Microsoft

Oppeja Ukrainasta, kybersota kriittistä infraa vastaan

Juha Karppinen
National Technology Officer
Microsoft
Juha.Karppinen@microsoft.com

Sisältö

- Taustaa Microsoftin kybertoiminnoista
- Kokemuksia Hybridistä Sodasta
- Hybridisodan opetukset


FUTURISTIC HUD INTERFACE TEMPLATE DESIGN
HUD SYSTEM INTERFACE DESIGN
Azure Regions

Microsoft Threat Analysis Center

Tavoite – *Havainnoida, arvioida ja torjua digitaliisia uhkia, jotka kohvistuvat Microsoftiin, asiakkaisiin tai demokratioille (valtioille)*

What is MTAC?

Team of expert analysts

- Detection of and response to foreign influence operations
- Cyber threat context analysis
- Coverage spanning languages, geographies, & online environments

Intersection of influence & cyber threats

- **Cyber-enabled influence**
  - Proprietary data fuels expert analysis
  - **Focus:** Nation state-aligned actors
- **Report:** Deliver analysis to enable response & build resilience

How MTAC Operates

Assessment & Proprietary Collection

Proprietary telemetry & automation

Intelligence Analysis & AI-Based Applications

Global "hubs"

>14 languages

Actionable Intelligence

Intelligence reports & threat briefs

Lopputulema

Kyky lieventää ja häiritä erilaisia vaikutus- ja kyberoperaatioita

Microsoftin hyperskaalautuva kyber resilienssi suojatoimet digitaaliseen ekosysteemiin

Maailman suurin tietoturvapalvelujen tarjoaja

1500+
kyberrikollisryhmää
(300+ v. 2023)
- 600+ valtiollista (160+ v. 2023)
- 300+ kyberrikollista (50+ v. 2023)
- 200+ vaikuttaja ryhmää

78T
signaalia / päivä
(65T v. 2023)

4 500
Ddos hyökkäystä / päivä
(1 700 v. 2023)

600M
identiteetti hyökkäystä/ päivää

7 000
Salasana hyökkäystä /sekuntti
(4000 v. 2023)

34 000
Microsoft tietoturvaosaajaa
(10.000+ 2023)

Strateginen ja taktinen hyöty kyberoperaatioista

Vaikuttaa
Kohteita häiritsemällä ja vaikuttamalla ohjata tekemään vapaaehtoisesti turvallisuuden kannalta haitallisia päätöksiä, käyttämällä virheellistä tietoa.

Vahingoittaa
Aggressiivisten ja näkyvien hyökkäysten suorittaminen tavoitteena polarisointiin, demoralisointiin ja/tai pirstoutumiseen.

Kiristää
Usein yhdistettynä kineettiseen hyökkäykseen, hallituksen tai siviili infrastruktuurin pakottaminen hyökkääjän tavoitteisiin tai jopa tuhoaminen

Kokemuksia Hybridistä Sodasta

Tuhoisat kyberhyökkäykset

Venäjän hallituksen tahot (Blizzard), jotka ovat vastuussa kyberhyökkäyksistä

GRU

STRONTIUM (*Forest Blizzard*)
Data theft, phishing (military targets)

IRIDIUM (*Seashell Blizzard*)
Destruction: FoxBlade wiper;
CaddyWiper, Industroyer2

DEV-0586 (Cadet Blizzard)
Destruction: WhisperGate wiper,
data theft, influence operations

SVR

NOBELIUM (*Midnight Blizzard*)
Password spray, phishing
(Ukrainian and NATO member diplomatic targets)

FSB

ACTINIUM (*Aqua Blizzard*)
Phishing, data theft

BROMINE (*Ghost Blizzard*)
Data theft

KRYPTON (*Secret Blizzard*)
Reconnaissance, phishing

Ensimmäisen **neljän kuukauden** aikana tapahtui enemmän kuin edellisten **kahdeksan vuoden.**

