Sophos Day Oporto

14 Marzo 2019

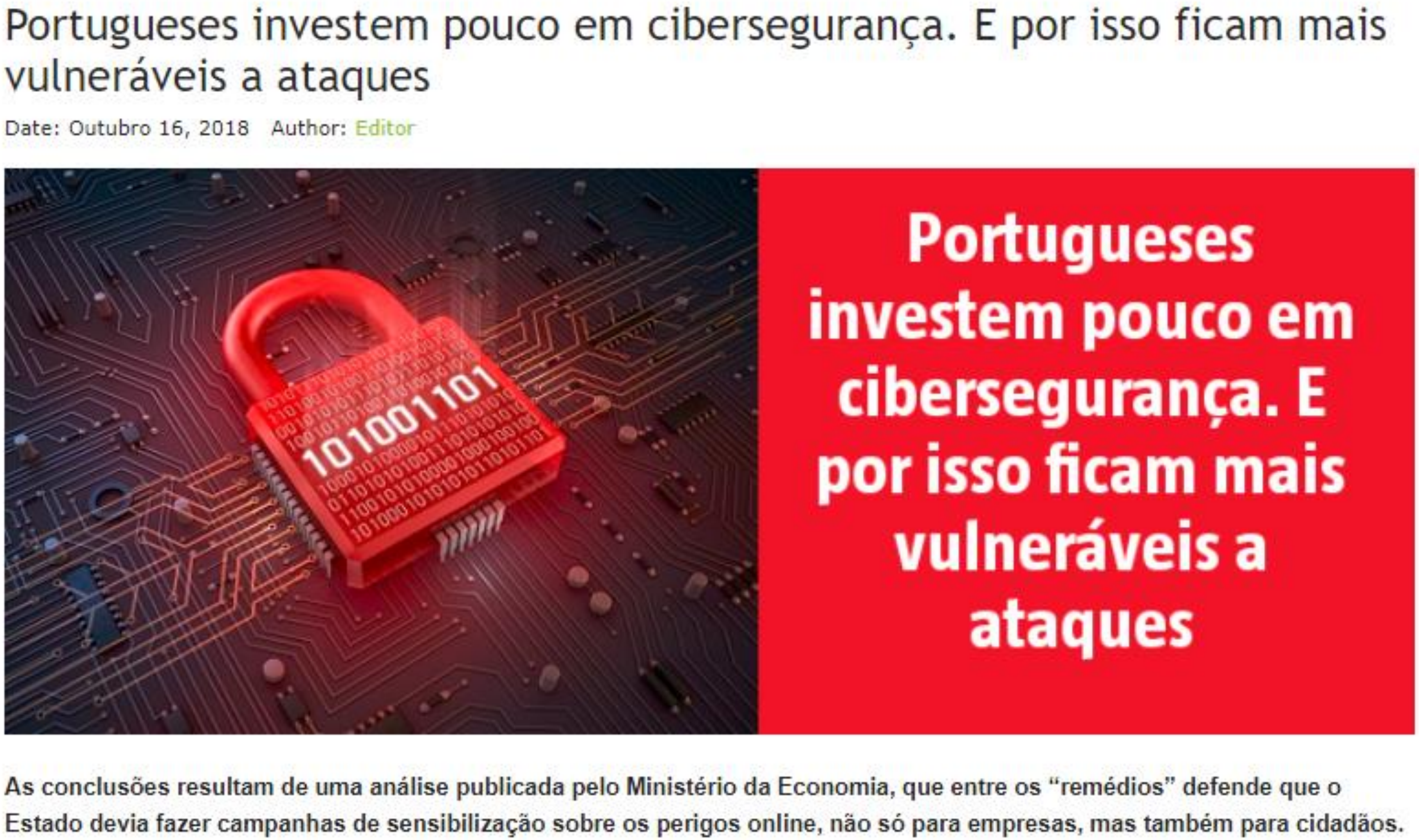
Ricardo Maté

Country Manager Iberia

@ricardomatesal

SEE THE FUTURE

SOPHOS DISCOVER



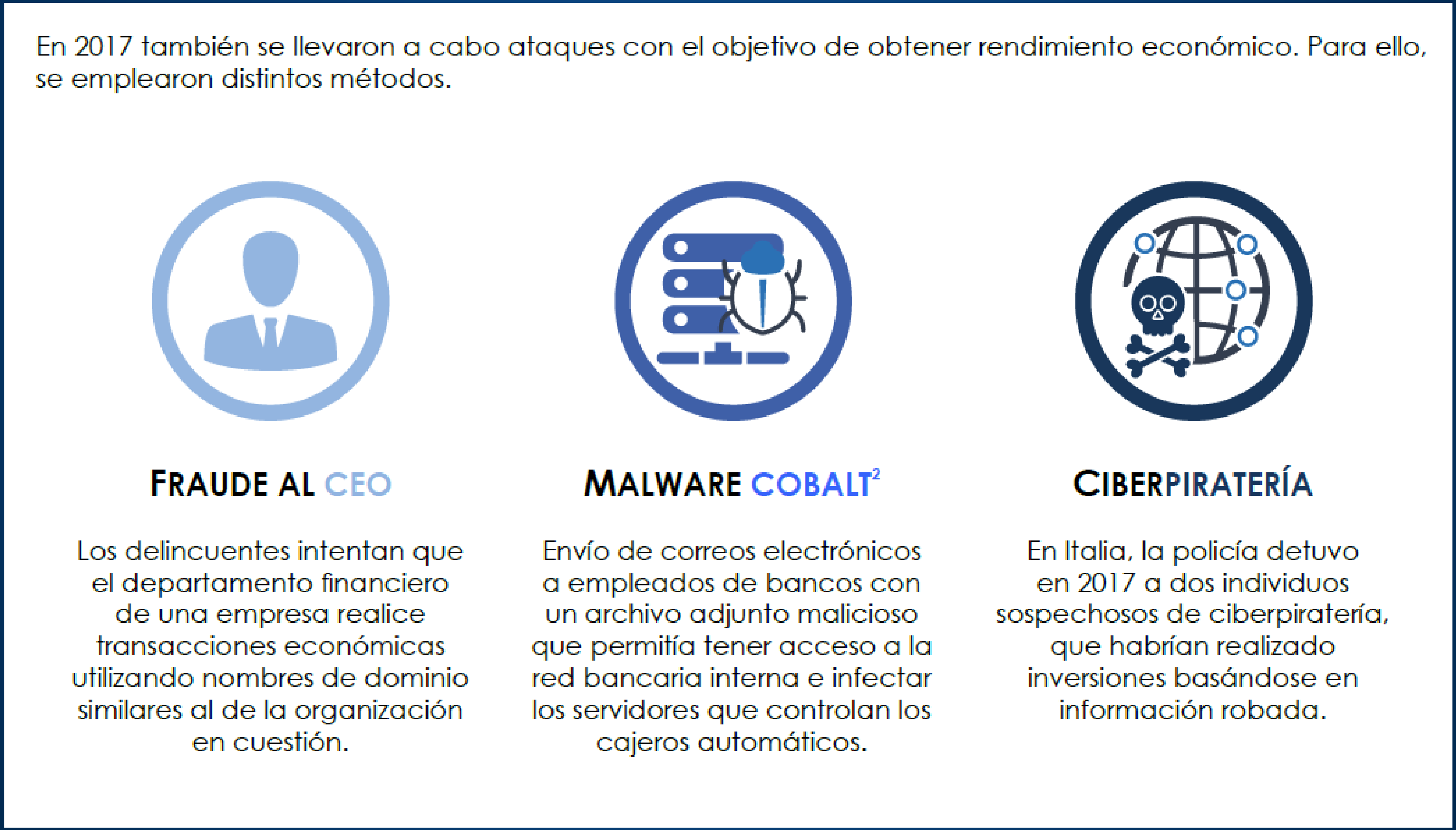
Portugueses investem pouco em cibersegurança. E por isso ficam mais vulneráveis a ataques

Date: Outubro 16, 2018 Author: Editor

Portugueses investem pouco em cibersegurança. E por isso ficam mais vulneráveis a ataques
101001101

As conclusões resultam de uma análise publicada pelo Ministério da Economia, que entre os “remédios” defende que o Estado devia fazer campanhas de sensibilização sobre os perigos online, não só para empresas, mas também para cidadãos.

CCN-CERT: Ciberamenazas y tendencias 2018
Centro Nacional de Cibersegurança (CCNS)



En 2017 también se llevaron a cabo ataques con el objetivo de obtener rendimiento económico. Para ello, se emplearon distintos métodos.

