RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

SESSION ID: SPO3-R11

Protecting You Better with Advanced Malware Research

Robert Lipovsky
Senior Malware Researcher
ESET

Juraj Janosik
Head of AI/ML team
ESET

Robert Lipovsky
Senior Malware Researcher

Juraj Janosik
Head of AI/ML team


GLOBAL VIEW
update activity
GLOBAL VIEW
11:01
infection ratio
EUROPE VIEW
11:01
infection ratio
ESET VIRUSLAB SCREEN #2

300,000+

unique malware samples daily

Malware researcher

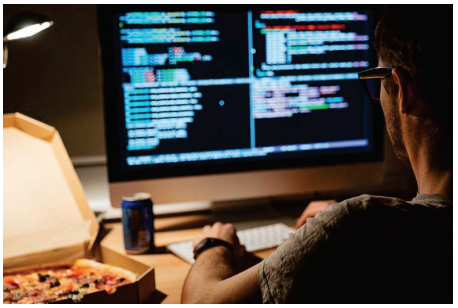
What my friends think I do.

What my mom thinks I do.

What users think I do.

What Finance thinks I do.

What I think I do.



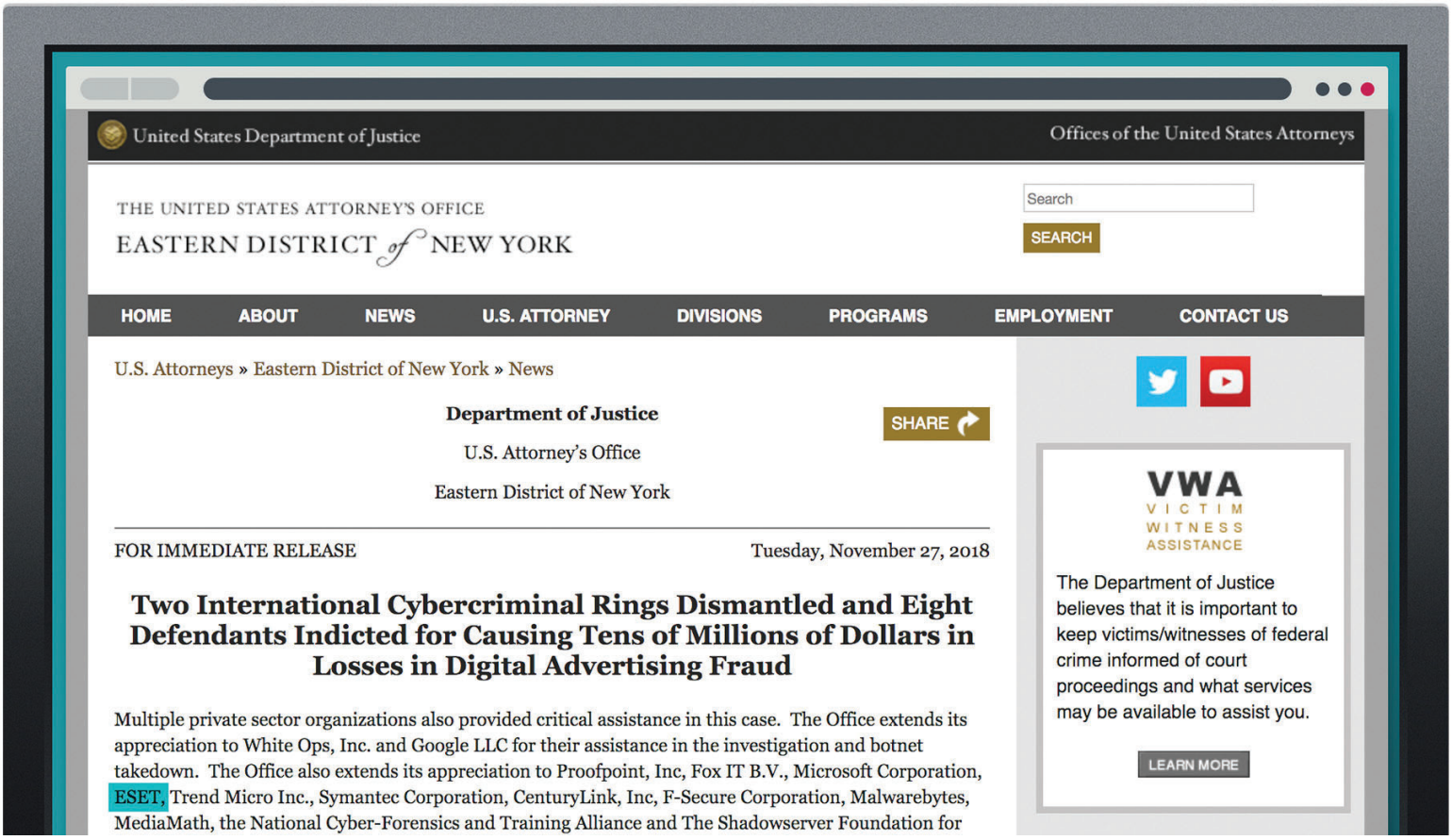
What I really do.

RSAConference2019

Fighting cybercrime

ESET works with cybercrime-fighting units

Microsoft



United States Department of Justice

Offices of the United States Attorneys

THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT of NEW YORK

Search
SEARCH

HOME ABOUT NEWS U.S. ATTORNEY DIVISIONS PROGRAMS EMPLOYMENT CONTACT US

U.S. Attorneys » Eastern District of New York » News

Department of Justice

U.S. Attorney's Office

Eastern District of New York

SHARE

FOR IMMEDIATE RELEASE

Tuesday, November 27, 2018

Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud

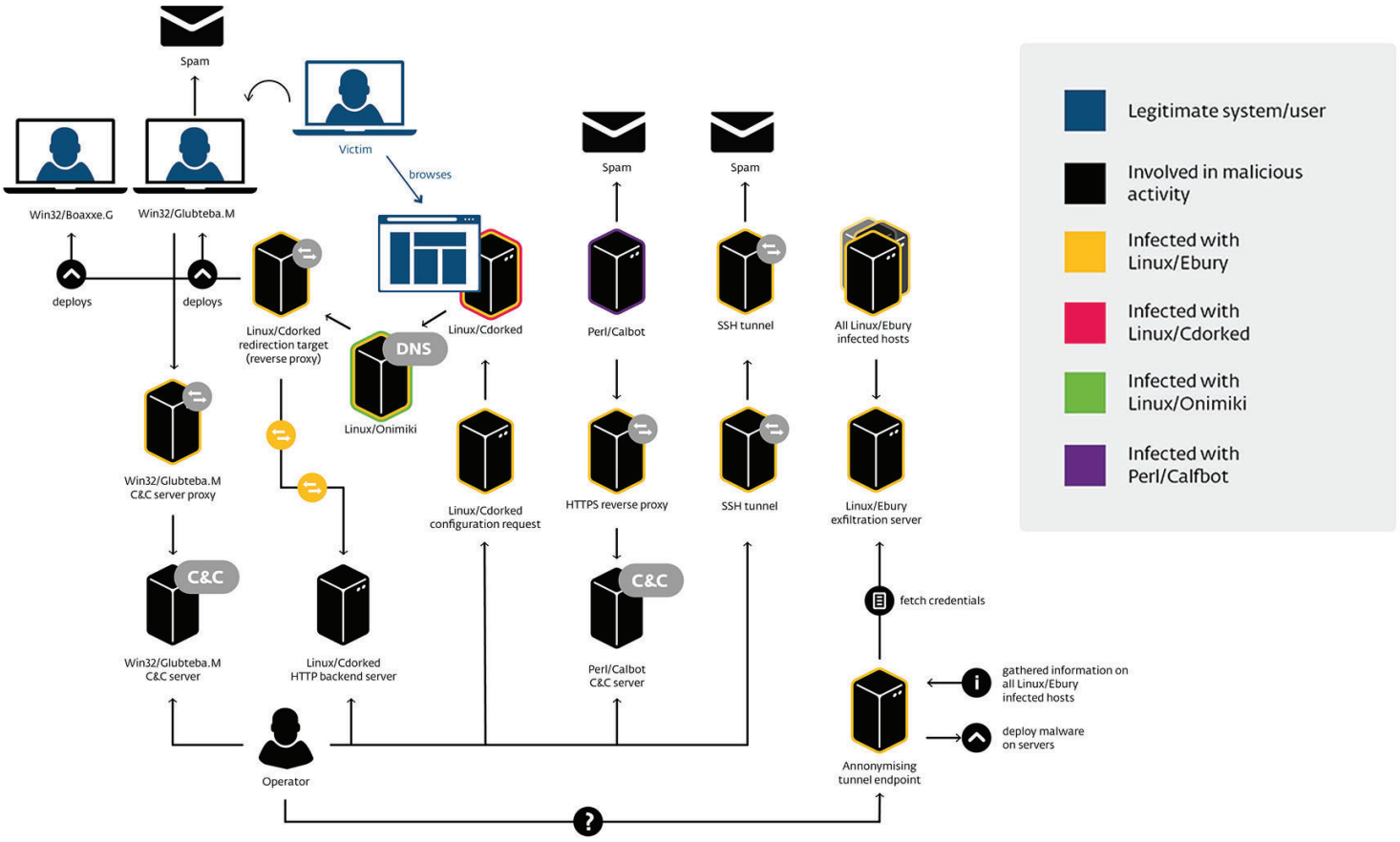
Multiple private sector organizations also provided critical assistance in this case. The Office extends its appreciation to White Ops, Inc. and Google LLC for their assistance in the investigation and botnet takedown. The Office also extends its appreciation to Proofpoint, Inc, Fox IT B.V., Microsoft Corporation, ESET, Trend Micro Inc., Symantec Corporation, CenturyLink, Inc, F-Secure Corporation, Malwarebytes, MediaMath, the National Cyber-Forensics and Training Alliance and The Shadowserver Foundation for

VWA
VICTIM WITNESS ASSISTANCE

The Department of Justice believes that it is important to keep victims/witnesses of federal crime informed of court proceedings and what services may be available to assist you.

