Check Pointin tietoturvaraportti 2015: Kohdistetut hyökkäykset ovat suurin vaara

Tietoturvayhtiö Check Pointin raportti näyttää yritysten tietoturvan pahimmat kipupisteet. Vaikka vanhojen ja muunneltujen virusten määrä on kasvanut eksponentiaalisesti, vaarallisimpia ovat mobiililaitteisiin ja yritysverkkoihin kohdistetut, räätälöidyt zero day -hyökkäykset.

Espoo, 3. kesäkuuta 2015 – Check Pointin kolmas vuosittainen tietoturvan uhkia kautta maailman luotaava 2015 Security Report on ilmestynyt. Raportti perustuu Check Pointin viime vuoden aikana kautta maailman yrityksestä ja organisaatiosta keräämiin tietoihin, ja siihen sisältyy tietoja 21 suomalaisesta lähteestä. Raporttia varten analysoitiin 300 000 tuntia tietoliikennettä. Mukana oli yli 16 000 tietoturvalaitetta ja yli miljoona älypuhelinta.

Viime vuosi oli Check Pointin mittausten mukaan tietoturvaloukkausten huippuvuosi – jälleen kerran.

– Yritysten toiminnan tehostaminen ja tietoturvariskit kulkevat usein käsi kädessä. Tietoturvasta ei aina huolehdita riittävästi, kun uusia teknisiä ratkaisuja otetaan käyttöön. Yksi vaaranpaikka on virtualisointi eli toimintojen ja palvelujen siirtäminen verkon yli tapahtuviksi. Myös tietojen liikkuminen henkilöstön mobiililaitteissa kaikkialle muodostaa riskin, toteaa Check Point Software Technologiesin Suomen maajohtaja **Petri Sonkeri.**

– Samaan aikaan virusten muuntelusta on tullut entistäkin helpompaa ja hakkerit kokevat tietoturvan haasteena. Fiksut ja armottomat kyberkriminaalit väijyvät verkon heikkouksia ja pyrkivät kiertämään tielleen asetetut esteet vaivojaan säästämättä, Sonkeri jatkaa.

Uusien tekniikoiden mukanaan tuomia riskejä voi hallita ajantasaisen tiedon ja vankkojen tietoturvaratkaisujen yhdistelmällä. Suojautuminen edellyttää kuitenkin, että tietoturvahyökkäysten muodostamat riskit ymmärretään organisaatiossa.

Uusia ja vanhoja haittaohjelmia enemmän kuin koskaan

Muunneltuja, tunnistamattomaksi tehtyjä haittaohjelmia pyrki yritysverkkoihin vuonna 2014 keskimäärin 106 kappaletta tunnissa, 48 kertaa useammin kuin edellisvuonna, jolloin vastaava luku oli 2,2 virusta tunnissa. Muunneltujen virusten määrän kasvu oli 71 %.

Vielä pahempia kuin muunnellut virukset ovat zero day -haittaohjelmat, jotka on alusta asti räätälöity hyödyntämään haavoittuvuuksia, joita ei ole vielä paikattu. Näitä on liikkeellä vähemmän kuin muunneltuja viruksia, koska niiden valmistaminen on hitaampaa ja kalliimpaa. Ne ovat kuitenkin tyypillisesti tarkasti kohdennettuja, ja onnistuessaan ne voivat tehdä suurta tuhoa. Kohdistettuja hyökkäyksiä voidaan tehdä niin mobiililaitteisiin kuin yritysverkkoihinkin. Vain yksi prosentti yrityksistä käytti zero day -hyökkäyksiltä suojaavaa teknologiaa.

Kyberrikolliset kiihdyttivät vanhojen ja uusien haittaohjelmien jakelua bottien avulla. 83 prosentissa tutkituista yrityksistä oli parhaillaan bottitartunta. Botit olivat jatkuvassa yhteydessä ohjaus- ja komentopalvelimensa kanssa. 47 prosenttia boteista onnistui toimimaan yli neljä viikkoa ennen kun ne havaittiin. Botit kommunikoivat aiempaa useammin yritysverkon ulkopuolelle, kasvu yhteydenpidossa lähes 70 %.

