Sector Industrial

Bajo Ciber Ataques como nunca antes

kaspersky

Dwayne Porr Lesli

Entendemos las amenazas globales

Privacy & data
protection challenge

Consumerization & mobility

Increasing
online commerce

Internet of Things

Cloud & virtualization

Critical infrastructure at risk

Big data

Fragmentation of the Internet

Malware for ATMs

Merger of cybercrime and APT

Commercialization of APT

Supply chain attacks

Decreasing cost of APTs

Targeted attacks

Hacktivism

Internet of Things

Mobile threats

Online banking at risk

Massive data leaks

**Targeting
hotel networks**

Cyber-mercenaries

“Wipers” & cyber-sabotage

Ransomware programs

Financial phishing attacks

Attacks on PoS terminals

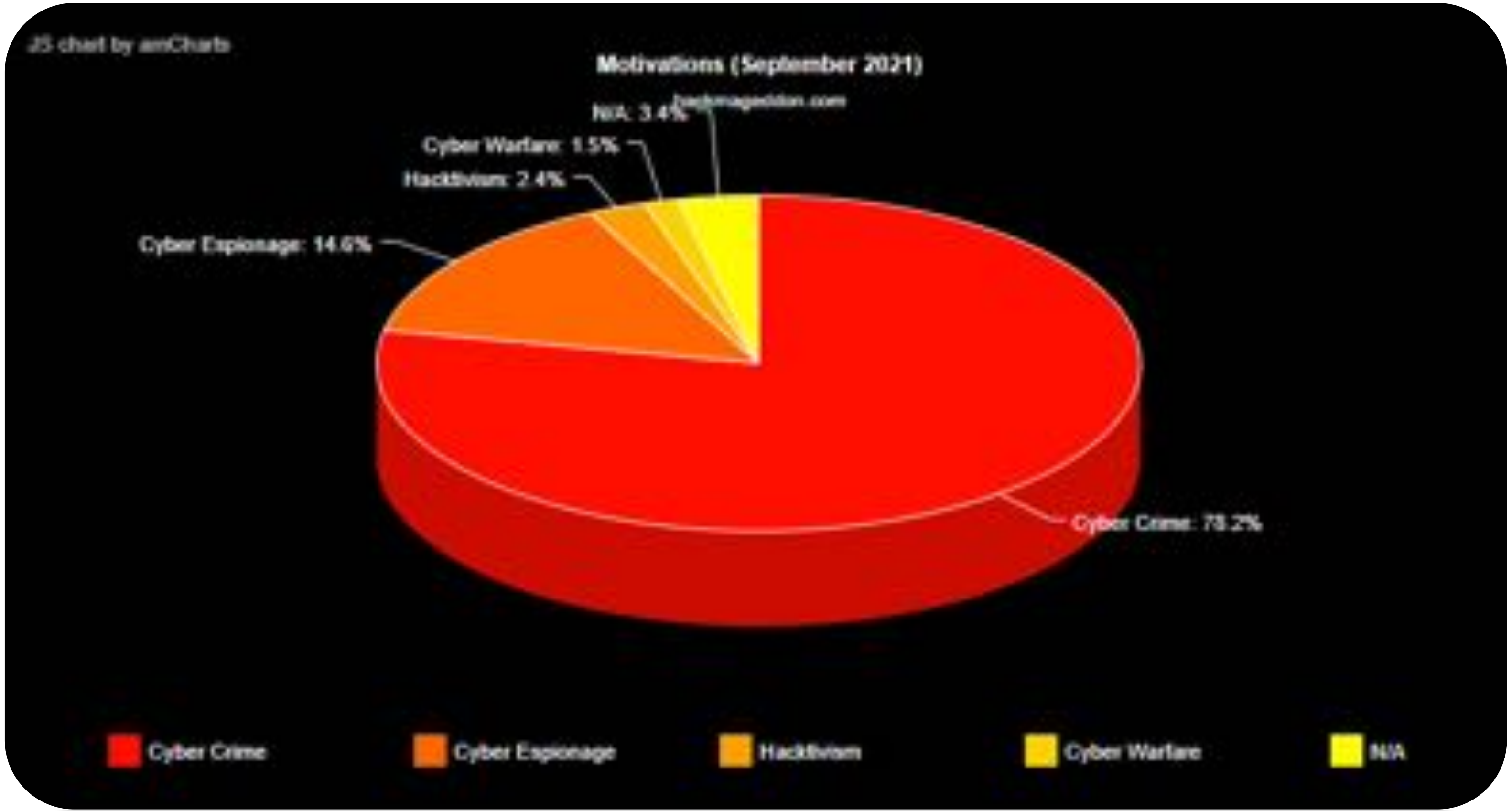
Threats
to Smart Cities

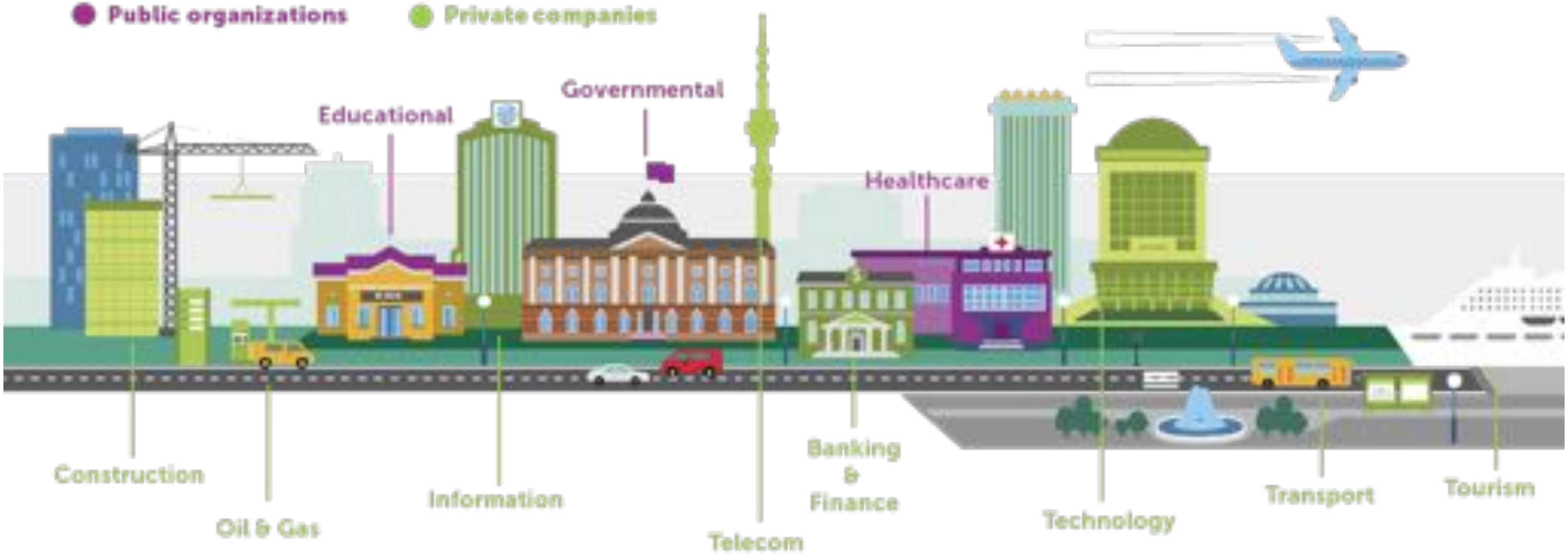
Los Ciberataques están Cambiando al mundo

Motivaciones, Actores y Objetivos

Image source: https://www.baesystems.com/en/cybersecurity/feature/the-unusual-suspects

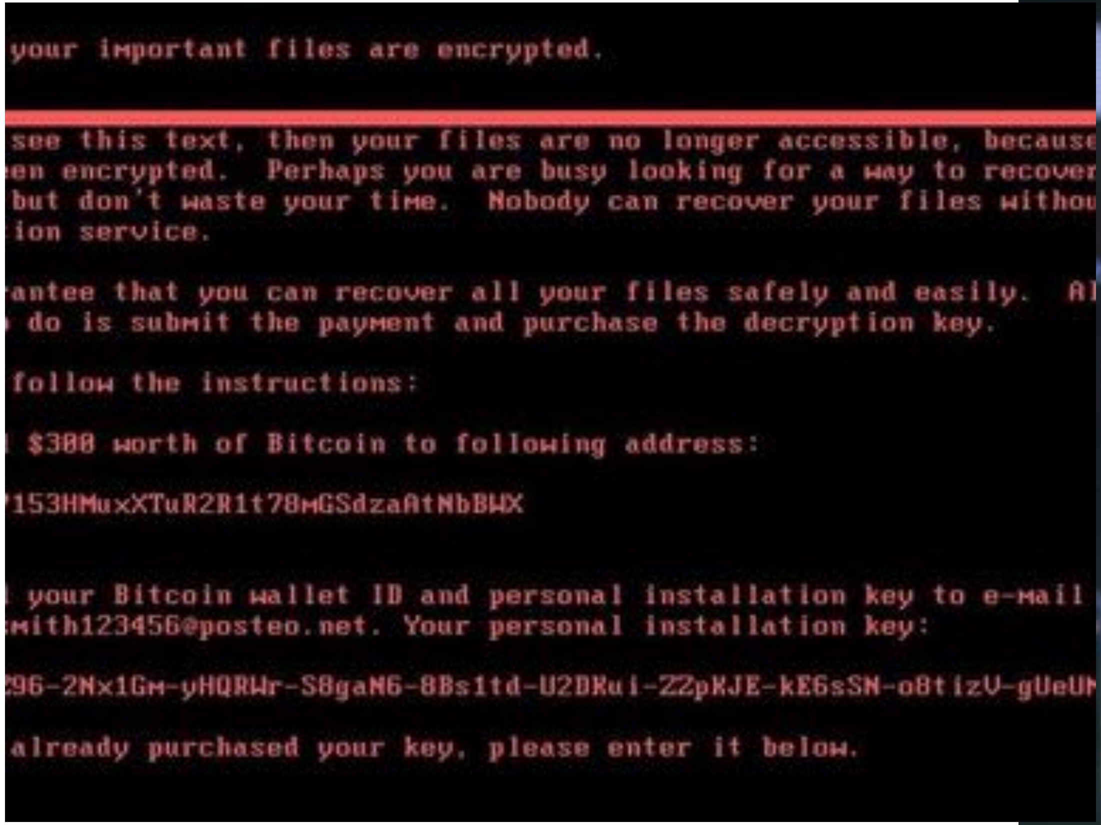
Estadísticas de ciberataques de septiembre de 2021





