CENTRE FOR CYBER SECURITY BELGIUM

SANS | GIAC

What can we learn from the war in Ukraine?

KEVIN HOLVOET

SANS FOR578 Instructor

Lead of Threat Research Centre

Team of CyTRIS (Cyber Threat Research & Intelligence Sharing)

@digihash

kevinholvoet

kevin.holvoet@ccb.belgium.be

TLP WHITE

27 April 2022

Today's Agenda

Who is the Centre for Cybersecurity Belgium?

Attacks related to the war

What did we learn from the war?

Recommen -dations

Page 2

Who is the Centre for Cybersecurity Belgium? - Mission

Make Belgium one of the least cyber vulnerable countries in Europe

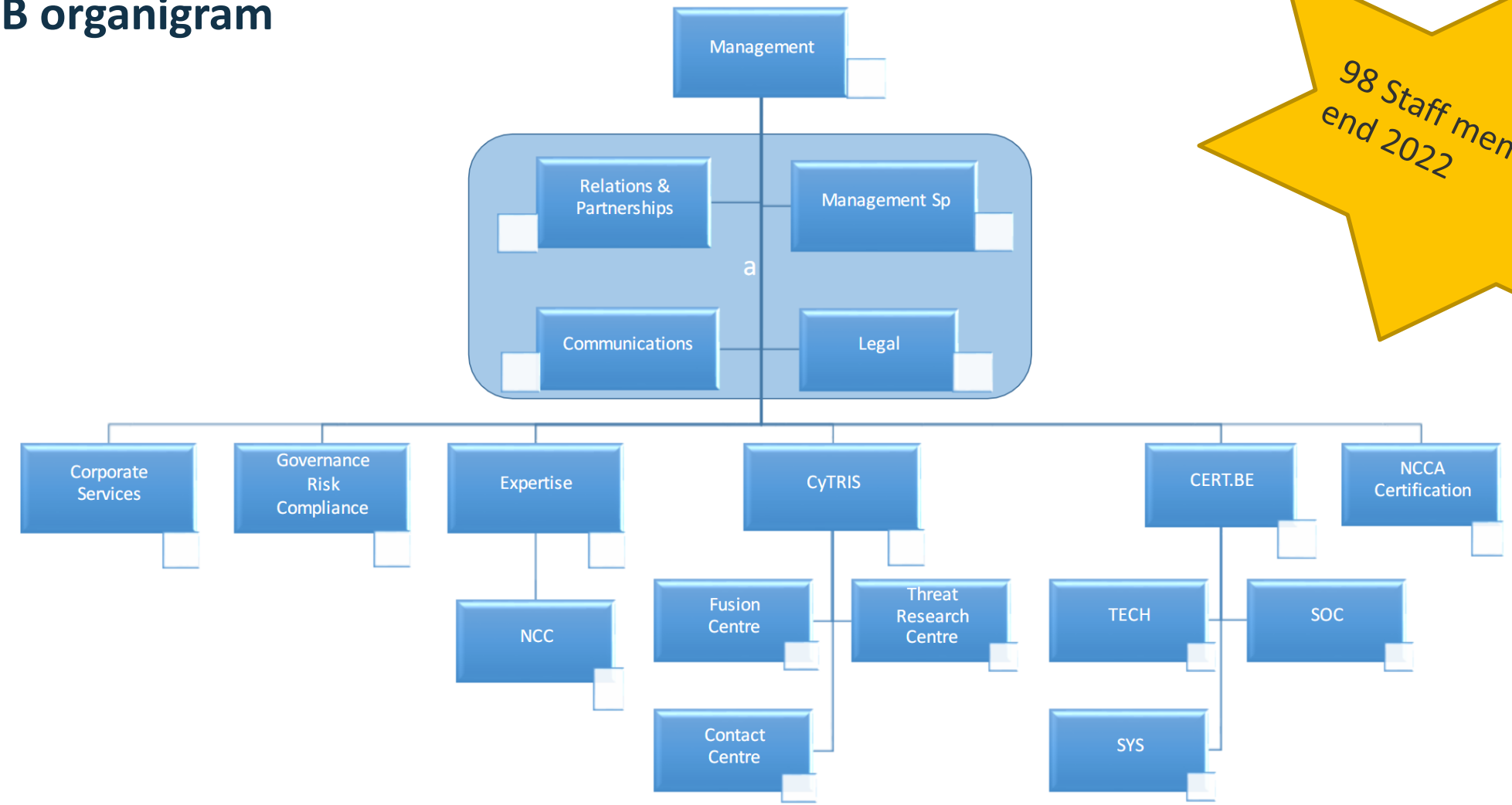
The task of CCB is to detect, observe and analyse online security problems, and to inform various target groups accordingly.

