Cyber Fortress Enterprise

CYBER FORTRESS
ENTERPRISE

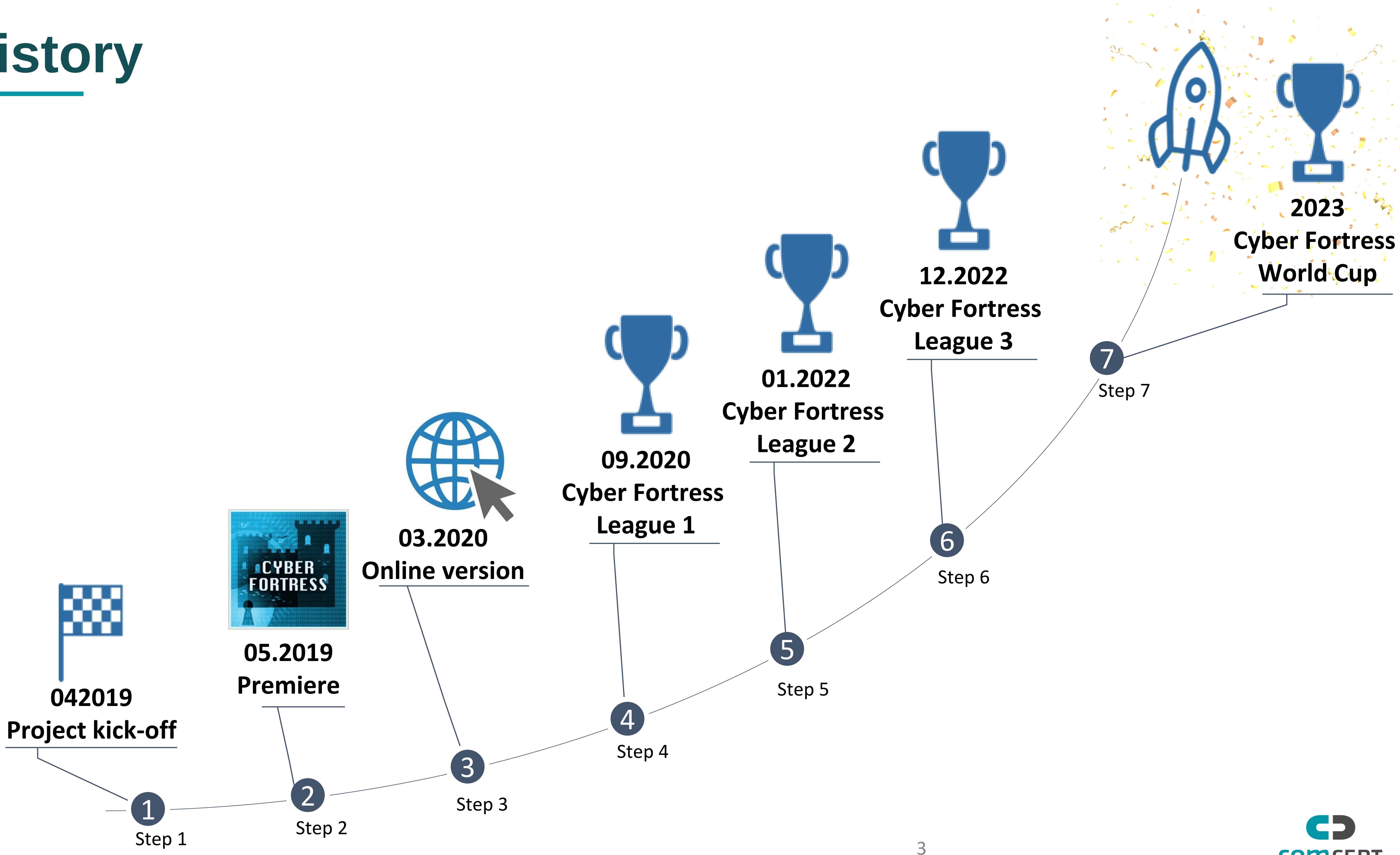
comCERT

Agenda

I.	13:30 – 13:45	Game History
II.	13:45 – 14:10	Introduction (concept, navigation, rules)
III.	14:10 – 14:50	1st Game Session
IV.	14:50 – 15:00	Summary of the 1st Game Session
VI.	15:00 – 15:30	Coffee Break
VII.	15:30 – 15:45	Introduction (2nd Game Session)
VIII.	15:45 – 16:35	2nd Game Session
IX.	16:35 – 16:45	Summary of the 2nd Game Session
X.	16:45 – 16:50	The Cyber Fortress Enterprise
XI.	16:50 – 17:00	Results & Rewards

comCERT

History



042019
Project kick-off

Step 1

05.2019
Premiere

Step 2

03.2020
Online version

Step 3

09.2020
Cyber Fortress
League 1

Step 4

01.2022
Cyber Fortress
League 2

Step 5

12.2022
Cyber Fortress
League 3

Step 6

2023
Cyber Fortress
World Cup

Step 7

History

Premiere 2019 – Polish Naval Academy, Summer Cybersecurity School

History

Hybrid version 2021

History

https://youtu.be/aPEZUnKSaEI

Cyber Fortress

Cyber Fortress is a strategic simulation game which main idea and the task is to build the best cybersecurity system to prevent players' organizations against the most likely threats and to effectively react during the incident mitigation phase

Safeguards represent cybersecurity measures that come from four main areas:

organizational
(CERT, SOC team, ...)

procedural
(incident response procedure, ...)

technical
(SIEM, anty-DDoS, ...)

data sources

CYBER FORTRESS
ENTERPRISE

comCERT

Cyber Fortress

Cyber Fortress is based on:

- VERIS Framework (http://veriscommunity.net/)
- MITRE ATT&CK Framework (https://attack.mitre.org/)
- Bow-Tie Risk Assessment model
- Defense-in-Depth model

CYBER FORTRESS
ENTERPRISE

comCERT

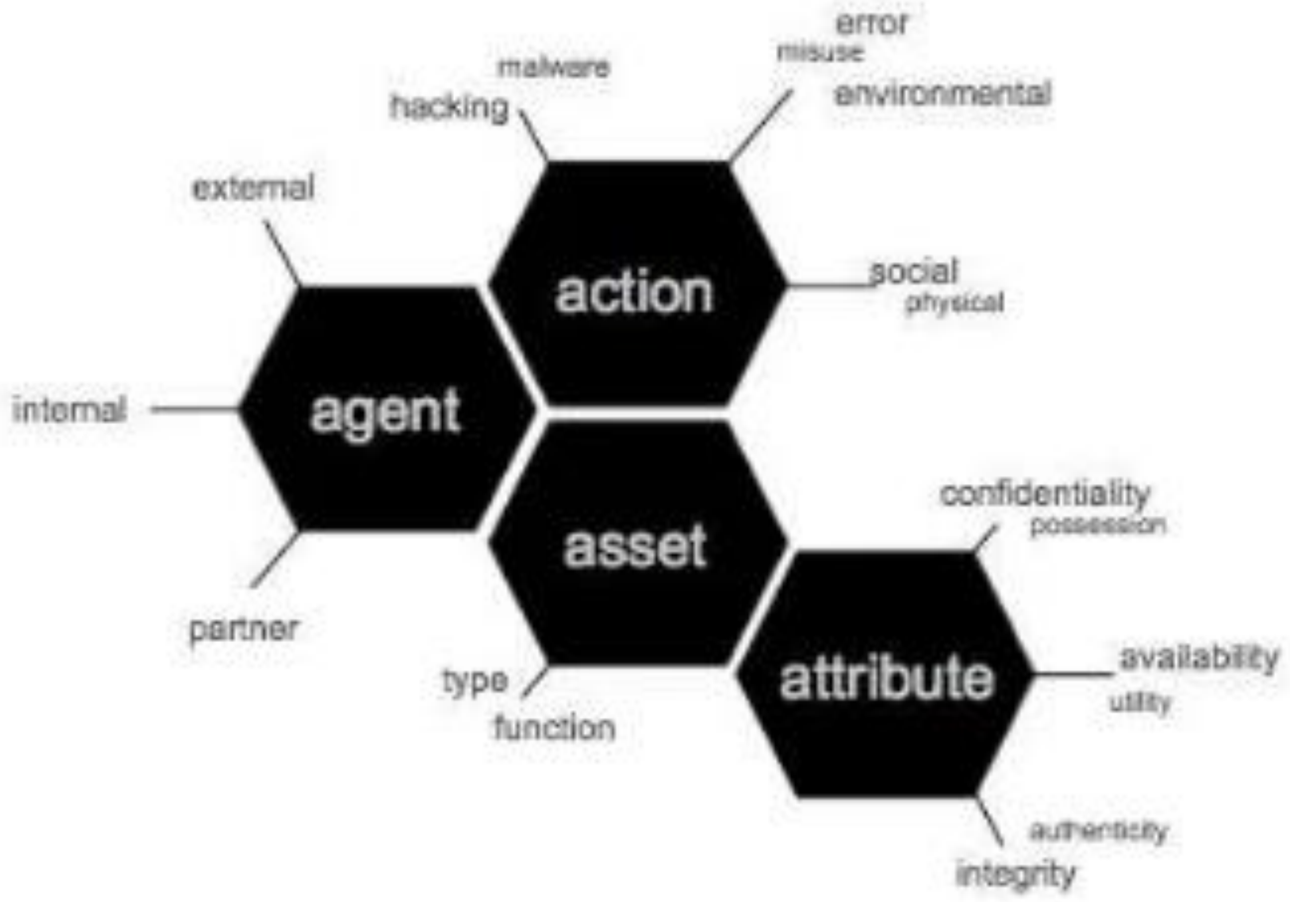
Cyber Fortress - VERIS Framework

VERIS Framework - a dictionary for recording events and sharing event information, a set of metrics designed to provide a common language for describing security events in a structured and repeatable way.

Kick-off: **2010 r.**

Project sites:

- https://github.com/vz-risk/veris
- http://veriscommunity.net/



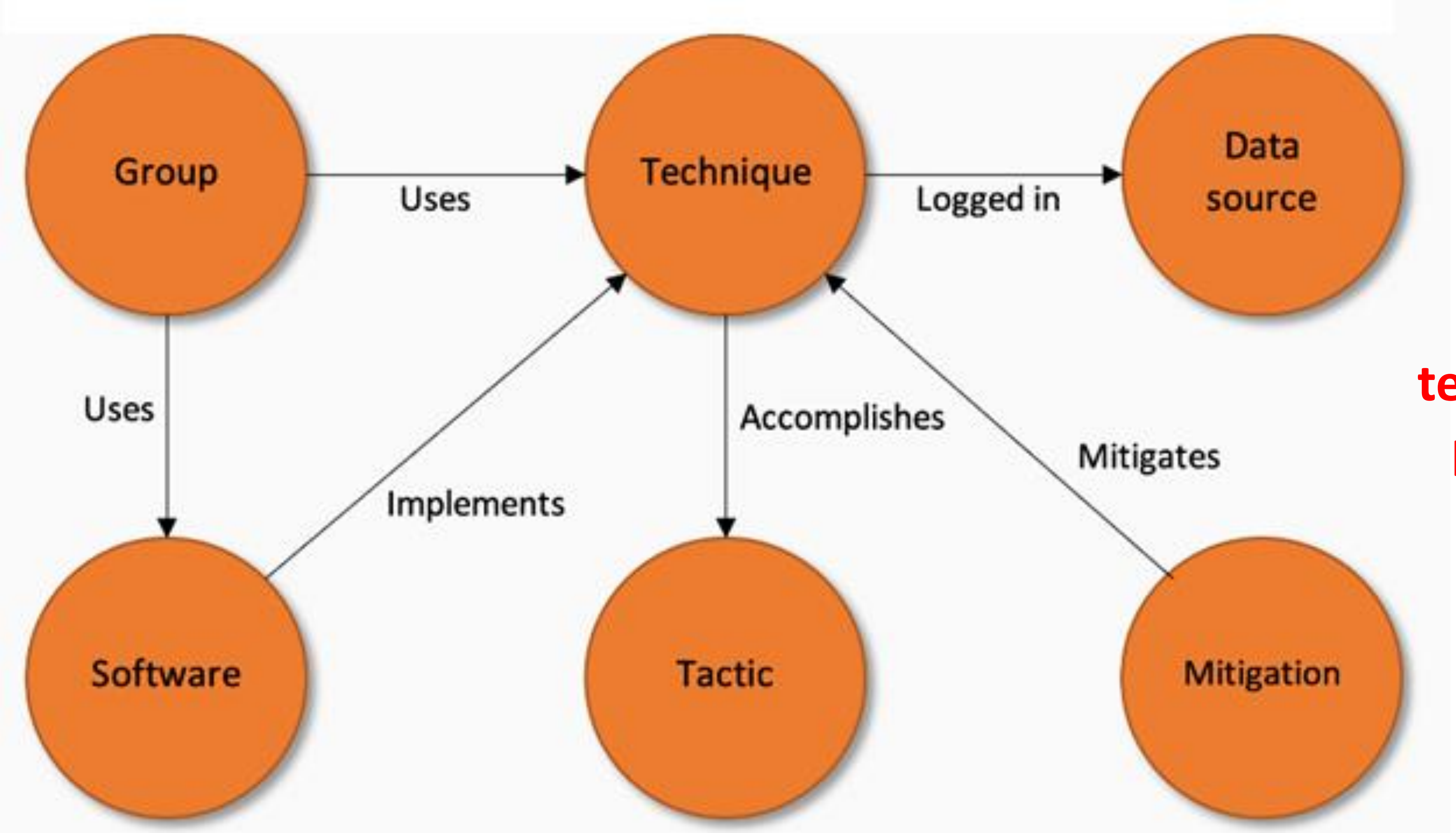
Cyber Fortress – MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Framework (https://attack.mitre.org/) - a structured, globally accessible knowledge base of tactics, techniques and procedures that are used by attackers, continuously updated and developed by a community of cyber security professionals.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

