mnemonic

Cyber Threat Landscape

Strategic review of 2021 and reflections on the Ukraine crisis

Presented by Bjørn Rasmussen
Mnemonic MSS - Threat Intelligence

TLP:WHITE

Agenda

1. Cyber threat landscape
   – Significant developments and trends from the previous year
2. Ukraine from a cybersecurity perspective
   – Observations and consequences

Observations and trends from last year

Cyber threat landscape

Nutrition Facts

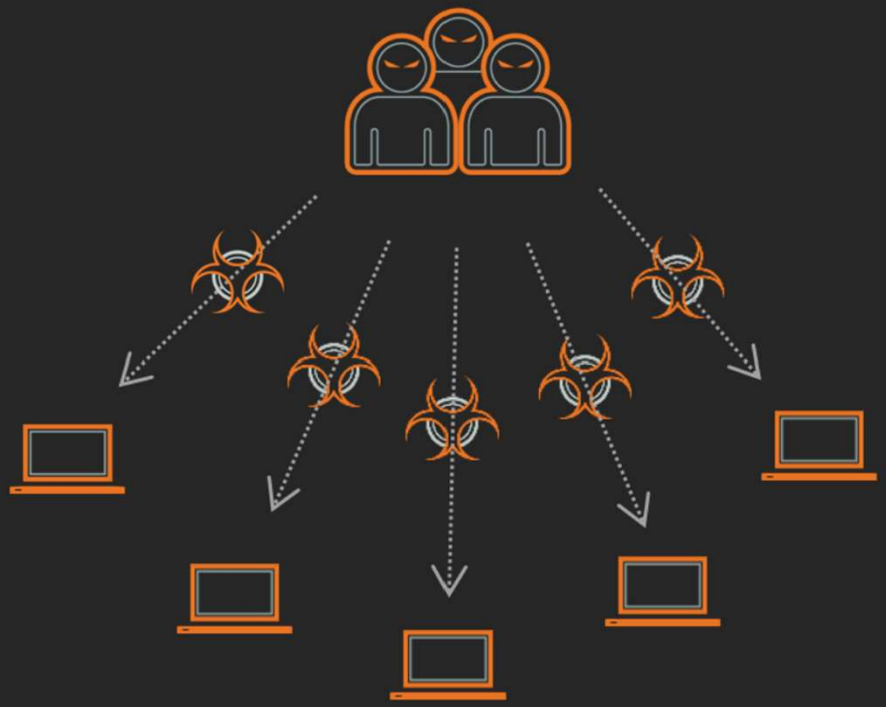
8 servings per container
Serving size **2/3 cup (55g)**

