
# APT ÚTOKY V EURÓPE

Robert Lipovský

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

# APT??

# Advanced Persistent Threat

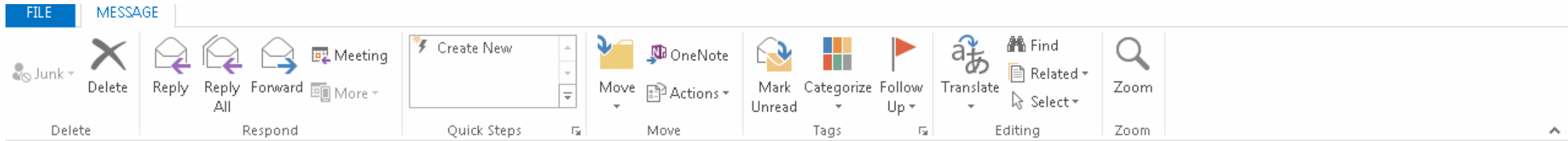
SECURITY DAYS

# XDSpy – kradnutie vládnych tajomstiev od 2011

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

# XDSpy ciele


Spearphishing email
The user clicks on the attachment or the malicious link
Malicious .lnk file
Downloads from the C&C server




Tue 8/25/2015 1:28 AM

ГУВД г. МОСКВЫ <guvdmo.moskva@mail.ru>

**Сотрудники склада находок ГУВД обнаружили ваш емайл адрес**

To [redacted]@minsvyaz.ru

Message | сканы.zip (752 KB)

Доводим до вашего сведения, что в стол находок при ГУВД поступила папка-скоросшиватель с документами и фотографиями. Внутри папки был тоже бумажник в котором сотрудники склада находок обнаружили ваш емайл адрес. С целию опознания в приложении отправляем сканы некоторых найенных фотографии. В случае если узнаёте потерянные вещи рекомендуется поступить следующим образом: нужно связаться с ГУВД, подать заявление (в заявлении нужно самым подробным образом описать потерянные вещи — особое внимание нужно уделить особым приметам: форме, размерам, весу, цвету), в акте указать свои контактны.

По инструкции все забытые вещи хранятся в течение трех месяцев со дня поступления в стол находок при ГУВД, затем передаются в Госсфонд. За каждые сутки хранения потеряного документа (или вещи) в камере забытых вещей с его владельца взыскивается 10 рублей.

Татьяна Соломатина
Сотрудник склада находок

**ГУВД г. МОСКВЫ**
бюро находок документов
ул. Маяковского, 31
+7(495) 200-9957
www.guvdmo.ru

СИСТЕМА СЕРТИФИКАЦИИ В ОБЛАСТИ ПОЖАРНОЙ БЕЗОПАСНОСТИ

# СЕРТИФИКАТ ПОЖАРНОЙ БЕЗОПАСНОСТИ

**ССПБ. RU. ОП034. Н. 00323**

№ _____

Зарегистрирован в Государственном реестре Системы сертификации в области пожарной безопасности РФ **02.06.2009 г.** Действителен до **02.06.2012 г.**

Настоящий сертификат удостоверяет, что идентифицированный надлежащим образом образец

**Состав теплоизоляционный «RE-THERM»**
**ТУ 2316-112-00209600-2009**

**23 1630**
*код К-ОКП*

наименование продукции

**---- -- ---**
*код ТН ВЭД*

соответствует требованиям пожарной безопасности, установленным в **НПБ 244-97: группа горючести – Г1 (слабогорючие по СНиП 21-01-97*) при испытаниях на негорючем основании по ГОСТ 30244-94, группа воспламеняемости – В1 по ГОСТ 30402-96 (трудновоспламеняемые по СНиП 21-01-97*), коэффициент дымообразования – Д1 (с малой дымообразующей способностью) по ГОСТ 12.1.044-89 (п.4.18), показатель токсичности Т1 (малоопасные) по ГОСТ 12.1.044-89 (п.4.20)**

*обозначение НД*

при добровольной сертификации

Сертификат распространяется **на серийный выпуск**

*серийное производство: номер, размер и дата выпуска партии, номер и дата контракта поставки, номер единичного изделия*