FRAUDE AL CEO

Los delincuentes intentan que el departamento financiero de una empresa realice transacciones económicas utilizando nombres de dominio similares al de la organización en cuestión.

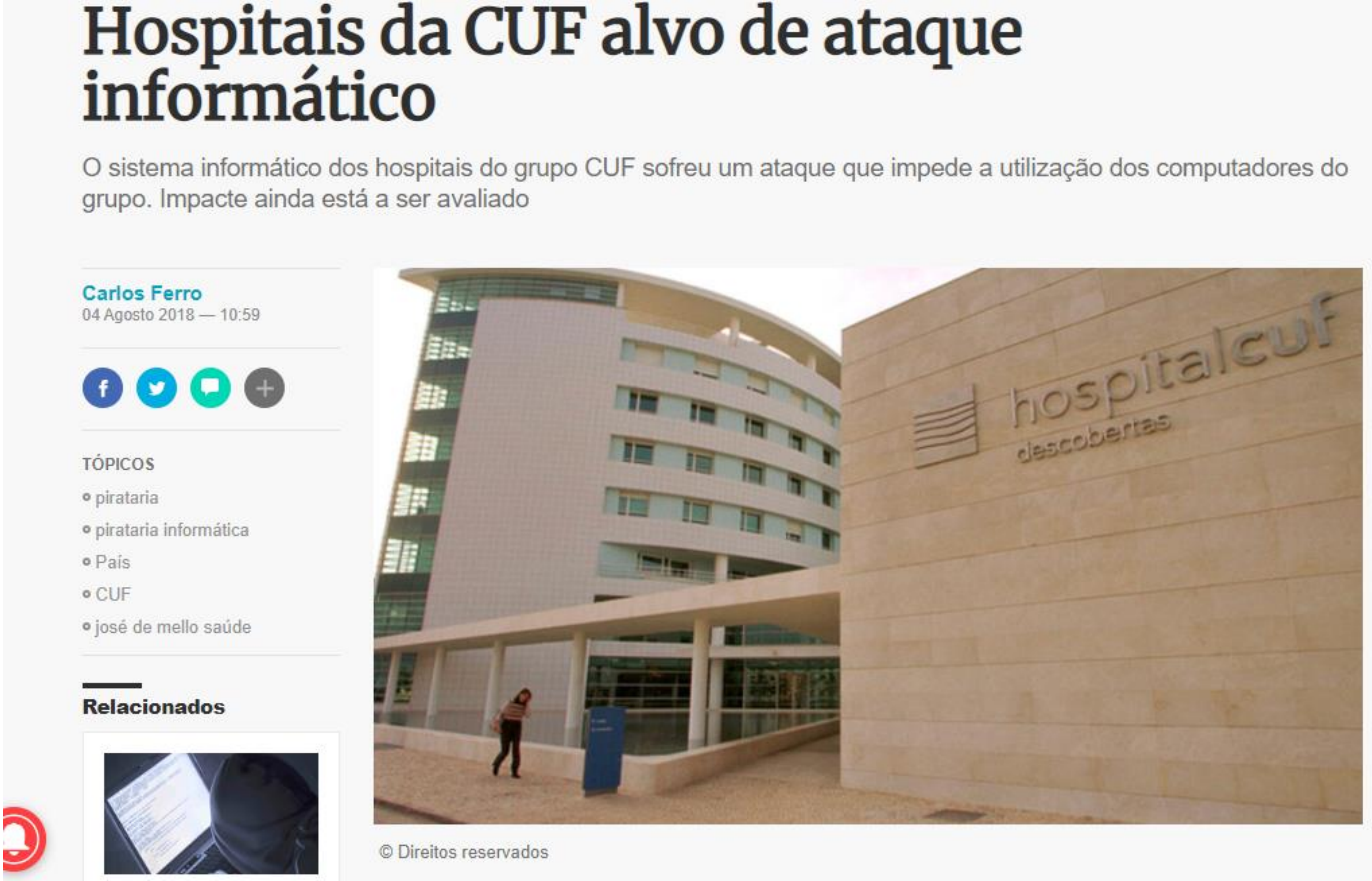
MALWARE COBALT[2]

Envío de correos electrónicos a empleados de bancos con un archivo adjunto malicioso que permitía tener acceso a la red bancaria interna e infectar los servidores que controlan los cajeros automáticos.

