Tampereen yliopisto

Pinja Rontu

# TIETOJENKALASTELUTEKNIIKOIDEN MUUTOS AJAN SAATOSSA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Toukokuu 2023

# TIIVISTELMÄ

Pinja Rontu: Tietojenkalastelutekniikoiden muutos ajan saatossa
Tampereen yliopisto
Tieto- ja sähkötekniikan tutkinto-ohjelma, Tietotekniikka
Kandidaatintyö
Toukokuu 2023

---

Ihminen on suurin uhka tietojärjestelmien turvallisuudelle. Hyökkääjän on helppo käyttää ihmisluonnon hyväuskoisuutta hyväkseen. Kun tätä hyväuskoisuutta käytetään hyökkääjän hyödyksi uhrin huomaamatta, kyseessä on kyberhyökkäystekniikka nimeltään käyttäjän manipulointi. Käyttäjän manipuloinnissa ihmistä huijataan esimerkiksi asian kiireellisyydellä tai tärkeydellä. Tämän alle lukeutuu myös tietojenkalastelu, joka on yksi käytetyimmistä hyökkäysmenetelmistä. Tietojenkalastelussa ihmiseltä kerätään tietoja naamioimalla hyökkäyskanava luotettavan oloiseksi käyttäjän manipuloinnin tapoja hyödyntäen. Lisäksi tietojenkalastelussa voidaan hyödyntää erilaisia teknisiä menetelmiä.

Tämä tutkielma on aikaisempaan tutkimustyöhön pohjautuva kirjallisuuskatsaus, joka tutkii, minkälaisia tietojenkalastelutekniikoita on olemassa ja miten ne ovat kehittyneet ajan saatossa. Työssä käydään läpi tietojenkalastelun tekniikoita, historiaa ja tulevaisuutta. Ensimmäiset tietojenkalastelutapaukset tapahtuivat vuonna 1995, kun hyökkääjät keräsivät käyttäjätunnuksia käyttäjän manipuloinnin keinoilla America Onlinen keskustelukanavilla. 1990-luvun lopulla tietojenkalastelu levisi kaikkialle internetiin ja pysyy yhtenä suosituimmista kyberhyökkäyskeinoista tänäkin päivänä.

Tunnetuin tietojenkalastelutekniikka on huijausviesti. Huijausviestin lisäksi tekniikoita on lukuisia muita, jotka hyödyntävät käyttäjän manipulointia, teknisiä menetelmiä tai niiden yhdistelmiä. Kaikilla hyökkäystekniikoilla on oma tarkoitus ja käyttökohde. Hyökkäyksen onnistumista voi parantaa tekemällä taustatutkimusta kohteesta. Tätä kutsutaan nimellä kohdennettu tietojenkalastelu.

Teknologian saatavuuden ja helppokäyttöisyyden parantuminen kasvattaa tietojenkalasteluhyökkäysten määrää eikä se todennäköisesti katoa tulevaisuudessa. Hyökkääjät kehittävät koko ajan uusia keinoja tehdä hyökkäyksiä, joten vanhojen tapojen tunteminen ei välttämättä auta. Tulevaisuuden trendejä tietotekniikassa ovat Internet of Things ja koneoppiminen. Niitä voidaan hyödyntää uudenlaisiin tietojenkalasteluhyökkäyksiin.

Tutkielmassa saatiin selville, että tietojenkalastelutekniikat ovat muuttuneet osittain. Alkuperäisten huijausviestien rinnalle on kehittynyt useita uusia hyökkäyskanavia, mutta hyökkäysten perusta on pysynyt pääosin samana. Käyttäjän manipulointi on siis yhä edelleen toimiva keino, jonka avulla tietojenkalasteluhyökkäykset toimivat.

Avainsanat: tietoturva, tietojenkalastelu, phishing, käyttäjän manipulointi

# SISÄLLYSLUETTELO



.

# 1. JOHDANTO

Teknologian nopean kehityksen mukana ovat kehittyneet myös erilaiset hyökkäys- ja tietomurtotavat. Kyberturvallisuus on tällä hetkellä yksi suurimmista haasteista niin yksilölle kuin organisaatioille. IBM:n raportin [1] mukaan 83 % sen tutkimista organisaatioista on joutunut tietomurron kohteeksi vuonna 2021. Myös moni yksilö on kohdannut huijausviestin elämänsä aikana. Kesänä 2022 oli liikkeellä huijausviestejä, joissa hyökkääjä kiristi rahaa. Hyökkääjä väitti, että heillä on videota käyttäjästä, kun hän on vieraillut aikuisviihdesivustolla [2]. Samantyylisistä huijauksista uutisoidaan usein.

IBM:n raportin mukaan [1] hyökkäyksistä 21 % johtui ihmisen tekemästä virheestä. Ihminen on siis erittäin suuressa roolissa tietomurroissa ja kyberhyökkäyksissä. Ihmisen mieltä on helppo harhauttaa, kun vastaavasti tietojärjestelmiin murtautuminen vaatii teknillistä osaamista. Yksi kyberhyökkäystekniikka on käyttäjän manipulointi (engl. social engineering) ja siihen liittyy tietojenkalastelu (engl. phishing). Joissain yhteyksissä käyttäjän manipulointia ja tietojenkalastelua verrataan toisiinsa, sillä niillä on paljon samoja piirteitä.

Teknologisen kehityksen ja historian tunteminen on tärkeää, koska ne auttavat hahmottamaan ja kuvaamaan nykyistä maailmamme paremmin. Buchananin artikkelin mukaan [3] historian tuntemista vaaditaan, jotta voidaan ymmärtää nykyaikaisia teknologioita. Historiallisesti verkossa tapahtuvaa tietojenkalastelua ei ole tapahtunut kuin kolmekymmentä vuotta, mutta tämä historia on tärkeä tietää, jotta emme sorru samoihin vanhoihin huijauksiin yhä uudestaan.