LEARN MORE


EUROPOL
ABOUT EUROPOL
ACTIVITIES & SERVICES
CRIME AREAS & TRENDS
PARTNERS & AGREEMENTS
CAREERS & PROCUREMENT
NEWSROOM
HOME
NEWSROOM
ANDROMEDA BOTNET DISMANTLED IN INTERNATIONAL CYBER OPERATION
Automated translation
ANDROMEDA BOTNET DISMANTLED IN INTERNATIONAL CYBER OPERATION
04 December 2017
Press Release
THIS NEWS/PRESS RELEASE IS ABOUT
CYBERCRIME
View all crime areas
On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue).
This widely distributed malware created a network of infected computers called the Andromeda botnet[1] . According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month. Andromeda was also used in the infamous Avalanche network, which was dismantled in a huge international cyber operation in 2016.


Spam
Victim
browses
Win32/Boaxxe.G
Win32/Glubteba.M
deploys
deploys
Linux/Cdorked redirection target (reverse proxy)
DNS
Linux/Onimiki
Linux/Cdorked
Win32/Glubteba.M C&C server proxy
C&C
Win32/Glubteba.M C&C server
Linux/Cdorked HTTP backend server
Linux/Cdorked configuration request
Spam
Perl/Calbot
HTTPS reverse proxy
C&C
Perl/Calbot C&C server
Spam
SSH tunnel
SSH tunnel
All Linux/Ebury infected hosts
Linux/Ebury exfiltration server
fetch credentials
gathered information on all Linux/Ebury infected hosts
deploy malware on servers
Annonymising tunnel endpoint
Operator
?
Legitimate system/user
Involved in malicious activity
Infected with Linux/Ebury
Infected with Linux/Cdorked
Infected with Linux/Onimiki
Infected with Perl/Calfbot

25,000+

infected servers

35m+

spam messages per day

THE UNITED STATES DEPARTMENT of JUSTICE

Search this site

ABOUT | OUR AGENCY | PRIORITIES | NEWS | RESOURCES | CAREERS | CONTACT

Home » Office of Public Affairs » News

SHARE

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, August 3, 2017

Russian Citizen Sentenced to 46 Months in Prison for Involvement in Global Botnet Conspiracy

The FBI Minneapolis Field Office investigated this case. Senior Counsels Aaron Cooper and Benjamin Fitzpatrick of the Criminal Division's Computer Crime and Intellectual Property Section and former Assistant U.S. Attorney Kevin Ueland of the District of Minnesota prosecuted the case. The government of Finland, the Bundeskriminalamt (BKA), CERT-Bund and the cyber security firm ESET all provided substantial assistance in this case. The Criminal Division's Office of International Affairs also provided substantial assistance.

Component(s):

Press Release Number:

RELATED LINKS

Speeches and Press Releases

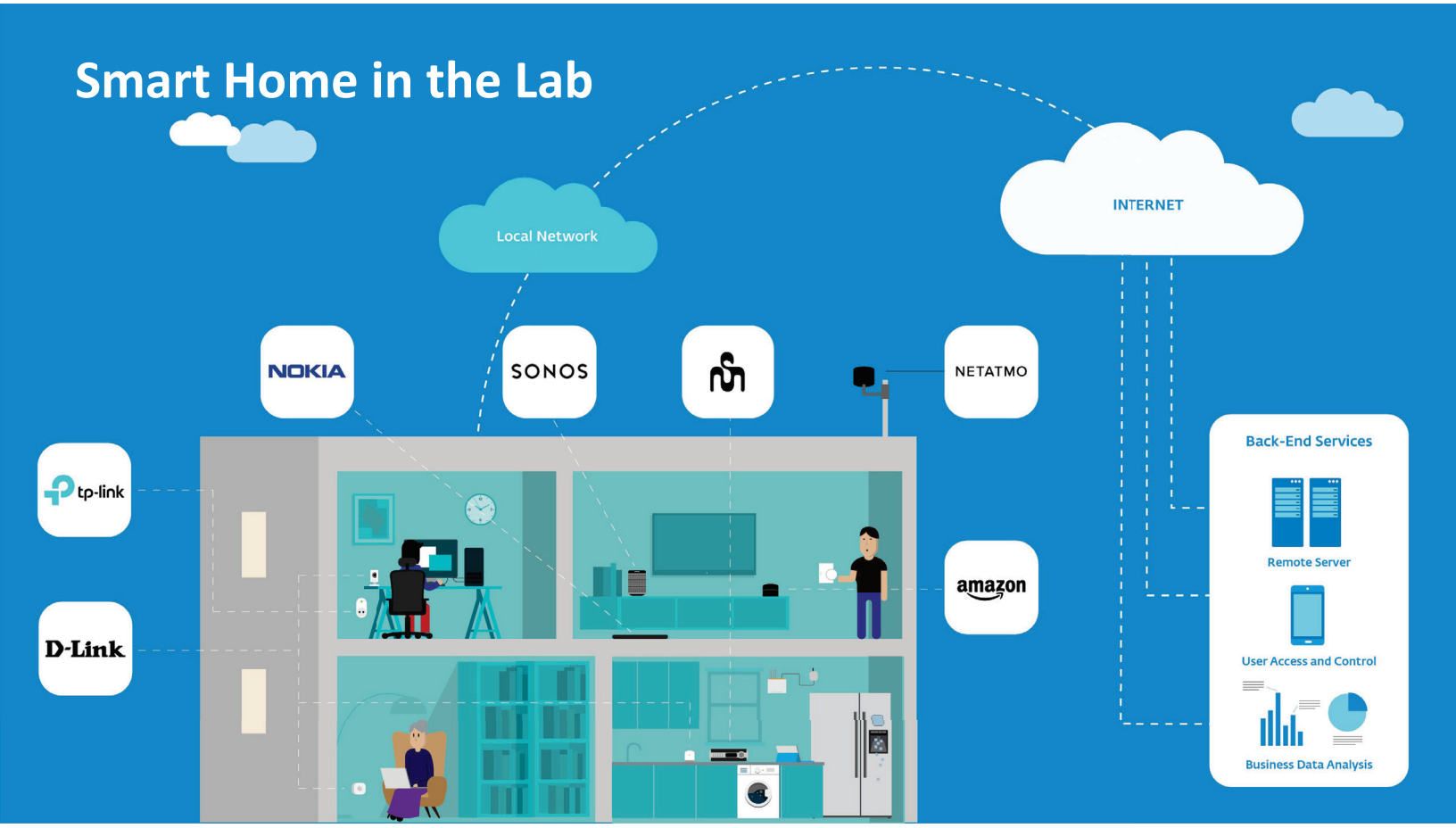
Videos

Photos

RSAConference2019

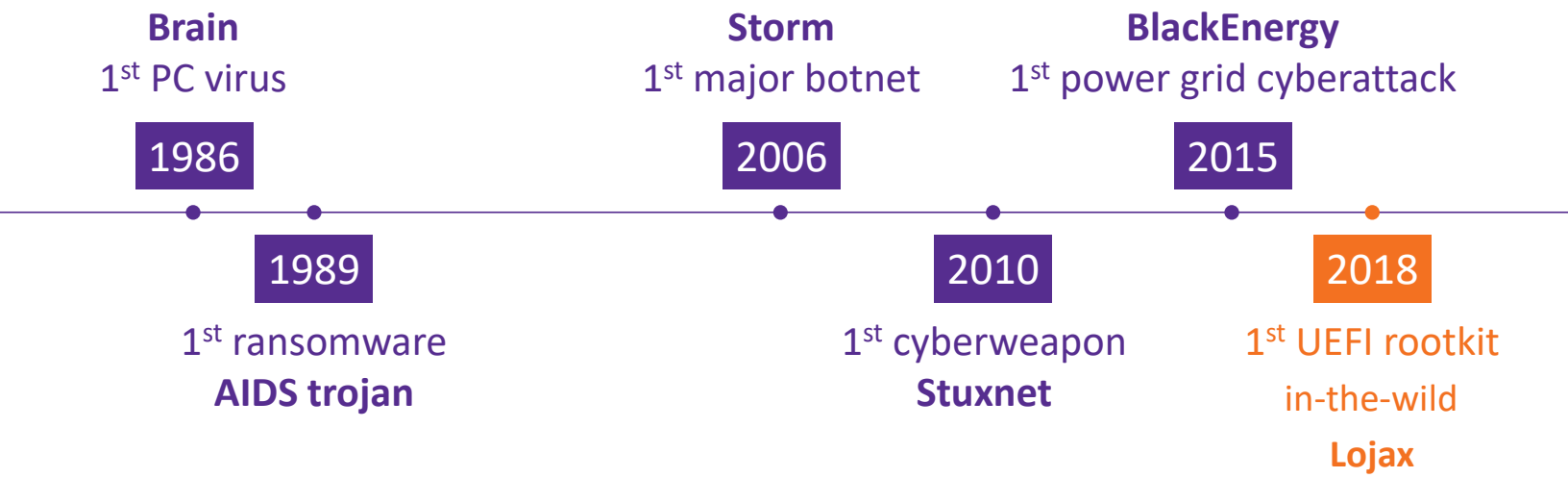
Internet of Targets

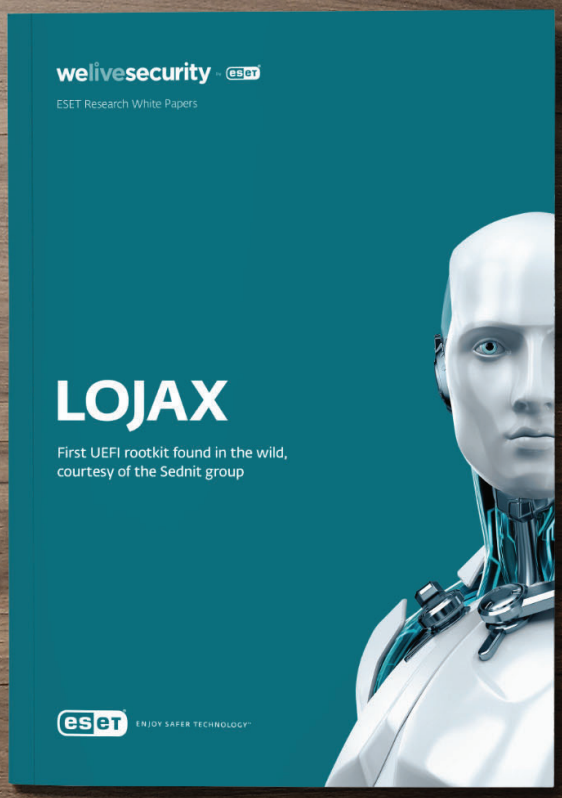
Smart Home in the Lab




PWNed
D-Link

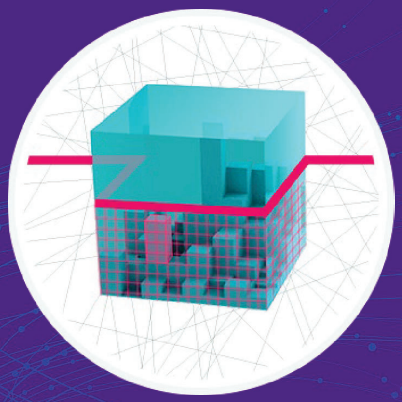
Malware attack firsts…




welivesecurity by ESET
ESET Research White Papers
LOJAX
First UEFI rootkit found in the wild,
courtesy of the Sednit group
ESET ENJOY SAFER TECHNOLOGY®

RSAConference2019

UEFI Scanner

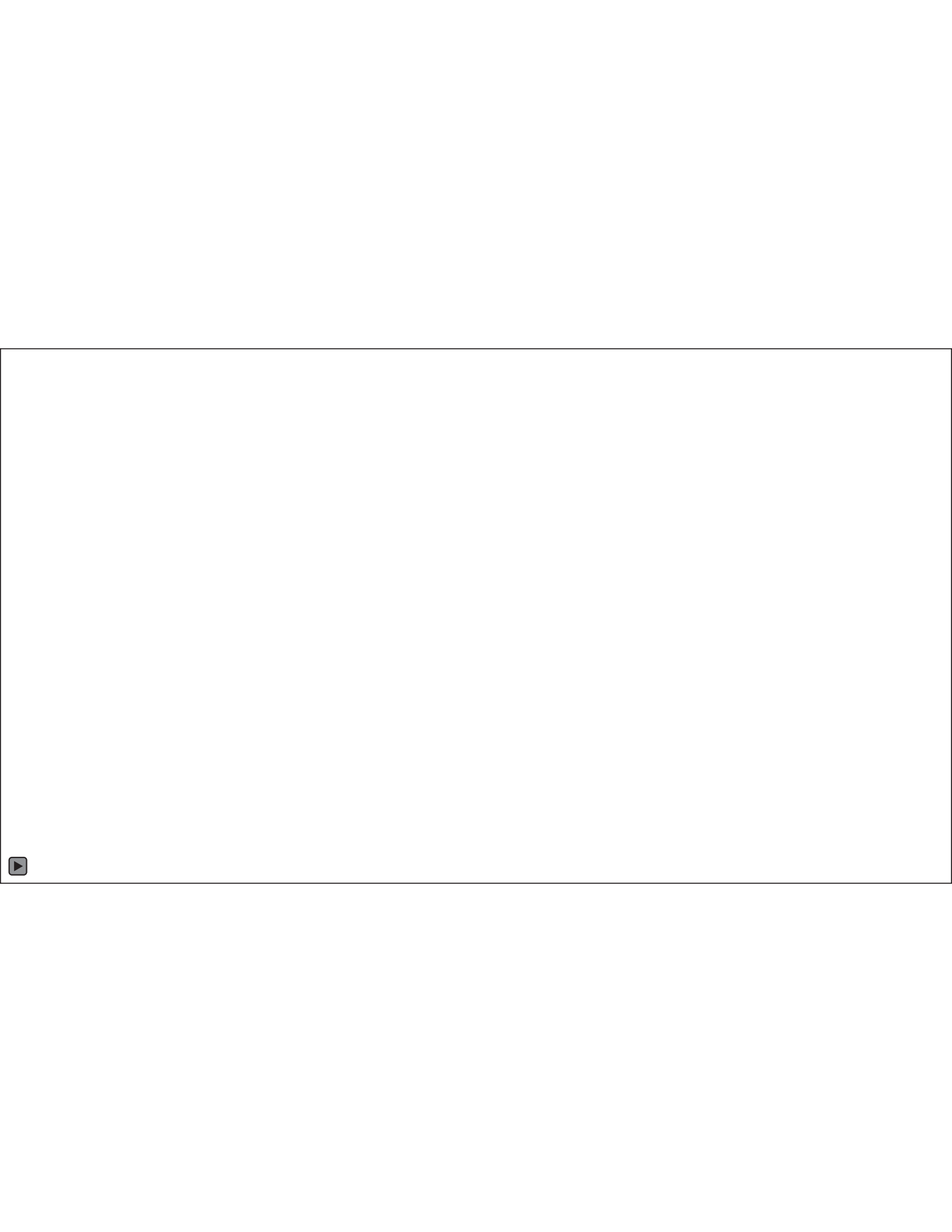


Do you trust your providers…?

… for example ISPs?