Ensimmäiset “laukaukset” käytiin cyberavaruudessa

23rd Feb 2022: The cyberwar started **10 hours** before the physical invasion

Venäjän kybertoimet

Käyttää kyberoperaatioita se tukeakseen kineettistä sotaa mutta pyrkii myöskin videoväärennyksillä ja huijaussisällöllä vaikuttamaan omiin kansalaisiin, että myös Ukrailaisiin ja erityisesti muihin NATO- maihin

Venäjän koordinoidut kyber- ja sotilasoperaatiot Ukrainassa

April 19
IRIDIUM launches destructive attack on Lviv-based logistics provider

April 29
IRIDIUM conducts reconnaissance against transportation sector network in Lviv

May 3
Russian missiles strike railway substations, disrupting transport service

March 4
STRONTIUM targets government network in Vinnytsia

March 6
Russian forces launch eight missiles at Vinnytsia airport[3]

March 16
Russian rockets strike TV tower in Vinnytsia

February 14
Odessa-based critical infrastructure compromised by likely Russian actors

April 3
Russian airstrikes hit fuel depots and processing plants around Odessa

February 28
Threat actor compromises a Kyiv-based media company

March 1
Missile strikes Kyiv TV tower

March 1
Kyiv-based media companies face destructive attacks and data exfiltration.

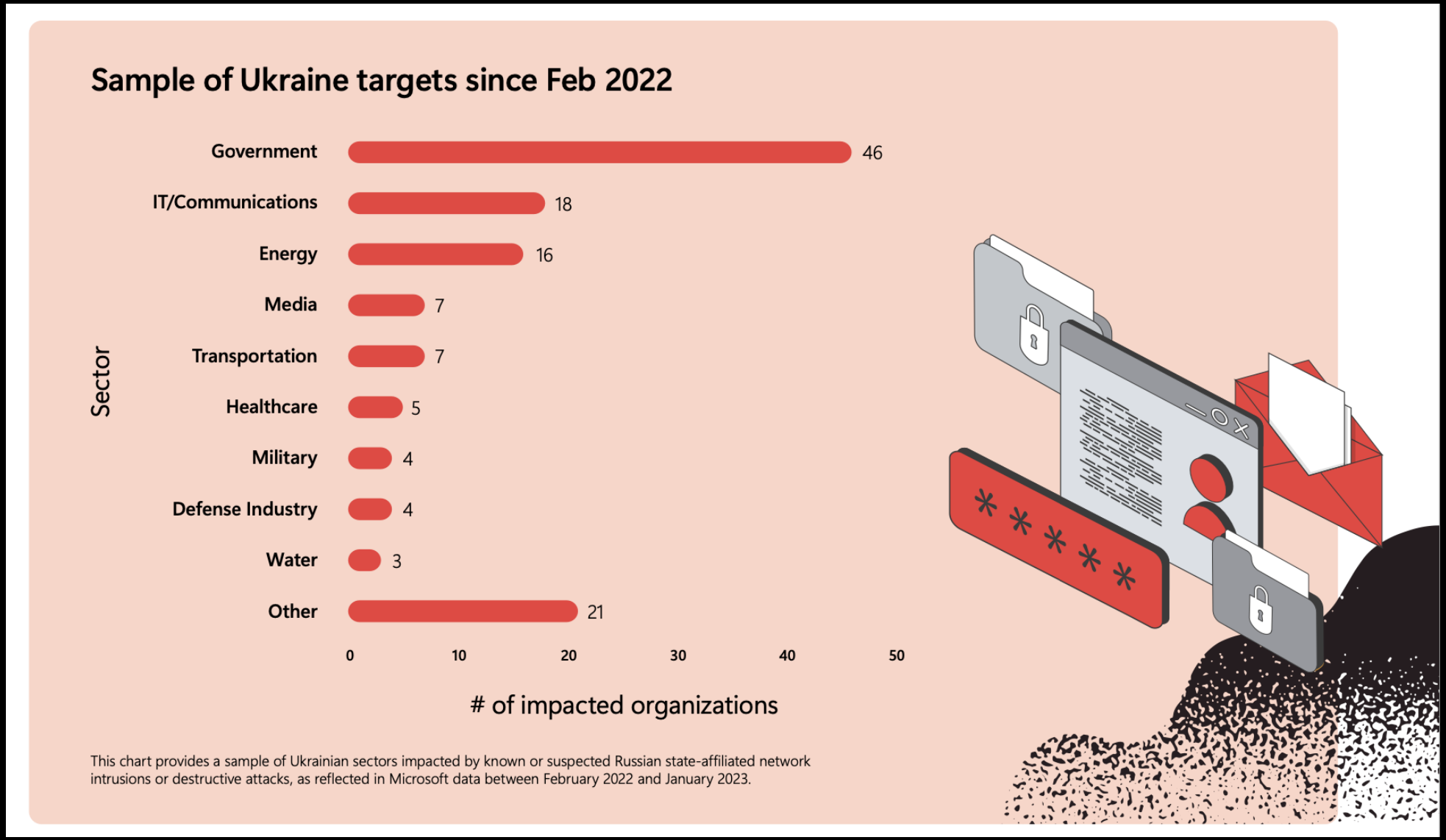
March 11
Dnipro government agency targeted with destructive implant