Todo Puede ser un blanco

Las Amenazas a la Seguridad de las Organizaciones se están Incrementando

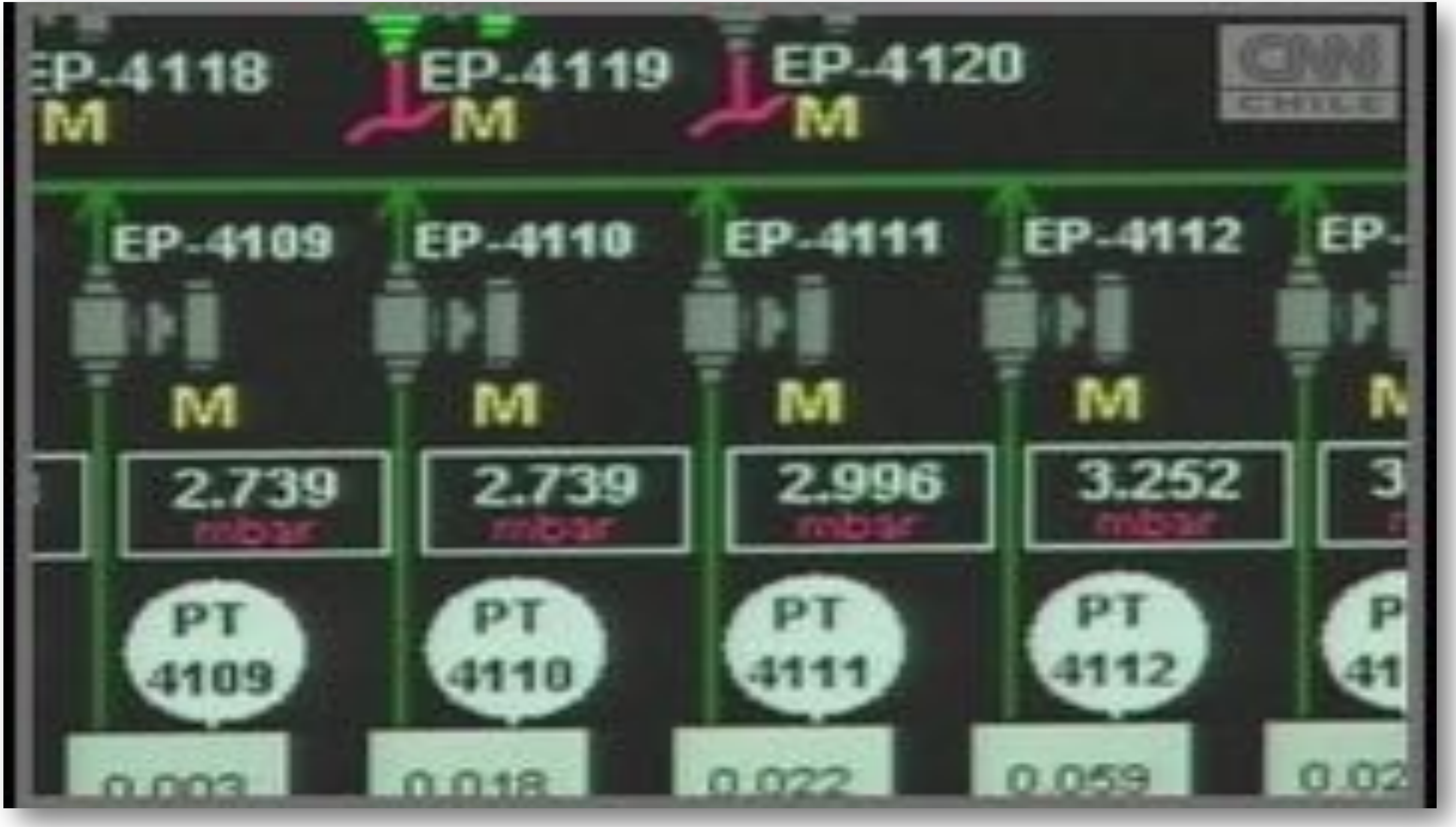


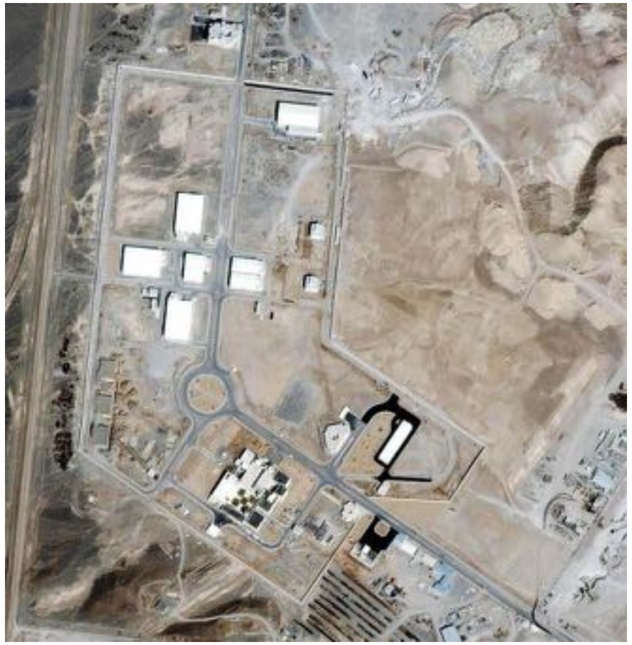
```
your important files are encrypted.

see this text, then your files are no longer accessible, because
en encrypted.  Perhaps you are busy looking for a way to recover
but don't waste your time.  Nobody can recover your files withou
ion service.

antee that you can recover all your files safely and easily.  Al
 do is submit the payment and purchase the decryption key.

follow the instructions:

 $300 worth of Bitcoin to following address:

153HMuxXTuR2R1t78mGSdzaAtNbBWX


 your Bitcoin wallet ID and personal installation key to e-mail
mith123456@posteo.net. Your personal installation key:

96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeU

already purchased your key, please enter it below.
```

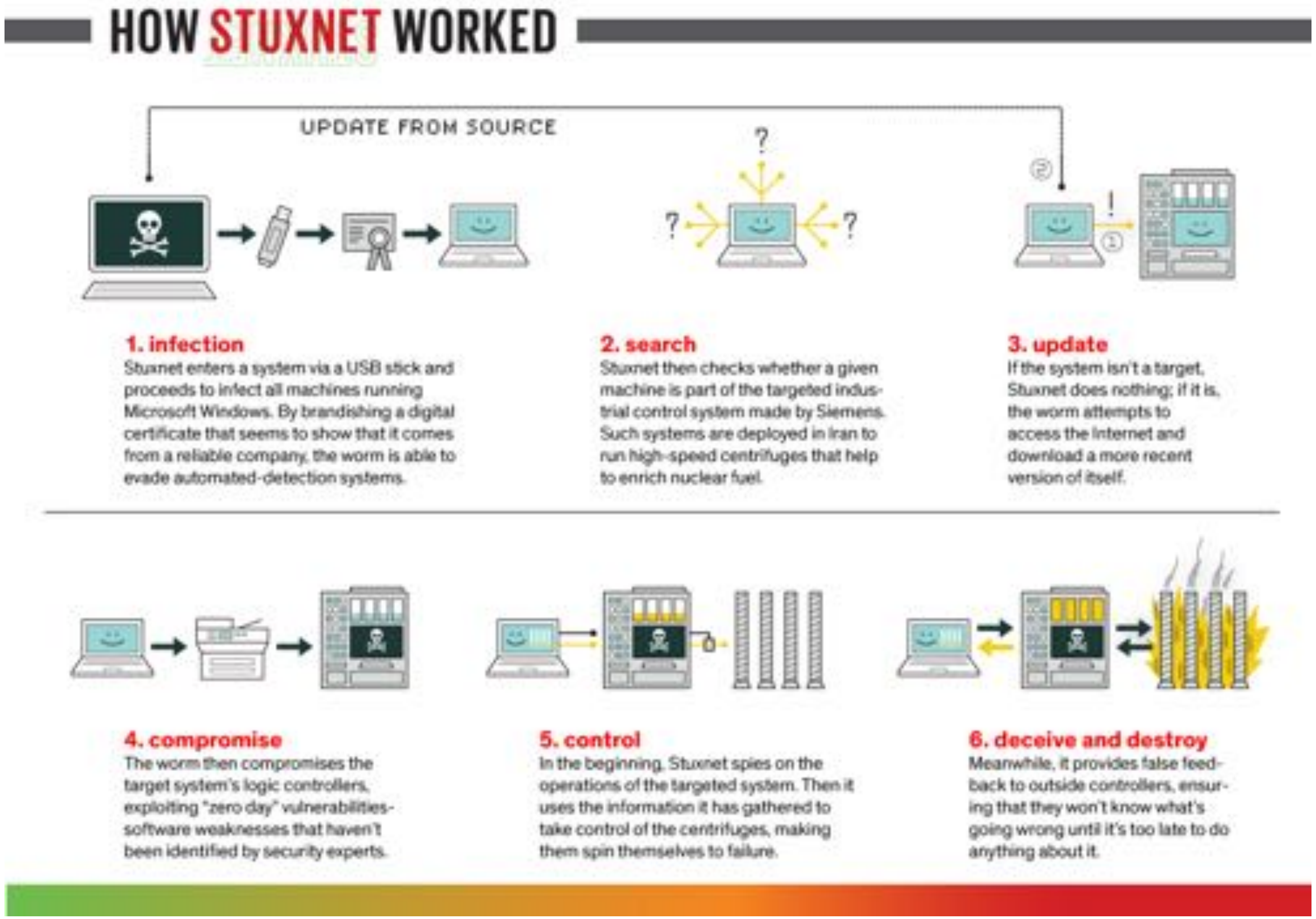
Ataques a Sistemas Industriales e Infraestructuras Críticas

kaspersky

Ficción vs. Realidad


EP-4118
M
EP-4119
M
EP-4120
M
CNN CHILE
EP-4109
M
2.739
mbar
PT 4109
0.003
EP-4110
M
2.739
mbar
PT 4110
0.018
EP-4111
M
2.996
mbar
PT 4111
0.022
EP-4112
M
3.252
mbar
PT 4112
0.059
EP-
M
3
PT 41
0.02





HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

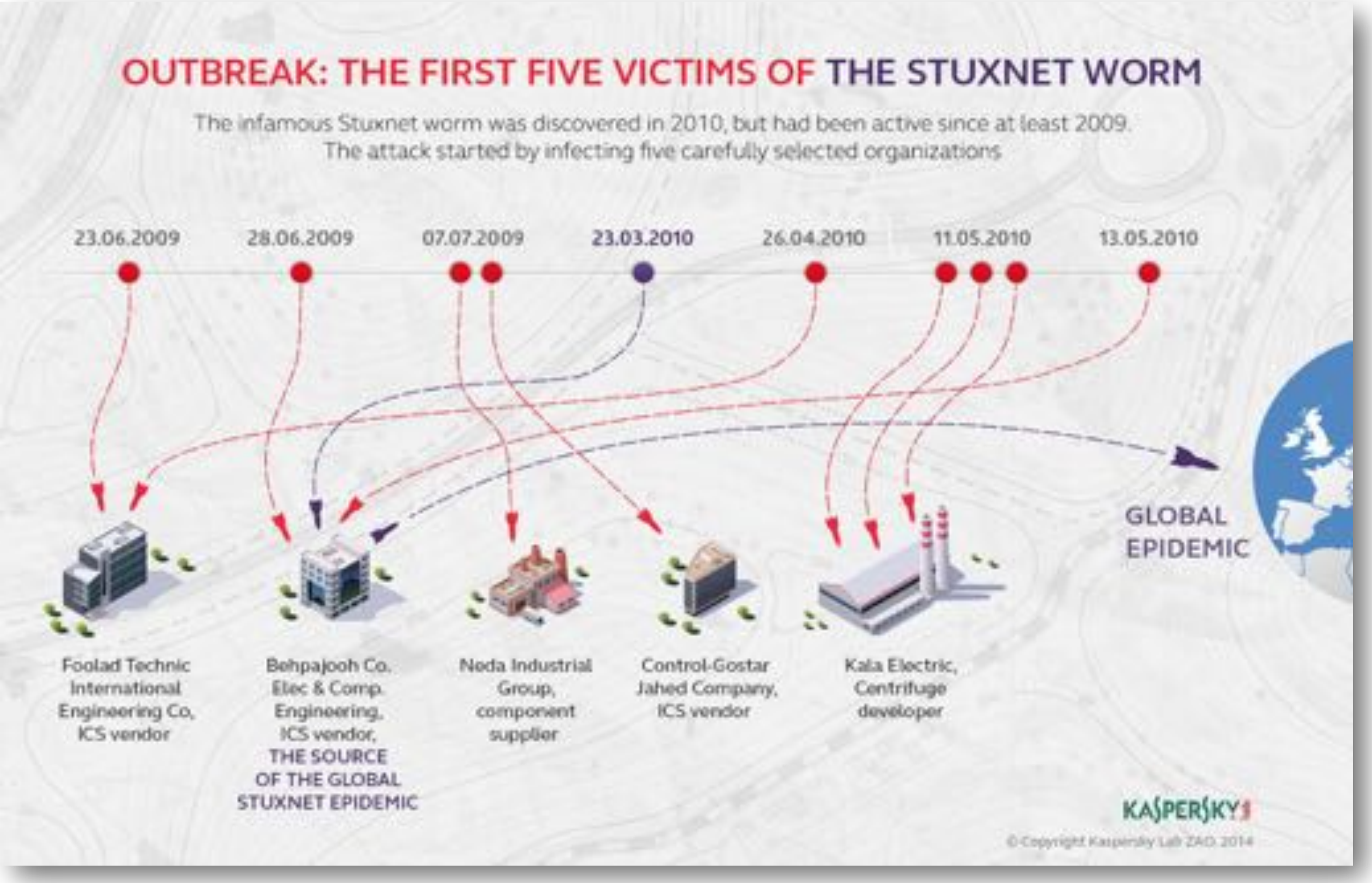
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet



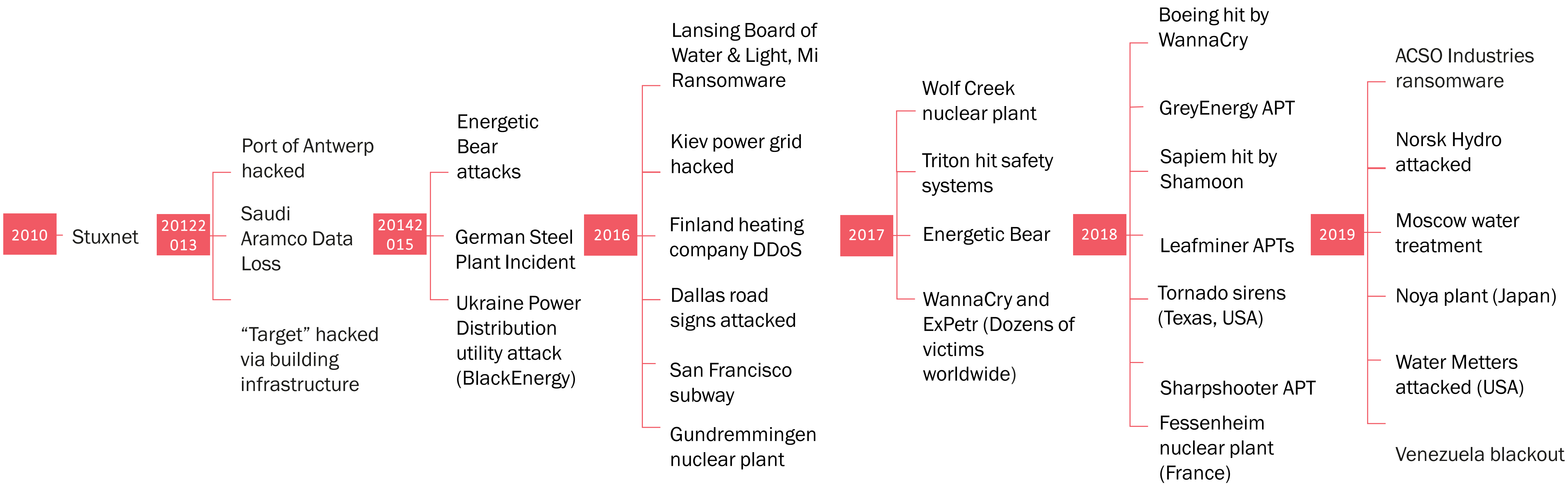
OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009.
The attack started by infecting five carefully selected organizations

23.06.2009
28.06.2009
07.07.2009
23.03.2010
26.04.2010
11.05.2010
13.05.2010
GLOBAL EPIDEMIC
Foolad Technic International Engineering Co, ICS vendor
Behpajooh Co. Elec & Comp. Engineering, ICS vendor, THE SOURCE OF THE GLOBAL STUXNET EPIDEMIC
Neda Industrial Group, component supplier
Control-Gostar Jahed Company, ICS vendor
Kala Electric, Centrifuge developer
KASPERSKY

© Copyright Kaspersky Lab ZAO 2014

Critical infrastructure being hacked every year (Public news)



2010
- Stuxnet

20122013
- Port of Antwerp hacked
- Saudi Aramco Data Loss
- “Target” hacked via building infrastructure

20142015
- Energetic Bear attacks
- German Steel Plant Incident
- Ukraine Power Distribution utility attack (BlackEnergy)

