Cyberwatch Finland

VIIKKOKATSAUS
VIIKKO 10/2024

”KYBERTURVALLISUUS SYNTYY PIENISTÄ TEOISTA JA KOKONAISUUDEN HALLINNASTA”

Cyberwatch Finland

KEY TAKEAWAYS

1. Venäjän sodanvastainen oppositio toimii verkossa. Toiminta on toistaiseksi keskittynyt informaatiovaikuttamiseen, vaikka myös muita keinoja olisi.

2. Kiinan kybertoiminnasta on saatu uutta tietoa. Maa hyödyntää luultua enemmän kybervakoilun ulkoistamista yksityisille toimijoille.

3. Kyberturvallisuuteen liittyvistä ilmiöistä on saatavilla paljon tilastoja. Niiden luotettavuutta heikentävät kuitenkin tulkintakysymykset ja eriävät koontitavat.

1. VERKKOULOTTUVUUDESTA SODAN VASTAISEN OPPOSITION TUKIJALKA VENÄJÄLLÄ?

Venäjällä eletään poliittisesti mielenkiintoista maaliskuuta. Merkittävimmän oppositiopoliitikko Navalnyin hautajaiset pidettiin kuun ensimmäinen päivä, presidentinvaalien odottaessa nurkan takana 15.–17. maaliskuuta. "Vaalien" tulos on jo etukäteen selvä maan oppositiotoimijoiden istuessa joko vankilassa tai ollessa maanpaossa. Samanaikaisesti lainsäädännöllä on pyritty suitsimaan informaatiotilaa. Tästä esimerkkinä ovat muun muassa epämääräiset lait nk. "valeuutisten" levittämisestä, jotka ulottuvat sosiaaliseen mediaan ja voivat johtaa jopa vuosien mittaisiin vankeusrangaistuksiin. Tästä huolimatta sosiaalinen media ja verkkoympäristö ovat sodanvastaiselle oppositiolle jo nyt merkittäviä kanavia vaikuttamiselle ja hallinnon vastustamiselle muiden keinojen ollessa vähissä. Voisiko verkkoulottuvuudesta tai kybertoiminnasta tulla sille toiminnan tukijalka?

Venäläinen oppositiotoiminta verkossa voidaan jakaa karkeasti kahteen kategoriaan: informaatiovaikuttamiseen sekä kybersabotaasiin ja siihen liittyvään kybertiedusteluun. Näistä ensimmäinen on huomattavasti jälkimmäistä yleisempää. Tunnetuimmat venäläiset oppositiopoliitikot, joihin lukeutuvat nuoremmasta sukupolvesta esimerkiksi Marija Pevtših, Kira Jarmyš ja Leonid Volkov, käyttävät taitavasti sosiaalista mediaa sisällön tuottamiseen ja jakamiseen. Merkittävimpänä alustana toimii YouTube, jota ei toistaiseksi ole Venäjällä kielletty. YouTube toimi alustana myös edesmenneelle Aleksei Navalnyille, joka tuli tunnetuksi erityisesti valtaapitävien korruptiota paljastavista videoista. Myös venäläinen oppositiomedia ja sanomalehdet elävät pääosin verkossa. Tällaisia ovat muun muassa Meduza sekä Novaya Gazeta Europa -verkkolehdet, joista molempien käyttö tosin vaatii Venäjällä VPN-yhteyttä, koska niiden käyttö maassa on estetty.

Informaatiovaikuttamisen kentällä toimii myös Yhdysvalloissa sijaitseva Vapaan Venäjän säätiö FRF (Free Russian Foundation), joka on koordinoidusti pyrkinyt niin kutsutun haltijalegioonan (Elf Legion) avulla vastaamaan venäläiseen propagandaan ja sosiaalisen median trolleihin. Tällaista työtä tekee 100 aktivistia. He ovat aktiivisia yli 900:lla Venäjän hallitusta tukevalla sosiaalisen median sivuilla ja jättävät jopa 160 000 hallitusta kritisoivaa kommenttia kuukaudessa.

Toinen kategoria eli kybersabotaasi, varsinaiset kyberhyökkäykset tai tietovuodot ovat huomattavasti harvinaisempia eikä toiminta vaikuta koordinoidulta. Yksittäisiä esimerkkejä kuitenkin löytyy. Tällainen nähtiin muun muassa Ukrainan sodan ensi viikoilla "Vulcan files" -tietovuodossa, jossa yksittäinen NTC Vulkanin työntekijä vuosi organisaation tietoja ja paljasti näin yrityksen yhteyden venäläisiin turvallisuuspalveluihin sekä tietoja muun muassa Venäjän kyberoperaatioista. Myös kybervastarintaa on nähty. Esimerkiksi Ukrainan puolesta DDoS-hyökkäyksiä tehnyt venäläinen tuomittiin maassa kolmen vuoden vankeuteen toukokuussa 2023.

