APT ÚTOKY V EURÓPE

Robert Lipovský

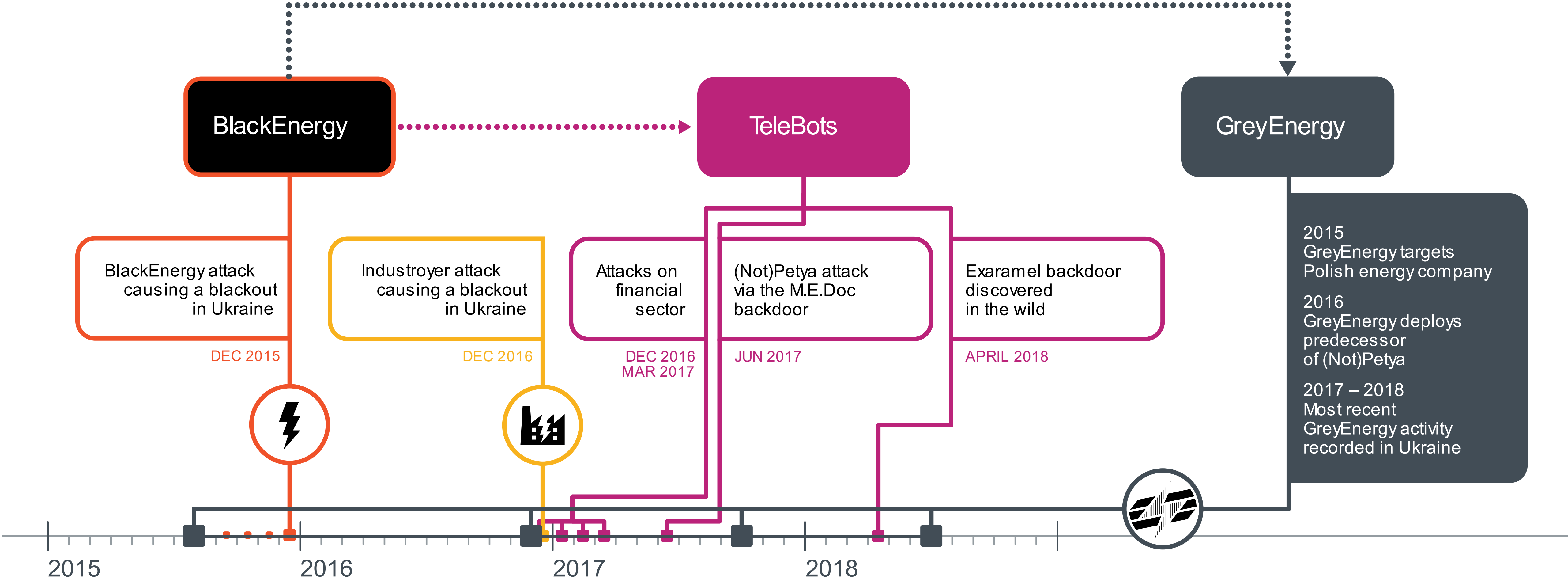
Senior Malware Researcher

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

APT??

Advanced Persistent Threat

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

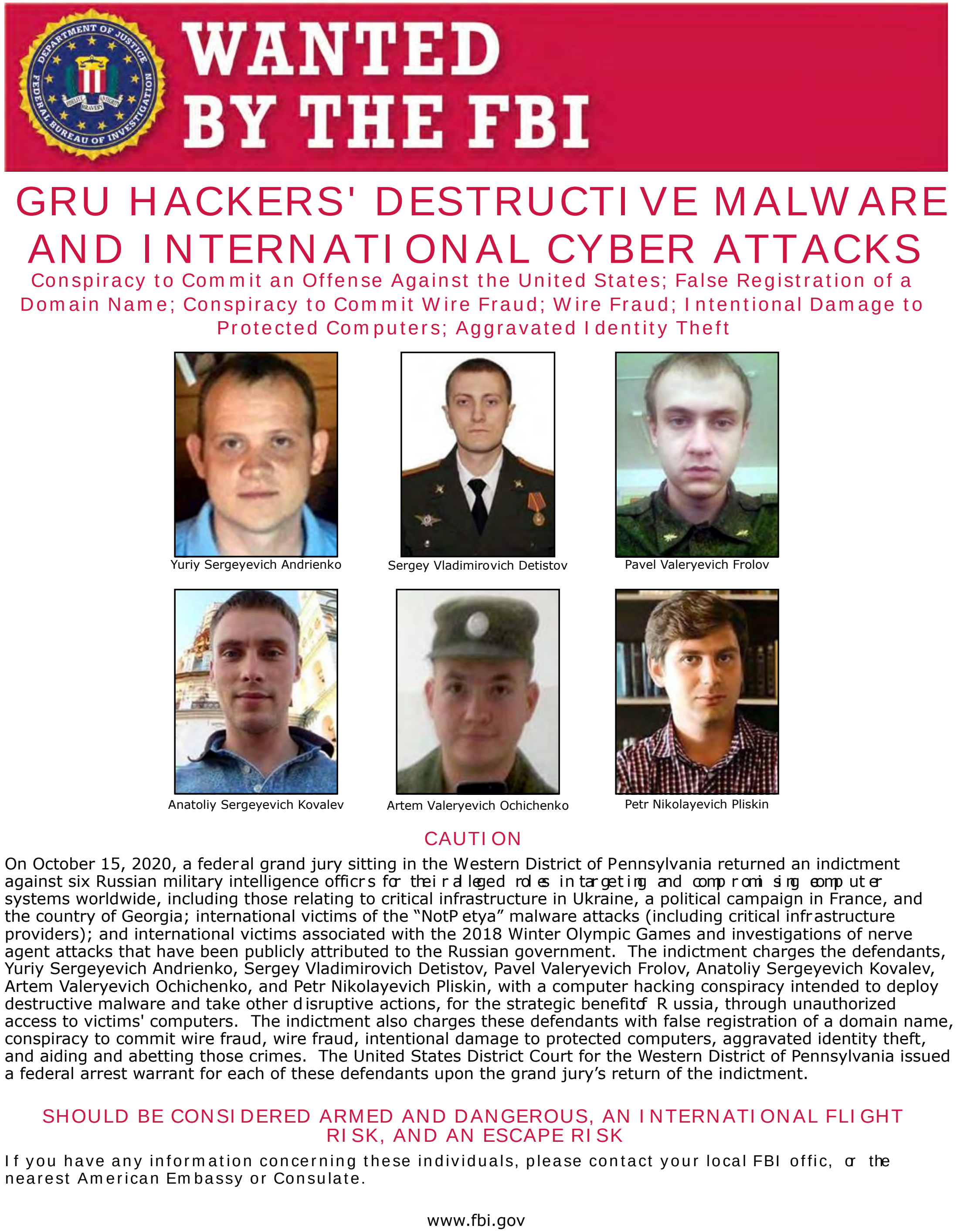
Exaramel backdoor discovered in the wild

