ADVANCED PERSISTENT THREATS

TARGETING BUSINESSES OF ALL SIZES

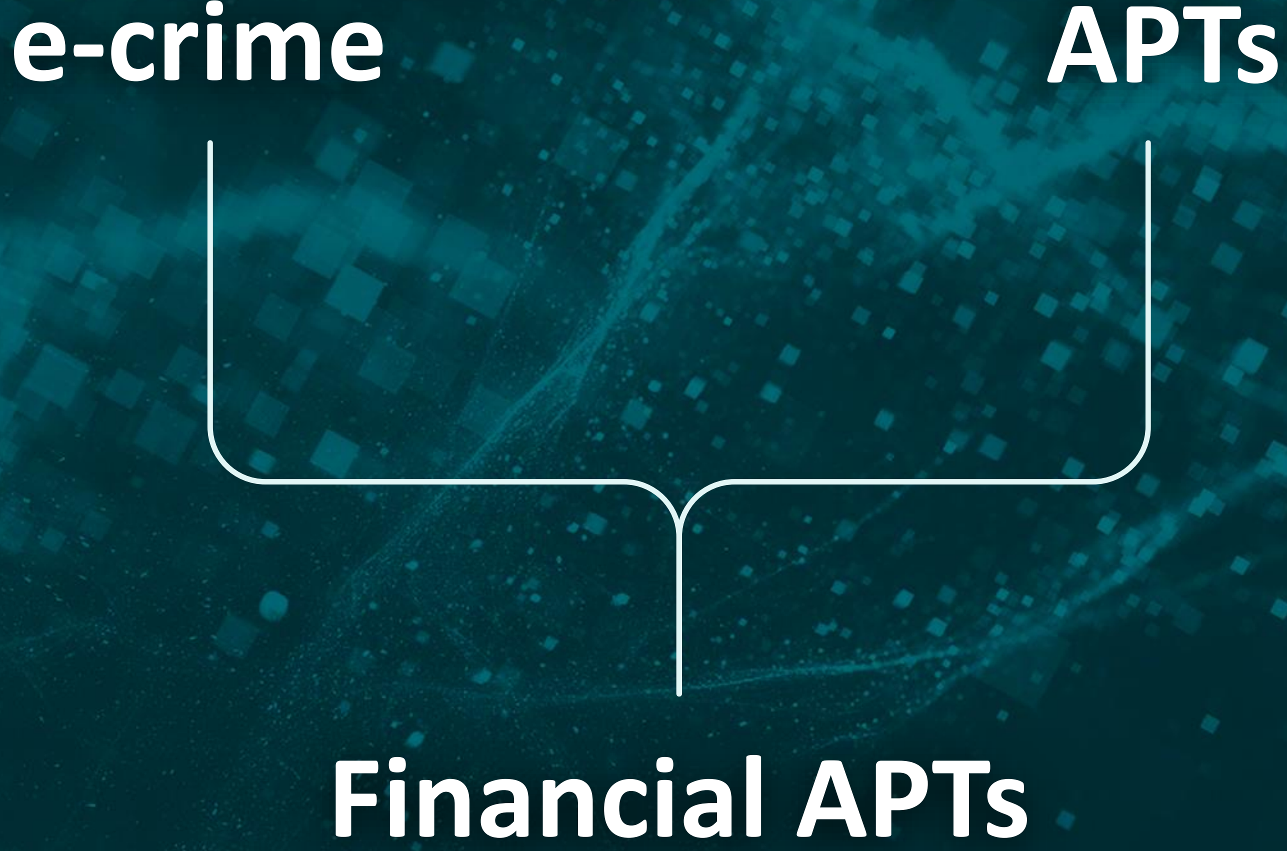
Robert Lipovský

Senior Malware Researcher

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

e-crime

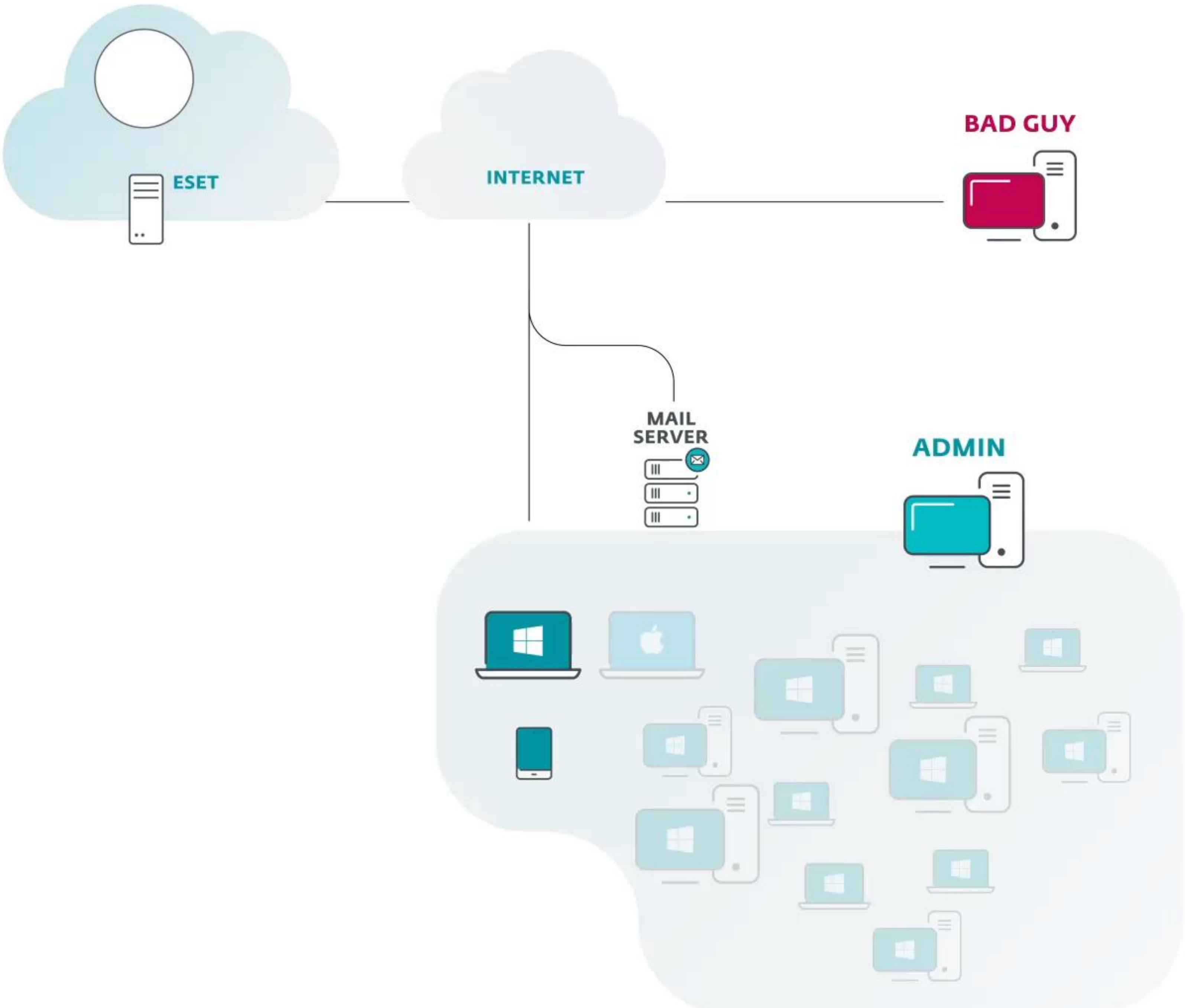
APTs

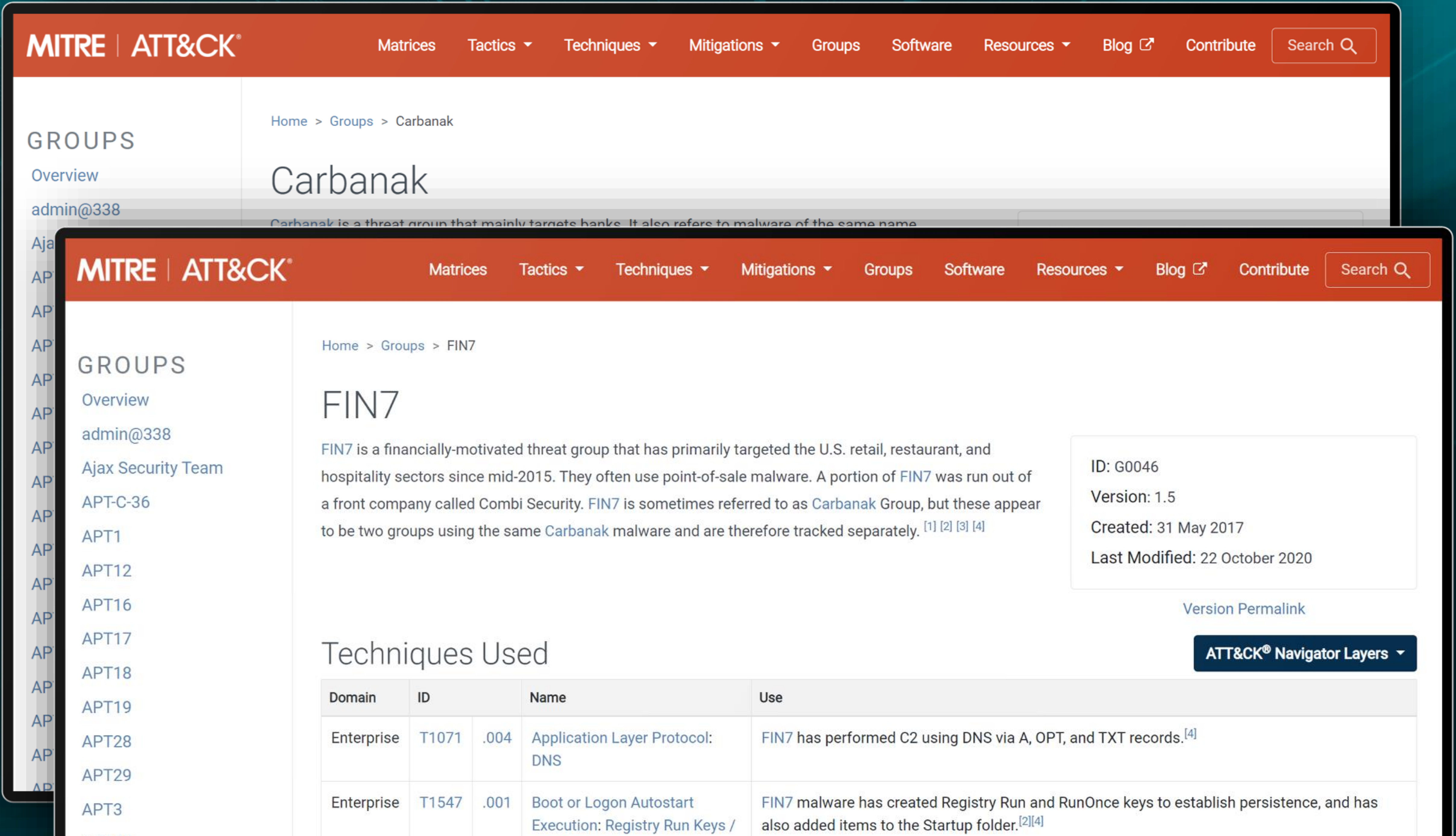


e-crime

APTs

Financial APTs


ESET
INTERNET
BAD GUY
MAIL
SERVER
ADMIN



Home > Groups > Carbanak

Carbanak

Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name.