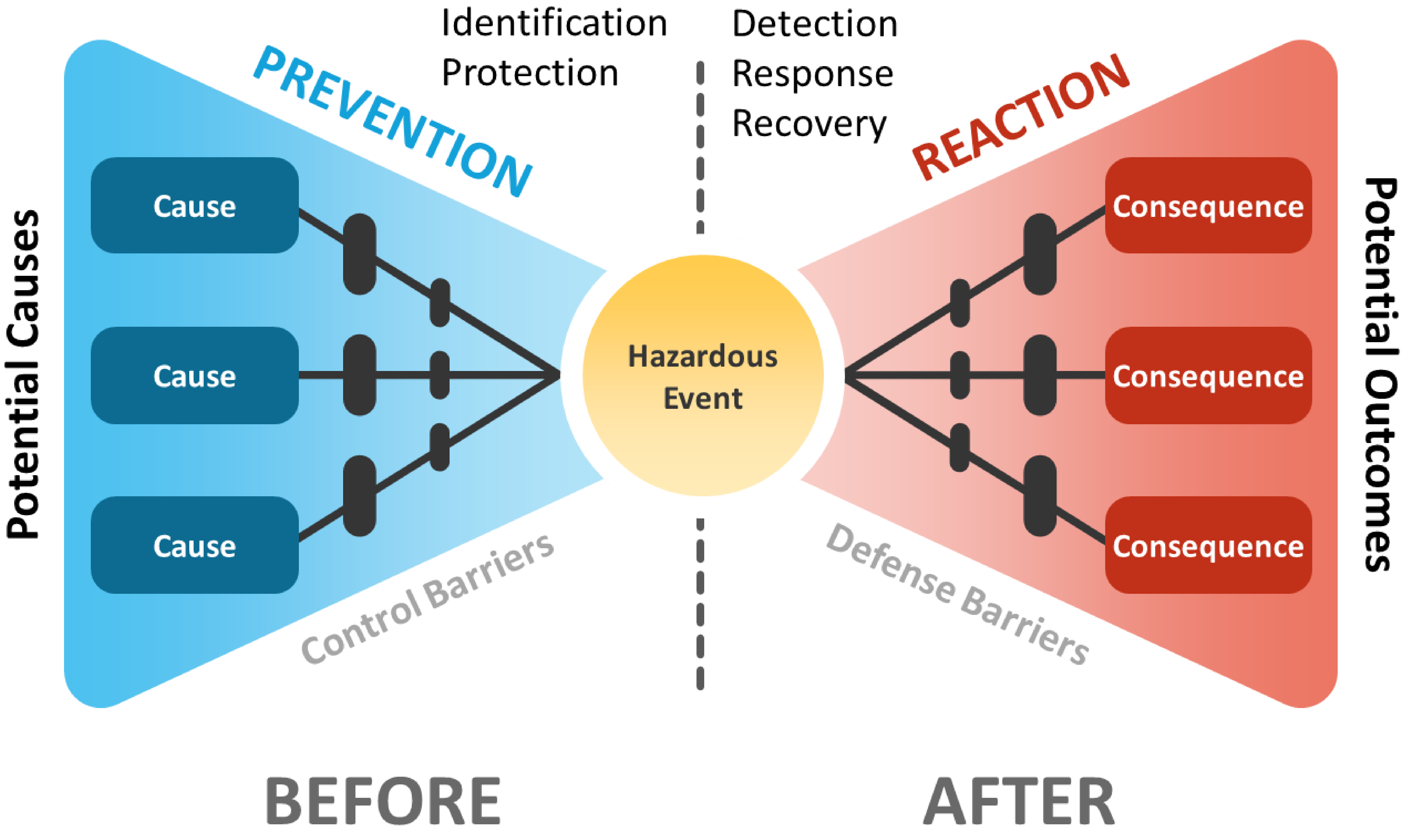
Cyber Fortress – MITRE ATT&CK Framework

Tactics, Techniques, Procedures (TTPs) define the specific behaviors and tools used by cybercriminals or cybercrime groups to achieve their goals at each stage of an attack. Knowing the modus operandi of attackers who are potentially motivated to attack us, we can better prepare to defend ourselves and detect the attack**.**



tactics = goal
technique = way of achieving the goal
procedure = way to implement the technique

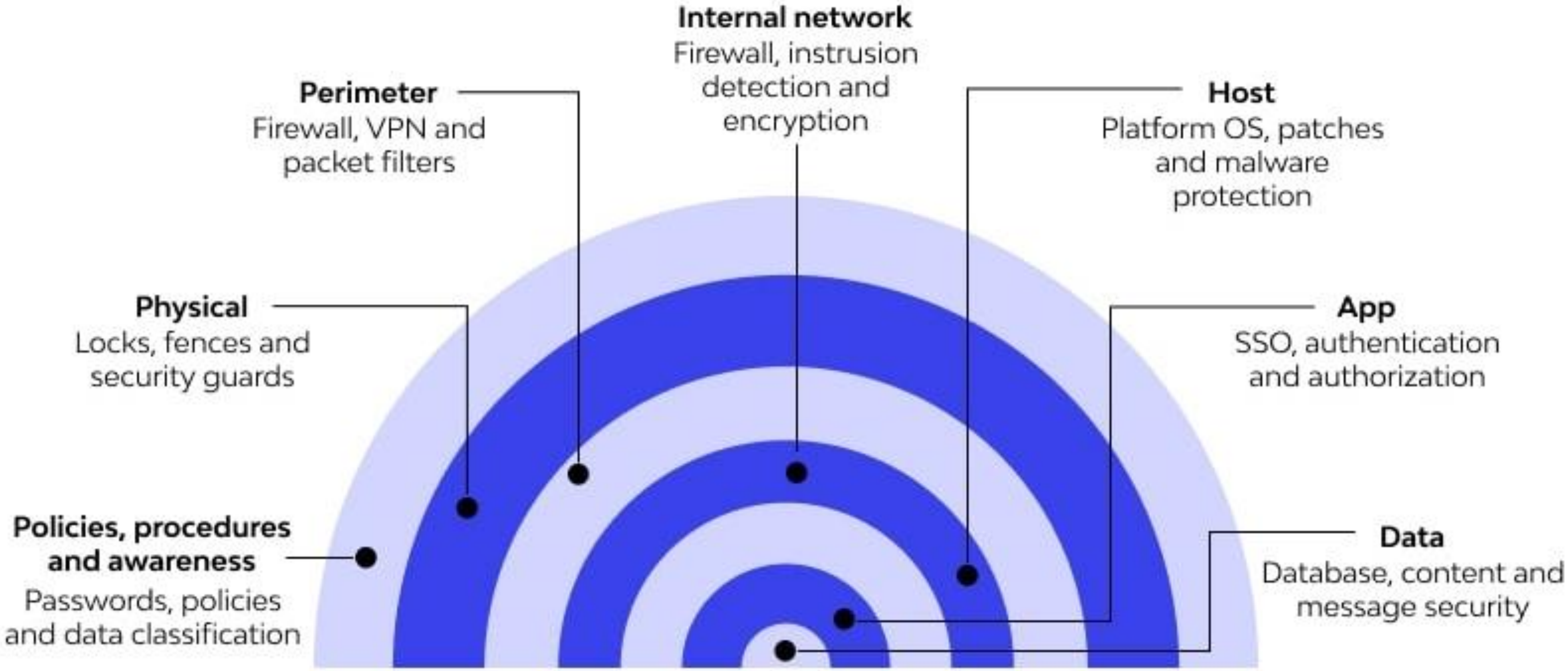
Cyber Fortress - Bow-Tie



comCERT

Cyber Fortress - Defense-in-Depth

Defense-in-Depth - multi-level defense strategy - a way of designing the security of information systems, involving the introduction of multiple independent levels of security.



Internal network
Firewall, instrusion detection and encryption
Perimeter
Firewall, VPN and packet filters
Host
Platform OS, patches and malware protection
Physical
Locks, fences and security guards
App
SSO, authentication and authorization
Policies, procedures and awareness
Passwords, policies and data classification
Data
Database, content and message security

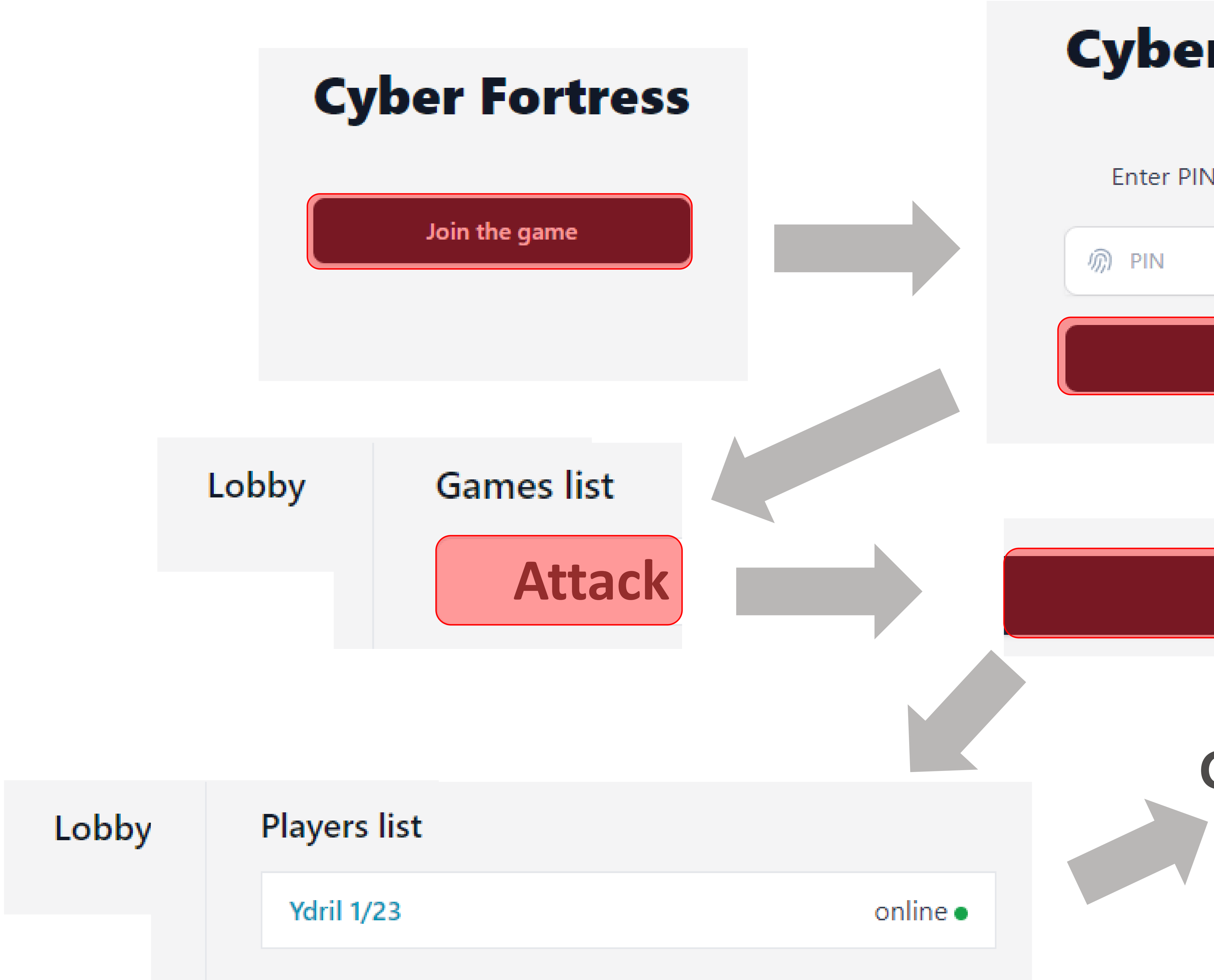
Practical information

- PC or phone, Chrome/Firefox/Safari browser (private mode)
- Internet access
- **If during the game, something goes wrong - RELOAD webpage**
- You will play 2 Games (3 Scenarios)
- Logging into the game is done with a PIN code
- **ONLY the team Captain logs into the game**
- The game consists of Events (Injects)
- Events could be Informational, Positive and Negative in nature
- In the Briefing section you will find the most important information about the Scenario
- Safeguards are divided into 8 categories (Organization, Physical infrastructure, Entire network, Network edge, Internal network, Host, Applications and Data)
- **There is a ninth category of Safeguard - Data Sources - which must be unlocked by purchasing the correct safeguard from the other eight categories**
- Some safeguards will not work unless they had been bought before the first Inject occurred
- Some safeguards will not work unless they had been bought before the Inject occurred
- You can find the list of Safeguards with description at: https://cyberfortress.comcert.pl/safeguards

