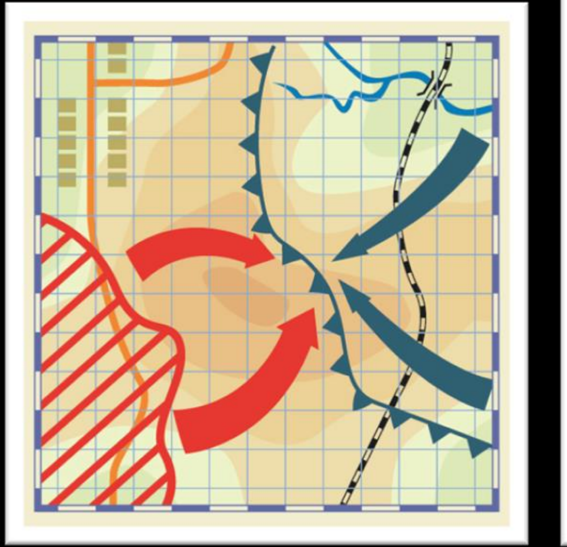
Cyber Weather

Situational Awareness Product For Our Non-technical Constituents

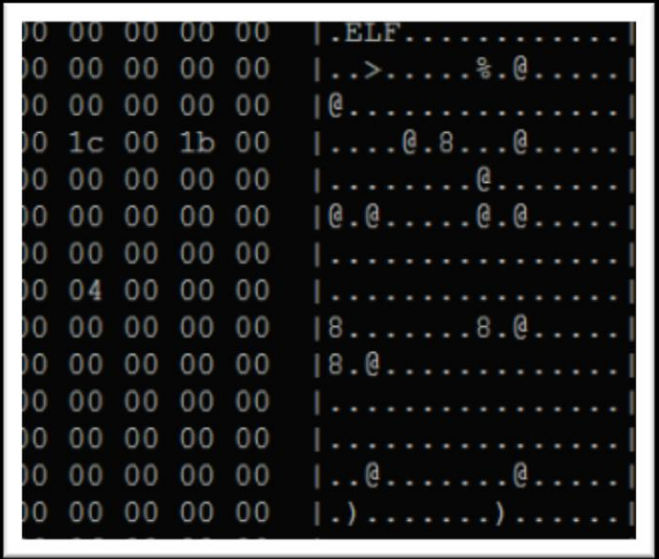
Cyber...WHAT?

Situational awareness?



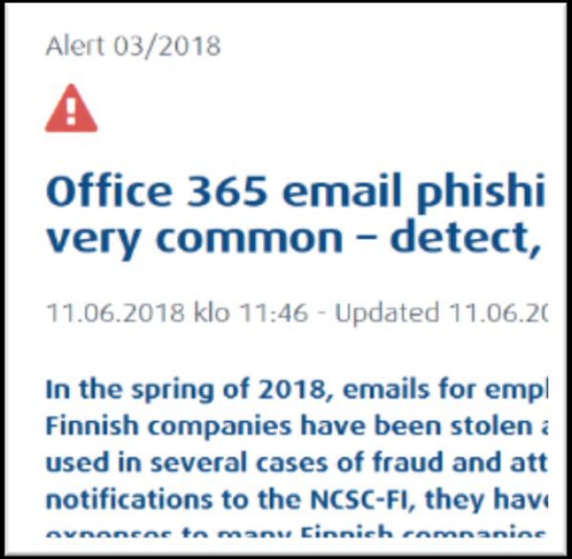
What our constituents think it is

What our management thinks it is



```
00 00 00 00 00   |.ELF...............
00 00 00 00 00   |..>......%.@......
00 00 00 00 00   |@.................
00 1c 00 1b 00   |....@.8...@......
00 00 00 00 00   |.........@........
00 00 00 00 00   |@.@......@.@......
00 00 00 00 00   |..................
00 04 00 00 00   |..................
00 00 00 00 00   |8........8.@......
00 00 00 00 00   |8.@...............
00 00 00 00 00   |..................
00 00 00 00 00   |..................
00 00 00 00 00   |..@.......@......
00 00 00 00 00   |.)........)......
```

What society thinks it is



Alert 03/2018

Office 365 email phishi
very common – detect,

11.06.2018 klo 11:46 - Updated 11.06.2(

In the spring of 2018, emails for empl
Finnish companies have been stolen a
used in several cases of fraud and att
notifications to the NCSC-FI, they hav
expenses to many Finnish companies

What it really is

The problem

Regardless of our communication efforts, our constituents were demanding better situational awareness.