March 11
First direct Russian strikes hit Dnipro government buildings, among others

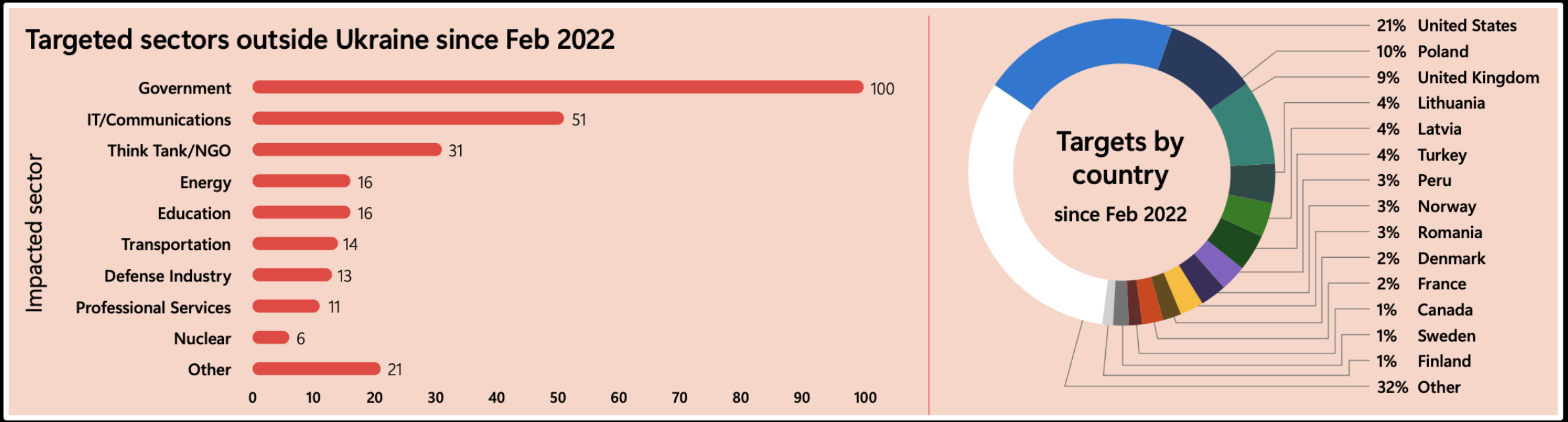
March 2
Russian group moves laterally on network of Ukrainian nuclear power company

