Markus Savolainen

Kalasteluhyökkäykset, huijaussivustot ja niiltä suojautuminen

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Markus Savolainen

Yhteystiedot: markus.k.savolainen@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Kalasteluhyökkäykset, huijaussivustot ja niiltä suojautuminen

Title in English: Phishing attacks, scam websites and how to protect user from them

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 18+0

Tiivistelmä: Kalasteluhyökkäykset ja niihin liittyvät huijaussivustot ovat ajankohtaisia uhkia, sekä myös suosituimpia hyökkäysmuotoja, joita kyberrikolliset käyttävät. Tämän tutkimuksen tavoitteena oli muodostaa kokonaiskuva kalasteluhyökkäyksistä ja huijaussivustoista, sekä kerätä tärkeimpiä keinoja niille altistumisen ehkäisemiseen. Tutkimuksesta selviää, että kalasteluhyökkäyksien eri muodot ovat kehittyneet huomattavasti tekniikan ja viestintäkanavien mukana ja, että tekoäly muodostaa uusia uhkia kalasteluhyökkäysten hyödyntämiseen. Tekoälyä voidaan myös käyttää avuksi suojautuessa kalasteluhyökkäyksiltä ja tunnistamaan niitä paremmin.

Avainsanat: kalasteluhyökkäys, huijaussivusto, kyberturvallisuus

Abstract: Phishing attacks and scam websites that are included with them are current threats and also one of the most popular attack methods that cybercriminals use. The purpose of this research was to form an overall picture of phishing attacks and scam websites and also to collect some of the most important means to prevent exposure to them. The research reveals that the forms of phishing attacks have developed considerably with the development of technology and channels of communication and that artificial intelligence creates new threats to make use of phishing attacks. Artificial intelligence can also be used to help protect from phishing attacks and to better recognize them.

Keywords: phishing attack, scam website, cybersecurity

Sisällys

1 Johdanto

Kalasteluhyökkäykset ovat olleet rikollisten suosiossa jo pitkään ja hyökkääjät ovat vuosien saatossa oppineet hyödyntämään niitä entistä paremmin. Kalasteluhyökkäystekniikat ovat monipuolistuneet huomattavasti alkuaikojen huijaussähköposteista ja huijaussivustoista. Rikolliset ovat ottaneet käyttöön mm. tekstiviestejä, twiittejä ja URL-osoitteita hyödyntävät kalasteluhyökkäykset (Abdillah ym. 2022). Viime vuosina yleistyneet tekoäly ja koneoppiminen ovat myös vaikuttamassa kalasteluhyökkäysten hyödyntämiseen (Mirsky ym. 2023), sekä myös niiden torjuntaan (Basit ym. 2021).

Tutkimusaiheena tässä tutkimuksessa on tarkastella kalasteluhyökkäyksiä ja huijaussivustoja käyttäjän näkökulmasta ja erityisesti se, millä eri keinoilla käyttäjä pystyy välttämään huijauksille altistumista ja tärkeän tiedon menetystä.

Tutkimuksessa keskitytään erityisesti niihin tiettyihin tekniikoihin ja työkaluihin, joilla käyttäjä pystyy tunnistamaan kalasteluhyökkäykset ja erottamaan huijaussivustot aidoista, turvallisista verkkosivustoista. Esimerkiksi Althobaiti, Rummani ja Vaniea (2019) käyvät läpi tekniikoita URL-pohjaisten hyökkäysten tunnistamiseen ja siten antavat konkreettisia keinoja hyökkäysten torjumiseen, kun taas Sadiq ym. 2021 tarjoavat universaalimpia keinoja, kuten ohjelmien päivityksistä huolehtimista, sekä palomuurien ja virustentorjuntaohjelmien asentamisen kaltaisia keinoja. Viime vuosina mukaan ovat tulleet koneoppimiseen, algoritmeihin ja tekoälyyn perustuvat kalasteluhyökkäysten tunnistuskeinot (Al-Qahtani ja Cresci 2022).

Luvussa 2 käsitellään motivaatiota kalasteluhyökkäyksille, sitä millä tavoin niille altistutaan ja sitä millaisia vaikutuksia hyökkäyksillä on kohteisiinsa. Luvussa 3 keskitytään itse hyökkäysten toteutustapoihin, erilaisiin kalasteluhyökkäysten muotoihin, huijaussivustojen muotoihin, sekä koneoppimisen ja tekoälyn hyödyntämiseen hyökkäyksissä. Luvussa 4 käsitellään hyökkäyksiltä suojautumisen keinoja yleisesti, erilaisia sosiaalisia ja teknisiä suojautumiskeinoja, sekä koneoppimista ja tekoälyä hyökkäyksiltä suojautumisessa.