Amount per serving
Calories **230**

	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%

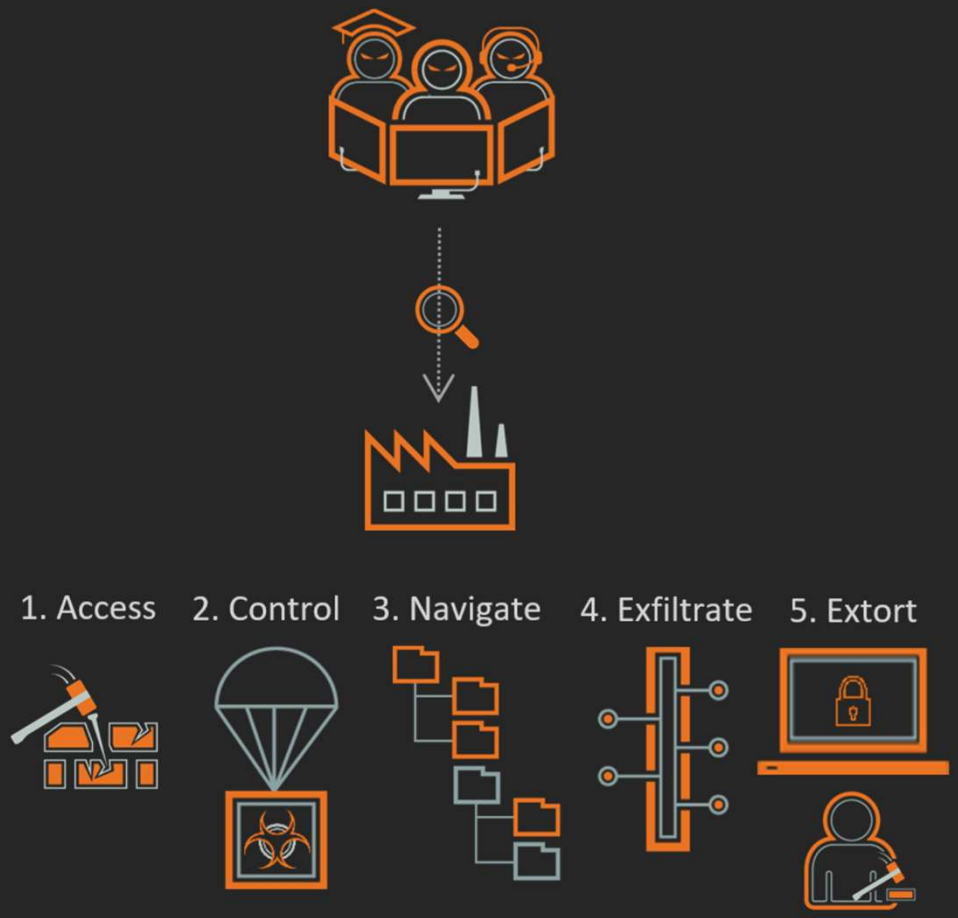
- 60%: Cybercrime professionalized
- 10%: Nation-state attacks
- 30%: Initial access methods

Cyber threat landscape | Cybercrime professionalized