Tulevaisuuden teknologiat tuovat mukanaan uusia uhkakuvia, esimerkiksi Internet of Things ja tekoäly ovat tämän hetken kehittyviä trendejä. Vuonna 2022 koneälyä hyödyntävä ChatGPT -keskustelubotti on kerännyt julkisuudessa paljon huomiota. Keskusteluominaisuuden lisäksi koneäly osaa kirjoittaa tehtävänannon pohjalta ohjelmakoodia. Uusia teknologioita voidaan myös väärinkäyttää. CheckPoint Researchin tekemässä raportissa [4] havattiin, että ChatGPT:tä on mahdollista käyttää myös kyberrikollisuuteen. Botilla on mahdollista muodostaa tietojenkalasteluviestejä ja luoda haittaohjelmia ilman aikaisempaa ohjelmointikokemusta.

Tässä tutkielmassa keskitytään tietojenkalasteluun, sillä se on yleisin keino manipuloida käyttäjää. Tutkielmassa keskitytään erilaisiin tietojenkalastelutekniikoihin aikaisempaan

tutkimukseen pohjautuen. Tekniikoita käydään läpi eri ajanjaksoilta eli 1990-luvulta lähitulevaisuuteen. Aloitusajaksi on valittu 1990-luku, sillä tällöin tietokoneet ja internet yleistyivät kodeissa ja organisaatioissa. Tällöin aloitettiin myös käyttämään termiä tietojenkalastelu kuvaamaan käyttäjätietojen keräämistä väärinkäyttöä varten. Tutkielma keskittyy pelkästään erilaisiin hyökkäystekniikoihin, eli tietojenkalastelun ehkäisymenetelmiä ei tässä työssä käsitellä lainkaan. Tutkielmassa pyritään selvittämään, minkälaisia tekniikoita on olemassa, ovatko tekniikat muuttuneet ja jos ovat, niin millä tavoin.

Tutkielma sisältää seitsemän lukua. Toisessa luvussa käydään läpi käyttäjän manipulointia ja tietojenkalastelua. Kolmannessa luvussa kerrotaan tietojenkalastelun historiasta. Neljännessä luvussa käydään läpi erilaisia tietojenkalastelutekniikoita ja -tapoja. Viidennessä luvussa kuvataan tietojenkalastelun tulevaisuutta. Kuudennessa luvussa esitetään tulokset. Viimeisessä luvussa esitetään yhteenveto tutkielmasta.

Tutkielma on toteutettu kirjallisuuskatsauksena aikaisempaan tutkimukseen pohjautuen. Lähdeaineistoa etsittiin Tampereen yliopiston Andor, ACM Digital Library ja ProQuest Computer Science Database -tietokannoista. Suurin osa lähteistä löytyi hakusanoilla ”phishing” ja ”social engineering”. Näiden lisäksi hakuja tarkennettiin hakusanoilla ”history” ja ”attack technique”. Olennaiset aineistot valittiin lukemalla hakutuloksista tiivistelmät ja johdantoluvut. Lisäksi lähteitä analysoitiin lukemalla ne pääosin läpi.

# 2. KÄYTTÄJÄN MANIPULOINTI

Tietoteknisten järjestelmien heikoin kohta on yleensä ihminen. Käyttäjän sosiaalinen manipulointi (engl. social engineering) on hyökkäystekniikka, joka hyödyntää ihmisluonnon hyväuskoisuutta. Hyökkääjä hyödyntää tekniikkaa päästäkseen käsiksi haluttuihin järjestelmiin kiertäen tekniset turvallisuustoimenpiteet. Laajempi määritelmä käyttäjän manipuloinnille on saada toinen henkilö tekemään jotain, yleensä haitallista, hänen ymmärtämättään [5].

Manipulointi sisältää erilaisia keinoja, mutta usein hyödynnetään kolmea tunnetta: uteliaisuutta, pelkoa tai empatiaa. Uteliaisuus laittaa ihmisen avaamaan linkkejä tai viestejä, jotka kiinnostavat häntä. Pelkoa voidaan hyödyntää esimerkiksi sanomalla, että uhrin pankkiin on hyökätty. Empatiaa käytetään esimerkiksi silloin, kun luodaan jonkinlainen surullinen taustatarina tai esitetään uhrin tuttua. [6] Näiden kolmen tunteen lisäksi asialle usein luodaan kiire, jolloin tunteet ovat enemmän vallassa kuin järki.

Hadnagy [5] väittää, että vuonna 2017 tehdyistä tietomurroista 80 % sisälsi käyttäjän manipulointia jossain muodossa. Hänen mukaansa käyttäjän manipulointi on ollut käytetyin kyberhyökkäystekniikka vuodesta 2010 lähtien. Tekniikan suosio johtuu monesta asiasta. Ensinnäkin hyökkäys on helppo ja halpa toteuttaa suhteessa muihin kyberhyökkäystapoihin ja hyökkäyksen onnistuessa voitot voivat olla suuret. Toiseksi oikein tehdyssä hyökkäyksessä kiinnijäämisen riski on pieni. Tekniikka toimii, sillä ihmiset eivät usko, että he voisivat joutua kyberhyökkäyksen kohteeksi huomaamattaan.

## Tietojenkalastelu

Tietojenkalastelu (engl. phishing), myös verkkourkinta, on yksi käyttäjän manipuloinnin tapa. Yhden määritelmän mukaan tietojenkalastelu perustuu manipuloitujen viestien lähettämiseen niin, että uhri saadaan tekemään haluttuja asioita hyökkääjän hyväksi [7]. Määritelmä on muuten hyvä, mutta muiden tutkimusten mukaan viestien lähettäminen ei ole ainoa tietojenkalastelutapa. Tietojenkalastelussa hyökkääjän tavoitteena on saada käsiinsä esimerkiksi uhrin käyttäjätunnukset, pankki- tai henkilötiedot. Käyttäjän manipulointia hyödyntävää tietojenkalastelua kutsutaan petolliseksi kalasteluksi (engl. deceptive phishing). Sana petollinen kuvaa hyökkäyksen luonnetta: käyttäjältä kerätään tietoja naamioimalla hyökkäyskanava luotettavan oloiseksi [8]. Erilaisia hyökkäyskanavia käsitellään luvussa 4 tarkemmin.