Requirements for the new situation awareness product

- Language that also non-technical audience can understand
- Periodically updated
- Cover wide variety of cyber security topics

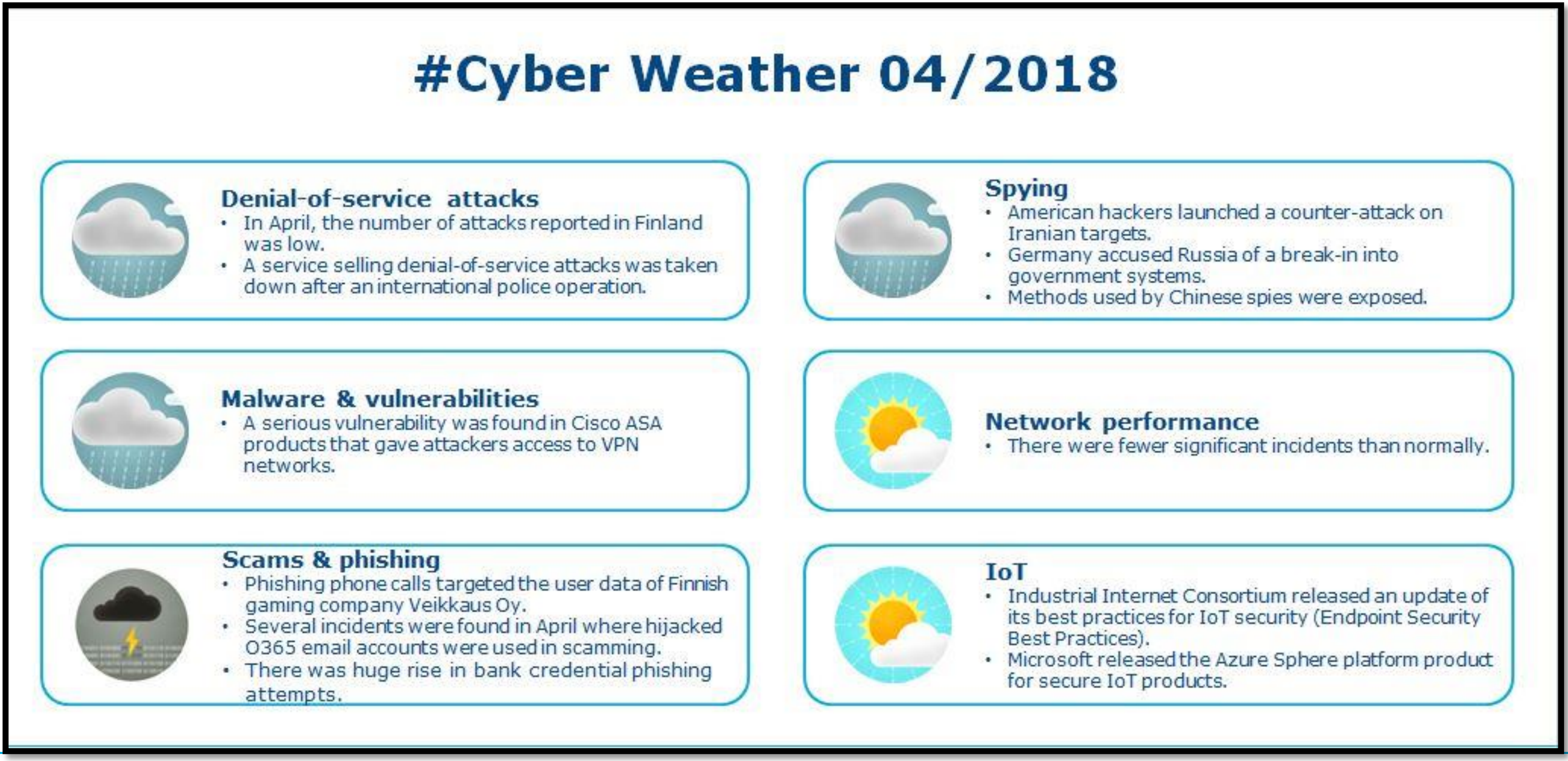
Six focus areas that are updated monthly