Сертификат выдан **ЗАО «Ареал»**

*наименование предприятия, организации*

**Адрес: ул. Вахитова, д. 6, г. Казань, 420034**
**Телефон/факс: (843) 227-07-12 ОКПО 54402746**

*юридический адрес, телефон, факс*

Изготовитель **ООО «Инновационные технологии»**

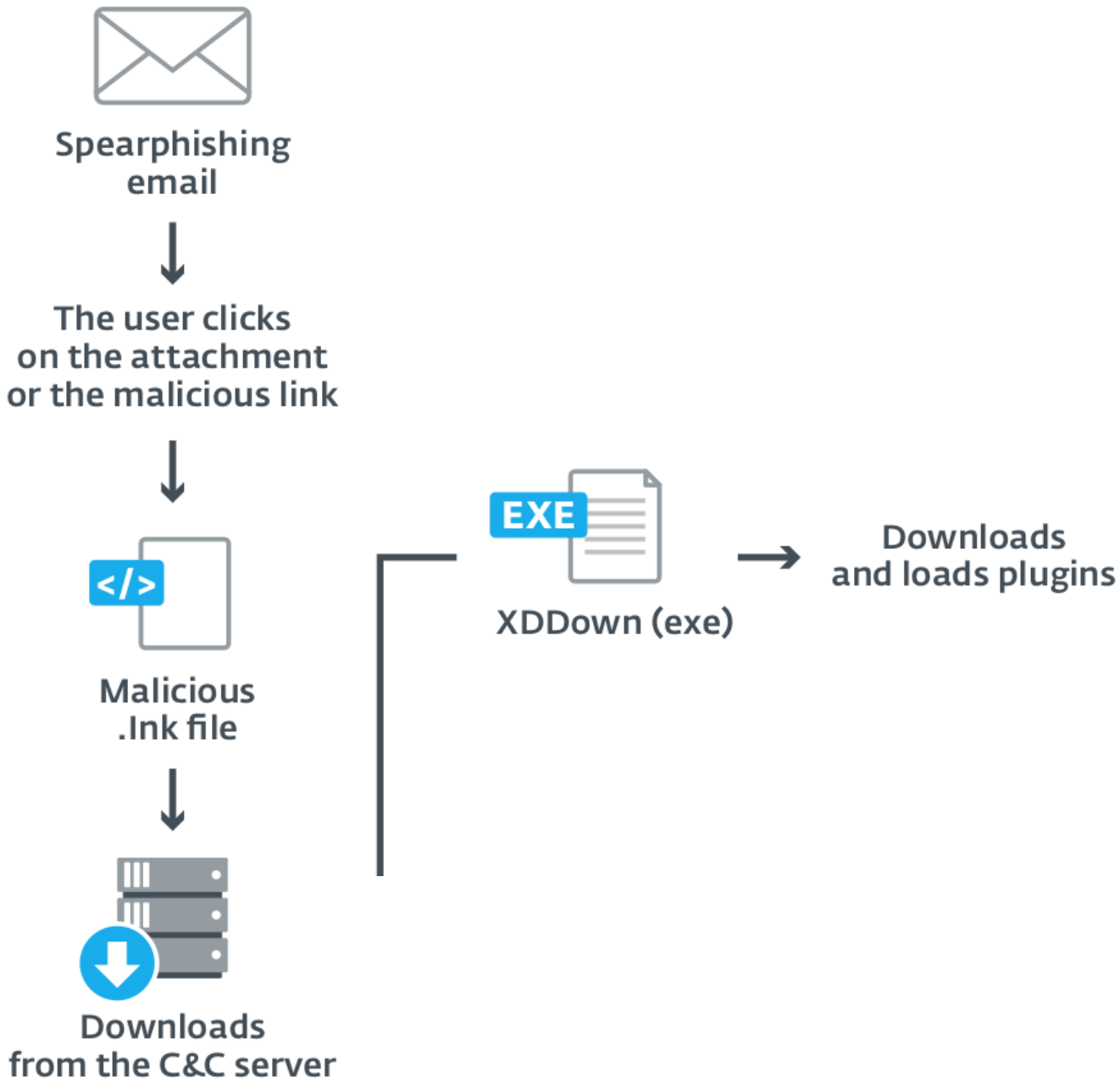
*наименование предприятия, организации*

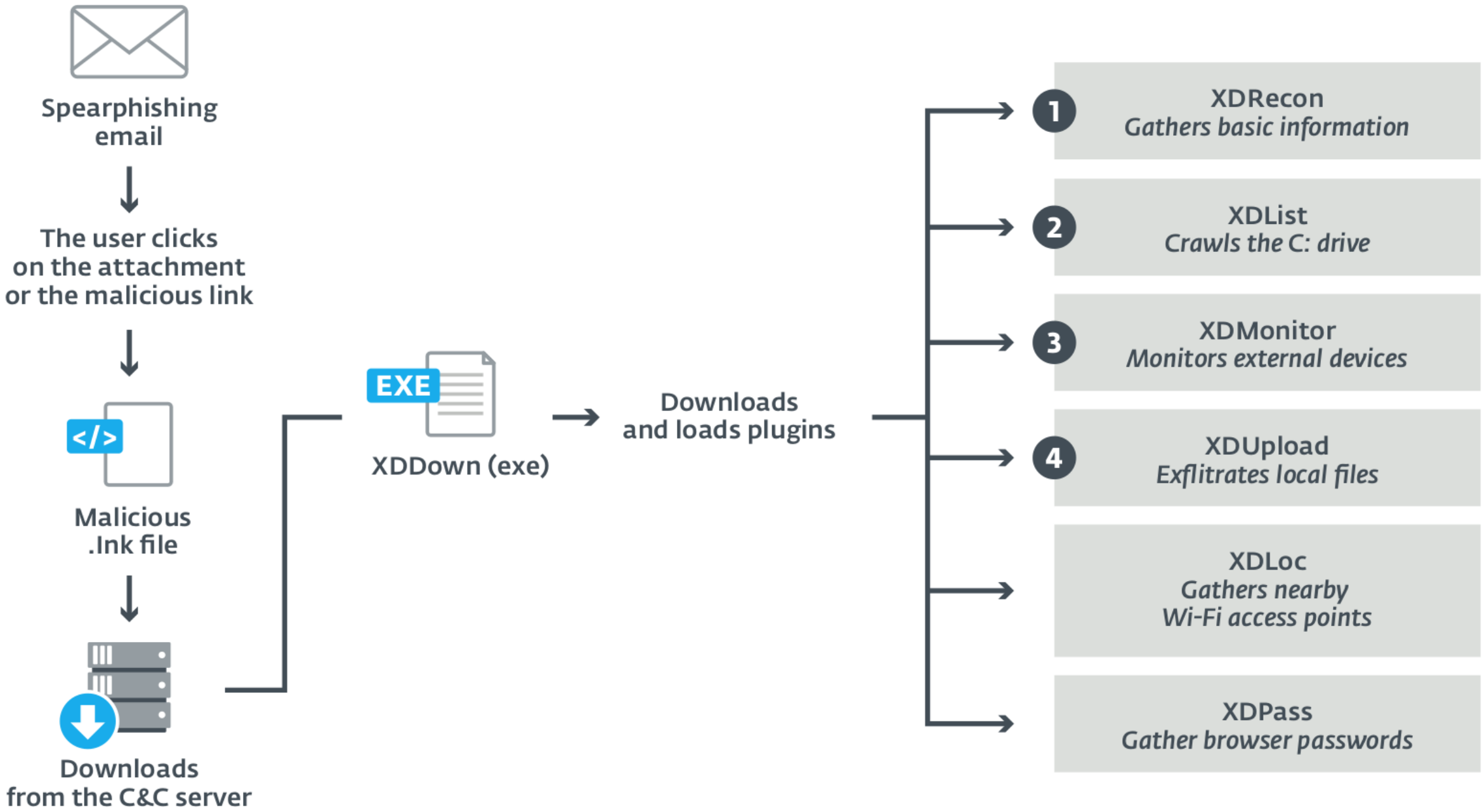
**Адрес: ул. Вахитова, д. 6, г. Казань, 420034**
**Телефон/факс: (843) 227-00-98 ОКПО 00209600**

*юридический адрес, телефон, факс*

М.П.