Nieuwsbericht 20 mei 2021

Een cyberstrategie 2.0 om van België een van de minst kwetsbare landen van Europa te maken

De Nationale Veiligheidsraad (NVR) heeft donderdag de details van de cybersecuritystrategie 2.0 goedgekeurd. Deze strategie vormt het kader voor de transversale aanpak door België van cyberdreigingen en -kansen voor ons land. Het moet van België een van de minst kwetsbare landen van Europa maken.

The CCB organigram



98 Staff members by end 2022

Example of ongoing operation – Ukraine / Russian war

Daily collection

- new geopolitical events
- new cyber attacks
- Underground chatter about the war

Evaluate impact of all events for Belgium

Collaboration

- European national certs
- Private companies
- International partners

Brief security & intelligence services in Belgium on a daily basis

Share Strategical / Operational / Tactical threat information with constituents

Overview of Cyberattacks on Ukraine

- 2015/2016: Power grid
  - Insufficient logging/monitoring
  - VPN access to OT environment without Multi-Factor Authentication
- 2017: NotPetya
  - **M.E. Doc** accountancy software spread inside the perimeter
- Wiper malware
  - Spread through GPO or standard Windows protocols (SMB, WMI)
  - No tight control on who can access the Domain Controller
  - **Controlled spreading. Lessons learned from NotPetya???**
  - WhisperGate (13 Jan)
  - HermeticWiper (23 Feb)
  - IsaacWiper (24 Feb)
  - Ukraine Border Control Station (25 Feb)
  - CaddyWiper (14 Mar)
  - DoubleZero wiper (17 Mar)
- **DDoS**
  - Users can't access organization's infrastructure => Can't work
  - Alternative communication plan???
  - Communication with customers?
- Influence operations / Disinformation
  - Causes confusion (what to believe?)
  - Creates tension
- **Supply Chain attacks**
  - Military comm issues due to Viasat KA-Sat modem attack
  - Defacement through Kitsoft admin access
- **Spear phishing**
  - Tailored phishing against specific targets
  - Using SPECTR, LoadEdge, and other malware against UA orgs
- **Attack on UA power company**
  - Industroyer2: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Is malware already PUT-IN place???

TLP WHITE

Important activity groups to track

- Sandworm (GRU): Destructive attacks since at least 2009
- APT28 (GRU): Espionage since 2004
- APT29 (SVR/FSB): Espionage since 2008
  - Lot's of spear phishing towards government in EU
- Turla (FSB): Linked to Moonlight maze from 1996
- DEV-0586: Destructive attack with WhisperGate Wiper
- Gamaredon: Targets Ukrainian government officials and organizations, aligned with Russian interests.
  - Past: off-the-shelf malware
  - Now: Custom developed malware per target
- UAC-0035 (InvisiMole): LoadEdge backdoor phishing
  - Allegedly ties to Gamaredon
- UNC1151 / Ghostwriter (Belarus APT)
  - Influence / Disinformation campaigns
- UAC-0088: DoubleZero Wiper attacks (5th wiper)

To make things more confusing…

GROUP	SUPPORTS	TYPE	COMMS	LOC
Anonymous Associated				
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia
LiteMods	Ukraine	Psyops/DDoS	Twitter	UNK
SHDWSec	Ukraine	Hackivism	Twitter	UNK
N3UR0515	Ukraine	DDoS	Twitter	UNK
PuckArks	Ukraine	Pysops	Twitter	UNK
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia
YourAnonNews	Ukraine	Psyops	Twitter	UNK
DeepNetAnon	Ukraine	Radio/hack	Twitter	UNK
Anonymous Younes	Ukraine	DDoS/Hack	Twitter	UNK
0xAnonLeet	Ukraine	DDoS/hack	Twitter	UNK
AnonGh0st	Ukraine	DDoS/Hack	Twitter	UNK
Anonymous Romania	Ukraine	DDoS/Hack	Twitter	Romania
Shadow_Xor	Ukraine	Databreach	Twitter	UNK
PuckArks	Ukraine	Defacement	Twitter	UNK
Squad303	Ukraine	DDoS/SMS	Twitter	Poland
Synthynt	Ukraine	Ransomware	Twitter	UNK
GhostSec	Ukraine	Hack	Telegram	UNK
DDoS Secrets	Ukraine	Databreach	Twitter	UNK
v0g3lSec	Ukraine	Hack	Twitter	UNK
Anonymous News	Ukraine	DDoS	Twitter	UNK
DoomSec	Ukraine	DDoS/Hack	Twitter	UNK
CyberNinja Security Team	Ukraine	Hack	Twitter	UNK
ReaperSec NEW	Ukraine	Hack/DDoS	Twitter	UNK
HAL9000 NEW	Ukraine	Hack/DDoS	Twitter	UNK
RedCult NEW	Ukraine	Hack/DDoS	Twitter	UNK
Nation-State				
GhostWriter UNC1151	Russia	Hack	UNK	Belarus
SandWorm	Russia	Hack	UNK	Russia
Gamaredon	Russia	Hack	UNK	Russia
DEV-0586 APT	Russia	Hack	UNK	Russia
DEV-0665 APT	Russia	Hack	UNK	Russia
FancyBear APT	Russia	Hack	UNK	Russia
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine
Internet Forces of Ukraine	Ukraine	Pysops	UNK	Ukraine
MustangPanda APT	UNK	Hack	UNK	China
Curious George	UNK	Hack	UNK	China

