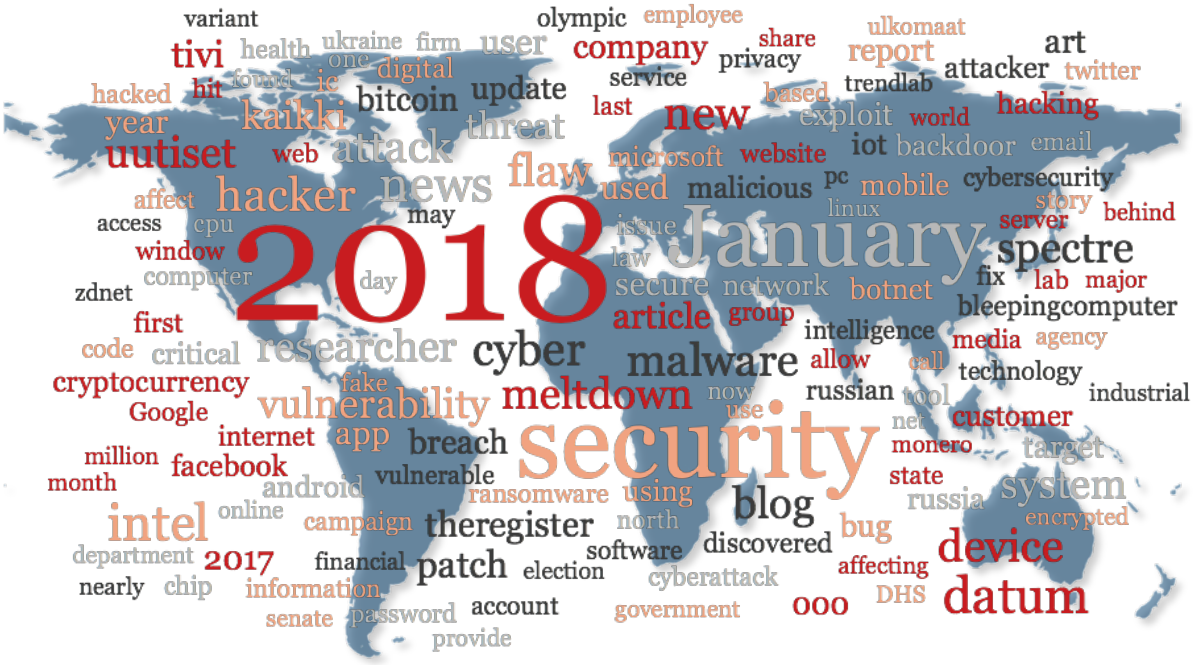
Cyberwatch-tilannekuva
Kuukausikatsaus 2018
tammikuu



1. *Suorittimien haavoittuvuudet koskevat lähes kaikkia tietokoneita ja useita älypuhelinmalleja.*
2. *2,8 miljoonan norjalaisen terveystiedot kyberiskun kohteena.*
3. *500 miljoonan dollarin arvoinen kryptovaluuttavarkaus Japanissa.*
4. *Kohdistettuja valtiollisia hyökkäyksiä Itä-Euroopan diplomaatteja kohtaan.*
5. *Olympialaiset ovat kiinnostava kohde kyberhyökkäyksille.*
6. *Yhdysvallat hyväksyi laajan verkkotiedustelulain ja suunnittelee 5G verkkojensa kansallistamista.*
7. *Pula kyberosaajista muodostaa riskin myös yrityksille.*
8. *Bottiverkot kehittyvät monimutkaisiksi vertaisverkoiksi.*
9. *Kryptovaluuttojen louhinta lisääntyy ja hakee uusi muotoja.*

Cyberwatch – trust beyond horizon

Kyber-tilannekuva - kuukausikatsaus tammikuu 2018

Vuosi 2018 alkoi lähes kaikkia tietokoneita koskevien haavoittuvuuksien **Meltdown** ja **Spectre** merkeissä. Lienevätkö nämä nykyaikaisen prosessoritekniikan turvallisuuden ytimeen kohdistuvat haavoittuvuudet esimakua sille, että digitaalisen turvallisuuden perustuksia tullaan todella ravistelemaan ja koettelemaan? Huolestuttavaa on myös kyberuhkan jatkuva laajentuminen ja muutos.