Edellä kuvattujen esimerkkien valossa verkkoympäristön merkitys oppositiolle on helppo tuomita pieneksi ja opposition vaikutusmahdollisuudet olemattomiksi. Venäläinen oppositio onkin saanut kritiikkiä esimerkiksi siitä, että konkreettisen toiminnan sijaan keskitytään esimerkiksi YouTube-videoiden tekemiseen ja vlogaamiseen ulkomailta. Vaikka verkko ja sen erilaiset alustat tarjoavat oppositiolle keinon pitää yhteyttä, yhdistyä ja koordinoida toimintaa, ei pelkällä informaatiovaikuttamisella todennäköisesti saavuteta useiden toivomaa lopputulosta eli Ukrainan sodan loppumista ja vallan vaihtumista Venäjällä. Potentiaalia parempaan kuitenkin olisi. Venäjällä yhteiskunnan kriittisiä toimintoja on kytketty verkkoon. Tämä avaisi mahdollisuuden esimerkiksi sotaa vastustaville sisäpiiriläisille konkreettisen haitan aiheuttamisen tai haavoittuvuuksien vuotamisen hyökkäyksen myöhemmin toteuttavalle taholle. Myös muu Venäjä-spesifi osaaminen, joita sotaa vastustavilla venäläisillä on, voisi toimia apuna oppositiotoiminnassa. Toisaalta oppositiotoimijoiden tämänhetkinen sijainti länsimaissa mahdollistaisi muun muassa länsimaisten neuvonantajien tuen sekä kyberoperaatioiden suunnittelussa että toteuttamisessa. Fyysisen vastarinnan ollessa Venäjällä käytännössä mahdotonta, voisi kyberulottuvuudesta muodostua oppositiolle keino aktiivisemman vastarinnan toteuttamiseen.

2. TIETOVUOTO ANTOI UUTTA NÄKÖKULMAA KIINALAISESTA KYBERVAIKUTTAMISESTA

Helmikuussa tapahtunut kiinalaisen kyberturvallisuusyhtiö I-Soonin massiivinen tietovuoto tarjoaa harvinaisen näköalan kiinalaiseen kybervaikuttamisen kenttään. Vaikka vuotajaa tai vuodettujen tietojen aitoutta ei ole vielä varmistettu, pidetään vuodetun materiaalin sisältöä yleisesti todenmukaisena. Vuodetusta materiaalista käy ilmi, että Kiinan valtio kilpailuttaa kybervakoilu- ja hakkeritoimeksiantoja yksityisillä palveluntarjoajilla. Vuotaneet tiedot olivat julkaistu GitHub-verkko-ohjelmistovarastossa, jossa voi muun muassa jakaa ilmaiseksi tiedostoja kaikkien nähtäville. Tietovuodon mukaan I-Soon toimii yksityisenä kybervakoilu-urakoitsijana Kiinan turvallisuusviranomaisille. Vuodosta käy ilmi, että I-Soon on kehittänyt omia haittaohjelmiaan ja osallistunut valtion järjestämiin kybervakoiluoperaatioiden kilpailutuksiin. Yrityksen uhreina on monenkirjava joukko, johon kuuluu ulkomaisia hallituksia, korkeakouluja sekä televiestinnän, terveydenhuollon ja lentoliikenteen toimijoita eri maissa.

Nyt tapahtunut tietovuoto muuttaa käsitystä kiinalaisesta kybervakoilutoiminnasta. Aikaisemmin Kiinan on ajateltu toteuttavan pääasiassa valtiojohtoista kybervakoilua käyttämällä APT-ryhmiä. Kyberoperaatioiden kilpailutus yksityisillä palveluntarjoajilla osoittaa kuitenkin sen, että Kiinassa kybervakoilukoneistoa on hajautettu. Ulkomaille eivät iske Kiinasta vain korkean tason APT-toimijat, vaan hyökkäysten takana voivat olla myös yksityiset kyberalan yritykset. Tällä tavoin Kiinan turvallisuusviranomaiset pystyvät räätälöimään operaatioita kustannusten, laadun ja määrän suhteen. Käytännössä kilpailutus toimii siten, että jokin valtion turvallisuusviranomainen jättää tarjouspyynnön, johon yksityiset palveluntarjoajat voivat jättää oman tarjouksensa toimeksiannon toteutuksesta.

