Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2011

Antti Virtanen

TIETOJENKALASTELU 2011

– Menetelmät, määrä ja suojautuminen

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Joulukuu 2011 | 50 sivua

Ohjaaja: Esko Vainikka

Antti Virtanen

TIETOJENKALASTELU 2011

Tietojenkalastelu on taloudellista hyötyä tavoittelevaa henkilötietojen varastamiseen tähtäävää toimintaa.

Opinnäytteen tavoitteena on paneutua tietojenkalasteluun ilmiönä ja selvittää tämän ilmiön erilaiset sovellutukset ja metodit verkkoympäristössä. Lisäksi tarkastellaan ilmiön laajuutta eri tutkimusten valossa sekä lopulta esitellään erilaisia keinoja pienentää tämän tietoturvauhan auheuttamia seuraamuksia ja tapoja jopa kokonaan välttää ne. Opinnäytetyö toteutettiin käyttäen erilaisia internetlähteitä tutkimuksen pohjana.

Työ jakaantuu karkeasti kolmeen osaan, joista ensimmäisessä käsitellään tietojenkalastelua teoreettisesta ja metodisesta näkökulmasta. Toinen osa keskittyy käytännön esimerkkeihin, jotka valaisevat edelleen ilmiötä ja viimeinen osa esittelee tehokkaita toimenpiteitä tämän uhan torjumiseksi sekä luo katseen tulevaisuuteen viitoittaen mahdollisia kehitysnäkymiä työssä esitettyjen faktojen perusteella.

ASIASANAT:

tietoturva, varmenteet, atk-rikokset, hakkerointi, tietovuoto, internet, www-sivut, informaatiosodankäynti

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Techonology | Datacommunications

December 2011 | 50 pages

Instructor: Esko Vainikka

Antti Virtanen

Phishing 2011

Phishing; activity to pursue financial gain based on gaining access to personal data.

The purpose of this bachelor's thesis is to delve into Phishing as a phenomenon and investigate the different applications and methods in the wilds, examine the scope of this phenomenon and finally present various means to mitigate the effects of this security threat or fully evade them. This thesis was realized mainly by using various web sources.

The work is divided roughly into three different parts. First part deals the problem from theoretical and methodical point of view. The second part is focusing on real life examples which further illuminate the phenomenon and the final part showcases effective measures to fight this threat and also takes a look upon the future and the possible development trends based on the facts presented in the thesis.

KEYWORDS:

IT-security, certificates, it-crime, hacking, data seepage, internet, websites, information warfare

SISÄLTÖ

KUVAT

KUVIOT

TAULUKOT

Käsitteet ja lyhenteet

Anti-Phishing Working Group eli APWG on kansainvälinen kattojärjestö, joka tuo yhteen tietojenkalastetusta kärsiviä yrityksiä, tietoturvatuotteiden ja palveluiden tarjoajia, lakia ylläpitäviä virastoja, hallitusten virastoja, kauppajärjestöjä, alueellisia kansainvälisiä sopimusorganisaatioita ja muita tietoliikenteen ja kommunikaatioalan yrityksiä. Se perustettiin 2003 David Jevansin toimesta ja APWG:llä on nykyään yli 3200 jäsentä yli 1700 yrityksestä ja virastossa ympäri maailman. (APWG 2010b, 11.)

DNS eli Domain Name System on internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi. Internetin laitteet kommunikoivat keskenään numeeristen osoitteiden avulla, mitkä ovat ihmisille vaikeita muistaa. Nimipalvelun ansiosta voidaan siis käyttää helpommin muistettavia nimiä. Nimipalvelun toinen tärkeä tehtävä on sähköpostien reititys. Nimipalvelun palvelintyyppejä on kaksi, eli nimipalvelukyselyihin vastauksia hakevat koneet eli resolverit (ratkaisijat) ja vastauksia antavat koneet eli autoritääriset nimipalvelimet. (Domain Name System 2011.)

Domain tarkoittaa verkkotunnusta. Ylätason verkkotunnukset (TLD) ovat lyhyitä tunnuksia, jotka jakavat verkkotunnukset eri luokkiin. Erimerkiksi fi-verkkotunnuksen alapuolella ovat suomalaiset verkkotunnukset, jotka sitten päättyvät kirjaimiin .fi. Nämä jakaantuvat alaverkkotunnuksiin. Esimerkiksi mail.example.com ja calendar.example.com ovat example.comin aladomaineja (subdomain).

Aladomain tarkoittaa suhteellista osallisuutta, ei absoluuttista. Esimerkiksi wikipedia.org muodostuu .org-domainin alaverkkotunnuksesta ja en.wikipedia.org muodostuu domainin wikipedia.org aladomainista. Teoriassa alaverkkotunnukset voivat mennä aina 127-tasoiseksi asti ja jokainen taso voi sisältää 63 merkkiä, kunhan koko verkkotunnuksen pituus ei ole yli 255 merkkiä. (Domain Name System 2011.)

EV-sertifikaatti (Extended Validation) on x.509 yleisen avaimen sertifikaatti, joka on annettu tietyille identiteetin tunnistuskriteereille. Nämä kriteerit vaativat laajempaa varmentamista CA:lle pyytäjätaholtaan ennen myöntämistä. Sertifikaatit, jotka myönnetään CA:lta EV:n ohjenuoran mukaan, eivät eroa rakenteellisesti muista halvemmista sertifikaateista, eivätkä tarjoa vahvempaa salausta. Ne on ennen kaikkea suunniteltu tiettyjen CA:iden menettelytapojen tunnistajaa varten, jotta EV-yhteensopiva sovellus toimii asianmukaisella tavalla. (Extended validation certificate 2011.)

Fast-flux hosting tarkoittaa verkkorikollisten käyttämää verkkotunnuksen ylläpitomenetelmää, jossa usean tuhannen bottikoneen IP-osoitteet ovat linkitettyjä täysin pätevään verkkotunnukseen. Näitä IP-osoitteita vaihdellaan sisään ja ulos virrasta äärimmäisen nopeassa tahdissa käyttäen yhdistelmänä IP-osoitteiden rinkiä ja erittäin lyhyttä elinaikaa (Time-To-Live, TTL) mille tahansa tietylle DNS:n resurssirekisterille. Nettisivun verkkotunnus voidaan liittää uuteen settiin IP-osoitteita aina niinkin usein kuin joka kolmas minuutti. Selain, joka yhdistäisi tällaiselle nettisivulle joka kolmas minuutti, yhdistäisi itse asiassa joka kerta eri saastuneelle koneelle. (The Honeynet Project 2011a.)

ICANN eli Internet Corporation for Assigned Names and Numbers on voittoa tavoittelematon organisaatio, jonka tehtävänä on valvoa lukuisia internetin ylläpitoon liittyviä tehtäviä.

IP-osoite (Internet Protocol) on TCP/IP-mallin Internetkerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä internetverkossa. Se muodostaa koko Internetin ytimen ja on ainoa asia, mikä yhdistää kaikkia internettiin liitettyjä koneita. IP-paketit toimitetaan perille IP-osoitteiden perusteella kuten esim. osoitteeseen 192.68.11.1 (ipv4) tai 2002:a00::260:1dff:fe22:5a85/64 (ipv6). Verkkotunnuksien muuttamisesta IP-osoitteiksi vastaa DNS-järjestelmä. IP-pakettien perille toimittamista sanotaan reitittämiseksi ja sen tekevät reitittimet perustuen reititysprotokollien välittämään tietoon IP-osoitteiden sijaintipaikoista internetissä ja lyhimmistä reiteistä näiden välillä. (Internet Protocol 2011.)

IRC eli Internet Relay Chat.

P2P, Peer-to-Peer eli vertaisverkko.

SMTP eli Simple Mail Transfer Protocol, jota käytetään viestien välittämiseen sähköpostipalvelimien välillä.

TSL – Transport Layer Security eli kuljettavan kerroksen turvallisuus. (Transport Layer Security 2011.)

URI (Uniform Resource Identifier) on merkkijono, jolla kerrotaan tietyn tiedon paikka (**URL**) tai yksikäsitteinen nimi (**URN**). Erityisesti URI:n erikoistapausta **URL:ää** (Uniform Resource Locator) käytetään osoittamaan www-sivuja. (URL 2011.)

Virtual hosting tarkoittaa virtuaalisten verkkotunnusten hallintaa yhdestä IP:stä käsin. (Virtual hosting 2011.)

X.509 on ITU-T standardi yleisen avaimen infrastruktuurille (PKI) ja etuoikeuksien hallintainfrastruktuurille (PMI). X.509 määrittää muun muassa standardimuodon PKI:lle, sertifikaattien peruutuslistat, ominaisuussertifikaatit sekä sertifikaatin polun varmentamisalgoritmin. (X.509 2011.)

1 Johdanto

Opinnäytetyön aiheena on tietojenkalastelun kuvaaminen ja tutkiminen ilmiönä nykyaikaisessa verkkoyhteiskunnassa. Sysäyksenä työn tekemiselle ja tämänkaltaisen tietopaketin kasaamiselle oli tekijän oma kiinnostus tietoturvauhkiin sekä havainto tietojenkalastelun määrän dramaattisesta kasvusta viime vuosina.

Tietojenkalastelu eli englanniksi phishing tarkoittaa rikollisten suorittamia toimia, joissa sosiaalinen manipulointi yhdistetään teknologian mahdollistamaan automatisointiin ja nimettömyyteen. Yleisimpänä motiivina on varastaa kuluttajan sähköinen identiteetti ja rahaliikenteessä käytettävät tunnukset. (APWG 2011a, 2.)

Perinteisenä keinona käytetään yleensä suurelle määrälle käyttäjiä lähetettäviä sähköposteja, joissa esiinnytään virallisten yritysten tai muiden organisaatioiden työntekijöinä tarkoituksena johdattaa kuluttaja aitoja sivuja jäljitteleville kopiosivuistoille. Näillä sivuilla uhri huijataan luovuttamaan kriittisiä taloutta koskevia tietoja. (APWG 2011a, 2.)

Toisena tapana harjoittaa tietojenkalastelua on rikosohjelmistojen käyttö, jolloin uhrin tietokoneelle istutetaan tämän henkilökohtaisia tietoja keräävä ohjelma. Tämä tapahtuu joko sähköpostin, nettisivujen tai muun internet-liikenteen välityksellä. Näitä rikosohjelmistoja käytetään myös keinona korruptoida paikallisia ohjauksellisia infrastruktuureja (välityspalvelimia) harhaanjohtamaan kuluttajia petollisille nettisivuille, tai vaihtoehtoisesti autenttisille nettisivuille välityspalvelimen kautta, minkä avulla nauhoitetaan kuluttajan näppäimistön painallukset. (APWG 2011a, 2.)

Nykyinen siirtymä perinteisestä tietojenkalastelusta rikosohjelmistojen jakeluun näyttäisi tapahtuneen tämäntyyppisten sovellusten paremman kannattavuuden vuoksi. Rikosohjelmia on mahdollista levittää useampia reittejä pitkin ja monesti ne ovat tehokkaampia kuin perinteiset menetelmät.

Työn olen rajannut karkeasti kolmeen osaan, joista ensimmäisessä käsittelen hieman tietojenkalastelun historiaa ja menetelmiä teoreettisessa valossa tilastoja apuna käyttäen. Toisessa osassa paneudun muutaman tärkeän esimerkin avulla konkreettisemmin siihen ilmiöön, jonka käsitän tietojenkalasteluksi ja tutustun sitä kautta paremmin koko toiminnan logiikkaan. Kolmannessa osassa käsittelen erilaisia vastatoimia näiden uhkien torjumiseksi. Lopuksi myös rohkenen esittää arvailuja tietojenkalastelun tulevaisuudesta.

Tutkimusmenetelmänä olen opinnäytteessä käyttänyt tutustumista eri tietoturvayhteisöjen julkaisemaan materiaaliin, jota olenkin löytänyt suuret määrät. Aiheen laajuuden vuoksi työ on rajattu raporttimaiseksi kokonaisuudeksi, jossa on jätetty tekniset yksityiskohdat vähemmälle. Toisaalta tämä palvelee näin kansantajuisempana laajempaa yleisöä, jonka kokisin hyötyvän aihepiiriin tutustumisesta. Samalla, kun esimerkiksi työelämä kietoutuu yhä suuremmassa määrin tietotekniikan ympärille, myös erilaiset uhkakuvat tähän liittyen kasvavat. Näiden uhkakuvien vähentämiseksi katsonkin ihmisten tietoisuuden lisäämisen aiheesta ensiarvoisen tärkeäksi.

2 Tietojenkalastelun historia lyhyesti

Tietojenkalastelu internetissä on vielä suhteellisen tuore ilmiö, mutta sitäkin merkittävämpi nykypäivää kohti tultaessa. Pohja tietojenkalastelun tarkasteluun internetissä saadaan lähtemällä liikkelle englanninkielisen termin ”phishing” määritelmästä. Siinä on yhdistetty kaksi sanaa, ”fishing” ja ”phreaking”. ”Phreaking” -sanasta paljastuvat termin juuret – sillä tarkoitetaan laitonta puhelinsysteemien seurantaa ja tutkimista (engl. phone breaking). (APWG 2011b.)