2 Hyökkäysten motivaatiot ja niille altistuminen

Tässä osiossa käsitellään sitä, mikä motivoi hyökkääjiä, miten käyttäjä altistuu hyökkäyksille ja mitä vaikutuksia hyökkäyksillä on kohteisiin. Kalasteluhyökkäykset ja huijaussivustot ovat yleisiä kyberhyökkäysten muotoja, joilla pyritään harhauttamaan käyttäjää luovuttamaan hyökkääjälle tärkeää tietoa.

2.1 Motivaatiot hyökkäyksille

Kalasteluhyökkäyksiä, kuten muitakin kyberrikollisuuden muotoja motivoivat erilaiset syyt. Dhanjani, Rios ja Hardin (2009) listaavat erilaisiksi motivaattoreiksi rahallisen hyödyn, koston, kiristyksen ja tiedon keruun. Lisäksi motivaatio riippuu siitä, käyttääkö hyökkääjä kohdennettuja vai opportunistisia hyökkäyksiä. Opportunistisissa hyökkäyksissä ei sinällään kohdenneta hyökkäystä tiettyyn kohteeseen, mutta niissä käytetään hyväksi kohteen heikkouksia, joita Lallie ym. (2021) nimittävät koukuiksi (engl. Hooks). Näitä koukkuja hyödyntäen rikolliset pyrkivät harhauttamaan uhrin tekemään virheitä ja lankeamaan huijaukseen (Lallie ym. 2021). Opportunistiset hyökkäykset yleistyvät usein merkittävien tapahtumien, kuten luonnonmullistusten ja julkisuuden henkilöihin kohdistuneiden tapahtumien yhteydessä (Lallie ym. 2021).

Suurin osa hyökkäyksistä tavoittelee jollain tavalla rahallista hyötyä suoraan tai välillisesti. Hyökkääjä kerää tietoa yleensä juuri hyötyäkseen siitä jotenkin myös rahallisesti (Dhanjani, Rios ja Hardin 2009). Kalasteluhyökkäyksillä voi myös olla muitakin kuin rahallisia motivaatioita. Alkhalil ym. (2021) jaottelee hyökkääjät neljään eri joukkoon: ns. script kiddiet, jolla tarkoitetaan muiden tekemiä hyökkäysskriptejä hyödyntäviä hyökkääjiä, vakavamieliset krakkerit, järjestäytyneet rikolliset ja terroristit. Näistä ryhmistä kaksi ensimmäistä keskittyy enimmäkseen rahallisen hyödyn tavoitteluun, tiedon varastamiseen ja tuhoamiseen, mutta järjestäytyneet rikollisryhmät ja terroristit voivat saada aikaan merkittävää vahinkoa jopa kansalliseen turvallisuuteen vaikuttavia tietoja varastamalla (Alkhalil ym. 2021). Ammattilaishakkereista koostuvat järjestäytyneet rikollisryhmät voivat myös myydä hyökkäyksiä valmiina palveluna muille ryhmille, kuten terroristeille (Alkhalil ym. 2021).

2.2 Altistumisvektorit

Kalasteluhyökkäyksen toteuttaja valitsee erilaisten keinojen välillä, joilla hyökkäyksen kohteeseen pyritään vaikuttamaan ja saamaan kohde altistumaan hyökkäykselle. Tyypillisimpiä keinoja ovat yleensä sähköpostin, tekstiviestien ja muiden viestintäsovellusten avulla levitettävät huijausviestit, joilla kohde saadaan erehdytettyä avaamaan esimerkiksi huijaussivusto. Myös sosiaalisen median ja äänipuhelujen kautta voidaan toteuttaa kalasteluhyökkäyksiä, esimerkiksi puheluja hyödyntäviä kalasteluhyökkäyksiä voidaan toteuttaa massoittain ja edullisin kustannuksin, kuten sähköpostien välityksellä kin. (Aleroud ja Zhou 2017). Sähköpostit ovat olleet perinteisesti kalasteluhyökkääjien eniten suosima viestintäkanava hyökkäysten toteuttamiseen, joissa viestin lähettäjä yleensä tekeytyy jonkin organisaation, kuten pankin edustajaksi ja kehottaa avaamaan viestissä mukana tulleen linkin huijaussivustolle tai troijalaisen sisältämän liitetiedoston Alkhalil ym. (2021).