- Denial of Service
- Malware & vulnerabilities
- Phishing & scams
- Spying
- Network performance
- Internet of Things

Behind the simple presentation goes a lot of information from different sources

Information sources	Content
Ticketing system	Recent cases and incident reports both from private and public sectors
Information Sharing and Analysis Centres (ISACs)	TLP: RED information from our critical constituents generalized to TLP:WHITE
National early warning and monitoring system (HAVARO)	Detections based on threat intelligence and IoC's
Autoreporter	Malicious network traffic detections in Finland
Open sources	News, social media, public reports

Cyber weather conditions may be calm, worrying or serious



#Cyber Weather 04/2018

Denial-of-service attacks

- In April, the number of attacks reported in Finland was low.
- A service selling denial-of-service attacks was taken down after an international police operation.

Spying

- American hackers launched a counter-attack on Iranian targets.
- Germany accused Russia of a break-in into government systems.
- Methods used by Chinese spies were exposed.

Malware & vulnerabilities

- A serious vulnerability was found in Cisco ASA products that gave attackers access to VPN networks.

Network performance

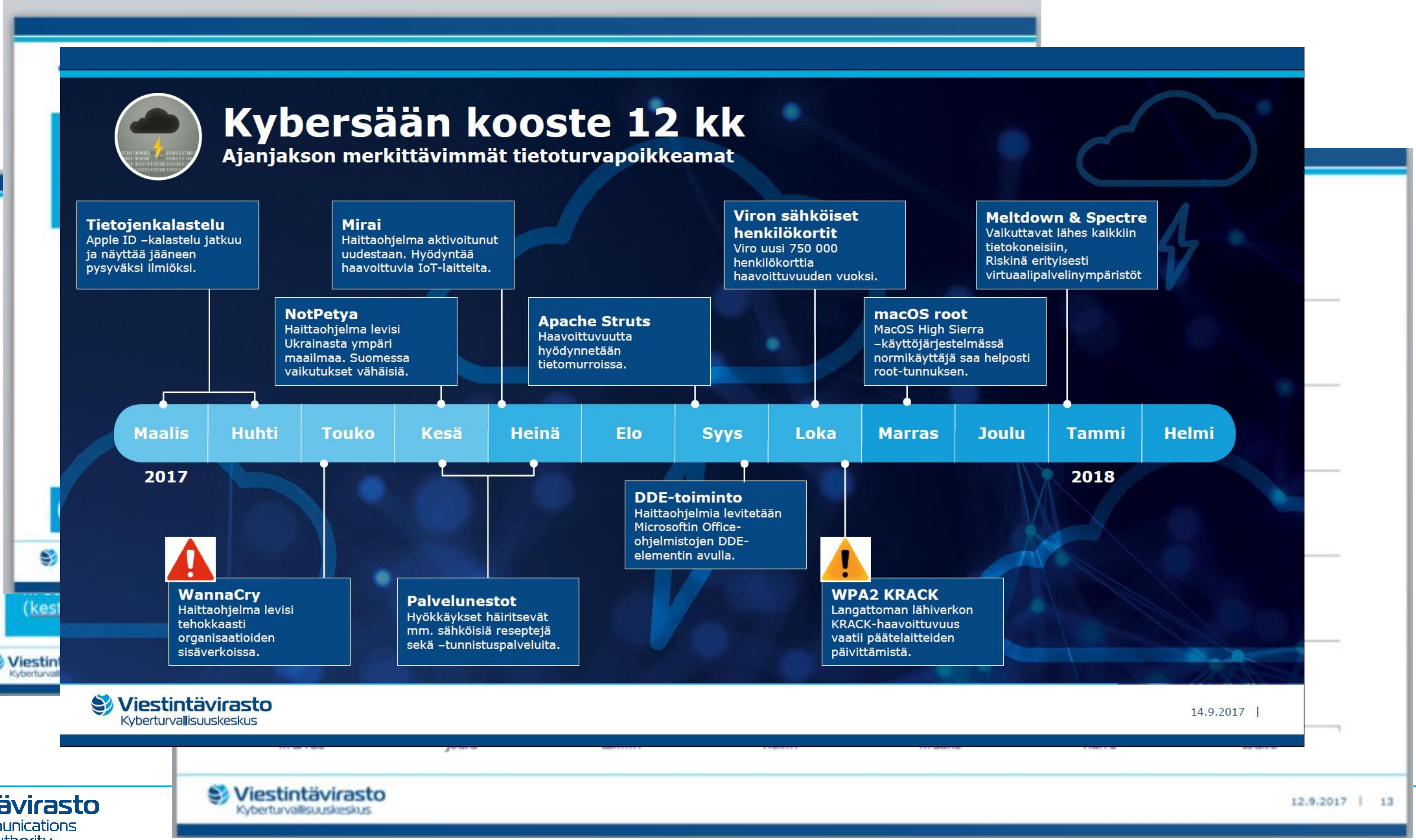
- There were fewer significant incidents than normally.