2.1 Vanhat Phishing-huijaukset

Ensimmäiset tutkimukset tietojenkalastelun metodeista löytyvät vuoden 1987 Interex -konferenssista. Siellä Jerry Felix ja Chris Hauck esittelivät dokumenttinsa, missä he erottelivat erilaisia tapoja, joilla kolmas osapuoli pystyisi naamioutumaan luotettavaksi henkilöksi tietoverkoissa. Termiä ”phishing” alettin puolestaan käyttää vasta 90-luvun puolessa välissä, jolloin se liitettiin eräisiin American Onlinen (AOL, operaattori) tilien väärinkäytöksiin.

Esimerkiksi ennen vuotta 1995 oli mahdollista avata AOL-tili käyttäen väärennettyjä algoritmien kanssa generoituja luottokorttinumeroita. Kuitenkin AOL korjasi tämän ongelman ajaen näin vuonna 1996 hyvinkin aktiivisen warez-yhteisön aloittamaan tietojenkalastelun saadakseen laillisia AOL-tilejä haltuunsa. Usein tämä tapahtui niin, että ensin lähetettiin pikaviesti käyttäjän AIM (AOL Instant Messenger) -tiliin. Viestissä väitettiin American Onlinen tarvitsevan heidän salasanaansa esimerkiksi tilin uudelleen verifiointiin. Tätä varten kehitettiin muun muassa sellainen työkalu kuin AOHell, jolla saatiin automatisoitua prosessia.

AOL kuitenkin kehitti nopeasti vastatoimia ja vuonna 1997 suurin osa kalastelijoista joutuikin luopumaan toimistaan käytännön toteutuksen hankaloituessa liikaa. Ajalta periytyy myös käytäntö, jossa palveluntarjoajan lähettämien viestien loppuun on lisätty ilmoitus, että he eivät koskaan kysy

käyttäjätunnustasi tai salasanaasi. Huolimatta tästäkin varokeinosta, perinteisiä kalasteluviestejä American Onlinen tapaan näkyy edelleen. (Phishing 2011; The Honeynet Project 2008b.)

2.2 Tietojenkalastelun kehittyminen

Pian huomattiin, että phishing-huijauksia voitaisiin toteuttaa myös monissa muissa systeemeissä. Varsinkin rahoituslaitokset näyttivät otollisilta kohteilta. Syyskuun 11. päivä 2001 oli tärkeä päivä myös tietojenkalastelun historiassa. Jälkiseurauksena terroristi-iskulle opportunistiset rikolliset lähettivät useille henkilöille niin sanotun ”post 9-11 ID check” (9.11. henkilöllisyyden jälkitarkastus) -sähköpostin varastaakseen rahaliikennetietoja E-Goldin digitaalisesta valuuttapalvelusta. Tämä oli jo astetta kehittyneempi hyökkäys saman vuoden kesäkuussa tapahtuneen aikaisemman E-Goldin vastaisen hyökkäyksen jälkeen. Molemmat nähtiin alun perin epäonnistumisina, mutta nykynäkökulmasta katsottuna nämä olivat tärkeitä pioneeritestejä, jotka edesauttoivat rikollisten tahojen kiinnostuksen lisääntymistä tietojenkalastelua kohtaan.

Vuoteen 2004 mennessä tietojenkalastelu alkoi olla jo vakiintunutta. Toukokuun 2004 ja 2005 välillä arvioitiin, että jo noin 929 miljoonaa dollaria hävisi tietojenkalastelun seurauksena rikolliselle. Sen jälkeen erilaiset tekniikat ovat vain kehittyneet ja yleistyneet tietojenkalastelun lisääntyessä vuosi vuodelta. (Phishing 2011.)

3 Tietojenkalastelun nykytilanne ja menetelmät

Nykypäivänä tietojenkalastelu on monitahoinen ongelma ja siinä yhdistellään erilaisia keinoja päämäärän saavuttamiseksi. Tietojenkalastelun toimintalogiikka voidaan jakaa neljään osa-alueeseen.

Ensimmäinen osa-alue on bottiverkko ja sen vuokraaminen. Tämä on jo olennainen osa nykyaikaista ammattimaista tietojenkalastelua. Bottiverkko toimiikin eräänlaisena infrastruktuurina phishinghyökkäyksille. Bottiverkon avulla voidaan lähettää uhreille roskapostia, ylläpitää haitallisia verkkotunnuksia sekä levittää rikosohjelmistoa (Rasmussen & Aaron 2010a, 6).

Toinen osa-alue on sähköposti. Sähköpostin avulla pyritään houkuttelemaan käyttäjä kalastelusivulle. Se voi olla geneerisempi suurelle määrälle lähetettävä viesti tai tietylle käyttäjälle henkilökohtaisesti räätälöity viesti. Sähköposti voi myös sisältää rikosohjelmistoa. (The Honeynet Project 2011b; Phishing 2011.)

Kolmas osa-alue on uskottavien phishing-sivujen luonti. Sivut esiintyvät monessa muodossa riippuen huijauksen kohteena olevasta brändistä. Yleensä sivuissa on mallinnettu kohteena olevan brändin kirjautumissivu ja joskus tälle sivulle on lisätty vielä ylimääräisiä tekstikenttiä liittyen muihin tietoihin, joita rikollinen katsoo tarvitsevansa. Monesti nämä sivut lataavat käyttäjän huomaamatta rikosohjelmiston sivulle kirjoitettujen skriptien avulla. (APWG 2010c, 2.)

Neljäs osa-alue on rikosohjelmistot. Rikosohjelmistot ovat ottamassa yhä tärkeämmän roolin tietojenkalastelussa niiden korkeamman kannattavuuden vuoksi. Niitä voi kohdata lukuisia reittejä pitkin. Tartunnan voi saada sähköpostin, haitallisen sivuston, ladatun saastuneen tiedoston, erinäisten webpalvelujen ja muiden yhteyksien kautta. (The Honeynet Project 2011b.)

3.1 Bottiverkot

Bottiverkot ovat yleensä muutamista sadoista kymmeniin tuhansiin ja jopa useisiin miljooniin tietokoneisiin asti koostuvia verkostoja, jotka hakkerit ovat ottaneet haltuunsa ja hallinoivat erilaisilla C&C (Command & Control) -systeemeillä. Vielä 2000-luvun puolessa välissä useimmat bottiverkot pohjautuivat IRC-kanavien kautta hallinoitaviin järjestelmiin, mutta nykyään ollaan menty yhä useammin P2P-protokollien käyttöön. (The Honeynet Project 2011a.)

Bottiverkoilla on neljä tärkeää sovellutuskäytäntöä tietojenkalasteluun liittyen: kalasteluviestien lähettäminen, kalastelusivujen ylläpito, rikosohjelmistojen asentaminen ja levittäminen sekä niiden keräämien tietojen hallinnointi.

3.2 Phishingviestit

Kalasteluviestit tulevat monessa eri muodossa ja niissä käytetään lukuisia tekniikoita, jotta uhri saadaan huijattua siirtymään viestissä mainostetulle sivulle tai avaamaan viestiin liitetyn tiedoston. Paras tapa luokitella viestit on kuitenkin tehdä jako selkeästi geneerisempiin, tietylle (suurehkolle) kohderyhmälle lähetettyihin viesteihin, ja ns. keihäskalasteluun, jossa lähetetään viesti tarkasti kohdennetulle kohderyhmälle, jopa yksittäiselle käyttäjälle esim. jonkin organisaation tietylle työntekijälle. Jälkimmäisessä tapauksessa hyökkäystä on voitu valmistella jopa kuukausia, jonka aikana on käytetty paljon aikaa mm. kyseisen käyttäjän profilointiin. (The Honeynet Project 2011b; Phishing 2011.)

Phishing-viestit itsessään ovat kehittyneet paljon alkuajoista. Nykyaikaiset viestit voivat näyttää täysin aidoilta sisältäen huijaamisen kohteena olevan yrityksen logot, värit, grafiikat, fonttityylit ja muut elementit - kuten yrityksen yksilökohtaiset tiedot käyttäjästä. Nämä tiedot on puolestaan voitu saada aikaisemmin esim. tietomurron yhteydessä. Yleensä viestin tarkoitus on hämmentää, järkyttää tai aktivoida vastaanottajaa. Tämä tarkoittaa sitä, että viestien aiheina on yleensä kuvitellut tiliongelmat jossain verkkopalvelussa, tarve tilin uudelleen verifiointiin, tärkeiden tietoturvapäivitysten asennukset,

uudet tuotteet tai palvelutarjoukset. Monesti viestien kohteita kehoitetaan reagoimaan mahdollisimman nopeasti, jolloin uhri saadaan tekemään nopea päätös harkitsematta ja napsauttamaan viestiin sisältyvää linkkiä. (TrendMicro 2006, 4.)

3.2.1 Linkit kalasteluviestissä

Linkkien manipuloinnissa on tavoitteena saada phishingviestin sisältämät linkit näyttämään asianmukaisilta ja uskottavilta sekä saada uhrit napsauttamaan niitä. Väärin kirjoitetut URL:t (www.nrdea.fi) tai alidomainien käyttö luovasti ovat tietojenkalastelijoiden yleisesti käyttämiä keinoja. (Phishing 2011.)

Esimerkiksi http://www.sinunpankkisi.esimerkki.fi osoite näyttää pikaisesti katsottuna siltä, että URL johtaa esimerkkiosioon sinunpankkisi -sivulla. Tosiasiassa linkki osoittaa ”sinunpankkisi” -osaan esimerkkisivustoa. (Phishing 2011.)

Toinen yleinen keino on tehdä linkistä näytettävä teksti johtamaan eri sivustolle, kuin minne se tosiasiassa vie. Tämä suoritetaan HTML-kielen avulla. Tällä tapaa saadaan vaikka linkki http://fi.esimerkki.org/pankki/aito viittaamaan sivuun http://fi.esimerkki.org/pankki/vale. Sen, mille sivulle linkki todellisuudessa johtaa, näkee helposti selaimen alalaidasta hiiren kursorin ollessa linkin päällä, mutta kaikki käyttäjät eivät linkkiä napsauttaessa aina huomaa tai muista tätä tarkistusta tehdä. (Phishing 2011; The Honeynet Project 2011b.)

Kolmas keino on sisällyttää suurin osa hyperlinkeistä johtamaan brändin oikealle nettisivulle, ja vain pieni osa kalastelusivulle. Tällöin käyttäjän selain muodostaa suurimman osan HTTP-yhteyksistä aidolle webserverille ja ainoastaan pienen määrän yhteyksiä valeserverille. Tämä onnistuu, mikäli käyttäjän sähköpostisovellus tukee sisällön automaattista yhdistämistä. Ohjelma saattaa muodostaa siis automaattisesti yhteyden valeserverille sillä aikaa, kun uhri lukee viestiä. (The Honeynet Project 2011b.)

IDN (Internationalized Domain Name) -huijaus on yksi työkalu kalastelijoiden pakissa linkkien manipuloimiseen. Tässä on tarkoituksena kirjoittaa hyperlinkki

käyttäen kansallisia merkkejä, jotka muistuttavat ulkoisesti hyvin paljon korvattavia merkkejä. Esim. kreikkalainen O tai kyrillinen o näyttävät ulkoisesti hyvin samoilta. Näitä hyökkäyksiä ei tosin juurikaan ole viime vuosina enää esiintynyt. (APWG 2010a, 18-19.)

3.2.2 Sähköpostifiltterien välttäminen

Tietojenkalastelijat saattavat käyttää kuvia tekstistä ennemmin kuin itse tekstiä välttääkseen tekstisisällön analysoimiseen pohjautuvia sähköpostifilttereitä (Phishing 2011). Mustat listat voidaan puolestaan kiertää käyttämällä uniikkeja numeroita hyperlinkeissä viestin sisällä, jotka kuitenkin kaikki ohjataan samalle phishing-sivustolle. Mustat listat tarvitsevat koko nettiosoitteen, joten niiden teho on rajallinen tällaisissa tapauksissa. (Stevens & Jackson 2010.)

3.3 Kalastelusivut

Kalastelusivut ovat ulkoisesti hyvin lähellä kohteenaan olevan brändin sivuja. Ne sisältävät kaikki samat aidon oloisen sivun tunnusmerkit samoin kuin sivulle johtava kalasteluviestikin (TrendMicro 2006, 4). Tämä johtuu muun muassa nykyisten nettisivuohjelmistojen tehokkuudesta, sillä näiden avulla on hyvin helppoa kopioida melkein mikä tahansa sivu (The Honeynet Project 2011b). Yleensä linkki johtaa tietojenkalastelusivulla kohtaan, jossa pyydetään uhria luovuttamaan pankkitilin kirjautumistiedot, luottokortin numero, henkilötunnus tai muuta arkaluonteista tietoa.

Yksi variaatio tästä on sivujen konfigurointi siten, että ohjataan ensin uhri aidon näköiselle kirjautumissivulle, jossa sitten tallennetaan käyttäjän syöttämät tiedot. Tämän jälkeen käyttäjä ohjataan oikealle sivulle. Tämä voi aihettaa ”salasana väärin, ole hyvä ja syötä se uudestaan” -virheen, jolloin uhri saattaa yksinkertaisesti olettaa, että on vain näppäillyt salasanansa väärin. (The Honeynet Project 2011b.)

