Cyberwatch

# Cyberwatch Monthly Review
# 2018 January

*1. Processor vulnerabilities affect almost all computers and multiple smartphone models.*

*2. 2,8 million Norwegian citizens´ health data subject to a cyber attack.*

*3. $ 500 million worth of cryptocurreny stolen in Japan.*

*4. Targeted attacks on Eastern European diplomats.*

*5. The Olympics is an attractive target for cyber attacks.*

*6. USA passed a bill to renew Internet surveillance program and plans to nationalize its 5G networks.*

*7. Lack of competent cybersecurity in-house staff poses a risk to companies.*

*8. Botnets evolve into complex peer-to-peer networks.*

*9. The cryptocurrency mining is increasing and taking new shapes.*

**Cyberwatch – trust beyond horizon**

# Cyberwatch Monthly Review - January 2018

The year started with two critical vulnerabilities called **Meltdown** and **Spectre**, which result from severe design flaws in modern microprocessors. Originally the attention was focused on Intel based chips but also many ARM and AMD-based processors were also affected. Are these design flaws and vulnerabilities at the core of modern processors a sing that all the foundations of digital security will be shaken?

**The Olympics** have always been very politicized sporting events. Data breaches, hacking and espionage are worth noticing as key elements of this political game. It seems, The PyeongChang 2018 Winter Olympic Games to be games of all times, at least in the cyber realm.

**The cyber attack to Norwegian healthcare data** underscore in a harsh manner the underestimated risk related to centralized healthcare data services. What genuine risks and consequences does the healthcare data breach cause to citizens or to national security?

**Cryptocurrency mining** malware widely used in different ways, e.g. using NSA exploit or public wireless routers, Android mobile devices, even computers of Lahti health-care center. It seems, that everything that could be used for cryptocurrency mining will be used.

**The development of botnets towards peer-to-peer (P2P) networks** indicates new rising threats with the rising number of IoT devices. New emerging P2P could be used not only for denial of service attacks, but also for data theft, cryptocurrency mining, extortion and espionage.

**The United States passed a bill to renew Internet surveillance program**, that continues *NSA* and *FBI* ”warrantless” Internet surveillance program for next six years. Along with this, Finland's long-planned and heavily debased intelligence law seems somewhat idealistic and modest.

**Many countries will improve their cybersecurity practices this year**. Time will show how this is affecting the amount, quality and type of future cyber events. The global intensity on the web is increasing, which makes it important to reflect on how to adapt to this changing situation.

- ✓ The digital environment is constantly evolving and looking new business models services. Does our own thinking and standpoint evolve, too?
- ✓ Do current practices, services and products meet the changing data security needs?
- ✓ What are the consequences if your company's sensitive data leaks?
- ✓ What if your own health record leaks?

# The most important cyber events and their significance

### 1. Processor vulnerabilities affect almost all computers and multiple smartphone models.

Severe design flaws found in modern microprocessors inflict two critical vulnerabilities called **Meltdown** and **Spectre.** Originally the attention was focused on Intel based chips but as of current knowledge, **almost every computer system is affected, including mobile phones**. Even if most software and hardware vendors were able to provide a security fix rather quickly, this type of vulnerability is extremely serious in terms of scope and potential risks.

Fixing design flaws and vulnerabilities of this level will most likely emergence new vulnerabilities and exploits in the near future. This also indicates that we are expected to see new vulnerabilities on foundations of current computer ecosystem, partly because of the increased attention to the subject but also as a result of new security fixes causing new unknown security issues.

Most home users probably don´t even notice the performance drop caused by the security update, but for businesses that depend on high performance calculating power this can be a noticeable setback.

An important point raised by these vulnerabilities is that many of the solutions currently in use are based on decades of old logic that may not be able to respond to today's challenges. The problem is not only technical but also human and systemic. The same challenge applies equally to people, businesses, various actors in society and countries that try to manage and maintain old familiar operating models in this ever-changing digital environment. Digital time requires a digital era operating model.