Kaikki tietojenkalasteluhyökkäykset eivät sisällä käyttäjän manipulointia. Hyökkäyksiä voidaan tehdä myös teknisiä menetelmiä käyttäen. Näihin menetelmiin lukeutuvat muun muassa haittaohjelmat (engl. malware) ja muut tekniset ansat (engl. technical subterfuge). Haittaohjelmat keräävät käyttäjän tietoja laitteelta ja lähettävät ne eteenpäin hyökkääjälle. Tietojenkalasteluhyökkäykset voivat myös yhdistää käyttäjän manipulointia ja teknisiä menetelmiä. Esimerkki tällaisesta hyökkäyksestä on huijausviesti, jonka sisältämää linkkiä painamalla käyttäjän laitteelle asentuu haittaohjelma.

# 3. TIETOJENKALASTELUN HISTORIA

Raderin ja Rahmanin tutkimuksen [6] mukaan termiä ”phishing” käytettiin ensimmäistä kertaa vuonna 1997 Ed Stanselin kirjoittamassa artikkelissa Florida Times Unionissa. Siinä kirjain f on muutettu ph:ksi, sillä hakkeroijien käyttämässä omassa kielessä tämä muutos oli yleinen. Ensimmäiset tunnetut tietojenkalastelutapaukset tapahtuivat kuitenkin jo 1995 Yhdysvalloissa, kun hakkerit halusivat käyttää internetiä ilmaiseksi. He käyttivät manipulointitekniikoita America Onlinen (AOL) keskustelukanavilla, joissa käyttäjät harhautettiin antamaan sisäänkirjatumistunnuksensa hakkereille. Hakkerit pystyivät näin käyttämään internetiä ilmaiseksi ja uhriksi joutunut maksoi käytön todennäköisesti huomaamattaan.

Tämän jälkeen kehitettiin AOHell, ohjelma, jonka tarkoituksena oli helpottaa hakkerointia ja aiheuttaa muille harmia. Ohjelmalla pystyi massageneroimaan sähköposteja, luomaan väärennettyjä AOL-käyttäjiä ja tietojenkalasteluviestejä, joissa viestin lähettäjä teeskenteli olevansa AOL:n henkilökuntaa ja pyysi käyttäjän salasanaa. Lisäksi sen avulla viestin pystyi lähettämään kaikille AOL:n tilaajille automaattisesti. Tämä viestinluontiruutu näkyy kuvassa 1.


***Kuva 1.*** *AoHell-ohjelman tietojenkalasteluruutu. Ohjelmalla pystyi luomaan tietojenkalasteluviestejä automaattisesti. [9]*

Yksi ohjelman kehittäjistä, käyttäjänimeltään ”Da Chronic”, kertoo [9], että ohjelma oli suunniteltu erittäin käyttäjäystävällisesti ja siinä esimerkiksi kerrottiin käyttäjälle, mitä tietojenkalastelu on ja mitä hyötyä siitä on. Ohjelman avulla kuka tahansa pystyi harrastamaan tietojenkalastelua. Tuohon aikaan tietojenkalastelu oli ilmiönä niin uusi, että uhrit eivät osanneet suojautua ja onnistumisprosentti oli suuri. Da Chronicin mukaan ohjelma oli niin helppokäyttöinen, että sitä voi pitää tietojenkalastelun nykyisen suosion alkulähteenä.

Vuoden 1995 lopulla AoHell-ohjelmiston kehitys lopetettiin, mutta markkinoilla oli jo kymmeniä muita samankaltaisia ohjelmia. 1990-luvun lopussa uusien ohjelmien kehittäjät ja käyttäjät alkoivat tuomaan tietojenkalastelua myös muualle internetiin, kuten viesti- ja videopelipalstoille. 2000-luvun alussa uusia tietojenkalastelutekniikoita olivat esimerkiksi näppäilytallentimet (engl. keylogger), näytöntallentimet (engl. screen logger), väärennetyt URL-osoitteet ja kohdennettu tietojenkalastelu. [10] Uusien ja vanhojen tekniikoiden avulla tietojenkalasteluhyökkäysten määrä kasvoi merkittävästi ja jatkaa kasvuaan edelleen.