COVID-19 -pandemia lisäsi kalasteluhyökkäysten määrää ja siten lisäsi altistumisvektoreita ihmisten jäädessä etätöihin. Kun etätöihin siirryttiin nopealla aikataululla ja työntekijöitä ei ehditty kouluttaa tarpeeksi turvalliseen etätyöskentelyyn, jäi tietoturvan taso vajaaksi. Myös pandemian ruuhkauttaman terveydenhuollon työntekijöiden havaittiin olevan alttiimpia kalasteluhyökkäyksille kiireen ja väsymyksen vuoksi. (He ym. 2021). Pandemian aiheuttaman paniikin varjolla kalasteluhyökkäyksiä toteutettiin myös rekisteröimällä paljon koronavirukseen liittyviä domain-nimiä ja lähetettiin kalasteluviestejä terveysviranomaisten ja järjestöjen nimissä yrittäen saada huolestuneita uhreja lankeamaan huijauksiin (Lallie ym. 2021).

2.3 Hyökkäysten vaikutukset

Kalasteluhyökkäysten vaikutukset kohteisiin voivat vaihdella suuresti riippuen kohteesta ja hyökkäyksen onnistumisesta. Erilaisia hyökkäysten vaikutuksia voivat olla mm. tiedon menetys, rahalliset menetykset, mainehaitat ja työresurssien hukkaaminen (Alkhalil ym. 2021). Pelkästään rahalliset menetykset voivat olla isoja ja vaihdella yksityishenkilöillä tuhansista ja yrityksillä jopa miljooniin dollareihin onnistunutta hyökkäystä kohden (Abbasi ym. 2015). Myös mainehaitat yrityksille voivat olla merkittäviä, kun kalasteluhyökkäyksissä käytetään hyväksi oikeiden ja rehellisten yritysten asiakkaita. Hadi, Aburub ja Alhawari (2016) to-

teavat, että kalasteluhyökkäysten takia pankkien asiakkaat olivat epävarmempia luottamaan pankkien palveluihin.

Kalasteluhyökkäysviestien mukana tulleet liitetiedostot voivat levittää järjestelmään monenlaisia haittaohjelmia. Alkhalil ym. (2021) mainitsevat mm. näppäintallentimet (engl. Keylogger) ja näytöntallentimet (engl. Screenlogger), jotka lähettävät käyttäjän kirjoittamat näppäinkomennot tai koko näytön näkymän suoraan hyökkääjälle. Alkhalil ym. (2021) mainitsevat myös virukset, tietoja varastavat spyware-vakoiluohjelmistot, mainoksia käyttäjälle näyttävät adware-mainosohjelmistot, sekä järjestelmän kaappaavat ransomware-kiristysohjelmistot, jotka salakirjoittavat käyttäjän tiedostot vaatien lunnaita maksettavaksi tiedostojen palautusta vastaan.

3 Hyökkäykset

Tässä osiossa käsitellään kalasteluhyökkäysten ja huijaussivustojen erilaisia toteutustapoja, sekä koneoppimisen ja tekoälyn hyödyntämistä hyökkääjien toimesta.

Kalasteluhyökkäyksiä voidaan toteuttaa monilla eri tavoilla ja niiden muodot vaihtelevat, sekä kehittyvät myös tekniikan kehittyessä. Lähteestä riippuen kalasteluhyökkäyksiksi lasketaan erilaisia hyökkäysmuotoja ja hyökkäystapoja. Gupta, Singhal ja Kapoor (2016) listaavat erilaisten kalasteluhyökkäysten tyypeiksi huijaussähköpostit, sosiaalisen median huijaustilit, tietomurrot ja troijalaiset. Abdillah ym. (2022) täydentävät listaa huijaussivuilla, huijaussivustoilla, URL-hyökkäyksillä, taloustietojen kalastelulla, huijaustwiiteillä ja -tekstiviesteillä.

Edellä mainituista kalasteluhyökkäyksistä melkein kaikille yhteistä on johdattaa kohde oikeaa verkkosivustoa muistuttavalle huijaussivustolle, jossa käyttäjältä pyritään onkimaan tietoa, jota hän sivustolle syöttää. Käyttäjä voi myös päätyä huijaussivustolle esimerkiksi suoraan hakukoneen kautta etsiessään virallista sivustoa. (Alkhalil ym. 2021). Yleisimpiä kalasteluhyökkäysten muotoja vuonna 2020 olivat huijaussivut ja -sivustot, sekä huijaussähköpostit (Abdillah ym. 2022).