CIBERPIRATERÍA

En Italia, la policía detuvo en 2017 a dos individuos sospechosos de ciberpiratería, que habrían realizado inversiones basándose en información robada.

Drone strikes, not carpet bombing



Hospitais da CUF alvo de ataque informático

O sistema informático dos hospitais do grupo CUF sofreu um ataque que impede a utilização dos computadores do grupo. Impacte ainda está a ser avaliado

Carlos Ferro
04 Agosto 2018 — 10:59

TÓPICOS

- pirataria
- pirataria informática
- País
- CUF
- josé de mello saúde

Relacionados

© Direitos reservados

7 UNCOMFORTABLE TRUTHS OF ENDPOINT SECURITY

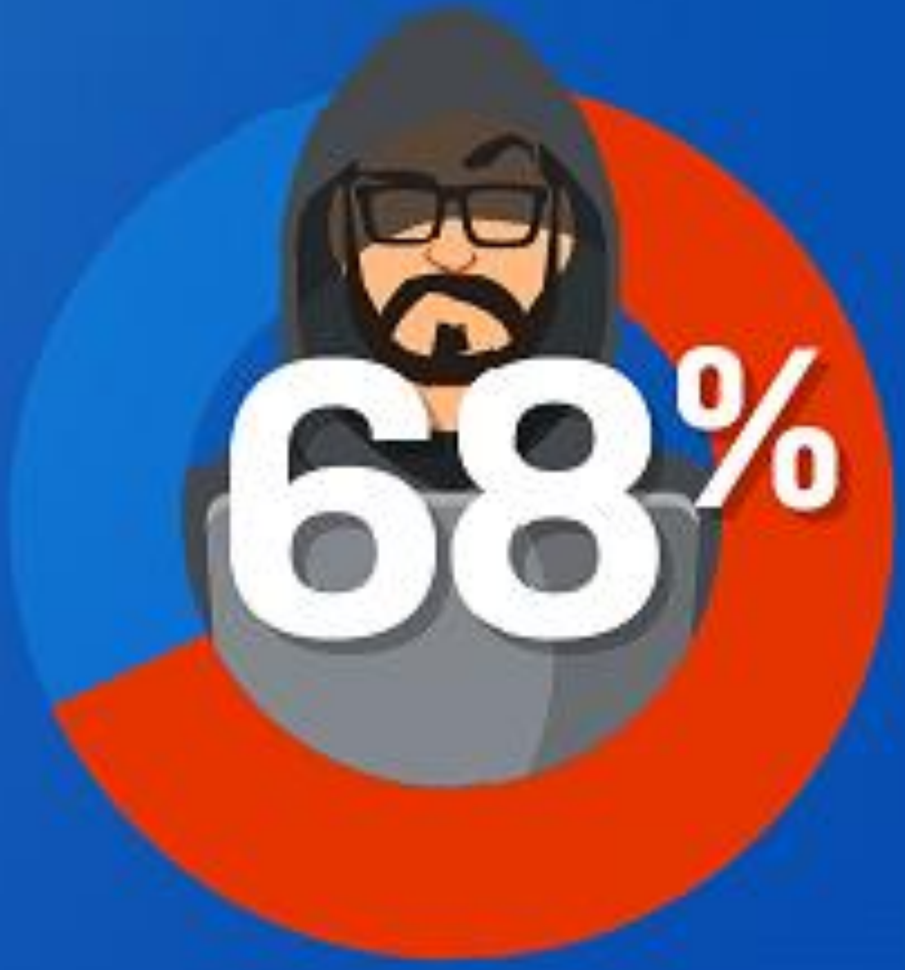
Results of an independent survey of 3,100 IT managers commissioned by Sophos

TRUTH #1

IT IS NOW THE NORM TO BE A CYBERATTACK VICTIM

68% of organizations say they were hit by a cyberattack in the last year, twice on average.

TAKEAWAY: **Assume you will be hit by a cyberattack when planning your security strategies.**



TRUTH #2

IT TEAMS LACK VISIBILITY INTO ATTACKER DWELL TIME

Organizations don't know how long nearly one in five threats (17%) was in their environment before being discovered. As a result, they don't know the damage caused.

TAKEAWAY: Worry about the threats you can track. Worry more about those you can't.