GROUP	SUPPORT	TYPE	COMMS	LOC
Pro-Ukraine Groups				
BlueHornetAPT49 (ATW)	Ukraine	Hack	Twitter	UNK
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK
GNG	Ukraine	DDoS	Twitter	Georgia
Spot	Ukraine	DDoS	Twitter	UNK
GhostClan	Ukraine	DDoS/Hack	Telegram	UNK
1LevelCrew	Ukraine	DDoS	Twitter	UNK
Hydra UG	Ukraine	Radio	Twitter	UNK
SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK
Ring3API	Ukraine	Hack	Twitter	Ukraine
Belarusian Cyber-Partisans	Ukraine	Ransomware	Twitter	Belarus
NB65	Ukraine	Ransomware	Twitter	UNK
Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey
Shadow_Xor	Ukraine	UNK	Twitter	UNK
The Connections	Ukraine	UNK	Twitter	UNK
Rabbit Two	Ukraine	Hack/DDoS	Twitter	UNK
SecDet	Ukraine	Hack	Twitter	US
BeeHive Cybersecurity	Ukraine	Phishing/hack	Twitter	UNK
Cyber_legion_hackers	Ukraine	Deface/DDoS	Twitter	UNK
Stand for Ukraine	Ukraine	hack/ DDoS	UNK	Ukraine
BrazenEagle (ATW)	Ukraine	Hack	Telegram	UNK
Bandera Hackers	Ukraine	Hack/DDoS	Twitter	UNK
HackenClub	Ukraine	DDoS/hack	Twitter	Ukraine
Pro-Russia Groups				
RedBanditsRU	Russia	Hack	Twitter	Russia
Stormous Ransomware	Russia	Ransomware	Telegram	UNK
Hydra	Russia	Dox/DDoS	Twitter	Russia
RaHDit	Russia	Hack	UNk	Russia
Xaknet	Russia	Hack	Site	Russia
Killnet	Russia	Hack/DDoS	Telegram	Russia
404 Cyber Defense	Russia	DDoS	Twitter	UNK
WeretheGoons	Russia	Hack	Twitter	Russia
punisher_346	Russia	PsyOps	Twitter	UNK
Lorec53	Russia	Hack	UNK	Russia
DDoS Hacktivist Team	Russia	DDoS	Telegram	Russia
cyberwar_world	Russia	Hack/ddos	Telegram	Russia
Zsecnet NEW	Russia	Hack/DDoS	Telegram	Russia
DivisionZ NEW	Russia	Hack/DDoS	Telegram	Russia

For real-time updates:
https://twitter.com/Cyberknow20

Cyberattacks related to the war

- List of Western companies operating in Russia
  - https://som.yale.edu/story/2022/over-750-companies-have-curtailed-operations-russia-some-remain