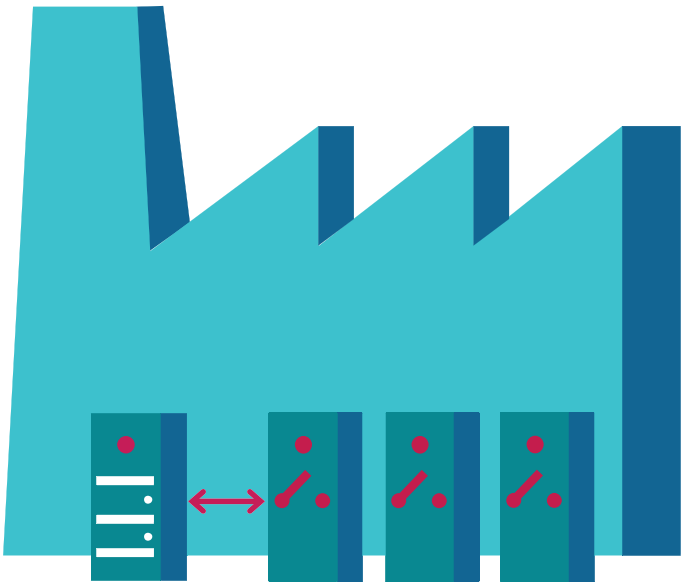

CYBER SOLUTIONS FOR THE
FIGHT AGAINST CRIME
FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

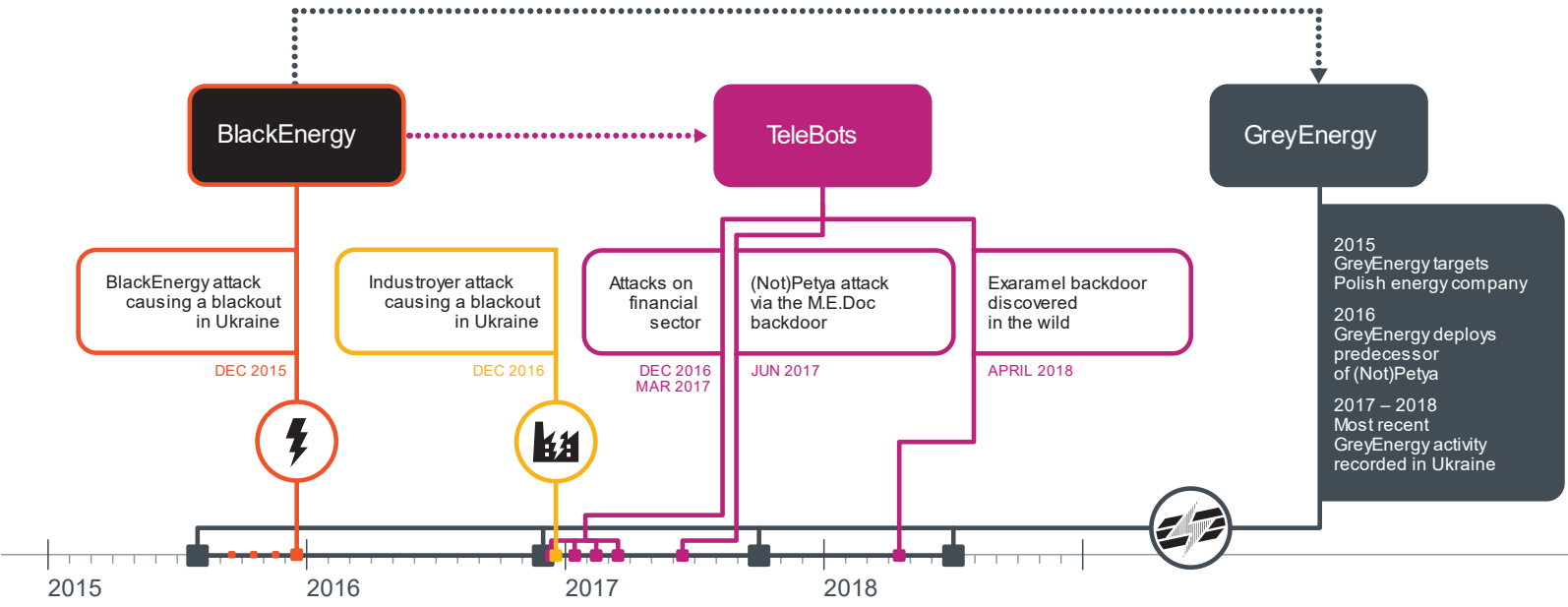
BlackEnergy



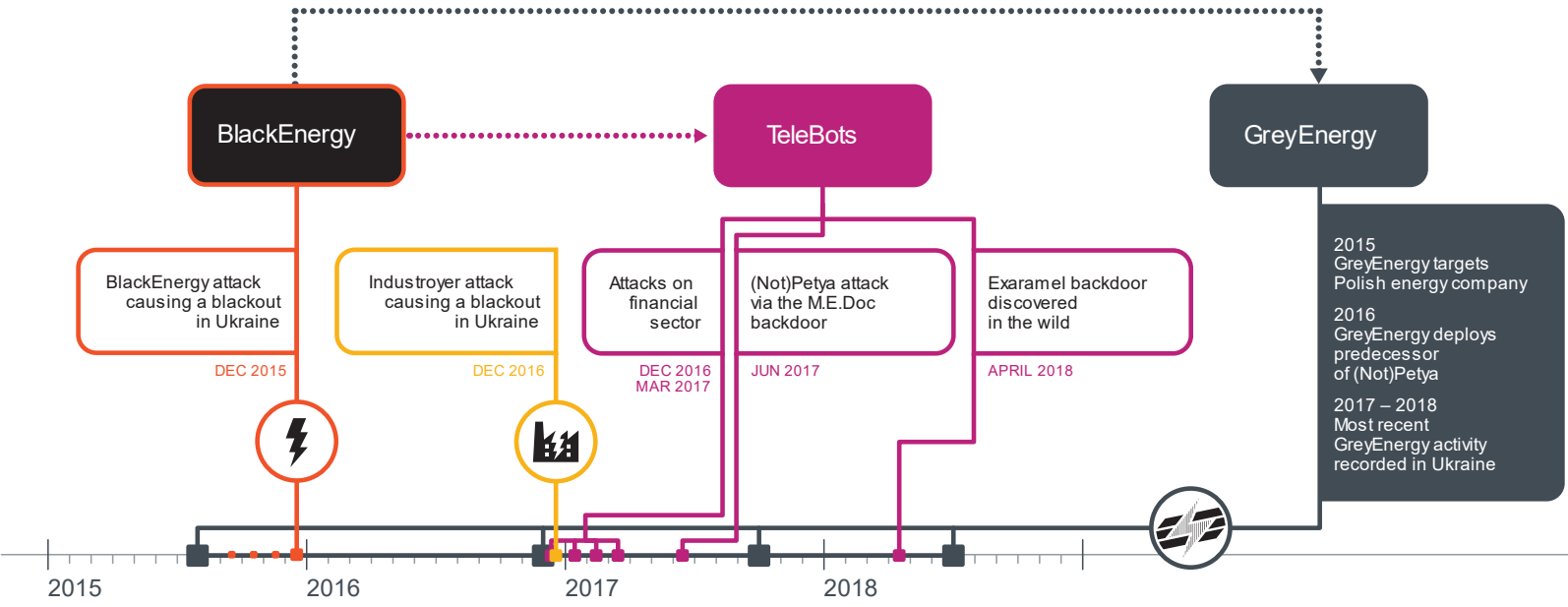
Industroyer

Industroyer

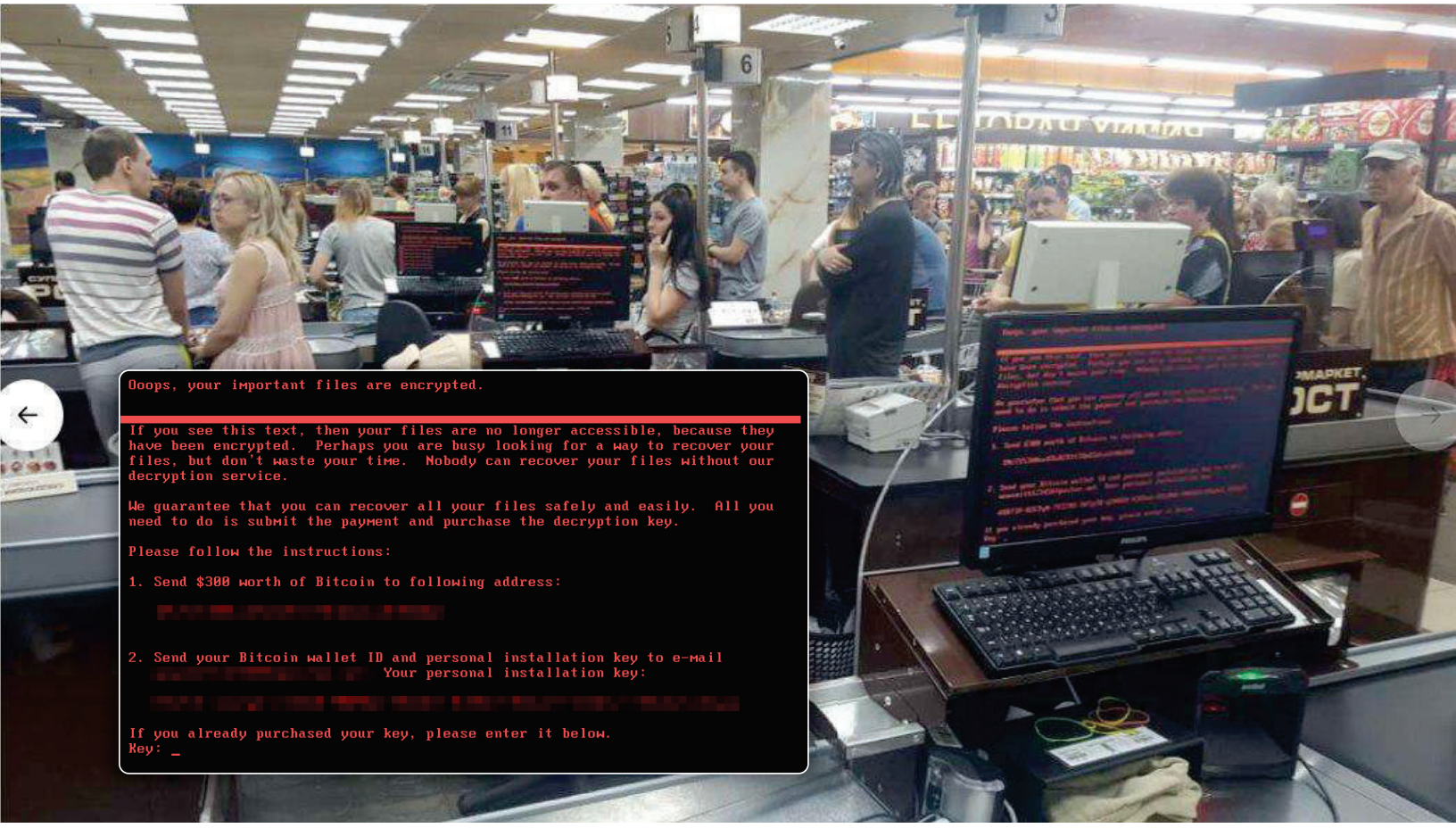



BlackEnergy
TeleBots
GreyEnergy
BlackEnergy attack causing a blackout in Ukraine
DEC 2015
Industroyer attack causing a blackout in Ukraine
DEC 2016
Attacks on financial sector
DEC 2016
MAR 2017
(Not)Petya attack via the M.E.Doc backdoor
JUN 2017
Exaramel backdoor discovered in the wild
APRIL 2018
2015
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


welivesecurity by ESET
Anton Cherepanov
GreyEnergy
Updated arsenal of one of the most dangerous threat actors
ESET ENJOY SAFER TECHNOLOGY