№ 0228750


Spearphishing email
The user clicks on the attachment or the malicious link
Malicious .lnk file
Downloads from the C&C server
EXE
XDDown (exe)
Downloads and loads plugins

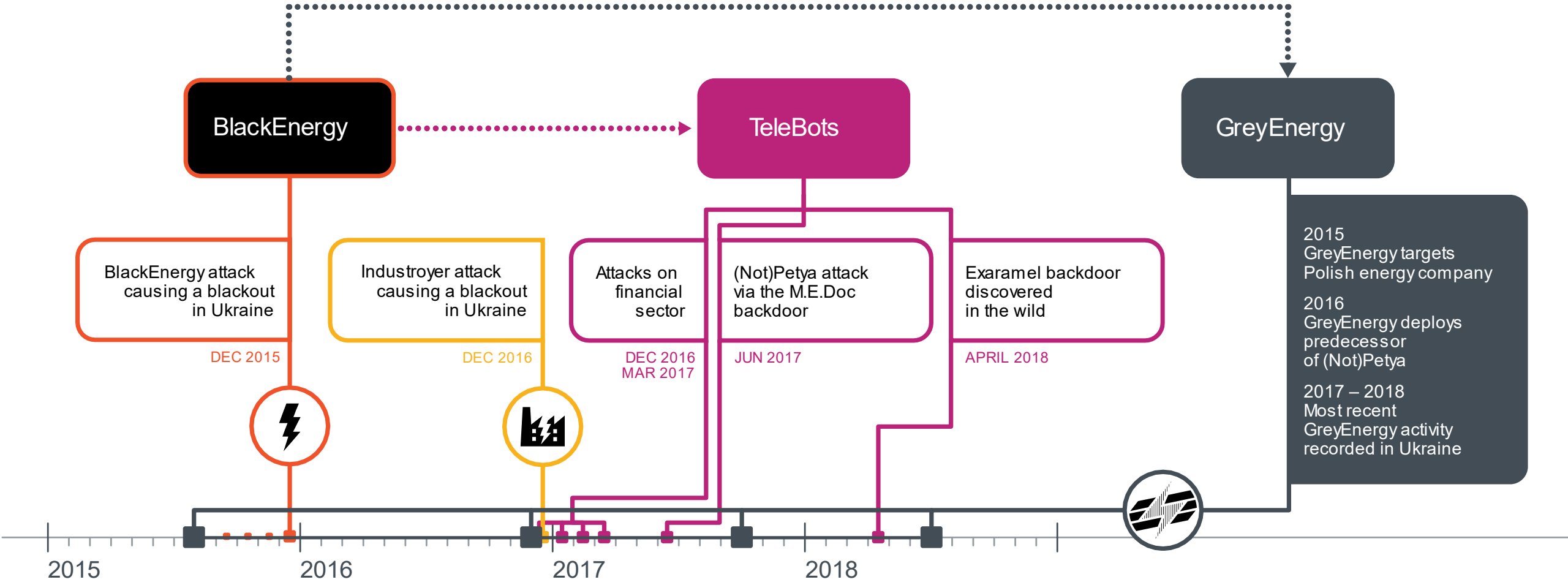

Spearphishing email
The user clicks on the attachment or the malicious link
Malicious .lnk file
Downloads from the C&C server
EXE
XDDown (exe)
Downloads and loads plugins
1
XDRecon
Gathers basic information
2
XDList
Crawls the C: drive
3
XDMonitor
Monitors external devices
4
XDUpload
Exfiltrates local files
XDLoc
Gathers nearby Wi-Fi access points
XDPass
Gather browser passwords