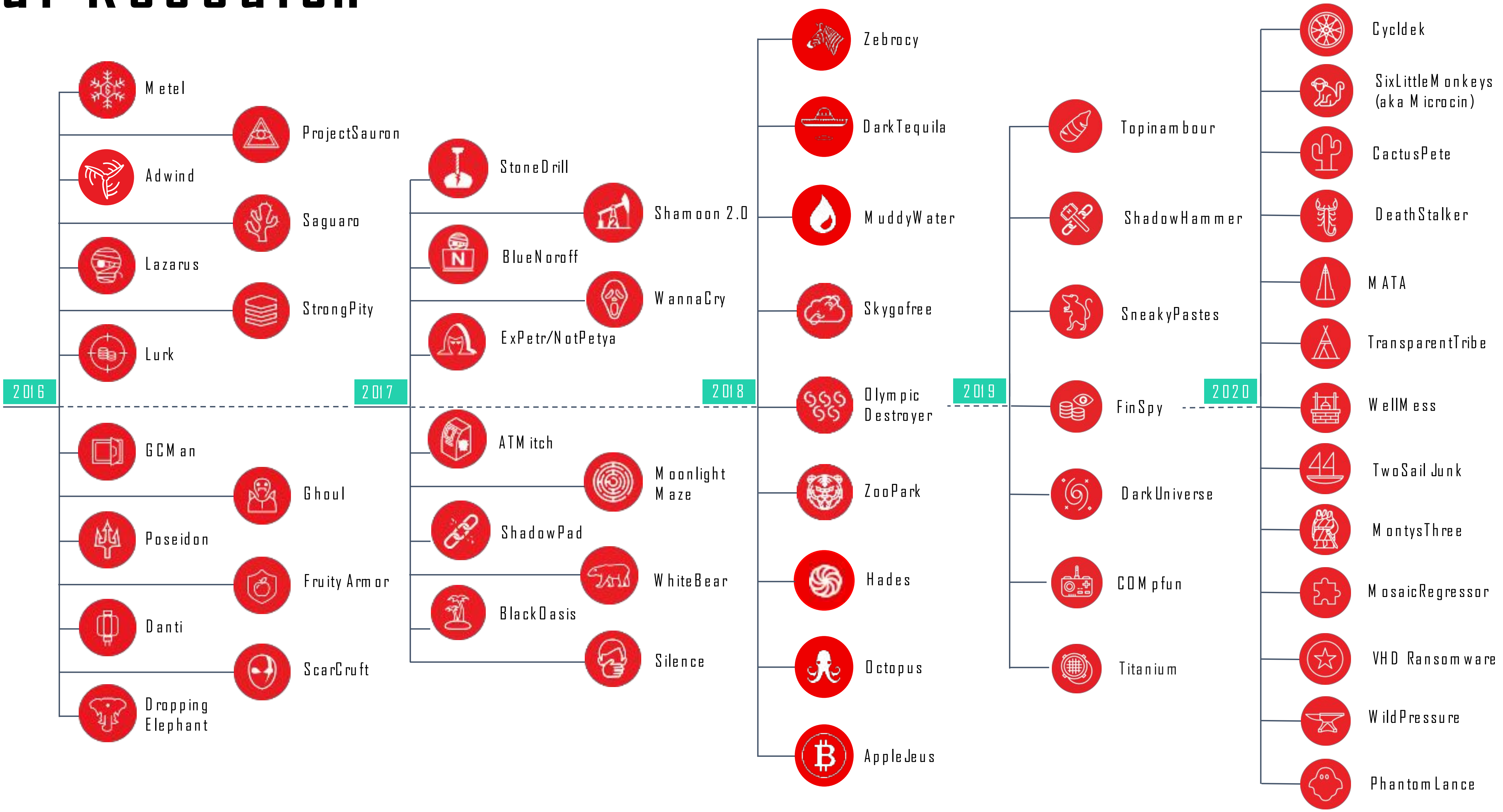
2016
- Lansing Board of Water & Light, Mi Ransomware
- Kiev power grid hacked
- Finland heating company DDoS
- Dallas road signs attacked
- San Francisco subway
- Gundremmingen nuclear plant

2017
- Wolf Creek nuclear plant
- Triton hit safety systems
- Energetic Bear
- WannaCry and ExPetr (Dozens of victims worldwide)

2018
- Boeing hit by WannaCry
- GreyEnergy APT
- Sapiem hit by Shamoon
- Leafminer APTs
- Tornado sirens (Texas, USA)
- Sharpshooter APT
- Fessenheim nuclear plant (France)

2019
- ACSO Industries ransomware
- Norsk Hydro attacked
- Moscow water treatment
- Noya plant (Japan)
- Water Metters attacked (USA)
- Venezuela blackout

Our Research



2016

Metel
ProjectSauron
Adwind
Saguaro
Lazarus
StrongPity
Lurk
GCMan
Ghoul
Poseidon
Fruity Armor
Danti
ScarCruft
Dropping Elephant

2017

StoneDrill
Shamoon 2.0
BlueNoroff
WannaCry
ExPetr/NotPetya
ATMitch
Moonlight Maze
ShadowPad
WhiteBear
BlackOasis
Silence

2018

Zebrocy
DarkTequila
MuddyWater
Skygofree
Olympic Destroyer
ZooPark
Hades
Octopus
AppleJeus

2019

Topinambour
ShadowHammer
SneakyPastes
FinSpy
DarkUniverse
COMpfun
Titanium

2020

Cycldek
SixLittleMonkeys (aka Microcin)
CactusPete
DeathStalker
MATA
TransparentTribe
WellMess
TwoSail Junk
MontysThree
MosaicRegressor
VHD Ransomware
WildPressure
PhantomLance

Black Energy

Ataques APT en Ucrania usando spearphishing con documentos de Word

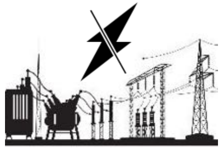
How it happens? – BlackEnergy example

Stage 1 - Intrusion

Phishing Emails
+
BlackEnergy Malware
↓
VPN & Credential Theft
Network & Host Discovery

Stage 2 – ICS Attack

Malicious Firmware Development
SCADA Hijack (HMI/Client)
↓
Breaker Open Commands
↓
UPS Modification
Firmware Upload
Killdisk Overwrites
↓
Power Outage



SANS ICS Industrial Control Systems

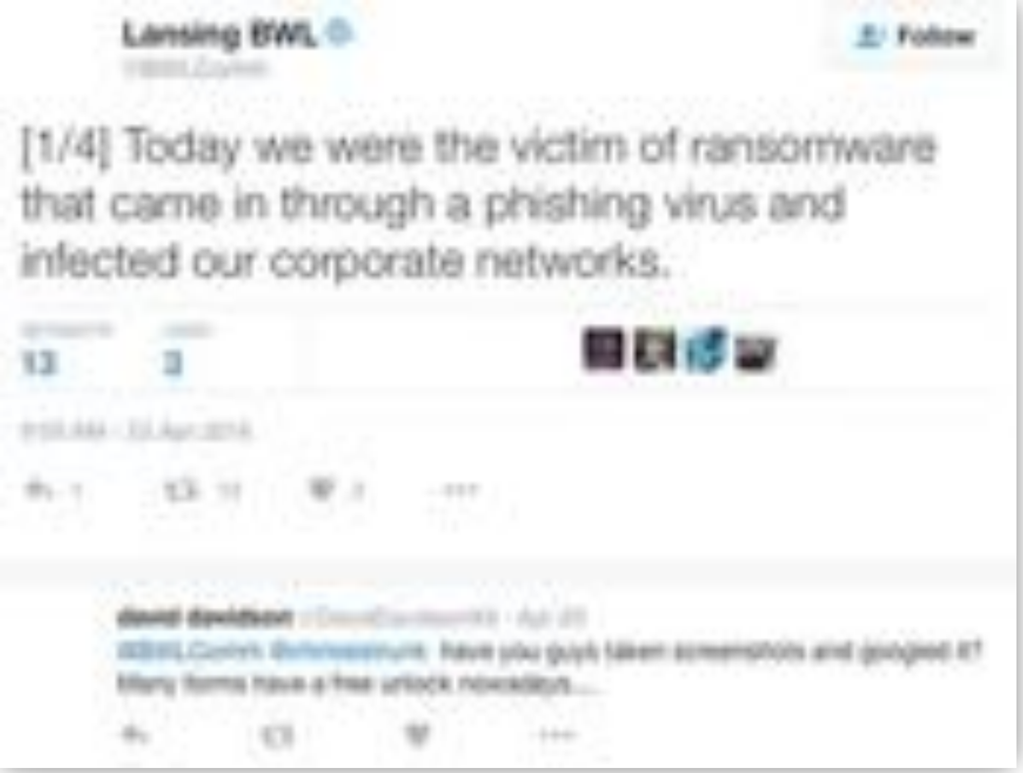
E-ISAC

Why it happens?

Large corporate infrastructures
Human factor
Supply chain attacks

OT is never isolated from IT
No visibility on OT communications
Vulnerable OT components

Lansing BWL, Michigan 2016



Lansing BWL
[illegible]

[1/4] Today we were the victim of ransomware that came in through a phishing virus and infected our corporate networks.

13 3

[illegible]

david davidson [illegible]
[illegible] have you guys taken screenshots and googled it? Many forms have a free unlock nowadays....

http://www.lansingstatejournal.com/story/news/local/2017/03/08/11-months-later-insurance-still-reviewing-bwl-cyber-attack/98847680/