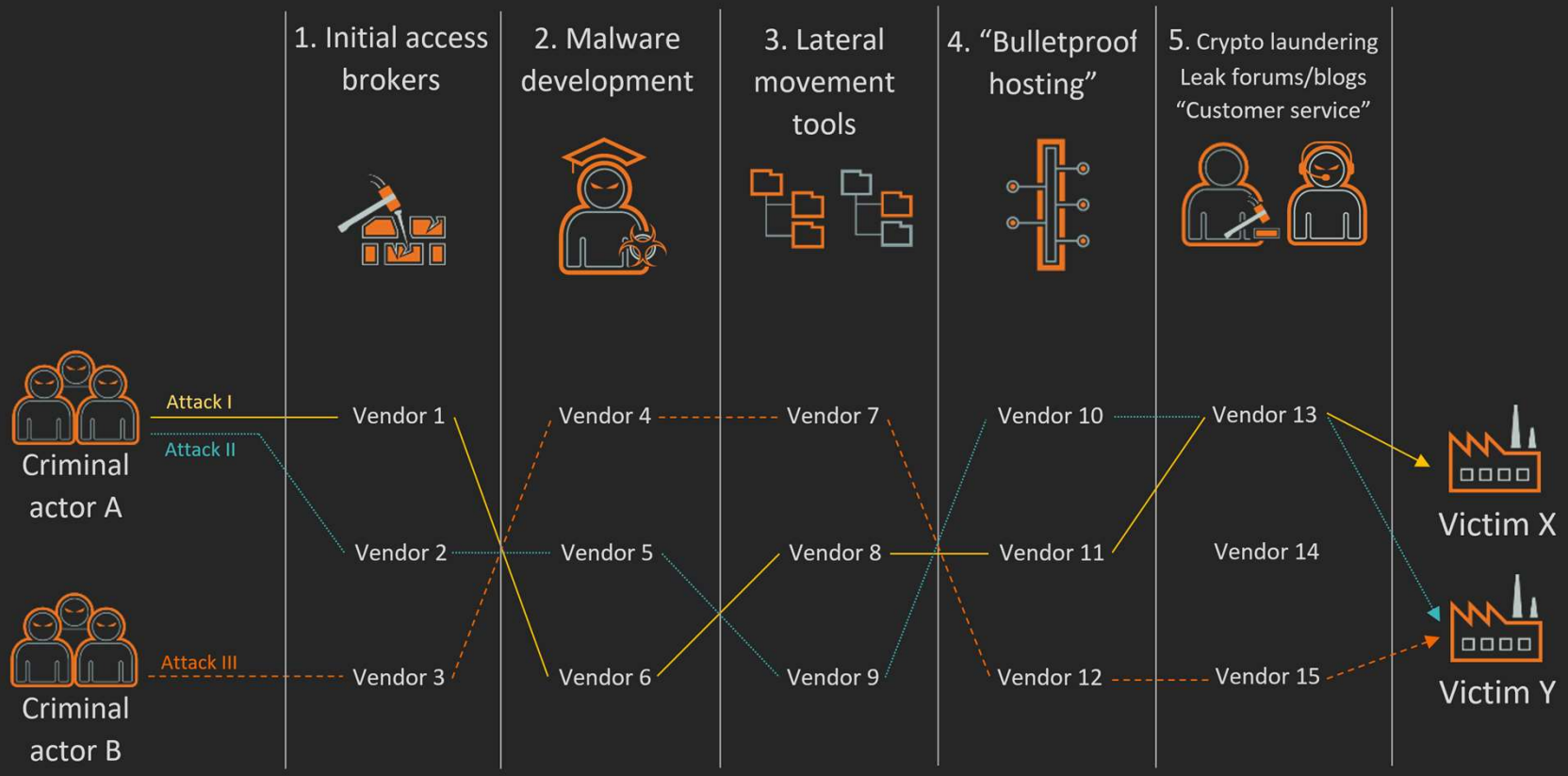
- Previously: «Shotgun» approach
- More users impacted -> higher profit
- Quantity over quality of attacks
- Little to no target discrimination
- Success dependent on some human response (social engineering)
- Relatively low hit-rate