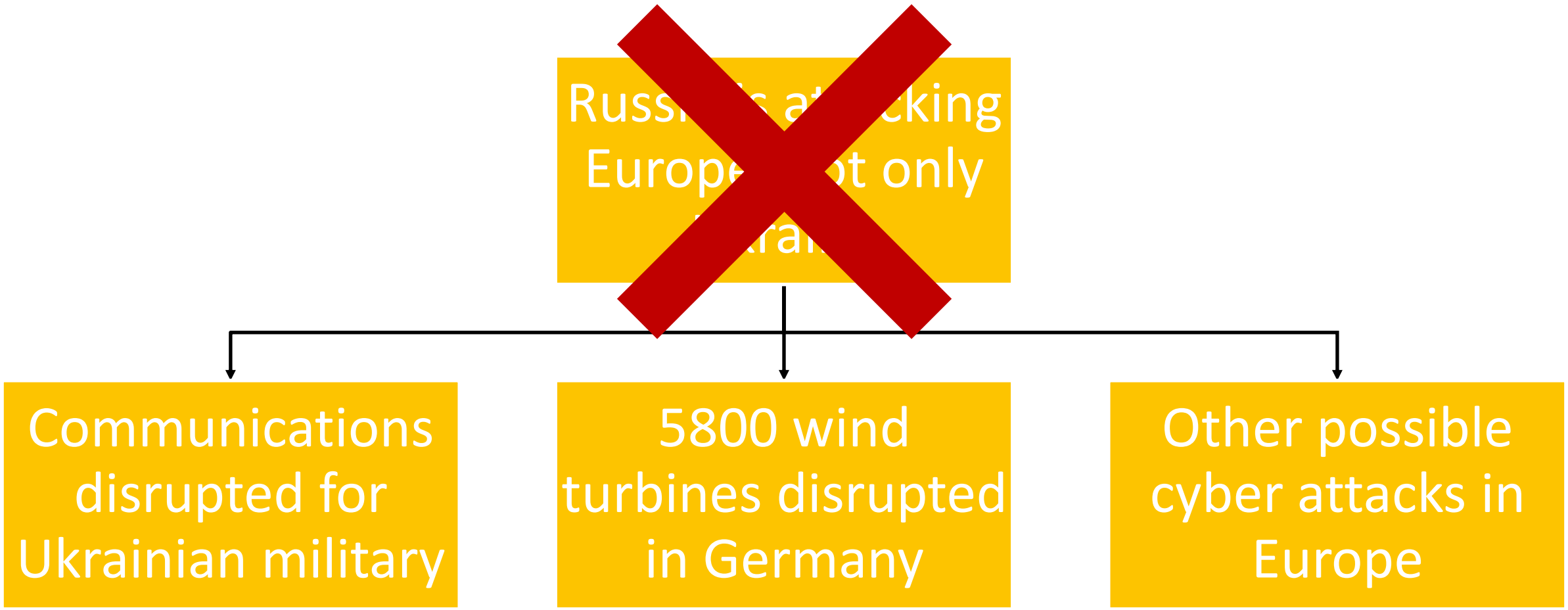
Cyberattacks related to the war

- Over 6 million Russian documents published
- Both government and private organisations in Russia are victimized by data leaks
  - DDoSecrets

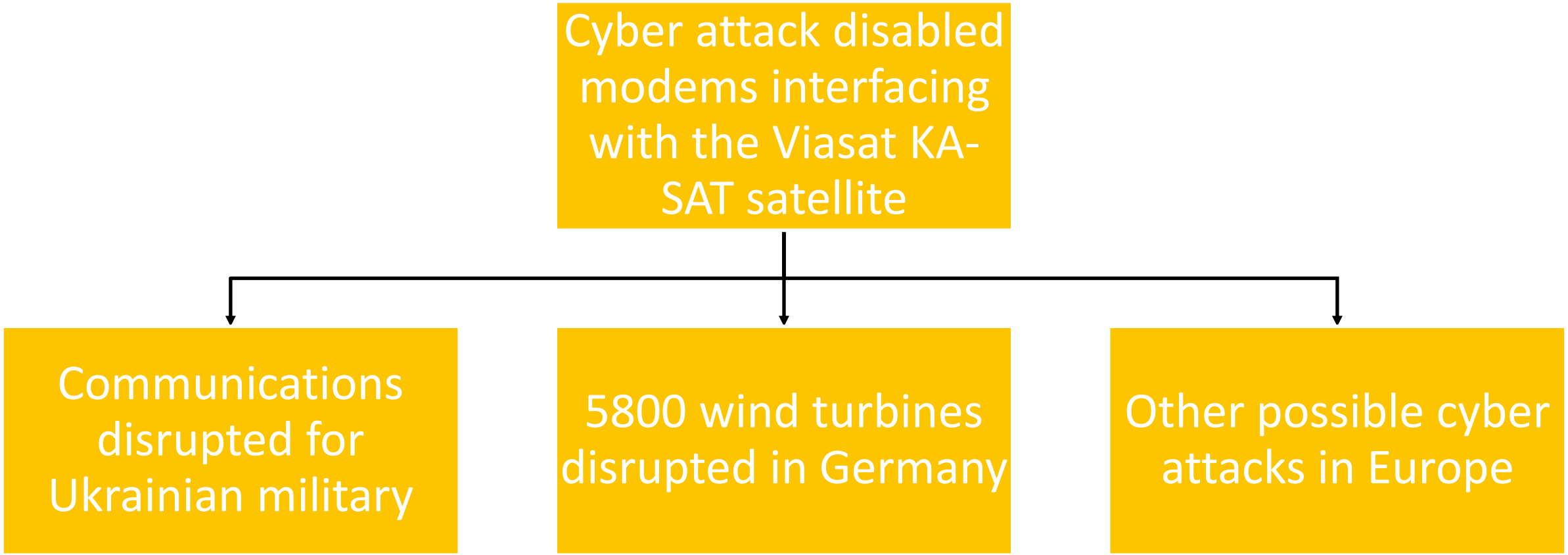
- Doxing of Russian military and intelligence personnel
  - https://gur.gov.ua/ua/content/list-of-news/