TRUTH #3

IT TEAMS CAN'T PLUG THEIR SECURITY GAPS BECAUSE THEY DON'T KNOW WHAT THEY ARE

One in five IT managers are unaware how their most significant cyberattack entered their organizations. As a result, they are unable to protect these entry points.

TAKEAWAY: To improve your long-term security, it's essential to understand your weaknesses.

TRUTH #4

ORGANIZATIONS LOSE 41 DAYS EACH YEAR INVESTIGATING NON-ISSUES

Organizations spend, on average, 48 days a year investigating potential security incidents, yet only 15% turn out to be actual infections.

TAKEAWAY: Endpoint detection and response (EDR) technologies that identify, prioritize, and analyze security incidents save you time while improving security.

TRUTH #5

ORGANIZATIONS STRUGGLE TO DETECT AND RESPOND TO THREATS DUE TO LACK OF SECURITY EXPERTISE

Four in five IT managers wish they had a stronger team in place to properly detect, investigate, and respond to security incidents. Yet 79% struggle to recruit the cybersecurity skills they need.

TAKEAWAY: Focus on technologies that enable you to add expertise without adding headcount.

TRUTH #6

MORE THAN HALF OF ORGANIZATIONS DON'T SEE THE VALUE OF THEIR EDR SOLUTIONS

While 93% of IT managers want EDR in their security arsenal, 54% of organizations that have invested in EDR can't get full value from it.

TAKEAWAY: Ensure you choose an EDR solution that you can use based on your current skills and resources.

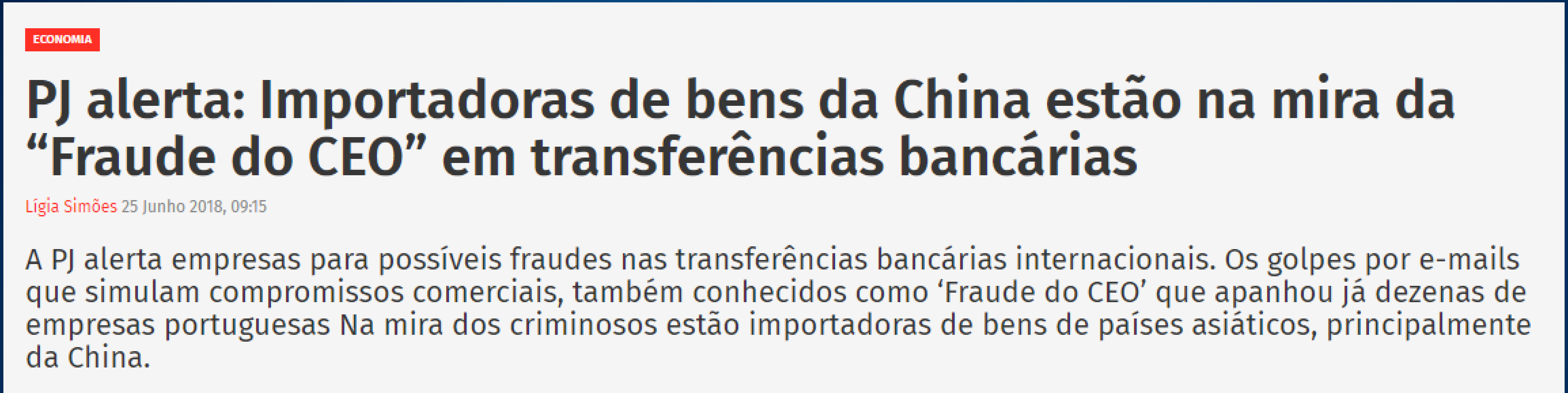
TRUTH #7

ONCE BITTEN, TWICE SHY – CYBER VICTIMS LEARN THE HARD WAY

Organizations that fell victim to a cyberattack in the last year investigate twice as many incidents as other organizations and spend 1/3 more time investigating potential security incidents.