CYBER FORTRESS
ENTERPRISE
SAFEGUARDS

https://cyberfortress.comcert.pl/safeguards

Interface of the Game



Cyber Fortress

Join the game

Cyber Fortress

Enter PIN and join the game

PIN

Next

Lobby

Games list

Attack

Next

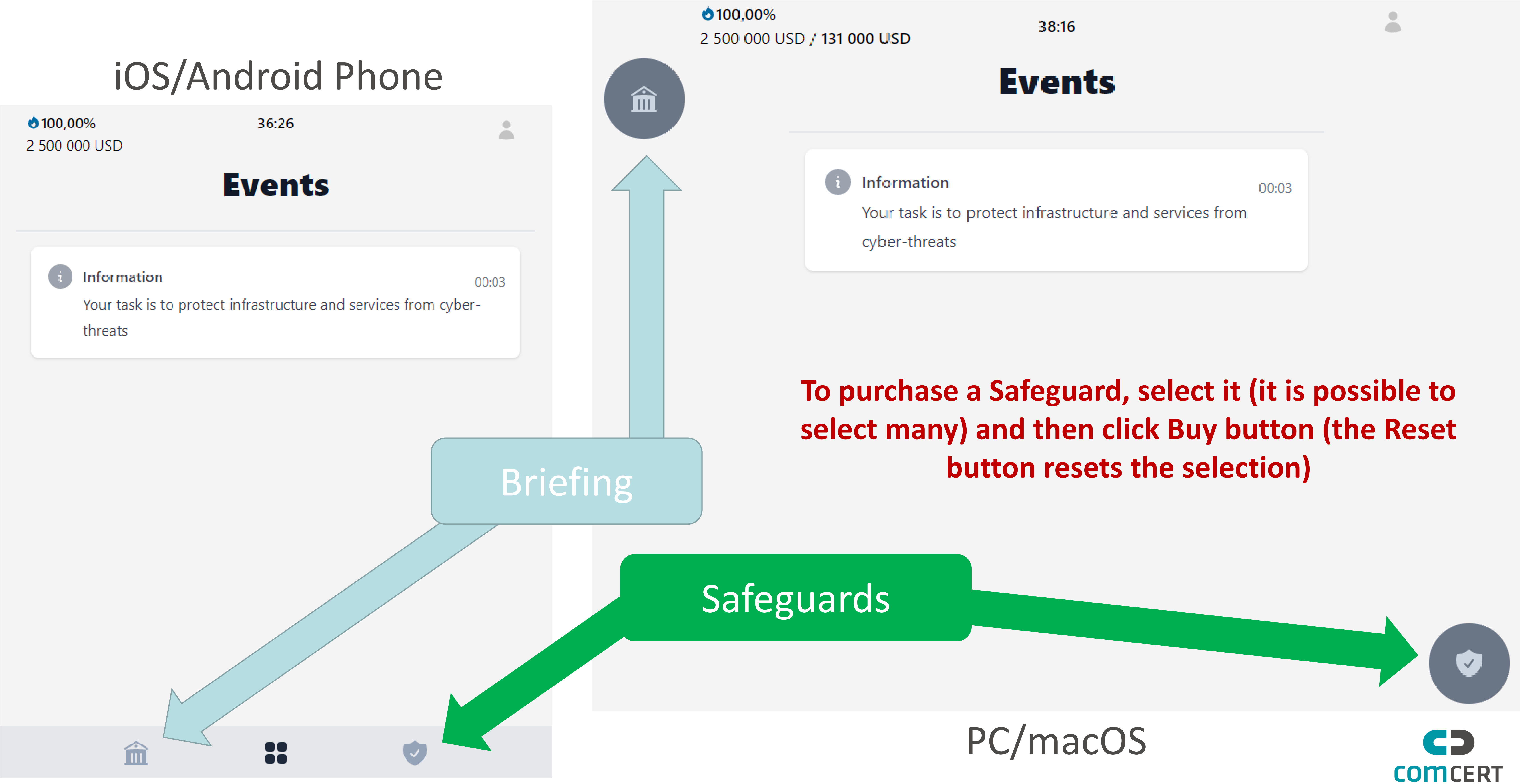
Lobby

Players list

Ydril 1/23 online ●

Game Master will start the game ☺

Interface of the Game



iOS/Android Phone

100,00%
2 500 000 USD

36:26

Events

Information 00:03
Your task is to protect infrastructure and services from cyber-threats

100,00%
2 500 000 USD / 131 000 USD

38:16

Events

Information 00:03
Your task is to protect infrastructure and services from cyber-threats

To purchase a Safeguard, select it (it is possible to select many) and then click Buy button (the Reset button resets the selection)

PC/macOS

comCERT

Cyber Fortress - Introduction

Link to the Cyber Fortress Game:

https://cyberfortress.comcert.pl/

The Game requires a PIN number to log you into the Lobby

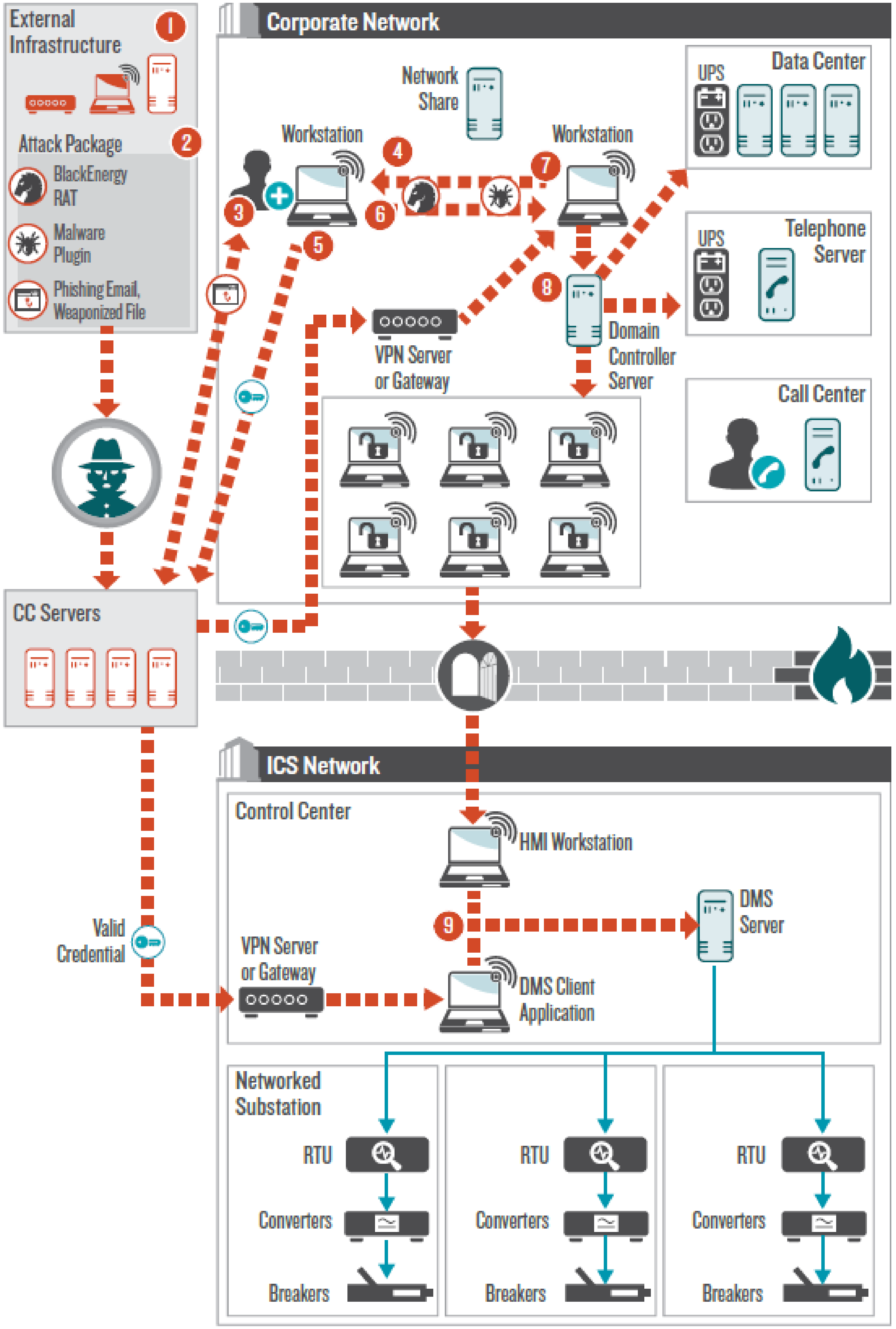
1ST GAME SESSION:
The Energy System Attack

The Energy System Attack Scenario

On 23 December 2015, hackers using the BlackEnergy 3 malware remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers. Most affected were consumers of Prykarpattyaoblenergo (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations (7 110kv substations and 23 35kv substations) were switched off, and about 230,000 people were without electricity for a period from 1 to 6 hours.

At the same time, consumers of two other energy distribution companies, Chernivtsioblenergo (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and Kyivoblenergo (Ukrainian: Київобленерго; servicing Kyiv Oblast) were also affected by a cyberattack, but at a smaller scale. According to representatives of one of the companies, attacks were conducted from computers with IP addresses allocated to the Russian Federation.

The Scenario has been based upon Events described above.



1. Reconnaissance – 2014 or earlier

2. Resource Development –
Develop Capabilities: Malware (BE3)– 2014 or earlier

CORPORATE NETWORK

3. Initial access - Phishing: Spearphishing Attachment – May 2014- June 2015

4. Execution - User Execution: Malicious File- May 2014- June 2015

5. Command and control Application Layer Protocol: Web Protocols - May 2014- June 2015

6. . Execution - Exploitation for Client Execution - June 2015- December 2015

7. Credential Access - Credentials from Password Stores: Credentials from Web Browsers, Keylogging, Network Sniffing, OS Credential Dumping: LSASS Memory- June 2015- December 2015

8. Discovery – Account discovery, Remote system discovery - June 2015- December 2015
Lateral Movement – Remote services - June 2015- December 2015

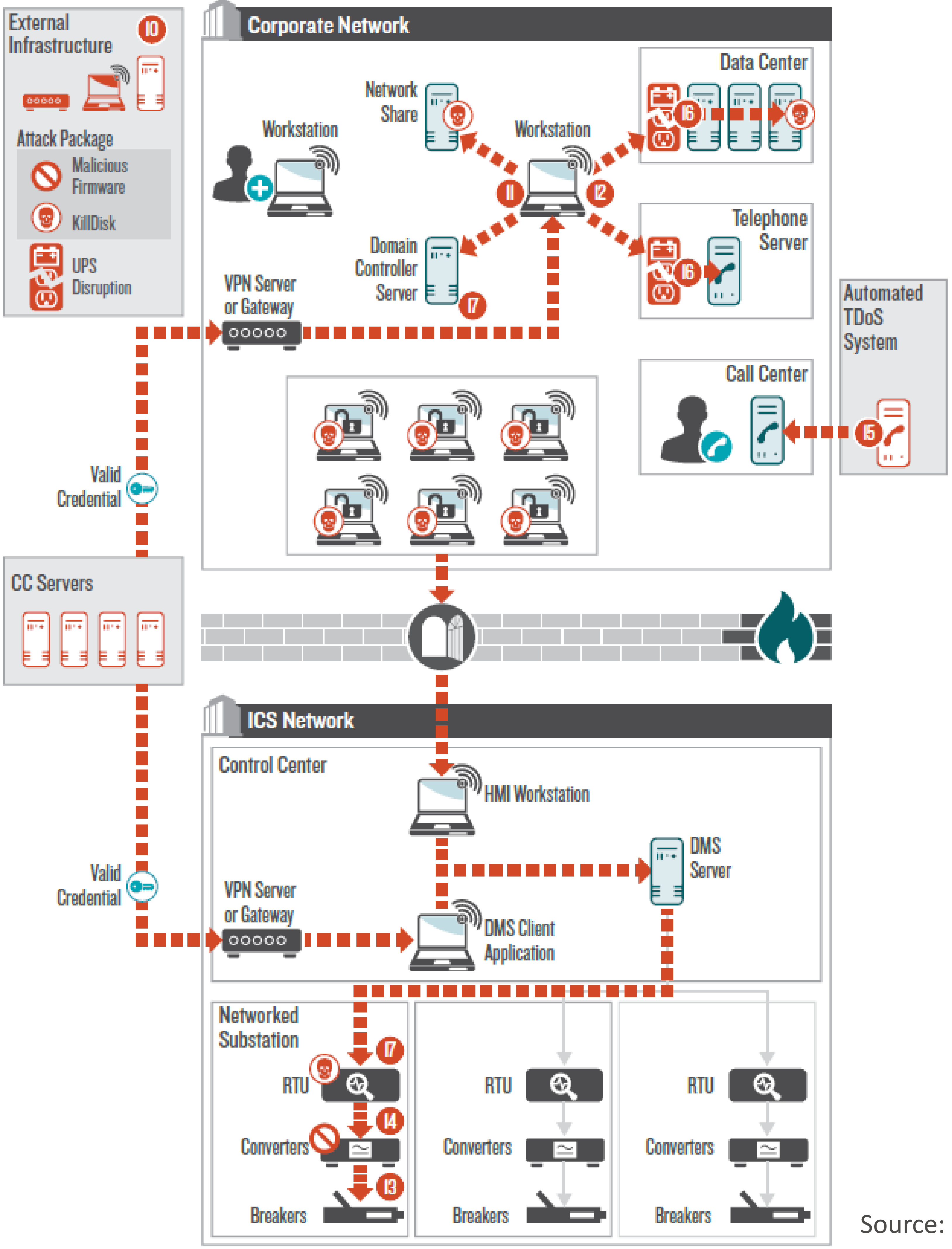
ICS NETWORK

9 . Initial Access – External remote services

Lateral movement – Valid accounts, External remote services

Source: When the lights when out – ukrainian attack report

comCERT



10. Resource Development –
 Develop Capabilities: Malware (KillDisk)– June 2015- December 2015

CORPORATE NETWORK

11. Lateral Movement – Lateral Tool Transfer- May 2014- June 2015

12. Execution – Scheduled Task- December 2015

ICS NETWORK

13. . Execution – Graphical User Interface- 23 December 2015

14. Persistence – System Firmware - 23 December 2015

CORPORATE NETWORK

15. Impact – Network Denial of Service: Direct Network Flood- 23 December 2015

16. Impact – Service Stop- 23 December 2015
Lateral Movement – Remote services - June 2015- December 2015

ICS NETWORK

17 . Impact– Data destruction

Source: When the lights when out – ukrainian attack report

comCERT

The Energy System Attack Scenario

Link to the Cyber Fortress Game:

https://cyberfortress.comcert.pl

(the Team Captain ONLY)