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

Pety…ent Zero


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
2. Send your Bitcoin wallet ID and personal installation key to e-mail
Your personal installation key:
If you already purchased your key, please enter it below.
Key: _

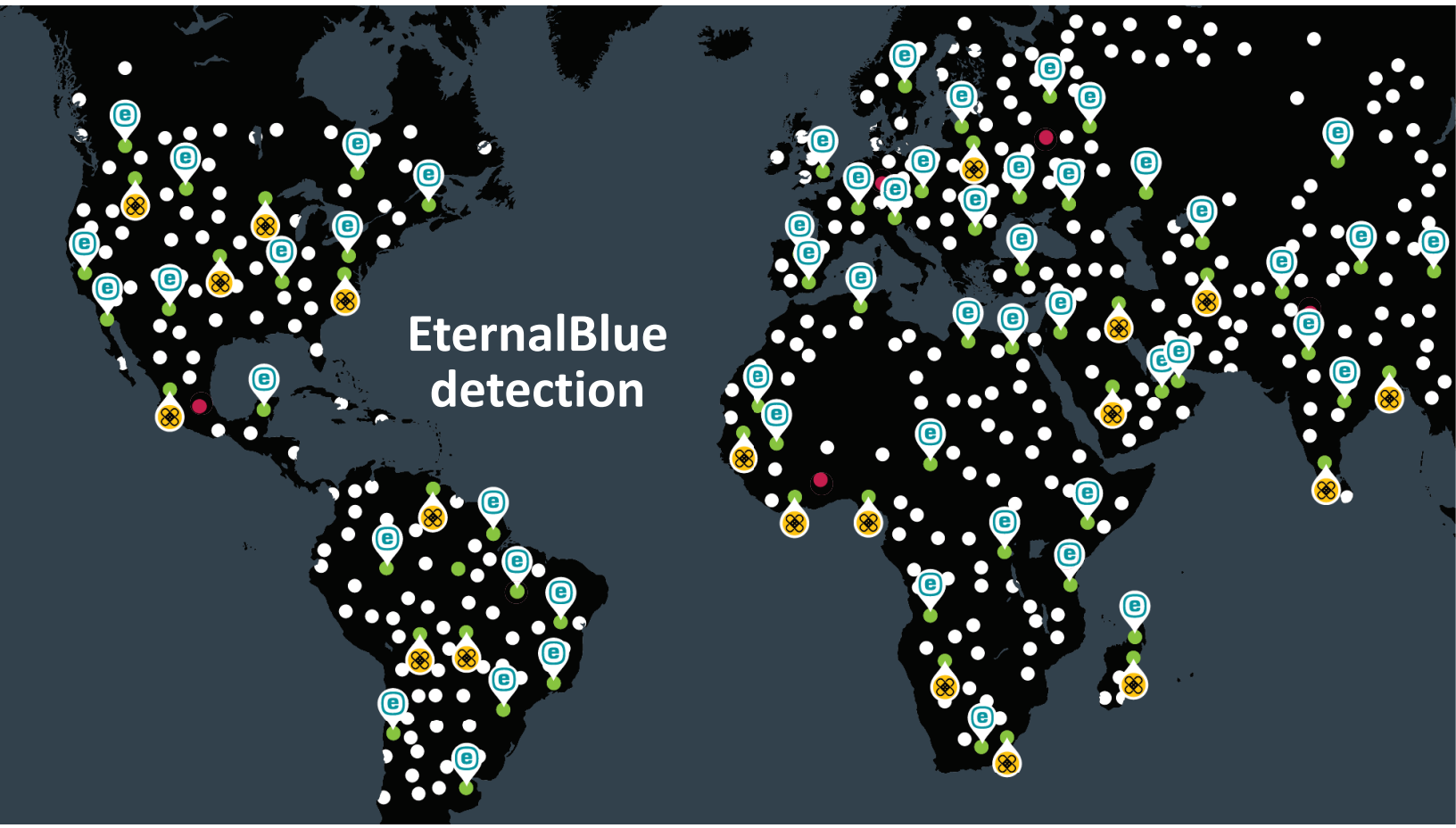

love sex
durex
Extra Safe
12 Pack
MAERS
POCHEФТ
FedEx
MERCK


$300m
$129m
love sex
durex
Extra Safe
12 Pack
$870m
$400m
FedEx
MERCK

$10 BILLION

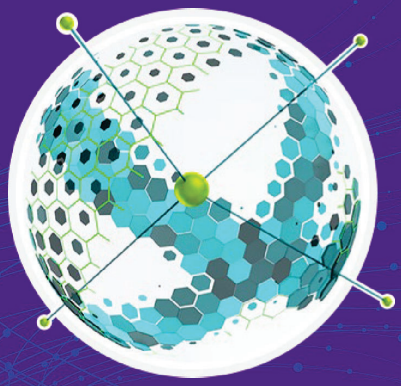
total estimated damage from NotPetya

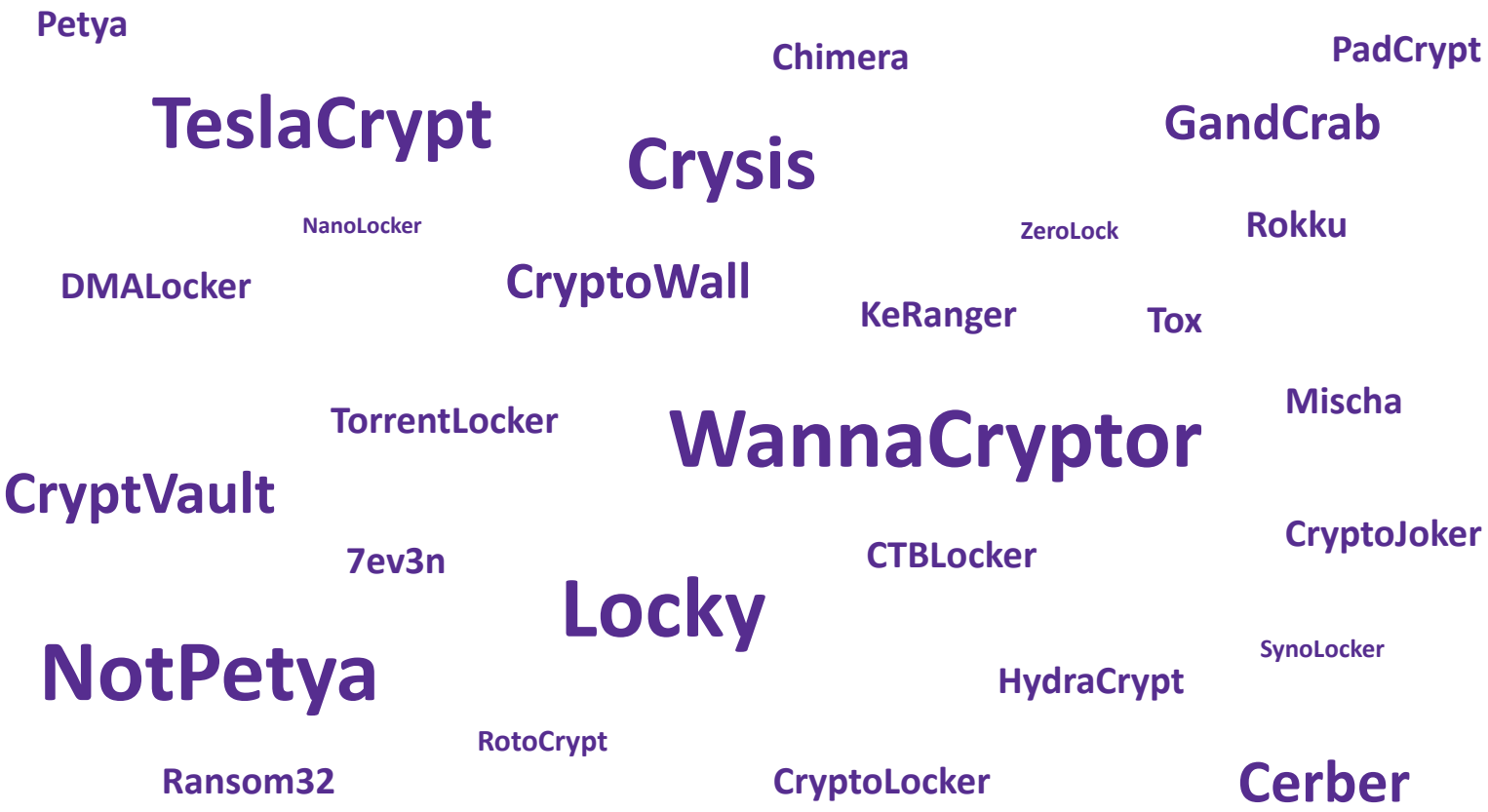
Source: U.S.White House as quoted by Wired