Home > Groups > FIN7

FIN7

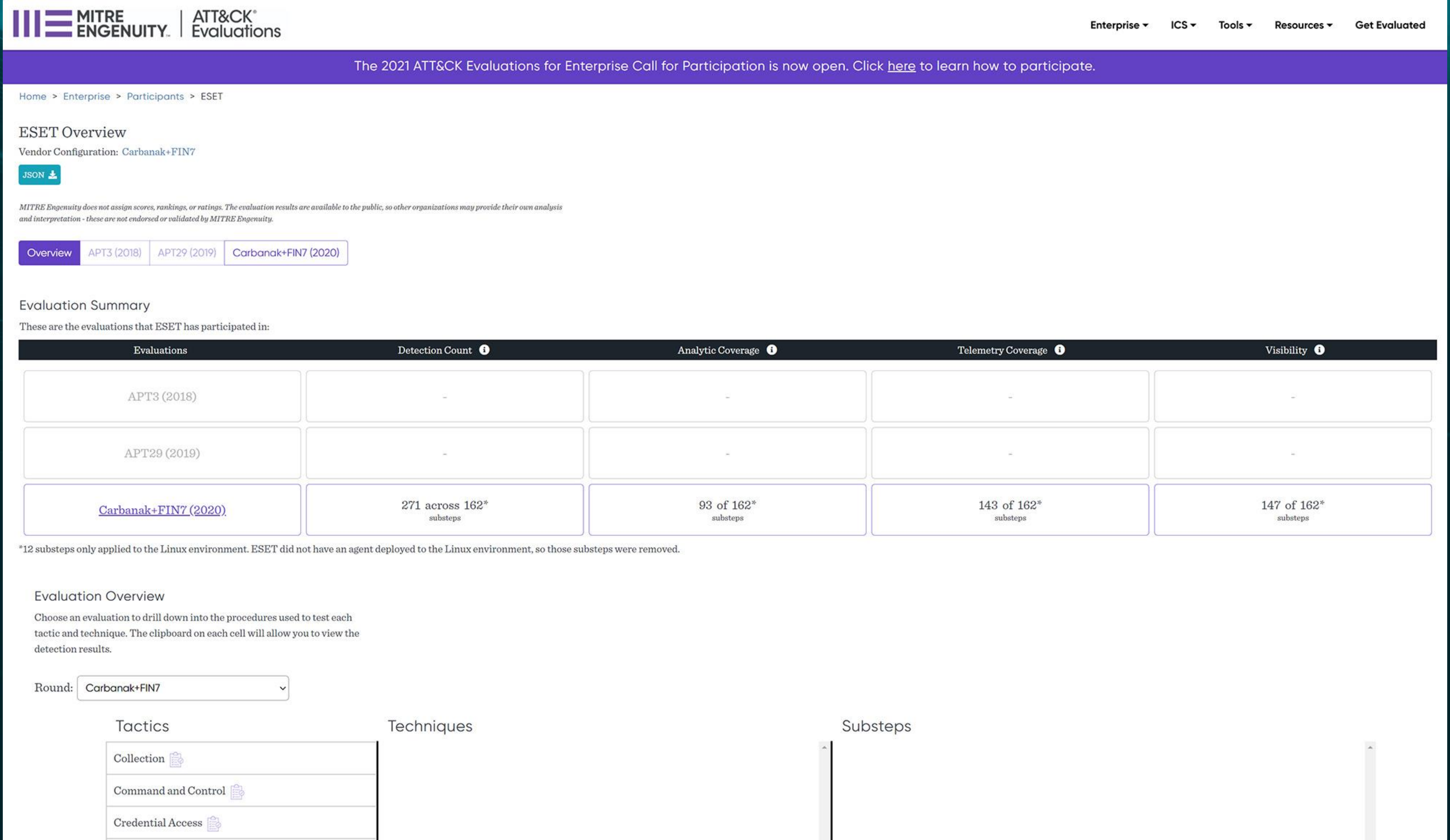
FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. [1] [2] [3] [4]

ID: G0046
Version: 1.5
Created: 31 May 2017
Last Modified: 22 October 2020

Version Permalink

Techniques Used

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	FIN7 has performed C2 using DNS via A, OPT, and TXT records.[4]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys /	FIN7 malware has created Registry Run and RunOnce keys to establish persistence, and has also added items to the Startup folder.[2][4]



The 2021 ATT&CK Evaluations for Enterprise Call for Participation is now open. Click here to learn how to participate.

Home > Enterprise > Participants > ESET

ESET Overview

Vendor Configuration: Carbanak+FIN7

MITRE Engenuity does not assign scores, rankings, or ratings. The evaluation results are available to the public, so other organizations may provide their own analysis and interpretation - these are not endorsed or validated by MITRE Engenuity.

Evaluation Summary

These are the evaluations that ESET has participated in:

Evaluations	Detection Count	Analytic Coverage	Telemetry Coverage	Visibility
APT3 (2018)	-	-	-	-
APT29 (2019)	-	-	-	-
Carbanak+FIN7 (2020)	271 across 162* substeps	93 of 162* substeps	143 of 162* substeps	147 of 162* substeps

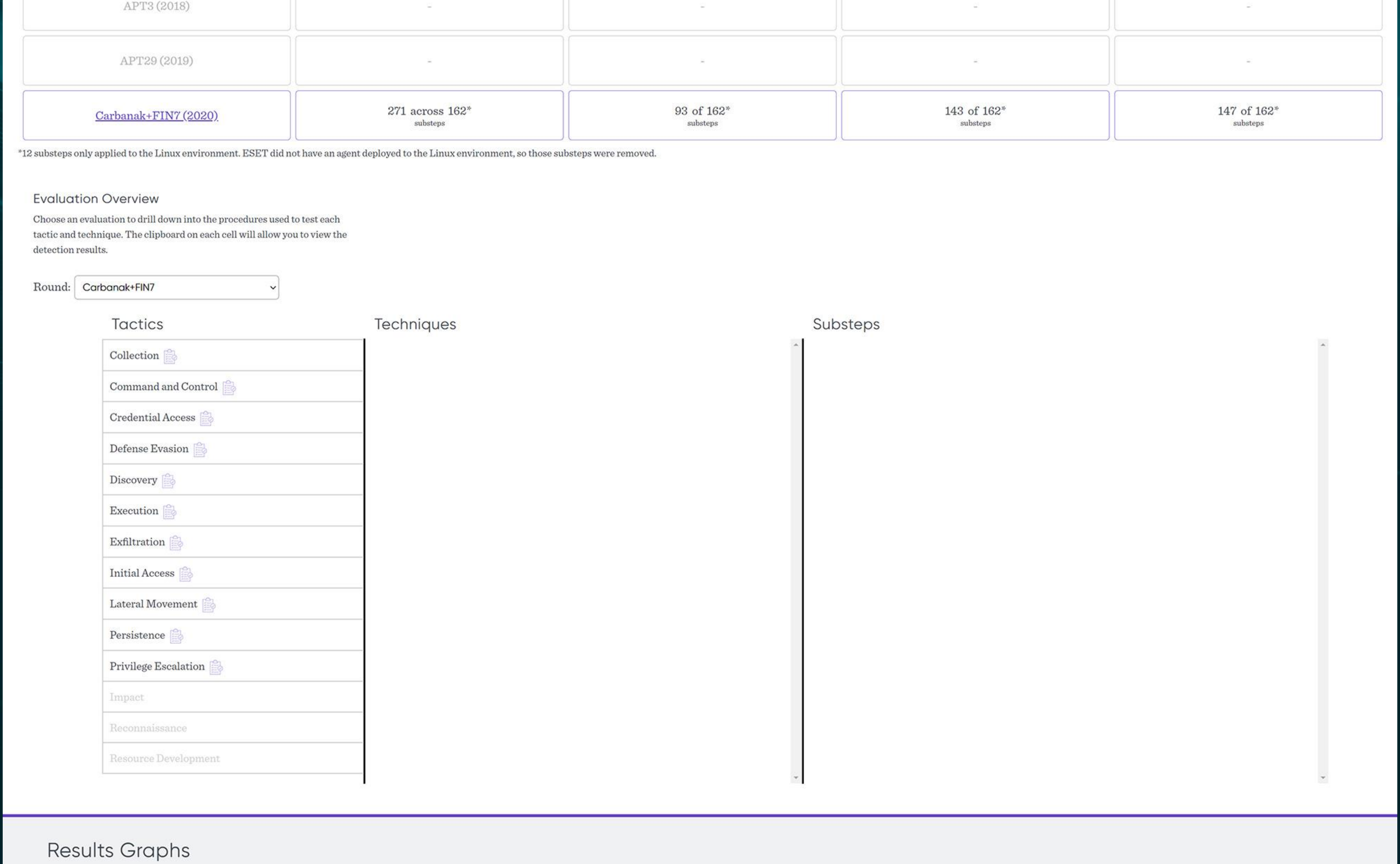
*12 substeps only applied to the Linux environment. ESET did not have an agent deployed to the Linux environment, so those substeps were removed.

Evaluation Overview

Choose an evaluation to drill down into the procedures used to test each tactic and technique. The clipboard on each cell will allow you to view the detection results.

Round: Carbanak+FIN7

Tactics	Techniques	Substeps
Collection		
Command and Control		
Credential Access		



APT3 (2018)	-	-	-	-
APT29 (2019)	-	-	-	-
Carbanak+FIN7 (2020)	271 across 162* substeps	93 of 162* substeps	143 of 162* substeps	147 of 162* substeps

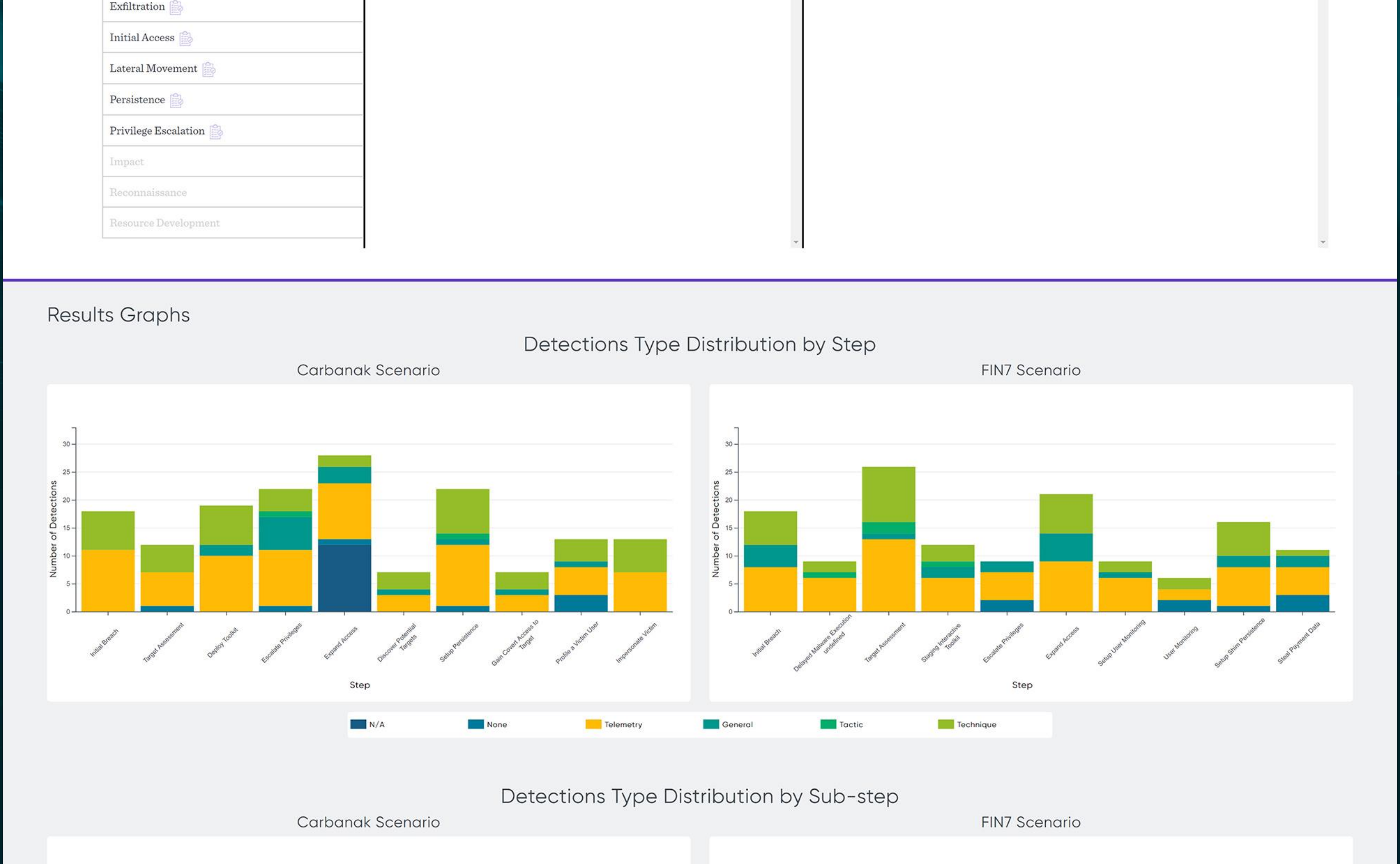
*12 substeps only applied to the Linux environment. ESET did not have an agent deployed to the Linux environment, so those substeps were removed.

Evaluation Overview

Choose an evaluation to drill down into the procedures used to test each tactic and technique. The clipboard on each cell will allow you to view the detection results.