APRIL 2018

2015
GreyEnergy targets Polish energy company

2016
GreyEnergy deploys predecessor of (Not)Petya

2017 – 2018
Most recent GreyEnergy activity recorded in Ukraine



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

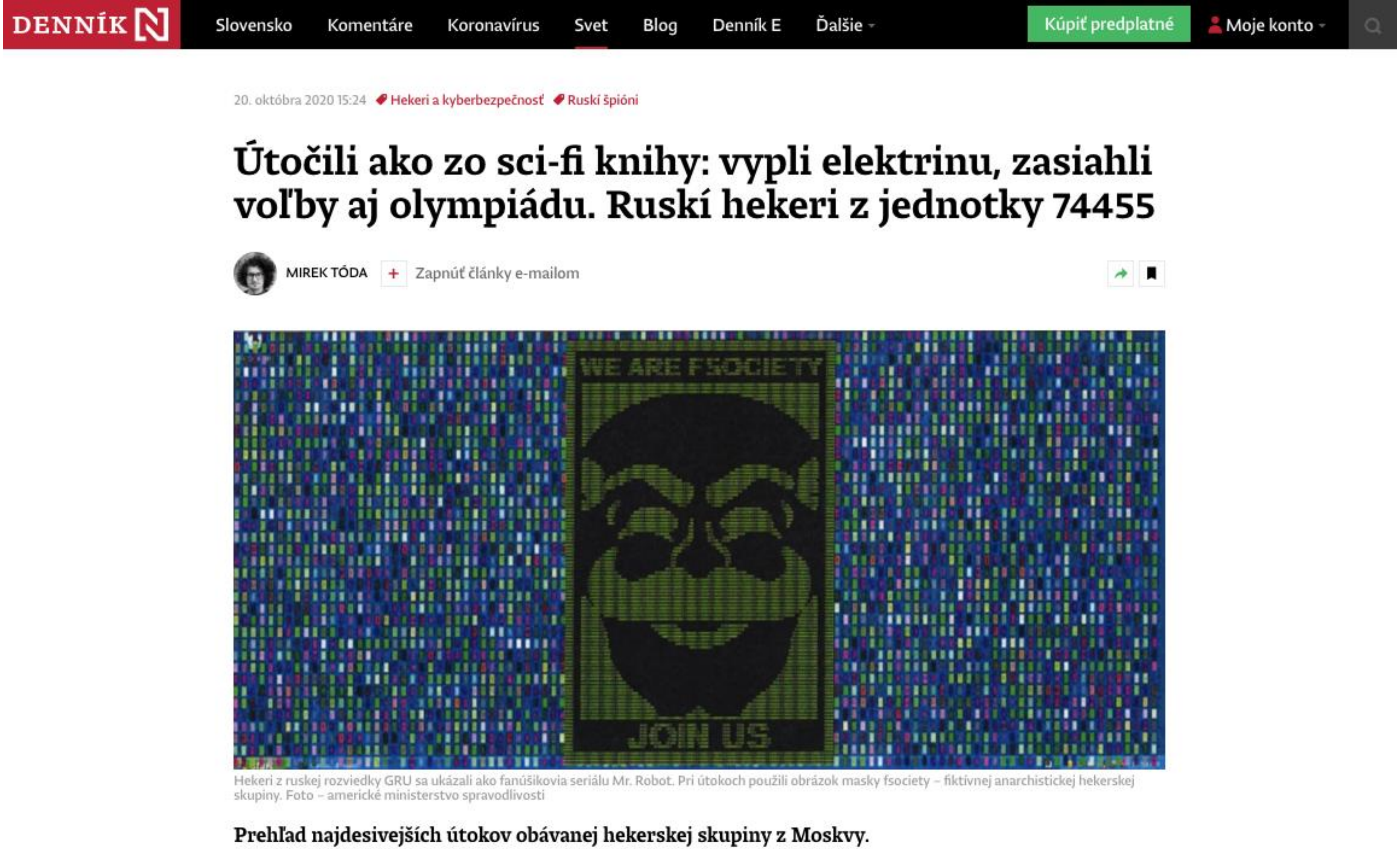
CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers 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 benefit of 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 office, or the nearest American Embassy or Consulate.

www.fbi.gov



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.

SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS

DESCRIPTION AND REMEDIATION

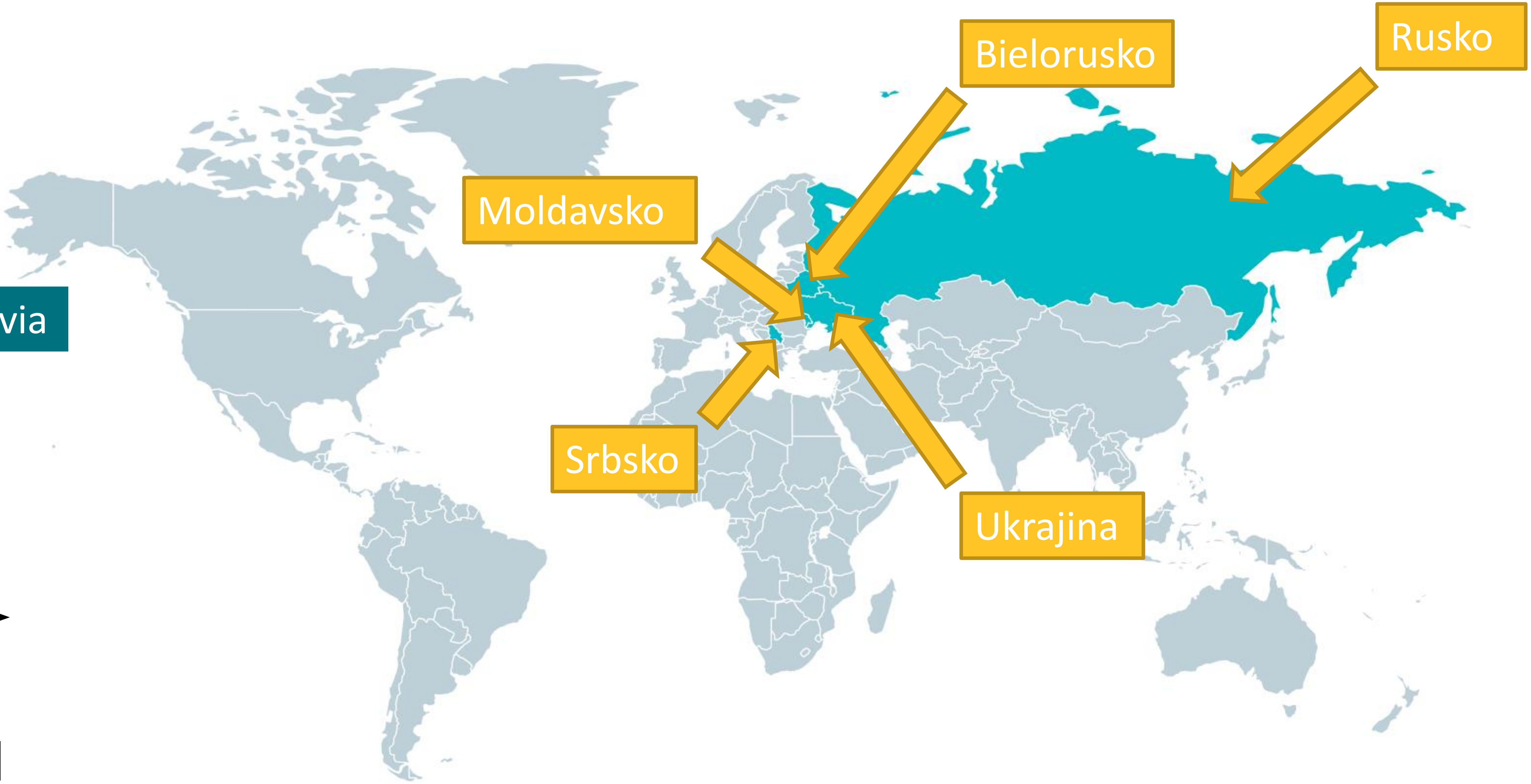
1.0

27/01/2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

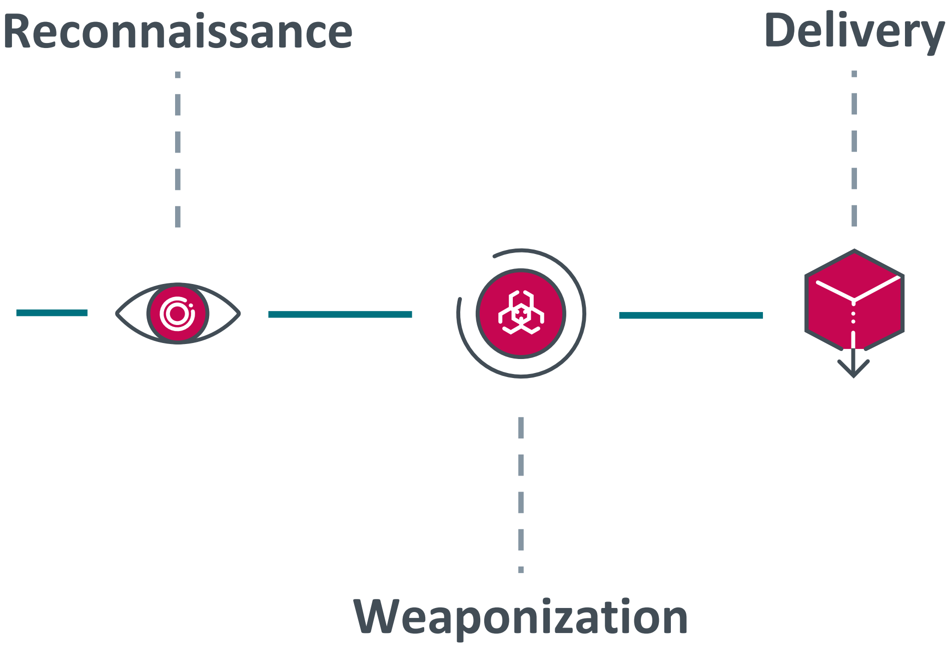
TLP:WHITE

XDSpy



Odvetvia

