia ovat esimerkiksi imagoa tai brändiä vahingoittavat tiedot sekä poliittiset- ja yrityssalaisuudet. Asiayhteyteen liitetään ajoittain yritysvakoilu ja kiristykset.

4.3 Tietojenkalasteluhyökkäyksen elinkaari

Tietojenkalasteluhyökkäyksen jakaminen vaiheisiin helpottaa hyökkäyksen lähempää tarkastelemista ja hahmottamista. Tässä tutkielmassa jako vaiheisiin auttaa myös tietojenkalasteluhyökkäyksen vertaamista luvun 3.3 järjestelmälliseen käyttäjän manipulaatio -hyökkäykseen. Jain ja Gupta ovat luoneet kuusiportaisen mallin (kuva 4), joka kuvaa tietojenkalasteluhyökkäyksen elinkaarta.

Kuva 4: Tietojenkalasteluhyökkäyksen elinkaari Jainin ja Guptan mukaan [13].

Tietojenkalasteluhyökkäyksen vaiheet Jainin ja Guptan mukaan:

- Suunnittelu (Planning and Setup): Ensimmäisessä vaiheessa rikollinen valitsee imitoitavan kohdeorganisaation avuksi hyökkäykseensä ja luo teknisen strategian tavoitteena olevien tietojen saamiseen. [13, luku 3]
- Tietojenkalastelusivun rakentaminen (Phishing Site Construction): Rikollinen luo tietojenkalastelusivuston, joka imitoi kohdeorganisaation virallisia nettisivuja ja kun työ on valmis hän lataa tekemänsä nettisivut internettiin. [13, luku 3]
- Tietojenkalastelusivun jakaminen (Phishing Spreading): Rikollinen valitsee kommunikaatiokanavat, joiden avulla hän jakaa linkkiä tietojenkalastelusivuille. [13, luku 3]
- Asennus (Installation): Petollisten linkkien luonti tietojenkalastelusivuille. Petollinen linkki voi sisältää haittaohjelman. [13, luku 3]
- Tulosten keräys (Data Collection): Rikollinen saa haltuunsa tietojenkalastelusivujen ja mahdollisen haittaohjelman kautta tulevia tietoja. [13, luku 3]
- Hallittu lopetus (Break Out): Saatuaan haluamansa rikollinen tuhoaa jälkensä eli tietojenkalastelusivut, sähköpostiosoitteet, jne. [13, luku 3]

Malli ei ota kantaa hyökkäyksen kohteisiin eikä näin ollen hyökkäyksen tyyppiin, mikä tekee siitä refleksisemmän. Jain ja Gupta eivät ota kantaa tietojenkalastelusivujen ajalliseen elinikään. Tämä on ymmärrettävää, sillä tietoturvan parantuessa tietojenkalastelusivujen elinikä vähenee. Tietojenkalastelusivustoja etsitään aktiivisesti ja esimerkiksi Chromen Enhanced Safe Browsing -moodi voi tehdä haitallisten nettisivujen tarkastuksen parhaimmillaan 30 minuutin välein. Tämä on verrattain uusi kehitysaskel, mutta osoitus siitä, että tietoturva jatkaa kehitystään.

Vaiheita tarkastelemalla paljastuu, että käyttäjän manipulaation osuus tietojenkalastelussa on vähäistä verrattuna käyttäjän manipulaatio- hyökkäyksiin. Peitetarinan pohja valikoituu kohdeorganisaation valinnalla. Peitetarina tarkentuu viestien sisältöä laatiessa ja samalla valitaan peitetarinaan soveltuvat suostuttelukeinot. Jos kyseessä on kohdennettu tietojenkalastelu, viestien sisältö kohdistetaan tarkemmin kohteiden mukaiseksi. Tehokkaimmillaan hyökkäykset ovat, kun kohdistus tehdään jokaiselle kohteelle erikseen.

5. YHTEENVETO

Tutkielman päätavoitteena oli tutkia rajapintaa ihmiseen kohdistuvissa kyberhyökkäyksissä. Hyökkäysmuotoja löytyi kaksi: käyttäjän manipulaatio- ja tietojenkalasteluhyökkäykset. Molemmille hyökkäysmuodoille on yhteistä kahden tärkeän elementin käyttö hyökkäyksissä: suostuttelukeinot ja peitetarina. Nämä kaksi manipuloinnin keinoa yhdistettynä yllä oleviin hyökkäysmuotoihin ovat ne tekijät, joiden avulla kyberrikollinen pystyy läpäisemään inhimillisen rajapinnan. Tutkielman toisena tavoitteena oli luoda selkeät rajat kahdelle tutkielman pääkäsitteelle: käyttäjän manipulaatiolle ja tietojenkalastelulle.