3.1 Kalasteluhyökkäykset

Kalasteluhyökkäykset (engl. Phishing), jakaantuvat itsessään monenlaisiin hyökkäystyyppeihin, joista mainittakoon Spear phishing, Whale phishing, Angler phishing, Smishing, Vishing ja Pharming. Tavallinen kalasteluhyökkäys on yleensä suuntaamaton ja kohdennettu sattumanvaraisesti. Suuntaamattoman kalasteluhyökkäyksen onnistumisprosentit ovat alhaisia ja niihin lankeavat yleensä vain varomattomimmat uhrit. (Abdillah ym. 2022).

Edellä mainittu Spear phishing tarkoittaa kohdennettua kalasteluhyökkäystä, jossa tiettyyn henkilöön tai organisaatioon kohdistetaan täsmähyökkäys (Aleroud ja Zhou 2017). Kohdennettujen hyökkäysten onnistumisprosentit ovat korkeammat kuin kohdentamattomien ja yksi niiden alamuoto on Whale phishing, jossa hyökkäys kohdennetaan mahdollisimman korkeaarvoiseen uhriin, kuten yritysjohtoon tai poliitikoihin (Abdillah ym. 2022). Angler phishing

tarkoittaa hyökkäystä, jossa jäljitellään jonkin organisaation sosiaalisen median tiliä, jonka myötä saadaan kyseisen organisaation asiakkailta kalasteltua tietoa. Myös Angler phishing hyökkäyksissä voidaan hyökkäys kohdentaa tiettyyn henkilöön. Smishing tarkoittaa tekstiviestien välityksellä toteutettuja kalasteluhyökkäyksiä. Vishing tarkoittaa äänipuhelujen kautta tehtyjä kalasteluhyökkäyksiä, joissa voidaan hyödyntää valmista tekstiä lukevaa robottiääntä kohteen harhauttamiseen. Pharming tarkoittaa hyökkäystä, jossa käyttäjän laitteelle asennettu troijalainen ohjaa oikealle verkkosivustolle tarkoitetun liikenteen huijaussivustolle. (Syafitri ym. 2022).

3.2 Huijaussivut ja huijaussivustot

Kuten luvun alussa jo mainittiin, on kalasteluhyökkäysten päämääränä yleensä saada kohde jollain keinolla johdateltua huijaussivulle (engl. Phishing webpage) tai -sivustolle (engl. Phishing website), joilla jäljitellään oikean organisaation verkkosivuja (Abdillah ym. 2022). Näille sivuille päädytään yleensä käyttäjän saaman viestin (Abdillah ym. 2022) välityksellä, klikkaamalla mainoslinkkiä (Varshney, Misra ja Atrey 2016) tai hakukoneen kautta oikeaa verkkosivustoa etsimällä (Alkhalil ym. 2021). Hakukoneen kautta levitettävien huijaussivustojen suosiota nostetaan keinotekoisesti hakukoneen optimointitaktiikkoja (engl. Search Engine Optimization Tactics) käyttäen, jotta huijaussivustot saataisiin nousemaan mahdollisimman korkealle hakukoneen hakutuloksissa (Alkhalil ym. 2021). Korkealle listattuina hakukoneissa olevat huijaussivustot voivat helposti harhauttaa käyttäjän päätymään oikean sivuston sijaan huijaussivustolle.

Näitä edellä mainittuja huijaussivustoja käytetään erilaisiin tarkoitusperiin, kuten rahallisen hyödyn tavoitteluun esimerkiksi jäljittelemällä aitoa verkkokauppaa (engl. Concocted website) ja käyttäjätunnusten varastamiseen (engl. Spoof website) (Abbasi ym. 2015). Huijaussivustot ovat yleensä melko vakuuttavasti tehtyjä jäljittelemään oikeaa verkkosivustoa ja varsinkin kokemattomat käyttäjät voivat syöttää epähuomiossa tärkeää tietoa huijaussivustolle, josta tiedot päätyvät siten hyökkääjän käsiin (Varshney, Misra ja Atrey 2016).

3.3 Koneoppiminen ja tekoäly hyökkäyksissä

Koneoppiminen ja tekoäly ovat yleistyneet viime vuosina hurjalla vauhdilla ja niitä käytetään yhä enemmän hyödyllisiin tarkoituksiin, kuten tiedon hakemiseen ja itseohjautuvien autojen ohjaamiseen. Uutta teknologiaa voidaan myös hyödyntää ikävämpiin tarkoituksiin, eivätkä kalasteluhyökkäykset ole poikkeus. Mirskyn ym. mukaan tekoälyä voitaisiin käyttää kalasteluhyökkäysten automatisointiin parantaen niiden tehokkuutta (Mirsky ym. 2023). Hyökkääjä voisi toteuttaa tekoälyn avulla massiivisia äänipuheluja hyödyntäviä hyökkäyskampanjoita. Tekoälyä voidaan myös käyttää Spear Phishingiä hyödyntäviin kohdennettuihin kalasteluhyökkäyksiin, jossa botti soittaa kohteelle puhelun jäljitellen oikean henkilön ääntä tai kuvaa. (Mirsky ym. 2023). Mirskyn ym. keräämään tiedon mukaan tekoälyä on jo hyödynnetty kalasteluhyökkäyksissä ja kohteilta on mm. varastettu suuria summia rahaa (Mirsky ym. 2023).