Scams & phishing

- Phishing phone calls targeted the user data of Finnish gaming company Veikkaus Oy.
- Several incidents were found in April where hijacked O365 email accounts were used in scamming.
- There was huge rise in bank credential phishing attempts.

IoT

- Industrial Internet Consortium released an update of its best practices for IoT security (Endpoint Security Best Practices).
- Microsoft released the Azure Sphere platform product for secure IoT products.



Kybersään kooste 12 kk

Ajanjakson merkittävimmät tietoturvapoikkeamat

Tietojenkalastelu
Apple ID –kalastelu jatkuu ja näyttää jääneen pysyväksi ilmiöksi.

Mirai
Haittaohjelma aktivoitunut uudestaan. Hyödyntää haavoittuvia IoT-laitteita.

Viron sähköiset henkilökortit
Viro uusi 750 000 henkilökorttia haavoittuvuuden vuoksi.

Meltdown & Spectre
Vaikuttavat lähes kaikkiin tietokoneisiin,
Riskinä erityisesti virtuaalipalvelinympäristöt

NotPetya
Haittaohjelma levisi Ukrainasta ympäri maailmaa. Suomessa vaikutukset vähäisiä.

Apache Struts
Haavoittuvuutta hyödynnetään tietomurroissa.

macOS root
MacOS High Sierra –käyttöjärjestelmässä normikäyttäjä saa helposti root-tunnuksen.

DDE-toiminto
Haittaohjelmia levitetään Microsoftin Office-ohjelmistojen DDE-elementin avulla.

WannaCry
Haittaohjelma levisi tehokkaasti organisaatioiden sisäverkoissa.

Palvelunestot
Hyökkäykset häiritsevät mm. sähköisiä reseptejä sekä –tunnistuspalveluita.

WPA2 KRACK
Langattoman lähiverkon KRACK-haavoittuvuus vaatii päätelaitteiden päivittämistä.

Viestintävirasto
Kyberturvallisuuskeskus

14.9.2017 |

Cyber weather is delivered widely to all our constituents

- Critical infrastructure providers (CIP)
- Government
- Media
- Publicly via our website
  - » Frontpage available also in English