Valenettisivu voidaan myös asettaa toimimaan välityspalvelimena oikealle nettisivulle, jolloin se tallentaa vaivihkaa käyttäjätunnuksen ja salasanan, jotka eivät ole salattuja esim. SSL:llä. (The Honeynet Project 2011b)

Yksi vakavimmista tavoista luoda aidonoloinen kalastelusivusto on aitojen sertifikaattien käyttö sivustolla. Tällöin rikolliset tahot ovat saaneet tietomurron yhteydessä työkalut juurivarmenteiden generoimiseen, jolloin selain ei tuota mitään virheilmoitusta käytetyistä varmenteista. Tämä johtuu siitä, että selaimeen on valmiiksi ohjelmoitu lista luotetuista juurivarmentajista. Tämän ongelman korjaaminen vaatiikin jo nopeaa reagoimista selainten kehittäjiltä ja ennen kaikkea avoimuutta juurivarmentajien puolesta. Tämä ongelma on tullut erityisesti esiin vuoden 2011 aikana hollantilaiseen DigiNotariin kohdistetun tietomurron seurauksena. (CERT-FI 2011.)

3.4 Rikosohjelmistot

Eri rikosohjelmistoja voidaan käyttää monin eri tavoin tietojenkalasteluun. Yksi käytetyimmistä on tällä hetkellä Zeus/Zbot, jolla voi mm. tehdä HTML-injektioita, varastaa selaimen lomaketietoja, välittää uhrin näppäimistön painallukset bottiverkon omistajalle ja ohjata etänä uhrin tietokonetta (Stevens & Jackson 2010). Zeukseen palaan tarkemmin esimerkit-kohdassa.

Uhrin kerran käytyä phishing-sivulla petos ei välttämättä ole ohi. Jotkut rikosohjelmistot käyttävät JavaScript-komentoja muuttaakseen nettisivupalkin. Tämä tehdään joko laittamalla kuva laillisesta URL:stä osoitepalkin päälle tai sulkemalla alkuperäinen osoitepalkki ja avaamalla sen tilalle uusi. (Phishing 2011.)

Hyökkääjä voi jopa käyttää tietoturva-aukkoja luotetun nettisivun omissa skripteissä uhria vastaan. Tämäntyyppiset hyökkäykset, jotka tunnetaan myös nimellä cross-site scripting, ovat erityisen ongelmallisia, koska ne ohjaavat käyttäjän kirjautumaan esim. oman pankkinsa viralliseen palveluun, jossa ovat kaikki asiat nettiosoitteesta tietoturvasertifikaatteihin kunnossa. Todellisuudessa linkki nettisivulle on rakennettu kulkemaan kalastelijan kontrolloiman

välityspalvelimen kautta, jolloin hyökkäyksen havaitseminen on todella vaikeaa ilman erityistä tietoa. Juuri tällaista aukkoa oli käytetty esimerkiksi vuonna 2006 PayPalia vastaan. (Phishing 2011.)

3.5 Muita tietojenkalastelun tekniikoita

Eräs onnistunut tapa kalastella tietoja on edelleenohjata asiakas ensin pankin virallisille nettisivuille ja sitten sijoittaa popup-ikkuna pyytämään nimikirjaimia nettisivun yläreunaan niin, että se näyttää siltä, kuin pankki itse pyytäisi tätä henkilökohtaista tietoa. (Phishing 2011.)

Tabnabbing puolestaan käyttää hyväkseen käyttäjien huomaamattomuutta tabien (välilehtien) suhteen. Tässä menetelmässä luodaan skripti, joka lataa jonkin avatun sivun tilalle väärennöksen jostain hyvin tunnetusta palvelusta. Käyttäjä, joka palaa välilehdelle hetken kuluttua ja näkee korvatun sivun alkuperäisen tilalla, voikin luulla sivua oikeaksi. Tällöin hän saattaa lisätä tälle sivulle käyttäjätunnuksensa ja salasanansa mitenkään asiaa sen kummemin pohtimatta. Hyökkäyksen voi tehdä vieläkin onnistuneemmaksi, mikäli skripti tarkistaa käyttäjän verkkohistoriasta hänen usein selaamansa sivut ja lataa simulaation tällaisesta sivusta. Tämän hyökkäyksen voi tehdä vaikka JavaScript olisi pois päältä käyttäen ”meta refresh” -elementtiä, joka on HTML:n ominaisuus sivujen uudelleenohjausta varten. Siinä käynnistetään sivun uudelleenlataus tietyn ajan kuluttua. Firefoxin NoScript-laajennus estää tämän hyökkäyksen toteutumisen. (Phishing 2011.)

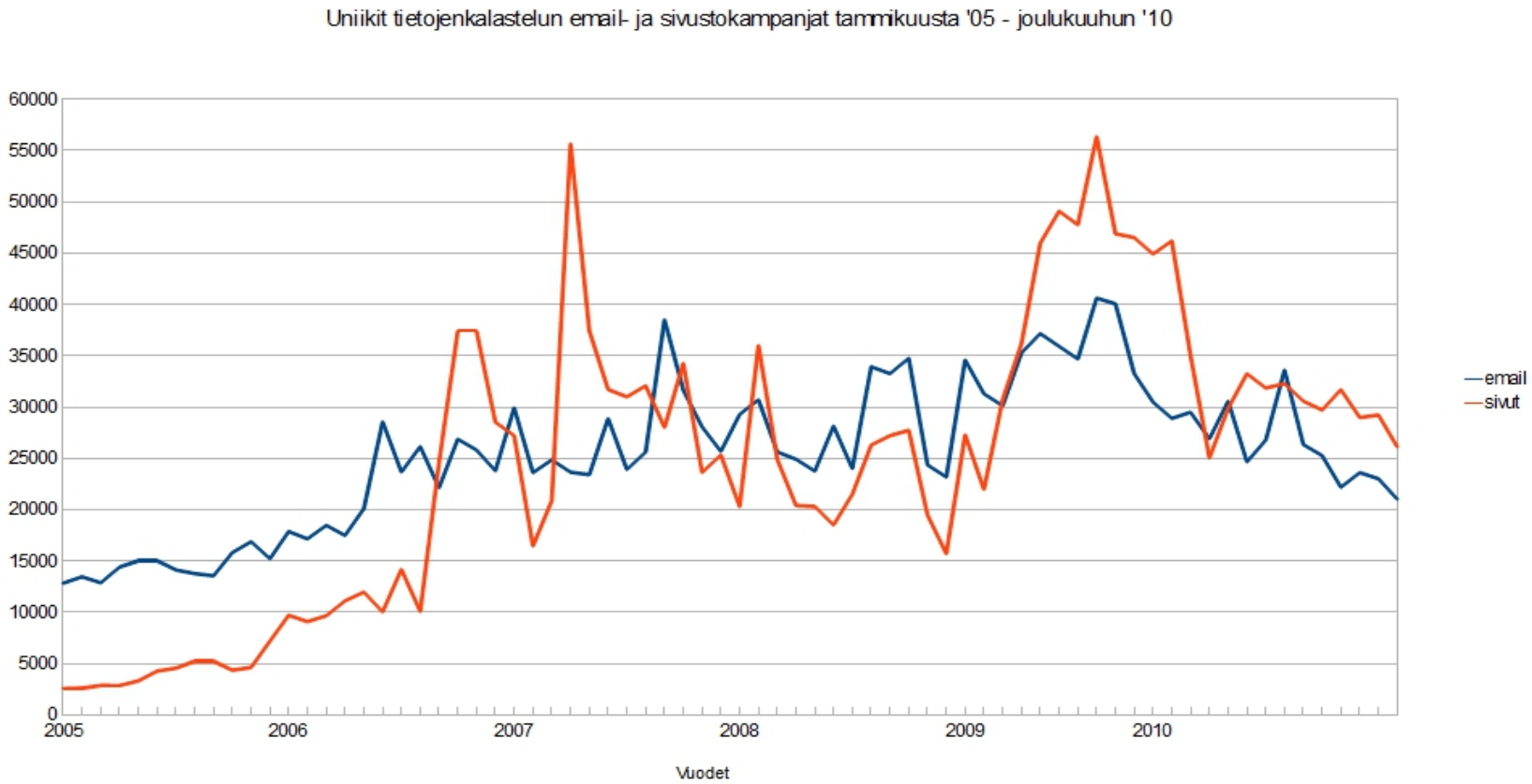
4 Tietojenkalastelun kehittyminen 2005 – 2011

Tässä osassa käsittelen tietojenkalastelun kehittymistä valikoitujen tilastojen valossa. Tilastot kokosin APWG:n osavuosikatsauksista tammikuusta 2005 lähtien. Johtuen APWG:n tilastointimenetelmien kehittymisestä Phishing Trends -raporteissa vuosien varrella, ei ollut mahdollista muodostaa yhtenäistä kuvaajaa kaikista tarkasteluun otetuista osa-alueista. Lisäksi on otettava huomioon, että osa tietojenkalasteluun liittyvistä ilmiöistä on tuoreempaa perua, joten osa seuraavissa kuvioissa esiintyvistä mitatuista ominaisuuksista oli vasta nupuillaan ja kehittymässä taustalla vuoden 2005 aikana.

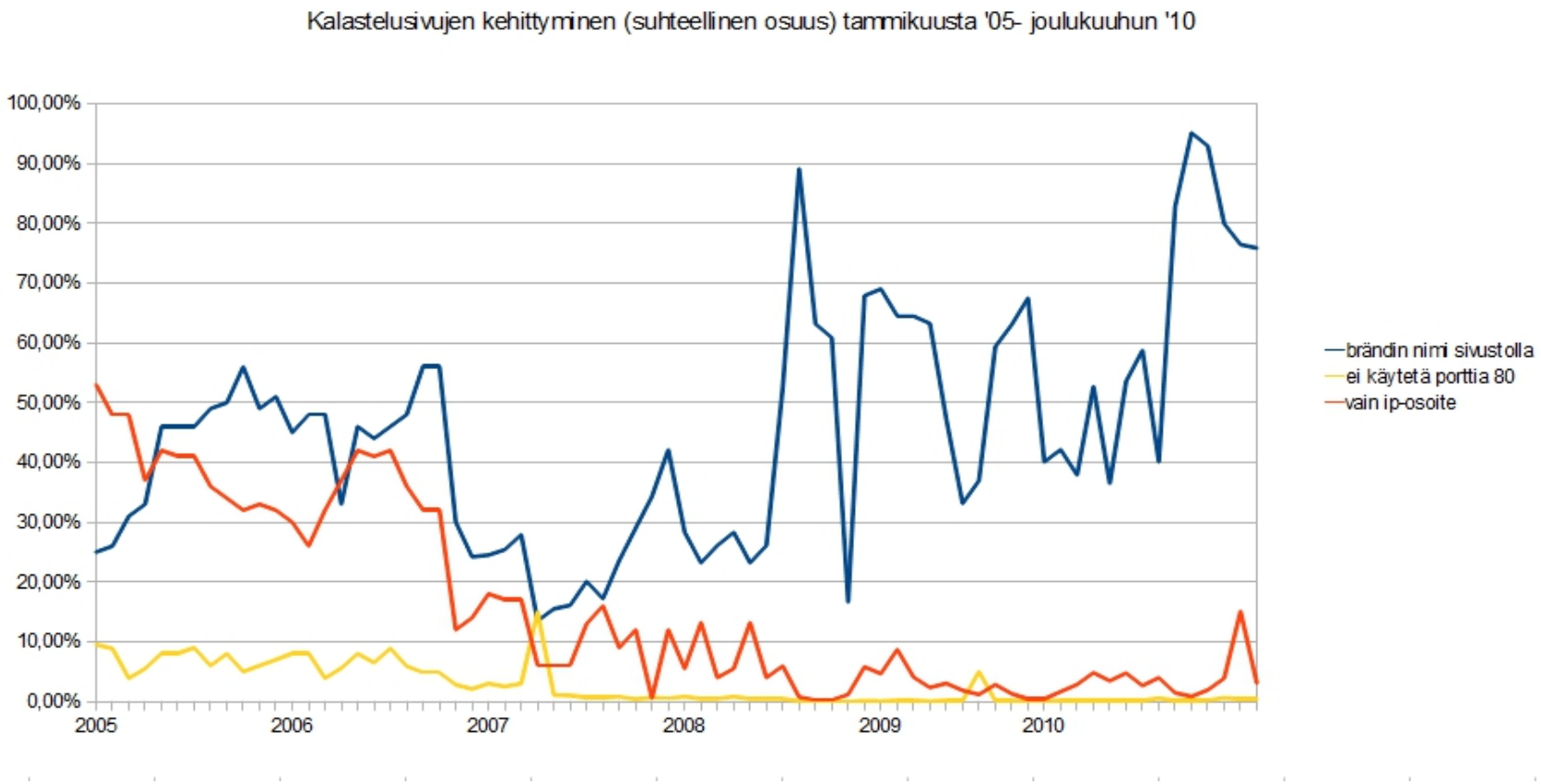
4.1 Uniikit email-kampanjat ja tietojenkalastelusivut

Kuviossa 1 mitataan uniikkien email-kampanjoiden ja phishing-sivustojen määrän kehittymistä vuoden 2005 alkupuolelta lähtien. Vaikka esimerkiksi kalasteluviestejä voidaan lähettää kappalemäärinä useita miljoonia, niin kuitenkin niiden alkuperä johtaa paljon pienempään määrään sähköpostikampanjoita. Samoin on kalastelusivujen laita. Vaikka monessa viestissä on niihin sisältyviin linkkeihin lisätty uniikkeja numeroita sähköpostifilttereiden välttämiseksi, johtavat ne kuitenkin samoille sivuille.