Round: Carbanak+FIN7

Results Graphs



- Exfiltration
- Initial Access
- Lateral Movement
- Persistence
- Privilege Escalation
- Impact
- Reconnaissance
- Resource Development

Results Graphs

Detections Type Distribution by Step

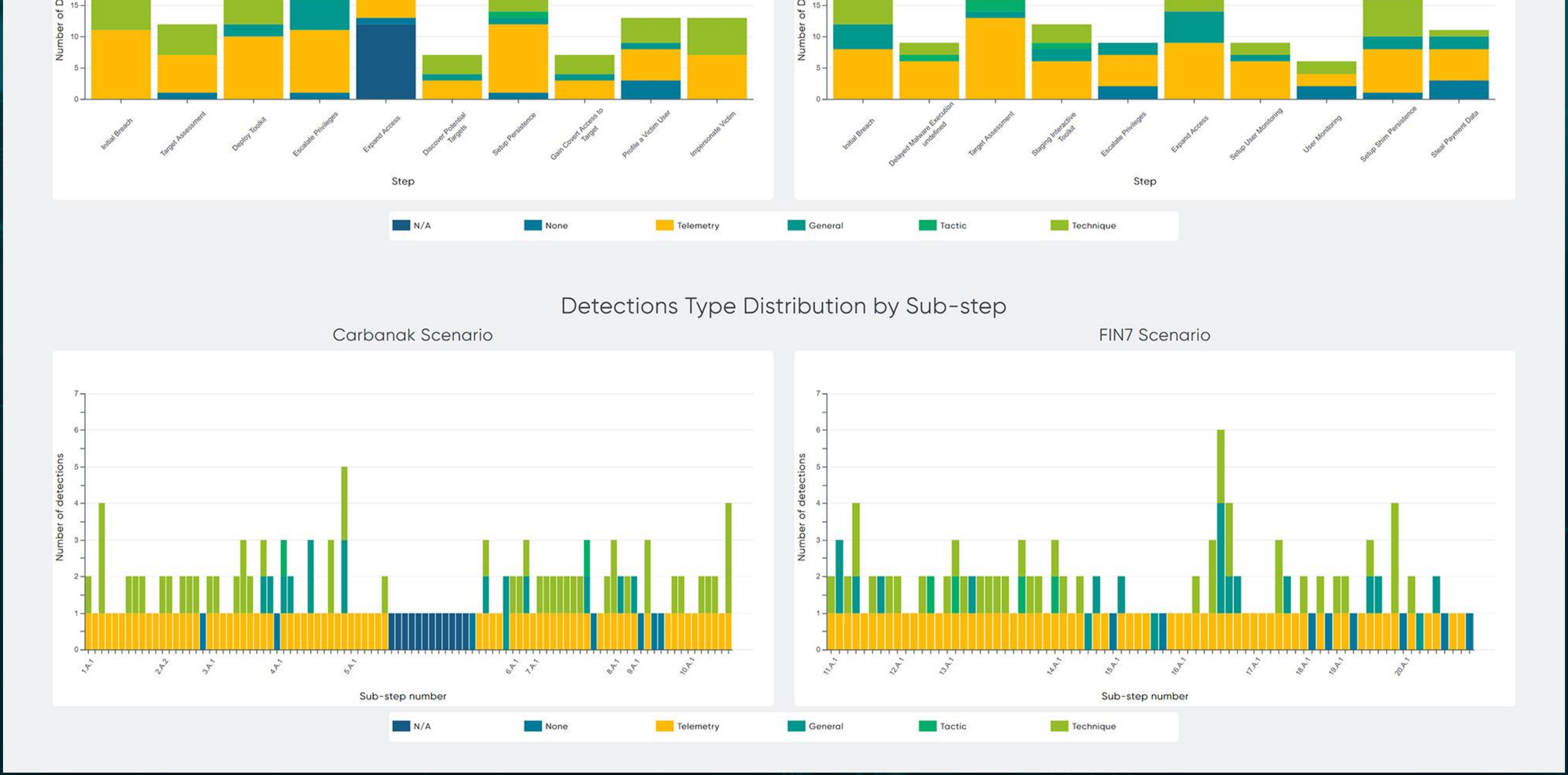
Carbanak Scenario

FIN7 Scenario

Detections Type Distribution by Sub-step

Carbanak Scenario

FIN7 Scenario

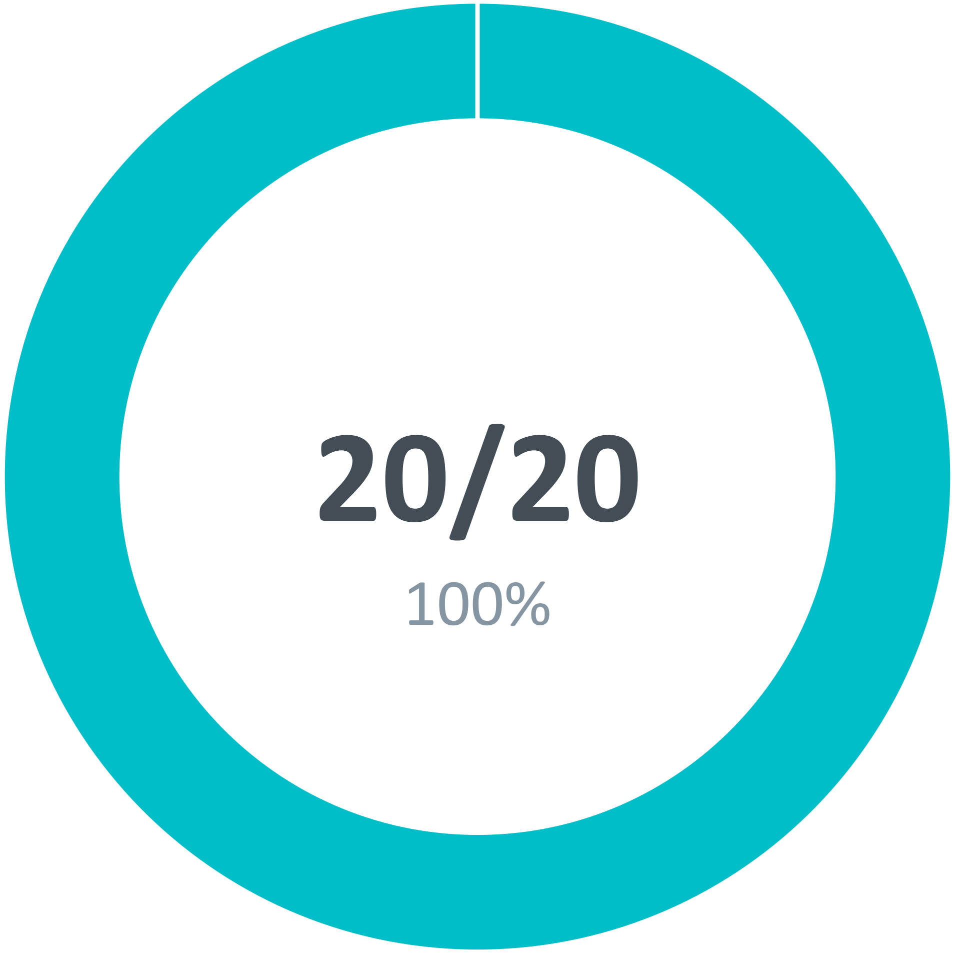


Detections Type Distribution by Sub-step

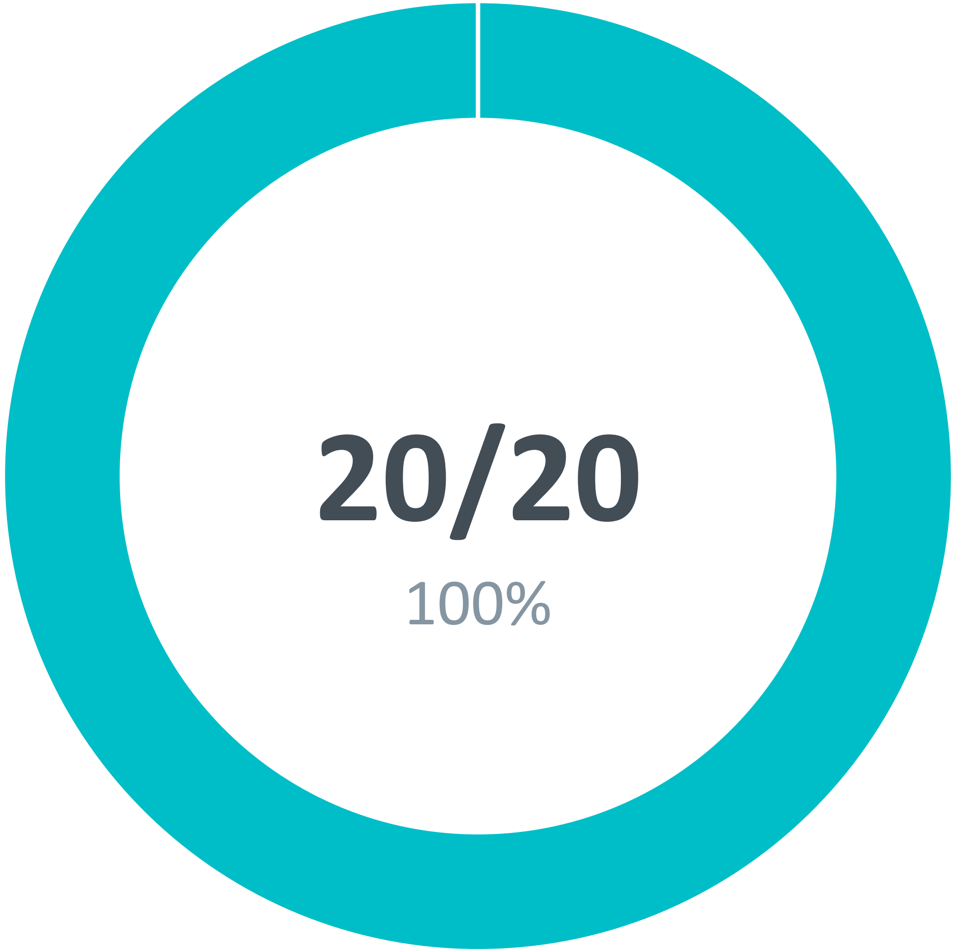
Carbanak Scenario

FIN7 Scenario

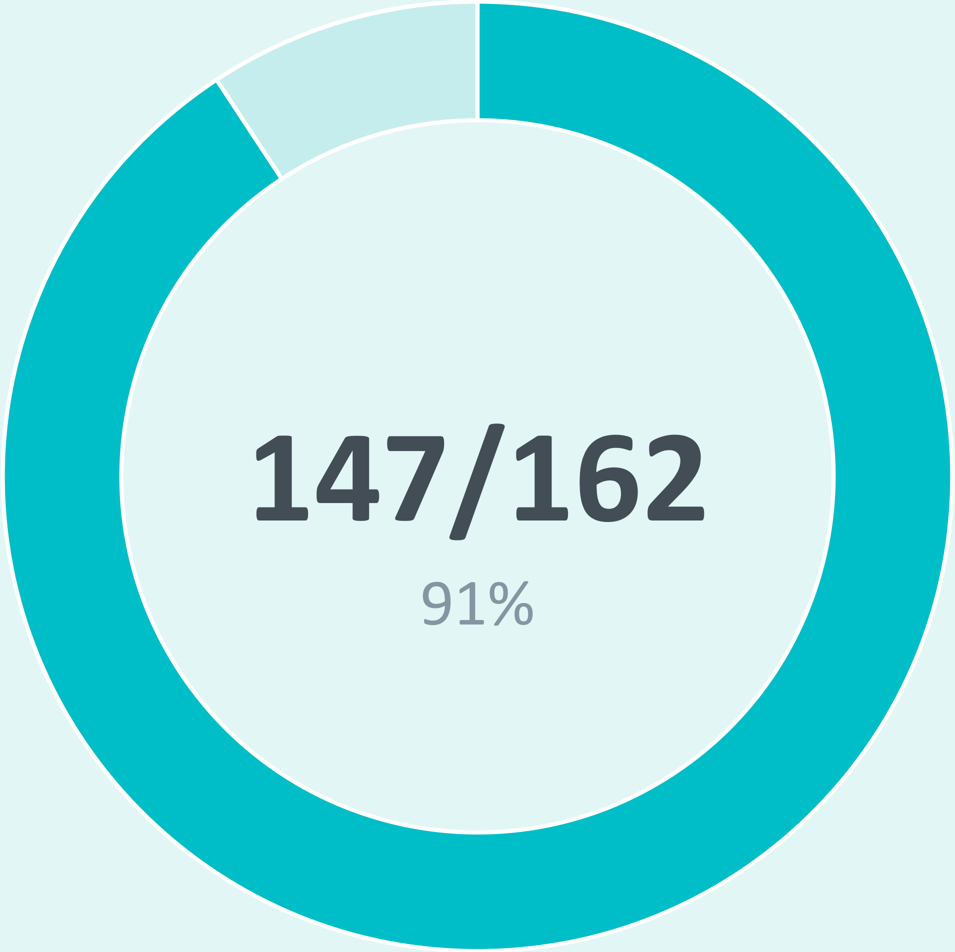
Steps detected



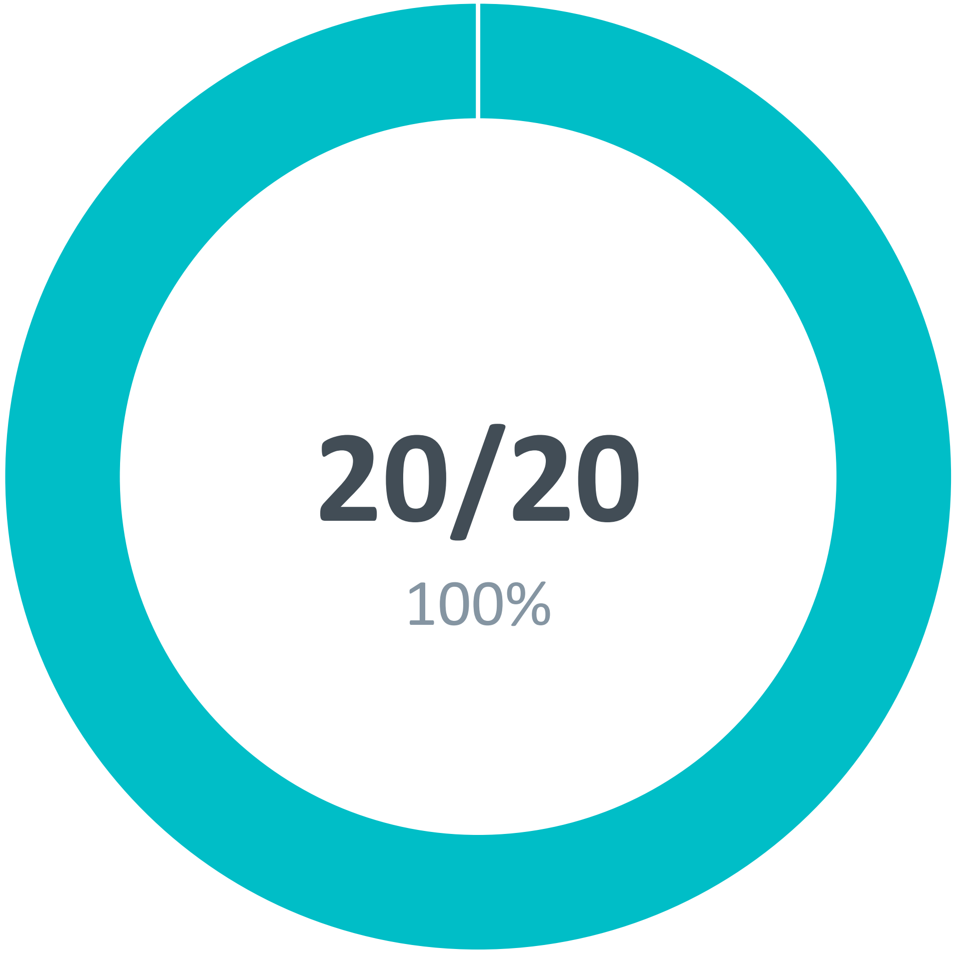
Steps detected

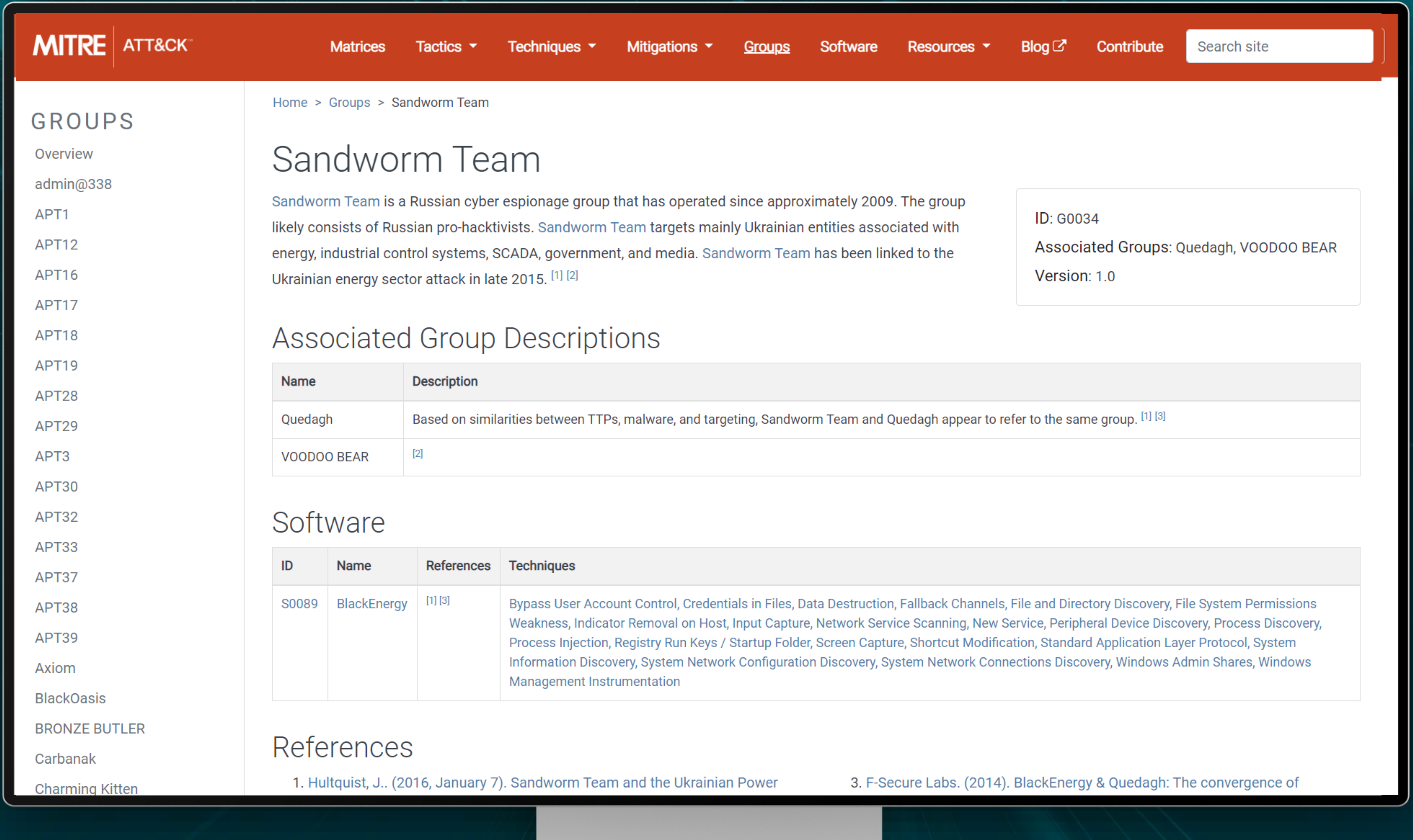


Sub-steps detected



Steps detected





Home > Groups > Sandworm Team

Sandworm Team

