Tietomurtojen ennaltaehkäisy, havaitseminen ja tutkinta

Erityisasiantuntija Antti Kurittu

Tietomurto?

- *"Meille ei ole IKINÄ tapahtunut tietomurtoa."*

"Eihän meillä ole mitään kiinnostavaa"

- **Myth 4: I don’t have any sensitive data**

  "You may not think so, but it is highly likely that you do. Passphrases, addresses, telephone numbers, credit card details, and other information is often stored in the cache of your computer. It is also easy to profile you by reading your email and examining your browsing history. This is not an uncommon approach to identity thefts among cyber criminals."

  Lähde: https://safeandsavvy.f-secure.com/2017/03/08/the-8-worst-online-security-myths/

Yritetäänkö meille muka murtautua?

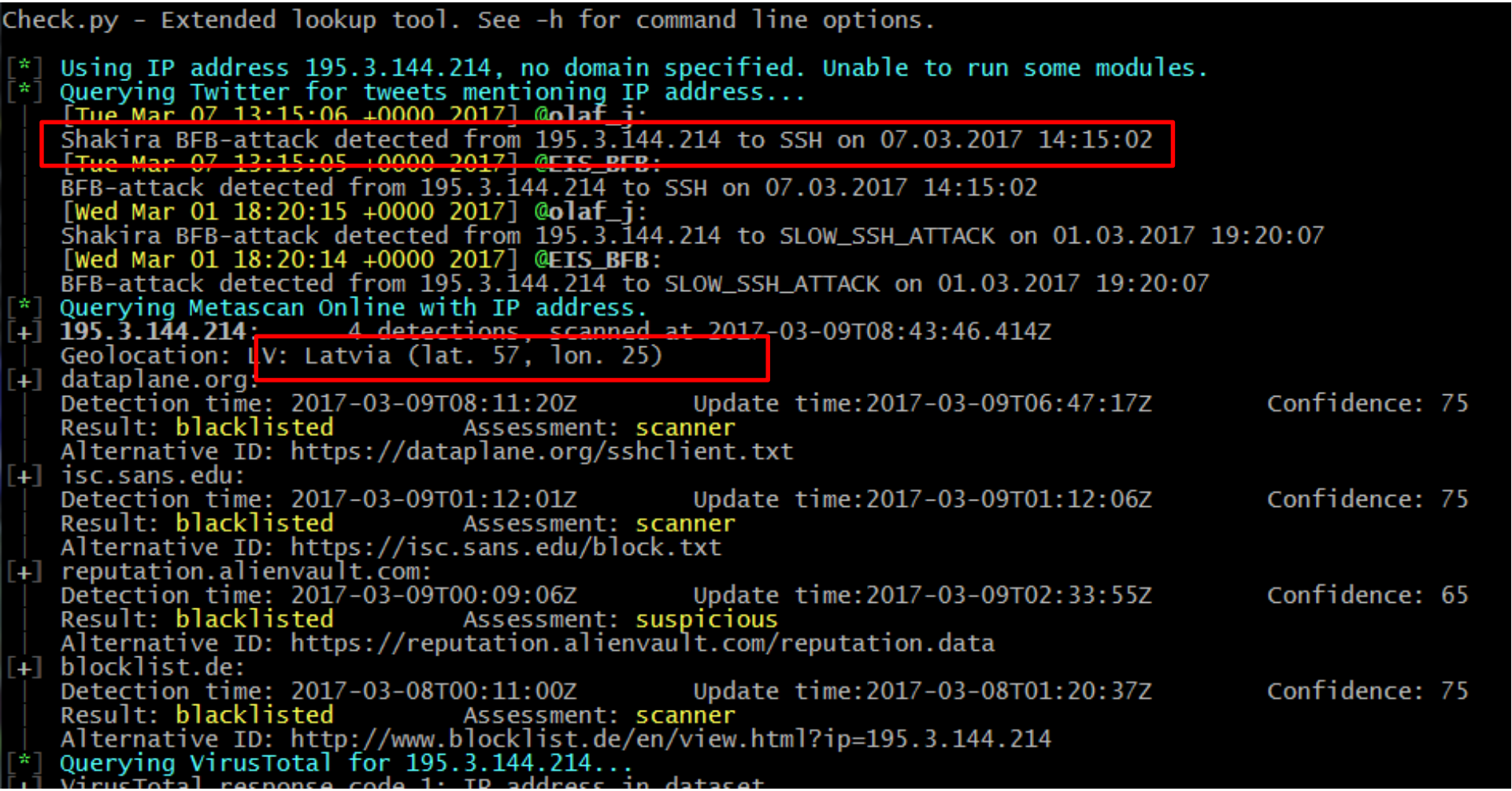
- Kyllä.

```
root@ubuntu-512mb-ams3-01:/var/log# tail -f auth.log
Mar  9 07:55:48 ubuntu-512mb-ams3-01 systemd-logind[1406]: New seat seat0.
Mar  9 07:55:48 ubuntu-512mb-ams3-01 sshd[1590]: Server listening on 0.0.0.0 port 22.
Mar  9 07:55:48 ubuntu-512mb-ams3-01 sshd[1590]: Server listening on :: port 22.
Mar  9 07:55:50 ubuntu-512mb-ams3-01 sshd[1590]: Received signal 15; terminating.
Mar  9 07:55:50 ubuntu-512mb-ams3-01 sshd[1632]: Server listening on 0.0.0.0 port 22.
Mar  9 07:55:50 ubuntu-512mb-ams3-01 sshd[1632]: Server listening on :: port 22.
Mar  9 07:55:53 ubuntu-512mb-ams3-01 sshd[1652]: Accepted publickey for root from 93.190.96.56 port 47439 ssh2: RSA SHA256:bQ5SZjO3o4
O+XBma3sIVHPqsV81I2nOaUc+KKNVCIUQ
Mar  9 07:55:53 ubuntu-512mb-ams3-01 sshd[1652]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar  9 07:55:53 ubuntu-512mb-ams3-01 systemd-logind[1406]: New session 1 of user root.
Mar  9 07:55:53 ubuntu-512mb-ams3-01 systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Mar  9 08:17:01 ubuntu-512mb-ams3-01 CRON[1762]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  9 08:17:01 ubuntu-512mb-ams3-01 CRON[1762]: pam_unix(cron:session): session closed for user root
Mar  9 08:33:18 ubuntu-512mb-ams3-01 sshd[1765]: Invalid user admin from 195.3.144.214
Mar  9 08:33:18 ubuntu-512mb-ams3-01 sshd[1765]: input_userauth_request: invalid user admin [preauth]
Mar  9 08:33:19 ubuntu-512mb-ams3-01 sshd[1765]: Connection closed by 195.3.144.214 port 51664 [preauth]
Mar  9 08:33:21 ubuntu-512mb-ams3-01 sshd[1767]: Invalid user admin from 195.3.144.214
Mar  9 08:33:21 ubuntu-512mb-ams3-01 sshd[1767]: input_userauth_request: invalid user admin [preauth]
Mar  9 08:33:22 ubuntu-512mb-ams3-01 sshd[1767]: Connection closed by 195.3.144.214 port 54906 [preauth]
Mar  9 08:33:23 ubuntu-512mb-ams3-01 sshd[1769]: Invalid user admin from 195.3.144.214
Mar  9 08:33:23 ubuntu-512mb-ams3-01 sshd[1769]: input_userauth_request: invalid user admin [preauth]
Mar  9 08:33:24 ubuntu-512mb-ams3-01 sshd[1769]: Connection closed by 195.3.144.214 port 32949 [preauth]
Mar  9 08:33:25 ubuntu-512mb-ams3-01 sshd[1771]: Invalid user admin from 195.3.144.214
Mar  9 08:33:25 ubuntu-512mb-ams3-01 sshd[1771]: input_userauth_request: invalid user admin [preauth]
Mar  9 08:33:25 ubuntu-512mb-ams3-01 sshd[1771]: Connection closed by 195.3.144.214 port 37626 [preauth]
Mar  9 08:33:26 ubuntu-512mb-ams3-01 sshd[1773]: Invalid user guest from 195.3.144.214