CYBER FORTRESS
ENTERPRISE

list of Safeguards with description:

https://cyberfortress.comcert.pl/safeguards

CYBER FORTRESS
ENTERPRISE
SAFEGUARDS

The Game Session will last for: 40 min

Budget: $ 2 500 000

comCERT

1ST GAME SESSION:
The Energy System Attack
EFFICIENT SAFEGUARDS

The Energy System Attack Scenario 1

Threat actors initiate phishing campaign against electricity distributors.	3 Security Awareness Training $36,000	50 Email security gateway $62,400	51 Email sandbox $30,000
Threat actors successfully install BlackEnergy after employees open the email attachments	3 Security Awareness Training $36,000	49 Workstation protection system (End Point Security) $88,800	57 Configuration Management Database System (CMDB) $48,000
Malware Establishes Command-and-Control (CC) Connection from malicious implant.	37 Edge firewall $138,000	38 Internal firewall $72,000	41 IDS/IPS -Intrusion Detection and Prevention System $165,000
Deliver Malware Plugins to enable credential harvesting and internal network reconnaissance.	41 IDS/IPS -Intrusion Detection and Prevention System $165,000	90 File Creation $5,000	125 Network Traffic Flow $5,000
BE3 malware plugins conduct credential harvesting and network discovery functions.	30 Multi-Factor Authentication (MFA) 85 000 USD	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800

Organization · Physical Infrastructure · Entire Network · Network Edge

Internal Network · Host · Applications · Data · Data Sources

comCERT

The Energy System Attack Scenario 2

Threat actors conduct internal reconnaissance on corporate network to discover potential targets and expand access.	57 Configuration Management Database System (CMDB) $48,000	77 Command Execution $5,000	135 Process Creation $5,000
Threat actors use stolen credentials to gain access and conduct reconnaissance on deployed systems.	30 Multi-Factor Authentication (MFA) 85 000 USD	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800
Attackers deliver KillDisk malware to network share and set policy on DC to retrieve malware and execute upon system reboot.	11 Separation of Network Resources 172 000 USD	41 IDS/IPS -Intrusion Detection and Prevention System $165,000	63 Active Directory Object Modification 5000 USD
Threat actors schedule unauthorized outage of UPS for telephone communication server and data center servers.	57 Configuration Management Database System (CMDB) $48,000	43 Privileged Access Management (PAM) System. $280,000	139 Scheduled Job Creation 5000 USD

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

The Energy System Attack Scenario 2

Threat actors use native remote access services and valid credentials to open breakers and disrupt power distribution to over 225,000 customers	11 Separation of Network Resources 172 000 USD	47 Backup System (redundancy) 305 000 USD	20 Business continuity management 38 000 USD
Threat actors deliver malicious firmware updates to communications devices that cause converters to malfunction and break connections	57 Configuration Management Database System (CMDB) $48,000	43 Privileged Access Management (PAM) System. $280,000	98 Firmware Modification 5000 USD
Threat actors initiate DoS attack on telephone call center at one of the targeted distributors.	37 Edge firewall $138,000	35 Anti-DDoS system 115 000 USD	125 Network Traffic Flow $5,000
Previously scheduled UPS outage cuts power to targeted telephone communications server and data center servers.	No mitigations		
Scheduled execution of KillDisk malware erases the master boot records and deletes system log data	44 Backups $178,000	20 Business continuity management 38 000 USD	91 File Deletion 5000 USD

ORGANIZATION · PHYSICAL INFRASTRUCTURE · ENTIRE NETWORK · NETWORK EDGE

INTERNAL NETWORK · HOST · APPLICATIONS · DATA · DATA SOURCES

comCERT

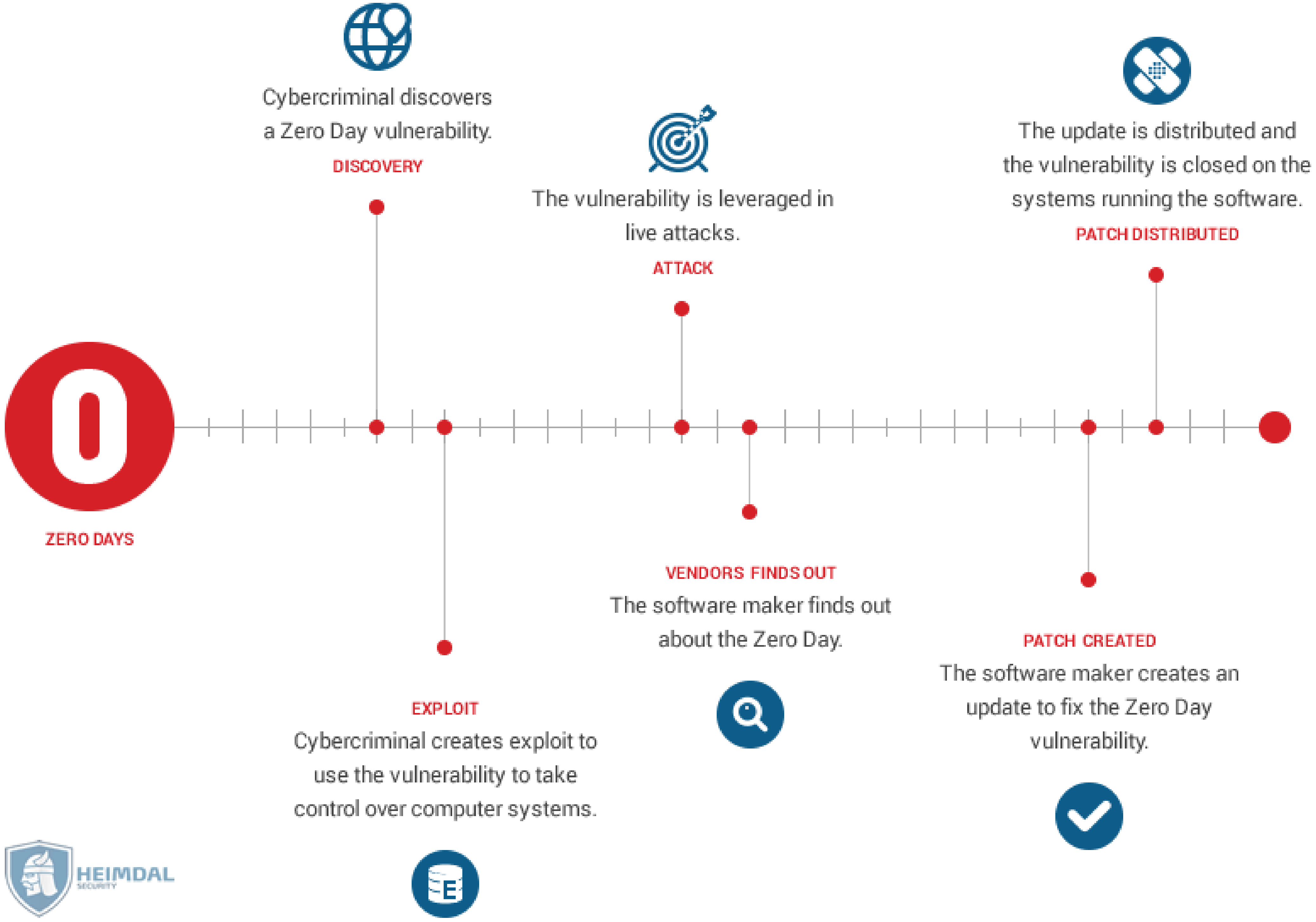
2nd Game Session:
Website Defacement
&
Ransomware Scenarios

Introduction

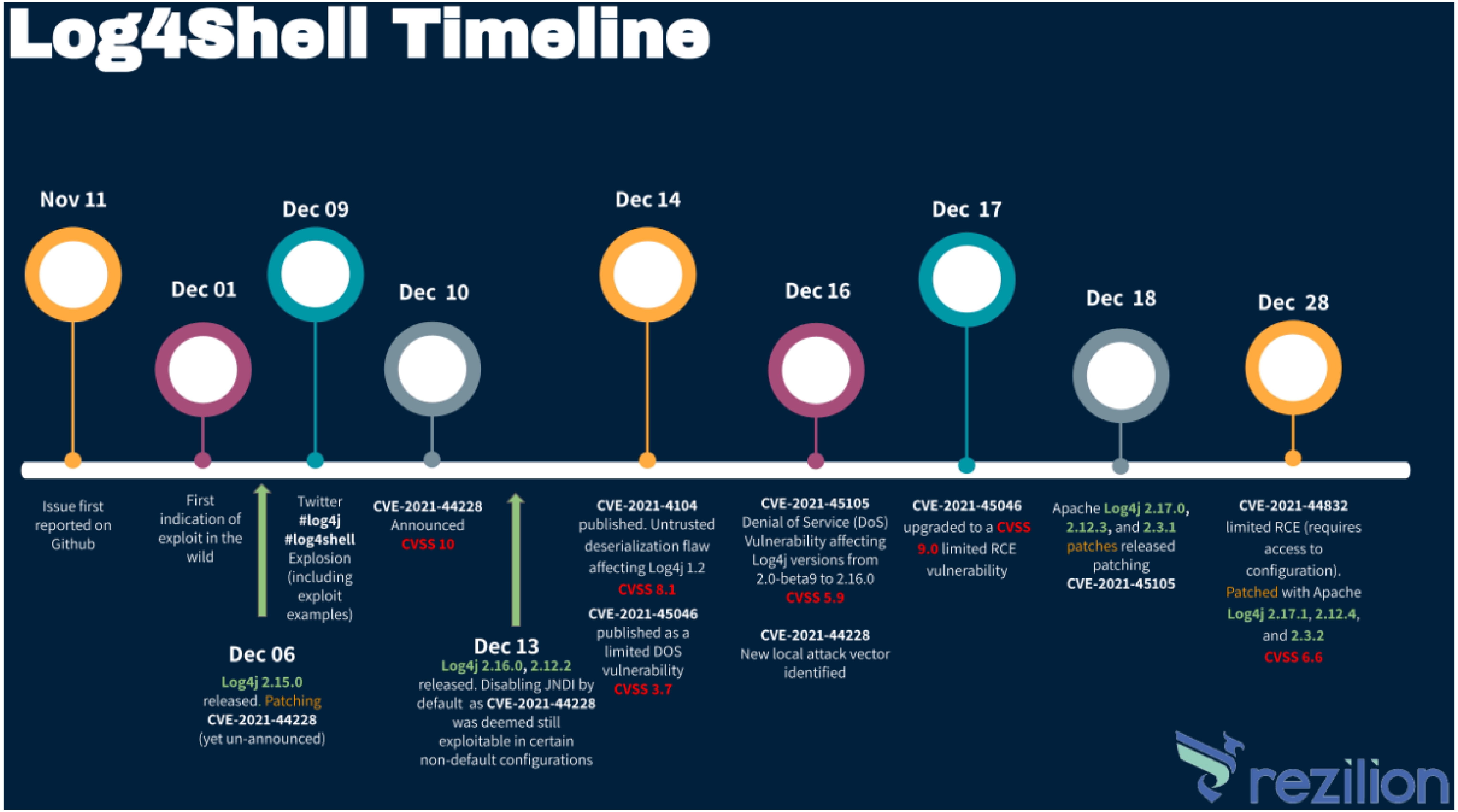
Website Defacement Scenario - 0-day (vulnerabilities)

Vulnerabilities (security vulnerabilities are flaws in a computer system that weaken the overall security of the device/system.

0-day vulnerabilities are those that the manufacturer or user of the software or system does not know about


0
ZERO DAYS
Cybercriminal discovers a Zero Day vulnerability.
DISCOVERY
EXPLOIT
Cybercriminal creates exploit to use the vulnerability to take control over computer systems.
The vulnerability is leveraged in live attacks.
ATTACK
VENDORS FINDS OUT
The software maker finds out about the Zero Day.
PATCH CREATED
The software maker creates an update to fix the Zero Day vulnerability.
The update is distributed and the vulnerability is closed on the systems running the software.
PATCH DISTRIBUTED
HEIMDAL SECURITY

Website Defacement Scenario - 0-day (vulnerabilities)



Log4Shell Timeline

Nov 11
Issue first reported on Github

Dec 01
First indication of exploit in the wild

Dec 06
Log4j 2.15.0 released. Patching CVE-2021-44228 (yet un-announced)

Dec 09
Twitter #log4j #log4shell Explosion (including exploit examples)

Dec 10
CVE-2021-44228 Announced
CVSS 10

Dec 13
Log4j 2.16.0, 2.12.2 released. Disabling JNDI by default as CVE-2021-44228 was deemed still exploitable in certain non-default configurations

Dec 14
CVE-2021-4104 published. Untrusted deserialization flaw affecting Log4j 1.2
CVSS 8.1
CVE-2021-45046 published as a limited DOS vulnerability
CVSS 3.7

Dec 16
CVE-2021-45105 Denial of Service (DoS) Vulnerability affecting Log4j versions from 2.0-beta9 to 2.16.0
CVSS 5.9
CVE-2021-44228 New local attack vector identified