EternalBlue
detection

RSAConference2019

Network Attack Protection

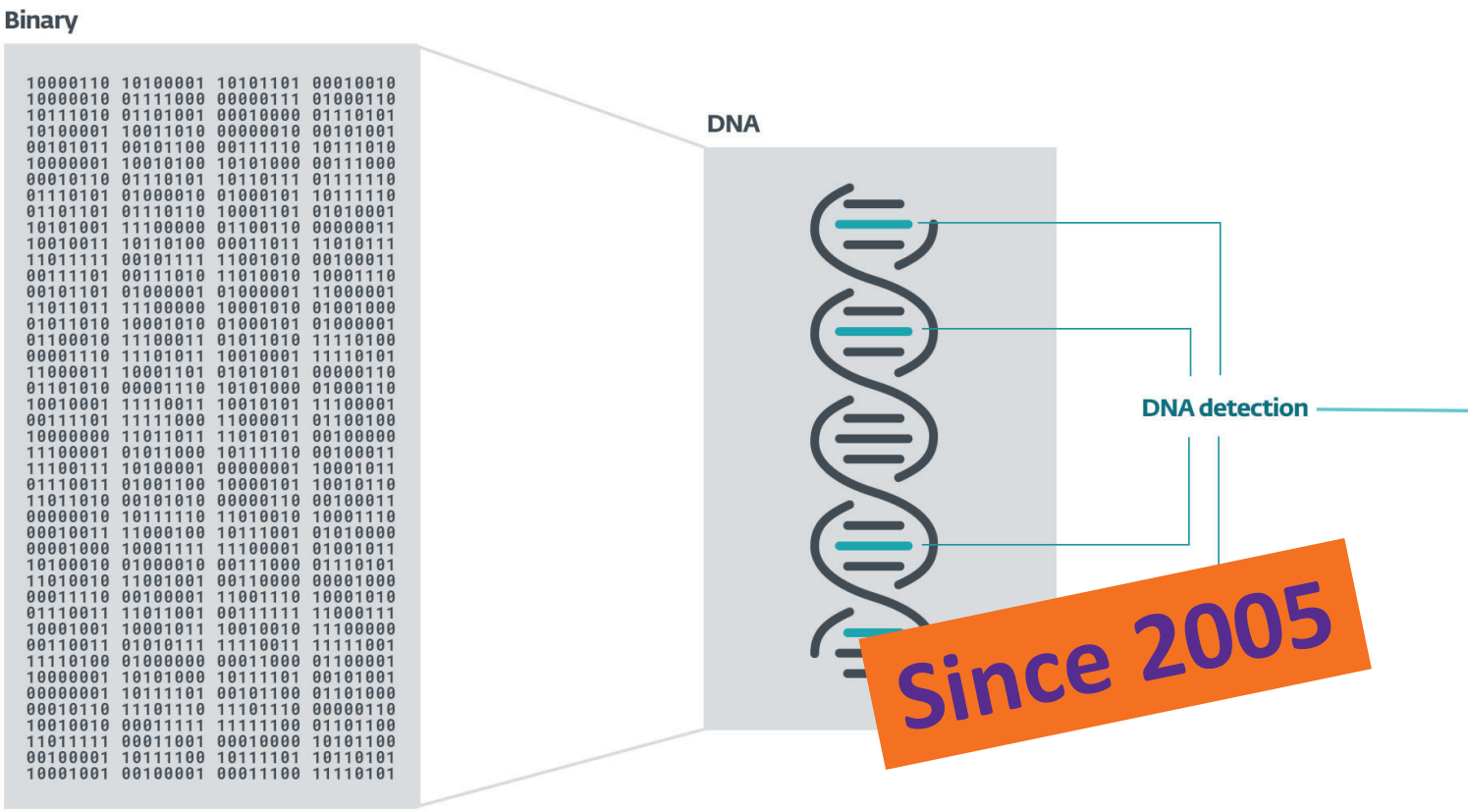



Petya
Chimera
PadCrypt
TeslaCrypt
Crysis
GandCrab
NanoLocker
ZeroLock
Rokku
DMALocker
CryptoWall
KeRanger
Tox
Mischa
TorrentLocker
WannaCryptor
CryptVault
CryptoJoker
7ev3n
CTBLocker
Locky
NotPetya
SynoLocker
HydraCrypt
RotoCrypt
Ransom32
CryptoLocker
Cerber