March 3
Russia's military occupies Ukraine's largest nuclear power station

Hybridin sodankäynnin kohteet toimialoittain Ukrainassa



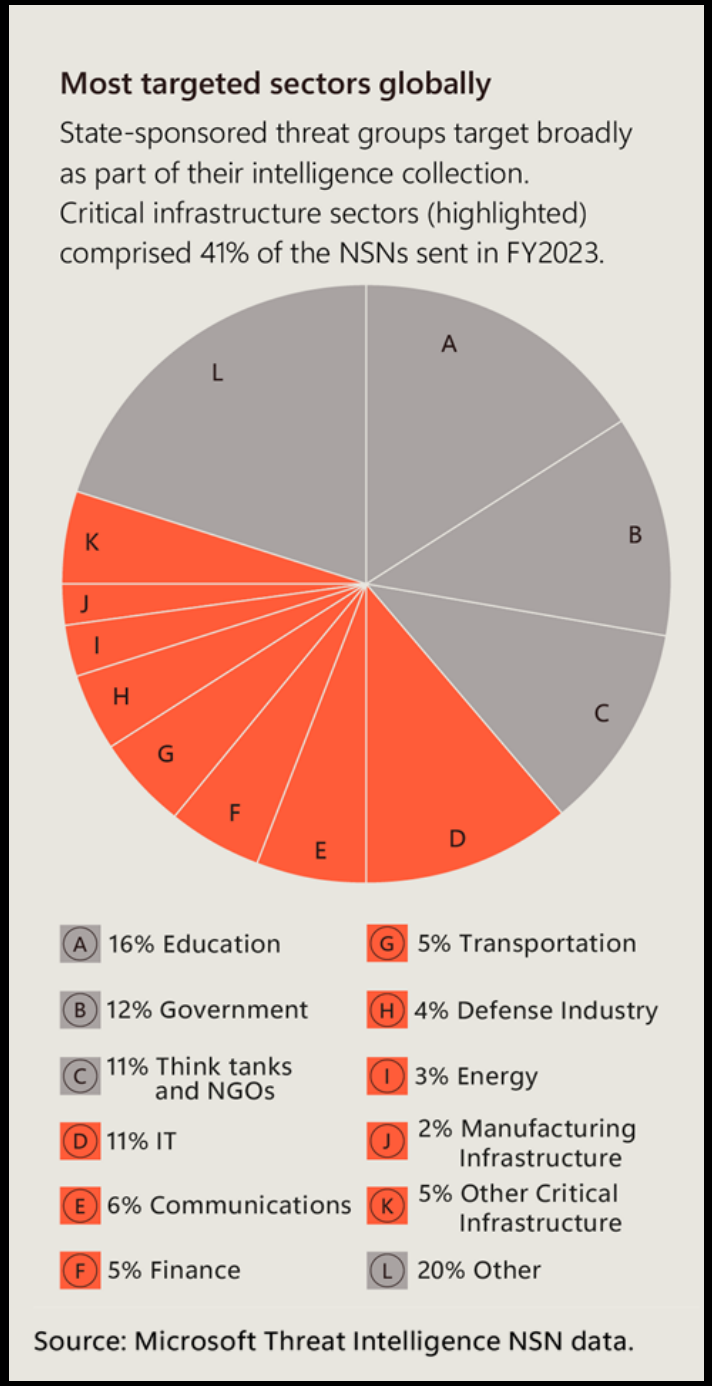
Tarketoidut toimialat muissa maissa (ei Ukraina)



