****Check Pointin haittaohjelmakatsaus 1/2017****

Vieras menneisyydestä: Slammer teki yllätyspaluun

*Tietoturvayhtiö Check Pointin joulukuun havainnot yllättävät. Suomen yleisin haittaohjelma ei enää ollutkaan nokkela kiristäjä Locky, vaan yksinkertainen Slammer-mato, muisto vuodelta 2003.*

**Espoo, 19. tammikuuta 2017 –** Check Point Software Technologies julkistaa kuukausittain listan maailman ja Suomen yleisimmistä haittaohjelmista. Slammer SQL nousi yllättäen joulukuun kansainvälisen listan kolmanneksi ja Suomen listan kärkeen. Kaikkiaan mato aiheutti neljä prosenttia haittaohjelmaliikenteestä kansainvälisesti.

”Slammerin paluu kertoo, etteivät kyberrikolliset ole luopuneet vanhoista aseistaan. Kokoamamme data viittaa siihen, että matoa on käytetty tunnustelumielessä, suojaamattomien laitteiden löytämiseksi. Microsoft on paikannut aukon, jota mato hyödyntää, joten sen aiheuttama tietoturvariski on pieni. Se, millaista tuhoa tällaiset vanhat hyökkäysmenetelmät saavat aikaan, riippuu täysin siitä, miten valveutuneita käyttäjät ovat. Päivitykset kannattaa aina ladata ajallaan”, kommentoi Managed Security Service Team Leader **Michelle Levy** Check Pointilta.

Vuonna 2003 Slammer kaatoi viisi internetin juurinimipalvelinta, teki pankkiautomaateista toimintakyvyttömiä Yhdysvalloissa ja levisi jopa ydinvoimalan tietojärjestelmään. Mato ei vaadi lunnaita eikä varasta tietoja, vaan sen tehokkuus perustuu nopeaan leviämiseen. Levitessään Slammer luo niin paljon tietoliikennettä, että verkko hidastuu.

Kansainvälisesti loppuvuoden Slammer-liikenne kohdistui etenkin yhdysvaltalaisiin ja israelilaisiin palvelimiin. Liikenne oli lähtöisin pääasiassa Kiinasta, Vietnamista, Meksikosta ja Ukrainasta.

Haittaohjelmia oli joulukuussa liikkeellä 8 prosenttia tavallista vähemmän koko maailmassa. Osa Locky-kiristyshaittaohjelman levittäjistä oli oletettavasti lomalla, sillä Locky-hyökkäyksiä saatiin kiinni 81 prosenttia vähemmän kuin loka- ja marraskuussa. Locky hallitsi listoja koko syksyn, mutta nyt se putosi pois kansainvälisestä kärkikymmeniköstä.

**Yleisimmät haittaohjelmat joulukuussa top 10, Suomi**

1. Slammer

2. Nivdort

3. Cryptowall

4. Rookie UA

5. Kelihos/Hlux

6. Locky

7. Nemucod

8. Tinba

9. HackerDefender

10. Bancos

**Yleisimmät haittaohjelmat joulukuussa top 3, koko maailma**

1. Conficker

2. Nemucod

3. Slammer

**Yleisimmät mobiililatteiden haittaohjelmat joulukuussa top 3, koko maailma**

1. HummingBad

2. Triada

3. Ztorg

--

Kuukausittain laadittava haittaohjelmatilasto perustuu Check pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Check Pointin uhkakartta näyttää kyberhyökkäykset reaaliaikaisesti: [ThreatCloud World Cyber Threat Map](https://www.threat-cloud.com/ThreatPortal/#/map)

Katso täältä, kun haluat tietää, mitä mikäkin haittaohjelma tekee: [Check Point ThreatWiki](https://threatwiki.checkpoint.com/threatwiki/public.htm)

Tietoja Check Pointin uhkientorjuntaresursseista: [Threat-prevention-resources](http://www.checkpoint.com/threat-prevention-resources/index.html)

Check Pointin tietoturvatiimin blogi: [Check Point Blog](http://blog.checkpoint.com)

**Lisätiedot ja haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, maija.rauha@osg.fi, p. 0400 630 065

Seuraa Check Pointia:

Check Pointin blogi: <http://blog.checkpoint.com/>

Twitter: [www.twitter.com/checkpointsw](http://www.twitter.com/checkpointsw)

Facebook: <https://www.facebook.com/checkpointsoftware>

YouTube: <http://www.youtube.com/user/CPGlobal>

**Check Point Software Technologies Ltd.**
Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin yksinomaan kyberturvallisuustuotteisiin keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, joiden kyky havaita haittaohjelmat ja muut tunkeutujat sekä suojata asiakkaat kyberhyökkäyksiltä on ainutlaatuisen tehokas. Check Pointin täydellisen kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava sekä intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.