SECURITY DAYS

# Sandworm aktivita vo Francúzsku

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

# 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
2015
2016
2017
2018

# 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.

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

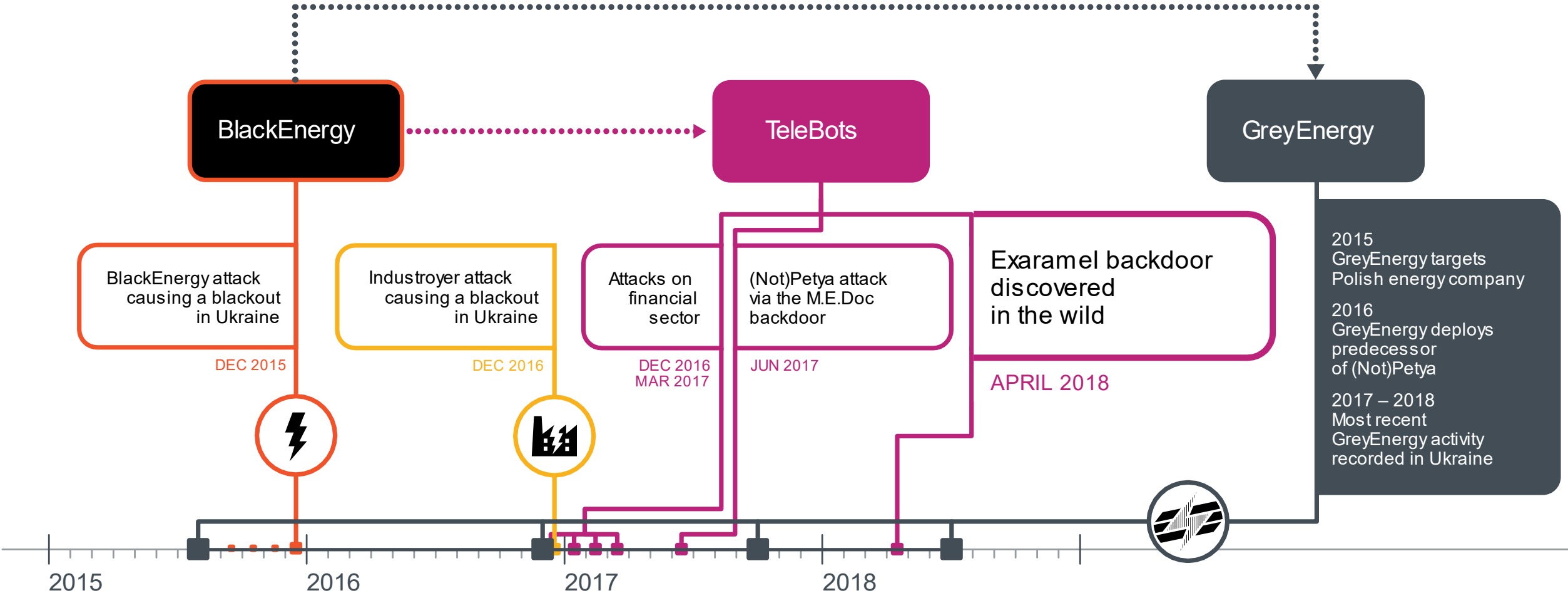
# Útočili ako zo sci-fi knihy: vypli elektrinu, zasiahli voľby aj olympiádu. Ruskí hekeri z jednotky 74455

MIREK TÓDA 


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


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
2015
2016
2017
2018

# SANDWORM INTRUSION SET CAMPAIGN TARGETING CENTREON SYSTEMS

## DESCRIPTION AND REMEDIATION

1.0

27/01/2021


TLP:WHITE

TECHNIQUES
Enterprise
Reconnaissance
Resource Development
Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Compromise Software Dependencies and Development Tools
Compromise Software Supply



# 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

# Telebots supply chain útoky

TECHNIQUES
Enterprise
Reconnaissance
Resource Development
Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Compromise Software Dependencies and Development Tools
Compromise Software Supply