Palveluntarjoajien välillä on myös kilpailua sekä jopa oikeuteen asti meneviä riitoja. Esimerkiksi Chengdu 404 -niminen yhtiö haastoi edellä mainitun I-Soonin oikeuteen ohjelmistokehitykseen liittyvässä sopimuskiistassa. Chengdu 404 on aiemmin yhdistetty APT41 –uhkatoimijaan, joka puolestaan linkittyy moniin ulkomaille kohdistuneisiin operaatioihin. Voidaankin pohtia, ovatko nämä kilpailutuksiin osallistuvat yksityiset yhtiöt, myös I-Soon, vain kulissiyhtiöitä erilaisille APT toimijoille.

Tulevaisuudessa Kiinan kybertoimintaympäristöä voidaankin tarkastella uudesta näkökulmasta, kun nyt tapahtuneen tietovuodon myötä tiedämme osan kiinalaisista uhkatoimijoista olevan yksityisiä yrityksiä. Tällä voi olla vaikutusta myös kyberoperaatioiden lopputulokseen. Tulevat operaatiot saattavat olla entistä tehok-kaampia ja tuhoisampia, kun toimijat kilpailevat “markkinoilla” keskenään. On myös mahdollista, että mikäli toimeksiantojen tilaajalla eli Kiinan valtion turvallisuusviranomaisilla valintaperusteet muuttuvat, voidaan myös kyberoperaatioiden alihankkijoiden valinnassa keskittyä laadun sijasta hintaan. Tällä taas olisi mahdollisesti päinvastainen vaikutus vaikuttavuuteen. Tässä mielessä, kun tarkastelee oman organisaation Kiina-sidonnaisuuksia, kannatta tämä muutos ottaa huomioon.

3. KYBERTURVALLISUUSTILASTOJEN HAASTEET

Kyberturvallisuusjulkaisuja lukiessa törmää usein tilastoihin. Ne voivat kertoa jonkin tietyn uhkatyypin lisääntymisestä, trendeistä rikollisuudessa tai muusta mitattavasta asiasta. Tilastot ovat hyödyllisiä, sillä ne auttavat hahmottamaan nopeasti, miten jokin ilmiö on kehittynyt tai kuinka merkittävästä asiasta on kyse. Tilastojen käyttöön liittyy aina merkittäviä haasteita –niin kyberturvallisuudessakin. Samaa ilmiöitä kuvaavat, eri lähteistä kerätyt ja eri toimijoiden kokoamat tilastot voivat poiketa merkittävästi toisistaan tai pahimmillaan olla ristiriidassa keskenään. Jos tarkastellaan esimerkiksi vuoden 2023 loppupuoliskolta koottuja tilastoja kiristyshaittaohjelmien esiintyvyydestä, voi lähteestä riippuen tilanne näyttää hyvin erilaiselta. Tietoturvatoimijoiden julkaisuja vertailemalla piirtyy ristiriitainen kuva. Esimerkiksi pilvi- ja verkkoturvallisuusyhtiö Sangorin mukaan ransomware-iskujen määrä kasvoi vuonna 2023 95 % verrattuna edelliseen vuoteen. Kyberturvallisuusratkaisuja toimittavan CheckPointin mukaan luku olisi lähempänä 33 %:a, uhkatiedusteluun keskittyvän CyberIntin mukaan 56 % ja tietoturvaohjelmisto- ja -laitteistoyritys Sophosin mukaan hyökkäysten yleisyys oli sama kuin edellisenä vuonna. Samaan aikaan verkkolehti BleepingComputer kirjoittaa, että vuonna 2023 ransomware-iskujen tienestit pienenivät, kun uhriksi joutuneet entistä useammin kieltäytyivät maksamasta. Kilpailija Wired taas kertoo, että vuosi 2023 oli kiristäjille historian paras vuosi ja maksettujen lunnaiden määrä ylitti miljardin dollarin rajapyykin. Mitä tästä kokonaisuudesta pitäisi sitten päätellä, ja miksi tilastot ovat niin ristiriitaisia?