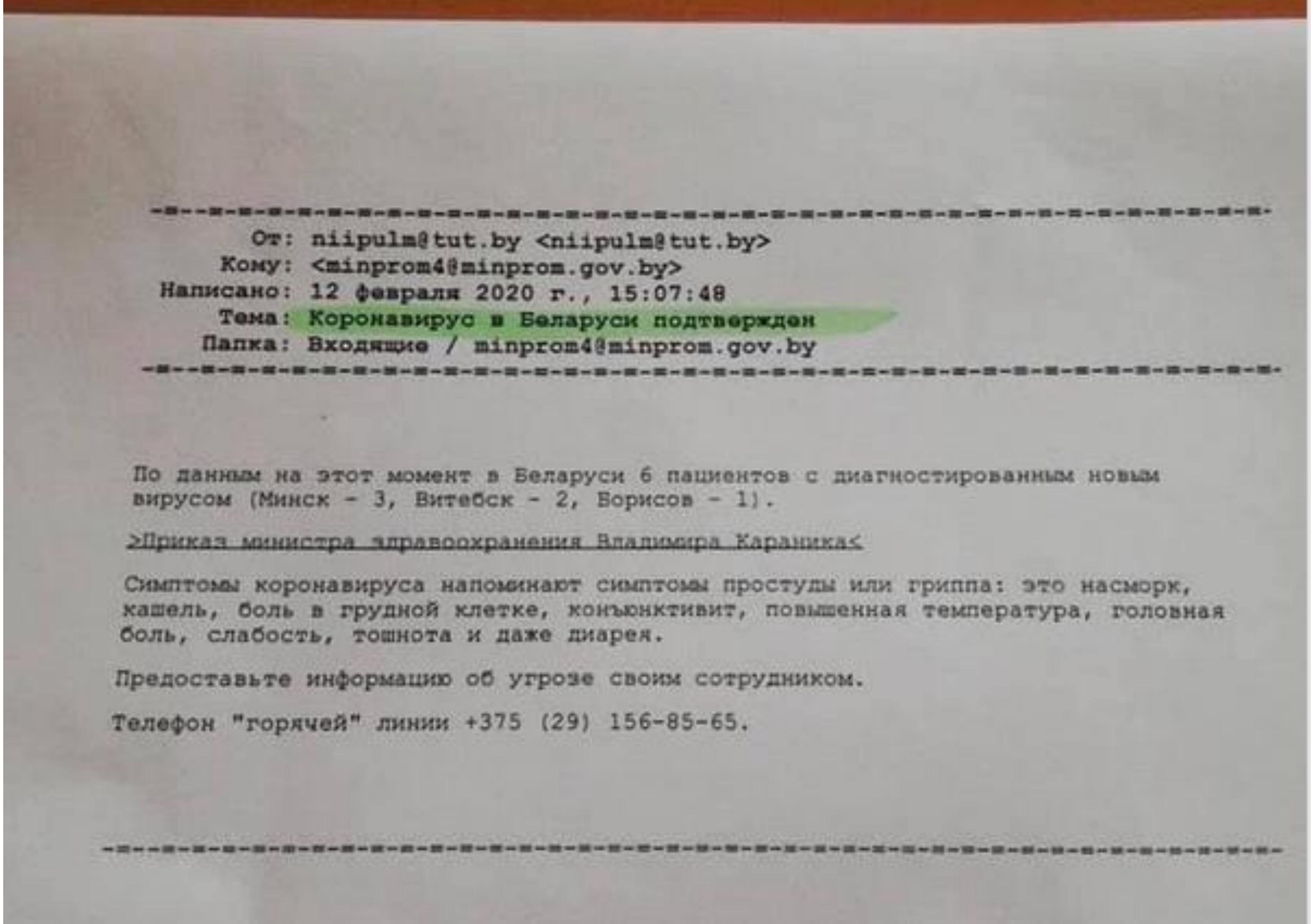
Cyber Kill Chain



Reconnaissance

Weaponization

Delivery



От: niipulm@tut.by <niipulm@tut.by>
Кому: <minprom4@minprom.gov.by>
Написано: 12 февраля 2020 г., 15:07:48
Тема: Коронавирус в Беларуси подтвержден
Папка: Входящие / minprom4@minprom.gov.by