# 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

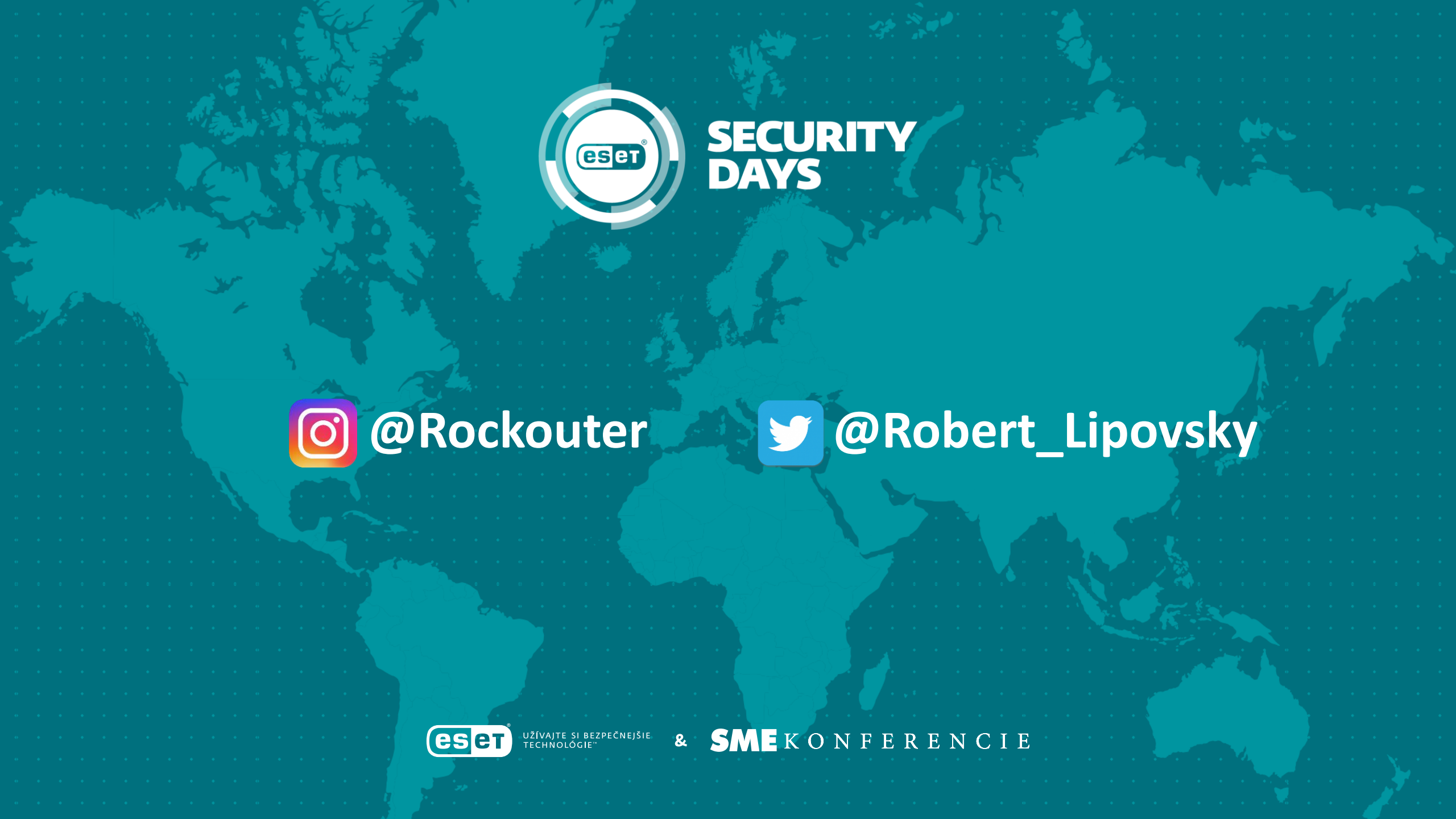
Version: 1.2

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
welivesecurity BY eset
Menu
Operation StealthyTrident: corporate software under attack
LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack
Mathieu Tartare


SECURITY DAYS
@Rockouter
@Robert_Lipovsky
UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE
&
SME KONFERENCIE