Mar  9 08:33:26 ubuntu-512mb-ams3-01 sshd[1773]: input_userauth_request: invalid user guest [preauth]
Mar  9 08:33:26 ubuntu-512mb-ams3-01 sshd[1773]: Connection closed by 195.3.144.214 port 40996 [preauth]
Mar  9 08:33:27 ubuntu-512mb-ams3-01 sshd[1775]: Invalid user manager from 195.3.144.214
Mar  9 08:33:27 ubuntu-512mb-ams3-01 sshd[1775]: input_userauth_request: invalid user manager [preauth]
Mar  9 08:33:27 ubuntu-512mb-ams3-01 sshd[1775]: Connection closed by 195.3.144.214 port 42308 [preauth]
Mar  9 08:33:28 ubuntu-512mb-ams3-01 sshd[1777]: Invalid user operator from 195.3.144.214
Mar  9 08:33:28 ubuntu-512mb-ams3-01 sshd[1777]: input_userauth_request: invalid user operator [preauth]
Mar  9 08:33:28 ubuntu-512mb-ams3-01 sshd[1777]: Connection closed by 195.3.144.214 port 43407 [preauth]
Mar  9 08:33:29 ubuntu-512mb-ams3-01 sshd[1779]: Connection closed by 195.3.144.214 port 46676 [preauth]
Mar  9 08:33:31 ubuntu-512mb-ams3-01 sshd[1781]: Invalid user osmc from 195.3.144.214
Mar  9 08:33:31 ubuntu-512mb-ams3-01 sshd[1781]: input_userauth_request: invalid user osmc [preauth]
Mar  9 08:33:31 ubuntu-512mb-ams3-01 sshd[1781]: Connection closed by 195.3.144.214 port 48560 [preauth]
Mar  9 08:33:33 ubuntu-512mb-ams3-01 sshd[1783]: Invalid user pi from 195.3.144.214
Mar  9 08:33:33 ubuntu-512mb-ams3-01 sshd[1783]: input_userauth_request: invalid user pi [preauth]
Mar  9 08:33:33 ubuntu-512mb-ams3-01 sshd[1783]: Connection closed by 195.3.144.214 port 53195 [preauth]
Mar  9 08:33:36 ubuntu-512mb-ams3-01 sshd[1785]: Connection closed by 195.3.144.214 port 57377 [preauth]
Mar  9 08:33:37 ubuntu-512mb-ams3-01 sshd[1787]: Connection closed by 195.3.144.214 port 33936 [preauth]
Mar  9 08:33:38 ubuntu-512mb-ams3-01 sshd[1789]: Connection closed by 195.3.144.214 port 36483 [preauth]
Mar  9 08:33:39 ubuntu-512mb-ams3-01 sshd[1791]: Invalid user support from 195.3.144.214
Mar  9 08:33:39 ubuntu-512mb-ams3-01 sshd[1791]: input_userauth_request: invalid user support [preauth]
Mar  9 08:33:39 ubuntu-512mb-ams3-01 sshd[1791]: Connection closed by 195.3.144.214 port 39570 [preauth]
Mar  9 08:33:40 ubuntu-512mb-ams3-01 sshd[1793]: Invalid user support from 195.3.144.214
Mar  9 08:33:40 ubuntu-512mb-ams3-01 sshd[1793]: input_userauth_request: invalid user support [preauth]
Mar  9 08:33:40 ubuntu-512mb-ams3-01 sshd[1793]: Connection closed by 195.3.144.214 port 41356 [preauth]
Mar  9 08:33:41 ubuntu-512mb-ams3-01 sshd[1795]: Invalid user tech from 195.3.144.214
Mar  9 08:33:41 ubuntu-512mb-ams3-01 sshd[1795]: input_userauth_request: invalid user tech [preauth]
Mar  9 08:33:41 ubuntu-512mb-ams3-01 sshd[1795]: Connection closed by 195.3.144.214 port 42734 [preauth]
Mar  9 08:33:43 ubuntu-512mb-ams3-01 sshd[1797]: Invalid user test from 195.3.144.214
Mar  9 08:33:43 ubuntu-512mb-ams3-01 sshd[1797]: input_userauth_request: invalid user test [preauth]
Mar  9 08:33:44 ubuntu-512mb-ams3-01 sshd[1797]: Connection closed by 195.3.144.214 port 44756 [preauth]
Mar  9 08:33:44 ubuntu-512mb-ams3-01 sshd[1799]: Invalid user ubnt from 195.3.144.214
Mar  9 08:33:44 ubuntu-512mb-ams3-01 sshd[1799]: input_userauth_request: invalid user ubnt [preauth]
Mar  9 08:33:44 ubuntu-512mb-ams3-01 sshd[1799]: Connection closed by 195.3.144.214 port 50363 [preauth]
```