Tekoälyn kehittyessä vielä entisestään voivat jo pitkään käytössä olleet kalasteluhyökkäyksiä muistuttavat huijausmuodot saada uusia, entistä vakuuttavampia muotoja. Ns. Nigerialaiskirjeet muistuttavat hyvin paljon tavallisia kohdentamattomia kalasteluhyökkäyksiä, mutta luottavat huijaussivustoille johtavien linkkien sijaan enemmän tekstiin ja motiivi on yleensä rahallinen (Stojnic, Vatsalan ja Arachchilage 2021). Romanssihuijauksissa motiivi on myös rahallinen, mutta uhria yritetään huijata keinotekoisen sosiaalisen median tilin avulla lähettämään rahaa hyökkääjälle vetoamalla romanttisiin tunteisiin (Whitty 2019). Stojnic, Vatsalan ja Arachchilage (2021) pitävät Nigerialaiskirjeitä lähinnä vanhentuneina ja enemmän nykyaikaisten kalasteluhyökkäysten esiasteina. Tekoäly tuo uusia mahdollisuuksia Nigerialaiskirjeitä ja romanssihuijauksia tehtailevien huijareiden käyttöön ja niiden suosio voi hyvinkin lähteä uudelleen nousuun.

Tekoälyn mahdollistamat syväväärennökset (engl. Deepfakes) ovat esimerkki uudesta uhasta, jota nämä edellä mainitut huijarit voisivat käyttää hyödyksi. Syväväärennökset mahdollistavat entistä vakuuttavampien henkilöväärennösten käytön tietojenkalasteluhyökkäyksissä tekoälyn kehittymisen myötä ja ne koetaankin suurimpina tekoälyn muodostamina uhkina (Mirsky ym. 2023). Syväväärennösten uhreiksi voisi joutua myös niitä, joihin perinteiset Nigerialaiskirjeet ja romanssihuijaukset eivät muuten tehoa. Whittyn mukaan oikeiden sosiaalisen median tilien ja romanssihuijauksissa käytettyjen väärennösten erottaminen toisistaan on

jo nyt vaikeaa (Whitty 2019). Syväväärennökset ovatkin oivallinen mahdollisuus rikollisille ottaa nämä vanhat huijausmuodot uudelleen käyttöön entistä vaarallisempina.

4 Hyökkäyksiltä suojautuminen

Tässä osiossa käsitellään keinoja, joilla hyökkäyksiltä voidaan suojautua. Erilaiset suojautumiskeinot on lajiteltu sosiaalisiin, teknisiin keinoihin, sekä koneoppimisen ja tekoälyn hyödyntämiseen hyökkäyksiltä suojautumisessa.

Kalasteluhyökkäyksiltä suojautuminen on haastavaa jo siinä mielessä, että kalasteluhyökkäykset tapahtuvat monilla eri tavoilla ja alustoilla. Kuten tietoturvassa yleisestikin, on tärkeintä ensin huolehtia, että laitteiden, käyttöjärjestelmien ja sovellusten tietoturva, sekä päivitykset ovat ajan tasalla. Vaikka tietoturvasta pitäisikin huolta, on erilaisten kalasteluhyökkäysten torjuminen kokonaan käytännössä mahdotonta. Esimerkiksi huijaussähköposteista voidaan torjua teknisin keinoin jopa 99 prosenttia (Aleroud ja Zhou 2017), mutta läpi pääsevä 1 prosentti aiheuttaa potentiaalisesti paljon ongelmia. Ihmisiä tarvitaan raportoimaan ja kouluttamaan automaattisia järjestelmiä, jotta ne toimisivat paremmin hyökkäyksiä vastaan (Althobaiti, Rummani ja Vaniea 2019).