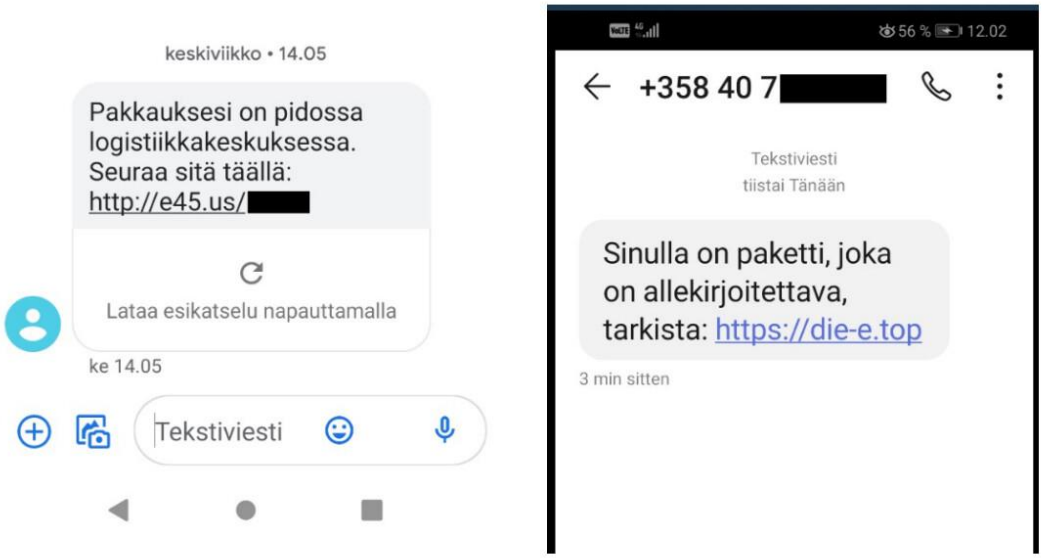
# 4. TIETOJENKALASTELUTEKNIIKAT

Erilaisia tietojenkalastelutekniikoita on monia. Tässä yhteydessä sana tekniikka viittaa käytettyyn hyökkäyskanavaan. Guptan ja muiden mukaan [10] tekniikat voidaan jakaa kahteen pääryhmään: teknisten menetelmien ja käyttäjän manipuloinnin avulla tehtyyn kalasteluun. Tekniset menetelmät voivat olla haittaohjelmia tai ne voivat edesauttaa käyttäjän manipulointia esimerkiksi muuttamalla nettisivun vääräksi käyttäjän huomaamatta. Käyttäjän manipuloinnissa uskotellaan käyttäjä luulemaan, että tietojen luovuttaminen on turvallista ja jopa vaadittua. Yleisesti käyttäjää huijataan asian kiireellisyydellä tai tärkeydellä.

## 4.1 Huijausviestit

Sähköposti on yleisin tapa välittää huijausviesti, mutta huijausviestejä välitetään myös pikaviestien ja sosiaalisen median avulla. Kaikki viestintäkanavat toimivat huijauksen kannalta suunnilleen samalla tavalla. Huijausviestin muodostukseen on eri tapoja. Ensimmäinen tapa on naamioida viesti matkimaan mahdollisimman aidosti luotettavaa tahoa, jolle kohde luovuttaisi tietojaan. Tällainen viesti voi kopioida matkitun tahon tyyliä kirjoittaa viestejä ja sisältää aidon logon. Viestin lähettäjä yrittää myös tehdä lähetyssähköpostiosoitteesta mahdollisimman aidon oloisen. Toinen tapa on lisätä viestiin aikaraja, joka lisää kiireisyyden tunnetta kohteessa. Kohdetta voidaan esimerkiksi pyytää luovuttamaan tiedot tietyssä ajassa jonkin asian uhalla. Kolmas tapa on lisätä viestiin linkki, joka vie väärennetylle nettisivulle. Tietojen luovutus tehdään silloin nettisivulla eikä viestitse. Viestin linkki voi myös sisältää haittaohjelman. Yleensä huijausviestit käyttävät kaikkia kolmea tapaa yhdessä luodakseen mahdollisimman aidon ja houkuttelevan viestin. [11]

Kyberturvallisuuskeskus uutisoi [12] 2021 Postin nimissä tapahtuvista huijausviesteistä. Viestit matkivat Postin paketin saapumisviestejä. Viesti sisälsi linkin, joka vei väärennetylle nettisivulle kysyen käyttäjän henkilö- tai pankkitietoja. Osa viesteistä sisälsi linkin, jota klikkaamalla haittaohjelma asentui käyttäjän laitteelle. Kyseinen viesti on esillä kuvassa 2. Viesti on hyvä esimerkki tyypillisestä huijausviestistä. Kyseisiä viestejä oli paljon liikkeellä.




***Kuva 2.*** *Huijausviestiesimerkki. Kyseiset viestit imitoivat Postilta tulevia viestejä ja veivät joko väärennetylle nettisivulle tai latasivat haittaohjelman. [12]*

## 4.2 Väärennetyt nettisivut

Väärennetyt nettisivut eli valesivustot matkivat jonkin luotetun ja suositun verkkosivuston sisältöä ja ulkoasua. Niiden tarkoituksena on hämätä käyttäjää antamaan hyökkääjälle tietojaan tai asentamaan haittaohjelma huomaamattaan päätelaitteelle. Sivusto voi olla kokonaan hyökkääjän tekemä tai hyökkääjä voi olla muuttanut osaa sivustosta hyödyntäen verkkosovelluksen heikkoutta. Jälkimmäistä kutsutaan nimellä sisällönlisäys (engl. content injection). Hyökkääjän muuttama tai lisäämä osuus kerää käyttäjältä esimerkiksi henkilötietoja ja lähettää ne hyökkääjälle. Muuten sivusto on täysin aito. [13]

Valesivustolle voi harhautua muita tietojenkalastelutekniikoita pitkin. Linkki valesivustolle voi tulla huijausviestin mukana tai hyökkääjä voi hyödyntää hakukoneen mainostilaa nostaakseen valesivuston haun kärkeen. Tällöin mainosta klikkaamalla joutuu valesivustolle. Mainokset hyödyntävät käyttäjän manipulointia esimerkiksi mainostamalla halpoja hintoja. Teknisiä tapoja hyödyntämällä käyttäjä voidaan uudelleenohjata valesivustolle hänen huomaamattaan. Näihin tapoihin lukeutuu DNS-palvelimen ja host-tiedoston myrkytys (engl. DNS and host file poisoning). Molemmat tavat muuttavat sivuston IP-osoitteen vääräksi. [14]