City-owned utility

Phishing attack

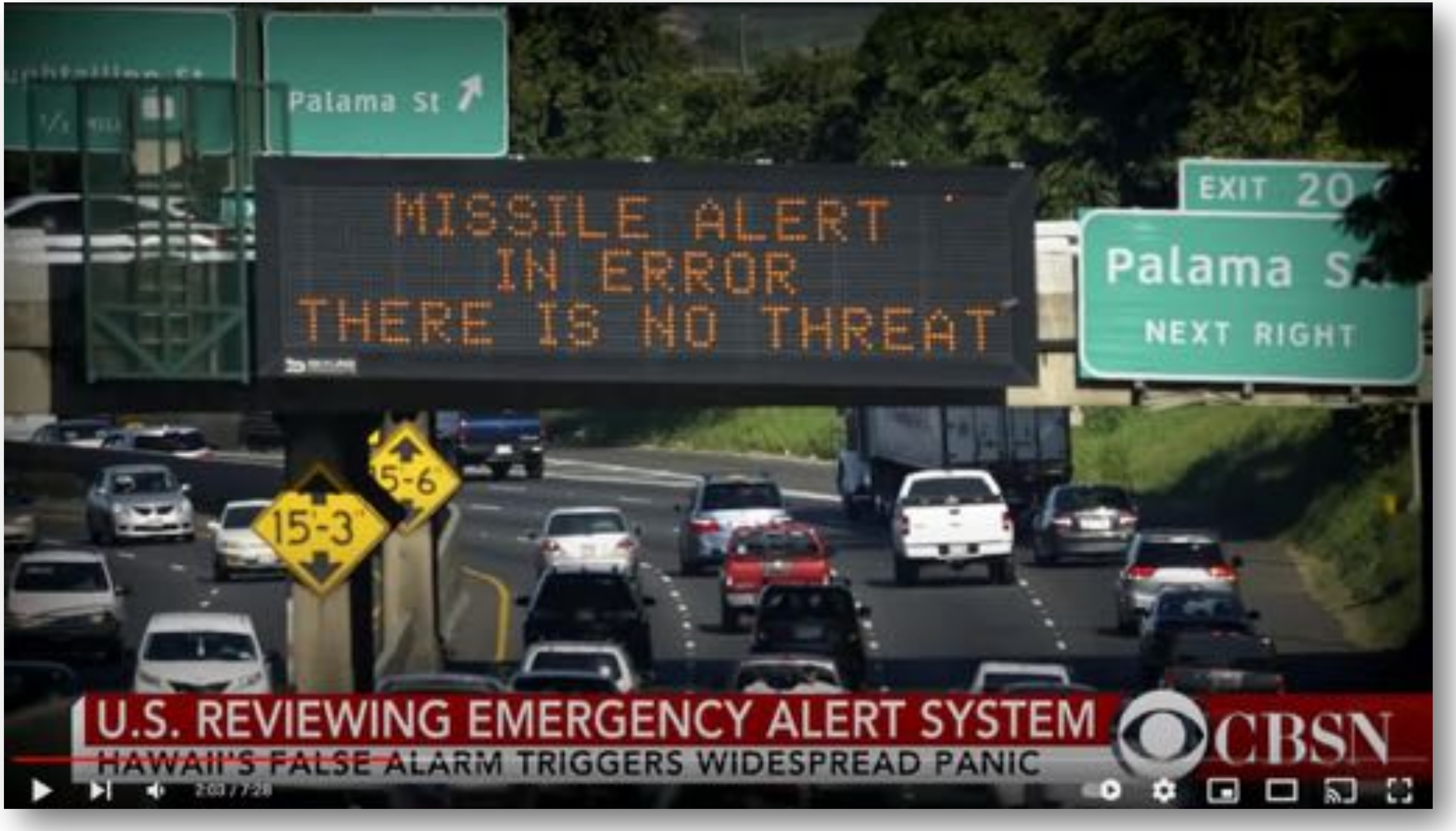
Cryptor ransomware

$25000 ransom

$2.4M cost / $1.9M insurance claim

It took the insurance > 11 months to review the BWL cyber attack

Falsa alarma de misiles balísticos obliga a Hawái a entrar en pánico



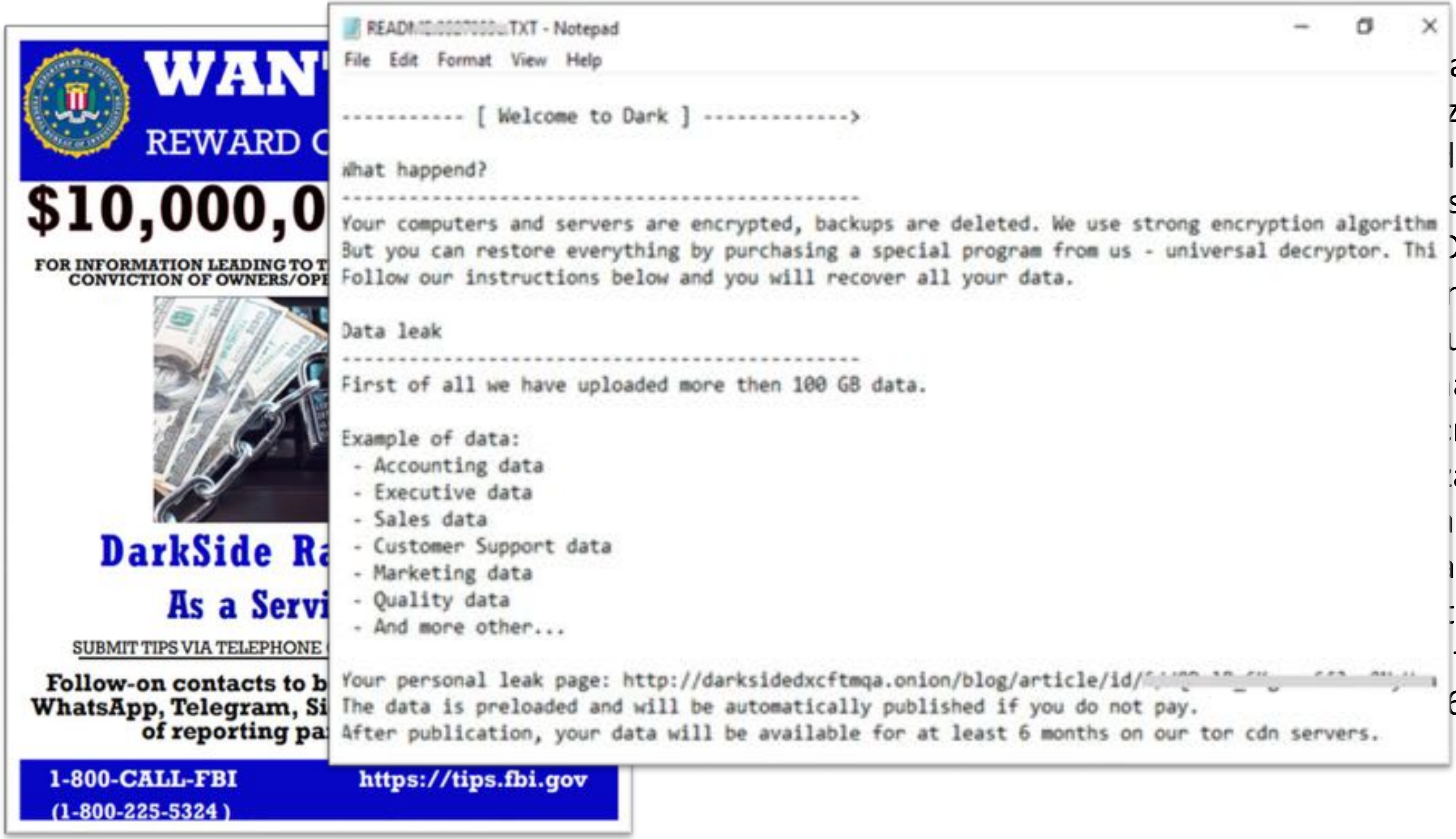
U.S. REVIEWING EMERGENCY ALERT SYSTEM

HAWAII'S FALSE ALARM TRIGGERS WIDESPREAD PANIC

Attacks-as-a-Service, Malware-as-a-Service and Fraud-as-a-Service

kaspersky

DarkSide Ransomware as a Service (RaaS)



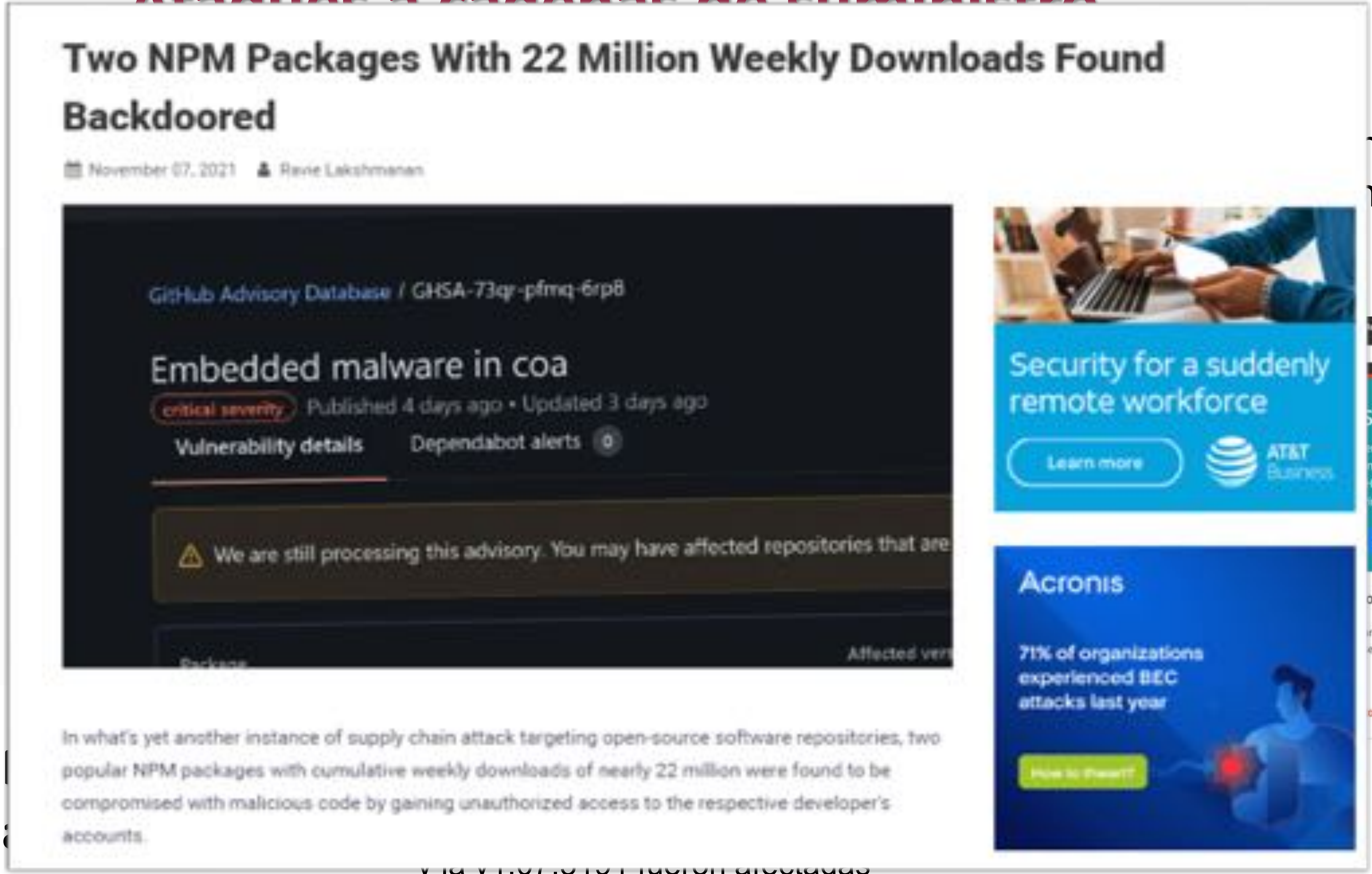
```
----------- [ Welcome to Dark ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithm
But you can restore everything by purchasing a special program from us - universal decryptor. Thi
Follow our instructions below and you will recover all your data.

Data leak
----------------------------------------------
First of all we have uploaded more then 100 GB data.

Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...

Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/[redacted]
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
```

a-Service (RaaS)
zados (de habla rusa)
lo varios anuncios en la
s para que participen
Darkside RaaS. Esta es,
nsomware moderna
utilizar el servicio
ar a empresas de todo
riptográfico, los
an ayudar a los
normalidad durante el
rgo, también advierten
ográfico, dejarán el
todos los datos
6 meses.