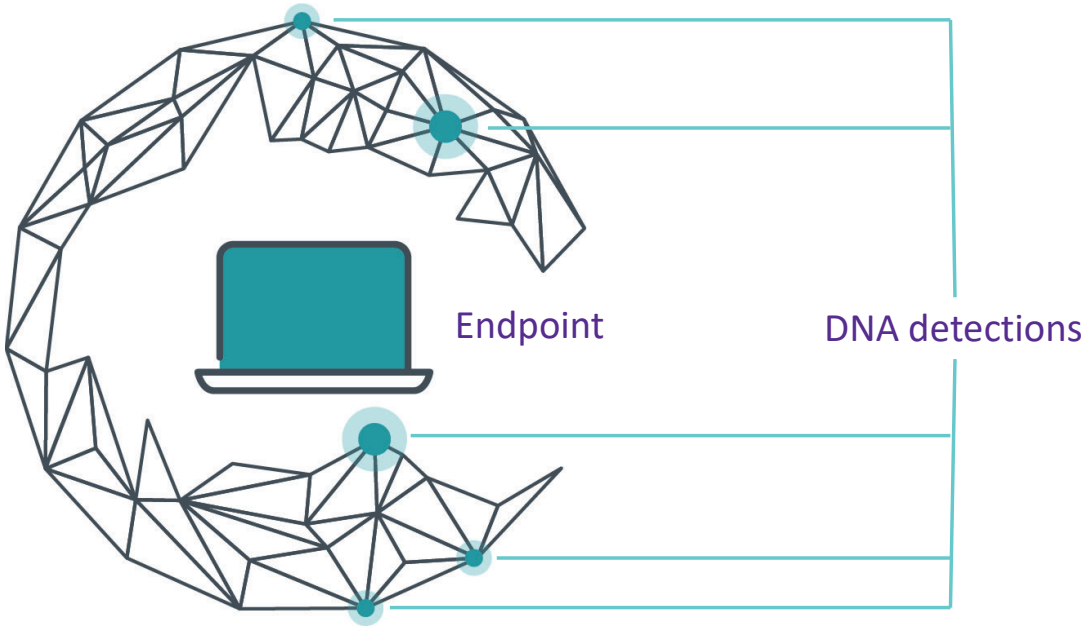
RSAConference2019

Juraj Janosik

Head of ESET AI/ML team

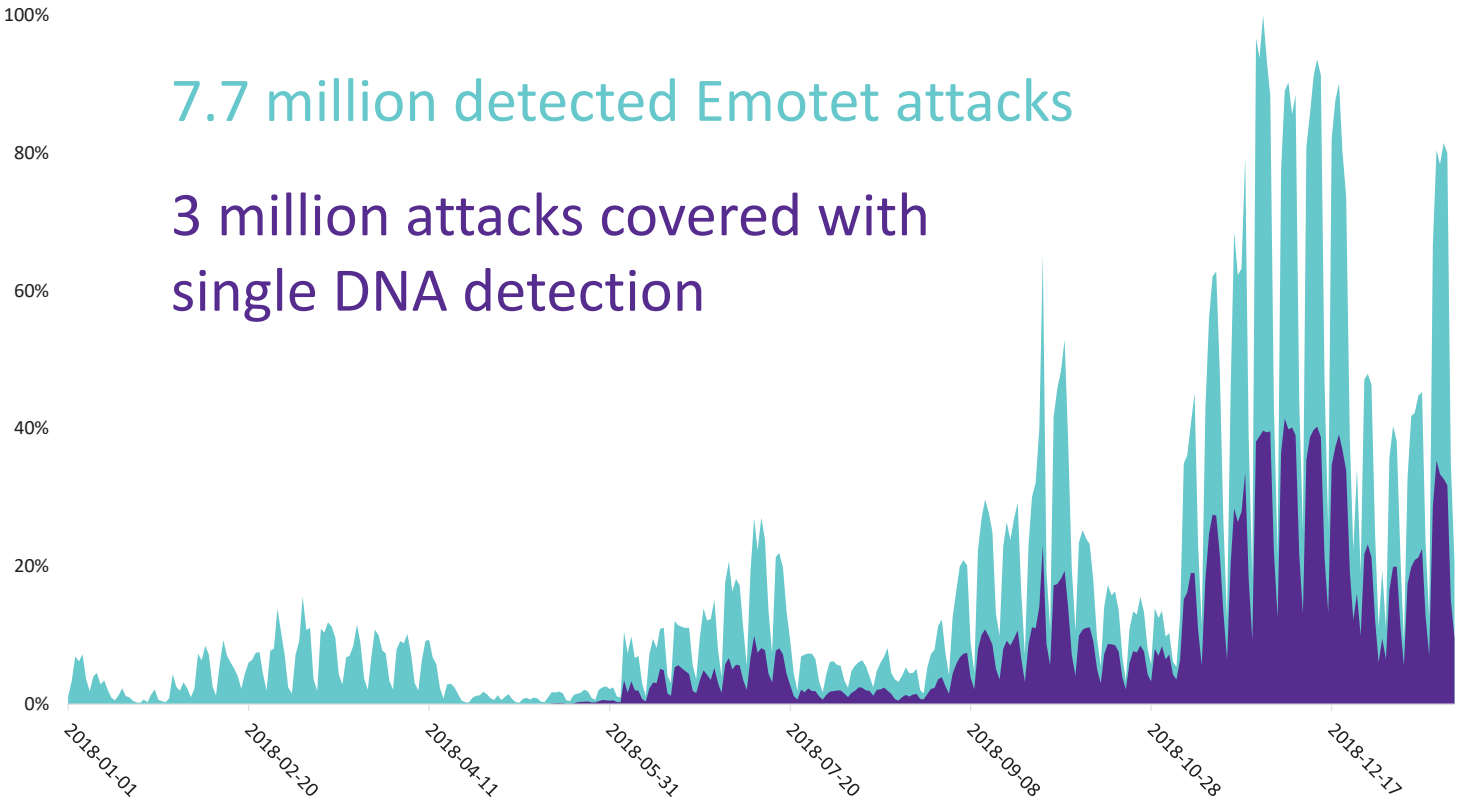

Binary
10000110 10100001 10101101 00010010
10000010 01111000 00000111 01000110
10111010 01101001 00010000 01110101
10100001 10011010 00000010 00101001
00101011 00101100 00111110 10111010
10000001 10010100 10101000 00111000
00010110 01110101 10110111 01111110
01110101 01000010 01000101 10111110
01101101 01110110 10001101 01010001
10101001 11100000 01100110 00000011
10010011 10110100 00011011 11010111
11011111 00101111 11001010 00100011
00111101 00111010 11010010 10001110
00101101 01000001 01000001 11000001
11011011 11100000 10001010 01001000
01011010 10001010 01000101 01000001
01100010 11100011 01011010 11110100
00001110 11101011 10010001 11110101
11000011 10001101 01010101 00000110
01101010 00001110 10101000 01000110
10010001 11110011 10010101 11100001
00111101 11111000 11000011 01100100
10000000 11011011 11010101 00100000
11100001 01011000 10111110 00100011
11100111 10100001 00000001 10001011
01110011 01001100 10000101 10010110
11011010 00101010 00000110 00100011
00000010 10111110 11010010 10001110
00010011 11000100 10111001 01010000
00001000 10001111 11100001 01001011
10100010 01000010 00111000 01110101
11010010 11001001 00110000 00001000
00011110 00100001 11001110 10001010
01110011 11011001 00111111 11000111
10001001 10001011 10010010 11100000
00110011 01010111 11110011 11111001
11110100 01000000 00011000 01100001
10000001 10101000 10111101 00101001
00000001 10111101 00101100 01101000
00010110 11101110 11101110 00000110
10010010 00011111 11111100 01101100
11011111 00011001 00010000 10101100
00100001 10111100 10111101 10110101
10001001 00100001 00011100 11110101
DNA
DNA detection
Since 2005

DNA detection model



RSAConference2019

DNA Detections


7.7 million detected Emotet attacks
3 million attacks covered with single DNA detection
100%
80%
60%
40%
20%
0%
2018-01-01
2018-02-20
2018-04-11
2018-05-31
2018-07-20
2018-09-08
2018-10-28
2018-12-17

RSAConference2019

Artificial Intelligence

RSAConference2019

~~Artificial Intelligence~~

RSAConference2019

Machine Learning

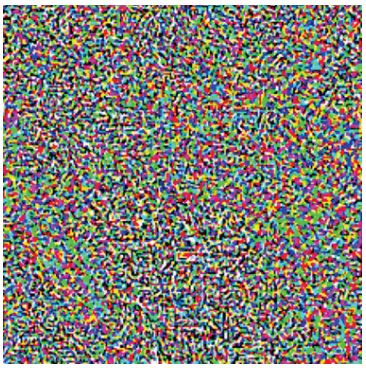
Machine Learning evolution

30+ years of experience and development

1998	2005	2006	2012
Neural Networks in Product	DNA Detections (Online Learning)	Expert System for Mass Processing	Automated Threat Mapping