Cyber threat landscape | Cybercrime professionalized



- Recent years: «Big game hunting» approach
- Research and targeting organizations, not individuals.
  - Opportunity, profitability
- Relies on executing several phases, in order.
- Requires wider set of skills, more people – **or does it**...?

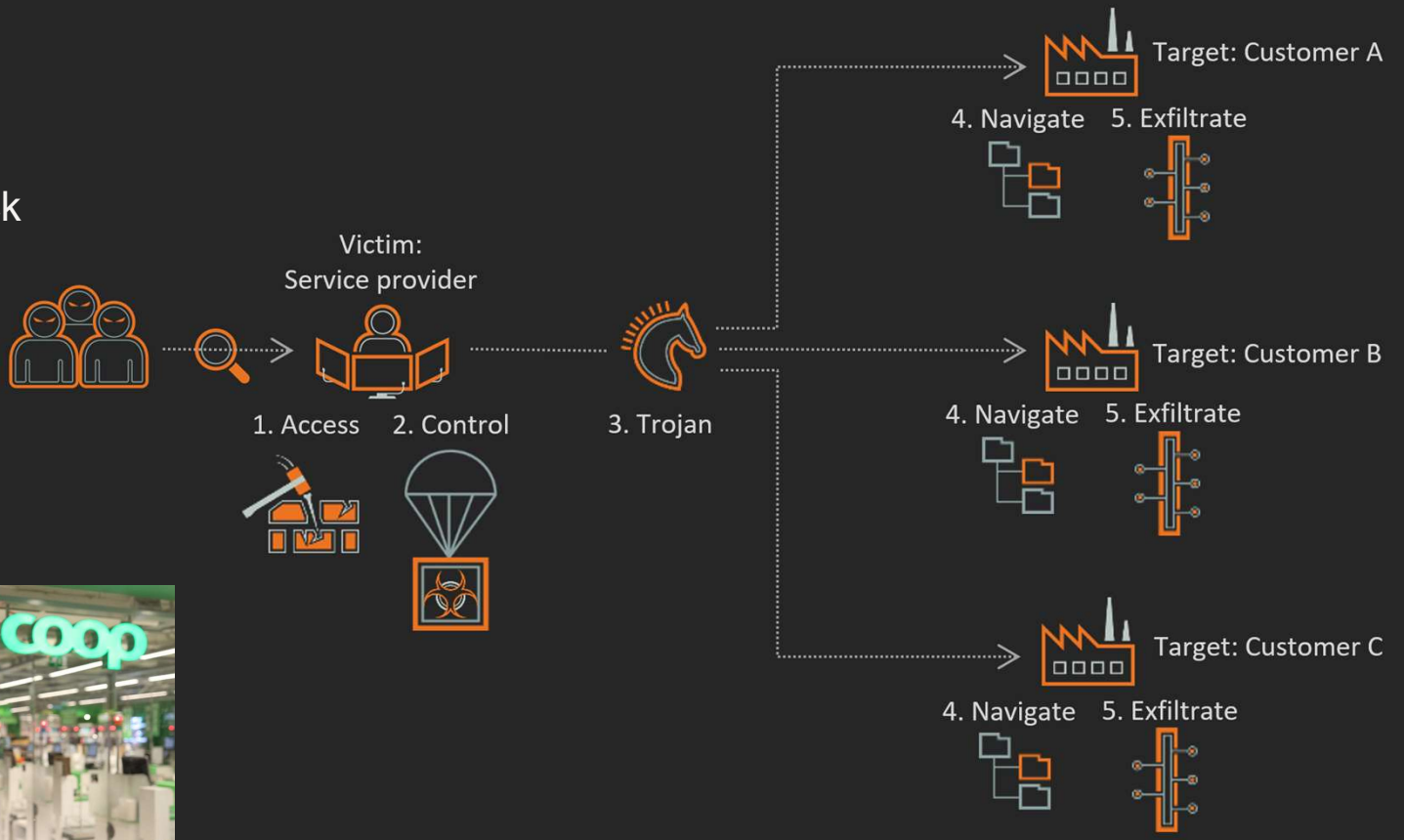
Cyber threat landscape | Cybercrime professionalized



mnemonic

Cyber threat landscape | Nation-state attacks

- The implications of SolarWinds
  - Supply chain attacks
- Criminals with supply chain attack capabilities?
  - Kaseya



solarwinds

mnemonic

Cyber threat landscape | Initial access methods

Phishing

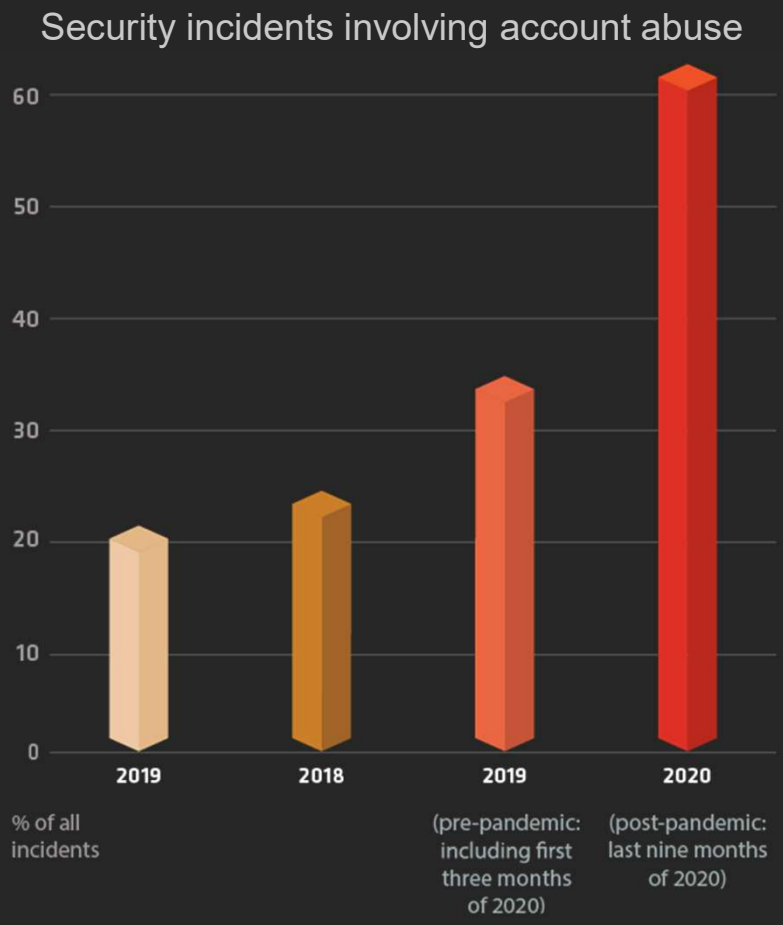
- Oldie but goldie – first phishing attack in 1995 – still prevalent and effective
- Degree of sophistication very variable
- If your security depends on no-one falling for phishing, then you have bad security…