Ataques a cadenas de suministro

n

ndes



Two NPM Packages With 22 Million Weekly Downloads Found Backdoored

November 07, 2021 Ravie Lakshmanan

GitHub Advisory Database / GHSA-73qr-pfmq-6rp8

Embedded malware in coa

critical severity Published 4 days ago • Updated 3 days ago

Vulnerability details Dependabot alerts 0

⚠ We are still processing this advisory. You may have affected repositories that are

Package Affected ver

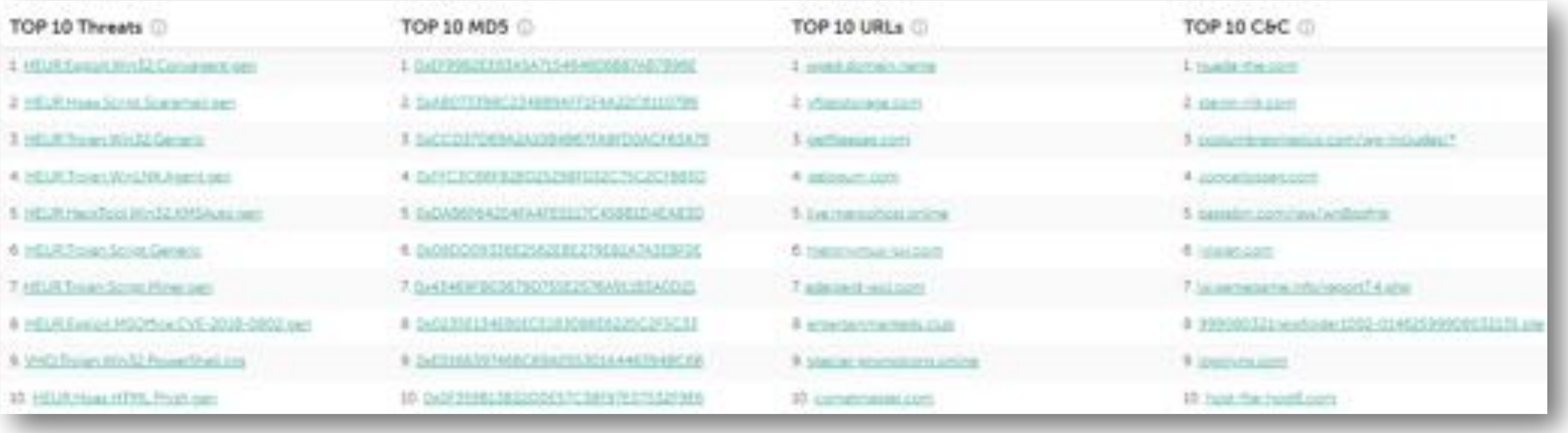
In what's yet another instance of supply chain attack targeting open-source software repositories, two popular NPM packages with cumulative weekly downloads of nearly 22 million were found to be compromised with malicious code by gaining unauthorized access to the respective developer's accounts.

Security for a suddenly remote workforce
Learn more
AT&T Business

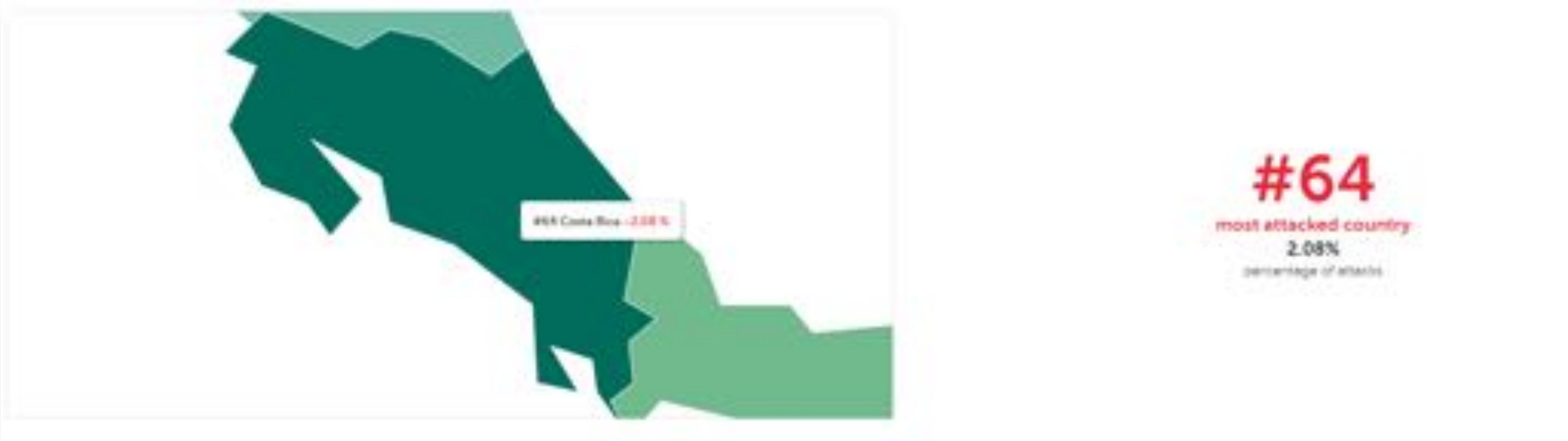
Acronis
71% of organizations experienced BEC attacks last year
How to thwart?

Reseller Login 한국어
Go
Solution
ensive set of
mple
H terminal
inter server.
Download
oftware
nd
ervice at secure
ore »