Olympialaiset ovat perinteisesti olleet hyvin poliittinen tapahtuma. Hakkerointi, tietovuodot ja vakoilu on merkittävä osa tätä poliittista peliä. Näistä olympialaista näyttäisi tulevan kaikkien aikojen kisat, ainakin kyberrintamalla.

Norjan terveystietoihin kohdistunut kohdistettu kyberhyökkäys nostaa karulla tavalla esiin keskitettyihin terveystietokantoihin kohdistuvan ja aliarvioidun riskin. Mitä riskejä ja vaikutuksia tietovuodolla oikeasti on kansalaisten ja kansallisen turvallisuuden kannalta?

Kryptovaluuttojen louhintaan käytettiin NSA:lta vuodettuja työkaluja, julkisia langattomien verkkojen tukiasemia, Android-älypuhelimia, sekä parhaillaan tätä analyysia kirjoittaessa, Lahden terveysaseman tietokoneita. Vaikuttaa, että kaikkea mitä voi käyttää kryptovaluuttojen louhintaan, myös käytetään.

Bottiverkkojen kehittyminen vertaisverkkojen suuntaan antaa viitteitä uusista uhkista lisääntyvää IoT-kehitystä ajatellen. IoT-laitteita hyödyntävät, jatkuvasti kehittyvät bottiverkot mahdollistavat palvelunestohyökkäysten lisäksi myös tietovuotoja, kryptovaluuttojen louhintaa, kiristystä ja vakoilua.

Yhdysvallat hyväksyi tiedustelulain, joka jatkaa NSA:n ja FBI:n lähes rajattomia tiedusteluoikeuksia verkossa seuraavaksi kuudeksi vuodeksi. Tämän rinnalla Suomen pitkään suunniteltu ja paljon parjattu tiedustelulaki näyttää hieman idealistiselta ja suppealta.

Useat maat parantavat kyberturvallisuuskäytänteitä tänä vuonna. Aika näyttää, kuinka tämä vaikuttaa kybertapahtumien määrään, laatuun ja tekniikkaan. Kyberrikollisuus ja valtiollinen toiminta verkossa ei ainakaan ole vähentymään päin. Globaali intensiteetti verkossa lisääntyy, joten parasta on pohtia, kuinka tähän muuttuvaan tilanteeseen tulisi itse mukautua.

- ✓ Digitaalinen ympäristö muuttuu jatkuvasti ja hakee uusia toimintamuotoja. Muuttuuko oma ajattelumme riittävästi?
- ✓ Vastaavatko yrityksen, organisaation, palveluiden ja tuotteiden nykyiset käytännöt nykyisiä ja tulevia tiedonturvaamisen tarpeita?
- ✓ Yksityisyyden suojan suuri vuosi vai vuoto?
  Mitä jos yrityksesi arkaluontoiset tiedot vuotavat?
  Mitä jos omat terveystiedot vuotavat?

Merkittävimmät Kyber-tapahtumat ja niiden merkitys

1. Suorittimien haavoittuvuudet koskevat lähes kaikkia tietokoneita ja useita älypuhelinmalleja.

Suorittimista löytynyt tekniseen arkkitehtuuriin liittyvä haavoittuvuus, joka vaikuttaa jokaiseen tietokoneeseen maailmanlaajuisesti. Löytö on merkittävä, sillä se kohdistuu yhteen keskeisemmistä turvaratkaisuista, jolla suojataan prosessorien muistinkäsittelyä. Vaikka ohjelmisto- ja laitevalmistajat saivat paikattua haavoittuvuudet ohjelmistopäivityksenä, saattavat ne hidastaa tietokoneiden suorituskykyä ollen riesana vielä useita vuosia, kunnes aikanaan tulevat korvatuksi uuden arkkitehtuurin mukaisilla laitteilla.

Merkittävä huomio jonka haavoittuvuus nostaa esiin on, että monet nykyisin käytössä olevista ratkaisuista perustuvat vuosikymmeniä vanhaan logiikkaan, joka ei välttämättä pysty vastaamaan tämän päivän haasteisiin. Ongelma ei ole ainoastaan tekninen vaan myös inhimillinen ja systeeminen. Sama haaste koskee yhtä lailla ihmisiä, yrityksiä, yhteiskunnan eri toimijoita ja valtioita, jotka yrittävät hallita ja ylläpitää vanhoja tuttuja toimintamalleja tässä jatkuvasti muuttuvassa digitaalisessa toimintaympäristössä. Digitaalinen aika vaatii digitaalisen ajan toimintamallin.