Sandworm Team is a Russian cyber espionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. [1] [2]

ID: G0034
Associated Groups: Quedagh, VOODOO BEAR
Version: 1.0

Associated Group Descriptions

Name	Description
Quedagh	Based on similarities between TTPs, malware, and targeting, Sandworm Team and Quedagh appear to refer to the same group. [1] [3]
VOODOO BEAR	[2]

Software

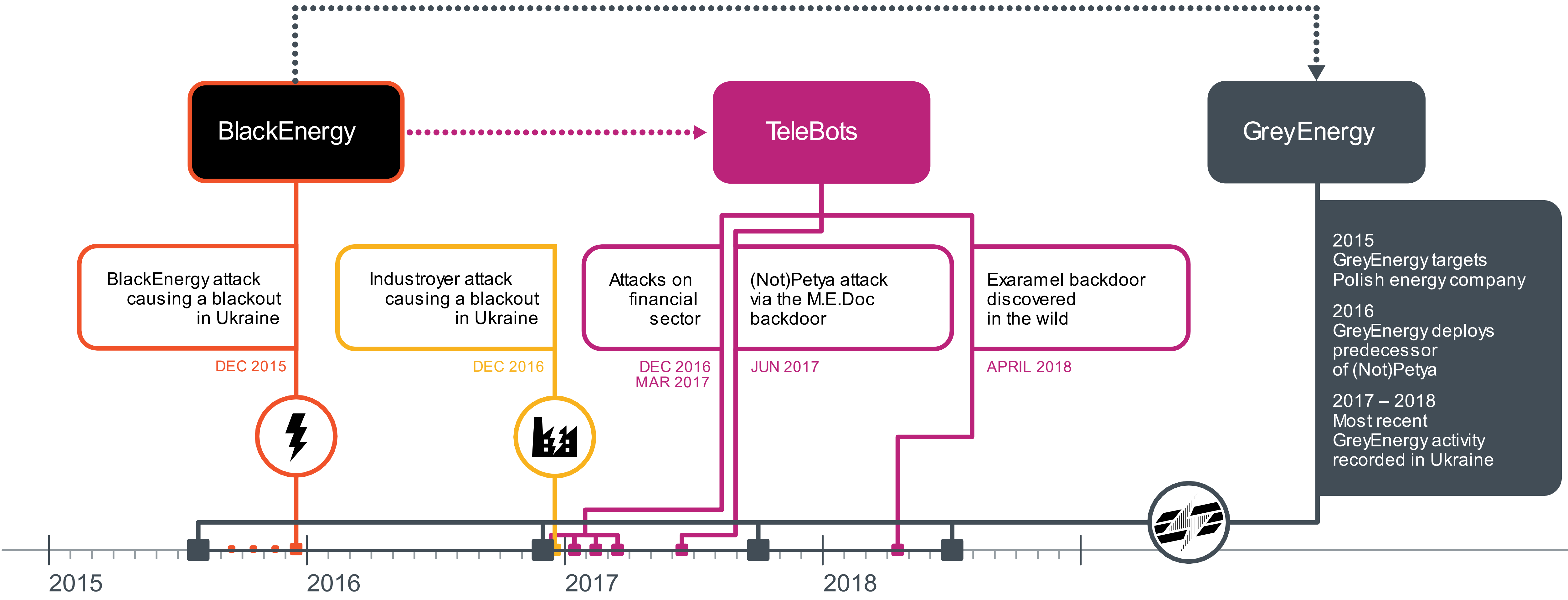
ID	Name	References	Techniques
S0089	BlackEnergy	[1] [3]	Bypass User Account Control, Credentials in Files, Data Destruction, Fallback Channels, File and Directory Discovery, File System Permissions Weakness, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Peripheral Device Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Windows Admin Shares, Windows Management Instrumentation