Käyttäjän manipulaatiossa ja tietojenkalastelussa perusajatus on sama. Hyökkäyksen kohde pyritään saada tekemään inhimillinen virhe manipulaation avulla. Käyttäjän manipulaatiossa virhe johtaa suoraan luvattomien tietojen saantiin. Tietojenkalastelussa pyritään saamaan haittaohjelma kohteen järjestelmään tai ohjaamaan kohde tietojenkalastelusivustolle, joka imitoi jotain peitetarinan mukaista luotettavaa tahoa. Tietojenkalastelu sisältää lähtökohtaisesti aina jonkin teknisen aspektin osana hyökkäystä. Käyttäjän manipulaatiossa ainoa tärkeä tekninen puoli on kommunikaatioväline.

Käyttäjän manipulaation ja tietojenkalastelun välinen suhde on kompleksinen. Järjestelmällinen käyttäjän manipulaatio -hyökkäys sisältää usein tietojenkalasteluhyökkäyksiä tiedonkeruu vaiheessa, jossa hyökkäyksen kohteesta yritetään saada mahdollisimman paljon taustatietoa ennen varsinaisen hyökkäyksen suunnittelua. Tietojenkalasteluhyökkäyksien tärkein elementti on käyttäjän manipulaatio, jota käytetään syöttinä hyökkäyksen kohteen huijaamisessa.

Käyttäjän manipulointi -hyökkäyksissä kohteeseen pyritään luomaan luottamussuhde, joka tämän tutkielman mukaan on tärkein elementti käyttäjän manipulaatio -hyökkäyksen onnistumisessa. Luottamussuhteen muodostaminen on luonteeltaan hidasta, joten suostuttelukeinoina voidaan käyttää myös enemmän aikaa vieviä vaihtoehtoja. Yleisimmät suostuttelukeinot käyttäjän manipulaatio -hyökkäyksissä ovat auktoriteetti, mieltymys, niukkuus, sosiaalinen hyväksyntä, vastavuoroisuus ja yhtenäisyys.

Tietojenkalasteluhyökkäyksissä tilanne on päinvastainen. Niissä suostuttelukeinona käytetään yleensä jotain aggressiivisempaa vaihtoehtoa. Hyökkäyksen tavoitteeseen pyritään pääsemään sinä aikana kuin tuo aggressiivisempi suostuttelukeino vaikuttaa kohteeseen heikentäen harkintaa ja maalaisjärjen käyttöä. Yleisimmät suostuttelukeinot tietojenkalasteluhyökkäyksissä ovat ahneus, kiire, uteliaisuus, pelko ja halu auttaa.

Suostuttelukeinojen yhdistely voi parhaimmillaan tehostaa merkittävästi hyökkäyksen onnistumismahdollisuuksia. Suostuttelukeinojen valinta tapahtuu yleensä taustatyön ja tiedonkeruun perusteella. Jos tällaista vaihetta ei ole kuten petollisessa tietojenkalastelussa, yritetään peitetarinaa ja suostuttelukeinoja käyttäen luoda uskottava massahyökkäys, jossa hyökkäyksen kohteiden suuri määrä kompensoi kohdennuksen puutetta.

Peitetarina ja peiterooli ovat molemmissa hyökkäysmuodoissa tärkeänä osana. Tietojenkalasteluhyökkäyksissä peitetarina liittyy kiinteästi teknisiin aspekteihin kuten imitoitavien nettisivujen rakentamiseen. Peitetarina ja -rooli ovat tällöin osa imitoinnin kohdetta. Käyttäjän manipulaatiossa peitetarina tehdään tiedonkeruu -vaiheen tulosten perusteella. Tehokkaimmillaan hyökkäys on, kun peitetarina, suostuttelukeinot ja hyökkäyksen tavoite ovat kaikki linjassa keskenään ja ne on määritelty riittävän tiedonkeruun perusteella.