Kuviosta 1 havaitaan, että vuoden 2006-2007 taitekohta on ollut eräänlainen virstanpylväs tietojenkalastelun historiassa. Tässä kohdassa saavutetaan ensimmäinen huippu vuosien aikana hitaasti kasvaneessa ilmiössä. Tällöin niin sanottu Rock Phish Gang oli vastuussa suuresta osasta tietojenkalastelua. Kuvaajassa havaitaan myös, miten tämän organisaation jälkimmäinen inkarnaatio Avalanche vaikutti tietojenkalastelun määrään vuoden 2009 lopulla. Vuoden 2010 loppupuolella tilanne on laskenut vuoden 2006 loppupuolen tasolle, mutta lienee vain ajan kysymys milloin Avalanchen toteuttaman massiivisen hyökkäyksen kaltainen uusi kampanja toteutetaan.



Kuvio 1. Uniikit phishing-hyökkäykset ja email-kampanjat. (APWG 2005a-k; 2006a-k; 2007a-l; 2008a-c; 2009a-c; 2010a-b;



Kuvio 2. Phishing-sivujen kehittyminen. (APWG 2005a-k; 2006a-k; 2007a-l; 2008a-c; 2009a-c; 2010a-b; 2011a.)

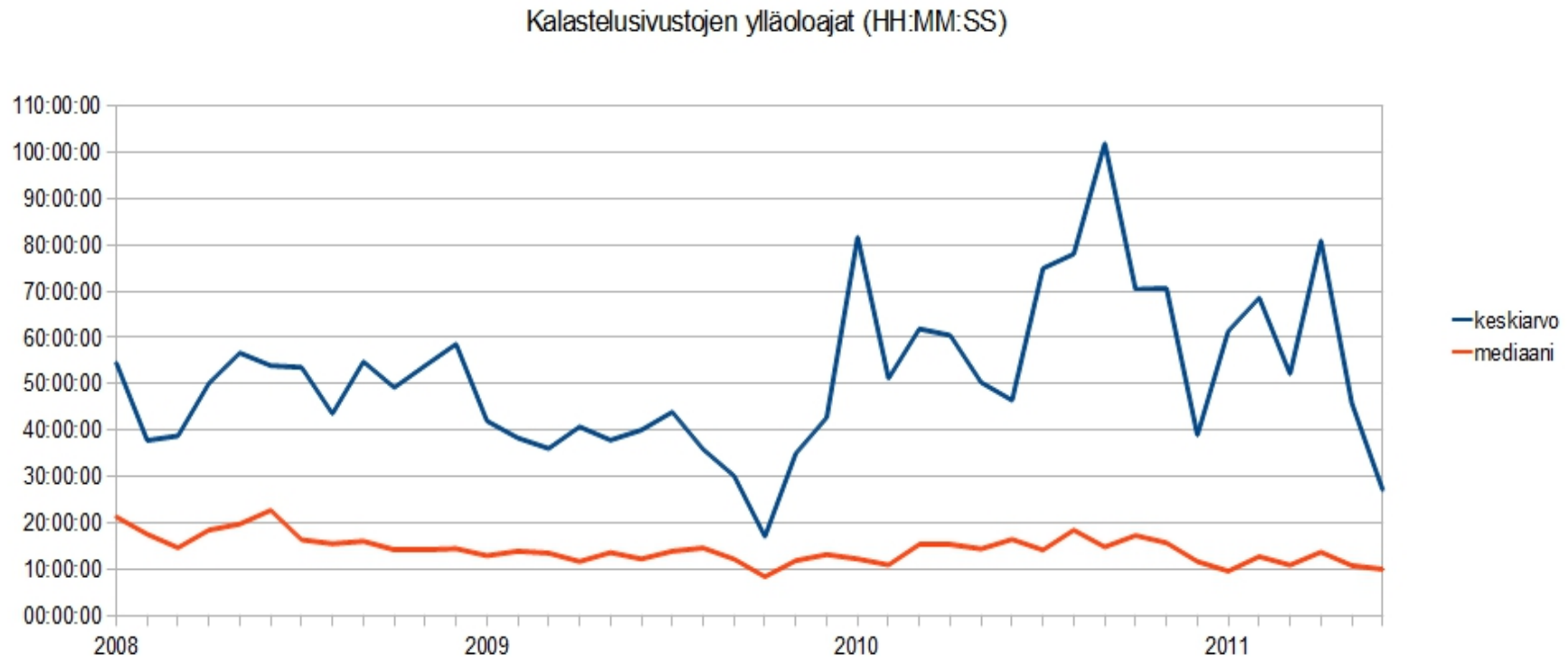
4.2 Phishing-sivujen kehittyminen vuodesta 2005 lähtien

Kuviossa 2 tarkastellaan kolmea phishing-sivujen ominaisuutta ja niiden kehittymistä vuosien varrella. Kun vielä vuoden 2005 aikana oli suhteellisen yleistä käyttää kalastelusivuissa jotain muuta porttia kuin 80 ja verkkotunnuksen sijasta pelkkää ip-osoitetta, havaitaan brändin nimen sisältyvän melkein kaikkiin nykyisiin kalastelusivustoihin. Voidaan tehdä johtopäätös, että tehokkaimpana keinona kalastelusivun onnistumiselle on sisällyttää brändin nimi osana verkkotunnusta. Muun kuin portin 80 käyttö on kutistunut lopullisesti kuriositeetiksi ilmeisesti sen merkityksettömyyden kannalta kalastelusivun tuottavuuden näkökulmasta. Kyseessä voi olla myös rikollisten rikosohjelmien käytön leviäminen, mikä on voinut johtaa tiettyjen tehokkaiden käytäntöjen yleistymisen vallitseviksi kalasteluyhteisöissä.

4.3 Phishing-sivujen ylläoloaikojen kehittyminen 2008-2011

Kuviossa 3 tarkastellaan phishing-sivujen ylläoloaikoja. Tämä on tärkeä mittari kalastelusivujen vahingollisuuden määrittelemiseksi. Mitä enemmän phishing-sivustoja on, ja mitä kauemmin nämä sivustot ovat pystyssä, määrittää hyvin pitkälti sen, kuinka paljon tietojenkalastelija hyötyy kampanjastaan. Vaikka absoluuttinen keskiarvo onkin vaihdellut suuresti, niin mediaani eli painotettu keskiarvo on pysynyt suhteellisen tasaisena ja jopa laskenut vuoden 2008 tasosta. Mediaanilla tarkoitetaan tässä kohtaa sitä, kuinka nopeasti sivu on ajettu alas sen pystyttämisestä sekä kuinka suuren suhteellisen osan nämä sivut muodostavat. Tämä arviointitapa karsii yksittäiset vääristävät ääritapaukset pois, jolloin jotkut sivut ovat olleet jopa kuukauden pystyssä.

Tilastossa havaitaan myös vuoden 2009 lopulla tietoturvayhteisön panos Avalanchen hyökkäyksien torjumisessa. Tällöin saatiin Avalanchen bottiverkko hetkeksi kaadettua. Sen jälkeen on jälleen tosin tapahtunut ylläoloaikojen kohoamista. (Rasmussen & Aaron 2010a.)



Kuvio 3: Phishing-sivujen ylläoloajat 2008-2011.(Rasmussen & Aaron 2008a; 2008b; 2009a; 2009b; 2010a; 2010b; 2011a;

4.4 Tietojenkalastelun kohdistuminen talouden eri sektoreihin

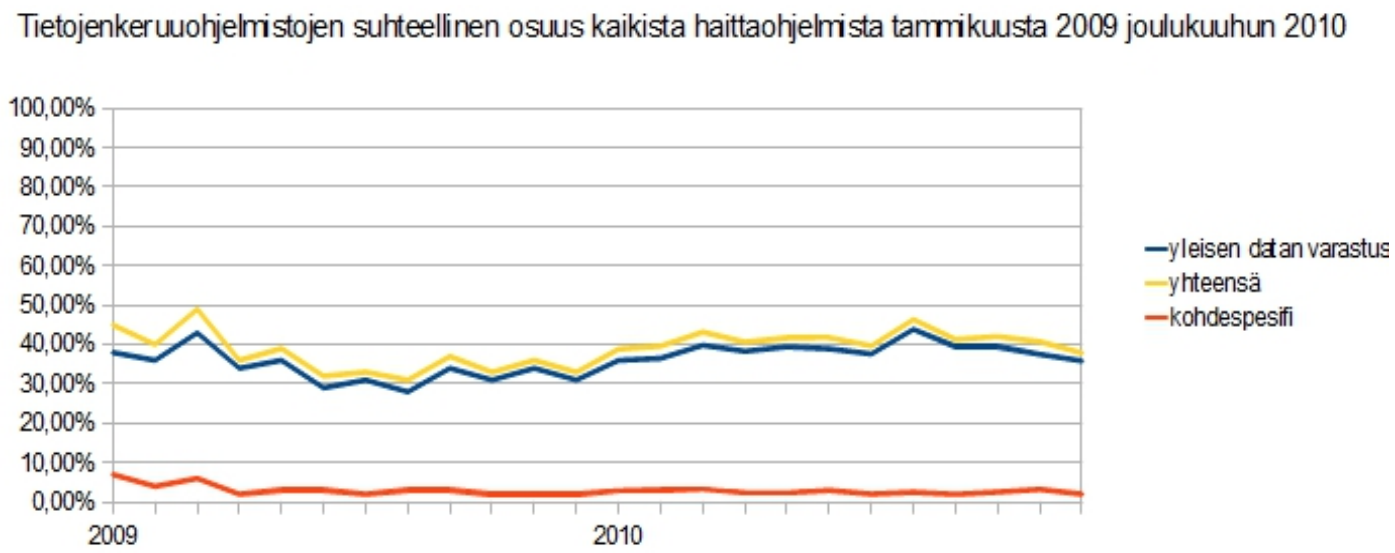
Taulukossa 1 tarkastellaan tietojenkalastelun kohdistumista eri talouden sektoreihin. Siitä havaitaan, että vaikka rahoitusala kokonaisuudessaan on säilyttänyt merkittävimmän osuutensa aina tarkastelujakson alusta saakka, niin viime vuosina rinnalle on noussut myös muita sektoreita. Tähän uuteen kategoriaan sisältyvät merkittävimpinä tekijöinä sosiaaliset mediat sekä pelit, joiden sisältämät tiedot ovat uutena trendinä rikollisten mielenkiinnon kohteena.

Taulukko 1. Tietojenkalastelun kohteet sektoreittain. (APWG 2008a-c; 2009a-c; 2010a-b; 2011a.)

	Finanssi	Maksupalvelut	Huutokaupat	Vähittäiskaupat	Muut
1Q2008	92,4			1,4	6,2
2Q	52	18	25	1	4
3Q	61	24	11	1	3
4Q	46	38	11	1	4
1Q2009	36	42	15	1	6
2Q	32	49	9	1	9
3Q	54	26	8	3	9
4Q	39	33	13	2	13
1Q2010	35,9	37	8,3	0,3	17,9
2Q	33,1	37,9	5,5	3,6	19,9
3Q	40,8	28,7	3,8	0,8	25,9
4Q	55,1	24,9	4,3	1	14,7

4.5 Rikosohjelmistojen suhteellinen osuus kaikista haittaohjelmista

Kuviossa 4 tarkastellaan viime vuosien ajan henkilötietoihin kohdistuvien rikosohjelmistojen suhteellista osuutta kaikista haittaohjelmista tietoverkoissa. Kohdespesifillä tarkoitetaan esim. tiettyyn yritykseen räätälöityä rikosohjelmistoa. Tarkastelujakson aikana on havaittavissa, että osuus on vakiintunut hyvin pitkälti samaan tasoon. Kuitenkin osuus on merkittävä, varsinkin ottaen huomioon trendin tuoreuden, sillä ilmiö on kehittynyt nopeasti vuoden 2005 muutamasta kymmenestä eri rikosohjelmasta nykyisiin lukuihin (APWG 2005a-k; 2006a-k; 2007a-l).



Kuvio 4. Rikosohjelmien suhteellinen osuus kaikista haittaohjelmista.(APWG 2009a-c; 2010a; 2010b; 2011a.)