MAIN INTELLIGENCE DIRECTORATE OF THE MINISTRY OF DEFENSE OF UKRAINE

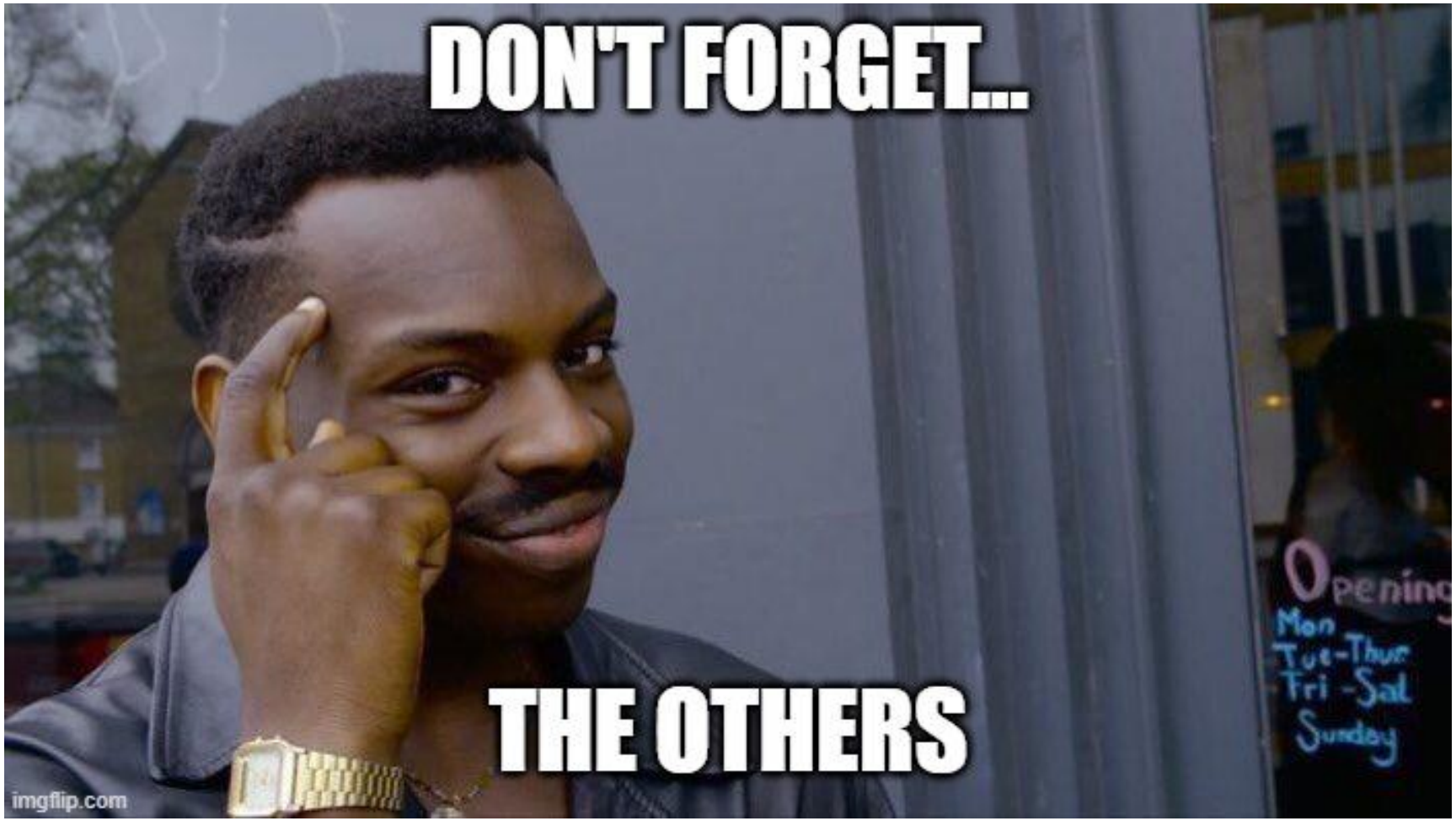
Correlation is NOT Causation BIAS



Correlation is NOT Causation BIAS



Russia is not the only one



Important activity groups to track – The Others

- Espionage
  - Initial access and info gathering through spear phishing targeting government and military individuals in EU / US
    - TA416 (or Mustang Panda, RedDelta)
    - APT31
  - Chinese People's Liberation Army (PLA) and other Chinese intelligence agencies
- Supply chain compromise
  - SolarWinds, Kaseya, NPM package compromises, Log4J in some cases (VMware Horizon)
  - NPM package compromised: https://jfrog.com/blog/large-scale-npm-attack-targets-azure-developers-with-malicious-packages/
  - Okta