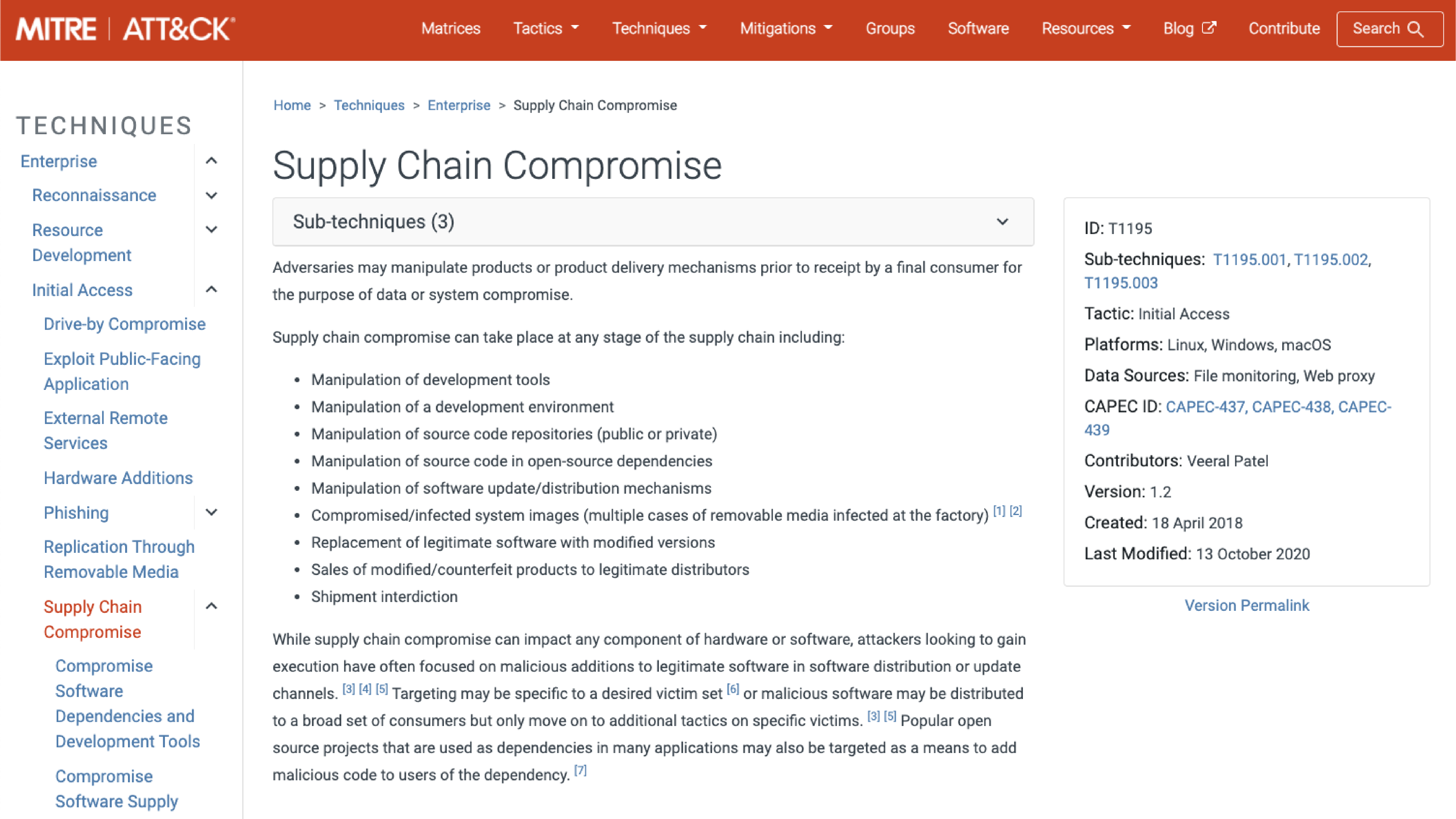
По данным на этот момент в Беларуси 6 пациентов с диагностированным новым вирусом (Минск - 3, Витебск - 2, Борисов - 1).

>Приказ министра здравоохранения Владимира Караника<

Симптомы коронавируса напоминают симптомы простуды или гриппа: это насморк, кашель, боль в грудной клетке, конъюнктивит, повышенная температура, головная боль, слабость, тошнота и даже диарея.

Предоставьте информацию об угрозе своим сотрудником.

Телефон "горячей" линии +375 (29) 156-85-65.