TAKEAWAY: **Act now. Ensure your endpoint security strategy is up to date to minimize the risk of being hit.**

Social Engineering – "Timo del CEO"

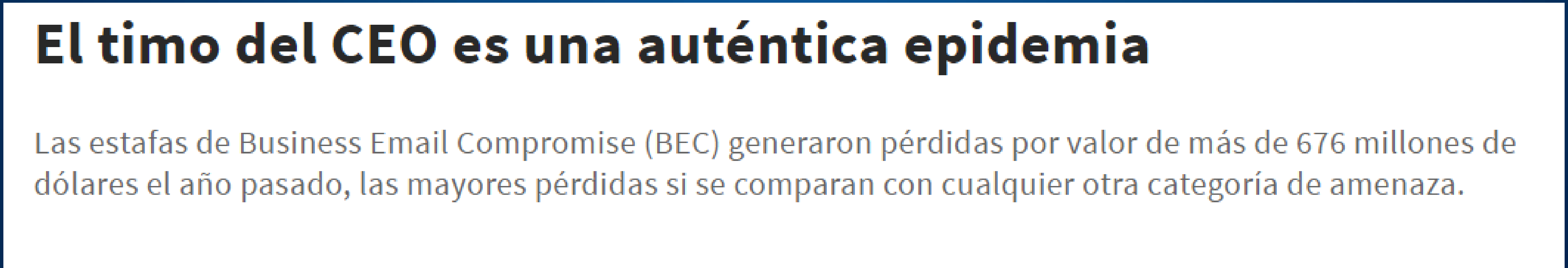


ECONOMIA

PJ alerta: Importadoras de bens da China estão na mira da "Fraude do CEO" em transferências bancárias

Lígia Simões 25 Junho 2018, 09:15

A PJ alerta empresas para possíveis fraudes nas transferências bancárias internacionais. Os golpes por e-mails que simulam compromissos comerciais, também conhecidos como 'Fraude do CEO' que apanhou já dezenas de empresas portuguesas Na mira dos criminosos estão importadoras de bens de países asiáticos, principalmente da China.



El timo del CEO es una auténtica epidemia

Las estafas de Business Email Compromise (BEC) generaron pérdidas por valor de más de 676 millones de dólares el año pasado, las mayores pérdidas si se comparan con cualquier otra categoría de amenaza.

SOPHOS

El **93%** das quebras de Segurança vem de um ataque de Phishing

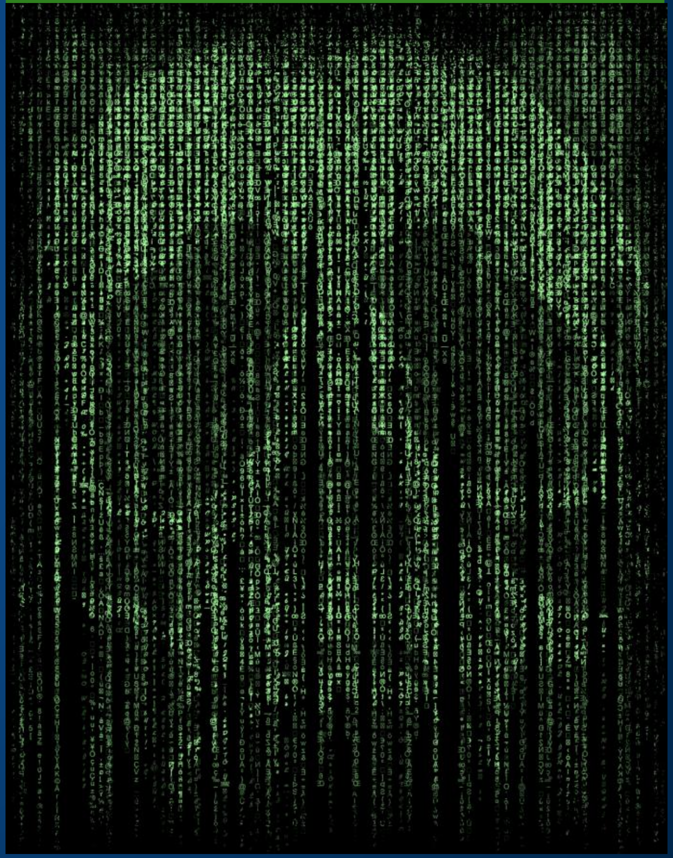
Inside Matrix And Emotet:

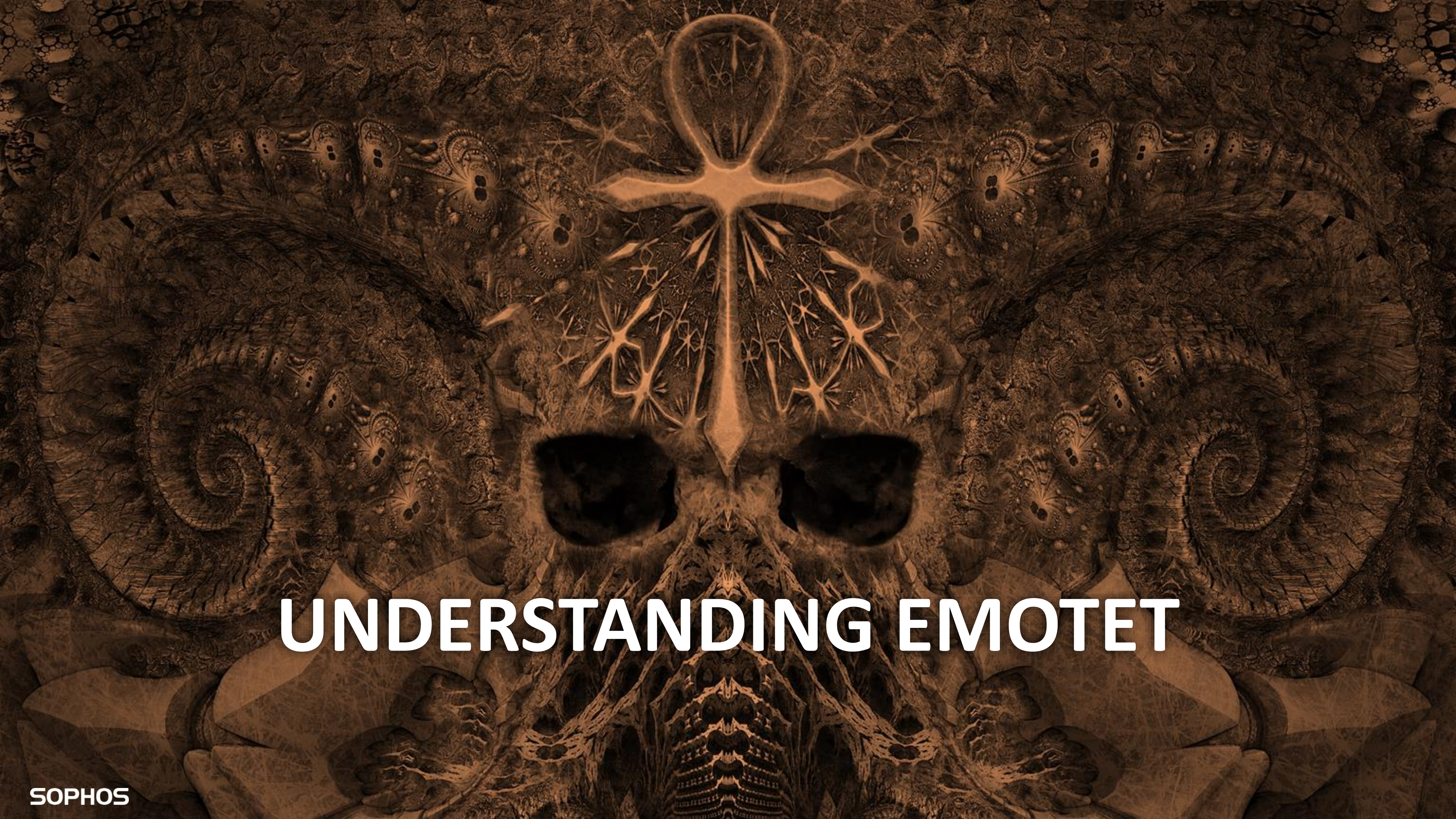
How they work and how to defend

Two Recent Examples

EMOTET

MATRIX





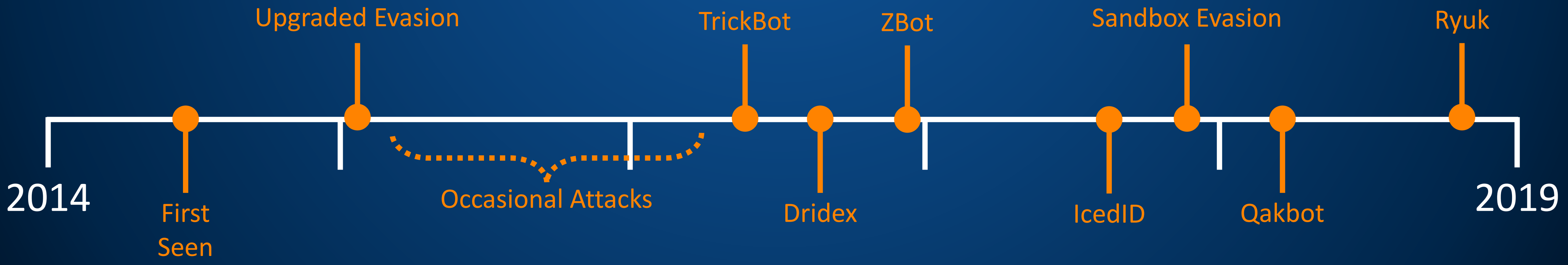
UNDERSTANDING EMOTET

EMOTET

> "Amongst the most costly and destructive threats to U.S. businesses right now"
>