41 prosentissa yrityksessä ladattiin vähintään yksi tuntemattoman tartunnan omaava tiedosto yritysverkkoon tutkimusaikana. Yli puolet (52 %) saastuneista tiedostoista oli PDF-muotoisia. Office-tiedostoja oli kolme prosenttia.

Yritysverkossa tapahtuu:

- **Joka 24. sekunti** joku ottaa yritysverkosta yhteyden vihamieliseen verkkosivuun
- **Joka 34. sekunti** joku lataa yritysverkkoon ennestään tuntemattoman haittaohjelman

- **Joka minuutti** yritysverkkoon päässyt botti ottaa yhteyden lähettäjätahoon
- **Joka 5. minuutti** joku käyttää turvattomaksi tiedettyä sovellusta
- **Joka 6. minuutti** tunnettu haittaohjelma ladataan verkkoon
- **Joka 36. minuutti** arkaluontoista tietoa lähtee organisaation ulkopuolelle

Raportissa lisäksi:

- Yleisimmät bottiperheet, hyökkäysmäärät ja mihin ne pystyvät. Ehdottomasti yleisimpiä olivat viime vuonna Zeus-perheen haittaohjelmat. (s. 20)
- Yleisimmät hyökkäystyypit ja niiden määrän kehitys Yleisimpiä olivat DDoS-hyökkäykset (60 prosentissa yrityksistä, edellisvuonna 23 prosentissa). DDos-hyökkäyksiä viime vuonna 48 vuorokautta kohti. (s. 22)
- Haavoittuvimmat ohjelmistot valmistajan mukaan. Johtopaikkaa piti IBM. (s.25)
- Yleisimmät yritysten päätelaitteisiin liittyvät tietoturvariskit, yleisimpänä Bluetooth-yhdistetyt laitteet. (s. 20)
- Mobiililaitteiden tietoturvariskit: 44 prosentissa yrityksistä ei valvota mitenkään yritysdataa, joka on henkilöstön omilla laitteilla. 33 prosenttia sovelluskehittäjistä ei turvatestaa ohjelmistojaan. (s.34)
- Yrityksissä yleisimmin käytössä olevat, tietoturvan kannalta epäilyttävät ohjelmistot ja palvelut. Nousua niiden käytössä 10 % edellisvuodesta. (s.45)
- Yleisimmin vuodetut tiedot tietotyypeittäin. Toiseksi yleisin tyyppi olivat luottokorttitiedot. (s. 50)

Grafiikat ylläolevista:
OS/G Viestintä, Maija Rauha, p. 0400 630 065, maija.rauha@osg.fi

Lisätietoja Suomen tilanteesta:

Check Point Software Technologies, maajohtaja Petri Sonkeri, p. 040 5047843, petris@checkpoint.com

Raportin tausta:
Check Point keräsi Security Reportin tiedot kolmesta lähteestä. Mukana ovat yli 1 300 yrityksessä tehtyjen tietoturvaseurantojen tulokset, 16 000 eri organisaatiosta tietoja keräävään, maailmanlaajuisen Check Point ThreatCloud™ -palvelun tiedot sekä tiedot yli 3 000 tietoturvalaitteelta, jotka välittävät tietonsa Check Point Threat Emulation Cloud -pilvipalveluun. Älypuhelimia oli seurannassa yli miljoona.

Alkuperäinen raportti: 2015 Security Report

Seuraa Check Pointia:
Check Pointin blogi: http://blog.checkpoint.com/
Twitter: 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) on maailman suurin yksinomaan tietoturvaan keskittynyt yhtiö. Se on alan edelläkävijä ratkaisuillaan, jotka torjuvat asiakkaisiin kohdistuvat kyberhyökkäykset havaiten haittaohjelmat ja muut tunkeutujat ainutlaatuisen tehokkaasti. Check Pointin täydellinen tietoturva-arkkitehtuuri suojaa yritysverkot mobiililaitteisiin asti, ja sen ratkaisuja ohjataan kattavan ja intuitiivisen hallintajärjestelmän kautta. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta. At Check Point, we secure the future.