Vaikuttaa, että haavoittuvuuksia kaivetaan yhä syvemmältä arkkitehtuurin ja toimintalogiikan syövereistä. Onkin todennäköistä, että tulemme näkemään useampia vakavia nykyisten systeemien ytimeen kohdistuvia haavoittuvuuksia ja hyökkäyksiä.

2. 2,8 miljoonan norjalaisen terveystiedot kyberiskun kohteena.

Norjan potilastietojärjestelmään epäillään kohdistuneen tarkkaan kohdistettu kyberisku, joka koskee yli puolta Norjan kansalaisista. Norjan tutkimuksesta vastaavan viranomaisen mukaan isku saattaa liittyä loka-marraskuussa 2018 suunnitellun suuren NATO-harjoituksen osallistujatietojen kalasteluun. Vielä ei tiedetä kuinka laajasta vuodosta on kyse. Mikäli kyseessä on ollut NATO-harjoitukseen osallistuvien terveystietojen kalastelu, osoittaa tämä uudentyyppistä strategista ajattelua vihollisen heikkouksien löytämiseksi ja taustalla voi olla halu vaikuttaa harjoituksen kulkuun uudella tavalla. Hyökkäys voi myös olla yritys paljastaa todisteita Norjan dopingin käytöstä.

Suomen kannalta tapaus on mielenkiintoinen meneillään olevien suurten sairaala- ja terveyssektorin hankkeiden ja GDPR:n näkökulmasta. Vastaako esimerkiksi Kanta-arkiston 10 vuotta sitten suunniteltu toimintamalli tulevaisuuden tarpeita? Kyberuhka yhtä yhteiskunnan elintärkeää toimintoa kohtaa vaikuttaa yhä ilmeisemmältä.

“Kanta-arkiston riskit voivat olla hyötyjä isommat”
- Lasse Lehtonen, hallintoylilääkäri, HUS

Nyt olisi hyvä mahdollisuus tarkistaa suunniteltujen ratkaisujen uhka-arvioita ja tehdä strategisia linjauksia turvallisemman tulevaisuuden varmistamiseksi.

3. 500 miljoonan dollarin arvoinen kryptovaluuttavarkaus Japanissa.

Tapahtumahetkellä lähes puolen miljardin dollarin arvosta kryptovaluuttaa varastettiin puutteellisesti suojatusta kryptovaluuttalompakosta. Huimiin lukemiin kasvaneen kyberrikollisuuden myötä myös yritysten ja yhteiskunnan toimijoiden on syytä huomioida, että myös rikollistahoilla voi olla käytössään resursseja, joita on perinteisesti ollut vain valtiollisten toimijoiden taustalla tai sitten kyberrikolliset toimivat yhteistyössä valtiollisten toimijoiden kanssa.

On odotettavissa, että finanssisektori tulee asettamaan rajoitteita kryptovaluutoille, osin suojellakseen omaa toimialaansa, osin rajoittaakseen villinä rehottavaa kryptovaluuttakauppaa.

4. *Kohdistettuja valtiollisia hyökkäyksiä Itä-Euroopan diplomaatteja kohtaan.*

Itä-Euroopan diplomaatit ovat olleet kohdistettujen hyökkäysten kohteena. Taustalla epäillään olevan venäläistaustainen hakkeriryhmä TURLA. Toisaalta herää epäilys, että kyseessä on informaatio-operaatioon liittyvä harhautus. Hyökkäyksessä käytettiin *Adobe Flash Playerin aidolta päivitystiedostolta vaikuttavaa ohjelmistopakettia valtiollisen vakoiluohjelman välityskanavana.*

Adobe Flash Player –on jo vuosia ollut yksi haittaohjelmalevittäjien suosikeista sen laajan levinneisyyden ja suuren haavoittuvuusmäärän vuoksi. Loppukäyttäjät ovat jo niin turtuneet jatkuviin päivityksiin, että harva kiinnittää niihin enää mitään huomiota.

Tämä jatkaa ohjelmistojakeluprosessien haavoittuvuuksien hyödyntämisen trendiä. Se myös osoittaa, että hyvin suunniteltua kohdistettua hyökkäystä edes valveutuneen loppukäyttäjän on lähes mahdotonta huomata.