Valesivustoille johtavia linkkejä voidaan naamioida aidoiksi eri tavoilla. Linkkejä voidaan muuttaa lisäämällä numeroita kirjainten tilalle, esimerkiksi tuni.fi voitaisiin muuttaa muotoon tun1.fi. Toinen tapa väärentää linkkiä on lisätä siihen väärä pääte. Esimerkinä tuni.fi.com, jolloin linkki vie sivustolle tuni.com, eikä oikealle sivustolle tuni.fi. URL-

osoitteita voi myös lyhentää ilmaisilla palveluilla, kuten tinyURL. Lyhennettyä linkkiä luodessa sen saa muokata haluamakseen, joten hyökkääjä voisi esimerkiksi luoda linkin tinyurl.com/tuni, joka vie väärennetylle sivustolle. [6]

## 4.3 Puhelinurkinta

Puhelinurkinta (engl. vishing, sanoista voice ja phishing) on tietojenkalastelua puhelimitse [5]. Puhelinurkinnassa hyökkääjä tekee huijauspuhelun kohteelle hyödyntäen käyttäjän manipuloinnin keinoja. Hyökkääjä esittää kohteelle tärkeää tahoa tavoitteenaan saada käsiinsä henkilö- tai pankkitietoja. Esimerkiksi soittaja esittää olevansa pankista ja kertoo havainneensa epätavallista toimintaa kohteen pankkitilillä. Sitten soittaja haluaa varmistaa kohteen pankkitietojen oikeuden.

Puhelinurkinta on toimiva keino varsinkin, jos siihen yhdistää kohdennettua tietojenkalastelua [5]. Jos aiemmassa esimerkissä hyökkääjä tietää kohteen pankin, se tekee hyökkäyksestä aidomman ja toimivamman. Kohde ei silloin välttämättä tajua, että kyseessä on huijaus, tai ei ainakaan huomaa sitä yhtä nopeasti.

## 4.4 Kohdennettu tietojenkalastelu

Kohdennettu tietojenkalastelu (engl. spear phishing) toimii siten, että hyökkääjä kerää tietoa kohteesta, esimerkiksi työpaikan nettisivuilta tai sosiaalisesta mediasta. Kerättyä tietoa hyödynnetään kohdennetun hyökkäyksen tekemiseen. Yleensä kohdennetussa hyökkäyksessä käytetään lopulta sähköpostia. Sähköposti on uskottavamman oloinen, kun se sisältää kerättyä tietoa kohteesta. Kyseessä on siis sosiaalisen manipuloinnin menetelmä. Verrattuna normaaliin huijausviestiin, kohdennetun viestin saanut lankeaa huijaukseen 4,5 kertaa todennäköisemmin [15]. Siksi kohdennettu tietojenkalastelu on yksi tämän hetken käytetyimmistä tekniikoista.

Tästä tavasta hyvä esimerkki on vuonna 2011 tapahtunut kohdennettu tietojenkalasteluhyökkäys RSA:ta kohtaan. Työntekijät olivat saaneet sähköpostiinsa uskottavan oloisen viestin otsikolla “2011 rekrytointisuunnitelma”. Viestissä oli liitteenä taulukko, jota klikatessa haittaohjelma asentui käyttäjän tietokoneelle käyttäen ennalta löydettyä haavoittuvuutta. Hyökkääjät saivat käsiinsä useita tilejä ja arkaluontoista tietoa. [8] Hyökkäys toimi, sillä hyökkääjä tiesi etukäteen, että RSA on lähettänyt samantyylisiä taulukoita työntekijöilleen ennenkin.

## 4.5 Näppäin- ja näytöntallennin

Näppäintallennin (engl. keylogger) ja näytöntallennin (engl. screen logger) ovat haittaohjelmia, jotka tallentavat ja lähettävät käyttäjän syötteet hyökkääjälle. Tallentimet ovat vaarallisia, sillä niiden olemassaoloa tietokoneella on hyvin vaikea huomata. Näppäintallennin seuraa näppäimistön lyöntejä ja lähettää ne hyökkääjälle [16]. Näin hän voi saada selville käyttäjän henkilötietoja ja salasanoja. Yksi tapa vältellä näppäintallenninta on käyttää virtuaalista näppäimistöä.

Näytöntallennin tallentaa uhrin näyttöä ja hiiren liikkeitä [16]. Näyttöä seuraamalla voi saada selville tietoa käyttäjästä tai hänen salasanoistaan. Näytöntallentimella voi myös seurata virtuaalisen näppäimistön lyöntejä. Molemmat ohjelmat vaativat ensin asennuksen käyttäjän laitteeseen. Haittaohjelma voi asentua huijausviestissä tullutta linkkiä painamalla tai käymällä salaamattomalla verkkosivulla.

## 4.6 DNS-tietojenkalastelu

DNS eli nimipalvelujärjestelmä (engl. Domain Name System) muuttaa ihmisen helposti ymmärtämiä verkkotunnuksia laitteiden ymmärtämiksi IP-osoitteiksi, jolloin laite löytää oikealle sivustolle. Jos DNS-palvelimen välimuistiin syötetään väärennettyä tietoa, palvelin myrkyttyy. Myrkytetty palvelin lähettää väärää tietoa eteenpäin ja ohjaa laitteita vääriin IP-osoitteisiin.

Kun hyökkääjä myrkyttää DNS-palvelimen saadakseen uhrin vierailemaan haluamallaan sivustolla, kutsutaan hyökkäystä nimellä DNS spoofing. Tässä hyökkäystekniikassa hyökkääjä on joko luonut oman tai muokannut jo olemassa olevaa nimipalvelinta. Sitten uhrin laite yhdistetään myrkytettyyn palvelimeen. [14] Seuraavaksi uhri ohjataan hyökkääjän luomille väärennetyille verkkosivustoille, joilla yritetään kerätä uhrin henkilö- ja pankkitietoja. Vaihtoehtoisesti verkkosivu voi sisältää haittaohjelmia.