...22 minuuttia ensimmäiseen yritykseen.

```
07:55:53 ubuntu-512mb-ams3-01 systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
08:17:01 ubuntu-512mb-ams3-01 CRON[1762]: pam_unix(cron:session): session opened for user root by (uid=0)
08:17:01 ubuntu-512mb-ams3-01 CRON[1762]: pam_unix(cron:session): session closed for user root
08:33:18 ubuntu-512mb-ams3-01 sshd[1765]: Invalid user admin from 195.3.144.214
08:33:18 ubuntu-512mb-ams3-01 sshd[1765]: input_userauth_request: invalid user admin [preauth]
08:33:19 ubuntu-512mb-ams3-01 sshd[1765]: Connection closed by 195.3.144.214 port 51664 [preauth]
08:33:21 ubuntu-512mb-ams3-01 sshd[1767]: Invalid user admin from 195.3.144.214
08:33:21 ubuntu-512mb-ams3-01 sshd[1767]: input_userauth_request: invalid user admin [preauth]
08:33:22 ubuntu-512mb-ams3-01 sshd[1767]: Connection closed by 195.3.144.214 port 54906 [preauth]
```

```
[*] Querying spamlists for 195.3.144.214...
    IP: 195.3.144.214 IS listed in zen.spamhaus.org (127.0.0.4: "https://www.spamhaus.org/query/ip/195.3.144.214")
    IP: 195.3.144.214 is NOT listed in spam.abuse.ch
    IP: 195.3.144.214 IS listed in cbl.abuseat.org (127.0.0.2: "Blocked - see http://www.abuseat.org/lookup.cgi?ip=195.3.144.214")
    IP: 195.3.144.214 is NOT listed in virbl.dnsbl.bit.nl
    IP: 195.3.144.214 is NOT listed in dnsbl.inps.de
    IP: 195.3.144.214 is NOT listed in ix.dnsbl.manitu.net
    IP: 195.3.144.214 is NOT listed in dnsbl.sorbs.net
    IP: 195.3.144.214 is NOT listed in bl.spamcannibal.org
    IP: 195.3.144.214 is NOT listed in bl.spamcop.net
    IP: 195.3.144.214 IS listed in xbl.spamhaus.org (127.0.0.4: "https://www.spamhaus.org/query/ip/195.3.144.214")
    IP: 195.3.144.214 is NOT listed in pbl.spamhaus.org
    IP: 195.3.144.214 IS listed in dnsbl-1.uceprotect.net (127.0.0.2: "IP 195.3.144.214 is UCEPROTECT-Level 1 listed. See http://www
eck.php?ipr=195.3.144.214")
    IP: 195.3.144.214 is NOT listed in dnsbl-2.uceprotect.net
    IP: 195.3.144.214 is NOT listed in dnsbl-3.uceprotect.net
    IP: 195.3.144.214 is NOT listed in db.wpbl.info
```