### 2. 2,8 million Norwegian citizens´ health data subject to a cyber attack.

The Norwegian healthcare data is suspected of being subjected to a highly targeted cyber attack involving more than half of Norway´s population. According to the Norwegian research authority, the attack may be related to acquiring the participant information for the major NATO exercise scheduled for October-November 2018. It is still unknown how large the leak is. If this turns out to be a phishing attack related to the NATO exercise, points it out a new type of strategic thinking to find the enemy's weaknesses. But, it could also be an attempt to unveil a national doping usage. An underlying cause of this type of an attack may be to influence the course of the exercise in a new way.

From Finland's point of view, the case is interesting because of ongoing large hospital and health sector projects alongside with the GDPR. A tangible cyber threat of one of the vital functions of Finnish society seems to be now even more obvious. For instance, how does the current approach of the Finnish Kanta.fi-archives, that has been designed ten years ago, meet the needs of the future? Now, it might still be possible to mitigate the risk and think ahead.

> *"Risks of the Kanta.fi – database may arise bigger than benefits."*
>
> *- Lasse Lehtonen, hallintoylilääkäri, (senior administration physician) HUS*

### 3. $ 500 million worth of cryptocurreny stolen in Japan.

Nearly half a billion dollars worth of cryptocurrency was stolen inadequately protected cryptocurrency online wallet. The incident could have been avoided by using simply security procedures – offline wallets and multi-signature security. With the blooming cybercrime industry, it is important to notice that criminals may also have access to resources that have traditionally been the backbone of state actors or cybercriminals in co-operation with them.

### *4. Targeted attacks on Eastern European diplomats.*

Eastern European diplomats have been objected to targeted attacks. A Russian based hacker group TURLA is suspected to be behind the attacks. On the other hand, there is a suspicion that this is a deception related to an information operation. The malware used in the attack was distributed by exploiting the Adobe Flash Player's software update package.

For years, Adobe Flash Player has been in favor of malicious software vendors as an easy target. End users are so frustrated with ongoing updates, that majority probably don´t pay attention to them anymore. But the case also demonstrates, that it is almost impossible to notice a well designed targeted attack even if being a security conscious end user. All in all, this continues the trend in exploiting the vulnerability of software delivering processes.

### *5. The Olympics is an attractive target for cyber attacks.*

Cyber attacks on the Olympic games have started well ahead of the sporting events themselves. The critical information systems of this year's Olympics have been implemented for the first time only in the form of a cloud service managed from Spain. Also all data is located in Barcelona. Reporters see the same information system regardless of whether they are on-site in Korea or home delivery on a computer.

There are many high profile people and actors who are the subjects of intelligence and espionage. Of particular note is the subject of North Korea's actions during the event. Russia may also be willing to "strike back" because of their anti-doping revelations, and the related non-competition clause.

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

### *6. USA passed a bill to renew Internet surveillance program and plans to nationalize its 5G networks.*

The United States renewed their Internet surveillance program, which continues *NSA* and *FBI* ”warrantless” Internet surveillance program for next six years. The law does add a narrow warrant requirement for cases if an investigation seeks emails related to an existing criminal investigation that has no relevance to national security. Under the law NSA is empowered to eavesdrop on vast amounts of digital communications via American companies like Facebook, Google, Verizon etc. The intelligence is targeted primarily to foreign people or Americans who communicate with foreign people. Along with this, Finland's long-planned and heavily debased intelligence law seems somewhat idealistic and restrictive. For great powers protection of privacy seems to be a secondary issue despite speeches.

The USA plans to build a 5G network for “domestic” solutions are understandable from a national security point of view. This could reduce the risk of foreign players, such as the Chinese, from online espionage. But in the end, it is somewhat questionable whether it would improve the security of the US in the data networks.

### *7. Lack of competent cybersecurity in-house staff poses a risk to companies.*

The increase in cybercrime, hacking and data leakage has formed a shortage of skilled cyber security people. Competition from experts raises a personnel risk also in those companies that have managed to recruit excellence.

For example, if a key player is suddenly hired to a competitor, filling a job description can be challenging - let alone lost knowledge. Is there a risk that cyber specialists will still have access to organizational systems, even without traces? How do the needs of information security change when a key person changes?