Home > Techniques > Enterprise > Supply Chain Compromise

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

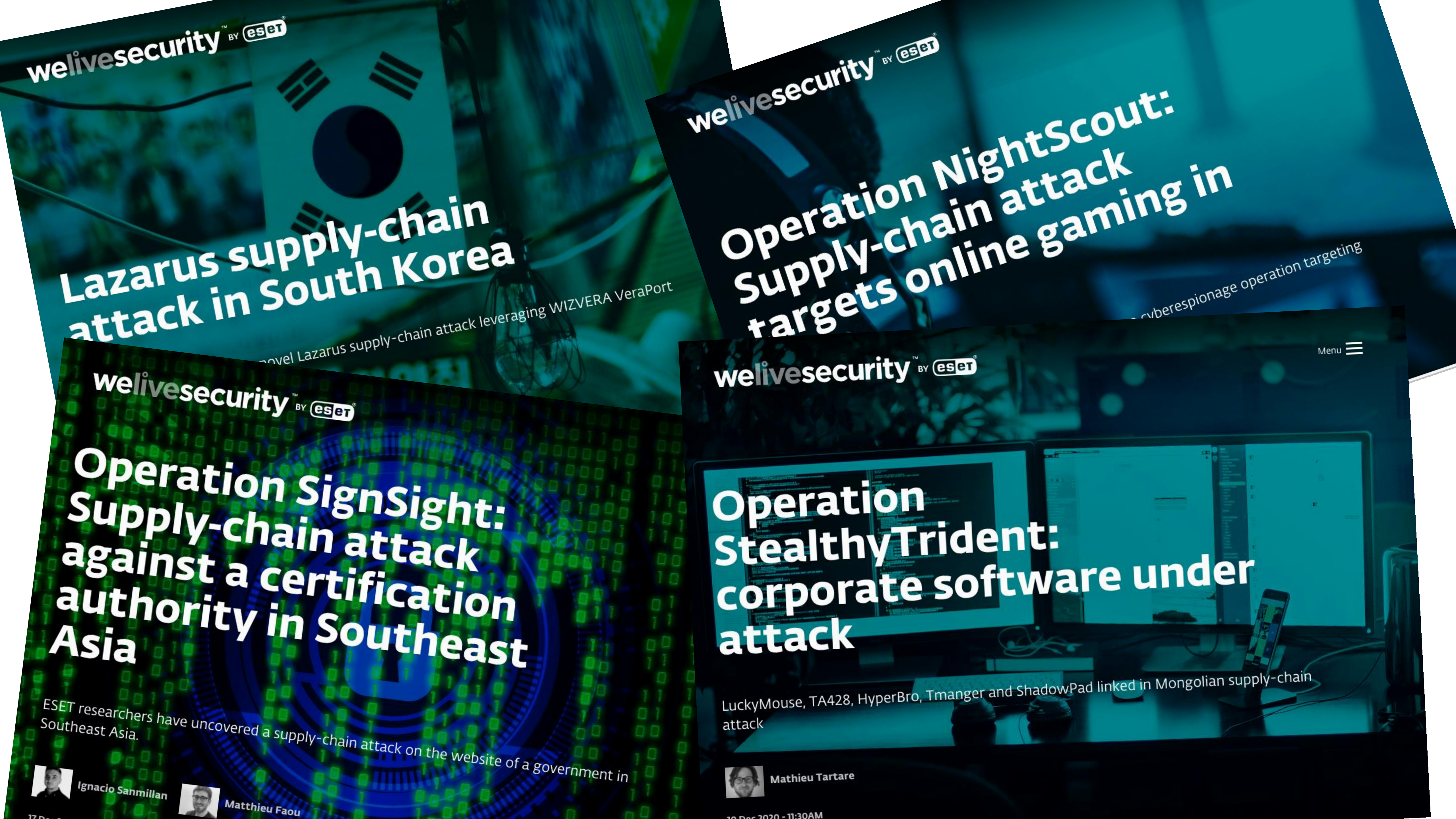
Contributors: Veeral Patel

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

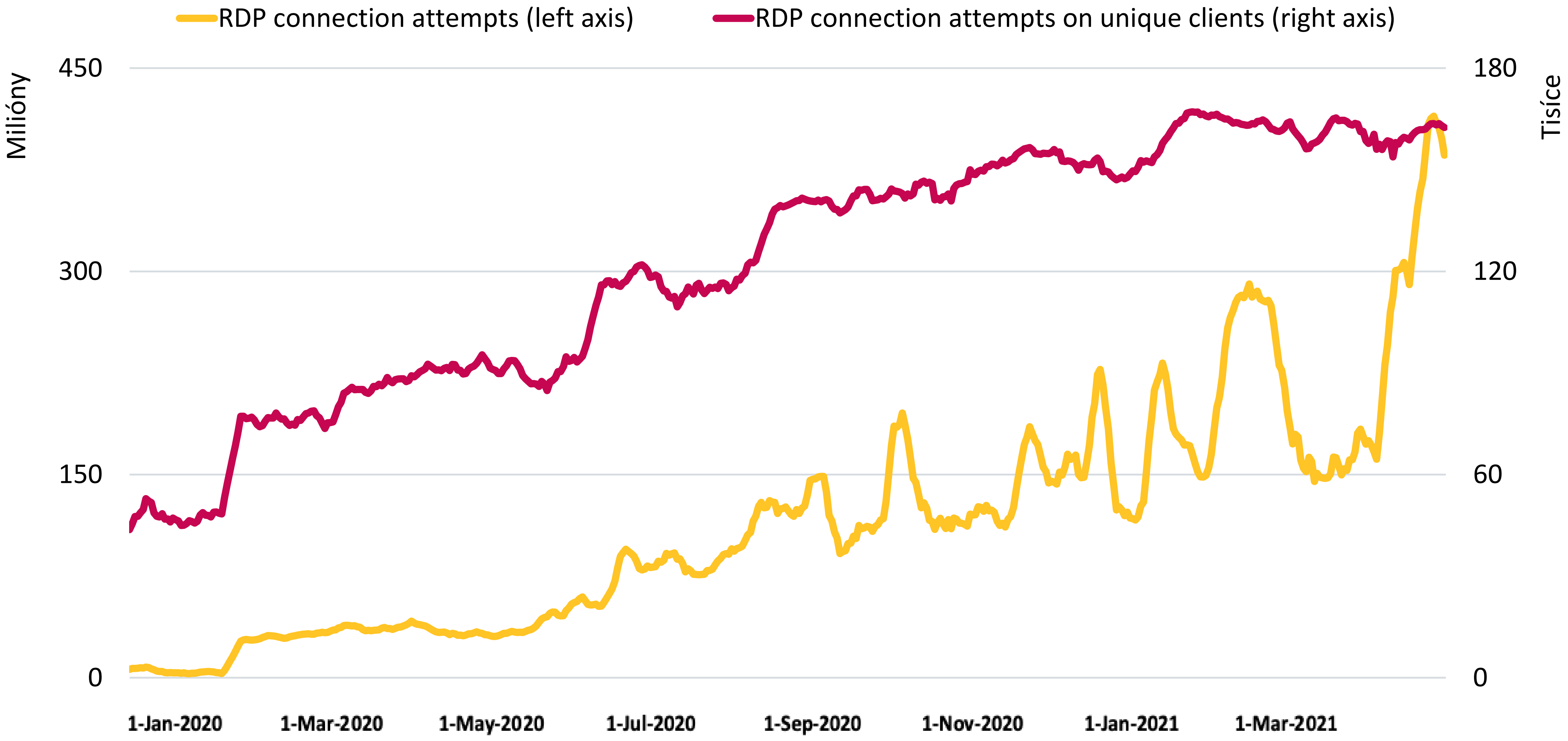
Operation StealthyTrident: corporate software under attack