5. *Olympialaiset ovat kiinnostava kohde kyberhyökkäyksille.*

Olympialaisiin kohdistuneet kyberhyökkäykset ovat alkaneet hyvissä ajoin ennen itse urheilutapahtumia. Tämän vuoden olympialaisten kriittiset tietojärjestelmät on ensimmäistä kertaa toteutettu kokonaan pilvipalveluna. Etelä-Korean olympialaisten pilvipalveluita ei ainoastaan johdeta Espanjasta, vaan kaikki data sijaitsee Barcelonassa. Toimittajat näkevät saman tietojärjestelmän riippumatta siitä, ovatko paikan päällä Koreassa vai kotitoimituksen tietokoneella.

Kisoihin osallistuu paljon korkean profiilin henkilöitä ja vaikuttajia, jotka ovat otollisia kohteita tiedustelulle ja vakoilulle. Erityisen huomion kohteena on Pohjois-Korean toimet kisojen aikaan. Venäjällä saattaa myös olla halua ”iskeä takaisin” heidän doping-paljastusten ja siihen liittyvien kilpailukieltojen takia.

> ”The Olympics have always been the most politicized sporting event of them all.”
>
> - Thomas Rid, Johns Hopkins University

6. *Yhdysvallat hyväksyi laajan verkkotiedustelulain ja suunnittelee 5G verkkojensa kansallistamista.*

Yhdysvallat hyväksyi lain, joka jatkaa NSA:n ja FBI:n hyvin laajoja verkkotiedusteluoikeuksia seuraavaksi kuudeksi vuodeksi. Laki sallii seurata verkkoliikennettä, sähköposti-, tekstiviesti- ja puheluliikennettä, sekä Yhdysvaltalaisten yritysten (esim. Google, Facebook, Amazon, Microsoft) verkkoliikennetietoja. Tiedustelu kohdistuu ensisijaisesti ulkomaisiin henkilöihin tai heidän kanssaan kommunikoiviin amerikkalaisiin. Tähän tietoon on oikeus tehdä hakuja ilman erillistä lupakäytäntöä. Tietoja voi käyttää myös oikeudessa todisteena. Tämän rinnalla Suomen pitkään suunniteltu ja paljon parjattu tiedustelulaki näyttää suppeahkolta ja erittäin tarkkaan rajatulta. Suurvalloille yksityisyyden suoja näyttää olevan toissijainen asia juhlapuheista huolimatta.

Yhdysvallat etsii vaihtoehtoja turvallisen kansallisen 5G verkon rakentamiseksi. Tavoitteena mm. kiinalaisten verkkovakoiluriskin minimointi. Huoli on validi, mutta samalla ohjaa internetin globaalia toimintaa hajanaisempaan suuntaan.

Yhdysvaltojen suunnitelmat rakentaa 5G-verkko ”kotimaisin” ratkaisuin on kansallisen turvallisuuden näkökulmasta strategisesti järkevää ja periaatteessa se vähentää riskiä ulkomaisten toimijoiden, kuten kiinalaisten jalansijaa verkkovakoilun näkökulmasta. Lopulta on hieman kyseenalaista, parantaisiko se kuitenkaan käytännössä yhdysvaltalaisten turvallisuutta tietoverkoissa.

7. *Pula kyberosaajista muodostaa riskin myös yrityksille.*

Valtavasti lisääntynyt kyberrikollisuus, hakkeroinnit ja tietovuodot ovat muodostaneet pulan kyberosaajista. Kilpailu osaajista aiheuttaa henkilöstöriskejä myös niissä yrityksissä, jotka ovat onnistuneet rekrytoimaan huippuosaajia.

Jos esimerkiksi avainroolissa toimiva kyberosaaja palkataan yllättäen kilpailijalle, voi toimenkuvan täyttäminen olla haastavaa – puhumattakaan menetetystä tietotaidosta. Miten tiedonturvaamisen tarpeet muuttuvat, kun avainhenkilö poistuu palveluksesta tai vaihtuu? Onko riskiä, että kyberosaajalla edelleen pääsy organisaation järjestelmiin, jopa jälkiä jättämättä? Siksi on tärkeää luoda kyberturvallisuudesta jatkuva prosessi, joka on integroitu organisaation toimintatapaan ja kulttuuriin, niin ettei edes avainhenkilöiden puuttuminen pysty lamauttamaan organisaation toimintaa.