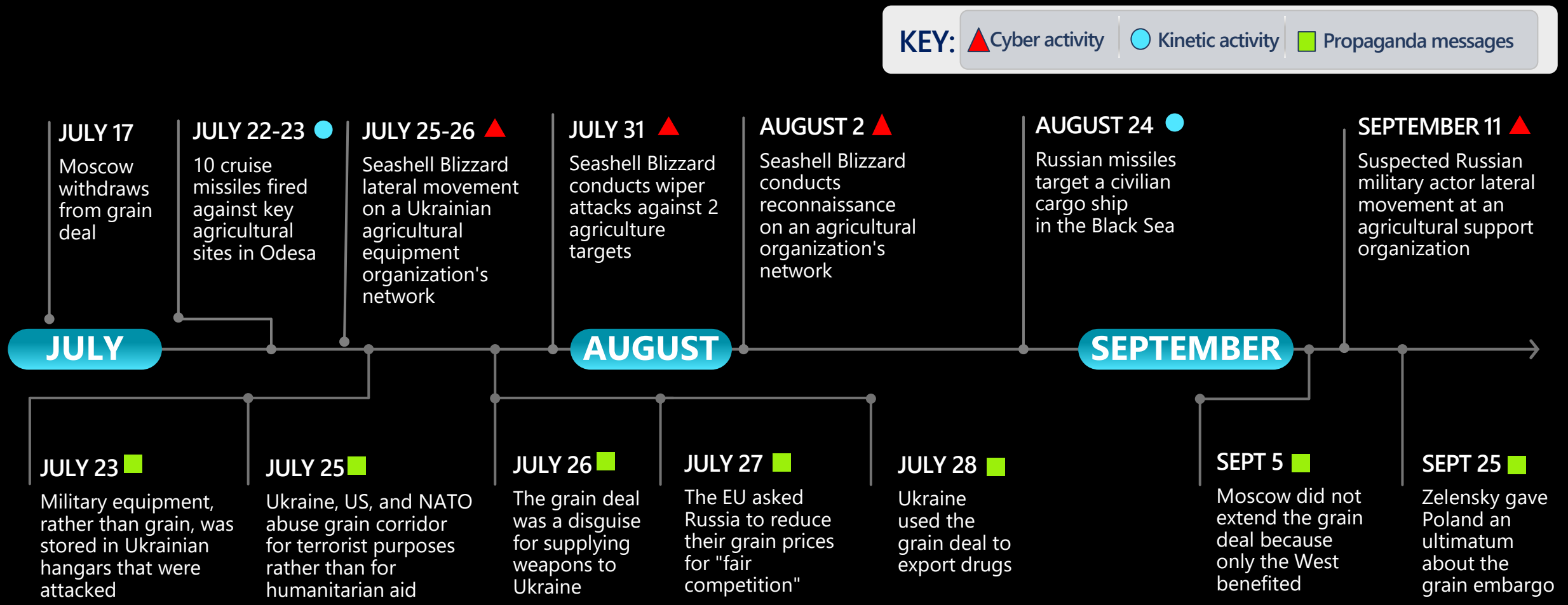
- *Activities range from reconnaissance to data exfiltration.*
- *Russian threat actors most interested in government and IT sectors. Several actors compromise IT firms to exploit trusted technical relationships and gain access to those firms' clients in government, policy, and other sensitive organizations.*

Kremlin kasvava focus kriittiseen infrastruktuuriin

- Critical infrastructure targeting increased in the last year
- Using techniques to establish persistence and evade detection



