Näin hakkeri toimii – Check Point löysi kansainvälisen kyberhyökkäyskampanjan tekijän

**SAN CARLOS, CA — 15. heinäkuuta 2017.** Tietoturvayhtiö Check Point Software Technologies kertoi tänään löytäneensä henkilön, joka on noin 4 000 yritykseen ulottuneen kyberhyökkäyskampanjan takana. Kampanja näytti alun perin valtiollisesti johdetulta.

Huhtikuussa 2017 alkaneen kampanjan kohteina oli isojakin yrityksiä esimerkiksi öljy- ja kaasualalta, pankkialalta ja rakennusteollisuudesta useissa maissa. Kampanjan laajuudesta ja kohdeyhtiöistä päätellen tekijä olisi saattanut olla esimerkiksi jonkin valtion rahoittama ammattihakkereiden ryhmä. Tosiasiassa kampanjan takana oli yksittäinen, noin 25-vuotias nigerialainen, joka asuu lähellä maan pääkaupunkia. Hänen Facebook-tilinsä tunnuslause on ”Get rich or die trying” eli vapaasti käännettynä ”Rikastu tai kuole”.

Hän käytti kampanjassaan sähköpostiviestejä, jotka näyttivät siltä kuin ne tulisivat Saudi Aramcolta, joka on maailman toiseksi suurin öljyntuottaja. Kohteina oli yritysten talousosastojen työntekijöitä, joiden hakkeri halusi paljastavan yhtiön pankkitietoja tai avaavan sähköpostin liitteen, joka sisälsi haittaohjelman.

Hakkerin käyttämät haittaohjelmat olivat NetWire, kauko-ohjattava troijalainen, joka antaa hakkerille täydet oikeudet tartunnan saaneeseen koneeseen sekä näppäimistön käyttöä tallentava Hawkeye. Hyökkäykset johtivat haittaohjelmatartuntaan 14 tapauksessa, ja hakkerin saama rahallinen hyöty lasketaan tuhansissa dollareissa.

”Vaikka hakkerin käyttämät sähköpostit olivat laadultaan huonoja ja haittaohjelmat helposti verkosta löytyviä, hän onnistui ulottamaan hyökkäyksensä tuhansiin yhtiöihin ja murtamaan useiden suojaukset. Tässä nähdään, miten helposti suhteellisen osaamatonkin hakkeri pystyy toimeenpanemaan laajan ja tehokkaan kampanjan, kommentoi Check Pointin tietoturvatutkijoiden ryhmää johtava **Maya Horowitz**.

”Tapaus tuo esiin, miten tärkeää organisaatioiden on parantaa tietoturvaansa siten, että se kattaa myös kalastelun ja toimitusjohtajahuijaukset variantteineen. Henkilöstö tulee kouluttaa valppauteen sähköpostien suhteen, vaikka ne näyttäisivätkin tulevan tutuilta lähettäjiltä”, Horowitz jatkaa.

Check Pointin tutkijaryhmä on kertonut tietonsa tapauksesta kansainvälisille ja Nigerian viranomaisille.

Yritysten sisäistä viestintää matkivat huijaussähköpostit (Business Email Compromise, BEC) ovat yleistyneet dramaattisesti 18 viime kuukauden aikana. [FBI raportoi](https://www.ic3.gov/media/2016/160614.aspx) 270 prosentin nousun uhrien määrässä vuoden 2016 alusta lukien. Uhrien taloudelliset menetykset ovat olleet keskimäärin 50 000 dollaria.

Check Pointin  [Anti-Spam & Email Security Software Blade](https://www.checkpoint.com/products/anti-spam-email-security-software-blade/) -ohjelmisto suojaa organisaatiota vastaavilta hyökkäyksiltä. Sen monitahoinen lähestymistapa suojaa sähköpostiliikenteen rakennetta, löytää roskapostit ja suojaa sähköpostilla levitettäviltä viruksilta ja muilta haittaohjelmilta. Lisäksi [SandBlast™ Agent with Zero Phishing™ -teknologia](https://www.checkpoint.com/products/endpoint-sandblast-agent/index.html) suojaa organisaatioita uusilta ja ennestään tuntemattomilta kalastelusivustoilta samoin kuin tiedostoissa ja sähköposteissa olevilta haittaohjelmilta.

Lisätietoja nigeriaishakkerista ja hänen toimintatavoistaan: <http://blog.checkpoint.com/2017/08/15/get-rich-die-trying-case-study-real-identity-behind-wave-cyberattacks-energy-mining-infrastructure-companies/>

**Lisätiedot ja haastattelupyynnöt:**

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065 (Maya Horowitzin puhelinhaastattelut)

Maajohtaja Robert Lindqvist, Check Point Software Technologies, [robertl@checkpoint.com](mailto:robertl@checkpoint.com), p. 050 368 4912

**Seuraa Check Pointia:**  
Twitter: <http://www.twitter.com/checkpointsw>Facebook: <https://www.facebook.com/checkpointsoftware>Blogi: [http://blog.checkpoint.com](http://blog.checkpoint.com/)YouTube: <http://www.youtube.com/user/CPGlobal>LinkedIn: <https://www.linkedin.com/company/check-point-software-technologies>

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yritysverkot kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.