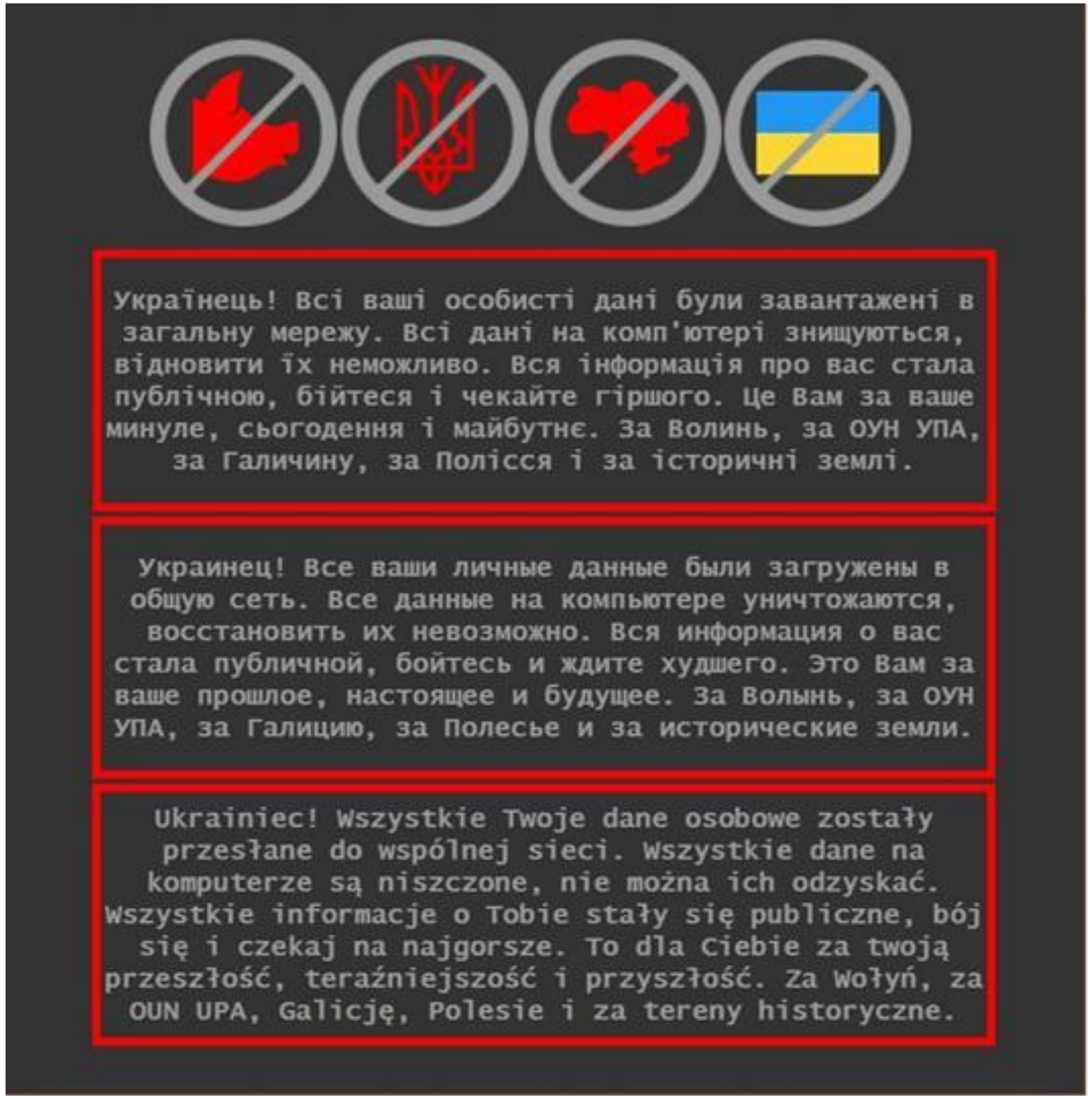
Dec 17
CVE-2021-45046 upgraded to a CVSS 9.0 limited RCE vulnerability

Dec 18
Apache Log4j 2.17.0, 2.12.3, and 2.3.1 patches released patching CVE-2021-45105

Dec 28
CVE-2021-44832 limited RCE (requires access to configuration). Patched with Apache Log4j 2.17.1, 2.12.4, and 2.3.2
CVSS 6.6

Website Defacement Scenario - Replacing site content

Website Defacement is an attack on a website that changes its appearance or content.



Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це Вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі.

Украинец! Все ваши личные данные были загружены в общую сеть. Все данные на компьютере уничтожаются, восстановить их невозможно. Вся информация о вас стала публичной, бойтесь и ждите худшего. Это Вам за ваше прошлое, настоящее и будущее. За Волынь, за ОУН УПА, за Галицию, за Полесье и за исторические земли.

Ukrainiec! Wszystkie Twoje dane osobowe zostały przesłane do wspólnej sieci. Wszystkie dane na komputerze są niszczone, nie można ich odzyskać. Wszystkie informacje o Tobie stały się publiczne, bój się i czekaj na najgorsze. To dla Ciebie za twoją przeszłość, teraźniejszość i przyszłość. Za Wołyń, za OUN UPA, Galicję, Polesie i za tereny historyczne.

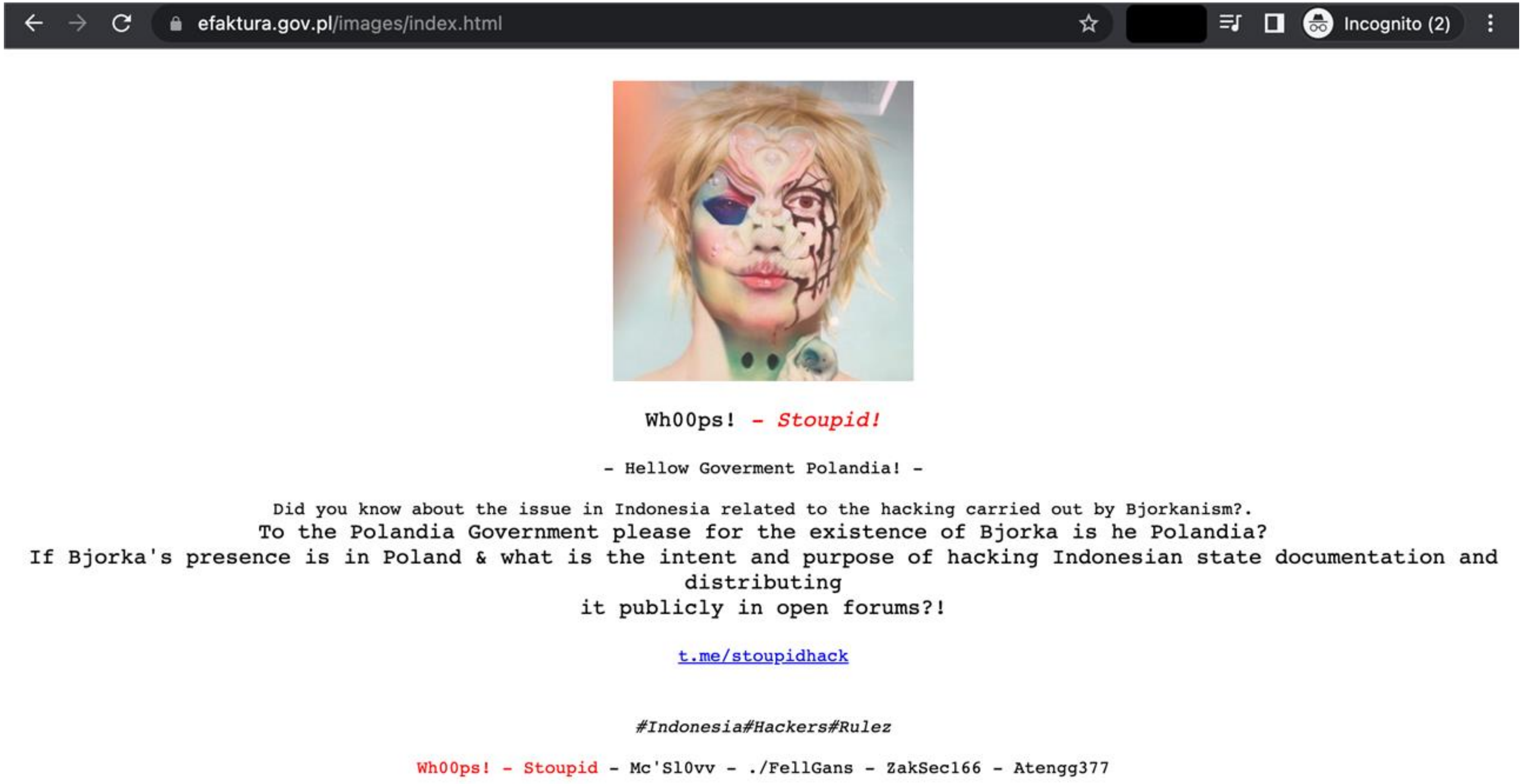
https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/analysis-cyberattack-ukrainian-government-resources/

Websites in the gov.ua domain were compromised (as of January 14, 2022):

- Government services portal "Diia" - diia.gov.ua
- Cabinet of Ministers - kmu.gov.ua
- Ministry of Foreign Affairs - mfa.gov.ua
- State Rescue Service - dsns.gov.ua
- Ministry of Education and Science - mon.gov.ua
- Ministry of Youth and Sport - sport.gov.ua Ministry of Energy - mpe.kmu.gov.ua
- Ministry of Agrarian Policy - minagro.gov.ua Ministry of Veterans Affairs - mva.gov.ua Ministry of Environment Protection and Natural Resources - mepr.gov.ua
- State Treasury Service - treasury.gov.ua

Website Defacement Scenario - Replacing site content

Defacement is an attack on a website that changes its appearance or content.



Wh00ps! *- Stoupid!*

- Hellow Goverment Polandia! -

Did you know about the issue in Indonesia related to the hacking carried out by Bjorkanism?.
To the Polandia Government please for the existence of Bjorka is he Polandia?
If Bjorka's presence is in Poland & what is the intent and purpose of hacking Indonesian state documentation and distributing
it publicly in open forums?!