Kreml hyökkää Ukrainan maataloussektoriin



Hybridisodan opetukset

Taistelu kriittisestä infrastruktuurista


The importance of moving fast
The need to move data across borders

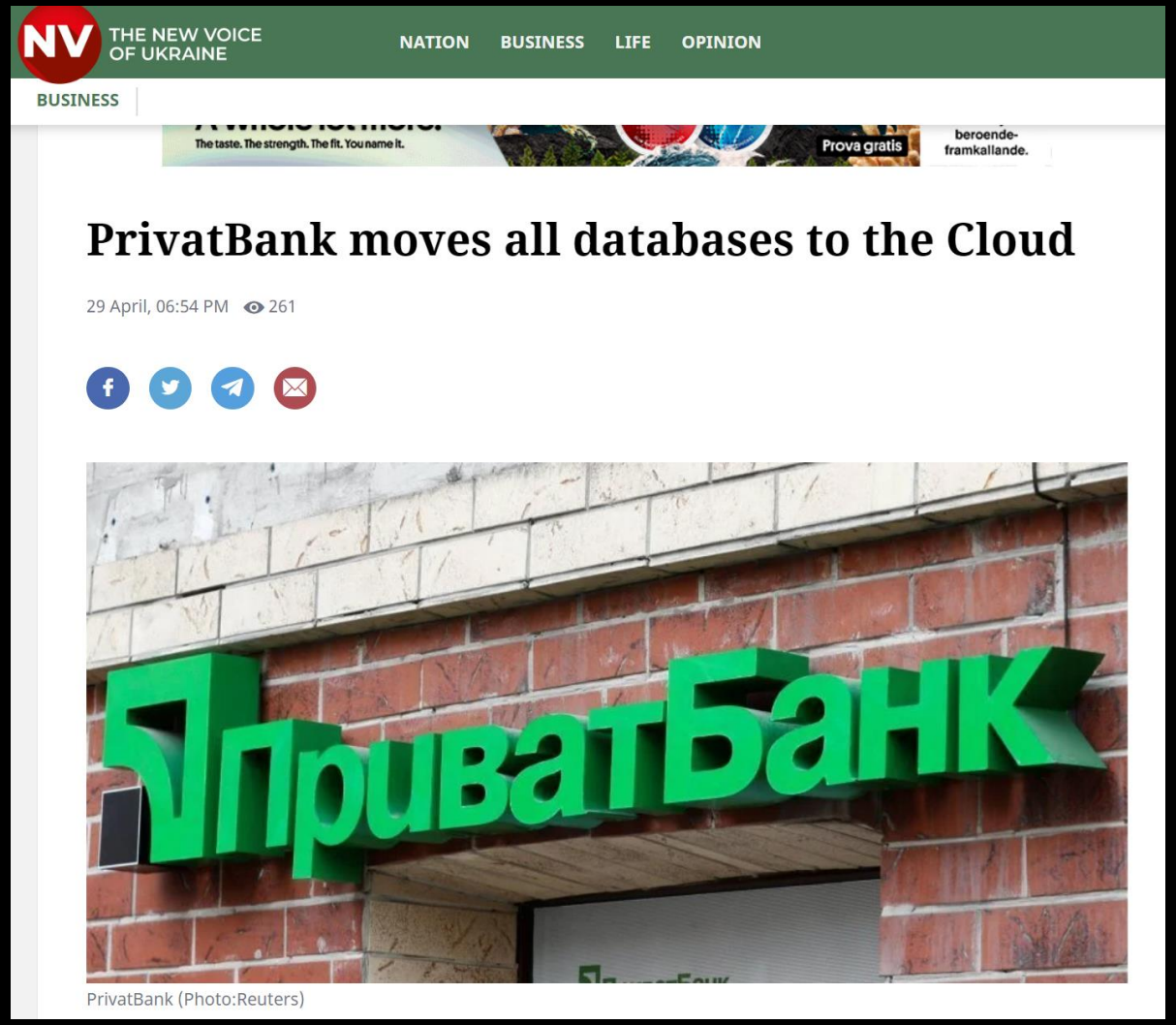
Vuoden 2022 loppu

Arviolta 10 miljoonaa gigatavua Ukrainan hallituksen dataa on tallennettu pilvipohjaisille alustoille.

Yli 100 valtion tietokantaa on siirretty **pilvialustoille** ympäri Eurooppaa. Ukraina on varonut paljastamasta, missä palvelimet sijaitsevat.