Initial reception

NCSC-FI managers

NCSC-FI Experts

External

After positive external feedback, also the internal attitude has turned positive

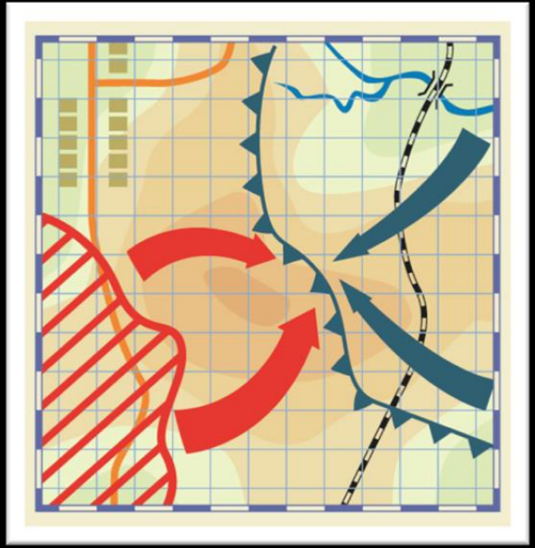
Success factors

- Easy-to-follow language
- Monthly updates
- Familiar metaphor

Benefits

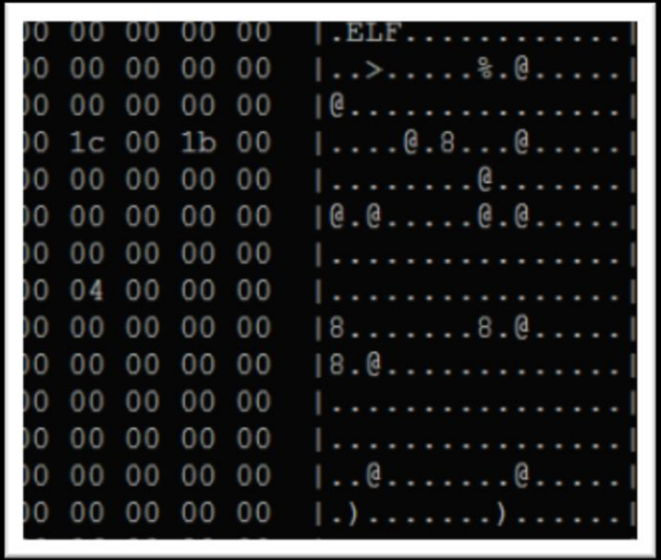
- Key trends and events of the cyberspace
- Device for constituents' internal communication
- Source in risk assessments
- NCSC-FI's own presentations

Situational awareness?



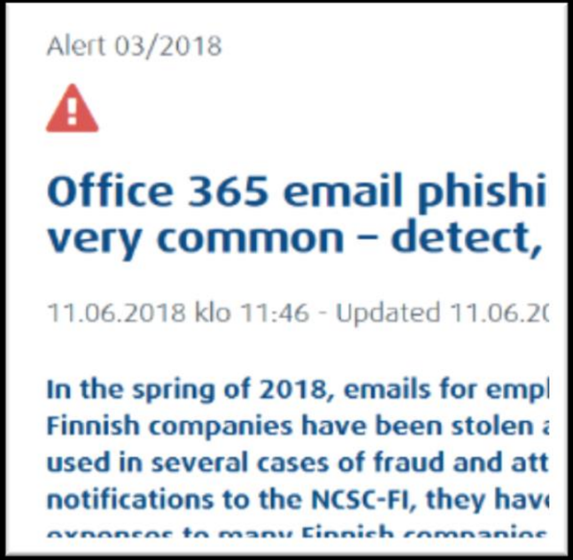
What our constituents think it is

What our management thinks it is



```
00 00 00 00 00   |.ELF.............|
00 00 00 00 00   |..>......%.@.....|
00 00 00 00 00   |@................|
00 1c 00 1b 00   |....@.8...@.....|
00 00 00 00 00   |.........@.......|
00 00 00 00 00   |@.@......@.@.....|
00 00 00 00 00   |.................|
00 04 00 00 00   |.................|
00 00 00 00 00   |8........8.@.....|
00 00 00 00 00   |8.@..............|
00 00 00 00 00   |.................|
00 00 00 00 00   |.................|
00 00 00 00 00   |..@........@.....|
00 00 00 00 00   |.)........)......|
```

What society thinks it is



Alert 03/2018

⚠

Office 365 email phishi
very common – detect,

11.06.2018 klo 11:46 - Updated 11.06.2(

In the spring of 2018, emails for empl
Finnish companies have been stolen a
used in several cases of fraud and att
notifications to the NCSC-FI, they hav
expenses to many Finnish companies

What it really is

Situational awareness?

Something the target audience
is able to understand and use in
their daily work

Viestintävirasto
Finnish Communications
Regulatory Authority

www.ficora.fi