4.1 Sosiaaliset suojautumiskeinot

Kalasteluhyökkäykset on suunniteltu kohdistumaan ihmisiin ja vaikka tekniset keinot auttavat niiden torjumisessa, on vähintään yhtä tärkeää kiinnittää huomiota sosiaalisiin suojautumiskeinoihin. Althobaiti, Rummani ja Vaniea (2019) nostavat esiin ihmisten kouluttamisen tärkeyden URL-kalasteluhyökkäysien tunnistuksessa, mutta toteavat että automaatiota tarvitaan väistämättä ihmisten tueksi hyökkäyksien välttämiseksi. URL-osoitteen tunnistaminen aidosta huijaukseksi ilman koneellista apua on joissain tapauksissa erittäin vaikeaa, koska URL-osoitteen muodostamiseen sallitaan sekä ASCII-, että unicode-merkkejä, jolloin samankaltaiset merkit voivat todellisuudessa olla täysin eri merkkejä (Althobaiti, Rummani ja Vaniea 2019). Alkhalil ym. (2021) toteavat, että käyttäjien koulutuksessa keskitytään enimmäkseen huijaussähköpostien ja huijaussivustojen tunnistukseen muiden kalasteluhyökkäysten muotojen varautumisen kustannuksella. Käyttäjien koulutuksessa pitäisi Alkhalilin ym. mukaan keskittyä kolmeen suuntaukseen: käyttäjien tiedon lisäämiseen kalasteluhyökkäyksistä, järjestämällä tekaistuja kalasteluhyökkäyksiä ja siten testaamalla käyttäjien toimintaa,

sekä pelillistämällä kalasteluhyökkäysten koulutusta (Alkhalil ym. 2021). Käyttäjien tulisikin tietää ainakin perusteet kalasteluhyökkäyksistä ja raportoida hyökkäyksistä aina eteenpäin organisaatiossa (Alkhalil ym. 2021).

4.2 Tekniset suojautumiskeinot

Tekniset keinot kalasteluhyökkäyksiltä suojautumisessa ovat isossa osassa, koska ihmisiin kohdistuvat hyökkäykset voidaan tehokkaasti torjua ennen kuin ne edes saavuttavat käyttäjän. Zuraiq ja Alkasassbeh (2019) listaavat neljä keinoa, joilla kalasteluhyökkäyksiä voidaan torjua: mustan listan (engl. Blacklist) käytön, sisältöpohjaisen (engl. Content based), heuristisen (engl. Heuristic) ja sumeiden sääntöjen (engl. Fuzzy rules) käytön.

Edellä mainituille mustille listoille kerätään epäiltyjä ja varmistettuja huijaussivustojen URL-osoitteita, joihin sivuja vertaillaan esimerkiksi Google Safe Browsing tai Phish Tank -palveluita hyödyntäen, sekä käyttäjän internet-selaimen avustuksella (Zuraiq ja Alkasassbeh 2019). Sisältöpohjaisilla keinoilla tarkastellaan tutkittavan URL:n ja HTML-sivuston, sekä oikean sivuston eroavaisuuksia sivustojen sisällön, kuten kuvien perusteella. Heuristisilla keinoilla vertaillaan tutkittavan ja oikean sivuston URL-osoitteiden ominaisuuksia. Sumeiden sääntöjen keinoilla tutkittavaa sivustoa vertaillaan kalastelusivustoihin erilaisten metriikoiden ja sääntöjen perusteella. (Zuraiq ja Alkasassbeh 2019).

Näistä edellä mainituista keinoista mikään ei kuitenkaan Zuraiqin ja Alkasassbehin mukaan yksistään osoittautunut toista paremmaksi, vaan kaikkia keinoja tarvitaan (Zuraiq ja Alkasassbeh 2019). Mustan listan käyttö yksinään ei kuitenkaan Zuraiqin ja Alkasassbehin mukaan riitä huijaussivustojen massiivisesta määrästä ja niiden tilapäisyydestä johtuen, vaan tarvitaan parempia tekniikkoja, kuten joku muista edellä mainituista (Zuraiq ja Alkasassbeh 2019). Althobaiti, Rummani ja Vaniea (2019) taas näkevät mustille listoille enemmän käyttömahdollisuuksia johtuen niiden tarkkuudesta, mutta myöntävät myös niiden riittämättömyyden kaikkien huijaussivustojen estoon. Sadiq ym. (2021) taas nostavat esiin näiden lisäksi konventionaalisempia keinoja, jotka ovat kaikkien käyttäjien käytettävissä, kuten palomuurien, kalasteluhyökkäyksiä tunnistavien lisäosien ja virustentorjuntaohjelmistojen käytön hyökkäysten torjunnassa.