Myös pankit siirtyivät pilvipalveluihin :

- Kesti 45 päivää siirtää kaikki kriittiset sovellukset pilvipalveluihin
- Tiedot siirrettiin 3 500 palvelimelta
- 4 petatavua dataa ja tapahtumia
- 270 tärkeää sovellusta
- Projektin teki 460 PrivatBankin IT-asiantuntijaa ja konsulttia

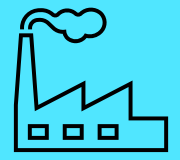


Ensimmäiset opit tulevaisuudessa puolustukseen

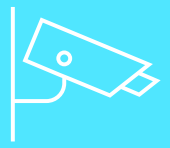
Microsoft on oppinut useita strategisia oppeja osallistumisestamme Ukrainan puolustamiseen

1. "Ei niin perusasioiden" merkitys
2. Jokainen sotaresurssi on kohde
3. Ihmisten ja luottamuksen kriittinen rooli
4. Tietojen jakamisella sekä julkisen ja yksityisen sektorin kumppanuuksilla on myönteinen vaikutus.

Sota-ajan painopisteet ja rauhan ajan valmius



Manufacturing companies
- Disrupt war production

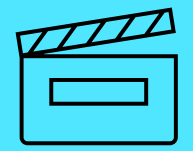


CCTV cameras
- Tactical view of the battlefield

Personal protective services
- Gain intelligence on VIPs

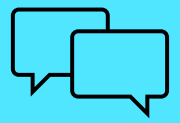
Natural resources
- Disrupt upstream war production

Industrial Controls
- Attacks against ICS systems associated with data centers



Electronic billboards
- Commandeered for news control

Logistics companies
- Gain picture/ disrupt support.



Communications & ISPs
- Disrupt comms. and info.

Local govs. along front lines
- Intel. gathering for occupation

Resiliency planning
- Migrate data outside borders

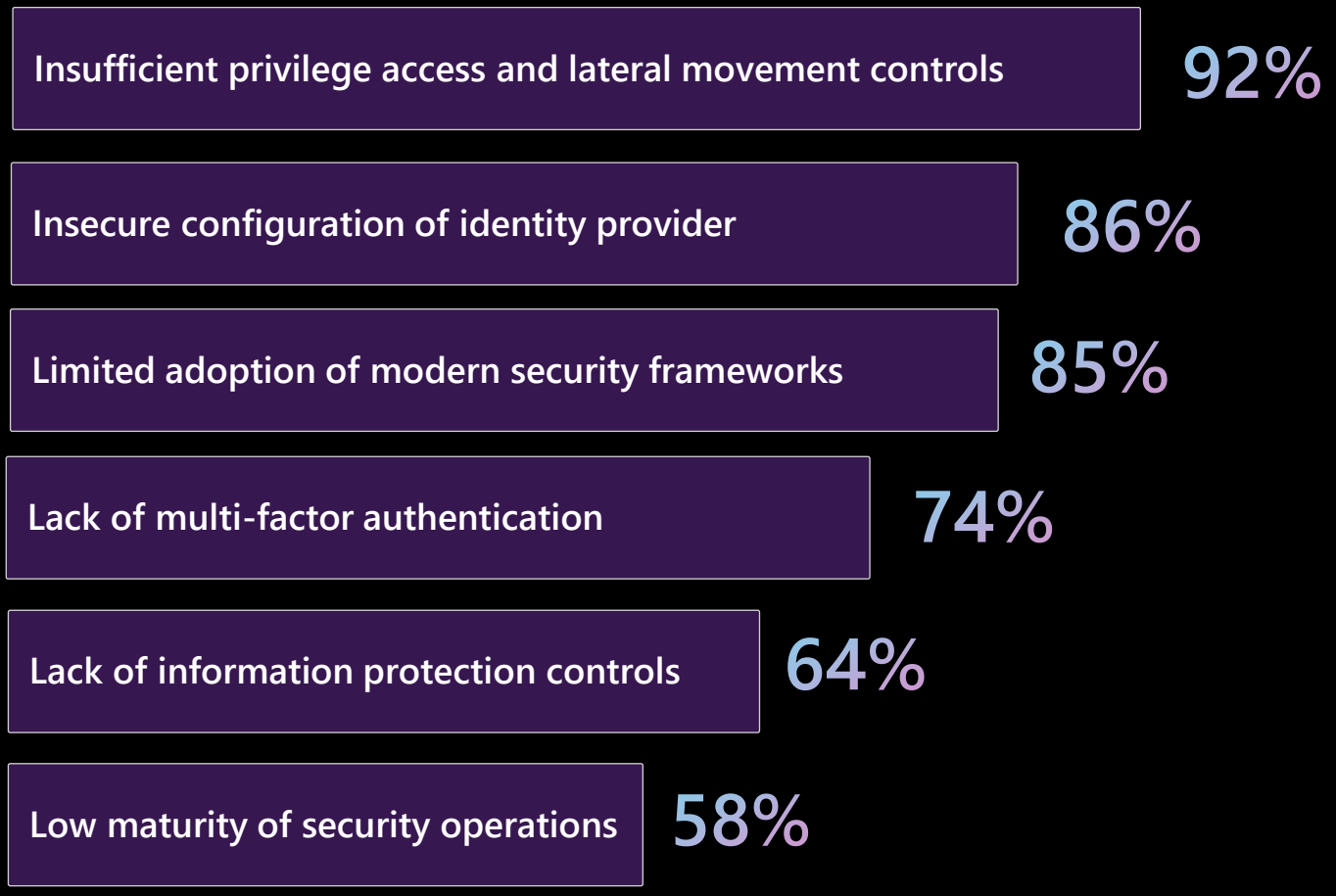
Keskeiset kyberuhkien sietokykyyn vaikuttavat asiat