## 4.7 Tietojenkalastelu mobiililaitteissa

Viimeisin pelikenttä tietojenkalastelussa ovat mobiililaitteet. Niiden yleistyessä hyökkääjät löysivät uuden kanavan hyökkäyksilleen. Mobiililaitteiden käyttäjät ovat jopa kolme kertaa alttiimpia tietojenkalasteluhyökkäyksille kuin pöytätietokoneen käyttäjät [14]. Syitä tähän ovat muun muassa näytön pieni koko, käyttöjärjestelmän avoin lähdekoodi ja mobiilikäyttäjien käytöstavat. Näytön koko vaikeuttaa esimerkiksi väärennetyn nettisivun tunnistamista oikeasta. Avointa lähdekoodia käytetään Android-käyttöjärjestelmässä. Lähdekoodin avulla hyökkääjien on helppo kehittää haitallisia sovelluksia. Mobiililaittei-

den käyttö voi olla hankalaa varsinkin vanhemmille ihmisille ja laitteiden monimutkaisuuden vuoksi he eivät välttämättä tiedä minkälaisia tietoturvauhkia sen käyttöön liittyy. Myös hyvin nuoret käyttäjät eivät osaa tunnistaa tietojenkalastelua puutteellisen lukutaidon takia.

Mobiilisovelluksia voidaan hyödyntää tietojenkalastelussa kahdella tapaa. Ensimmäinen tapa on kaapata jo olemassa oleva sovellus ja asentaa sovellukseen vakoilu- tai haittaohjelma. [14] Suosittujen sovellusten tietosuoja on kuitenkin korkea, joten tämä tapa on hyökkääjille vaikea toteuttaa. Toinen tapa on luoda väärennetty sovellus. Väärennetyt sovellukset matkivat aitojen sovellusten logoa ja sisältöä. Sovelluksen mukana voi asentua haittaohjelma tai sovellus voi pyytää useita käyttölupia, jolloin sovelluksen kehittäjä saa mobiililaitteesta paljon tietoa itselleen [14]. Käyttölupien avulla hyökkääjä saa haltuunsa esimerkiksi yhteystiedot, gallerian kuvat ja kameran tai mikrofonin hallinnan. Haittaohjelmat voivat luoda väärennettyjä ilmoituksia, joissa pyydetään uhrin käyttäjätunnuksia tai ne voivat vakoilla uhrin sisäänkirjautumista muihin sovelluksiin. Väärennettyjä sovelluksia on vaikea saada julkaistua valtuutettuihin mobiilisovelluskauppoihin ja niiden lataus tapahtuukin yleensä vain luvattomista sovelluskaupoista.

# 5. TIETOJENKALASTELUN TULEVAISUUS

Sosiaalisen median yleistyessä, myös väärennetyt käyttäjät ja huijausviestit yleistyivät. Samalla tavalla teknologian uusimmat tulokkaat, kuten Internet of Things (IoT) ja koneäly, tuovat mukanaan uusia tietojenkalastelun muotoja. Vaikka erilaisia huijaustekniikoita on jo lukuisia määriä, tekniikat muuttuvat ja niiden määrä kasvaa edelleen. Teknologian saatavuus ja helppokäyttöisyys kasvattavat tietojenkalasteluhyökkäysten määrää, eikä se todennäköisesti häviä tulevaisuudessa. Vaikka käyttäjät tunnistavat huijausyrityksiä entistä paremmin, se ei vähennä hyökkäysten määrää, sillä hyökkääjät kehittävät jatkuvasti uusia tekniikoita. [13]

IoT luo uusia haasteita tietojenkalasteluongelmiin, sillä kaikki yleisimmät turvallisuusmekanismit ovat vaikeita toteuttaa sulautettuihin järjestelmiin [17]. Hyökkääjän on siis helppo kaapata IoT-laitteita omaan käyttöön. Monet IoT-laitteet tallentavat käyttäjän tietoja, joista osa voi olla hyvin arkaluontoisia, kuten terveystietoja. Laitteita voidaan myös käyttää välikäsinä siten, että niiden kautta lähetetään tietojenkalasteluviestejä. Vaikka IoT:tä on kehitetty monia vuosia, sen turvallisuusongelmat ovat edelleen ratkaisematta ja todennäköisesti ovat siten myös läsnä tulevaisuudessa.

Koneäly ja koneoppiminen ovat helpottaneet olemassa olevien ja uusien huijaustapojen kehittämistä. Koneälyä voidaan käyttää nyt myös huijauspuheluissa luomaan väärennettyä ääntä [18]. Tapauksessa hyökkääjä oli luonut koneälyn avulla nuoren naisen apuahuutoja. Hän soitti naisen äidille käyttäen huutoja puhelun taustalla ja väitti kidnapanneensa tyttären vaatien äidiltä lunnaita. Muita koneälyn käyttökohteita ovat olleet haittaohjelmien ohjelmakoodin ja kalasteluviestien kirjoittaminen. Sen avulla kalasteluviestejä voidaan myös muokata kohdennetuiksi tietyille henkilöille. Koska koneälyä kehitetään koko ajan paremmaksi, keksitään sille varmasti lisää uusia väärinkäyttökohteita tulevaisuudessa. Toisaalta koneälyä voidaan myös käyttää ja kehittää avuksi tietojenkalastelun torjumiseen.

Yksi vuoden 2022 hyökkäystrendi oli nollapäivähyökkäykset (engl. zero-day attack) [19]. Hyökkäykset hyödyntävät nollapäivähaavoittuvuuksia eli tietoturva-aukkoja, joille ei ole löydetty korjausta. Hyökkäyksen nimi tulee siitä, että haavoittuvuutta hyödynnetään samana päivänä kuin se löydetään. Tapa tekee hyökkäyksen torjumisen lähes mahdottomaksi, sillä haavoittuvuutta ei ehditä korjata tai hyökkäystä lisätä mustalle listalle. Slash-

Nextin raportin [19] mukaan yli puolet heidän löytämistään hyökkäyksistä oli nollapäivähyökkäyksiä. Tämä tieto vahvistaa ajatusta siitä, että hyökkääjät löytävät jatkuvasti uusia hyökkäysreittejä. Nollapäivähyökkäykset lisääntyvät tulevaisuudessa, sillä ne toimivat.