Outcomes of successful phishing e-mails (Proofpoint, 2021)

Cyber threat landscape | Initial access methods

Account login abuse

- Pandemic pushes implementation of remote work
- Rising trend of attackers gaining access through the abuse of user and administrator credentials
- Correlation to the increasing adoption of cloud services
- Identity is the new perimeter



“Since the Russian aggression in 2014, this unit has carried out over 5,000 cyber attacks and attempted to infect over 1,500 government computer systems. They are officers of the ‘Crimean’ FSB and traitors who defected to the enemy during the occupation of the peninsula in 2014.”

- SSU Gamaredon report, November 4th, 2021

Ukraine from a cybersecurity perspective

Ukraine from a cybersecurity perspective | Key observations

Past: Pre-invasion

How long had Russia planned this?

What kind of preparations?

Present: Armed conflict

Spillover

Hacktivism

Targeting of OT-networks

Future: Post-war consequences

Russian government vs. economic sanctions?

Ukrainian hacktivists vs. aftermath of war?

Ukraine from a cybersecurity perspective | Past preparations

Apr. 13
Wiper malware code signing certificate issued

Oct. 19
Isaac Wiper compiled

Dec. 28
Hermetic Wiper compiled

Jan. 13-14
"Whispergate" Ukraine govt. assets wiped, 70+ websites defaced

Feb. 15
DDoS attacks Ukraine Defense Ministry and large banks

Feb. 23
Hermetic Wiper deployed

Feb. 24
Isaac Wiper deployed

2021 | 2022

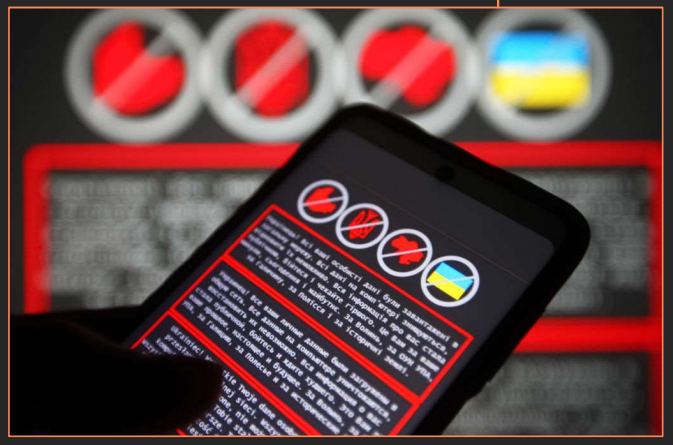
Feb. 24
Ukraine invaded

Hermetica Digital Ltd.