How resilient is my organization?

80%

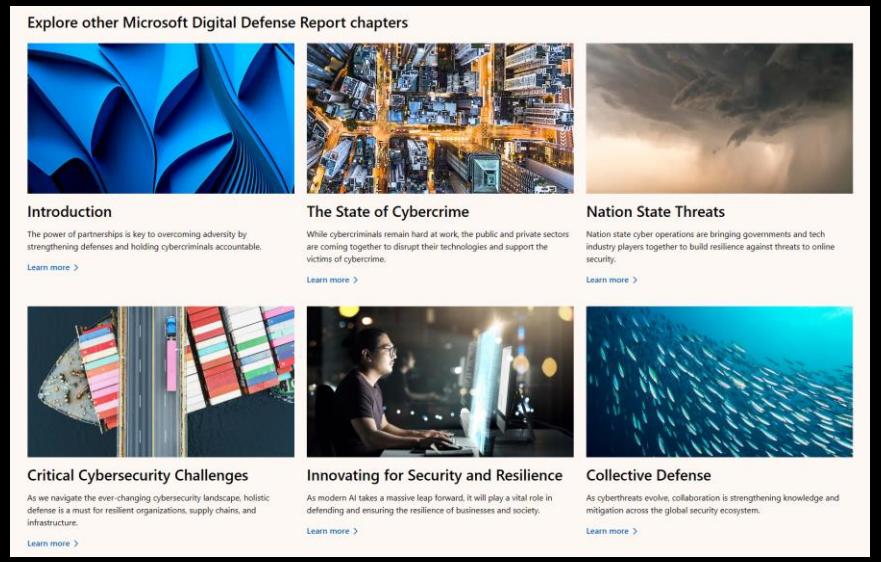
of incidents can be stopped by basic Security approaches (including Zero Trust, timely patching, MFA, and identity hygiene)

Microsoft studied victims of cyberattacks and found these factors to be the top 6 contributors to their vulnerability



Microsoft Defense Report https://microsoft.com/mddr

Viimeisin ilmestyi lokakuussa 2024



Muita raportteja:

Cyber Signals: Cyber signals Archives | Security Insider (microsoft.com)

Nation State reports: Reports | Security Insider (microsoft.com)

Kiitos