References

1. Hultquist, J.. (2016, January 7). Sandworm Team and the Ukrainian Power

3. F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of

Sandworm



BlackEnergy

TeleBots

GreyEnergy

BlackEnergy attack causing a blackout in Ukraine

DEC 2015

Industroyer attack causing a blackout in Ukraine

DEC 2016

Attacks on financial sector

DEC 2016 MAR 2017

(Not)Petya attack via the M.E.Doc backdoor

JUN 2017

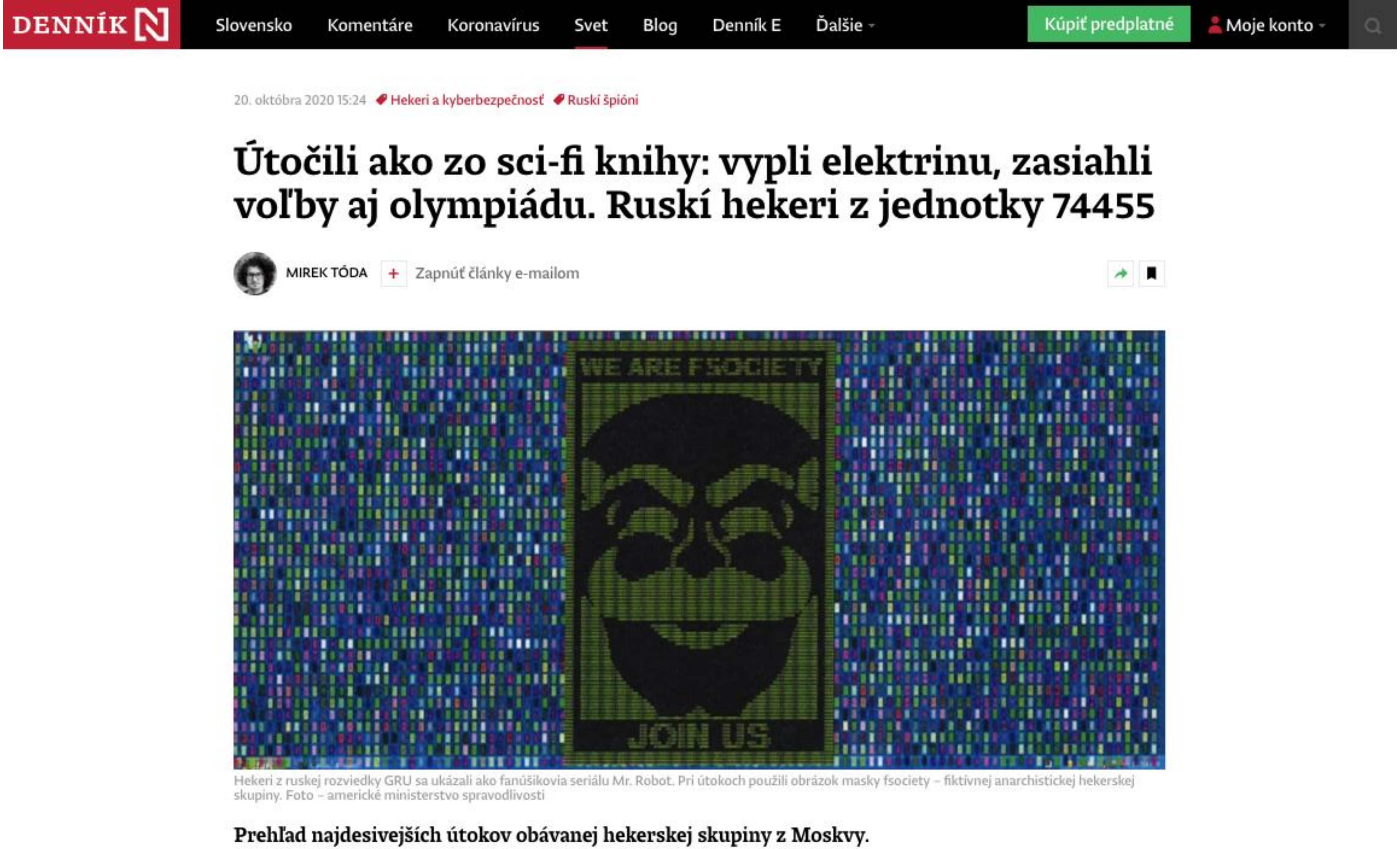
Exaramel backdoor discovered in the wild

APRIL 2018

2015
GreyEnergy targets Polish energy company

2016
GreyEnergy deploys predecessor of (Not)Petya

2017 – 2018
Most recent GreyEnergy activity recorded in Ukraine



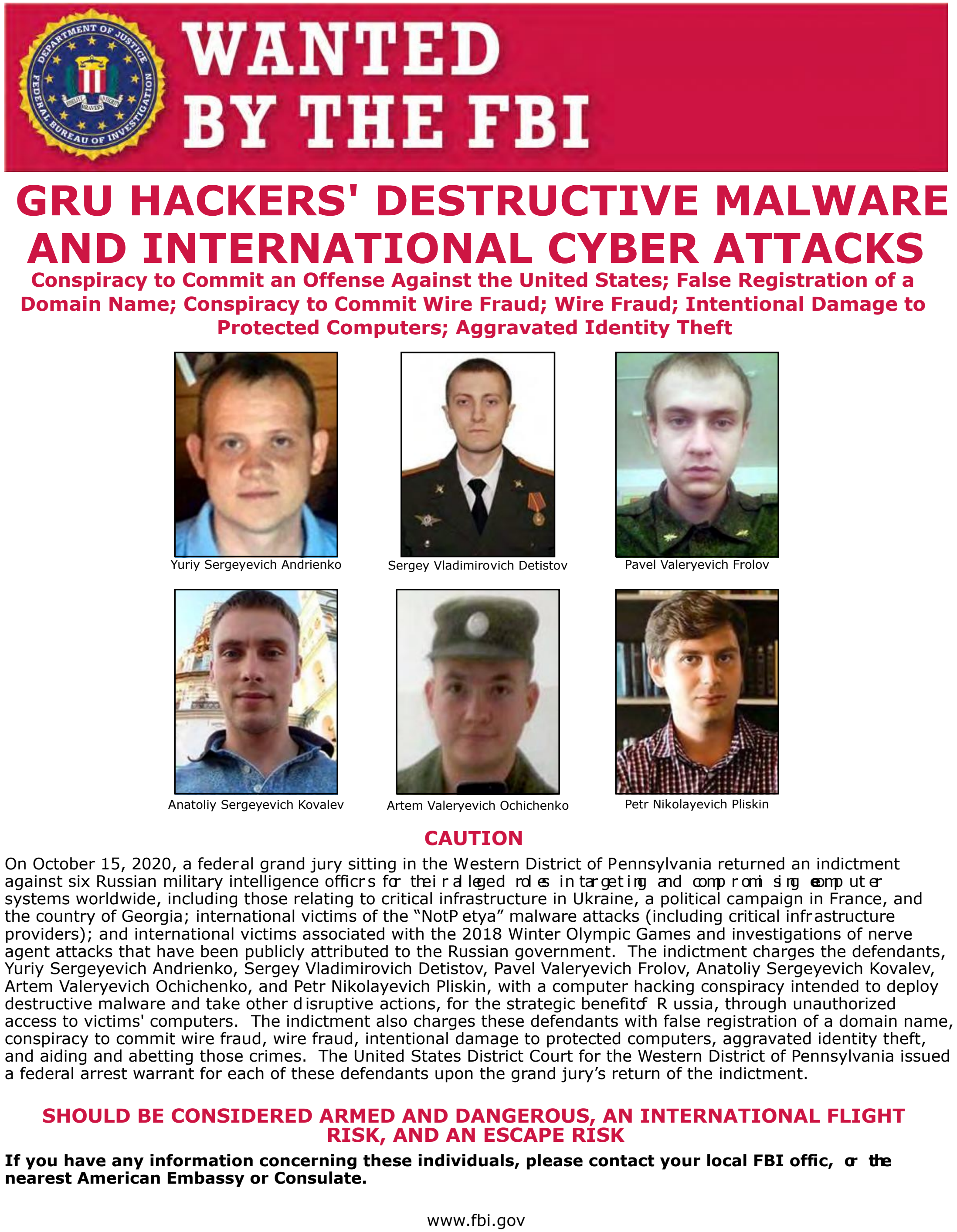
20. októbra 2020 15:24 Hekeri a kyberbezpečnosť Ruskí špióni

Útočili ako zo sci-fi knihy: vypli elektrinu, zasiahli voľby aj olympiádu. Ruskí hekeri z jednotky 74455

MIREK TÓDA + Zapnúť články e-mailom

Hekeri z ruskej rozviedky GRU sa ukázali ako fanúšikovia seriálu Mr. Robot. Pri útokoch použili obrázok masky fsociety – fiktívnej anarchistickej hekerskej skupiny. Foto – americké ministerstvo spravodlivosti

Prehľad najdesivejších útokov obávanej hekerskej skupiny z Moskvy.



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officrs for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the “NotPetya” malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefitof Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aiding and abetting those crimes. The United States District Court for the Western District of Pennsylvania issued a federal arrest warrant for each of these defendants upon the grand jury’s return of the indictment.

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI offic, or the nearest American Embassy or Consulate.

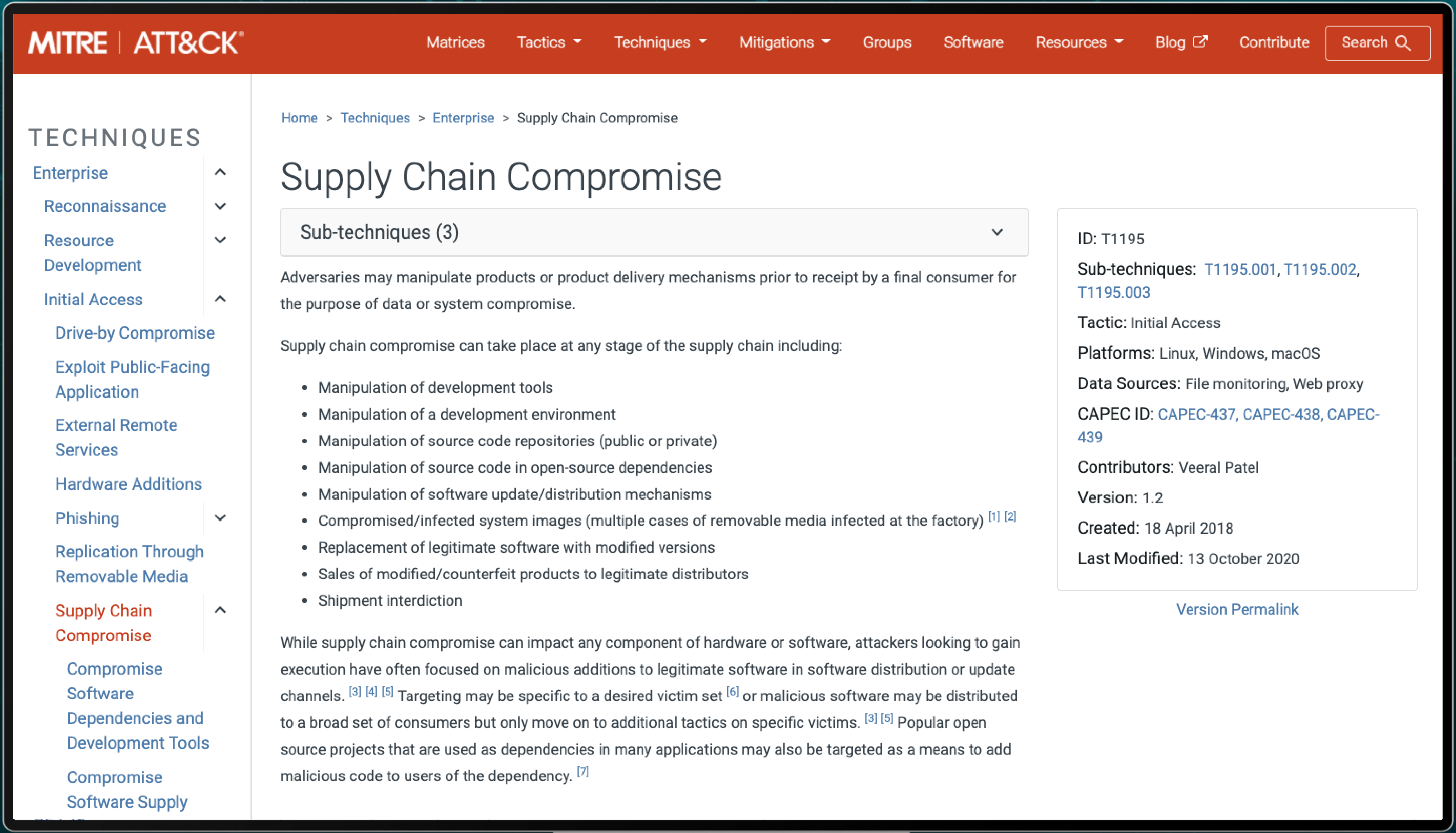
www.fbi.gov

SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS

DESCRIPTION AND REMEDIATION

1.0
27/01/2021

TLP:WHITE



Supply Chain Compromise

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory) [1] [2]
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. [3] [4] [5] Targeting may be specific to a desired victim set [6] or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. [3] [5] Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency. [7]

ID: T1195

Sub-techniques: T1195.001, T1195.002, T1195.003

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: File monitoring, Web proxy