Toinen uusi trendi on käyttää kahta hyökkäysreittiä samassa hyökkäyksessä [20]. Tällaisessa hyökkäyksessä hyökkääjä lähettää uhrille huijaussähköpostiviestin ja sen lisäksi sähköpostia koskevan teksti- tai ääniviestin. Toisen viestin tarkoitus on lisätä kiireisyyden ja aitouden tunnetta uhrissa ja saada hänet siten avaamaan huijaussähköposti.

Tulevaisuuden tekniikoita voi olla vaikeaa ennustaa, mutta tutkimusta tehdään jatkuvasti. Uusimmista trendeistä saadaan tietoa suoraan hyökkääjiltä esimerkiksi asettamalla heille eräänlaisia ansoja. Yksi näistä tavoista on hunajapurkki (engl. honeypot). Ansa toimii siten, että verkkosivua tai ohjelmaa pidetään tahallaan huonosti suojattuna, jolloin se houkuttelee tekemään hyökkäyksen. Hyökkäystä seurataan, jotta opitaan hyökkääjän tapoja ja mahdollisia uusia trendejä. [21]

# 6. KESKUSTELU

Aiempien tutkimusten perusteella löytyi useita tietojenkalastelutekniikoita. Osa tekniikoista pohjautuu suoraan käyttäjän manipulointiin, osa teknisiin toteutuksiin ja osa on näiden molempien yhdistelmiä. Tutkimusten valossa hyökkääjien käytössä on selkeästi sekä vanhat että uudet tekniikat. Tämä voi tarkoittaa sitä, että vaikka uusien tekniikoiden määrä kasvaa, vanhat tekniikat ovat edelleen suosittuja.

Monelta tietojenkalastelutekniikalta on onneksi yksinkertaista suojautua. Tieto on tärkein osa suojautumista. Jos tuntee mahdolliset huijaukset, niitä on myös helpompi vältellä. Tämä pätee varsinkin sosiaalista manipulointia hyödyntäviin hyökkäyksiin. Tietojenkalasteluhyökkäysten lukumäärän kasvaessa myös tietämys hyökkäyksistä on kasvanut. Koska uusista hyökkäyksistä uutisoidaan laajalti, moni osaa jo tunnistaa ainakin perinteisimmät hyökkäystavat eikä lankea niihin.

Teknisiä hyökkäyksiä on vaikeampi välttää. Suurimpaan osaan niitä auttaa viruksentorjuntaohjelmat, ajantasaiset ohjelmistopäivitykset ja vain salattujen verkkosivujen käyttäminen. Tietoisuus auttaa myös siis teknisten tapojen ehkäisyyn. Myös moni tietokoneohjelma vaatii nykyään toimiakseen sen, että päivitykset ovat ajan tasalla.

Tutkitun aineiston perusteella tietojenkalastelutekniikat ovat muuttuneet osittain. Ensimmäisissä AOL-keskustelupalstan hyökkäyksissä hyödynnettiin käyttäjän manipulointia eri tavoin. Samanlaisia manipulointihyökkäyksiä tehdään edelleen, melkein kolmekymmentä vuotta myöhemmin, esimerkkinä luvussa 5 kuvailtu puhelinhyökkäys. Hyökkäysten perusta, käyttäjän manipulointi, on siis edelleen samanlaista, mutta toteutustapa on voinut muuttua. Oletettavissa on, että taas kolmenkymmenen vuoden päästä on keksitty uusi tapa hyödyntää käyttäjän manipulointia. Huijausviestit ovat yksi asia, joka ei juurikaan ole muuttunut. Viestejä oli jo 1990-luvulla ja ne ovat edelleen hyvin samantyylisiä, siten luultavasti myös tulevaisuudessa.

Uusia tekniikoita 1990-lukuun verrattuna ovat esimerkiksi koneälyä, sosiaalista mediaa ja IoT:tä hyödyntävät hyökkäykset. Uutta hyökkäyksissä on vain hyökkäyksen reitti, sillä hyökkäykset perustuvat edelleen ihmisen heikkouksiin. Koneäly on vasta kehittymässä ja kaikkia sen mahdollisuuksia ei osata ennustaa, joten uusia hyökkäysmahdollisuuksia on todennäköisesti tulossa lisää. Toisaalta koneälyn avulla on luotu myös uusia estämiskeinoja tietojenkalastelulle. On siis hyvin mahdollista, että sen keksimien hyökkäyksien tahtiin kehittyvät myös puolustuskeinot.

# 7. YHTEENVETO

Tämän tutkielman tarkoituksena oli selvittää, millaisia tietojenkalastelutekniikoita on olemassa ja ovatko tekniikat muuttuneet tarkastelulla aikavälillä. Tarkoituksessa onnistuttiin, sillä tekniikoita löydettiin useita. Myös tekniikoiden muutoksia ja samankaltaisuuksia löydettiin ja analysoitiin.

Tietojenkalastelu on merkittävä kyberturvallisuusriski ja siitä koituu paljon haittaa yhteiskunnalle, niin organisaatioille kuin yksilöillekin. Sitä on tapahtunut aina, mutta viimeisen kahdenkymmenen vuoden aikana hyökkäysten lukumäärä on räjähtänyt. Tietojenkalastelusta on tullut yksi vaarallisimmista kyberhyökkäystavoista nykyaikana. Hyökkäykset ovat myös käyneet todella kalliiksi organisaatioille.