Tulevaisuudennäkymä on suotuisampi käyttäjän manipulaatiolle kuin tietojenkalastelulle. Käyttäjän manipulaatio -hyökkäyksissä ei ole pakollista tarvetta teknologialle muuten kuin kommunikaatiovälineiden muodossa. Tiedonkeruuvaiheessa voidaan käyttää tietojenkalastelua apuna, mutta se ei ole välttämätöntä. Hyvin suunniteltua käyttäjän manipulaatio -hyökkäystä on vaikea havaita ja siinäkin tapauksessa, että se havaitaan, rikollisen kiinnisaaminen on vaikeaa. Jos tulevaisuudessa siirrytään käyttämään sähköistä tunnistautumista aktiivisemmin asiointien yhteydessä, voisi sillä olla suuri vaikutus myös käyttäjän manipulaatiohyökkäysten hallinnassa. Tietojenkalastelussa tekniikka on keskeisessä roolissa ja näin ollen sitä on helpompi hallita teknisen tietoturvan avulla.

LÄHTEET

[1] K. Mitnick, W. Simon, The Art of Deception: Controlling the Human Element of Security, Wiley, 2002. Saatavissa (Viitattu 23.11.2023): https://learning.oreilly.com/library/view/the-art-of/9780764542800/

[2] I. Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh, Social Engineering Attack Strategies and Defence Approaches, 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, Päivitetty 26.9.2016. Saatavissa (Viitattu 23.11.2023): https://doi.org/10.1109/FiCloud.2016.28

[3] T. Chamorro-Premuzic, Human Error Drives Most Cyber Incidents. Could AI Help?, Harward Business Review, 2023, Päivitetty 3.5.2023. Saatavissa (Viitattu 14.11.2023): https://hbr.org/2023/05/human-error-drives-most-cyber-incidents-could-ai-help.

[4] D. Harley, Re-Floating the Titanic: Dealing with Social Engineering Attacks, EICAR, 1998. Saatavissa (Viitattu 14.11.2023): https://smallbluegreen-blog.files.wordpress.com/2010/04/eicar98.pdf

[5] G. Sonowal, Phishing and Communication Channels: A Guide to Identifying and Mitigating Phishing Attacks, APress, 2022. Saatavissa (Viitattu 23.11.2023): https://learning.oreilly.com/library/view/phishing-and-communication/9781484277447/

[6] F. Mouton, M. Malan, L. Leenen. H. Venter, Social engineering attack framework, 2014 Information Security for South Africa, 2014, Päivitetty: 10.11.2014. Saatavissa (Viitattu 23.11.2023): https://doi.org/10.1109/ISSA.2014.6950510

[7] F. Mouton, L. Leenen, M. Malan, H. Venter, Towards an Ontological Model Defining the Social Engineering Domain, Berlin, Heidelberg: Springer International Publishing, 2014. Saatavissa (Viitattu 23.11.2023): https://link-springer-com.libproxy.tuni.fi/chapter/10.1007/978-3-662-44208-1_22

[8] R. Cialdini, Influence: the psychology of persuasion (EPub edition, HarperCollins Publishers, 2007. Saatavissa (Viitattu 23.11.2023): https://learning.oreilly.com/library/view/influence/9780061899874/

[9] C. Hadnagy, Social engineering: the science of human hacking (Second edition.), Wiley, 2018. Saatavissa (Viitattu 23.11.2023): https://learning.oreilly.com/library/view/social-engineering-2nd/9781119433385/

[10] J. Anderson, Greed, Fear and Kindness: The Evolution of Phishing and Spam, University of Minnesota, 2019. Saatavissa (Viitattu 23.11.2023): https://it.umn.edu/news-alerts/news/greed-fear-kindness-evolution-phishing-spam

[11] G. Watson, A. Mason, R. Ackroyd, Social engineering penetration testing: executing social engineering pen tests, assessments and defense (1st edition), Elsevier, 2014. Saatavissa (Viitattu 23.11.2023): https://learning.oreilly.com/library/view/social-engineering-penetration/9780124201248/

[12] APWG, Phishing Activity Trends Report (4th Quarter), 2022. Saatavissa (Viitattu 23.11.2023): https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf

[13] A. Jain, B. Gupta, A survey of phishing attack techniques, defence mechanisms and open research challenges, Enterprise Information Systems, Vol 16(4), 527–565, 2021. Saatavissa (Viitattu 23.11.2023): https://doi.org/10.1080/17517575.2021.1896786