4.3 Koneoppiminen ja tekoäly hyökkäyksiltä suojautumisessa

Tekoälyn ja koneoppimisen kehitys on mahdollistanut myös kalasteluhyökkäysten torjunnan parantumisen. Tekoäly on auttanut mm. parantamaan huijaussähköpostien tunnistamista ja koneoppiminen, sekä syvän oppimisen algoritmit parantaneet huijaussivustojen tunnistusta. Basit ym. näkevät haasteina skaalauksen ongelmat koneoppimisessa, sekä väärien positiivisten tunnistusten ilmeneminen heuristiikkoja käytettäessä. (Basit ym. 2021). Zuraiq ja Alkasassbeh (2019) käyttivät koneoppimista osana erilaisia keinoja tunnistaa huijaussivustoja, kuten osana sisällön tunnistusta kuvien vertailussa ja heuristisen mallin apuna URL-osoitteiden tunnistuksessa.

Zuraiq ja Alkasassbeh (2019) vertailivat näitä edellä mainittuja koneoppimisen tekniikoita eri tutkimuksissa, joissa tekniikoiden paremmuus riippui käytetyn vertailuaineiston suuruudesta ja huijaussivustojen tunnistus onnistui 90 - 98 prosentin välillä. Al-Qahtani ja Cresci taas vertailivat eri tutkimuksissa käytettyjä työkaluja huijaussähköpostien tunnistukseen, ja koneoppimista hyödyntänyt työkalu, HOLMES päihitti jopa kaupalliset työkalut tehokkuudessa (Al-Qahtani ja Cresci 2022). Toinen eri tutkimuksessa käytetty työkalu, EDITH tunnisti huijaussähköpostit myös hyvin, vaikka käyttikin koneoppimisen sijaan vain edellisessä luvussa mainittuja mustia listoja ja heuristiikkoja (Al-Qahtani ja Cresci 2022). Al-Qahtani ja Cresci ehdottavat samantyyppisen työkalun kehittämistä koneoppimista ja tekoälyä hyödyntäen, sekä nostavat vielä esiin ongelmia tekoälyn kouluttamiseen liittyvien tietoaineistojen saatavuudessa ja lajittelualgoritmien käytön koneoppimisessa tehokkaamman syväoppimisen sijaan (Al-Qahtani ja Cresci 2022).

5 Yhteenveto

Tutkimuksesta käy ilmi se, että kalasteluhyökkäykset ja huijaussivustot aiheuttavat edelleen merkittäviä uhkia tietoturvallisuudelle ja tietojen menetykselle. Kalasteluhyökkäysten suosio ei osoita merkkejä hiipumisesta vaan päinvastoin kasvattaa suosiotaan kyberrikollisten keskuudessa. Teknologian kehitys on mahdollistanut uusia kalasteluhyökkäysten muotoja ja kaikki merkittävät viestintäkanavat on valjastettu myös kyberrikollisten käyttöön. Osansa kalasteluhyökkäysten suosion kasvuun viime vuosina on tarjonnut COVID-19 -pandemia, joka etätyöskentelyn lisääntymisen myötä lisäsi altistumisia hyökkäyksille.

Huijaussivustot ovat menneet suosiossa jo kalastelusähköpostien edelle ja ovat uhka myös navigoitaessa verkkosivuille hakukoneen kautta, koska käyttäjä ei välttämättä huomaa ollenkaan tarkistaa sivun oikeellisuutta ennen hakutuloksen valitsemista. Koneoppiminen ja tekoäly mahdollistavat entistä vakuuttavampien kalasteluhyökkäysten tehtailun ja varsinkin oikeita henkilöitä jäljittelevät syvävääreennökset voivat johtaa helposti käyttäjiä harhaan ääni- ja videopuheluissa. Syvävääreennöksistä hyötyjiin kuuluvat mahdollisesti myös rikolliset, jotka tehtailevat Nigerialaiskirjeitä ja romanssihuijauksia.

Kalasteluhyökkäyksiltä suojautuessa käyttäjien kouluttaminen tunnistamaan hyökkäyksiä ja tekniset keinot kalasteluhyökkäysten suodattamiseen ja tunnistamiseen ovat keskiössä. Näiden keinojen avuksi on tullut tekoäly ja koneoppiminen, jotka tehostavat kalasteluhyökkäysten tunnistusta ja siten ehkäisevät hyökkäysten onnistumisia.

Lisää tutkimusta kalasteluhyökkäyksistä tarvitaan myös tulevaisuudessa, varsinkin kun tekoäly kehittyy jatkuvasti mahdollistaen entistä petollisempia ja vakuuttavampia hyökkäyksiä. Käyttäjän onneksi myös kalasteluhyökkäysten tunnistus- ehkäisytekniikat kehittyvät samaa tahtia, joten teknologian kehitys tuo myös turvaa näiltä uhilta.