Toinen merkittävä haaste on kyberturvallisten ratkaisujen ostamisen osaamisessa. Jotta organisaatio osaisi ostaa turvallisen sovellusratkaisun tai palvelun, on ostajan tarkoin ymmärrettävä mitä on tilaamassa, osattava toimialakohtaiset erityistarpeet ja lakimääräiset vaatimukset, oltava hyvä käsitys käytettävissä olevista ratkaisuvaihtoehdoista, niiden vahvuuksista ja heikkouksista. Lisäksi olisi ymmärrettävä, millä turvallisuusratkaisuilla on merkitystä ja osattava arvioida eri ratkaisujen tulevaisuuden näkymiä sekä laillisuusaspekteja. Ja luonnollisesti, kuinka ratkaisu ja sen toimintamalli täyttää GDPR:n vaatimukset? Tästä tuoreena esimerkkinä, kun Helsingin seudun liikenteen (HSL) hanke ladata matkakortille arvoa netin kautta viivästyi jälleen, koska jo valittu tekniikka todettiin Suomessa laittomaksi Finanssivalvonnan toimesta tammikuussa.

8. *Bottiverkot kehittyvät monimutkaisiksi vertaisverkoiksi.*

IoT laitteita hyödyntävät, jatkuvasti kehittyvät bottiverkot mahdollistavat palvelunestohyökkäysten lisäksi myös tietovuotoja, kryptovaluuttojen louhintaa, kiristystä ja vakoilua. Vertaisverkko-mallilla toimivat ja ajoittain itsensä piilottavat “Hide ‘N Seek (HNS)” –bottiverkot antavat viitteitä uusista uhkista lisääntyvää IoT –kehitystä ajatellen. Tämä tarkoittaa käytännössä yhä laajempaa ja monipuolisempaa alustaa kyberrikollisten käyttöön. Toivottavasti viimeistään tämä kehityssuunta herättäisi laite- ja ohjelmistovalmistajat ottamaan turvallisuuskysymykset vakavasti.

9. *Kryptovaluuttojen louhinta lisääntyy ja hakee uusi muotoja.*

ADB Miner: Uusi Android –laitteita hyödyntävä bottiverkko kasvaa nopeasti. Virusmaisesti leviävä Monero –kryptovaluuttaa louhiva haittaohjelma hyödyntää tartuttamiseen Android -laitteiden ohjelmistokehitykseen tarkoitettua ominaisuutta.

Kryptovaluuttojen louhinta näyttää lisääntyvän aggressiivisesti ja hakevan uusi muotoja. Siksi on tärkeää huolehtia, että kaikkien laitteiden tietoturvapäivitykset toimivat automaattisesti ja ajallaan.

> - *“Crypto-miners steal computing resources from 20% of enterprises.*
> - *Smartphones infected with bots are the new vector for DDoS attacks.*
> - *Attacks have shifted to lateral movements in which computers infect each other.”*
>
> *- Check Point*

Cyberwatch

LÄHTEET

Tilannekuva

Kuva: https://pixabay.com/en/sochi-2014-russia-olympiad-262145/
Kuva: https://commons.wikimedia.org/wiki/File:The_Thinker_MET_100500.jpg

1. Suorittimien haavoittuvuudet koskevat lähes kaikkia tietokoneita ja useita älypuhelimia

https://meltdownattack.com
https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html
https://www.mikrobitti.fi/2018/01/intelista-alkanut-haavoittuvuus-vaikuttaa-melkein-kaikkiin-tietokoneisiin-ja-puhelimiin-tasta-on-kyse/
https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2018/haavoittuvuus-2018-001.html
https://blog.fortinet.com/2018/01/30/the-exponential-growth-of-detected-malware-targeted-at-meltdown-and-spectre
Kuva: https://www.flickr.com/photos/intel_de/9662277285

2. 2,8 miljoonan norjalaisen terveystiedot kyberiskun kohteena.

https://www.tivi.fi/Kaikki_uutiset/kyberisku-2-9-miljoonan-norjalaisen-potilastiedot-sisaltavaan-jarjestelmaan-tiedustelupalvelu-tutkii-6696551
https://www.aldrimer.no/lette-etter-pasientjournaler-og-forsvarsinfo/
https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/
http://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements
http://lasselehtonen.puheenvuoro.uusisuomi.fi/249492-hyvapahakantaarkisto

3. 500 miljoonan dollarin arvoinen kryptovaluuttavarkaus Japanissa.