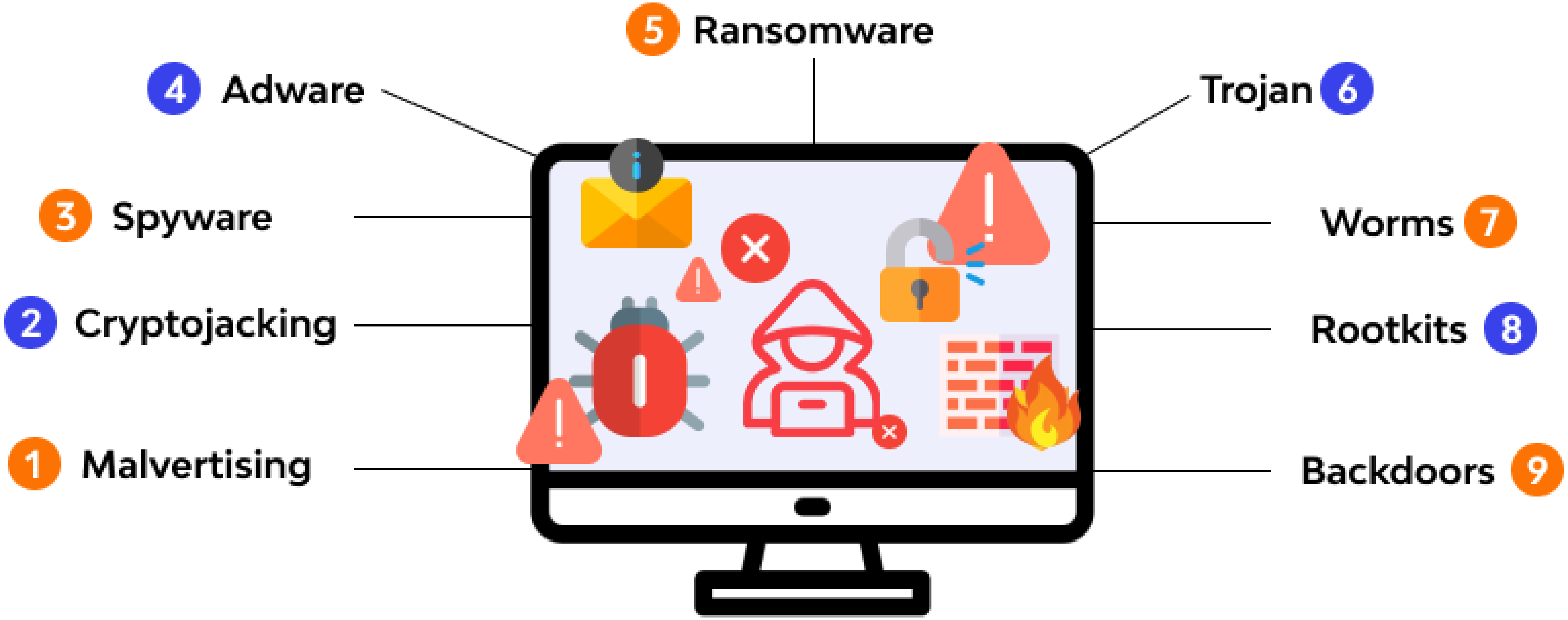
t.me/stoupidhack

#Indonesia#Hackers#Rulez

Wh00ps! - Stoupid - Mc'Sl0vv - ./FellGans - ZakSec166 - Atengg377

Ransomware Scenario

Types of malware



1 Malvertising

2 Cryptojacking

3 Spyware

4 Adware

5 Ransomware

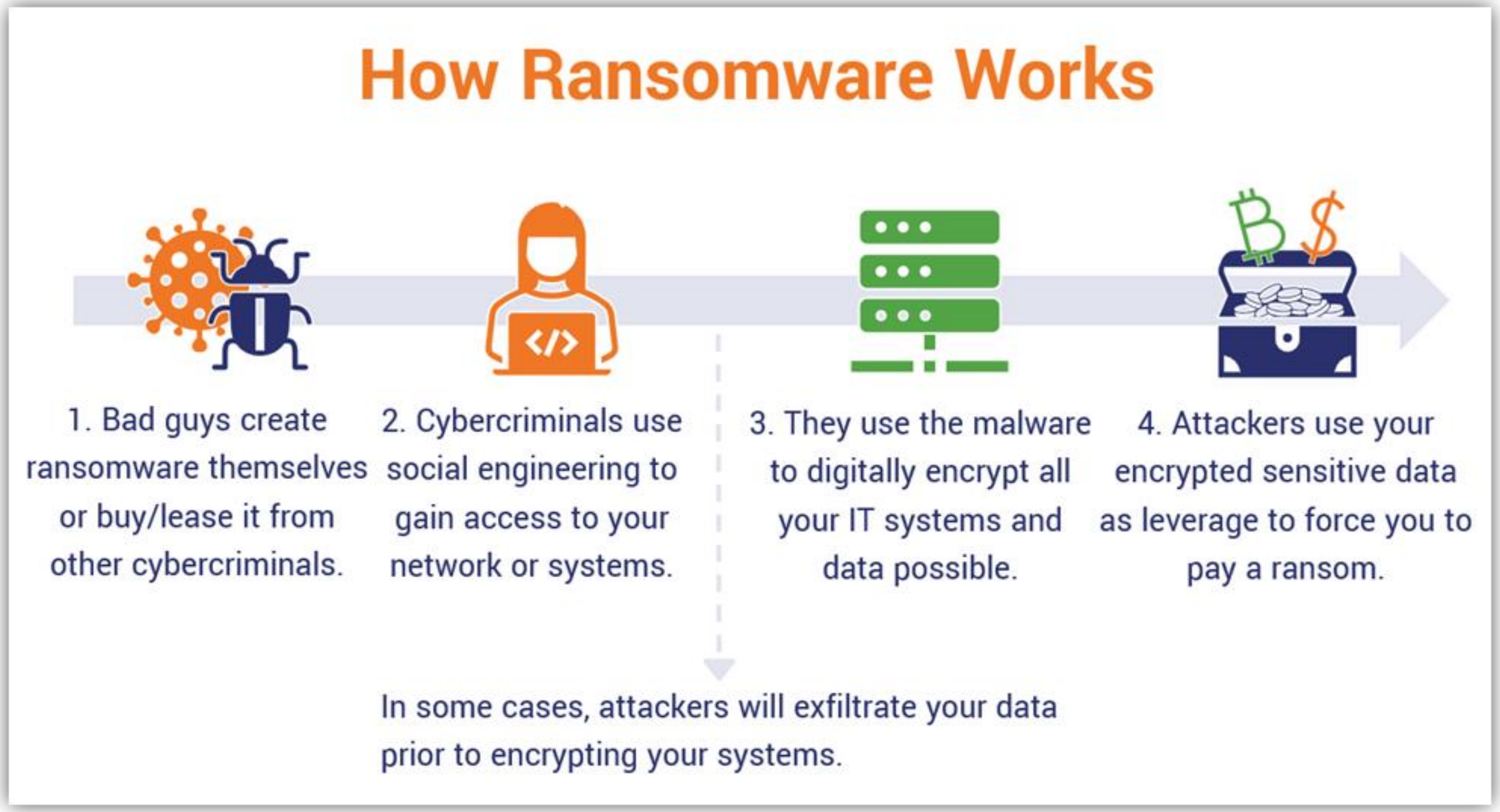
6 Trojan

7 Worms

8 Rootkits

9 Backdoors

Ransomware Scenario



How Ransomware Works

1. Bad guys create ransomware themselves or buy/lease it from other cybercriminals.

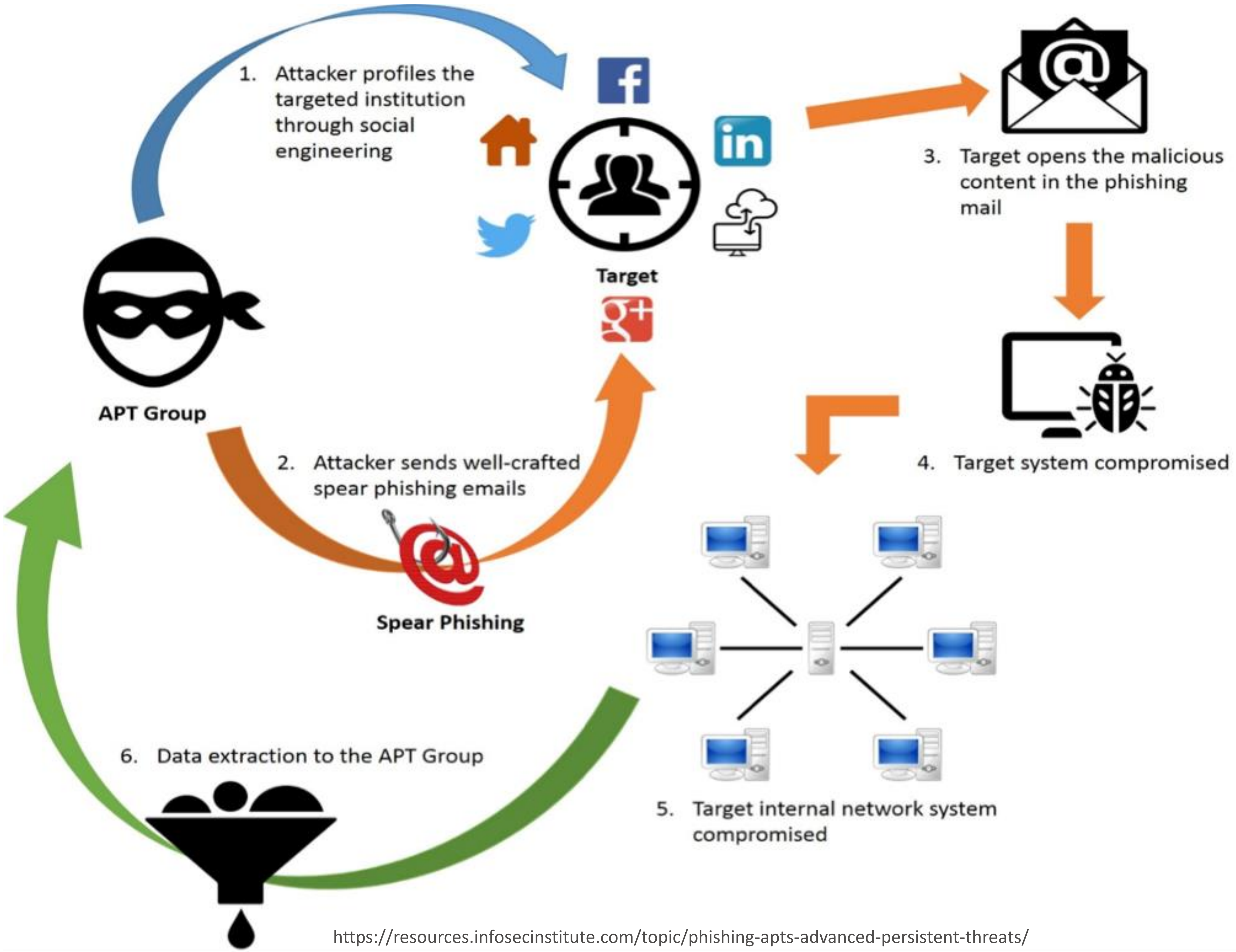
2. Cybercriminals use social engineering to gain access to your network or systems.

3. They use the malware to digitally encrypt all your IT systems and data possible.

4. Attackers use your encrypted sensitive data as leverage to force you to pay a ransom.

In some cases, attackers will exfiltrate your data prior to encrypting your systems.

Ransomware Scenario



1. Attacker profiles the targeted institution through social engineering

Target

3. Target opens the malicious content in the phishing mail

4. Target system compromised

APT Group

2. Attacker sends well-crafted spear phishing emails

Spear Phishing

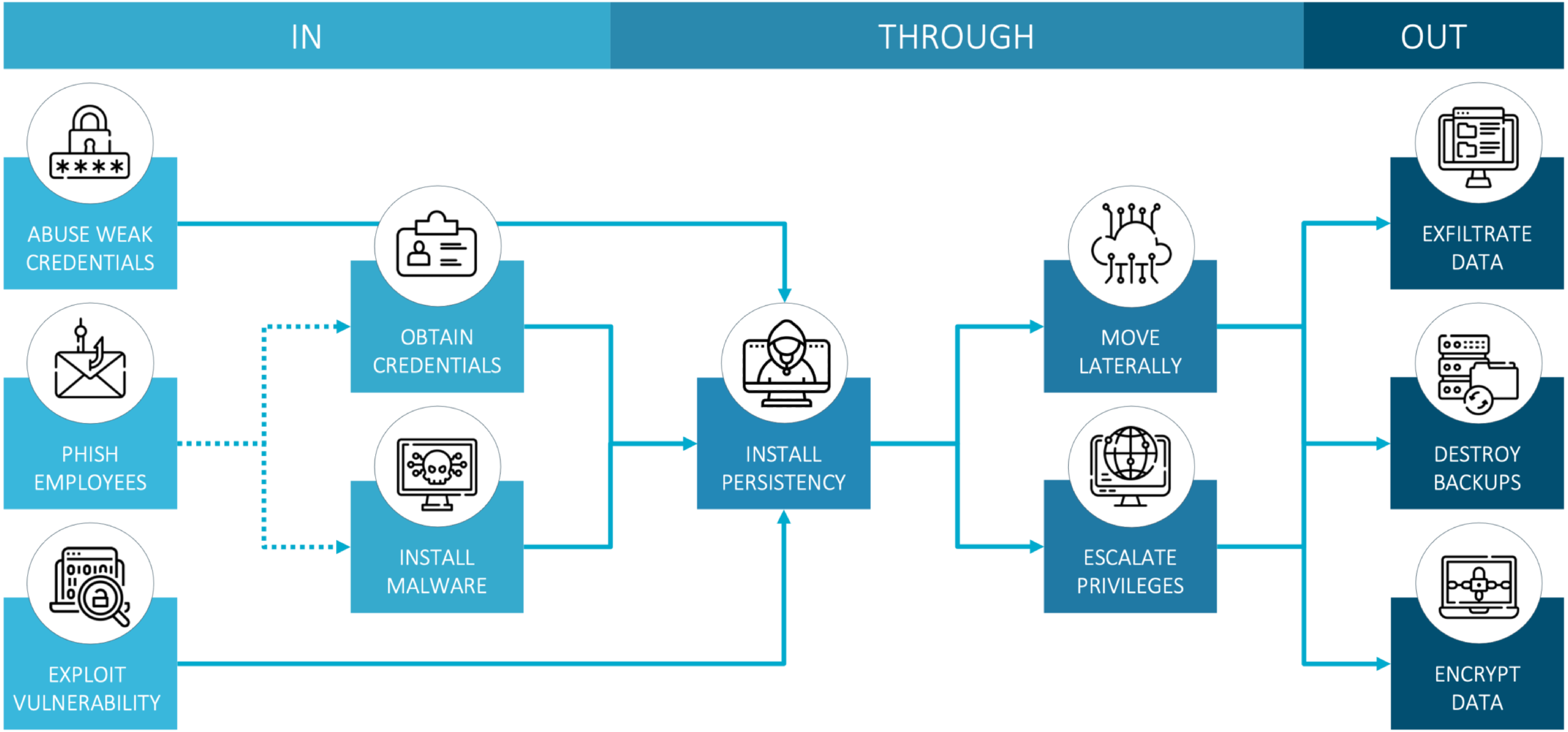
5. Target internal network system compromised

6. Data extraction to the APT Group

https://resources.infosecinstitute.com/topic/phishing-apts-advanced-persistent-threats/

comCERT

Ransomware Scenario



comCERT

2nd Game Session:
Website Defacement
&
Ransomware Scenarios

Website Defacement Scenario

You are a government organization responsible for ensuring national security and you run several websites that are a trusted source of information for citizens and news agencies.

In November 2021, security researchers discovered a vulnerability that allows an attacker to take over a web server called Log4shell. Security updates resolving the issue were released on December 3, 2021. Your Organization uses the software in which the Log4shell vulnerability was discovered on all Web portals that are published on the Internet.

without any verification

Ransomware Scenario

You are a government organization responsible for ensuring national security and you run several websites that are a trusted source of information for citizens and news agencies.

On December 20, 2022, all employees of your organization received an email with the title „The Obligatory Cyber Awareness Training - announcement." In the body of the message, the Organization's Board of Directors informed employees that due to the growing number of cyberattacks, all employees are required to undergo a cyber-awarness training. Attached to the message was a pdf file with the Board's resolution and an Excel spreadsheet containing a list of available training dates. Many employees of the Organization opened both files without any verification.