„panda“
57.7% confidence

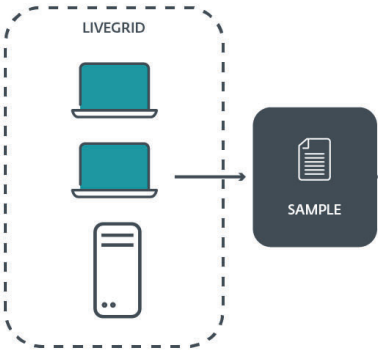
$+\epsilon$



$=$

„gibbon“
99.3% confidence

Source: OpenAI

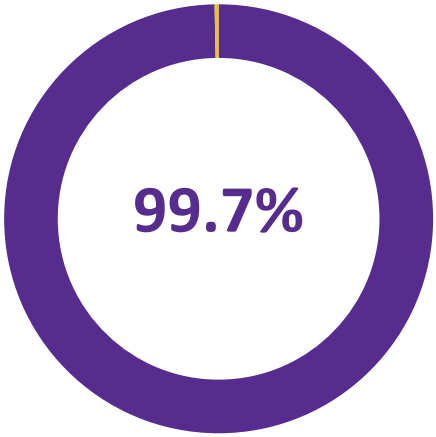

LIVEGRID
SAMPLE

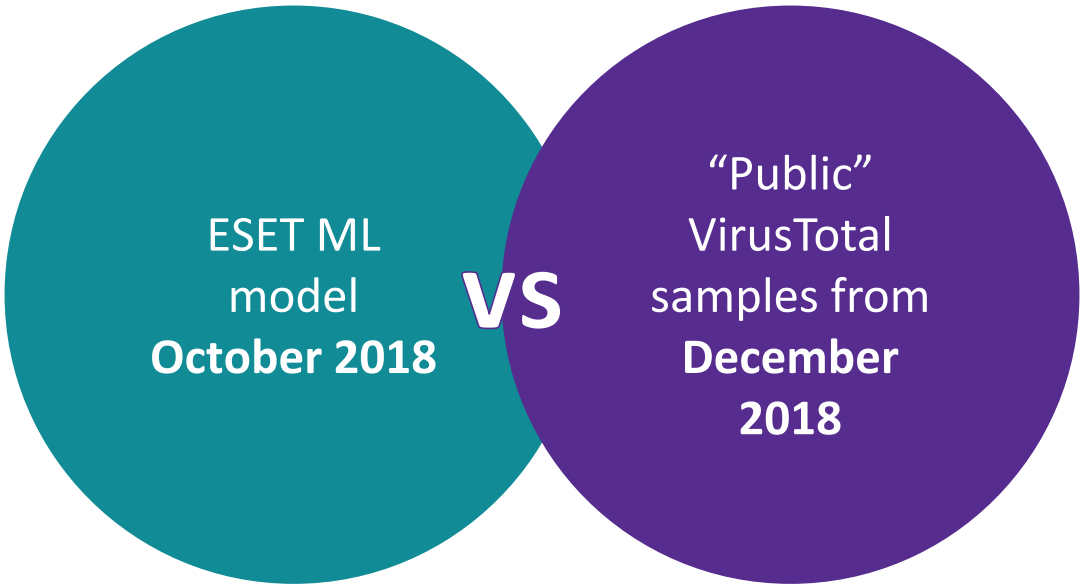
Old ML model vs. new malware samples

200+ ransomware samples

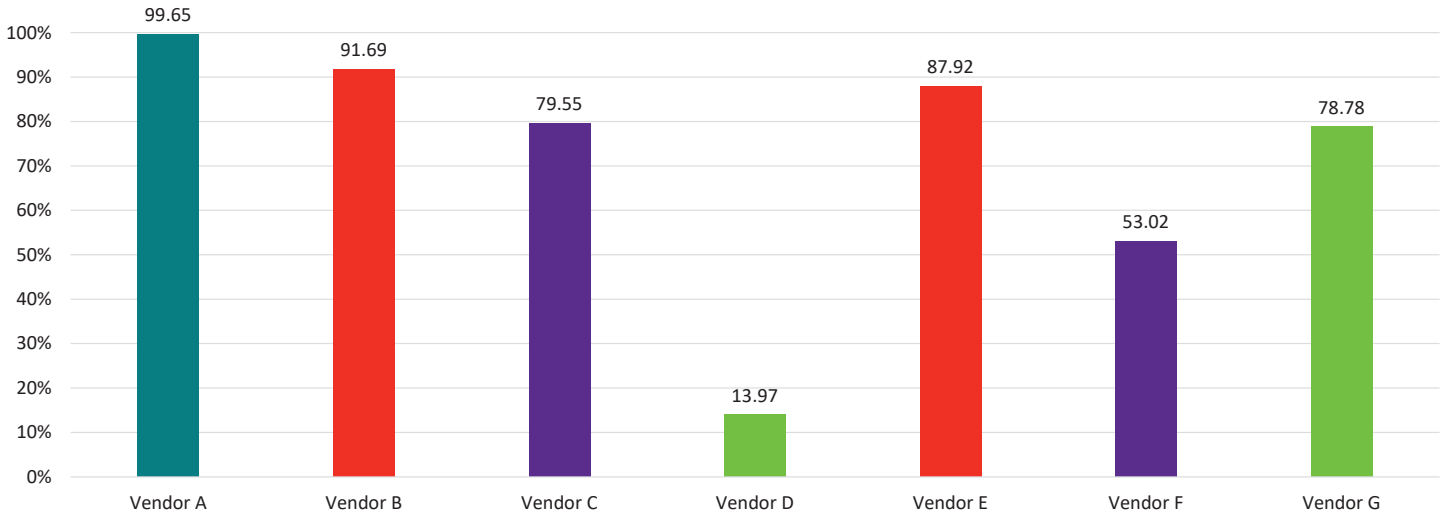
NotPetya
BadRabbit
Crysis
WannaCryptor

Detection ratio

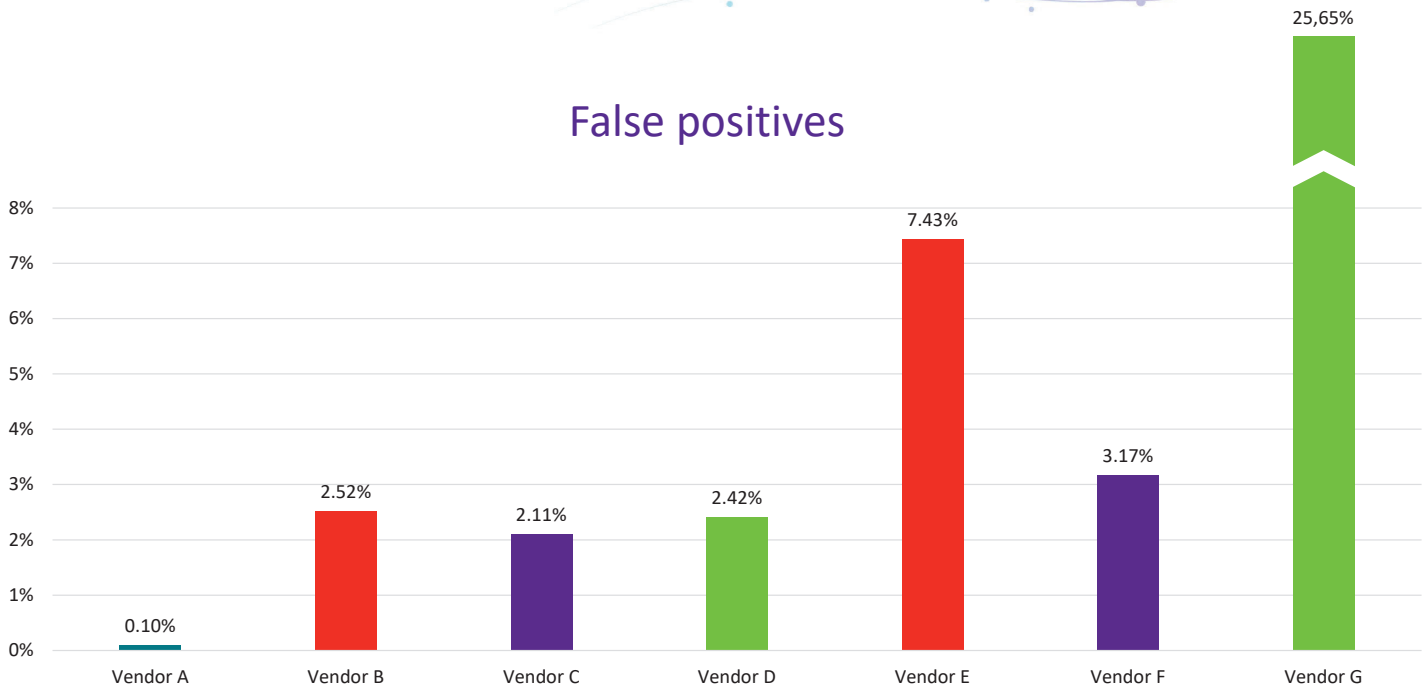



ESET ML
model
October 2018
VS
"Public"
VirusTotal
samples from
December
2018

Detection ratio



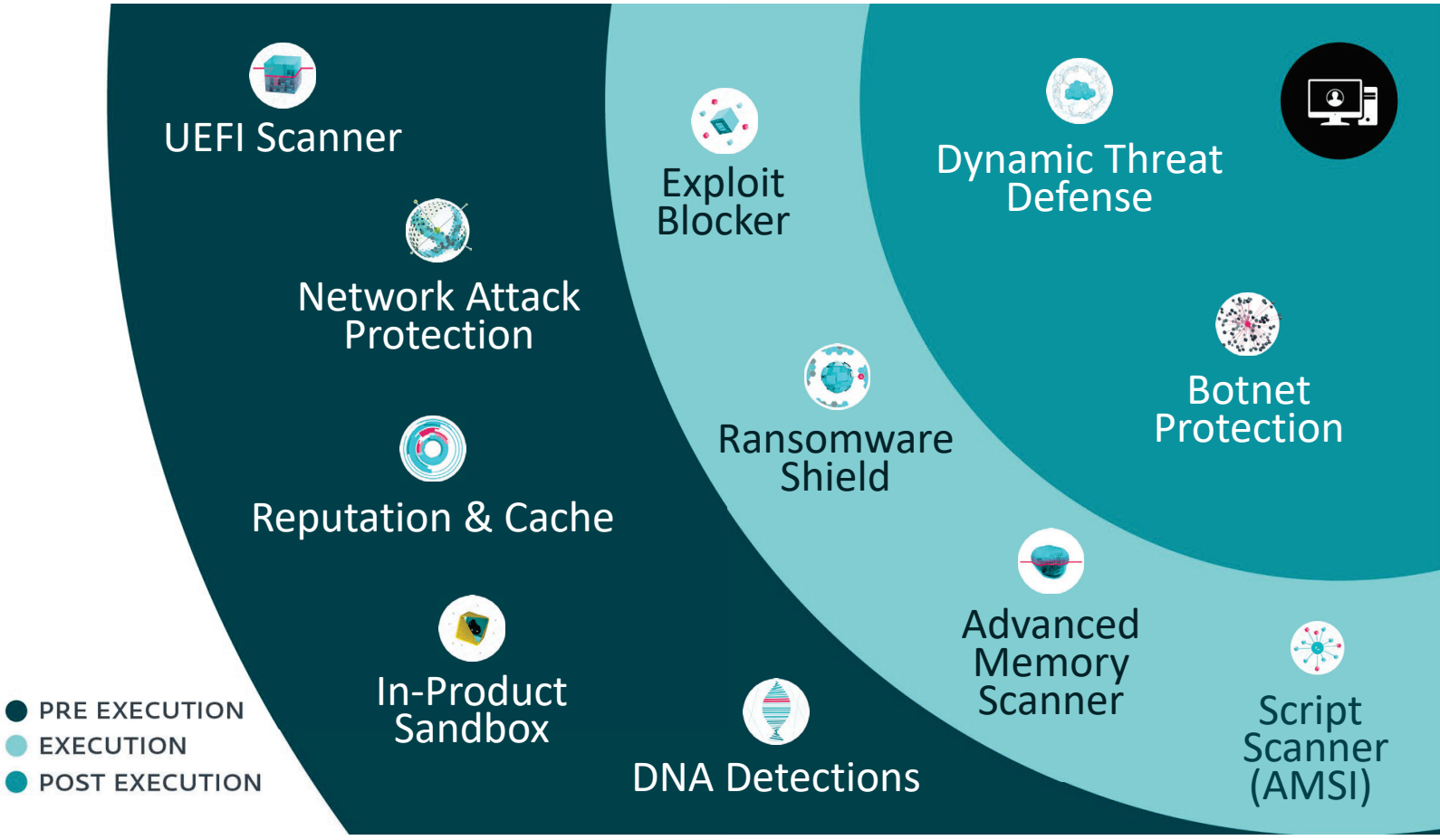
False positives



Big Data

Machine Learning

Human Expertise


UEFI Scanner
Network Attack Protection
Reputation & Cache
In-Product Sandbox
Exploit Blocker
Ransomware Shield
DNA Detections
Dynamic Threat Defense
Botnet Protection
Advanced Memory Scanner
Script Scanner (AMSI)
PRE EXECUTION
EXECUTION
POST EXECUTION

RSAConference2019