y la v1.07.0191 fueron afectadas

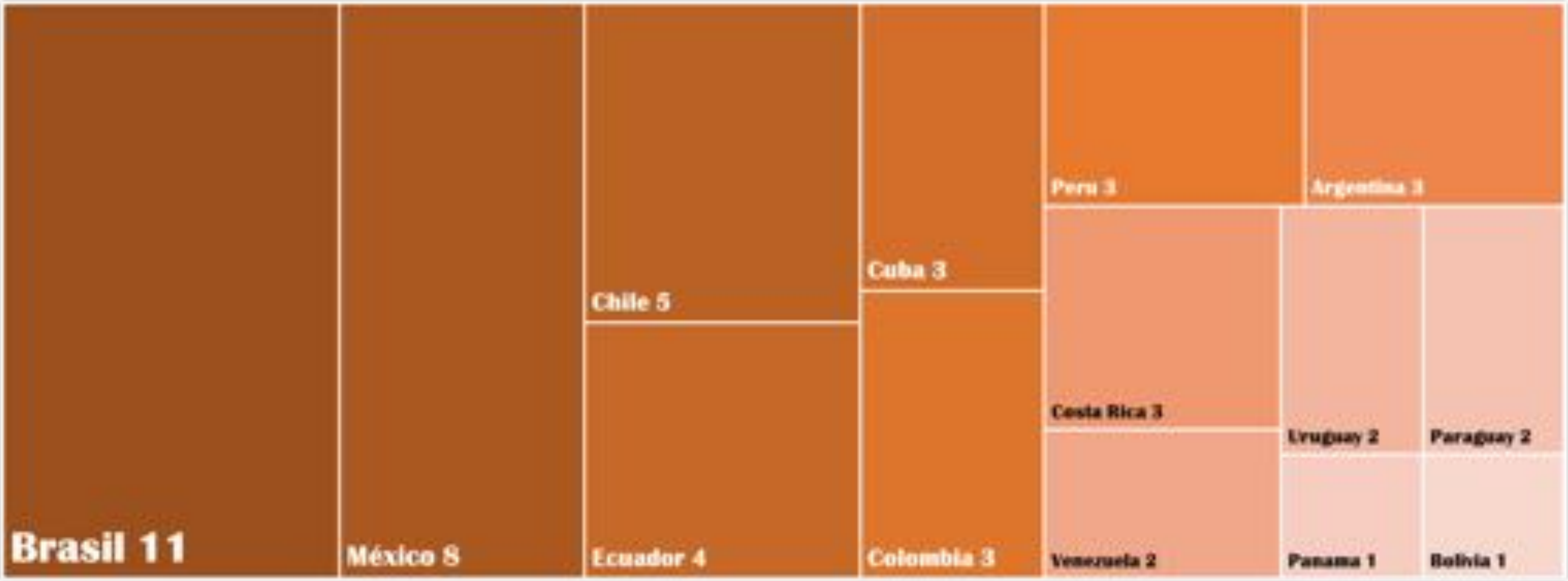


TOP 10 Threats	TOP 10 MD5	TOP 10 URLs	TOP 10 C&C
1. HEUR:Exploit.Win32.Convagent.gen	1. 0x0F3962E153A5A71546480D6887A57B96E	1. sweet.domain.name	1. husella-the.com
2. HEUR:Hoax.Script.Scareware.gen	2. 0xA8077E9B8C23488BAFF1F4A22C81107B6	2. vfilesstorage.com	2. sterm-nik.com
3. HEUR:Trojan.Win32.Generic	3. 0xCCD37D6BA2A39B4967AB9D0AC463A75	3. getfilesapp.com	3. costumbreshistorias.com/wp-includes/*
4. HEUR:Trojan.WinLNK.Agent.gen	4. 0xF4C3C6BFB2BD252987032C75C2CFB85D	4. aabsum.com	4. poncelonsan.com
5. HEUR:HackTool.Win32.KMSAuto.gen	5. 0xDA0606A2D4FA4FE0117C45881D4EAE3D	5. live.mansohost.online	5. passalon.com/new/wrdbothx
6. HEUR:Trojan.Script.Generic	6. 0x08DD0931EE25A2E8E2796B2A7A3E9F0E	6. memmymus-ssl.com	6. rdacon.com
7. HEUR:Trojan.Script.Miner.gen	7. 0x41469FBC067BD75E2576AB1B5A0D21	7. adelaid-ssl.com	7. lacarnetarme.info/report?4.php
8. HEUR:Exploit.MSOffice.CVE-2018-0802.gen	8. 0x0235813468B01C5183086E6220C2F5C31	8. entertainmentads.club	8. 99900032.1newfolder1002-0146259990603215.php
9. VHO:Trojan.Win32.PowerShell.gen	9. 0xE3168397468C8B6A0553014467848C66	9. telesiae-promotions.online	9. ipservice.com
10. HEUR:Hoax.HTML.Phish.gen	10. 0xF35981382D0DE57C3819787C7552F3E6	10. cometmaster.com	10. host-the-host8.com



#64
most attacked country
2.08%
percentage of attacks

Países y Actores



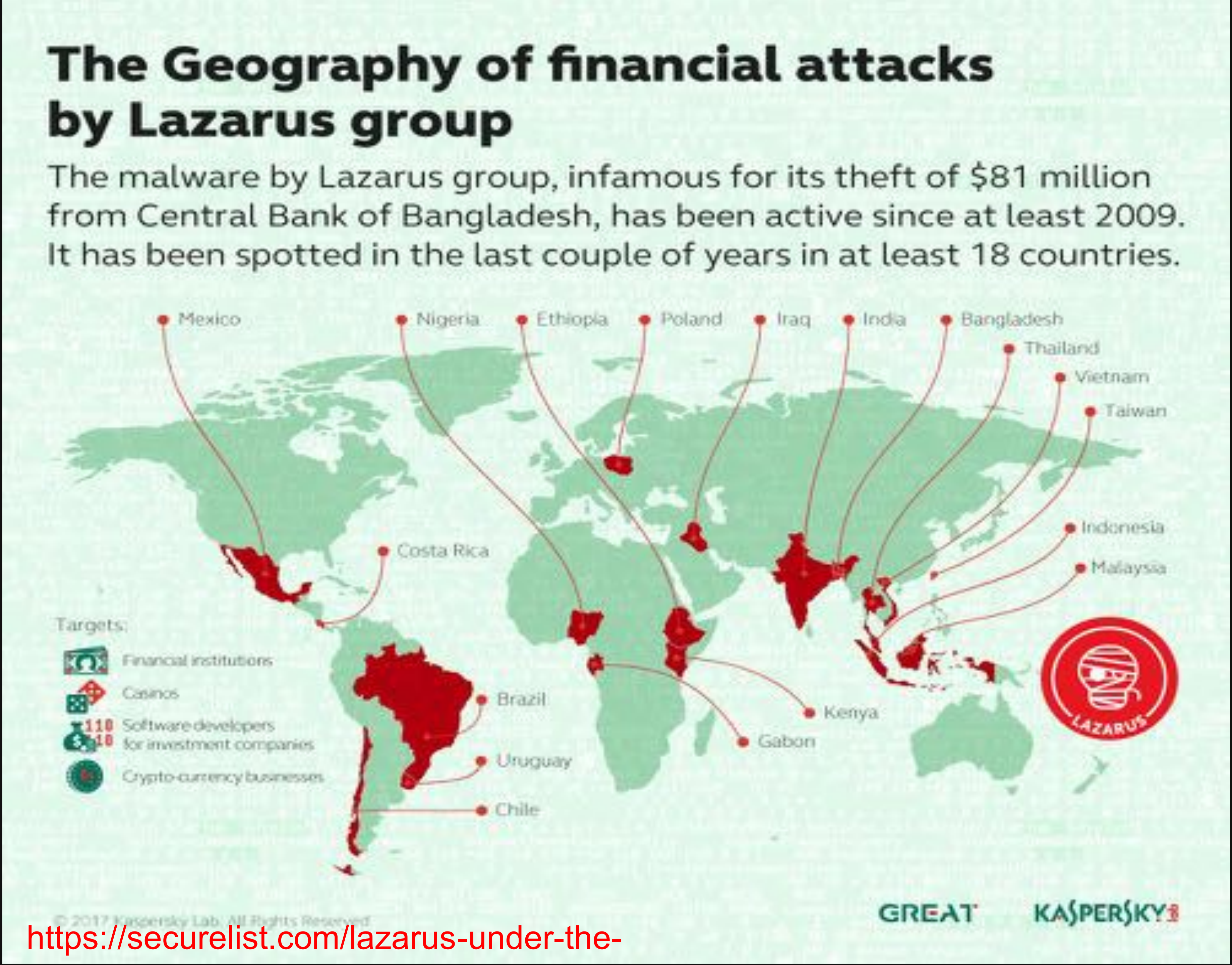
LAZARUS GROUP

Lo conocemos desde 2015

Publicado en Abril de 2020

Watering Hole:

- México
- Costa Rica
- Uruguay
- Rusia
- Norway
- India
- Nigeria
- Perú
- Polonia



The Geography of financial attacks by Lazarus group

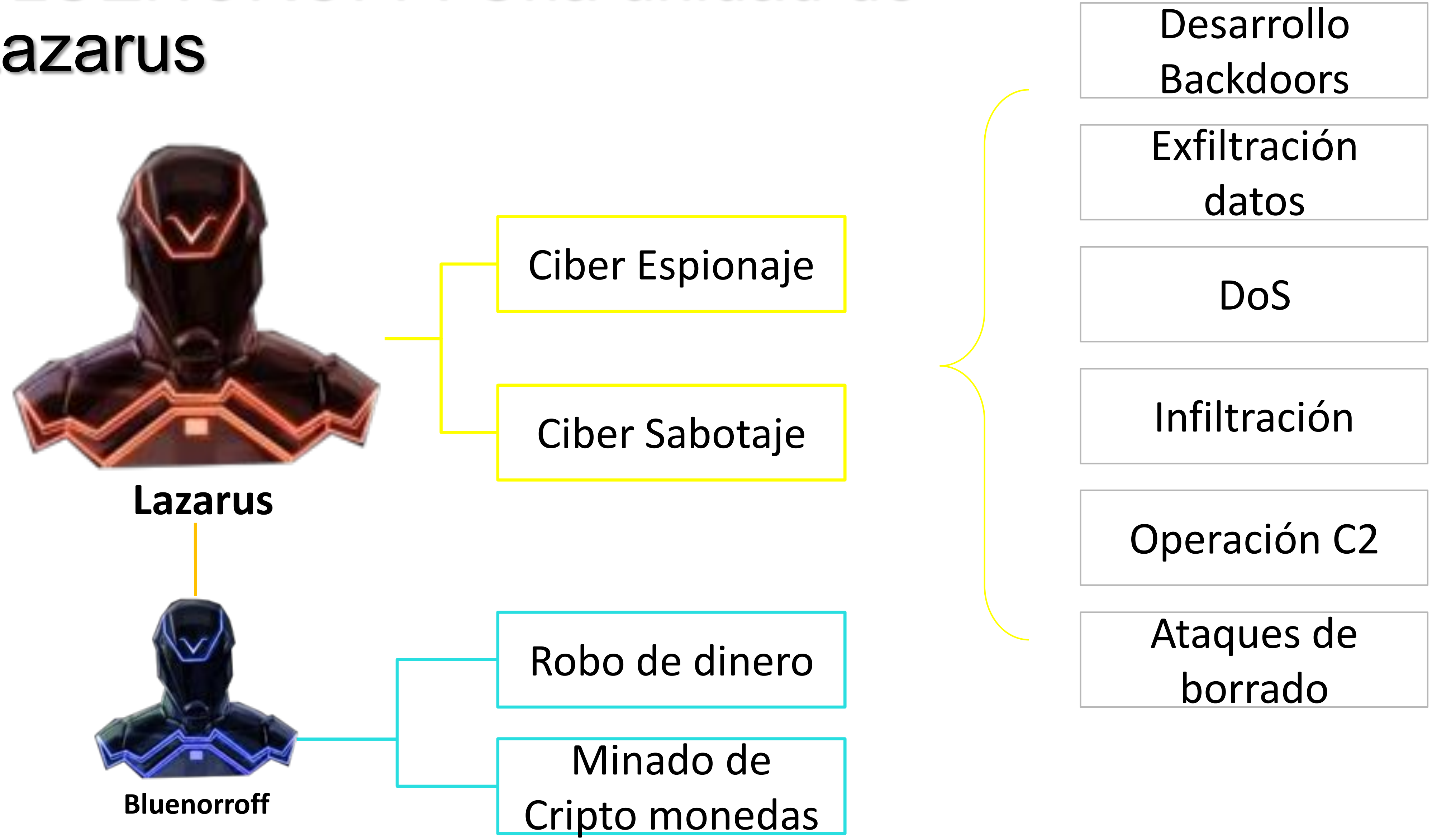
The malware by Lazarus group, infamous for its theft of $81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.