Check.py - Extended lookup tool. See -h for command line options.
[*] Using IP address 195.3.144.214, no domain specified. Unable to run some modules.
[*] Querying Twitter for tweets mentioning IP address...
[Tue Mar 07 13:15:06 +0000 2017] @olaf_j:
Shakira BFB-attack detected from 195.3.144.214 to SSH on 07.03.2017 14:15:02
[Tue Mar 07 13:15:05 +0000 2017] @EIS_BFB:
BFB-attack detected from 195.3.144.214 to SSH on 07.03.2017 14:15:02
[Wed Mar 01 18:20:15 +0000 2017] @olaf_j:
Shakira BFB-attack detected from 195.3.144.214 to SLOW_SSH_ATTACK on 01.03.2017 19:20:07
[Wed Mar 01 18:20:14 +0000 2017] @EIS_BFB:
BFB-attack detected from 195.3.144.214 to SLOW_SSH_ATTACK on 01.03.2017 19:20:07
[*] Querying Metascan Online with IP address.
[+] 195.3.144.214: 4 detections, scanned at 2017-03-09T08:43:46.414Z
Geolocation: LV: Latvia (lat. 57, lon. 25)
[+] dataplane.org:
Detection time: 2017-03-09T08:11:20Z Update time:2017-03-09T06:47:17Z Confidence: 75
Result: blacklisted Assessment: scanner
Alternative ID: https://dataplane.org/sshclient.txt
[+] isc.sans.edu:
Detection time: 2017-03-09T01:12:01Z Update time:2017-03-09T01:12:06Z Confidence: 75
Result: blacklisted Assessment: scanner
Alternative ID: https://isc.sans.edu/block.txt
[+] reputation.alienvault.com:
Detection time: 2017-03-09T00:09:06Z Update time:2017-03-09T02:33:55Z Confidence: 65
Result: blacklisted Assessment: suspicious
Alternative ID: https://reputation.alienvault.com/reputation.data
[+] blocklist.de:
Detection time: 2017-03-08T00:11:00Z Update time:2017-03-08T01:20:37Z Confidence: 75
Result: blacklisted Assessment: scanner
Alternative ID: http://www.blocklist.de/en/view.html?ip=195.3.144.214
[*] Querying VirusTotal for 195.3.144.214...