Kuva: https://pixabay.com/fi/bitcoin-kolikon-sähköisen-rahan-3031818/
https://www.reuters.com/article/us-ico-ernst-young/more-than-10-percent-of-3-7-billion-raised-in-icos-has-been-stolen-ernst-young-idUSKBN1FB1MZ

4. Kohdistettuja valtiollisia hyökkäyksiä Itä-Euroopan diplomaatteja kohtaan.

https://www.welivesecurity.com/2018/01/09/turlas-backdoor-laced-flash-player-installer/
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
kuva: https://commons.wikimedia.org/wiki/File:Adobe_Flash_Player_SVG.svg

5. Olympialaiset ovat kiinnostava kohde kyberhyökkäyksille.

https://www.cyberscoop.com/fancy-bear-us-senate-winter-olympics-trend-micro-threatconnect/
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/
https://medium.com/@LanceUlanoff/2018-winter-olympic-games-may-medal-in-technology-e9eda6e2a87a
http://www.silicon.co.uk/cloud/winter-olympics-cloud-205270
https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

6. Yhdysvallat hyväksyi laajan verkkotiedustelulain ja suunnittelee 5G verkkojensa kansallistamista.

https://www.reuters.com/article/us-usa-congress-surveillance/senate-passes-bill-renewing-internet-surveillance-program-idUSKBN1F72JX
https://cdt.org/insight/section-702-what-it-is-how-it-works
https://mobile.slashdot.org/story/18/01/29/0224236/trump-team-considers-nationalizing-americas-5g-network
Kuva: https://en.wikipedia.org/wiki/Flag_of_the_United_States

7. Pula kyberosaajista muodostaa riskin myös yrityksille

https://www.darkreading.com/vulnerabilities---threats/cisos-no-1-concern-in-2018-the-talent-gap/d/d-id/1330800?
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/adb-miner/
https://www.bleepingcomputer.com/news/security/android-devices-targeted-by-new-monero-mining-botnet/
https://www.tivi.fi/Kaikki_uutiset/hsl-valitsi-tekniikan-joka-urkkii-kayttajan-verkkopankkitunnuksia-yle-pitkaan-kaivattu-palvelu-myohastyy-taas-6700307

8. Bottiverkot kehittyvät monimutkaisiksi vertaisverkoiksi.

https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-hide-n-seek-botnet-uses-peer-to-peer-infrastructure-to-compromise-iot-devices

9. Kryptovaluuttojen louhinta lisääntyy ja hakee uusi muotoja.

https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
http://www.zdnet.com/article/how-to-hack-public-wi-fi-to-mine-for-cryptocurrency/
https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/
https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html

Tilauslomake

Cyberwatch Oy Tarjoaa tilaaljille kyberturvallisuustilannekuvakatsauksia. Kuukausikatsaukset ilmestyvät kuukausittain. Ilmestymispäivä on kulloinkin edellisen kuukauden katsauksen osalta, seuraavan kuukauden toisella viikolla. Mikäli tilaaja on tilannut myös kvartaalikatsaukset, ilmestyvät kvartaalikatsaukset vastaavasti kahden viikon kuluttua edellisen kvartaalin päätymisestä. Lisäksi tilaus voi käsittää erillisiä teemakatsauksia, jotka tilataan aina yrityskohtaisesti erikseen. Tilaus on voimassa 12kk ja jatkuu automaattisesti, ellei tilausta erikseen irtisanota. Tarkemmat käyttöehdot on cyberwatch.fi-sivustolla.

Katsaukset toimitetaan suomeksi. Katsauksien engalnnikielisiä käännöksiä toimitetaan tilaajille erityispyynnöstä. Käännökset ilmestyvät keskimäärin viikon kululuttua suomenkielisen katsauksen ilmestymispäivästä.

Tilaajan tiedot	
Tilaaja organisaation nimi	
Tilaajan VAT-numero	
Tilaajan katuosoite	
Tilaajan postiosoite	
Tilaan www-sivusto	
Tilaajan yhetyshenkilön nimi	
Tilaajan yhetyshenkilön titteli	
Tilaajan yhteyshenkilön sähköposti	
Tilaajan yhteyshenkilön gsm numero	
Tilaajan katsauksien toimitussähköpostiosoite	mikäli useampia sähköpostiosoitteita, ne toimitetaan erillisellä liitteellä
Tilataan kk- katsaukset [rasti]	
Tilataan kk- katsaukset sekä kvartaalikatsaukset [rasti]	
Tilauksen päivämäärä	

Lomake voidaan lähettää täytettynä sähköpostilla: kim.waltzer@cyberwatch.fi - osoitteeseen.