- Financially-motivated
  - TA551
- Ransomware
  - Conti (see leak to learn), BlackCat (ALPHV), LockBit 2.0
  - TheHive, Vice Society, Grief

General threats

- Mobile malware on Android
  - FluBot
  - TeaBot
  - Medusa
  - Xenomorph
- Initial Access Brokers
  - Qbot
  - Bazar
  - IcedID
  - Emotet
  - TrickBot
- Abuse of Remote Monitoring and Management (RMM) software

- Common malware
  - Cobalt Strike
  - Mimikatz
  - Impacket
  - SocGholish
  - Yellow Cockatoo
  - Gootkit
  - Bloodhound

What did we learn from the war?

Focus on targeted country by Russia

Information warfare used by both sides

Most attacks were preceded by prior information collection campaigns

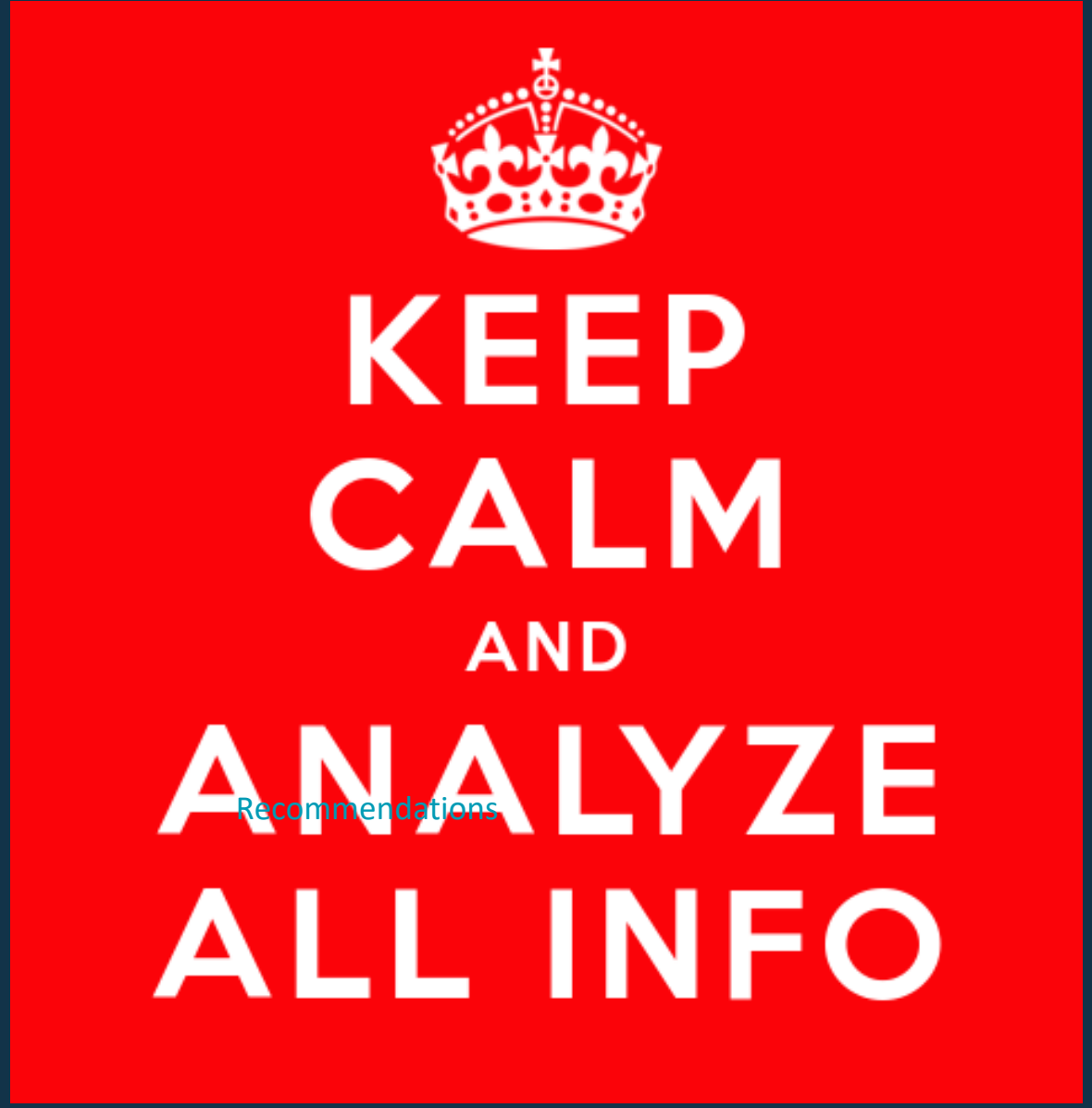
- Could have been discovered by monitoring and defences already in place