Tietotekniikkarikokset rikoslaissa

- Rikoslaki 38 luku (21.4.1995/578)
  Tieto- ja viestintärikoksista
  - » 3 § (10.4.2015/368) Viestintäsalaisuuden loukkaus
  - » 5 § (21.4.1995/578) Tietoliikenteen häirintä
  - » 7 a § (10.4.2015/368) Tietojärjestelmän häirintä
  - » 8 § (10.4.2015/368) Tietomurto
  - » 9 a § (10.4.2015/368) Identiteettivarkaus
- 35 luku (24.8.1990/769) Vahingonteosta
  - » 3 a § (10.4.2015/368) Datavahingonteko
- Myös muissa luvuissa sovellettavia pykäliä.
  - » 7 § (24.8.1990/769) Luvaton käyttö
- Tietotekniikkarikos-luokiteltuja juttuja 2010-2017 yhteensä 2245 kpl (Poliisi)

5 § (21.4.1995/578) Tietoliikenteen häirintä

Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava. (11.5.2007/540)

8 § (10.4.2015/368) Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta

1) teknisen erikoislaitteen avulla tai

2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

Esimerkki

- Olavi kirjautuu tyttöystävänsä Jaanan Facebook-tilille tunnuksilla, jotka ovat hänen tiedossaan. Olavi lukee Jaanan ja tämän miespuolisten ystävien välisiä viestejä. Olavi kirjoittaa Jaanan nimissä miehille viestejä.
  - » Tietomurto
  - » Viestintäsalaisuuden loukkaus
  - » Identiteettivarkaus?
    - Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.

Esimerkki

- Keijo ja Jonne löytävät verkkosivustolta SQL-injektiohaavoittuvuuden, jonka avulla saavat haltuunsa verkkosivuston rekisteröityneiden käyttäjien tietokantataulun.
  - » Tietomurto vai petos?
  - » "Syyttäjä katsoo miehen toiminnan täyttävän niin sanotun tietojenkäsittelypetoksen tunnusmerkistön. Tekoaikaan vuosina 2011-13 toiminta ei kuitenkaan syyttäjän näkemyksen mukaan täyttänyt tietomurron tunnusmerkistöä."

    Lähde: http://www.iltalehti.fi/digi/20170112220005259 7_du.shtml

Esimerkki

- Urho perustaa uuden yrityksen, mutta seuraa uudessa yrityksessä vielä vanhan firmansa sähköpostia.
  - » Tietomurto
  - » Petos
  - » Viestintäsalaisuuden loukkaus

Onko porttiskannaus rikos?

- Virallinen syyttäjä vaati A:lle rangaistusta tietomurron yrityksestä seuraavasti:
- A oli 23.11.1998 Helsingissä yrittänyt murtaa turvajärjestelyn tunkeutuakseen oikeudettomasti Osuuspankkikeskus-OPK osuuskunnan tietojärjestelmään.
- A oli suorittanut niin sanotun porttiskannauksen eli erityistä tietokoneohjelmaa käyttämällä skannannut läpi osuuskunnan internetiin yhteydessä olevan verkon kaikki osoitteet tarkoituksin löytää avoimia välityspalvelimia. Skannaus ei ollut läpäissyt osuuskunnan tietojärjestelmän palomuuria. Mikäli A olisi löytänyt avoimen välityspalvelun, hän olisi sitä kautta kyennyt saamaan jatkoyhteyden internetiin niin, että yhteys olisi näyttänyt tulleen tästä välityspalvelimesta.

Onko porttiskannaus rikos?

- Hovioikeus katsoi selvitetyksi, että A oli syyllistynyt siihen tietomurron yritykseen, josta hänelle oli vaadittu rangaistusta. Perusteluinaan hovioikeus lausui seuraavan:
- Syytteessä oli kuvattu teko, jossa tekijä oli pyrkinyt selvittämään mahdollisuutta tunkeutua suojattuun tietojärjestelmään, ja edelleen oli kuvattu se, että tekijä olisi tunkeutunut tietojärjestelmään, jos mahdollisuus olisi löytynyt. Tässä tapauksessa teko oli jäänyt siihen, ettei tuollaista mahdollisuutta ollut löytynyt. Syytteessä mainittu porttiskannaus ja siihen liittyvä tekijän tarkoitus tunkeutua suojattuun järjestelmään tilaisuuden löytyessä oli tietomurron yritys.

Lähde: http://www.fredman-mansson.fi/fi/henkilosto/markku-fredman/kirjoituksia/194-tietomurto

Onko porttiskannaus rikos?