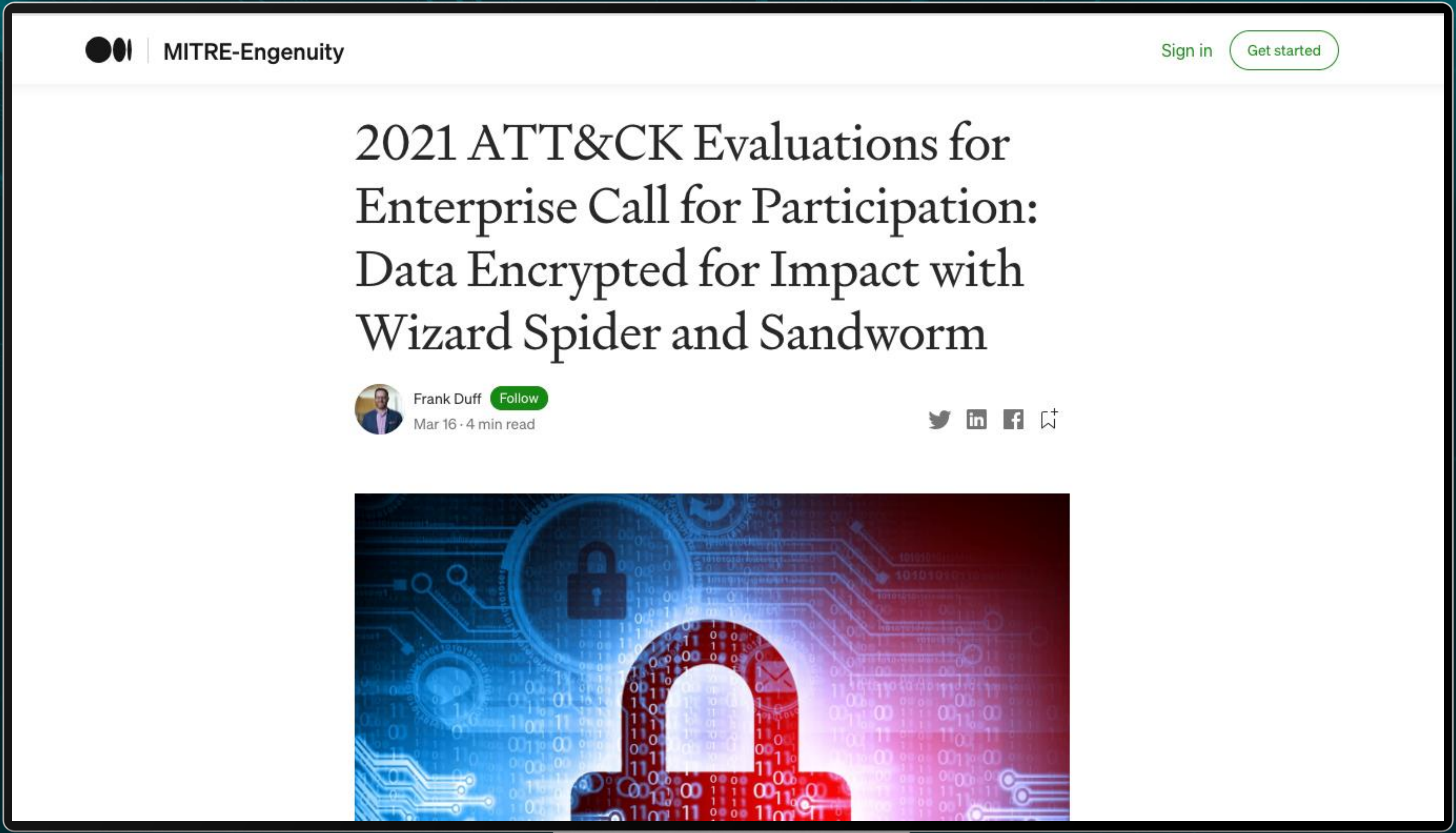
CAPEC ID: CAPEC-437, CAPEC-438, CAPEC-439

Contributors: Veeral Patel

Version: 1.2

Created: 18 April 2018

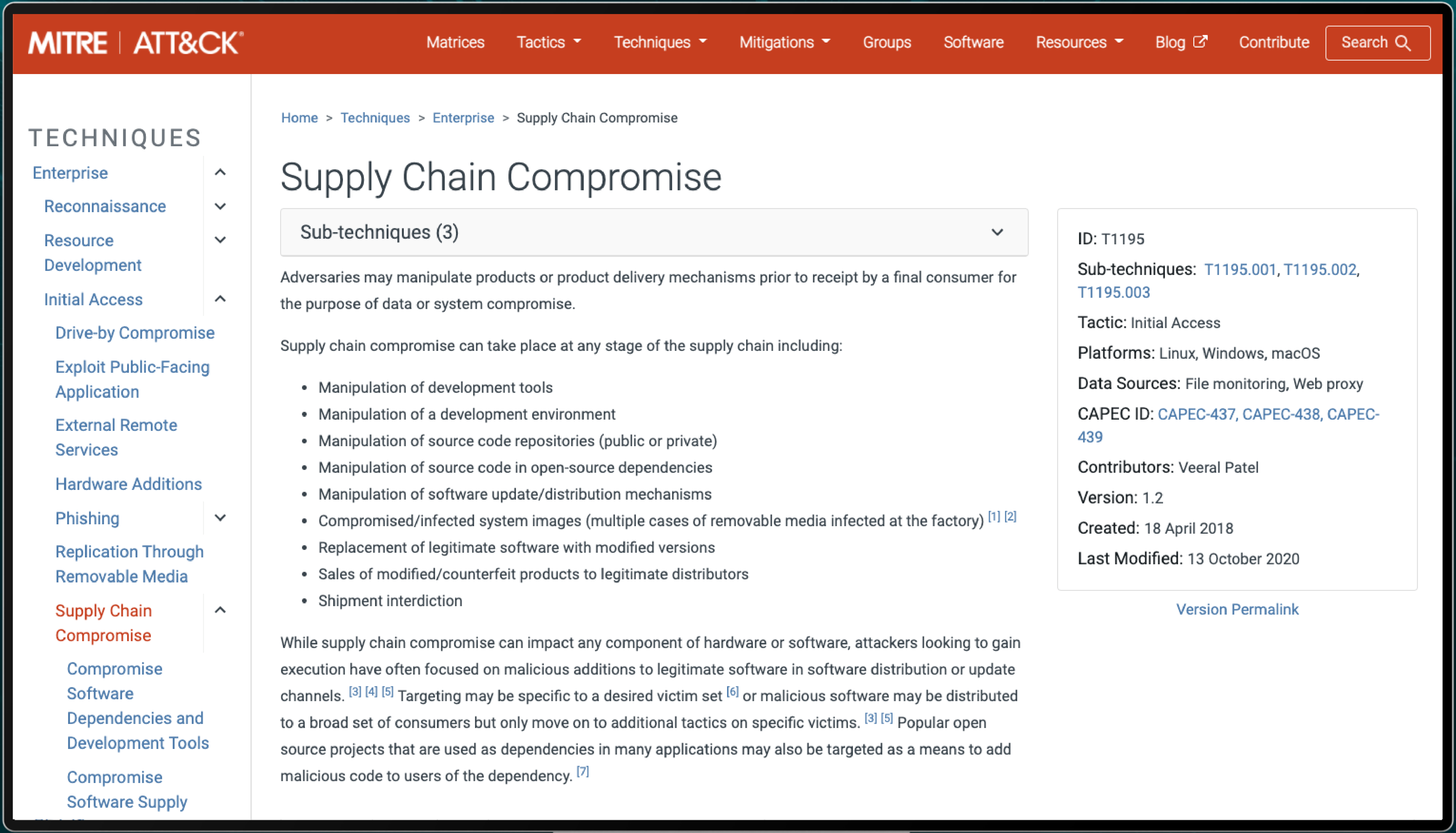
Last Modified: 13 October 2020



2021 ATT&CK Evaluations for Enterprise Call for Participation: Data Encrypted for Impact with Wizard Spider and Sandworm

Frank Duff

Mar 16 · 4 min read



Supply Chain Compromise

Sub-techniques (3)

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory) [1] [2]
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. [3] [4] [5] Targeting may be specific to a desired victim set [6] or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. [3] [5] Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency. [7]

ID: T1195

Sub-techniques: T1195.001, T1195.002, T1195.003

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: File monitoring, Web proxy