Criminals and hacktivists align with one or the other side

- But make their own decisions on who to target, see Anonymous…

Public decisions by countries or companies can change the hostile intent of actors

- Companies continuing operations in Russia targeted by Anonymous
- Stormous ransomware gang targeting French organisations because of a president's speech
- Fibre optic cables cut causing internet issues in multiple French cities???



Recommendations

Recommendations (1) – Plan and look beyond Cyber

- Stick with your security plan!
  - https://cyberguide.ccb.belgium.be/en
  - https://www.cisecurity.org/controls/cis-controls-list
  - https://www.cybersecuritycoalition.be/resource/incident-management-guide/
  - https://www.disasterrecoveryplantemplate.org/download/business-continuity-plan-template/
- Connect with your national CSIRT before PEEEEEP
- Intel teams should not only focus on cyber events
  - Sit together with risk management and learn from each other
  - Geopolitical events
  - Warnings towards your sector/region/country

Recommendations (2) – Focus on threats to YOUR organization

- Collect on important Activity Groups for your organization
  - Based on your own intrusions → build your own activity groups
  - Public/private reports on attacks against your sector/country/type of organization
- Sources
  - https://attack.mitre.org/groups/
  - OSINT
  - Commercial Intel vendor (focused on your kind of organization)
- Build defenses using
  - https://attack.mitre.org/
  - https://github.com/rabobank-cdc/DeTTECT
  - https://d3fend.mitre.org/
  - SANS FOR578: Cyber Threat Intelligence

Recommendations (2) – Focus on threats to YOUR organization

- Implement shared IOCs in your defences (MISP)
- Implement Mitigations and Detections based on MITRE ATT&CK techniques shared (MISP / OpenCTI)
- Example: Spear phishing with attachment, link through trusted channel (T1566.003):
  - Compromised account of colleague, contact, customer, or friend used to send phishing by
    - Mail, LinkedIn chat, WhatsApp, Facebook, Instagram

Mitigations

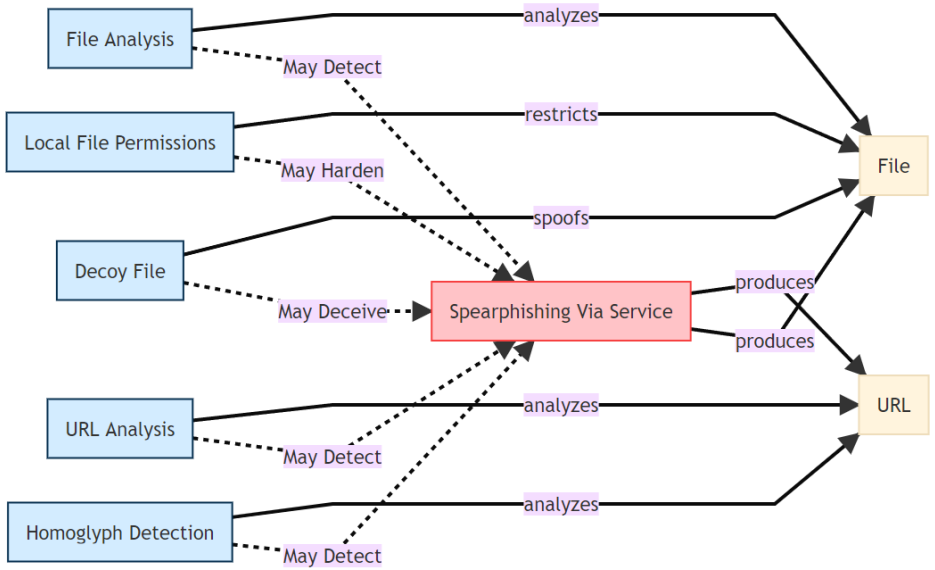
ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
M1021	Restrict Web-Based Content	Determine if certain social media sites, personal webmail services, or other service that can be used for spearphishing is necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1017	User Training	Users can be trained to identify social engineering techniques and spearphishing messages with malicious links.