Tietojenkalastelu perustuu käyttäjän manipulointiin ja on sen yleisin esiintymismuoto. Käyttäjän manipulointi perustuu ihmisluonteeseen, jonka yksi heikkous on hyväuskoisuus. Manipuloinnin avulla tehdyt tietojenkalasteluhyökkäykset toimivat usein, sillä uhri ei osaa aavistaa kyseessä olevan hyökkäys. Manipulointihyökkäykset ovat suosittuja, sillä ne eivät vaadi paljon resursseja. Lisäksi kiinnijäämisen riski on pieni. Onnistuessaan hyökkäykset ovat rahallisesti kannattavia.

Teknisten apukeinojen käyttäminen on myös mahdollinen tapa tehdä tietojenkalastelua. Tekniset hyökkäykset ovat vaikeampia toteuttaa, mutta ne onnistuvat useammin kuin manipulointia hyödyntävät. Usein teknisten hyökkäysten yhteydessä hyödynnetään myös käyttäjän manipulointia. Tällaisissa hyökkäyksissä toinen tapa vahvistaa toista.

Tietojenkalastelulle on tullut monia uusia hyökkäystekniikoita ajan saatossa. Tässä tutkielmassa kuitenkin huomattiin, että sekä uudet että vanhat tekniikat hyödyntävät käyttäjän manipulointia enemmän tai vähemmän. Uusia kanavia hyökkäyksille on tullut paljon, esimerkiksi mobiililaitteet ja sosiaalinen media. Näistä uusia kanavia käyttävistä hyökkäyksistä suurin osa perustuu edelleen käyttäjän manipulointiin.

Tulevaisuuden hyökkäystekniikoita on vaikea ennustaa. Esimerkiksi koneäly on vielä kehittymässä ja tutkimukset sen mahdollisuuksista ovat kesken. Varmana voi kuitenkin pitää sitä, että tietojenkalastelu ja käyttäjän manipulointi eivät tule häviämään pitkään aikaan. Uusia keinoja kehittyy jatkuvasti ja niiltä suojautuminen vaatii kaikilta tietämystä ja tarkkaavaisuutta.

# LÄHTEET


[1] Cost of a Data Breach Report, IBM, verkkosivu
Saatavissa (viitattu 28.2.2023):
https://www.ibm.com/reports/data-breach

[2] Viheliäinen pornokiristys leviää suomalaisten sähköposteissa – Kyberturvallisuuskeskus antaa ohjeet tilanteiden varalle, Aamulehti, verkkosivu
Saatavissa (viitattu 28.2.2023):
https://www.aamulehti.fi/rikos/art-2000009025776.html

[3] A. Buchanan, Power and Conservation: The Importance of the History of Technology, Icon, Vol. 17, Iss. 17, 2011, pp. 3–11.

[4] OPWNAI: Cybercriminals starting to use ChatGPT, CheckPoint Research, verkkosivu
Saatavissa (viitattu 28.2.2023):
https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

[5] C. Hadnagy, Social Engineering: The Science of Human Hacking, John Wiley & Sons, Incorporated, 2018.

[6] M. Rader, S. Rahman, Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks, International Journal of Network Security & Its Applications (IJNSA), Vol. 5, No. 4, July 2013, pp. 23–41.

[7] M. Khonji, Y. Iraqi, A. Jones, Phishing Detection: A Literature Survey, IEEE Communications Surveys and Tutorials, Vol. 15, No. 4, 2013, pp. 2091—2121.

[8] K. Krombholz, H. Hobel, M. Huber, E. Weippl, Advanced social engineering attacks, Journal of Information Security and Applications, Vol. 22, 2015, pp. 113–122.

[9] K. Rekouche, Early Phishing, 2011.

[10] B. B. Gupta, A. Tewari, A. K. Jain, D. P. Agrawal, Fighting against phishing attacks: state of the art and future challenges, Neural Computing & Applications, Vol. 28, No. 12, 2017, pp. 3629–3654.

[11] J. Rastenis, S. Ramanauskaitė, J. Janulevičius, A. Čenys, A. Slotkienė, K. Pakrijauskas, E-mail-Based Phishing Attack Taxonomy, Applied Sciences, Vol. 10, Iss. 7, 2020, pp. 2363.

[12] Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus, Kyberturvallisuuskeskus, verkkosivu.
Saatavissa (viitattu 3.3.2023):
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

[13] A. Smith, Content Spoofing, OWASP, verkkosivu
Saatavissa (viitattu 25.3.2023):
https://owasp.org/www-community/attacks/Content_Spoofing

[14] D. Goel, A. K. Jain, Mobile phishing attacks and defence mechanisms: State of art and open research challenges, Computers & Security, Vol. 73, 2017, pp. 519–544.

[15] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, Social phishing, Communications of the ACM, Vol. 50, No. 10, 2007, pp. 94–100.

[16] N. Adhikary, R. Shrivastava, A. Kumar, S. Verma, M. Bag, V. Singh, Battering Keyloggers and Screen Recording Software by Fabricating Passwords, International Journal of Computer Network and Information Security, Vol. 4, Iss. 5, 2012, pp. 13–21.

[17] R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, Computer, Vol. 44, No. 9, Sept. 2011, pp. 51–58.

[18] A. Cuthbertson, AI clones child's voice in fake kidnapping scam, Independent, verkkosivu
Saatavissa (viitattu 15.4.2023):
https://www.independent.co.uk/tech/ai-voice-clone-scam-kidnapping-b2319083.html

[19] The State of Phishing Report 2022, SlashNext, verkkosivu
Saatavissa (viitattu 8.5.2023):
https://www.slashnext.com/the-state-of-phishing-2022/

[20] Bob Violino, Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them, verkkosivu.
Saatavissa (viitattu 8.5.2023):
https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

[21] A. Bhadane, SB. Mane, State of Research on Phishing and Recent Trends of Attacks, I-Manager's Journal on Computer Science, Vol. 5, No. 4, 2018, pp. 14–35.