- Porttiskannaus on toimenpide, jonka avulla pyritään selvittämään tietojärjestelmän eri tietoliikenneporteissa toimivia ohjelmia ja käyttöjärjestelmiä sekä niiden haavoittuvuutta. Tavanomaisesti porttiskannaus suoritetaan käyttäen hyväksi tätä varten laadittua ohjelmaa, joka voi - käytetystä ohjelmasta riippuen - esimerkiksi palauttaa raportin skannauksen kohteena olevasta koneesta, sen tietoliikenneporteista, ohjelmistoista ja niiden tiedetyistä tietoturva-aukoista. Porttiskannausohjelmaa voidaan käyttää luvallisessa tarkoituksessa esimerkiksi tietojärjestelmän turvallisuusjärjestelyjen selvittämiseen.

Onko porttiskannaus rikos?

- Porttiskannausohjelmalla on näin ollen mahdollista järjestelmällisesti selvittää tietojärjestelmän mahdollisia aukkoja ja sen heikkoja kohtia. Toimenpiteen avulla kyetään saamaan tietoja, jotka mahdollistavat myös luvattoman pääsyn kohteena olevaan järjestelmään. Ohjelmaa käyttämällä hankitun tiedon avulla voidaan siten laissa tarkoitetuin tavoin murtaa tietojärjestelmän turvajärjestely. Kuten lain esitöissä todetaan jo se, että yrittää hankkia tällaisen luvattoman pääsyn järjestelmään mahdollistavan tiedon, on rangaistavaa, jos se tehdään tarkoituksella oikeudettomasti tunkeutua tietojärjestelmään.

Onko porttiskannaus rikos?

- Riippuu siis käyttötarkoituksesta
- Viestintävirasto skannaa portteja...
  - » Tietoturvaperuste
  - » Haavoittuvuuksien löytäminen niistä tiedottamiseksi
  - » Perusteltu, lainmukainen käyttötarkoitus
- Työkalu ei itsessään ole laiton, mutta työkalua voi käyttää laittomasti.

Oikeudenkäyttö on tulkinnanvaraista!

- Laki ja sen soveltaminen ei ole ohjelmakoodia
- Tutkinta ja tuomio riippuvat monesta seikasta
- Rikollinen teko edellyttää useimmiten rikollista tarkoitusta!

Ennaltaehkäisy

- Ajantasaiset laitteet ja ohjelmistot
- Aktiivinen ylläpito ja valvonta
- Pelkkä virustorjunta ja palomuuri eivät riitä
- Työkaluja:
  - » Lokien hallinta
  - » Intrusion Detection System (IDS)
  - » Honeypotit
  - » Netflow-loki
  - » White / blacklist
    - Applikaatiot, IP-osoitteet

Sopiva teknisen suojautumisen taso

- Riittävä teknisen suojautumisen taso on määritettävä verkon käyttäjien ja käyttötarkoituksen mukaan
- Käsiteltävän tiedon laatu ja luonne asettaa vaadittavan suojaustason ja suojauksen toteutuksen kriteerit
- Tietoturva ei ole ohjelmistotuote, vaan tapa toimia
- Reunasuojaus ei riitä

Inhimillinen suojautuminen tärkeintä

- Vaikka lukko on hyvä, se ei auta jos käyttäjä avaa sen vapaaehtoisesti
  - » Phishing
  - » Spearphishing
- Haittaohjelmat
- Fyysiset hyökkäykset
  - » BadUSB, USB Killer, keyloggerit, USB-tikut
- "*In order to break into the American military's network - which was classified and not connected to the public internet - the Russians planted bugged thumb drives in kiosks near NATO headquarters in Kabul, hoping that an American serviceman or woman would buy a drive and plug it into a secure computer. It worked.*"

  Lähde: http://nordic.businessinsider.com/russia-planted-bugged-thumb-drives-to-break-into-us-govt-computers-2017-3?r=US&IR=T

Havaitseminen

- SOC
  - » Tunne verkkosi
  - » Valvo verkkoasi
  - » Seuraa päivityksiä
- Jaa verkko osiin
- Pelkkä lokien passiivinen kerääminen ei riitä
- Computer Security Incident Response Team
  - » Käsittelyä syytä harjoitella
  - » Kuka tekee päätökset? Eskalaatio?
  - » Kenen puoleen käännytään, kun hätä iskee?
- Ulkopuoliset tietolähteet

Tietomurron sattuessa

- Älä tuhoa todisteita!
- Pidä tietokoneet käynnissä
  - » Muistijälki haittaohjelmasta
  - » Live-forensiikka
  - » Verkkoyhteys irti tilanteen mukaan
- Ota oikeat lokitiedot talteen
- Varmuuskopioi todistusaineisto, jos mahdollista
  - » Levykuva
- Jos kotiin murtaudutaan, älä siivoa nurkkia!