5 Käytännön esimerkkejä tietojenkalastelusta

5.1 Avalanche

Avalanche on nimi, joka on annettu maailman laajimmalle tietojenkalasteluryhmittymälle ja infrastruktuurille, jota se käyttää sivujensa ylläpitämiseen. Tämä rikollisjärjestö hioi huippuunsa systeeminsä pystyttää massatuotettuja tietojenkalastelusivuja. Lisäksi järjestö on vastuussa Zeus Trojan Kitin levityksestä, mikä antaa käyttäjilleen uusia mahdollisuuksia identiteettivarkauteen. Avalanche oli vastuussa uskomattomasta kahdesta kolmasosasta kaikista kalasteluhyökkäyksistä, joita havaittiin vuoden 2009 toisessa periodissa. Tuona aikana se kohdisti hyökkäyksensä yli 40 suureen rahoitusalan instituutioon, online-palveluun sekä työnhaun palveluntarjoajaan. Avalanchen toiminta myös muuttui merkittävästi vuoden 2009 lopulla, jolloin kalastelukampanja hiljalleen loppui. (Rasmussen & Aaron 2010a, 5.)

On olemassa viitteitä siitä, että Avalanche olisi seuraaja rikolliselle ”Rock Phish” -operaatiolle, mikä sekin oli tuottoisa ja onnistunut operaatio vuoden 2006 alusta kesään 2008 asti. Rock Phish oli ensimmäinen järjestäynyt ryhmittymä, joka toi merkittävän skaalan ja automaation tietojenkalasteluun. Rock rekisteröi verkkotunnuksia säännöllisesti ja suurissa määrin käyttäen ”fast-flux” -ylläpitoa tukeakseen kalastelusivujaan ja pidentääkseen niiden ylläoloaikaa. (Rasmussen & Aaron 2010a, 6.)

Avalanche nähtiin ensimmäisen kerran joulukuussa 2008 ja se oli vastuussa 24 prosentista kaikista vuoden 2009 ensimmäisen puoliskon aikana havaituista kalasteluhyökkäyksistä. Avalanche käytti Rock Phishin tekniikoita paranneltuina ja toi niihin mukaan suuremman voluumin. Avalanchen verkkotunnuksia ylläpidettiin myös bottiverkon avulla. ”Fast-flux” -ylläpito tekee näiden ongelmallisten verkkotunnusten alasajosta hankalampaa – ei ole mitään operaattoria tai webhotellipalveluntarjoajaa, jolla olisi kontrolli sivustoon ja joka

voisi ajaa kalastelusivun alas. Verkkotunnuksen nimi itsessään täytyy siis jäädyttää verkkotunnusrekisteristä. (Rasmussen & Aaron 2010a, 6.)

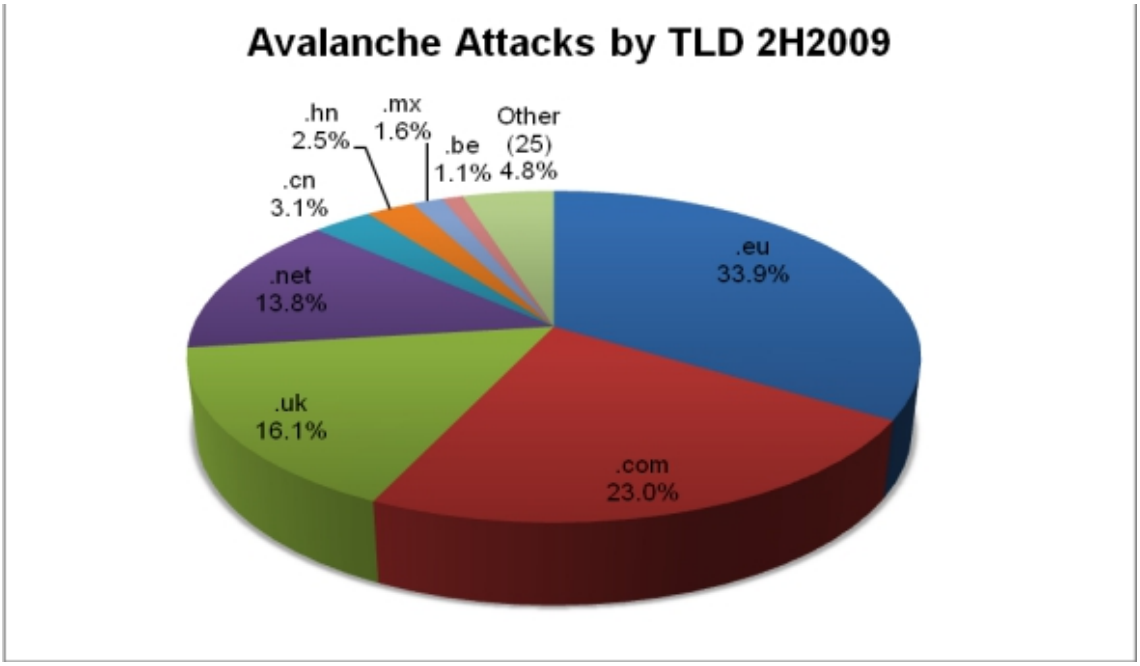
Vuoden 2009 toisessa periodissa tyypillinen Avalanche-verkkotunnus yleensä piti yllä ja välitti noin 40 erillistä hyökkäystä kerrallaan. Vaikka siis Avalanchen hyökkäysten määrä oli valtava, niin Avalanchen verkkotunnukset muodostivat vain noin 14% kaikista kalastelutarkoituksiin käytetyistä verkkotunnuksista. Jos Avalanchen verkkotunnus pysyi aktiivisena pidemmän aikaa, tekijät aloittivat joskus uuden kalastelukampanjan tällä palvelimella. (Rasmussen & Aaron 2010a, 6.)

Lisäksi rikolliset käyttivät Avalanchen infrastruktuuria levittääkseen Zeus-rikosohjelmistoa. Potentiaalisille uhreille lähetettiin kalasteluviestejä, joissa mainostettiin suosittuja ohjelmistopäivityksiä, tiedostonjakopalveluja tai ladattavia lomakkeita veroviranomaisilta. Mikäli vastaanottaja avasi viestin linkin ja sai tartunnan, niin rikollisten oli tämän jälkeen helppo ottaa etäyhteys uhrin koneeseen ja varastaa siihen talletetut henkilökohtaiset tiedot ja salasanat. Tämä Avalanchen ensi kertaa käyttämä yhdistelmä tietojenkalastelua ja haittaohjelmia, mitä vielä mainostettiin roskapostilla, on jälkeenpäin muodostunut yhdeksi kaikkein tehokkaimmista huijauskeinoista internetissä. (Rasmussen & Aaron 2010a, 6-7.)

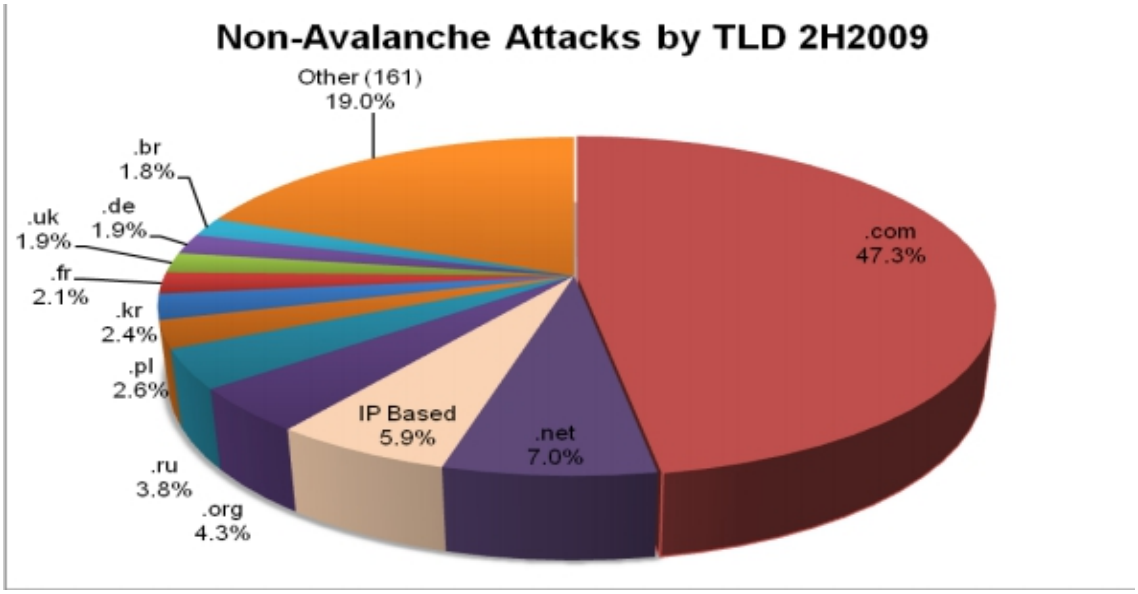
Avalanchen hyökkäyskampanja käytti verkkotunnuksia, jotka olivat melkein identtisiä keskenään. Tällaisia olivat esimerkiksi 11f1iili.com, 11t1jtiil.com, 11t1kt1il.com ja 11t1kt1pl.com. Nämä verkkotunnussetit olivat siten helposti havaittavissa niille, jotka osasivat niitä etsiä. Hyökkäykseen valmistautuessaan Avalanche rekisteröi ensin lukuisia verkkotunnuksia yhdestä kolmeen webhotellin kautta. Ryhmä myös kohdisti yksittäisiä rekisteröintejä pieneen määrään muita rekisteröintipalveluja testimielessä. Jos jokin rekisteröinpalvelu reagoi nopeasti, ja alkoi jäädyttää Avalanchen rekisteröimiä verkkotunnuksia tai ottaa käyttöön muunlaisia turvallisuustoimenpiteitä, rikolliset yksinkertaisesti siirtyivät toisiin haavottuvaisempiin rekisteröintipalveluihin. Yhden haavoittuvaisen tai muuten reagoimattoman rekisteröintipalvelun oli helposti

mahdollista muuttua portiksi jatkuville kalasteluhyökkäyksille. (Rasmussen & Aaron 2010a, 7.)

Avalanche teki saman ylätason verkkotunnuksille rekisteröiden jatkuvasti TLD:tä siellä, missä verkkotunnuksia ei suljettu riittävän nopeasti. Avalanche käytti verkkotunnuksia 33 TLD:ssä vuoden 2009 toisessa periodissa, mutta pääosa rekisteröinneistä sijoittui muutamaan suureen TLD:hen, kuten .net-, .com-, .eu-, ja .uk-päätteisiin. Esimerkiksi Avalanche rekisteröi 645 .eu nimeä vuoden 2009 ensimäisessä periodissa ja nosti sen sitten 1044:ään toisessa periodissa. Verkkotunnusten sulkeminen näissä paljon jatkuvien hyökkäyksien kohteena olevissa TLD:ssä riippui suurimmaksi osaksi tai kokonaan verkkotunnusten rekisteröintipalveluyrityksistä. (Rasmussen & Aaron 2010a, 8.)



Kuvio 5. Avalanchen hyökkäykset. (Rasmussen & Aaron 2010a, 8.)



Kuvio 6. Muiden kuin Avalanchen hyökkäykset.(Rasmussen & Aaron 2010a, 8.)

Toiset TLD:t, kuten .biz, .info ja .org jäivät puolestaan melkein koskemattomiksi Avalanchen toimesta – todennäköisesti johtuen siitä, että ne olivat nostattaneet tehokkaat puolustukset ja tehneet siten itsestään epäkiinnostavan kohteen. Näiden TLD-rekisterien ylläpitäjät tarkkailivat rekisteröintejä hyökkäysten varalta ja viestittävät ne sitten nopeasti webhotellipalveluntarjoajille. Ne olivat myös taipuvaisia jäädyttämään verkkotunnuksia siinä tapauksessa, että webhotellipalveluntarjoaja oli tehoton niin tekemään. (Rasmussen & Aaron 2010a, 9.)

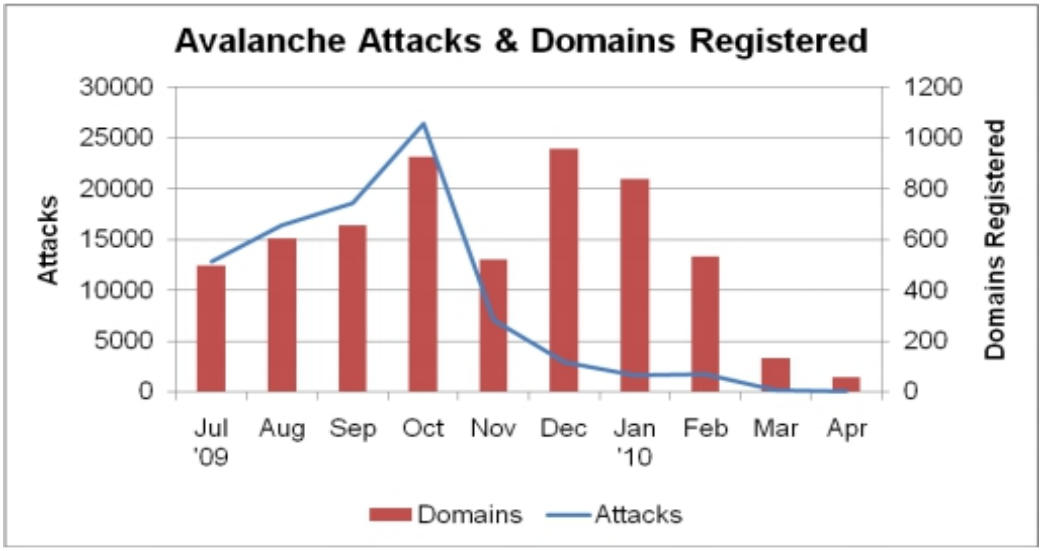
Vuoden 2009 aikana muutamat TLD-rekisterien ylläpitäjät ympäri maailman päivittivät vastatoimenpiteensä väärinkäytöksille johtuen Avalanchen valtavasta hyökkäysmäärästä. Esimerkiksi Nominet ja .uk-rekisteri kehittivät ulospäin suuntautuvia ohjelmia verkkotunnusrekistereihin tarjoten uutta ”kalastelulukko”-palvelua, jonka tarkoituksena on tehdä olennaisten verkkotunnusten jäädyttäminen helpommaksi näiden palveluiden tarjoajille. (Rasmussen & Aaron 2010a, 9.)