Website Defacement & Ransomware Scenarios

Link to the Cyber Fortress Game:

https://cyberfortress.comcert.pl

(the Team Captain ONLY)

list of Safeguards with description:
https://cyberfortress.comcert.pl/safeguards

The Game Session will last for: 50 min
Budget: $ 1 700 000

2nd Game Session: Website Defacement & Ransomware Scenarios

Efficient Safeguards

Ransomware Scenario

The mandatory cyber-awareness training email contains an attachment with malicious content	3 Security Awareness Training $36,000	50 Email security gateway $62,400	51 Email sandbox $30,000
An employee launched a malicious attachment	3 Security Awareness Training $36,000	49 Workstation protection system (End Point Security) $88,800	57 Configuration Management Database System (CMDB) $48,000
Malware executed commands on the command line to establish a connection to the Command&Control server	34 Antivirus Software $114,000	49 Workstation protection system (End Point Security) $88,800	52 Application sandbox $45,000
Malware has established a connection to the C&C server using non-standard ports	37 Edge firewall $138,000	38 Internal firewall $72,000	41 IDS/IPS -Intrusion Detection and Prevention System $165,000
Malware has downloaded a file containing a malicious script	41 IDS/IPS -Intrusion Detection and Prevention System $165,000	90 File Creation $5,000	125 Network Traffic Flow $5,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Ransomware Scenario

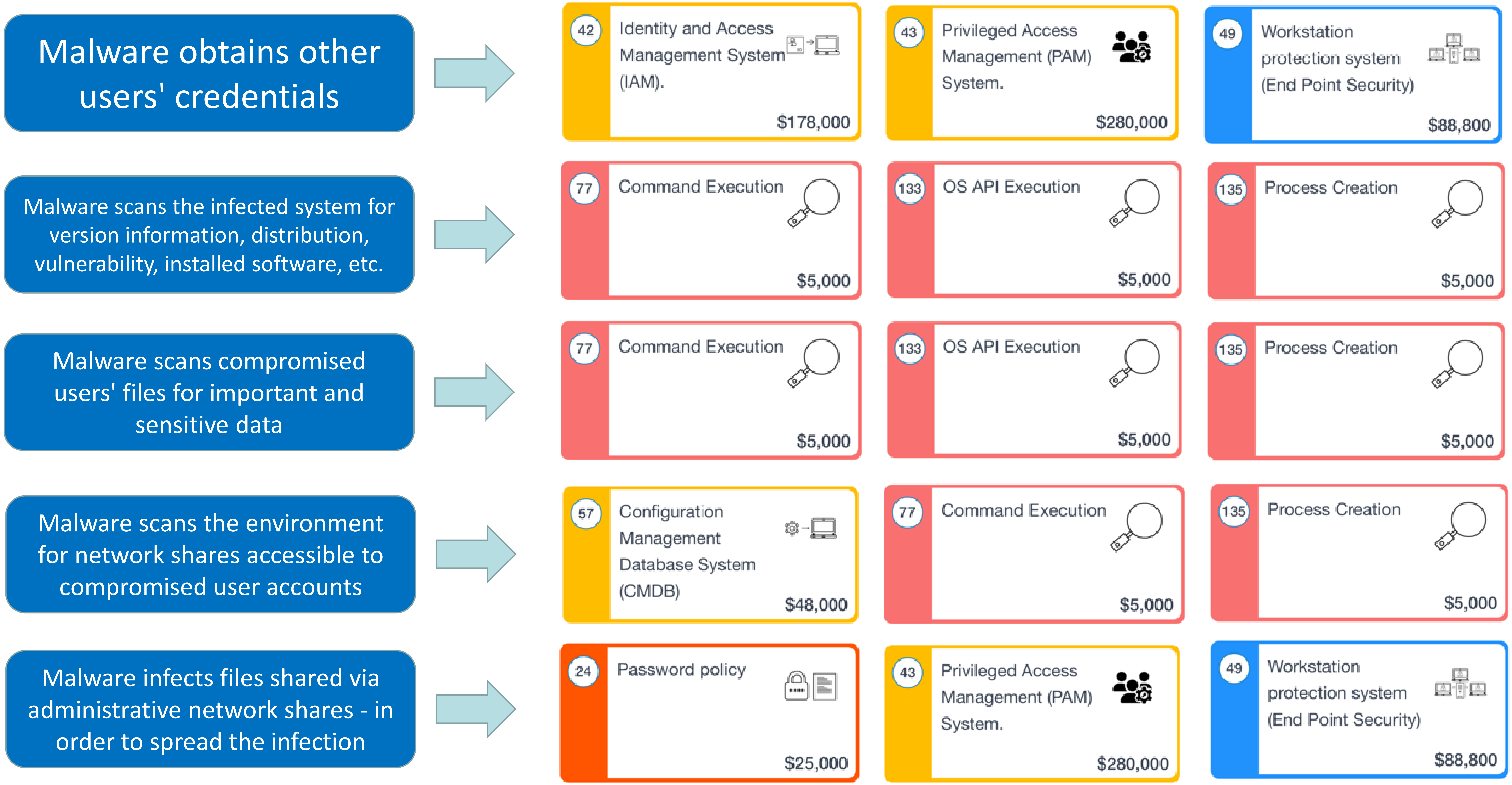
Malware adds a malicious script to the user account properties. The script will be executed every time the user logs in	49 Workstation protection system (End Point Security) $88,800	53 Software whitelisting $88,800	57 Configuration Management Database System (CMDB) $48,000
Malware tries to get the administrator credentials of the infected device	49 Workstation protection system (End Point Security) $88,800	52 Application sandbox $45,000	57 Configuration Management Database System (CMDB) $48,000
Malware acquires administrative credentials of the infected device	24 Password policy $25,000	42 Identity and Access Management System (IAM). $178,000	43 Privileged Access Management (PAM) System. $280,000
Malware disables antivirus protection and event logging	42 Identity and Access Management System (IAM). $178,000	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800
Malware seeks other users' credentials	8 Hardening and updating of Network Servers and Devices $88,000	15 Configuration management $72,000	57 Configuration Management Database System (CMDB) $48,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Ransomware Scenario



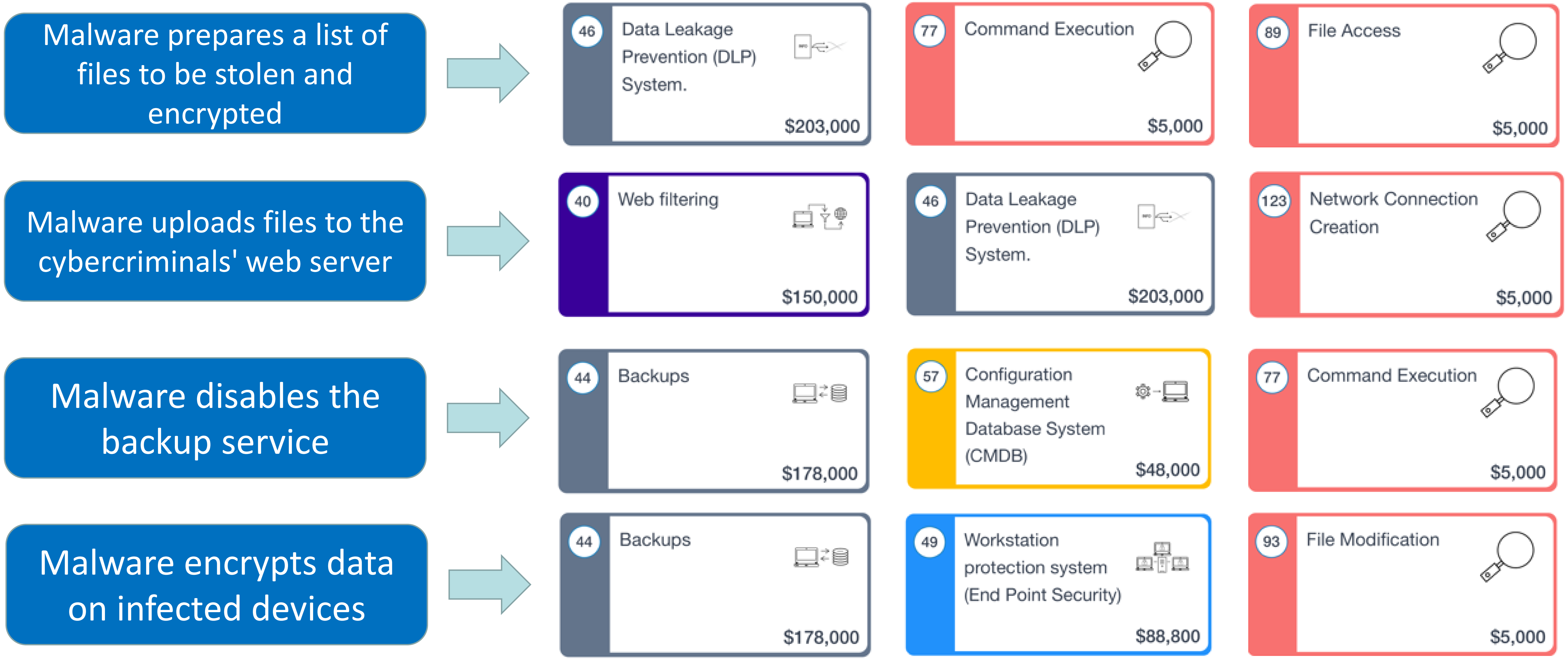
Step			
Malware obtains other users' credentials	42 Identity and Access Management System (IAM). $178,000	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800
Malware scans the infected system for version information, distribution, vulnerability, installed software, etc.	77 Command Execution $5,000	133 OS API Execution $5,000	135 Process Creation $5,000
Malware scans compromised users' files for important and sensitive data	77 Command Execution $5,000	133 OS API Execution $5,000	135 Process Creation $5,000
Malware scans the environment for network shares accessible to compromised user accounts	57 Configuration Management Database System (CMDB) $48,000	77 Command Execution $5,000	135 Process Creation $5,000
Malware infects files shared via administrative network shares - in order to spread the infection	24 Password policy $25,000	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Ransomware Scenario

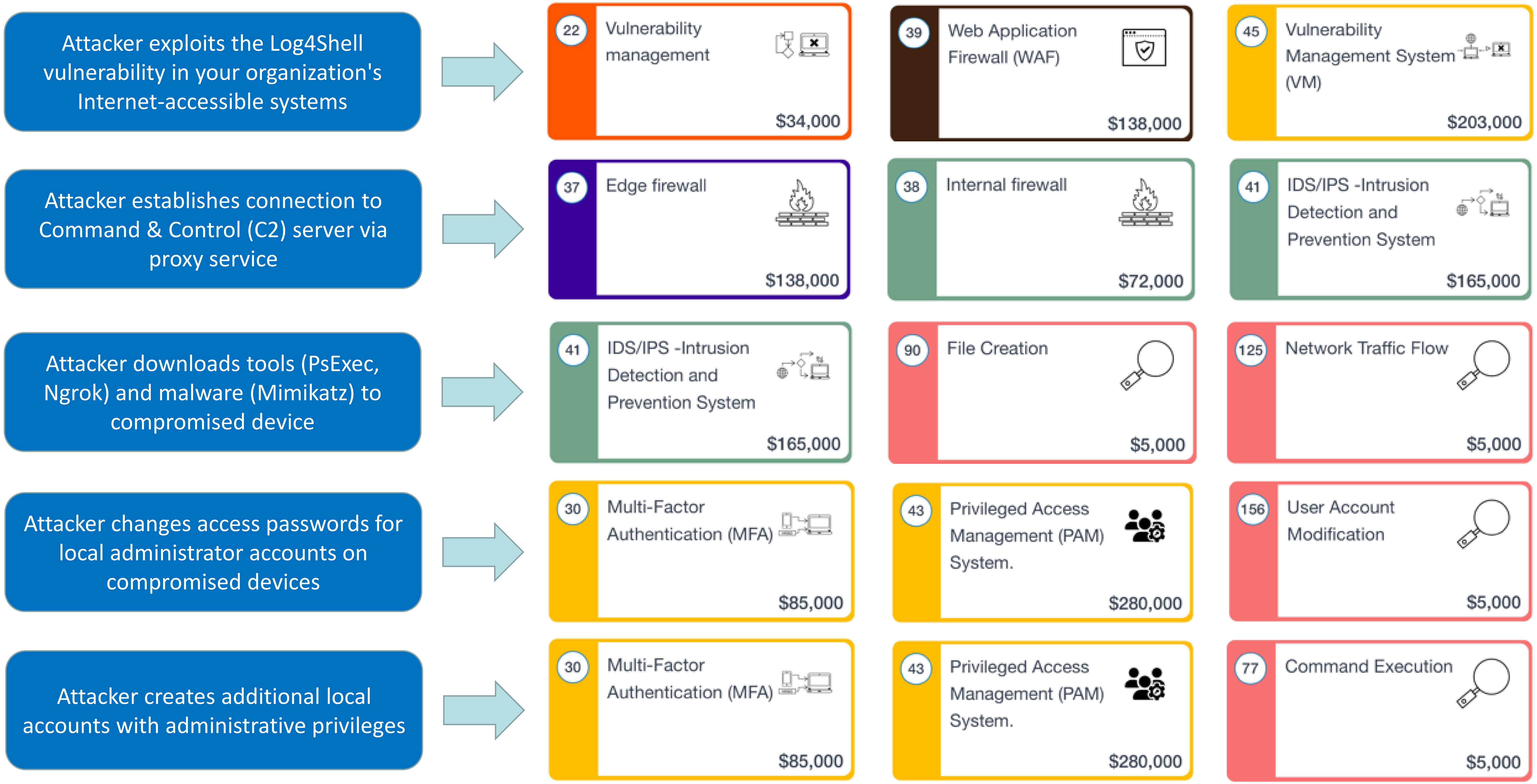


Malware prepares a list of files to be stolen and encrypted	46 Data Leakage Prevention (DLP) System. $203,000	77 Command Execution $5,000	89 File Access $5,000
Malware uploads files to the cybercriminals' web server	40 Web filtering $150,000	46 Data Leakage Prevention (DLP) System. $203,000	123 Network Connection Creation $5,000
Malware disables the backup service	44 Backups $178,000	57 Configuration Management Database System (CMDB) $48,000	77 Command Execution $5,000
Malware encrypts data on infected devices	44 Backups $178,000	49 Workstation protection system (End Point Security) $88,800	93 File Modification $5,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