Tietomurron sattuessa

- Ilmoita Kyberturvallisuuskeskukselle
- Tee rikosilmoitus paikallispoliisille
  - » Rikosilmoituksen voi tehdä henkilö, jolla on yrityksen nimenkirjoitusoikeus
  - » Nimeä yhteyshenkilö, joka voi toimia asianomistajan edustajana
  - » Ota yhteyttä juristiin
  - » Nimeä tekniset asiantuntijat todistajiksi
- Harkitse, tarvitsetko ulkopuolista incident response-apua
  - » Nopeuttaa ja helpottaa tutkintaa

Tietomurron sattuessa

- Varaudu tutkinta-ajan venymiseen
- Kyberturvallisuuskeskus voi auttaa tilanteen arvioinnissa ja eskaloinnissa poliisin suuntaan
- Älä murehdi rikosnimikkeestä, poliisi arpoo sopivan tutkintanimikkeen
- Nimike voi muuttua tutkinnan ja oikeusprosessin aikana
- Tee rikosilmoitus, vaikka et tietäisikään tekijää tai uskoisi kiinnijäämiseen.

Tietomurron sattuessa

- Poliisi kerää tietoa useista lähteistä
- Ilmoitus voi sisältää tärkeän palasen kokonaisuutta, josta organisaatio ei ole tietoinen
- Kaikki tieto on arvokasta
- Piilorikollisuus ei tue poliisin työtä eikä näy resursseissa

Alihankinta

- Sopimusasiat kuntoon!
  - » Suostuuko alihankkija luovuttamaan lokeja?
  - » Onko lokeissa myös muiden asiakkaiden tietoja?
    - Käsittelystä ja siivoamisesta viivettä
  - » Helpointa, jos asiakas noutaa lokit ja toimittaa poliisille
  - » Poliisin pyytäessä lokeja suoraan toimittajalta saatetaan tarvita televalvontalupa

Rikosprosessi

- Esitutkinta
  - » Esitutkintaviranomainen, yleensä poliisi
- Syyteharkinta
  - » Syyttäjä
- Oikeudenkäynti
  - » Käräjäoikeus, hovioikeus, korkein oikeus
- Tuomio
  - » Lainvoimaisuus
- Rikosseuraamus

Poliisin toiminta

- Tekninen tutkinta
  - » Forensiikka
- Taktinen tutkinta
  - » Kotietsintä
  - » Kuulustelu
  - » Kiinniotto
  - » Muut pakkokeinot
- Kansainvälinen yhteistyö
  - » Oikeusapu vieraan valtion viranomaisille
  - » Yhteistyö muiden viranomaisten kanssa
    - Kansallisesti ja kansainvälisesti

Nuori mies myönsi petoskäräjillä vieneensä salasanoja ja käyttäjätunnuksia lukuisilta verkkosivuilta

Torstai 12.1.2017 klo 09.56 (päivitetty klo 16.54)

Syyttäjä vaatii Helsingin käräjäoikeudessa nuorelle miehelle noin vuoden ehdollista vankeutta laajassa petosjutussa. Kansankielellä kyse on tietomurtojutusta.

Nuorta miestä syytetään petoksista sekä petoksista ja petoksen yrityksistä nuorena henkilönä. Hän myöntää syytteet oikeiksi.

Suomalaismies myöntää saaneensa käsiinsä huomattavan määrän käyttäjätietoja erilaisilta verkkosivustoilta. Syytekohtia on yhteensä 33. Valtaosan aikaan hän on ollut alle 18-vuotias.

Syyttäjän mukaan syytetty on tavoitellut taloudellista hyötyä tai toiminut vahingoittamistarkoituksessa.

LUE MYÖS

Nuorelle miehelle neljän tonnin sakot satojentuhansien tunnusten hakkeroinnista - kohteina muun muassa Riemurasia ja Wilma

Suomalaista epäillään valtavasta tietomurrosta – kaappasi 3500 tietokonetta, hyökkäyksiä myös ministeriöihin

RIKOS | JULKAISTU 05.08.2016 11:48 (PÄIVITETTY 05.08.2016 12:27)

Lehtikuva

Poliisi epäilee parikymppistä miestä valtavasta tietomurrosta. Poliisi kertoo STT:lle, että miestä epäillään 3500 tietokoneen kaappaamisesta Youtubessa olleen linkin kautta.