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

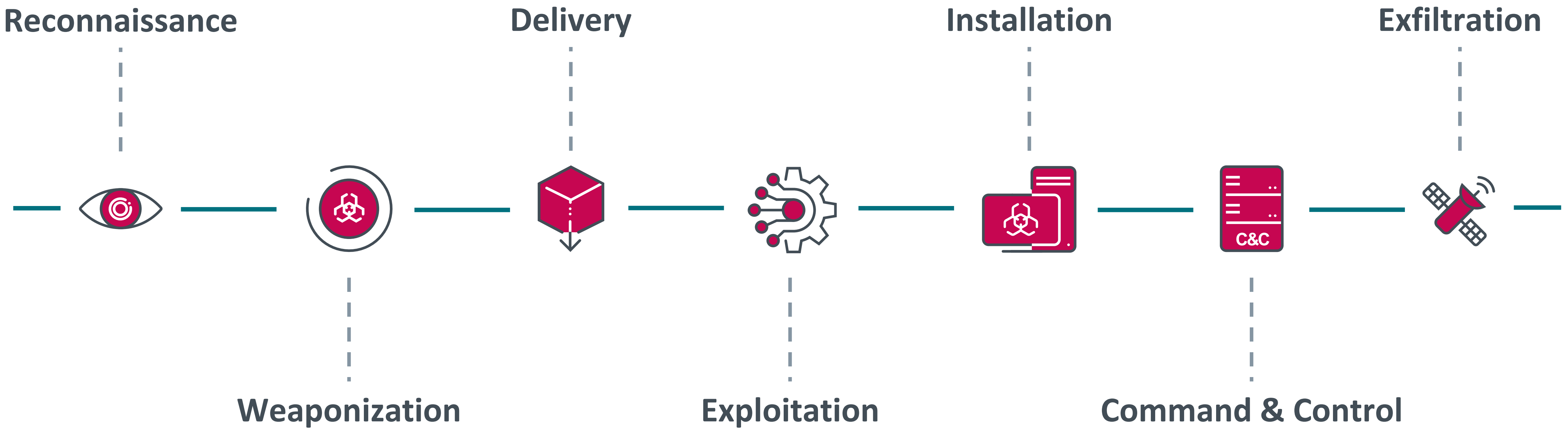
Mathieu Tartare

10 Dec 2020 - 11:30AM

Rast RDP brute-force pokusov od začiatku pandémie



Cyber Kill Chain



Reconnaissance

Weaponization

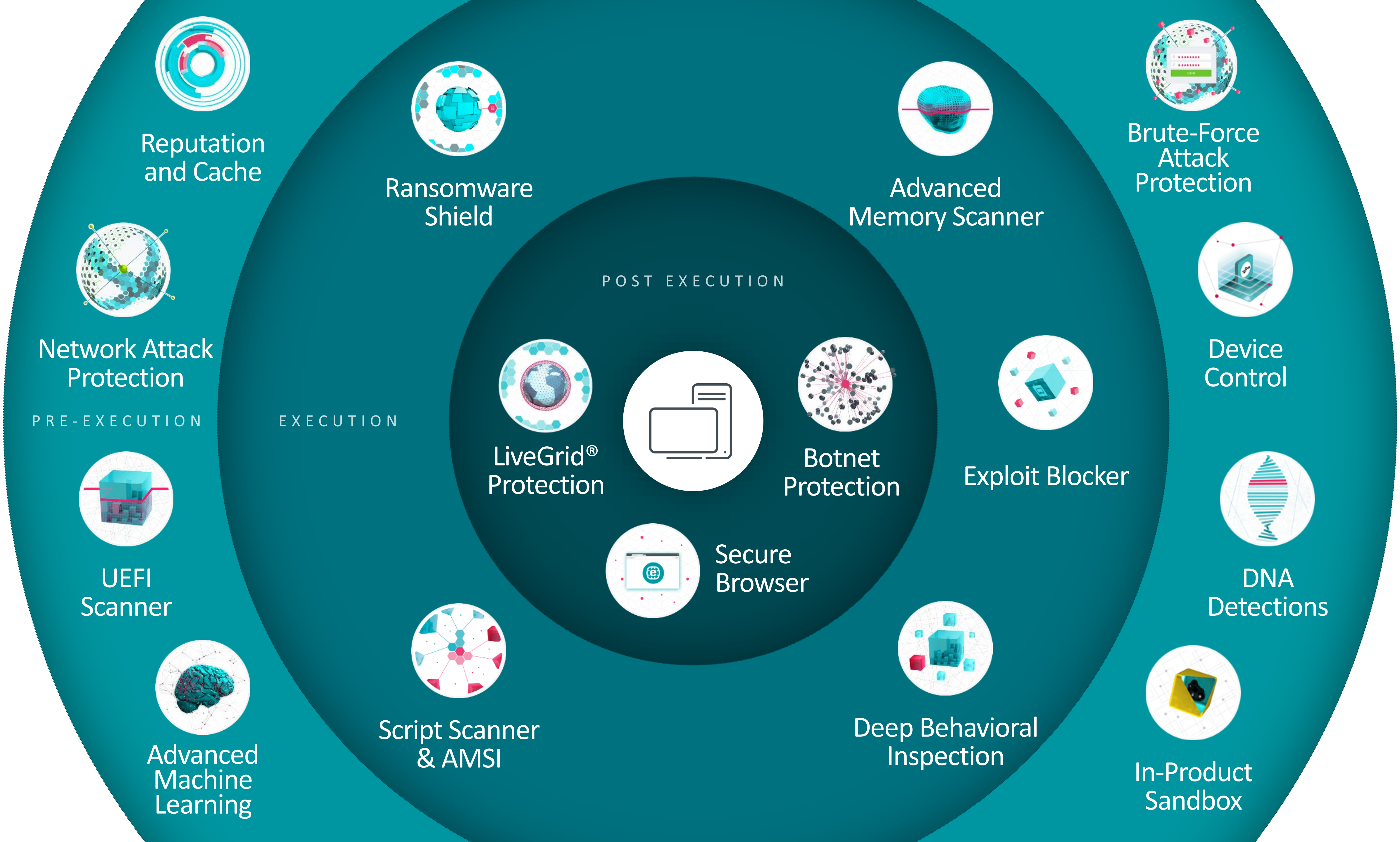
Delivery

Exploitation

Installation

Command & Control

Exfiltration



POST EXECUTION

LiveGrid® Protection

Botnet Protection

Secure Browser

EXECUTION

Ransomware Shield