Muutamat pienemmät rekisterit olivat myös vastanneet tehokkaasti Avalanchen hyökkäyksiin tarkastelujakson aikana. Esimerkiksi hondurasilaista .hn

verkkotunnusrekisteriä varoitettiin silloin, kun sen palvelimia käytettiin lukuisten hyökkäyksien alustana aina heinäkuuhun 2009 asti. Rekisteri työskenteli webhotellien kanssa ahkerasti kunnes Avalanche siirtyi pois viikkoa myöhemmin. Myös toinen pieni rekisteri, eli Mansaarten (.im) rekisteri oli yhteistyöhalukas ja suostui jäädyttämään monia rikollisia verkkotunnuksia. (Rasmussen & Aaron 2010a, 9.)

Koska Avalanchen hyökkäykset olivat niin vahingollisia, laajalle levinneitä ja tunnistettavia, ne saivat kohdistettua huomiota tietoturvayhteisöltä. Avalanchen kampanjan aikana ei ollut epätyypillistä, että hyökkäysten kohteena olleet instituutiot, verkkotunnusrekisterit, webhotellit sekä muut palveluntarjoat olivat hyvinkin tietoisia kampanjasta ja toimivat yhdessä hyökkäysten torjumiseksi. Tuloksena Avalanchen hyökkäyksillä oli paljon keskimääräistä pienempi ylläoloaika verrattuna muuhun tietojenkalasteluun ja yhteisön työpanos osittain neutralisoi fast-flux-ylläpidon edun. Huolimatta tästä, hyökkäykset olivat ilmiselvästi kannattavia. (Rasmussen & Aaron 2010a, 9.)

Marraskuun puolivälissä 2009 tietoturvayhteisön jäsenet saivat hetkeksi ajettua Avalanchen bottiverkon alas. Kesti kuitenkin vain noin viikon ennen kuin rikolliset saivat sen uudelleen käynnistettyä. Tämän tapahtuman jälkeen Avalanchen toiminta kuitenkin muuttui merkittävästi. (Rasmussen & Aaron 2010a, 9.)



Kuvio 7: Avalanchen hyökkäykset ja verkkotunnusten rekisteröinti. (Rasmussen & Aaron 2010a, 9.)

Avalanchen domainien rekisteröiminen oli korkeimmillaan joulukuussa 2009, mutta silloin Avalanche teki yhä vähemmän ja vähemmän hyökkäyksiä kokonaisuudessaan. Maaliskuussa 2010 Avalanche toimi taustavoimana enää yhdelle hyökkäykselle verkkotunnusta kohden, ja hyökkäykset vähenivät 59:ään huhtikuussa 2010. (2010a, 10.)

Taulukko 2. Hyökkäysten ja verkkotunnusten suhde. (Rasmussen & Aaron 2010a, 10)

Month	Attacks	Domains
July 2009	12,793	498
August 2009	16,372	603
September 2009	18,633	656
October 2009	26,411	924
November 2009	7,089	523
December 2009	2,952	959
January 2010	1,654	839
February 2010	1,784	532
March 2010	133	133
April 2010	59	59

Vanha Rock Phish -operaatio muuttui uinuvaksi kesällä 2008 vain syntyäkseen uudestaan muutama kuukausi myöhemmin vielä pahempana Avalanchena.

Tulevaisuus näyttää, syntyykö Avalanche uudestaan vielä jossain uudessa muodossa.

5.2 ZeuS/Zbot

ZeuS on hyvin tunnettu pankkipalvelujen troijalaisten luontiohjelmisto. Kerran saastuttuaan tietokone lähettää varastetun datan bottien komento- ja kontrollointiserverille (C&C), minne se tallennetaan. (Stevens & Jackson 2010.)

ZeuSta myydään rikollisessa alamaailmassa ohjelmistopakettina hintaan 3000-4000 dollaria ja se on todennäköisesti kaikkein yleisimmin finanssisektorin huijauksiin keskittyneiden rikollisten käytössä. ZeuS on kehittynyt ajan myötä ja sisältää nykyään hyvin tehokkaita työkaluja tiedon varastamiseen. Sen avulla voidaan suorittaa seuraavia toimintoja:

- varastaa dataa, joka jätetään HTTP kaavioihin
- varastaa tilitiedot, jotka ovat talletettuja Windows Protected Storageen
- varastaa asiakkaan puolen X.509 PKI-sertifikaatteja
- varastaa FTP- ja POP-tilien kirjautumistiedot
- varastaa tai poistaa HTTP- ja flashkeksit
- muokata kohdenettisivujen HTML:ää informaation varastamistarkoituksiin
- uudelleenohjata uhrit kohdesivuilta hyökkääjän kontrolloimille sivuille
- ottaa kuvankaauppauksia ja haalia HTML-koodia kohdesivuilta
- etsiä ja ladata tiedostoja saastuneelta tietokoneelta
- muokata local hosts tiedostoa (%systemroot%\system32\ drivers\etc\hosts)
- ladata ja suorittaa mielivaltaisia ohjelmia
- poistaa tärkeitä rekisteriavaimia tehden tietokoneen mahdottomaksi käynnistää Windowsia.

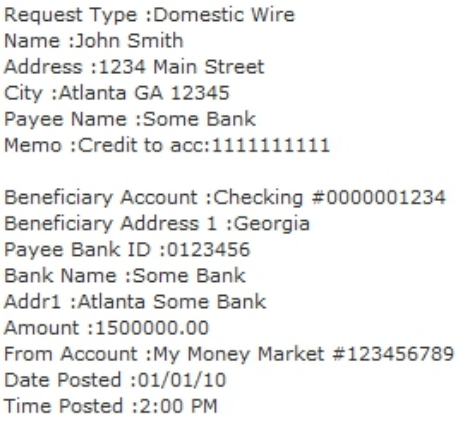
Viimeisimpiä versioita ZeuS-ohjelmistosta on tällä hetkellä 1.3.4.x ja se on yksityisesti myynnissä. Ohjelmiston tekijä on käyttänyt paljon aikaa

suojatakseen tämän systeemin käyttäen laitteistopohjaista lisensointisysteemiä, jotta sitä voi ajaa ainoastaan yhdessä tietokoneessa. Tämä on ensimmäinen kerta, kun rikolliset ovat käyttäneet näin pitkälle meneviä toimia suojatakseen ohjelmansa lähdekoodin. (Stevens & Jackson 2010.)

Viimeisin julkinen versio, johon CTU (SecureWorks Counter Threat Unit) on törmännyt kentällä on 1.2.7.19. Tätä versiota myydään aktiivisesti ja siinä on Firefoxin lomakkeensieppaustoiminto sisällytettynä. Firefoxin moduuli sallii ZeuS-troijalaisen siepata dataa kaikista esitäytetyistä Firefoxin lomakkeista. Webinjects-tekstitiedosto, joka sallii tekstikenttien lisäämisen Internet Explorerissa, ei puolestaan toimi Firefoxissa. Webinjects-moduulin tarkoituksena on lisätä ylimääräinen tekstikenttä uhrin täytettäväksi silloin, kun hän kirjautuu sisään pankin sivuille. Näiden tekstikenttien tarkoituksena on kysyä ylimääräistä dataa käyttäjänimen ja salasanan lisäksi. (Stevens & Jackson 2010.)

Vuonna 2010 listaus Zeuksen moduuleista oli seuraava:

- Zeus kit 1.3.4.x, $3000-$4000
- Backconnect $1500
    - Mahdollistaa hyökkääjän yhdistämisen takaisin saastuneeseen koneeseen rahansiirtojen suorittamista varten. Tällä tavalla pankkien yrittäessä jäljittää rahansiirtojen alkuperää se palaa aina tilinomistajan tietokoneeseen.
- Firefox form grabber $2000
    - Tämä moduuli sieppaa dataa lomakekentistä, joita Firefox tallentaa. Tämä data voi sisältää mm. käyttäjänimiä ja salasanoja pankkitileistä.
- Jabber (IM) chatti-ilmoittaja $500
    - Jabber moduuli sallii hyökkääjän vastaanottaa varastettua dataa reaaliajassa. Jos pankkitili on suojattu kortilla, joka generoi satunnaisia numeroja, niin hyökkääjä voi päästä silti käsiksi uhrin tiliin reaaliajassa sen jälkeen, kun uhri on kirjautunut sisään käyttäen tätä puolustuskeinoa.



Kuva 1. Jabber-moduulin dataa. (Stevens & Jackson 2010.)

- VNC (Virtual Network Computing) yksityinen moduuli $10,000
    - Tämä on samankaltainen moduuli kuin takaisinyhdistämismoduuli sillä erotuksella, että se sallii käyttäjän perustaa täysin toimivan virtuaalisen yhteyden. Hyökkääjä voi ottaa täyden kontrollin saastuneesta koneesta uhrin tietämättä. VNC siis tarjoaa hakkerille ei pelkästään mahdollisuuden verkon ohjaamisesta vaan täyden läsnäolon etäohjaamisesta sallien hakkerin käyttää uhrin laitteistoa ja ohjelmia välttääkseen pankkien tunnistussysteemit. Kokonaisuudessaan se sallii hakkerin päästä yli monista laitteistopohjaisista autentikaatiosysteemeistä.
- Windows 7 / Vista tuki $2000
    - Tämä moduuli tarjoaa nimensä mukaisesti tuen Windows 7:lle ja Vistalle. Ilman tätä botnetin hallintaohjelma on rajoittunut Windows XP -pohjaisille systeemeille.

Vuoden 2010 aikana Zeus 1.4. oli betatestausvaiheessa. Se sisältää kaksi avainominaisuutta, jotka tekevät Zeus Banking Trojanista vielä entistäkin vaarallisemman. Toinen on uusi kyky tehdä webinjektioita Firefoxselaimella. Toinen on puolestaan monimuotoinen salaus. Tällä tarkoitetaan troijalaisen kykyä uudelleensalaukseen jokaisen tartunnan yhteydessä. Jokainen tartunta on siis yksilöllinen. Versio 1.4 mahdollistaa myös Zeuksen tiedostonimien satunnaisen generoinnin, joka toimii vastaavalla tavalla. Nämä ominaisuudet tekevät tästä rikosohjelmistosta erittäin vaikean havaita antivirusohjelmistoilla.

Tästä seuraakin, että oikeastaan ainoa tapa suojautua ohjelmalta on kokonaan erillisen tietokoneen käyttäminen pelkästään verkkopankkiasiointiin. (Stevens & Jackson 2010.)

6 Suojautuminen ja vaikutusten minimointi

Tietojenkalastelua vastaan voidaan taistella monin keinoin aina lainsäädännön kehittämisestä teknologisiin ratkaisuihin. Tärkeimpänä osa-alueena on kuitenkin koulutus, jonka avulla käyttäjät osaavat paremmin tunnistaa kalasteluviestit, sillä mikään tekninen ratkaisu ei yksistään ole sataprosenttisen luotettava.

6.1 Käyttäjien tietouden lisääminen

Yleensä minkä tahansa nykyisen tietoteknisen infrastruktuurin keskellä käyttäjä on tietoturvan näkökulmasta se heikoin lenkki. Koulutus onkin tässä tapauksessa kaikkein tehokkain menetelmä pienentää tietoturvauhan toteutumisen riskiä.

Kalastelutekniikoista tämä koskee kaikkein lähimmin niin sanottua keihäskalastelua. Tässä tekniikassa on kyse hyvin spesifin viestin lähettämisestä tietylle yrityksen käyttäjälle. Tätä ennen käyttäjästä on voitu eri tekniikoilla kerätä tietoja pitkän ajan kuluessa, jotta viestistä saataisiin mahdollisimman aidon oloinen. Vaikka tämän kaltaiseen viestiin voi langeta alan ammattilainenkin, koulutuksen merkitys on tällaisissa hyökkäyksissä joka tapauksessa ratkaisevassa asemassa.

Tämä tekniikka on osittain valjastettu jopa opetuskäyttöön eri paikoissa, mukaan lukien Yhdysvaltain sotilasakatemia West Point New Yorkissa. Esimerkiksi toukokuussa 2004 tehtiin aiheeseen liittyvä koe, jossa lähetettiin kaikille West Pointin kadeteille räätälöity kalasteluviesti. Heistä jopa 80% saatiin luovuttamaan tietojaan tällä tavalla. (Phishing 2011.)