CAPEC ID: CAPEC-437, CAPEC-438, CAPEC-439

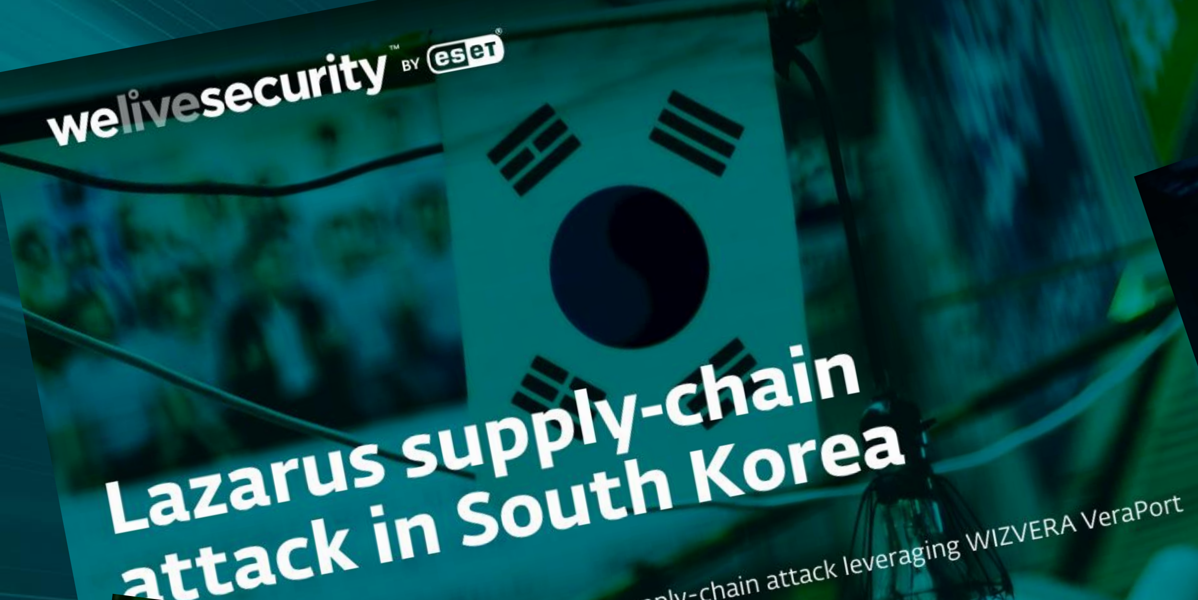
Contributors: Veeral Patel

Version: 1.2

Created: 18 April 2018

Last Modified: 13 October 2020

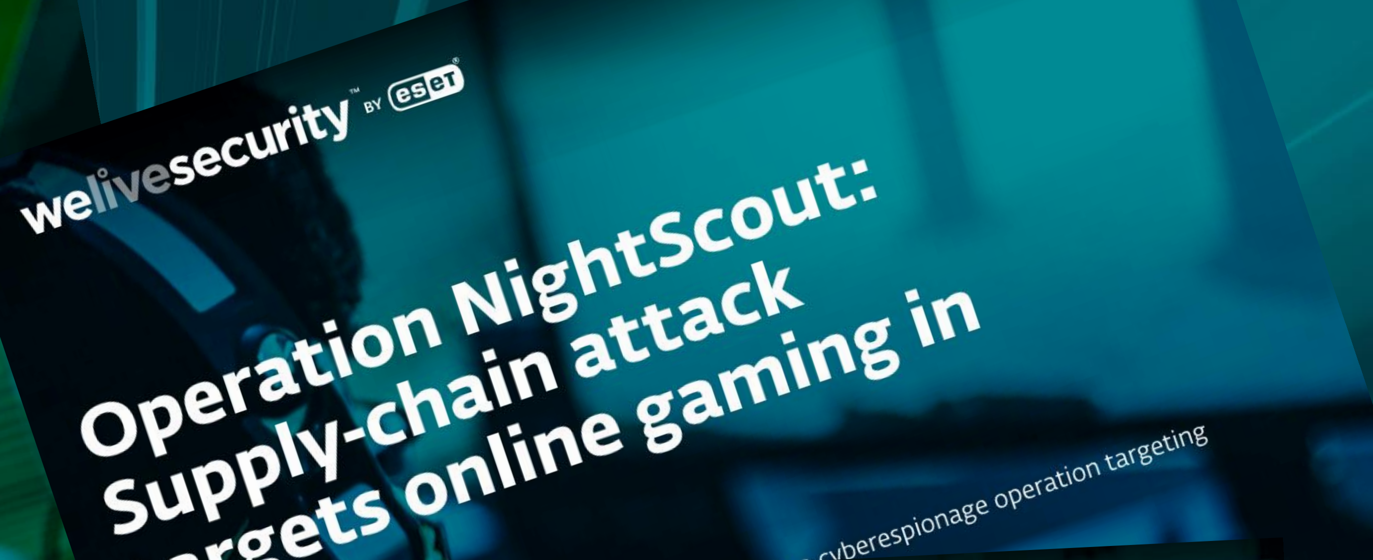
Version Permalink



welivesecurity™ BY eset

Lazarus supply-chain attack in South Korea

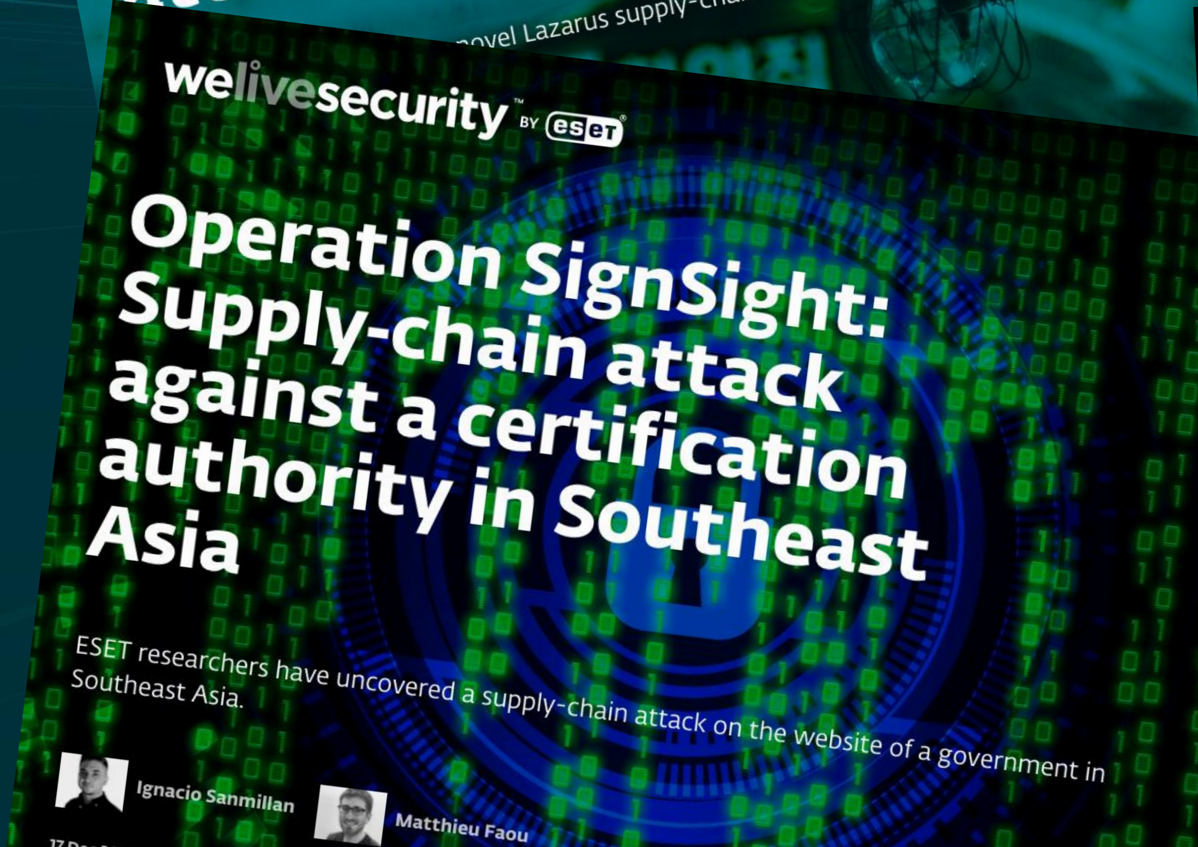
…novel Lazarus supply-chain attack leveraging WIZVERA VeraPort



welivesecurity™ BY eset

Operation NightScout: Supply-chain attack targets online gaming in

…cyberespionage operation targeting



welivesecurity™ BY eset

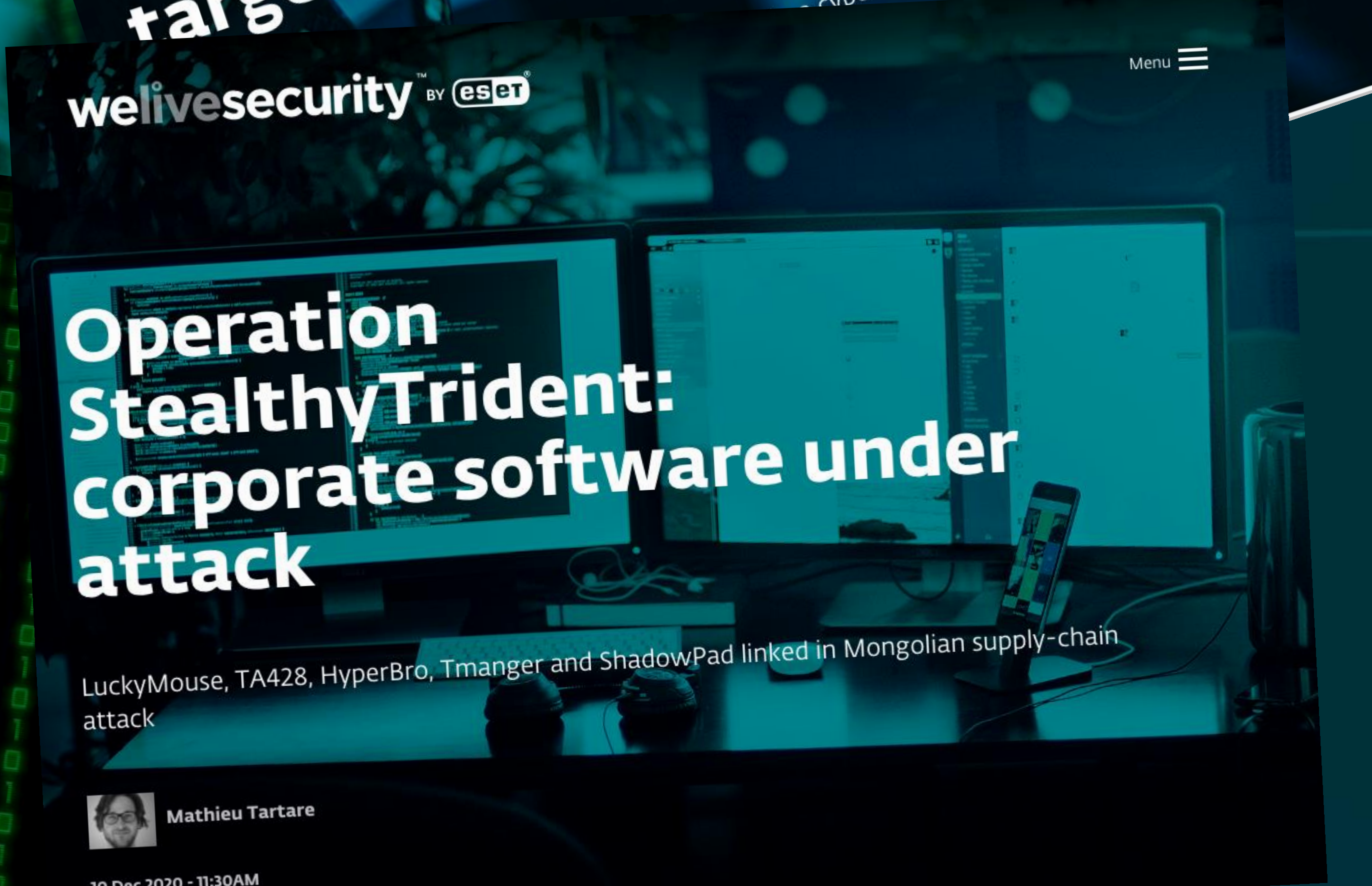
Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

ESET researchers have uncovered a supply-chain attack on the website of a government in Southeast Asia.

Ignacio Sanmillan

Matthieu Faou

17 Dec



welivesecurity™ BY eset

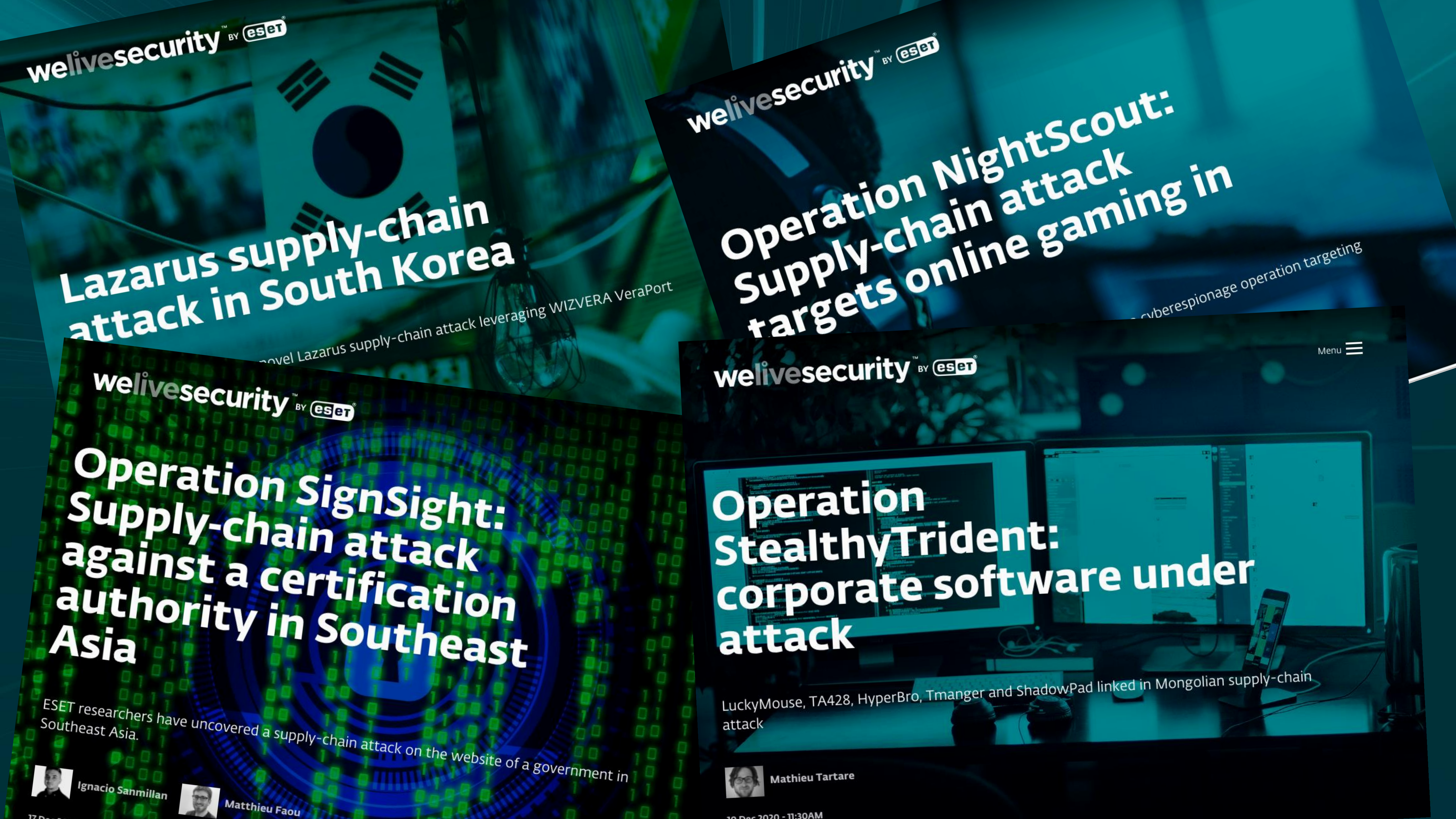
Menu

Operation StealthyTrident: corporate software under attack

LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack

Mathieu Tartare

10 Dec 2020 - 11:30AM



welivesecurity BY eset

Lazarus supply-chain attack in South Korea

novel Lazarus supply-chain attack leveraging WIZVERA VeraPort

welivesecurity BY eset

Operation NightScout: Supply-chain attack targets online gaming in

cyberespionage operation targeting

welivesecurity BY eset

Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia

ESET researchers have uncovered a supply-chain attack on the website of a government in Southeast Asia.