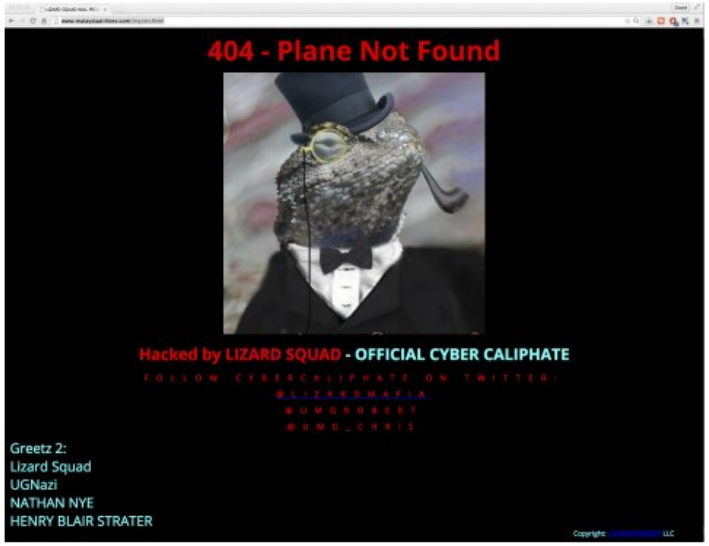
A 17-year-old has been convicted of 50,700 charges related to Lizard Squad's notorious hacks

Cale Guthrie Weissman
Jul. 7, 2015, 3:29 PM 17,216

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

A 17 year old by the name of Julius "zeekill" Kivimaki has been convicted of 50,700 computer crimes charges in relation to a series of hacks committed by the infamous computer hacking gang Lizard Squad.

The teen was given a two-year suspended prison sentence and ordered to fight cybercrime, reports the Daily Dot, citing Finnish newspaper Kaleva.



A screen grab of the official website of national carrier Malaysia Airlines after it was hacked on January 26, 2015 by a group calling itself the "Official Cyber Caliphate". REUTERS/Handout

Lizard Squad has taken credit for a slew of big hacks over the last few years, including a massive distributed denial-of-service (DDoS) attack on the PlayStation and Xbox networks, as well as a reported assault on the anonymizing communication service Tor.

Helsingin syyttäjänviraston tiedote: Syyteharkinta ns. Tekesin tietomurtoa koskevassa asiassa on valmistunut

Julkaistu 18.11.2016

Helsingin kihlakunnansyyttäjä Kukka-Maaria Kankaala on tehnyt kolme samansisältöistä syyttämättäjättämispäätöstä ns. Tekesin tietomurtoa koskevassa rikosepäilyssä, joka koski törkeää petosta ja viestintäsalaisuuden loukkausta (5500/R/12692/15). Päätökset on tehty ei näyttöä -perusteella.

Rikoksesta epäiltyinä on ollut kolme mieshenkilöä. Heitä on esitutkinnassa kuultu epäiltyinä törkeästä petoksesta ja viestintäsalaisuuden loukkauksesta. Esitutkinnan alussa epäiltynä rikosnimikkeenä on ollut myös tietomurto. Rikoksesta epäillyt ovat kiistäneet syyllistyneensä asiassa rikokseen.

HELSINGIN poliisi epäilee Tullin pääjohtajaa **Antti Hartikaista** viestintäsalaisuuden loukkaamisesta ja virkavelvollisuuden rikkomisesta. Hartikainen kiistää rikosepäilyt.

”Tehty rikosilmoitus perustuu virheellisiin olettamuksiin ja on siten täysin aiheeton. Toivottavasti totuus asiassa voidaan tuoda julki mahdollisimman pian. Harmi, kun viranomaisten aikaa hukataan tällaiseen turhaan työhön”, Hartikainen kirjoittaa lähettämässään sähköpostiviestissä.

Helsingin Sanomien kahdesta eri lähteestä hankkiman tiedon mukaan asian ytimessä on pääjohtajan väärälle vastaanottajalle vahingossa lähettämä sähköposti. Vahingossa viestin vastaanottanut on merkittävässä asemassa Tullissa.

Yhteenveto

- Pidä verkkosi terveenä ja tunne se
- Tiedä, mitä tietoa käsittelet
- Jos rikosvahinko sattuu, älä tuhoa todistusaineistoa
- Tee tapahtuneesta heti rikosilmoitus
- Poliisi ja Kyberturvallisuuskeskus auttavat tapauksen selvittämisessä
- Maksat jo viranomaispalveluista, joten niitä kannattaa käyttää