Yksinkertaisin syy etenkin eri tietoturvatoimijoiden tilastojen poikkeavuudelle on niissä käytetyt eri lähteet ja erilaiset tavat mitata ilmiötä. Sangor pohjaa arvionsa vakuutusyhtiö Corvuksen lukemiin, CheckPoint on tuottanut datan omalla tekoälysovelluksellaan, Cyberint ei erittele lähteitään ja Sophos kertoo lukeman perustuvan sen asiakkailla teetetyn kyselyn vastauksiin. Samoin verkkolehdissä on käytetty eri toimijoiden julkaisuja lähteenä. BleepingComputerin luku perustuu IT-yhtiö Covewaren Incident Response -tiimin keräämiin tilastoihin, kun taasen Wiredin luku juontaa juurensa kryptovaluuttoja analysoivan Chainalysis-toimijan tietoihin siitä, kuinka paljon kryptovaluuttaliikenteestä voidaan yhdistää ransomwaretoimintaan. Tilastoja kerätään ja kootaan siis huomattavan eri tavalla. Luonnollisesti nämä eri tavoin tiedot eivät ole vertailukelpoisia keskenään. On myös huomioitava, että lähes kaikkien mainittujen toimijoiden kohdalla kyseessä on kyberturvallisuuspalveluja myyvä yritys, jonka intresseissä voi olla esittää tilanne uhkaavana ja samalla liittää raportin loppuun lyhyt kuvaus omista palveluista, joilla uhkaa voidaan pienentää. Luotettavia, ilman markkinointitarkoitusta koostettuja tilastoja on toki saatavilla. Esimerkiksi monet viranomaistahot tuottavat kattavia kuvauksia tietystä uhkakentästä. Näiden käyttöä haastaa toisaalta usein joko toimiala- tai valtiospesifisyys eikä niitä ole tarkoitettukaan koko uhkakentän kuvaamiseen. Kaiken tämän lisäksi kyberturvallisuuteen liittyvää tilastointia haastaa vielä siihen liittyvän piilorikollisuuden tai ilmoittamatta jätettyjen tapausten määrä. Kybertapahtumista huomattava osa jää aina pimentoon. Aina hyökkäyksen kokenut taho ei syystä tai toisesta myöskään halua julkisesti tiedottaa tapahtumasta.

Kyberturvallisuustilastoja lukiessa tulee siis olla tarkkana siitä, mikä taho ja miten tiedot on koonnut ja julkaissut, ja kuinka relevantteja tulokset ovat omalle organisaatiolle. Asiallisesti laaditut ja rehellisesti esitetyt tilastot voivat olla hyödyllisiä omaa uhkakuvaa kartoittaessa, ja eri toimijoiden samasta asiasta tekemiä tilastoja vertailemalla voi saada kuvan laajemmasta trendistä, vaikka itse tulokset eivät vertailukelpoisia olisikaan. Tilastoja tarkasteltaessa tulee siis pystyä katsomaan yksittäisiä lukuja laajemmalle. On syytä pitää mielessä, että omaa väitettä tukevia tilastoja on lähes aina saatavilla. Mitä taas tulee esimerkkinä käytettyihin kiristyshaittaohjelmiin, lienee selvää, että kaikkien toimijoiden mielestä uhka on todella kasvamassa, vaikkakin kasvun nopeus vaihtelee alueen tai toimialan perusteella. Kiristyshaittaohjelmien tuottavuudesta voidaan olla montaa mieltä, mutta kenties tilastoja paremmin taloudellisesta hyödystä kertoo se, että ”markkinoille” nousee jatkuvasti uusia rikastumisesta haaveilevia toimijoita, ja pitkään kiristystä harjoittaneet hakkeriryhmät kehittävät jatkuvasti omaa toimintaansa.

LÄHTEET

1. Verkkoulottuvuudesta sodan vastaisen opposition tukijalka Venäjällä?

https://aif.ru/society/rostovskogo_it-specialista_osudili_na_tri_goda_za_ukrainskuyu_ddos-ataku

https://meduza.io/feature/2022/03/04/meduza-zablokirovana-v-rossii-my-byli-k-etomu-gotovy-i-prodolzhaem-rabotat https://novayaga-zeta.eu/articles/2022/04/29/budem-govorit-kak-est

https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics https://me-duza.io/en/feature/2023/11/18/elves-vs-trolls

2. Tietovuoto antoi uutta näkökulmaa kiinalaisesta kybervaikuttamisesta

https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/

https://hongkongfp.com/2024/02/24/hackers-for-sale-what-we-know-about-chinas-massive-i-soon-cyber-leak/

https://thereadable.co/the-i-soon-data-leak-chinese-apts-and-implications-for-southeast-asia/

https://www.crunchbase.com/organization/i-soon

https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/

https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/

https://readwrite.com/chinas-hired-hackers-a-massive-cybersecurity-breach-exposing-chinas-operations/

https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41

https://www.infosecurity-magazine.com/news-features/isoon-github-leak-chinese-cyber/

3. Kyberturvatilastojen haasteet

https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023

https://www.corvusinsurance.com/blog/q3-ransomware-report?utm_campaign=FY23-Q4-Quarterly%20Ransomware%20Report&utm_source=ransomware%20blog&utm_medium=press

https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/

https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/

https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-as-victims-refuse-to-pay/

https://www.wired.com/story/ransomware-payments-2023-breaks-record/

Kuvat: Pixabay