- One-man game dev. company in Nicosia, Cyprus

Legitimate certificate from real company

- Malicious "wiper"-malware impersonating legitimate software



Destructive wiper malware posing as ransomware

- Fake ransom notes demanding $10,000 in Bitcoin

False flag defacement

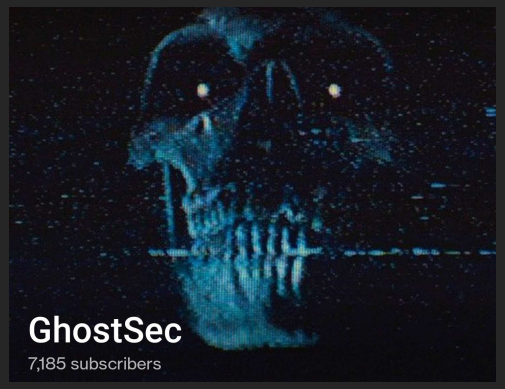
- Defacement message included Polish anti-Ukrainian slogans

Present conflict

Spillover

- Attackers gained access via misconfigured VPN to Viasat European management network.
- Disabled modems connected to the Viasat satellite covering Europe.
- Not attributed yet, but:
  - Same time as invasion (Feb. 24th)
  - Viasat com vendor to Ukrainian military and police units?
- Remote monitoring and control systems of approx. 6000 wind turbines in Germany offlined.
- 30.000 satellite modems of Viasat customers across Europe replaced (so far).

Hacktivism



Death by 1000 needles
Good evening, we are from Ukraine! This is an instruction manual for those who want to provide their computers to the centralized management of the Ukrainian IT Army, so that the power of your device can be used to help Russian websites follow the "Russian warship". Death by 1000 needles Our great friends have developed db1000n - a solution that allows the list of destinations to change automatically from the main

Present conflict

Targeting of OT-networks

April 1st - “PIPEDREAM” aka. “INCONTROLLER”

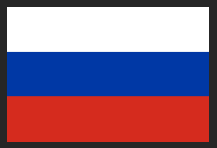
- Built to target specific PLCs from Schneider Electric and Omron, as well as OPC UA servers
- Consist of 3 different Python frameworks
- May disrupt, sabotage, and potentially cause physical destruction to ICS components
- Exploits commonly used modbus protocol to target PLCs
- Very rare and dangerous cyber attack capability. Comparisons to TRITON (2017), INDUSTROYER (Ukraine 2016) and STUXNET (Iran 2010)

April 12th - “INDUSTROYER2”

- Code overlap with the INDUSTROYER malware used by Sandworm on the Ukrainian power grid in 2016
- Only IEC-104 protocol supported
- Deployed in the ICS network as a scheduled task executing on Friday evenings
- Followed by CaddyWiper for anti-forensics

Future consequences

«Necessity is the mother of invention»



Western economic sanctions:
- Energy
- Finance

+

Russian Federation offensive cyber capabilities

=

State-sponsored attacks:
- Targeting energy and finance sectors.
- Disruption and profit, rather than intelligence.

Large number of hacktivists engaged by the war

+

Post-war shortages:
- Goods and services.
- Short-term income.
- Long-term unemployment.

=

Cybercrime:
- Increased recruitment.
- Synergy with cybercrime as a service.

mnemonic

Thank you!

bjornr@mnemonic.no

Please visit mnemonic.io
or follow us at

- @mnemonic
- @mnemonic_sec
- mnemonic.no/podcast
- github.com/mnemonic-no
- youtube.com/c/mnemonic/

References

1. https://www.mnemonic.no/security-report-2021/
2. https://www.justice.gov/usao-wdwa/pr/citizen-kazakhstan-known-fxmsp-charged-computer-fraud-wirefraud-and-conspiracy-hacking
3. https://go.chainalysis.com/2022-Crypto-Crime-Report.html
4. https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish/
5. https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise
6. https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy
7. https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
8. https://www.reuters.com/world/europe/cyprus-games-writer-denies-links-malware-found-before-russian-invasion-2022-02-24/
9. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
10. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/
11. https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
12. https://www.reuters.com/business/media-telecom/exclusive-hackers-who-crippled-viasat-modems-ukraine-are-still-active-company-2022-03-30/
13. https://www.cisa.gov/uscert/ncas/alerts/aa22-103a