Recommendations (2)

Spearphishing Via Service - T1566.003

D3FEND Inferred Relationships

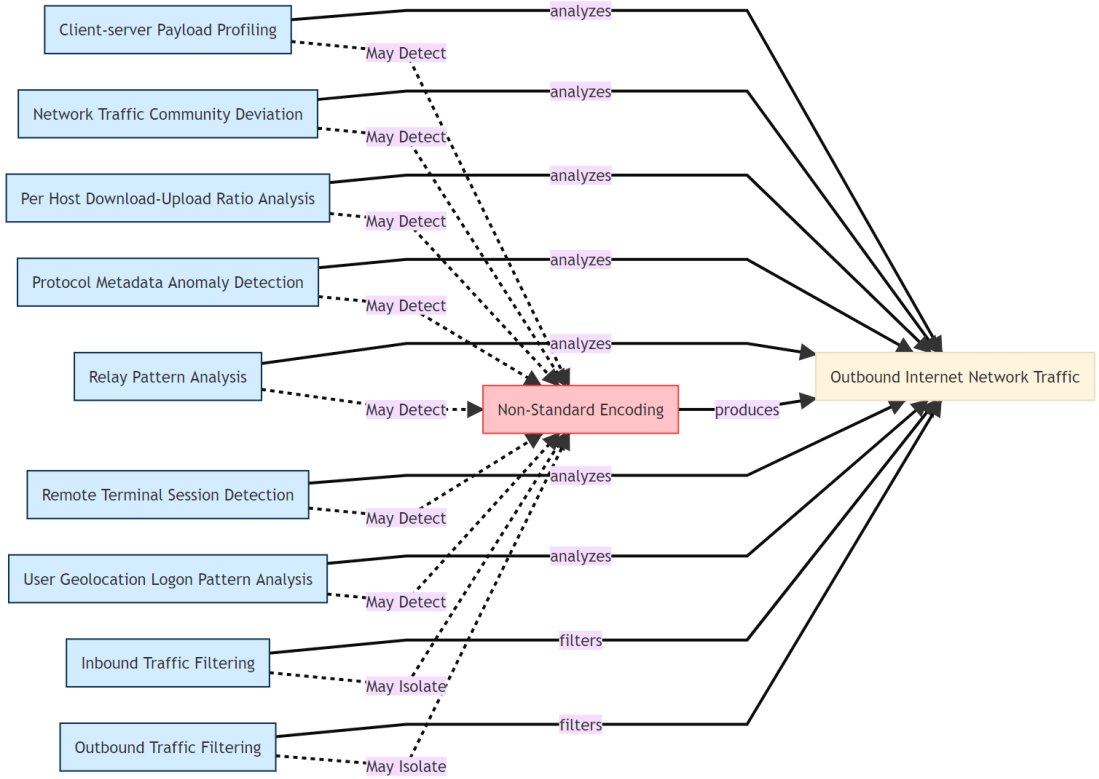
Browse the D3FEND knowledge graph by clicking on the nodes below.



Non-Standard Encoding - T1132.002

D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.



Recommendations (3)

- Know yourself
  - Baseline network and endpoint usage
  - Asset management
  - Threat model your attack surface
- Focus on the user, not your perimeter defences:
  - Perform OSINT check on your organization/most important employees (agree with HR 😜)
  - EDR/XDR on all endpoints: remote management, log collection, contain infected endpoints
- Detect anomalies using SIEM / Behaviour analytics
- Automate defences with SOAR

Recommendations (4) – SLEEP

Employee training

- Employees need to realize that they are a weakness to
  - Themselves
  - The organisations they work for
  - Their family, friends, and colleagues
  - If you don't care about your own data and safety, do it for others!!!
- Train your employees to be vigilant everywhere (also at home)
  - Password hygiene (free password database subscription for all employees?)
  - Use MFA everywhere, also on personal mail/SM profiles!!!
  - Report suspicious mails to suspicious@safeonweb.be
  - Report strange behaviour to your security department
  - Report others ignoring policy to your security department

Questions?

KEVIN HOLVOET
SANS FOR578 CTI Instructor
Lead of Threat Research Centre
Team of CyTRIS
kevin.holvoet@ccb.belgium.be
https://www.linkedin.com/in/kevinholvoet/
@digihash

UPCOMING: Online CCB Share & Connect event on 4 May 2022

Subscribe on: https://app.livestorm.co/ccb/