Ignacio Sanmillan

Matthieu Faou

welivesecurity BY eset

Menu

Operation StealthyTrident: corporate software under attack

LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack

Mathieu Tartare

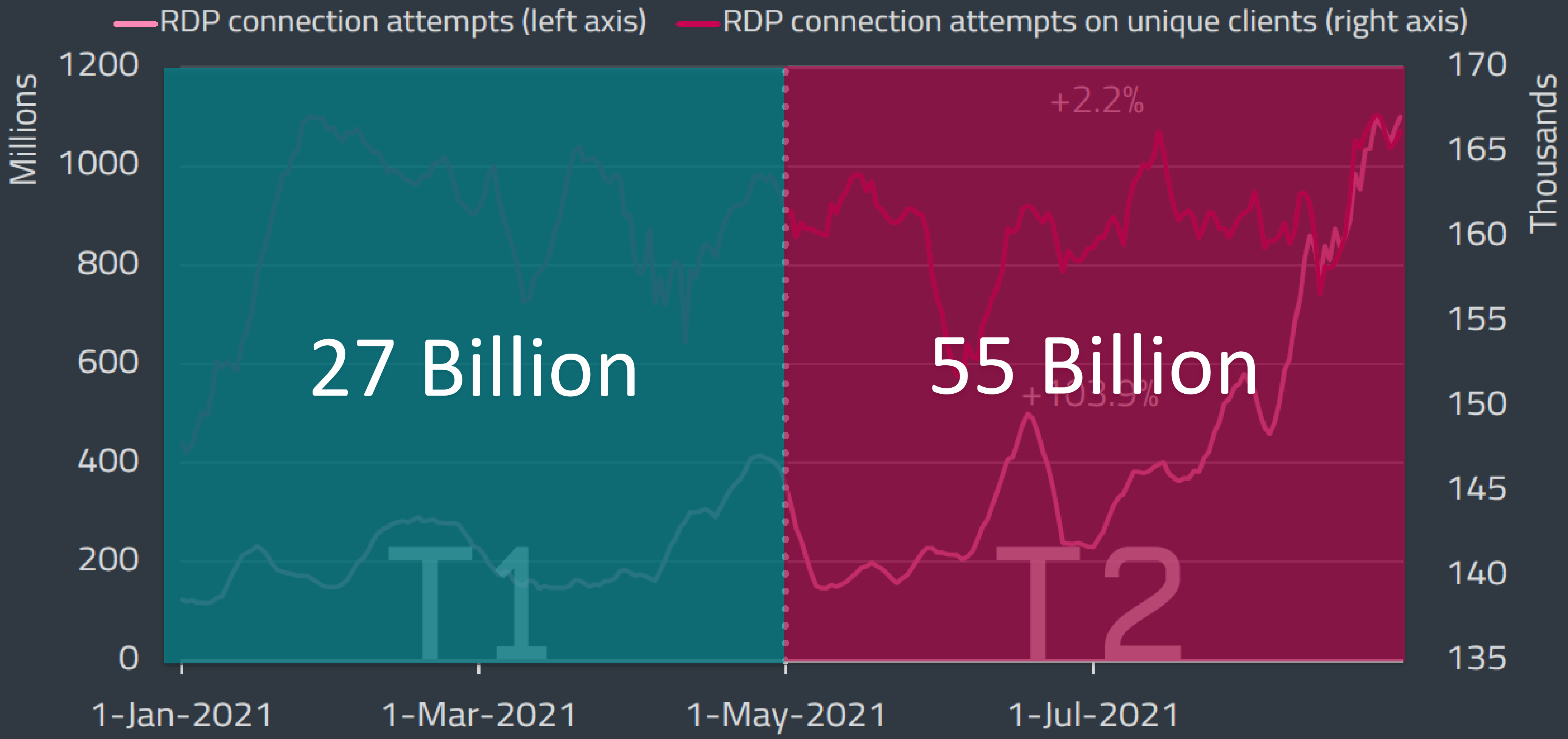
10 Dec 2020 - 11:30AM

Defending against supply-chain attacks

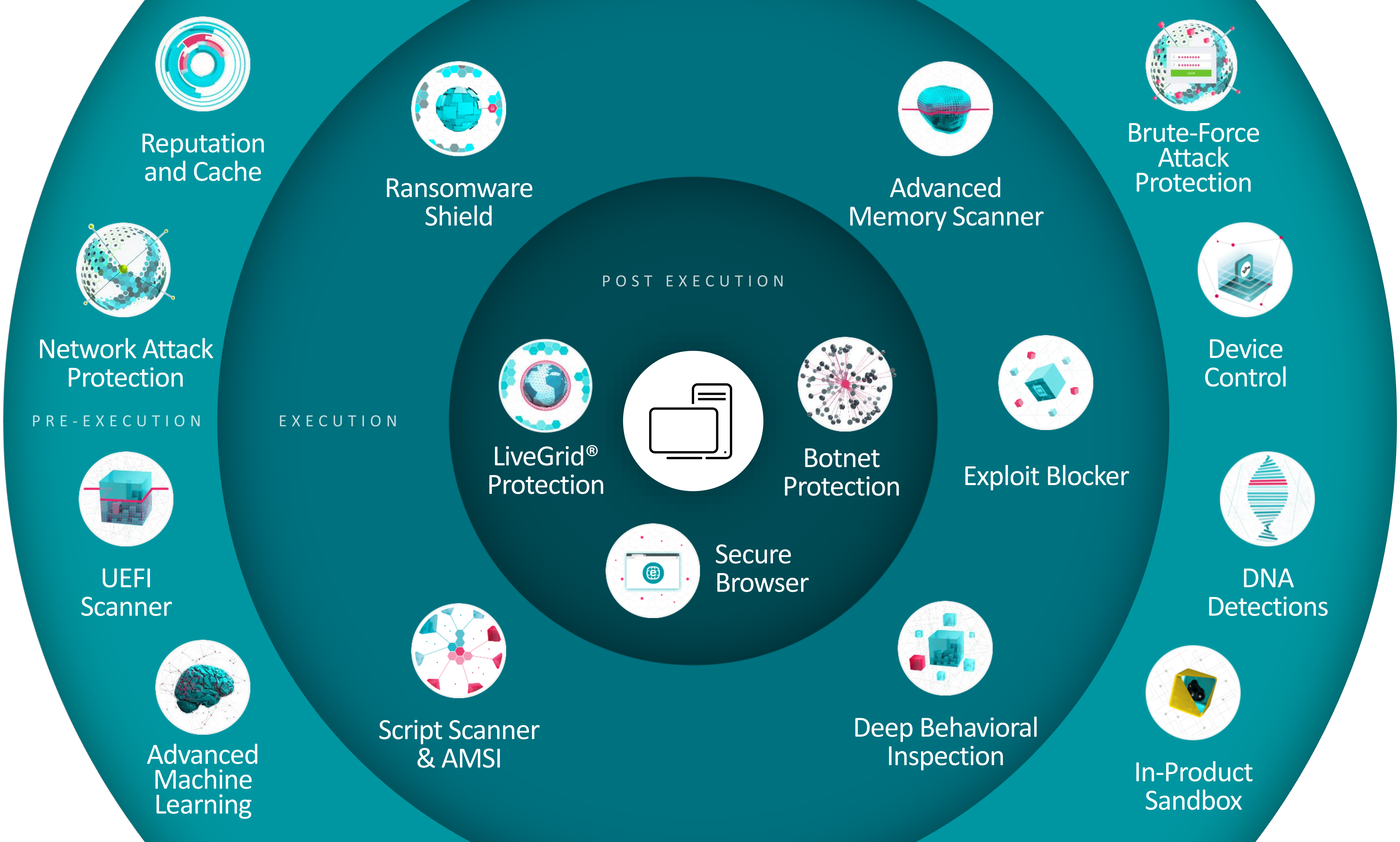
- Know your software!
- Watch out for known vulns, apply patches ASAP
- Stay alert for breaches of software vendors
- Drop redundant / outdated systems, services, protocols

- Do regular code audits & penetration tests
- Harden access controls, use 2FA
- Use a multi-layered security solution

Number of RDP attack attempts accelerates again



Trends of RDP connection attempts and unique clients in T1 2021 – T2 2021, seven-day moving average



PRE-EXECUTION

Reputation and Cache

Network Attack Protection

UEFI Scanner

Advanced Machine Learning

Brute-Force Attack Protection

Device Control

DNA Detections

In-Product Sandbox

EXECUTION

Ransomware Shield

Advanced Memory Scanner

Exploit Blocker

Script Scanner & AMSI

Deep Behavioral Inspection

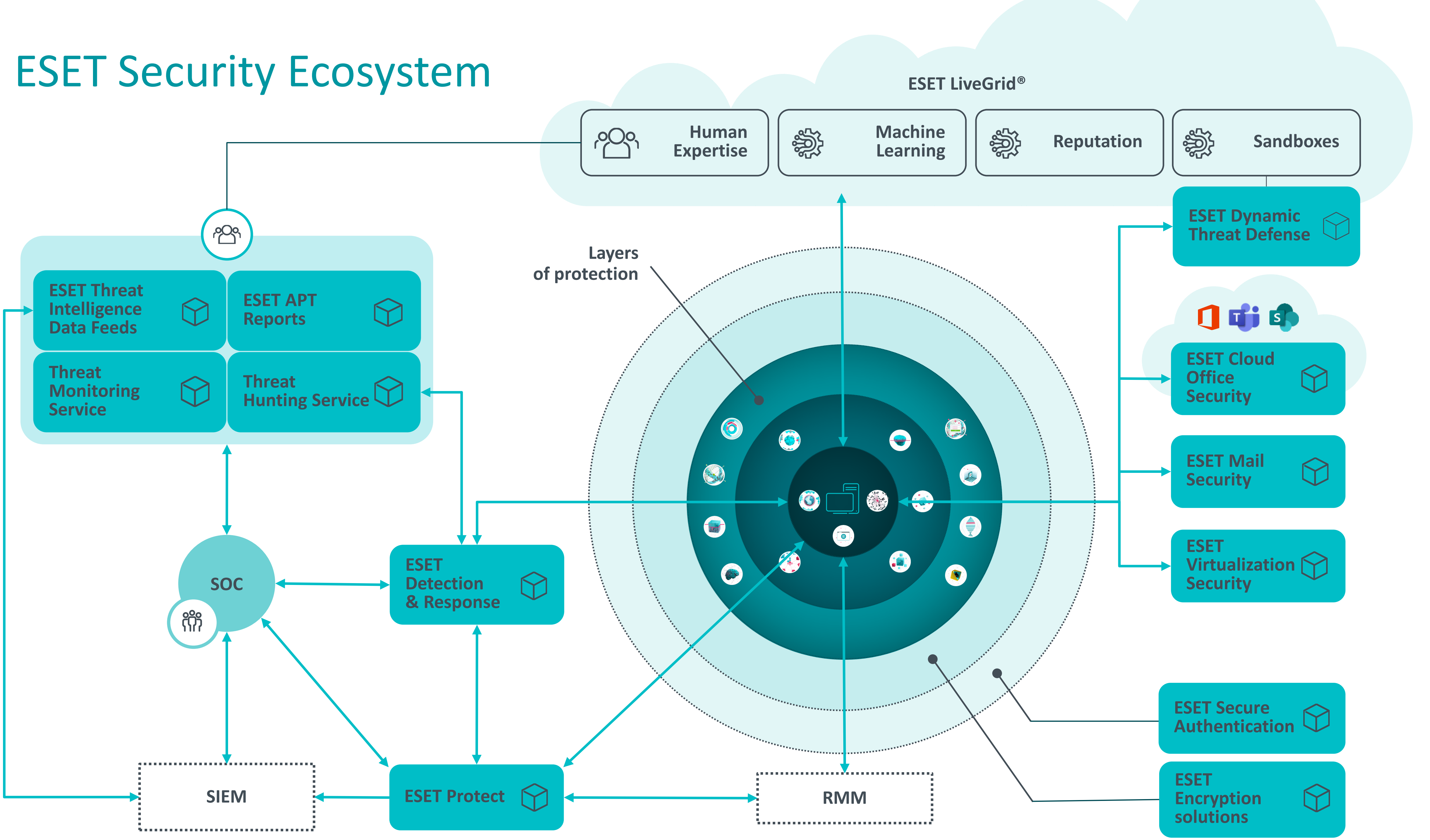
POST EXECUTION

LiveGrid® Protection

Botnet Protection

Secure Browser

ESET Security Ecosystem


ESET LiveGrid®
Human Expertise
Machine Learning
Reputation
Sandboxes
ESET Dynamic Threat Defense
ESET Cloud Office Security
ESET Mail Security
ESET Virtualization Security
ESET Secure Authentication
ESET Encryption solutions
Layers of protection
ESET Threat Intelligence Data Feeds
ESET APT Reports
Threat Monitoring Service
Threat Hunting Service
SOC
ESET Detection & Response
ESET Protect
SIEM
RMM

Thank you!

@Rockouter

@Robert_Lipovsky

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™