Koulutuksen merkitys on tärkeä myös geneerisimmissä hyökkäyksissä. Yhä edelleen kiertää viestejä, joissa kalastelija yksinkertaisesti kysyy käyttäjän salasanaa ja käyttäjänimeä naamioituen esimerkiksi sen organisaation verkkoherraksi, jonka nimissä hän näitä kyselee. Kuten historiaosiossa

kuvattiin, niin tätä samaa hyökkäysmallia on käytetty jo 1990-luvun puolesta välistä asti ja edelleenkin se vaikuttaa toimivan.

Mikäli käyttäjään siis otetaan yhteyttä salasanan tai käyttäjänimen kyselytarkoituksessa, niin todennäköisesti kyseessä on kalasteluyritys. Jos se vaikuttaa kuitenkin aidolta, niin siinä kohtaa on järkevää ottaa yhteyttä suoraan tähän yritykseen, mistä viesti näytti tulevan ja tarkistaa, onko sähköposti paikkansapitävä (Phishing 2011).

Epäilyttävien osoitteiden kohdalla puolestaan on järkevää syöttää haluttu osoite itse suoraan osoiteriville, tai syöttää sellainen osoite, jonka itse tietää yrityksen lailliseksi osoitteeksi ennemmin kuin vain luottaa epäilyn kohteena olevan sähköpostin hyperlinkkiin (Phishing 2011).

Viestin sisältämät henkilökohtaiset tiedot

Melkein kaikki oikeat sähköpostit yrityksiltä asiakkaille sisältävät sellaista informaatiota, mikä ei ole vapaasti saatavilla kalastelijoille (Phishing 2011). Tällaiset yritykset, kuten esimerkiksi PayPal, osoittavat sähköpostinsa asiakkaansa käyttäjänimellä. Mikäli sähköposti on osoitettu hyvin yleisesti, kuten esim. ”Dear PayPal customer”, se on todennäköisesti yritys kalastella tietoja. Sähköpostit pankeilta ja luottokorttiyhtiöiltä sisältävät yleensä osittaisia tilinumeroita. Ihmisten tulisikin olla epäluuloisia, jos viesti ei sisällä mitään erityisen henkilökohtaista tietoa. (Phishing 2011.)

Toisaalta kalasteluyrityksissä jo vuoden 2006 alusta lähtien on käytetty henkilökohtaisia tietoja, jolloin henkilökohtaisen tiedon olemassaolo itsessään ei takaa viestin aitoutta (Phishing 2011). Tässä niin kuin monessa muussakin asiassa täytyisi käyttäjän itse osata päätellä, minkälainen on luotettava viesti ja mikä ei. Ainoa keino puolestaan kehittää tällaista päättelytaitoa on kokeneisuus ja sitä kautta pääsemme taas koulutuksen tärkeyteen.

Vaikka näin suomalaisena phishingviestit ovat vielä melko hyvin havaittavissa johtuen osittain suomen kielen käännösohjelmien vaillinaisuuksista, ei kuitenkaan kannata tuudittautua siihen, etteikö tämä seikka muuttuisi

lähitulevaisuudessa. Luulisin, että jo muutaman vuoden sisällä alkaa Suomessakin esiintyä täysin aidon oloisia kalasteluviestejä.

6.2 Tekniset vastatoimet

Phishingin vastaisia suojatoimia on jo sisällytetty ominaisuuksina selaimiin, joko lisäosina, työkaluriveinä tai osana nettisivun kirjautumiskäytäntöjä. Seuraavassa on esitelty muutamia yleisimpiä lähestymistapoja teknisten vastatoimien problematiikkaan. Sitä ennen on kuitenkin syytä selvittää varmenteisiin liittyviä käytäntöjä.

6.2.1 Varmenteet

Varmenteiden avulla käyttäjä voi varmistua siitä, että verkon palvelujen tarjoaja on se taho, joka hän väittääkin olevansa. Varmenteita käytetään myös ohjelmistojen aitouden todistamiseen ja käyttäjien tunnistamiseen. Varmenteita myöntävät varmennepalveluja tarjoavat luotetut varmenteiden myöntäjät (Certificate Authority, CA). Tavallisesti varmenteista muodostetaan hierarkia, jossa ylimmän tason juurivarmenteella allekirjoitetaan alivarmentajien varmenteita, jotka vuorostaan allekirjoittavat myönnettävät varmenteet. Varmennepuun haarat ovat toisistaan erillisiä eikä yhden haaran eli alivarmentajan ja sen alla olevien varmenteiden mitätöinti vaikuta muihin haaroihin. (CERT-FI 2011.)

Esimerkiksi www-sivustovarmenteet sisältävät tiedon varmennettavan sivuston verkkotunnuksesta, erinäisiä tietoja tahosta, jolle varmenne on myönnetty, varmenteen varmentajakohtaisen sarjanumeron, voimassaoloajan, tiedon varmentajan varmenteiden sulkulistasta (CRL, Certificate Revocation List) ja varmenteen tilan tarkastamispalvelun (Online Certificate Status Protocol, OCSP) sijainnista, varmenteen myöntäjästä, julkisesta avaimesta ja varmenteen eri käyttötarkoituksista. Varmenteiden käyttökohteena voi yksittäisten verkkotunnusten lisäksi olla muun muassa verkkotunnusten aliverkkoja, sähköpostiosoitteita tai ohjelmistokehittäjiä. (CERT-FI 2011.)

Käyttöjärjestelmiin ja joissain tapauksissa myös selaimiin on sisäänrakennettuna luotettujen juurivarmenteiden luettelot. Näiden tahojen myöntämiä sivustokohtaisia varmenteita selain pitää luotettavina. Varmenteita käytetään muun muassa salatuissa SSL/TLS-tietoliikenneyhteyksissä (HTTPS). Jos sivuston varmenne ei ole juurivarmentajien listalla tai tämän avaimella allekirjoitetun varmenteen allekirjoittama, selain varoittaa siitä käyttäjää. (CERT-FI 2011.)

6.2.2 Aitojen sivujen tunnistaminen

Useimmat phishingin kohteena olevat nettisivut ovat suojattuja, eli niiden palvelimen autentikoimiseen käytetään SSL:ää tai vahvaa PKI-kryptografiaa. Itse sivujen tunnistamiseen liittyy kuitenkin seuraavia ongelmia.

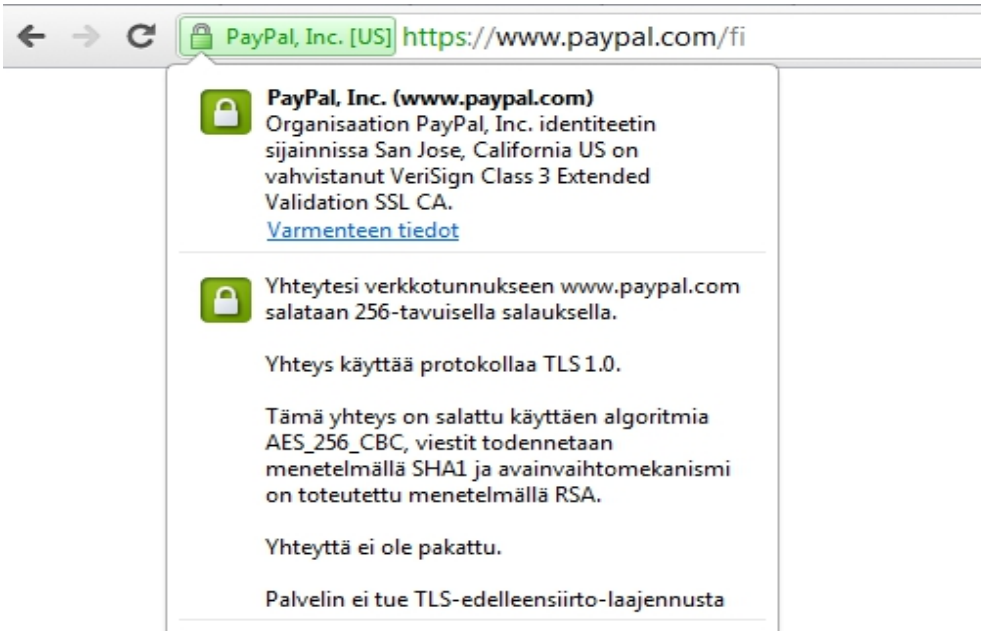
Turvallisessa sivujen autentikoinnissa käytettäessä TLS:ää (Transport Layer Security) on kolme tärkeää osa-aluetta:

- autentikoidun tilan osoittaminen
- verkkotunnuksen osoittaminen
- varmentajan osoittaminen.

Nämä kaikki tiedot pitäisi olla kenelle tahansa käyttäjälle ensinnäkin näkyvissä ja toisekseen jokaisen käyttäjän pitäisi olla tietoinen niiden sisällöstä. Vain sillä tavalla käyttäjä voi olla varma sivun aitoudesta.

6.2.3 Autentikoidun tilan osoittaminen

Nykykäytäntönä suojatun yhteyden merkkinä on yleisesti näyttää sivun osoitepalkissa lukko, ”http”:n sijasta ”https” ja nämä kaikki vielä vihreällä pohjalla. Jotkut palvelut vielä näyttävät näiden merkkien lisäksi, mihin yritykseen kyseinen varmenne on liitetty, kuten esimerkiksi yrityksen PayPal kohdalla. Tämä viimeinen käytäntö on liitetty EV-varmenteisiin. Lukkoa napsauttamalla saadaan esiin sertifikaatin tiedot. Nämä tiedot näkyvät seuraavassa esimerkkikuvassa 2.



Kuva 2. Esimerkki EV-sertifikaatista.

6.2.4 Verkkotunnuksen osoittaminen

Käyttäjän odotetaan vahvistavan omatoimisesti, että verkkotunnus on juuri se, minkä he olettavat sen olevan. Monesti URL:t ovat kuitenkin liian monimutkaisia helposti jäsenneltäviksi. Käyttäjät eivät yleensä tiedä tai tunnista sen laillisen sivun osoitetta, johon he ajattelivat surffata, joten autentikoinnista tulee merkityksetöntä. Edellytys mielekkäälle palvelimen varmentamiselle on luoda järjestelmä, joka on merkityksellinen käyttäjälle. Esimerkiksi monet nettikaupat saattavat muuttaa verkko-osoittettaan koko sivustonsa sisällä, mikä lisää mahdollisuuksia hämmennykseen. Pelkän verkkotunnuksen näyttäminen nettisivulla – kuten jotkut kalastelunvastaiset työkalurivit tekevät – ei ole riittävää. (Phishing 2011.)

Parannuksena tähän on Internet Explorer 8:sta lähtien käytännöksi muodostunut verkkotunnuksen näyttäminen mustalla ja lopun osoitteen näyttäminen harmaana. (Phishing 2011). Tämä parantaa jo huomattavasti

URL:n jäsentämistä nopealla vilkaisulla. Myös muut selainvalmistajat Googlesta Mozillaan käyttävät nykyään tätä tekniikkaa.

6.2.5 Varmentajan osoittaminen

Selaimen täytyy esittää, kuka on se auktoriteetti, joka osoittaa käyttäjän olevan yhteydessä juuri sinne, minne on tarkoituskin. Yksinkertaisimmalla tasolla mitään auktoriteettiä ei esitetä ja silloin nettiselain on se auktoriteetti - ainakin käyttäjän puolesta. Selainten kehittäjät ottavat vastuun kontrolloimalla juurilistaa hyväksyttävistä CA:ista. Tämä on nykyinen tapa toimia. (Phishing 2011; CERT-FI 2011).

Ongelma on siinä, että kaikki CA:t eivät kuitenkaan toteuta keskenään yhtä tehokasta tietoturvapolitiikkaa. Esimerkiksi sivun varmenteen juurivarmentajan allekirjoitus voidaan korvata toisen juurivarmentajan allekirjoituksella ilman, että selain ottaa tähän kantaa. Tällä tavalla voidaan muuttaa koko varmenteen sisältö. Tämä malli on erityisen haavoittuvainen, mikäli saadaan murrettua jokin juurivarmentaja, kuten kävi 2011 DigiNotarin tapauksessa (CERT-FI 2011). Tällöin nopea reagointi ja yrityksen läpinäkyvä tietoturvapolitiikka on ratkaisevaa.

Yksi ratkaisu tähän ongelmaan olisi se, että selaimen tulisi näyttää - ja käyttäjän tuntea - kyseisen juurivarmentajan nimi. Tämä esittäisi CA:n brändinä ja antaisi käyttäjille mahdollisuuden oppia tunnistamaan ne CA:t, joiden varmenteita hän yleisimmin tulisi tarvitsemaan. Brändien käyttäminen olisi myös hyödyllistä pakottaen CA:t käyttäjäpalautteen pohjalta kehittämään laatustandardejaan. (Phishing 2011). Esimerkiksi DigiNotarin tapauksessa tietomurto oli mahdollinen juuri löysän tietoturvapolitiikan takia, mikä asettaa koko järjestelmän epäilyttävään valoon (CERT-FI 2011).