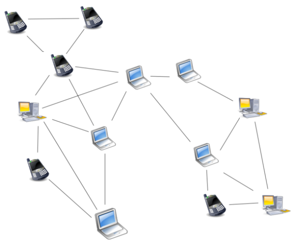
Therefore, it is important to create cyber security a continuous process that is integrated into the organization's processes and culture, so that even the lack of key people is not able to cripple the organization's operations.

Another major challenge is the know-how of buying cyber-safe solutions. In order for an organization to buy a secure solution or a service, the buyer should have wide knowledge about cyber related issues of the acquisition. This includes specific needs and legal requirements of the industry, a good understanding of the available solutions, their strengths and weaknesses. In addition, the buyer should be able to evaluate relevant security solutions and assess their future prospects. And of course, how do the solution and its operating model meet the requirements of GDPR?

As a recent example, the Helsinki Region Transport (HSL) project (to reload the value of the travel card via the Internet) was delayed again because the technology selected was found to be illegal in Finland.

### *8. Botnets evolve into complex peer-to-peer networks.*

New emerging botnets are growing around the world. A new laterally spreading decentralized peer-to-peer type botnet called ***Hide N' Seek (HNS)*** is infecting unsecured IoT devices. This type of botnets would deliver cybercriminals an advanced versatile platform to be used not only for denial of service attacks, but also for data theft, cryptocurrency mining, extortion and espionage. Hopefully, this trend will prompt IoT hardware and software manufacturers to take security issues seriously.



### *9. The cryptocurrency mining is increasing and taking new shapes.*

ADB Miner: A new botnet is expanding fast laterally using virus-like methods. This crypto miner malware exploits software development properties of Android devices.

The cryptocurrency mining seems to be aggressively increasing and seeking new forms. Therefore, it's vital to ensure that security automatic update process for all devices work perfectly.

> - *"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*

## Sources

### Review

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

### 1. Processor vulnerabilities affect almost all computers and multiple smartphone models.

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
Picture: https://www.flickr.com/photos/intel_de/9662277285

### 2. 2,8 million Norwegian health data subject to a cyber attack.

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 million worth of cryptocurreny stolen in Japan.

Picture: 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. Targeted attacks on Eastern European diplomats.

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
Picture: https://commons.wikimedia.org/wiki/File:Adobe_Flash_Player_SVG.svg

### 5. The Olympics is an attractive target for cyber attacks.

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://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/
https://medium.com/@LanceUlanoff/2018-winter-olympic-games-may-medal-in-technology-e9eda6e2a87a
http://www.silicon.co.uk/cloud/winter-olympics-cloud-205270

### 6. USA passed a bill to renew Internet surveillance program and plans to nationalize its 5G networks.

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
Picture: https://en.wikipedia.org/wiki/Flag_of_the_United_States

### 7. Lack of competent cybersecurity in-house staff poses a risk to companies.

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. Botnets evolve into complex peer-to-peer networks.

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
Picture: https://en.wikipedia.org/wiki/Peer-to-peer

### 9. The cryptocurrency mining is increasing and taking new shapes.

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

# Subscribe

Cyberwatch Finland provides strategic situational awareness reviews based on a holistic view of the cyber world events. Our reviews are based on data collected from publicly available sources including major vulnerabilities, news, reports, events and trends of the cyber security. The data is processed using Artificial Intelligence (AI) and analysed by professional cyber security specialist making perceptions and conclusions of the most important issues from the leaders point of view. Subscription is valid 12 months - more information www.cyberwatch.fi.

**Englsih version is publish one week after finnish version.**
**English version is of the review availble upon separate request**

| | | |
|---|---|---|
| **Subscriber** | | |
| **Organization official name** | | |
| **VAT number (registration number)** | | |
| **Street address** | | |
| **Email address** | | |
| **www-site** | | |
| **Contact person** | | |
| **Contact person's title** | | |
| **Contact person's email** | | |
| **Contact peroson's gsm number** | | |
| **Subscriber delivery email address** | | if more email address, send those with separate appendix list |
| **Subscribe *only* monthly rewies [x]** | | |
| **Subscribe *both* monthly and quarter reviews [x]** | | |
| **Ordering date** | | |

**Send the form via email to: kim.waltzer@cyberwath.fi.**