Advanced Memory Scanner

Exploit Blocker

Deep Behavioral Inspection

Script Scanner & AMSI

PRE-EXECUTION

Reputation and Cache

Network Attack Protection

UEFI Scanner

Advanced Machine Learning

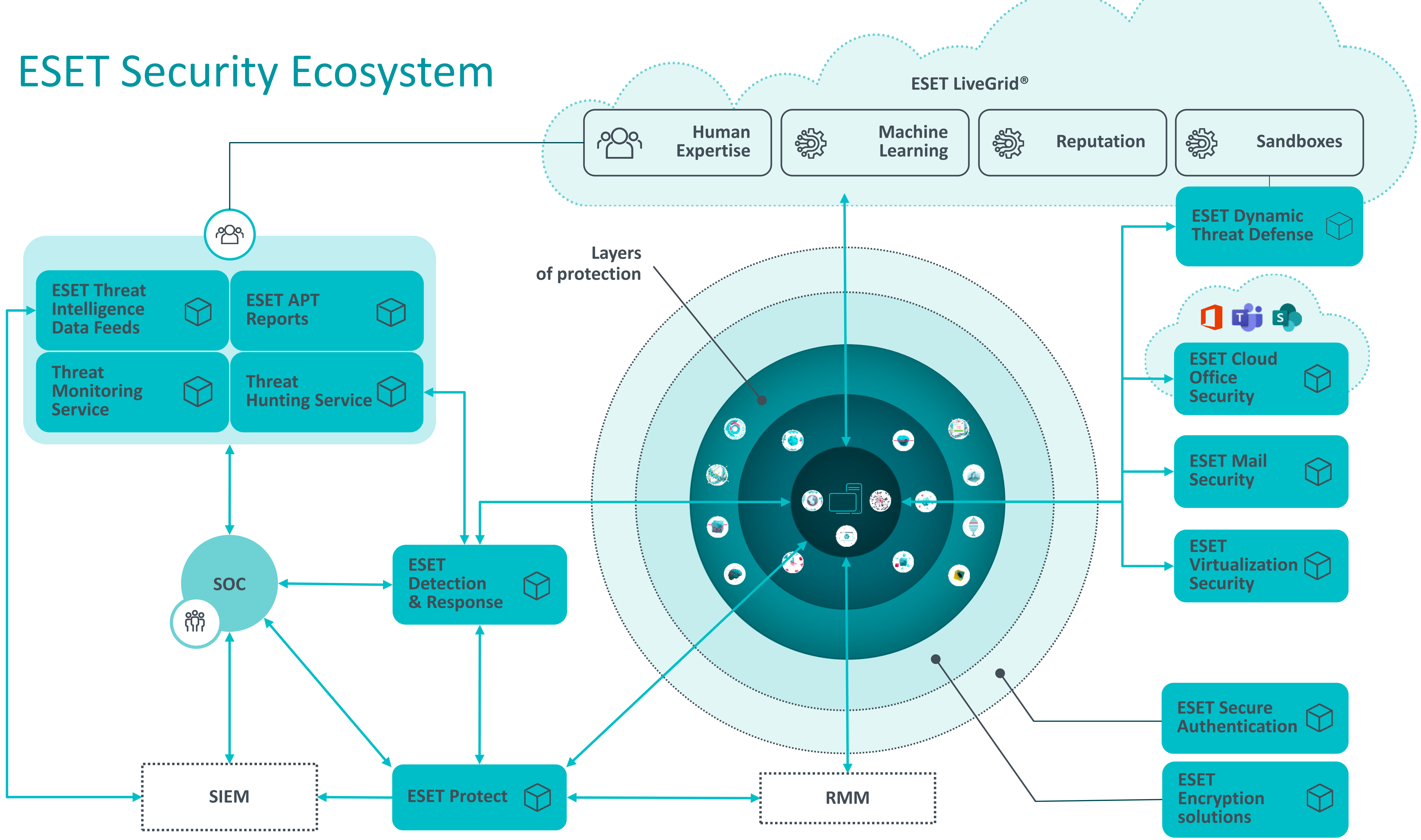
Brute-Force Attack Protection

Device Control

DNA Detections

In-Product Sandbox

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

Ďakujem!

@Rockouter

@Robert_Lipovsky

ESET® UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™