6.3 Kalasteluviestien ja sivujen analysointi

Erityiset roskapostifiltterit voivat vähentää sitä kalasteluviestien määrää, mikä saavuttaa käyttäjän postilaatikon. Tämän tyyppiset ratkaisut pohjautuvat

koneoppimiseen ja luonnollisen kielen prosessoinnin lähestymistapoihin kalasteluviestien määrittelemiseksi (Phishing 2011). Tätä samankaltaista datan analysointikeinoa voidaan käyttää myös eri sivujen sisällön tarkistamiseen, jolloin kohteena olevasta sivusta etsitään tietojenkalastelulle tyypillisiä piirteitä.

6.4 Yhteenveto tietoturvakäytännöistä

Ohjeita kaikille käyttäjille:

- Asennetaan aina palomuurit, virustorjuntaohjelmistot sekä haittaohjelmien tunnistusohjelmat jokaiseen käytettyyn koneeseen ja pidetään ne ajantasalla päivitysten suhteen.
- Käytetään viimeisimpiä selainversioita ja asennetaan niihin kaikki tietoturvapäivitykset heti, kun ne ovat saatavilla.
- Otetaan selvää viestin alkuperästä ja aitoudesta aina, kun saadaan viesti, jossa pyydetään tilitietoja, sillä talousorganisaatiot eivät lähestulkoon ikinä pyydä näitä tietoja.
- Ei koskaan lähetetä sähköpostin välityksellä taloudellisia tai muita henkilökohtaisia tietoja.
- Avataan sähköpostiliitteet ainoastaan täysin luotettavilta tahoilta tulleista viesteistä.
- Ei koskaan seurata vähänkään epäilyttävien sähköpostien linkkejä.
- Raportoidaan epäilyttävistä viesteistä virallisille tahoille.
- Seurataan säännöllisesti uutisia liittyen uusiin tietoturvauhkiin ja tietojenkalasteluun.

Ohjeita yrityksille:

- Tarkkaillaan lokeja palomuureista, tietomurron tarkkailusysteemeistä, DNS palvelimista ja välityspalvelimista päivittäin tartunnan varalta.
- Tarkkaillaan ulospäin suuntautuvia SMTP-yhteysyrityksiä, jotka eivät ole peräisin normaaleista SMTP sähköpostiyhdyskäytävistä.

- Luodaan tiukat salasanakäytännöt asiakkaille, servereille ja reitittimille ja pidetään huolta, että niitä noudatetaan.
- Varmistetaan, että vain hyväksyttävät laitteet voidaan yhdistää organisaation verkkoon.

(TrendMicro 2006, 10.)

7 Yhteenveto ja tietojenkalastelun tulevaisuus

Opinnäytteessa lienee tullut selkeästi esiin tietojenkalastelun menetelmien moninaisuus. Vaikka motiivit liittyvät nykyään tietojenkalastelun osalta yhä useammin rahallisen hyödyn tavoitteluun, niin keinot ovat hyvinkin erilaisia ja koko ajan keksitään uusia. Tutkimusongelman rajaaminen onkin osoittautunut hankalaksi alueen ollessa niin valtava. Tästä syystä olen joutunut jättämään pois monien sellaisten keinojen kuvauksia, jotka liikkuvat tietoteknisten ja muiden sovellutuksien rajamailla sekä sellaisia keinoja, joissa käytetään hyvin laajaa kirjoja eri menetelmiä yhdessä. Tähän kuuluvat esimerkiksi nykyään vähän väliä raportoidut tietomurrot eri yrityksiin tai valtion virastoihin.

Yksi vakavimmista viime aikojen tietomurroista kohdistui hollantilaiseen tietoturvasertifikaatteja jakavaan DigiNotariin (Linnake, T. 2011). Hyökkääjät saivat haltuunsa DigiNotarin varmenteiden tekoon liittyvää tietoa, jonka avulla he pystyivät generoimaan aitoja uusia sertifikaatteja. Tällä tavalla voitiin esimerkiksi luoda täysin toimiva Googlen varmenne, johon selain luotti selaimessa olevan juurivarmentajien listan perusteella. Seurauksena oli murtoja esimerkiksi iranilaisten Google-tileihin, sillä käyttäjät eivät kyenneet millään erottamaan sertifikaattien valheellisuutta. (CERT-FI 2011.)

Tämä tapaus paljastaa suuria puutteita nykyisessä varmennejärjestelmässä, jossa CA on keskitetysti vastuussa palvelinten varmentamisesta. Tietomurto tällaiseen juurivarmentajaan aiheuttaa valtavia tietoturvauhkia, jotka voivat paisua suuriinkiin mittasuhteisiin. Se myös syö luottamusta koko varmennejärjestelmään, mikä vaatisi tulevaisuudessa mittavia uudistustoimia.

Lisäksi tämä on vain yksi esimerkki tietojenkalastelun valtavaksi paisuneessa rikollisessa bisneksessä. Informaatioyhteyskunnassa näyttäisi informaation arvo vain kohoavan ja samalla tietomurrot, tietojenkalastelu ja niihin liittyvät lieveilmiöt tulevat vain lisääntymään. Tällä hetkellä käydään jatkuvaa kilpavarustelua tietoturvayhteisöjen ja rikollisten välillä kummankaan saamatta niskalenkkiä toisesta - rikollisten tosin kulkiessa aina askeleen edellä. Tästä on

seurauksena valtava kentän monimutkaistuminen ja paisuminen rikollisten kehittäessä yhä uusia keinoja päämääränsä saavuttamiseksi.

Se, mikä alkoi 1990-luvun puolivälissä nykynäkökulmasta liki viattomana American Onlinen käyttäjien tilitietojen kalasteluna, on muuttunut ammattirikollisten bisnekseksi, jossa pyörivät aina vain suuremmat rahat. Joidenkin arvioiden mukaan tietojenkalastelu on kasvanut viime vuosina nopeammin kuin mikään muu talouden haara tämän taantuman aikana.

Tilanne ei ole kuitenkaan täysin synkkä. Yksityisen käyttäjän näkökulmasta tietojenkalastelun voi huolellisella nettikäyttäytymisellä välttää sekä sen aiheuttamia vahinkoja pienentää. Ratkaisevassa asemassa on koulutus aiheesta. Se, mitä monessa eri paikassa on viime aikoina ilmaistu, pätee edelleen: kukaan ammattimainen verkkopalvelujen ylläpitäjä ei koskaan kysy käyttäjänsä salasanaa tai tunnusta. Ei kannata käyttää samaa salasanaa tai tunnusta eri palveluissa. Ei ole myöskään syytä avata epäilyttävää sähköpostiviestiä, tai viesteissä olevia hyperlinkkejä. Virustorjunta ja järjestelmäpäivitykset on järkevää pitää ajan tasalla. Ei myöskään kannata ladata epäilyttäviä tiedostoja koneelle tai seikkailla internetin synkemmällä puolella.

Näillä yksinkertaisilla keinoilla kotikäyttäjä pystyy edelleen suurimmaksi osaksi välttämään internetin sudenkuopat. Yrityspuolella sama pätee yksittäisen työntekijän kohdalla, tietenkin yrityksen sisäisen tietoturvapolitiikan huomioon ottaen. Nykyään tietojenkalastelun vastainen yhteisö on aktiivinen ja järjestäytynyt. Se pyrkii ajamaan alas mahdollisimman nopeasti uudet vahingolliset sivustot sekä torjumaan uusien rikosohjelmien tuomat uhat. Yhteistyön tiivistämistä operaattorien, verkkotunnusrekisterien ja webhotellipalvelujen tarjoajien sekä muiden internetin infrastruktuurin toimijoiden välillä olisi kuitenkin vielä kehitettävä entisestään.

Ilmiötä ei voida koskaan täysin kitkeä pois, sillä on aina olemassa tahoja, jotka hyötyvät tämänkaltaisesta toiminnasta. Kuitenkin jokainen yritys niin kuin

yksityinenkin käyttäjä voi omalla nettikäyttäytymisellään vaikuttaa merkittävästi riskin suuruuteen.

LÄHTEET

APWG 2005a. Phishing Activity Trends Report – January 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005b. Phishing Activity Trends Report – February 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005c. Phishing Activity Trends Report – March 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005d.Phishing Activity Trends Report – April 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005e. Phishing Activity Trends Report – May 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005f. Phishing Activity Trends Report – June 2005. Viitattu 5.12.2011. www.apwg.org > resources.

APWG 2005g. Phishing Activity Trends Report – July 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005h. Phishing Activity Trends Report – August 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005i. Phishing Activity Trends Report – September 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005j. Phishing Activity Trends Report – October 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2005k. Phishing Activity Trends Report – November 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006a. Phishing Activity Trends Report – December 2005. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006b. Phishing Activity Trends Report – January 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006c. Phishing Activity Trends Report – February 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006d. Phishing Activity Trends Report – March 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006e. Phishing Activity Trends Report – April 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006f. Phishing Activity Trends Report – May 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006g. Phishing Activity Trends Report – June 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006h. Phishing Activity Trends Report – July 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006i. Phishing Activity Trends Report – August 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006j. Phishing Activity Trends Report – Sept/Oct 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2006k. Phishing Activity Trends Report – November 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007a. Phishing Activity Trends Report – December 2006. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007b. Phishing Activity Trends Report – January 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007c. Phishing Activity Trends Report – February 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007d. Phishing Activity Trends Report – March 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007e. Phishing Activity Trends Report – April 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007f. Phishing Activity Trends Report – May 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007g. Phishing Activity Trends Report – June 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007h. Phishing Activity Trends Report – July 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007i. Phishing Activity Trends Report – August 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007j. Phishing Activity Trends Report – September 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007k. Phishing Activity Trends Report – October 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2007l. Phishing Activity Trends Report – November 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2008a. Phishing Activity Trends Report – December 2007. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2008b. Phishing Activity Trends Report - First Quarter 2008. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2008c. Phishing Activity Trends Report - Second Quarter 2008. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2009a. Phishing Activity Trends Report - Second Half 2008. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2009b. Phishing Activity Trends Report - First Half 2009. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2009c. Phishing Activity Trends Report - Q3 2009. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2010a. Phishing Activity Trends Report - Q4 2009. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2010b. Phishing Activity Trends Report - Q1 2010. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2010c. Phishing Activity Trends Report - Q2 2010. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2011a. Phishing Activity Trends Report - 2H 2010. Viitattu 5.12.2011. www.apwg.org > resources

APWG 2011b. Origins of the Word “Phishing”. Viitattu 6.12.2011. http://apwg.org/word_phish.html

CERT-FI 2011. Tietoturvakatsaus 3b/2011. Viitattu 6.12.2011. http://www.cert.fi > katsaukset > 2011

Domain Name System 2011. Wikipedia. Viitattu 5.12.2011. http://en.wikipedia.org/wiki/Domain_Name_System

Extended Validation Certificate 2011. Wikipedia. Viitattu 5.12.2011. http://en.wikipedia.org/wiki/extended_validation_certificate

Internet Protocol 2011. Wikipedia. Viitattu 5.12. 2011. http://en.wikipedia.org/wiki/Internet_Protocol

Linnake, T. 2011. DigiNotar yllättää – missasi Googlen. IT-viikko. Viitattu 5.12.2011. http://www.itviikko.fi/tietoturva/2011/08/31/diginotar-yllattaa--missasi-googlen/201112193/7

Phishing 2011. Wikipedia. Viitattu 6.12.2011. Wikipedia. http://en.wikipedia.org/wiki/Phishing

Rasmussen, R. & Aaron, G. 2008a. Global Phishing Survey: Domain Name Use and Trends in 2007. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2008b. Global Phishing Survey: Domain Name Use and Trends in 1H2008. Viitattu 5.12.2011. www.apwg.org > resources.

Rasmussen, R. & Aaron, G. 2009a. Global Phishing Survey: Trends and Domain Name Use in 2H2008. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2009b. Global Phishing Survey: Trends and Domain Name Use in 1H2009. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2010a. Global Phishing Survey: Trends and Domain Name Use in 2H2009. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2010b. Global Phishing Survey: Trends and Domain Name Use in 1H2010. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2011a. Global Phishing Survey: Trends and Domain Name Use in 2H2010. Viitattu 5.12.2011. www.apwg.org > resources

Rasmussen, R. & Aaron, G. 2011b. Global Phishing Survey: Trends and Domain Name Use in 1H2011. Viitattu 5.12.2011. www.apwg.org > resources

Stevens, K. & Jackson, D. 2010. ZeuS Banking Trojan Report. Viitattu 6.12.2011. http://www.secureworks.com/research/threats/zeus

The Honeynet Project 2011a. Know Your Enemy: Tracking Botnets. Viitattu 5.12.2011. http://www.honeynet.org/papers/bots

The Honeynet Project 2011b. Know Your Enemy: Phishing. Viitattu 5.12.2011. http://www.honeynet.org/papers/phishing

TrendMicro 2006. Botnet Threats And Solutions: Phishing. Viitattu 5.12.2011. http://www.apwg.org > resources

Transport Layer Security 2011. Wikipedia. Viitattu 5.12.2011. http://en.wikipedia.org/wiki/transport_layer_security

Url. 2011 Wikipedia. Viitattu 5.12. 2011. http://en.wikipedia.org/wiki/Url

Virtual Hosting 2011. Wikipedia. Viitattu 5.12. 2011. http://en.wikipedia.org/wiki/Virtual_hosting

X.509 2011. Wikipedia. Viitattu 5.12. 2011. http://en.wikipedia.org/wiki/X.509