Website Defacement Scenario



Attacker exploits the Log4Shell vulnerability in your organization's Internet-accessible systems	22 Vulnerability management $34,000	39 Web Application Firewall (WAF) $138,000	45 Vulnerability Management System (VM) $203,000
Attacker establishes connection to Command & Control (C2) server via proxy service	37 Edge firewall $138,000	38 Internal firewall $72,000	41 IDS/IPS -Intrusion Detection and Prevention System $165,000
Attacker downloads tools (PsExec, Ngrok) and malware (Mimikatz) to compromised device	41 IDS/IPS -Intrusion Detection and Prevention System $165,000	90 File Creation $5,000	125 Network Traffic Flow $5,000
Attacker changes access passwords for local administrator accounts on compromised devices	30 Multi-Factor Authentication (MFA) $85,000	43 Privileged Access Management (PAM) System. $280,000	156 User Account Modification $5,000
Attacker creates additional local accounts with administrative privileges	30 Multi-Factor Authentication (MFA) $85,000	43 Privileged Access Management (PAM) System. $280,000	77 Command Execution $5,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Website Defacement Scenario

Attacker uses the Mimikatz malware to create a domain account with domain administrator rights	30 Multi-Factor Authentication (MFA) $85,000	43 Privileged Access Management (PAM) System. $280,000	153 User Account Creation $5,000
Attacker installs service that runs malware daily with SYSTEM privileges	30 Multi-Factor Authentication (MFA) $85,000	43 Privileged Access Management (PAM) System. $280,000	139 Scheduled Job Creation $5,000
Attacker uses Windows built-in accounts to run tools and commands	15 Configuration management $72,000	57 Configuration Management Database System (CMDB) $48,000	152 User Account Authentication $5,000
Attacker adds exception to Microsoft Defender rules and lists Active Directory devices with use of Powershell commands and scripts	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800	77 Command Execution $5,000
Attackers add exception to Microsoft Defender rules to bypass virus scanning and disable Defender's GUI (graphical interface)	42 Identity and Access Management System (IAM). $178,000	43 Privileged Access Management (PAM) System. $280,000	49 Workstation protection system (End Point Security) $88,800

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Website Defacement Scenario

Attacker gains credentials of other users previously logged on to compromised devices

- 42 Identity and Access Management System (IAM). $178,000
- 43 Privileged Access Management (PAM) System. $280,000
- 49 Workstation protection system (End Point Security) $88,800

Attacker obtains the credentials of other users from other systems of the organization using the Mimikatz malware

- 57 Configuration Management Database System (CMDB) $48,000
- 77 Command Execution $5,000
- 135 Process Creation $5,000

Attacker executes a Powershell script to get a list of all devices in the Organization's Active Directory

- 77 Command Execution $5,000
- 123 Network Connection Creation $5,000
- 135 Process Creation $5,000

Attacker verifies access to the Internet by pinging 8.8.8.8

- 77 Command Execution $5,000
- 135 Process Creation $5,000

Attacker uses RDP connections to infect devices in the Organization's Active Directory environment

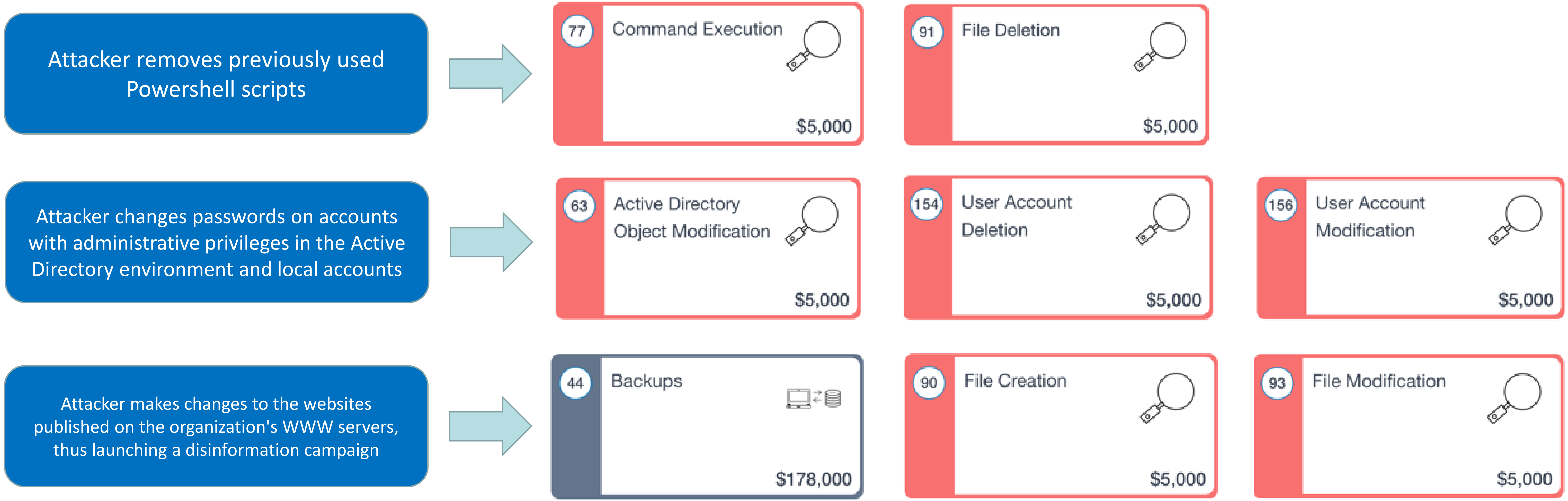
- 32 Secure remote access $45,000
- 38 Internal firewall $72,000
- 43 Privileged Access Management (PAM) System. $280,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

comCERT

Website Defacement Scenario



Attacker removes previously used Powershell scripts

77 Command Execution $5,000

91 File Deletion $5,000

Attacker changes passwords on accounts with administrative privileges in the Active Directory environment and local accounts

63 Active Directory Object Modification $5,000

154 User Account Deletion $5,000

156 User Account Modification $5,000

Attacker makes changes to the websites published on the organization's WWW servers, thus launching a disinformation campaign

44 Backups $178,000

90 File Creation $5,000

93 File Modification $5,000

ORGANIZATION PHYSICAL INFRASTRUCTURE ENTIRE NETWORK NETWORK EDGE

INTERNAL NETWORK HOST APPLICATIONS DATA DATA SOURCES

Summary (MITRE - Mitigations)

Mitigation	Mitigated techniques use count by Threat Actors	Mitigated techniques use count by Malware	Techniques mitigated count
Privileged Account Management	102	103	103
User Account Management	83	94	82
Pre-compromise	74	74	75
Audit	66	66	67
Execution Prevention	62	62	63
Network Intrusion Prevention	58	57	58
Restrict File and Directory Permissions	55	55	56
Disable or Remove Feature or Program	55	54	55
Password Policies	42	43	43
User Training	40	39	40
Network Segmentation	43	41	39
Filter Network Traffic	39	38	39
Behavior Prevention on Endpoint	37	36	37
Operating System Configuration	35	35	36
Multi-factor Authentication	40	38	36
Update Software	31	33	31

https://jkb-s.github.io/snake-attack/

comCERT

Summary (MITRE – Data Sources)

Data source	Data component	Sum of techniques' use count by Threat Actors	Sum of techniques' use count by Malware	Techniques count
Process		2051	6431	326
Network Traffic		1620	3367	236
Command		1530	4364	256
File		1390	3304	280
Windows Registry		374	1314	86
Script		302	720	26
Application Log		292	127	55
Module		256	532	50
Logon Session		240	117	41
Service		150	493	32

https://jkb-s.github.io/snake-attack/

Summary (MITRE – Data Sources)

Data source	Data component	Sum of techniques' use count by Threat Actors	Sum of techniques' use count by Malware	Techniques count
Process	OS API Execution	474	2176	78
	Process Access	102	236	18
	Process Creation	1361	3659	207
	Process Metadata	68	160	11
	Process Modification	26	128	9
	Process Termination	20	72	3
Process Summary		**2051**	**6431**	**326**
Network Traffic	Network Connection Creation	436	855	58
	Network Traffic Content	609	1358	96
	Network Traffic Flow	575	1154	82
Network Traffic Suma		**1620**	**3367**	**236**
Command	Command Execution	1530	4364	256
Command Summary		**1530**	**4364**	**256**
File	File Access	270	560	46
	File Creation	534	1031	88
	File Deletion	53	236	10
	File Metadata	249	676	37
	File Modification	284	801	99
File Summary		**1390**	**3304**	**280**
Windows Registry	Windows Registry Key Access	40	118	7
	Windows Registry Key Creation	99	342	17
	Windows Registry Key Deletion	38	162	4
	Windows Registry Key Modification	197	692	58
Windows Registry Summary		**374**	**1314**	**86**

https://jkb-s.github.io/snake-attack/

Cyber Fortress Enterprise - training

The Vendor Event

Cyber Fortress Education

POLITECHNIKA WARSZAWSKA
WARSAW UNIVERSITY OF TECHNOLOGY

WAT
Military University of Technology

WSB Universities

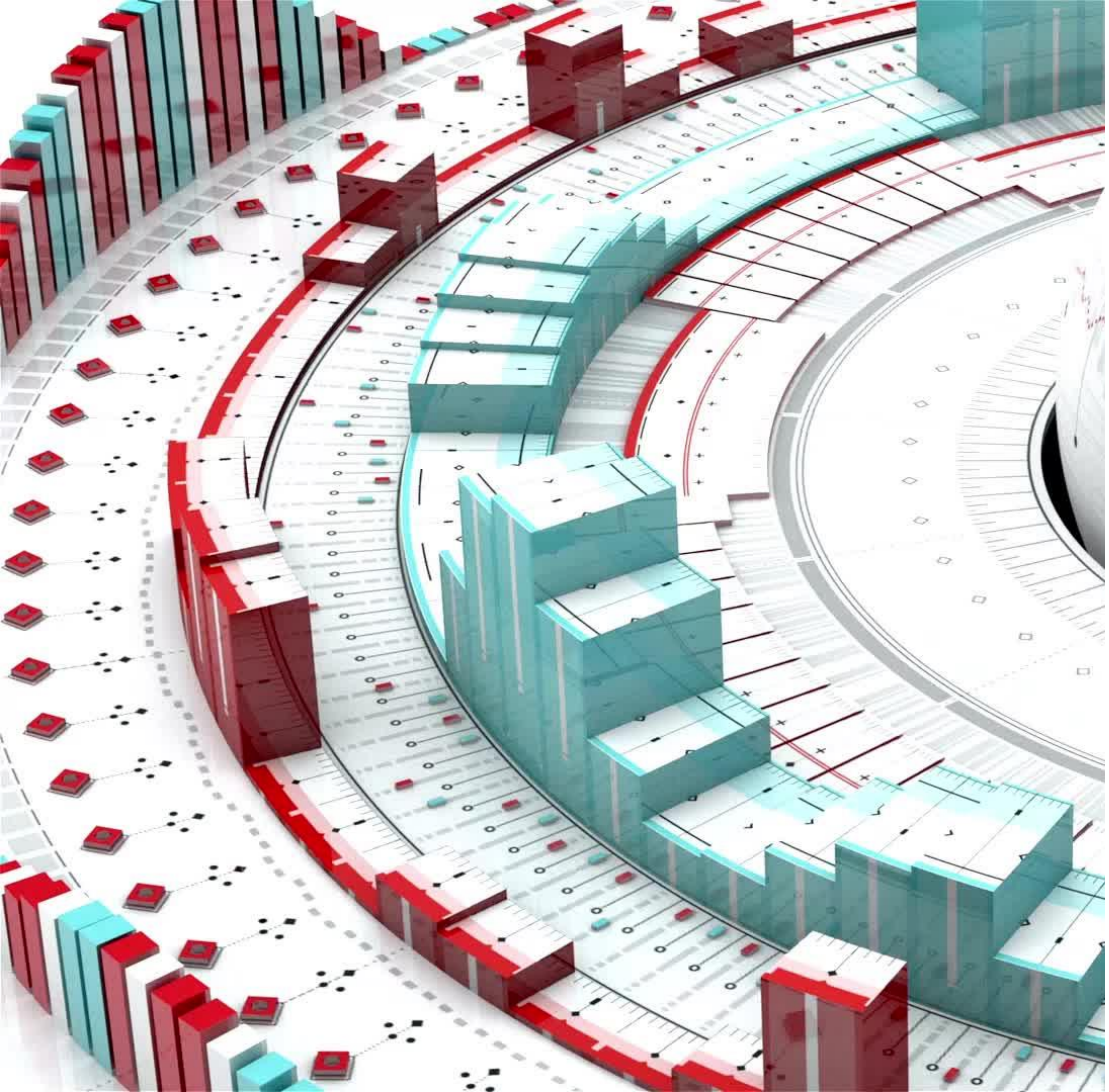
PJAIT
POLISH-JAPANESE ACADEMY OF INFORMATION TECHNOLOGY

ISSA POLSKA

ISACA®

POLISH NAVAL ACADEMY
of the Heroes of Westerplatte

comCERT



Cyber Fortress LAB

- Using Real Life IT and OT Environments
- Emulation of TTP used in game scenarios
- Checking of efficiency chosen safeguards and data sources
- Verification of resiliense and visibility of real environments

And the Winner is…

1st Game Session	
Ardenia	55,14%
Delmarva	52,06%
Calendria	47,08%
Talgar	41,13%
Rivia	40,57%
Eledor	27,27%
Verden	27,12%

2nd Game Session	
Verden	67,04%
Calendria	65,78%
Rivia	64,39%
Eledor	61,59%
Ardenia	58,84%
Delmarva	54,00%
Talgar	53,03%

And the Winner is…

1st place:	Ardenia	– 113,98
2nd place:	Calendria	– 112,86
3rd place:	Delmarva	– 106,06

Thank you!

CYBER FORTRESS
ENTERPRISE

comCERT

ComCERT SA

Adama Branickiego 13 Street, 02-972 Warsaw

E-mail: biuro@comcert.pl   tel: +48 22 112 06 83

NIP: 5252524691   **KRS:** 0000406425   **REGON:** 145934931