https://securelist.com/lazarus-under-the-

LAZARUS: ataques al sistema Swift

En 2015 11,000 instituciones financieras estaban conectadas al SWIFT, en más de 200 países y territorios, que cambiarán 15 millones de mensajes por día

BLUENOROFF: Una unidad de Lazarus



Lazarus

Ciber Espionaje

Ciber Sabotaje

Desarrollo Backdoors

Exfiltración datos

DoS

Infiltración

Operación C2

Ataques de borrado

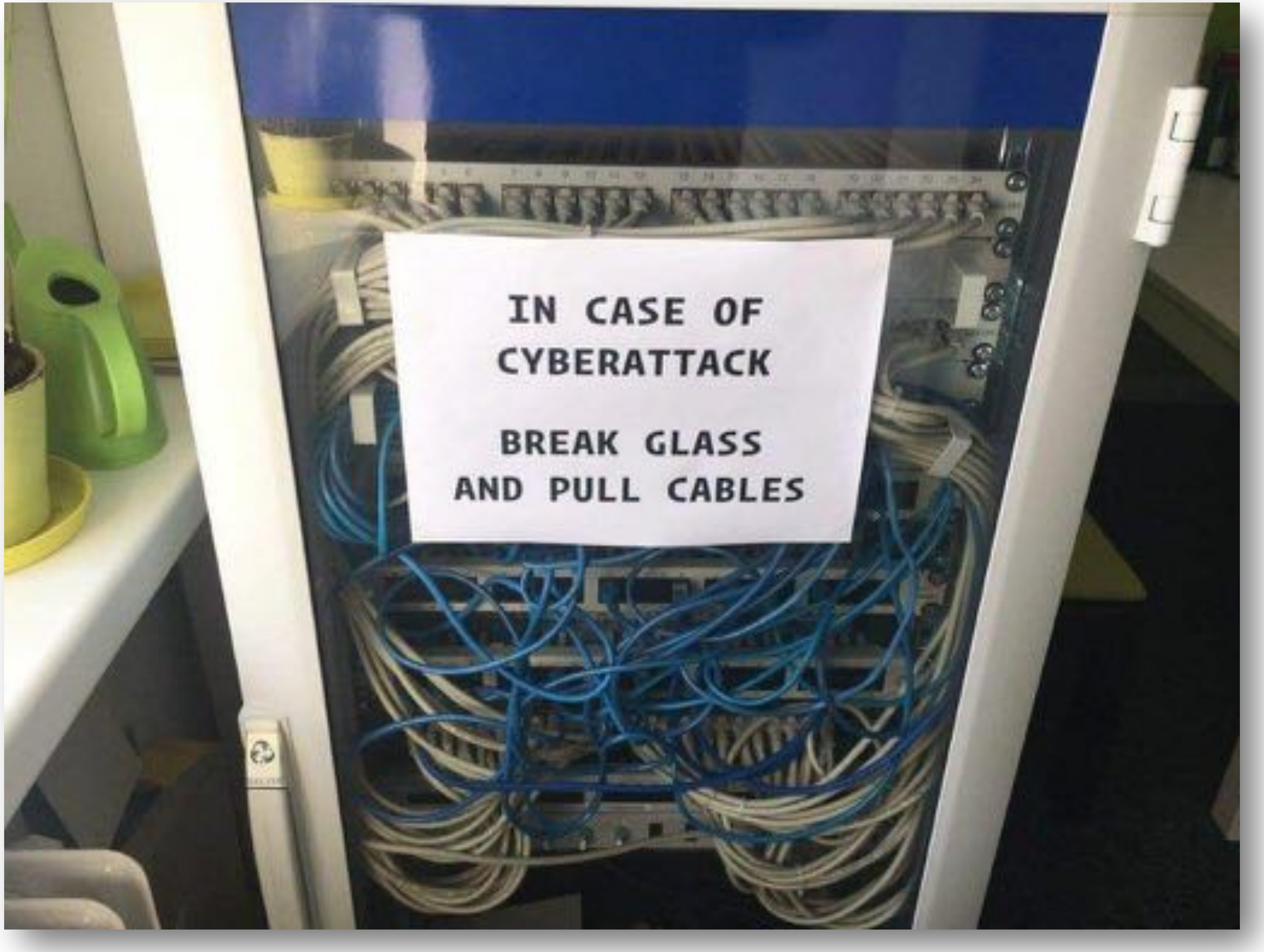
Bluenorroff

Robo de dinero

Minado de Cripto monedas

Bianchi

“Respuesta a Incidentes”



Cybersecurity Strategy:

PROACTIVE
REACTIVE

Panorama de amenazas 2021 / 2022

- Una re-integración e internalización de las operaciones dentro del ecosistema de la ciberdelincuencia.
- El ransomware dirigido se ha convertido en una amenaza relevante para el sector financiero.
- Los grupos ransomware usan exploits de día 0 para comprometer las organizaciones y ya no solo mediante correo electrónico.
- Incremento de los Attackers as a Services

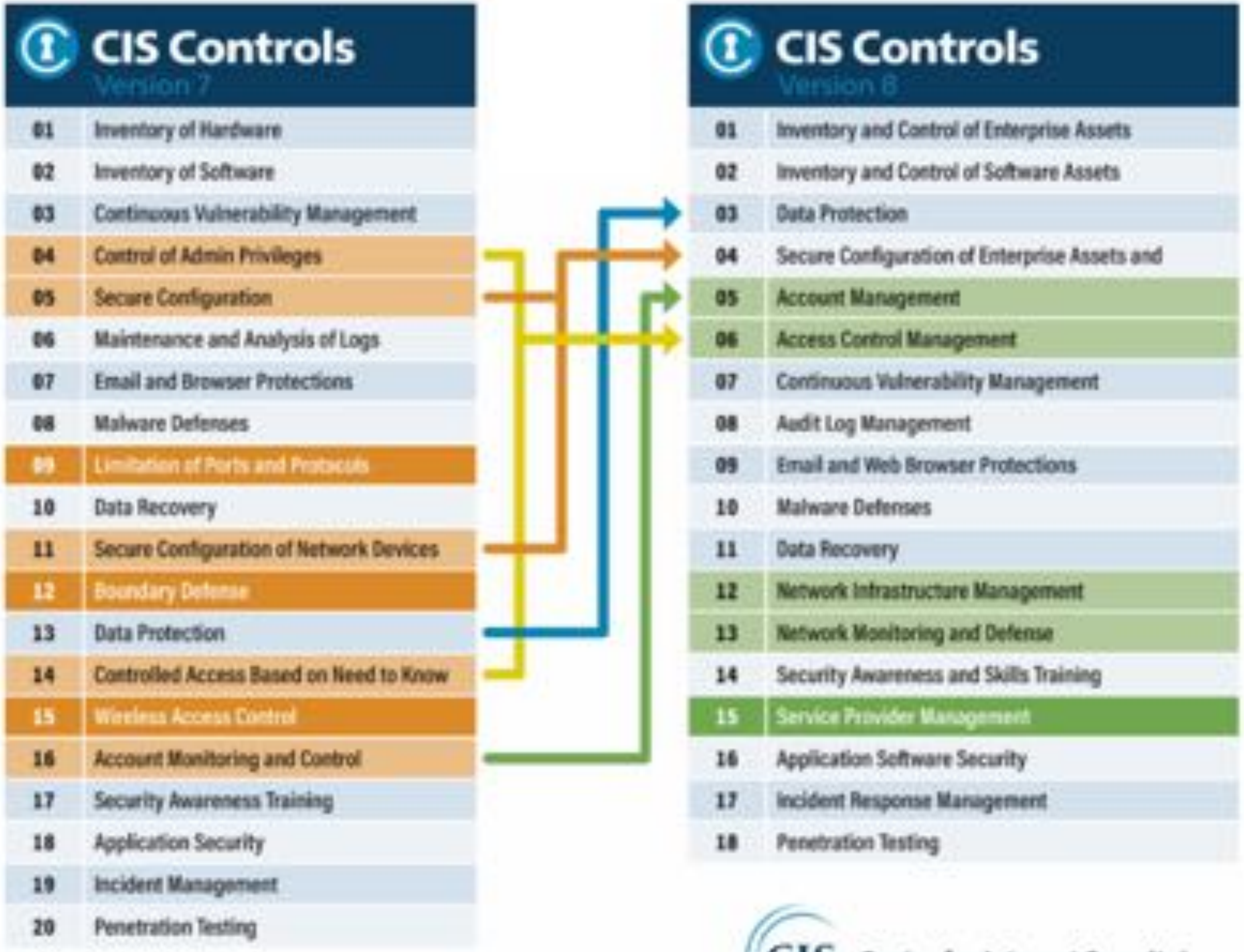
Panorama de amenazas 2021 / 2022

Expansión de los actores de amenazas brasileños al resto del mundo (España, Latinoamérica, África y Portugal).

Guildma, Javali, Melcoz, Grandoreiro ("la Tétrade“) Amavaldo, Lampion y Bizarro.

Ataques a puntos de venta PoS y ATMs.

Prilex se convirtió en Malware as a Service (MaaS). El ecosistema alrededor de Prilex integra grupo de hackers maliciosos que atacan ATMs, PoS, servicios DDoS, software para clonar tarjetas de pago y otros.



CIS Controls
Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

“Fundamentalmente, si alguien quiere comprometer su red o dispositivo, seguramente lo va a hacer…… asumámoslo

Debemos entender que estamos en medio de una batalla, lo queramos o no y seguramente su red ya fue comprometida de alguna manera”

Michael Hyden

Ex-director CIA, NSA

Microsoft Enterprise Cloud Teaming Whitepaper

Preguntas?

Dwayne Porr Lesli

@dporrles

ITSN Networks

kaspersky

Gerson Castro Valverde
Director de Negocios Corporativos

gcastro@itsnetworks.net
Tel: (506) 8842-5568