Lähteet

Abbasi, Ahmed, Fatemeh “Mariam” Zahedi, Daniel Zeng, Yan Chen, Hsinchun Chen ja Jay F Nunamaker Jr. 2015. “Enhancing predictive analytics for anti-phishing by exploiting website genre information”. *Journal of Management Information Systems* 31 (4): 109–157. https://doi.org/10.1080/07421222.2014.1001260.

Abdillah, Rahmad, Zarina Shukur, Masnizah Mohd ja Mohd Zamri Murah. 2022. “Phishing classification techniques: A systematic literature review”. *IEEE Access,* https://doi.org/10.1109/ACCESS.2022.3166474.

Aleroud, Ahmed, ja Lina Zhou. 2017. “Phishing environments, techniques, and countermeasures: A survey”. *Computers Security* 68:160–196. ISSN: 0167-4048. https://doi.org/https://doi.org/10.1016/j.cose.2017.04.006.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf ja Imtiaz Khan. 2021. “Phishing attacks: A recent comprehensive study and a new anatomy”. *Frontiers in Computer Science* 3:563060. https://doi.org/10.3389/fcomp.2021.563060.

Althobaiti, Kholoud, Ghaidaa Rummani ja Kami Vaniea. 2019. “A Review of Human- and Computer-Facing URL Phishing Features”. Teoksessa *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSPW),* 182–191. Kesäkuu. https://doi.org/10.1109/EuroSPW.2019.00027.

Basit, Abdul, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil ja Kashif Kifayat. 2021. “A comprehensive survey of AI-enabled phishing attacks detection techniques”. *Telecommunication Systems* 76:139–154. https://doi.org/10.1007/s11235-020-00733-2.

Dhanjani, Nitesh, Billy Rios ja Brett Hardin. 2009. *Hacking: The Next Generation: The Next Generation.* 224–225. "O’Reilly Media, Inc.".

Gupta, Surbhi, Abhishek Singhal ja Akanksha Kapoor. 2016. “A literature survey on social engineering attacks: Phishing attack”. Teoksessa *2016 International Conference on Computing, Communication and Automation (ICCCA),* 537–540. https://doi.org/10.1109/CCAA.2016.7813778.

Hadi, Wa'el, Faisal Aburub ja Samer Alhawari. 2016. "A new fast associative classification algorithm for detecting phishing websites". *Applied Soft Computing* 48:729–734. https://doi.org/10.1016/j.asoc.2016.08.005.

He, Ying, Aliyu Aliyu, Mark Evans ja Cunjin Luo. 2021. "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review". *J Med Internet Res* 23, numero 4 (huhtikuu): e21747. ISSN: 1438-8871. https://doi.org/10.2196/21747.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple ja Xavier Bellekens. 2021. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic". *Computers Security* 105:102248. ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2021.102248.

Mirsky, Yisroel, Ambra Demontis, Jaidip Kotak, Ram Shankar, Deng Gelei, Liu Yang, Xiangyu Zhang ym. 2023. "The Threat of Offensive AI to Organizations". *Computers Security* 124:103006. ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2022.103006.

Al-Qahtani, Ali F, ja Stefano Cresci. 2022. "The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19". *IET Information Security* 16 (5): 324–345. https://doi.org/10.1049/ise2.12073.

Sadiq, Ashina, Muhammad Anwar, Rizwan A Butt, Farhan Masud, Muhammad K Shahzad, Shahid Naseem ja Muhammad Younas. 2021. "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0". *Human behavior and emerging technologies* 3 (5): 854–864. https://doi.org/10.1002/hbe2.301.

Stojnic, Tatyana, Dinusha Vatsalan ja Nalin AG Arachchilage. 2021. "Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails". *Security and Privacy* 4 (5): e165. https://doi.org/10.1002/spy2.165.

Syafitri, Wenni, Zarina Shukur, Umi A Mokhtar, Rossilawati Sulaiman ja Muhammad Azwan Ibrahim. 2022. "Social engineering attacks prevention: A systematic literature review". *IEEE Access,* https://doi.org/10.1109/access.2022.3162594.

Varshney, Gaurav, Manoj Misra ja Pradeep K Atrey. 2016. “A survey and classification of web phishing detection schemes”. *Security and Communication Networks* 9 (18): 6266–6284. https://doi.org/10.1002/sec.1674.

Whitty, Monica T. 2019. “Who can spot an online romance scam?” *Journal of Financial Crime* 26 (2): 623–633. https://doi.org/10.1108/JFC-06-2018-0053.

Zuraiq, AlMaha Abu, ja Mouhammd Alkasassbeh. 2019. “Phishing detection approaches”. Teoksessa *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS),* 1–6. IEEE. https://doi.org/10.1109/ictcs.2019.8923069.