> *U.S. Department for Homeland Security, 2018*

Trojan that silently steals victims' banking credentials

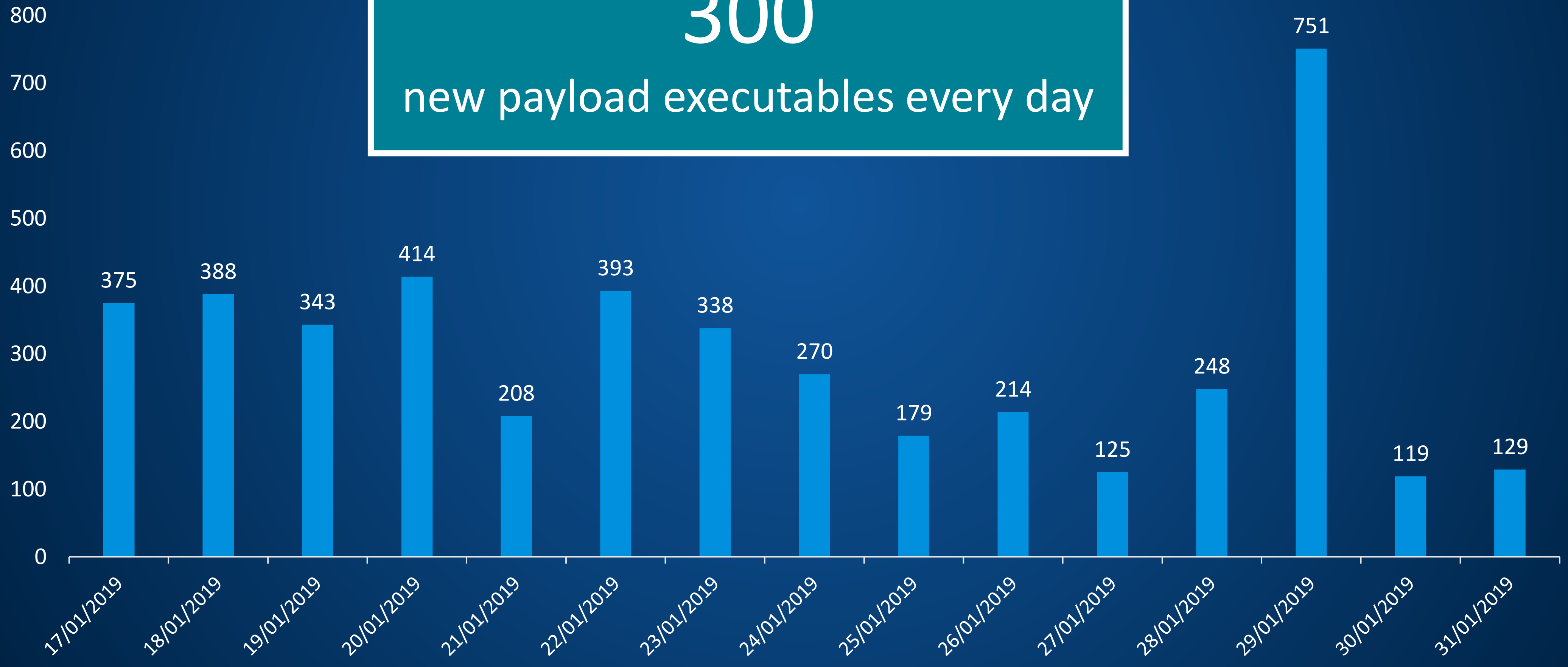
Highly sophisticated network worm with global reach that distributes other malware, mostly banking Trojans



Emotet payloads change **constantly**

300

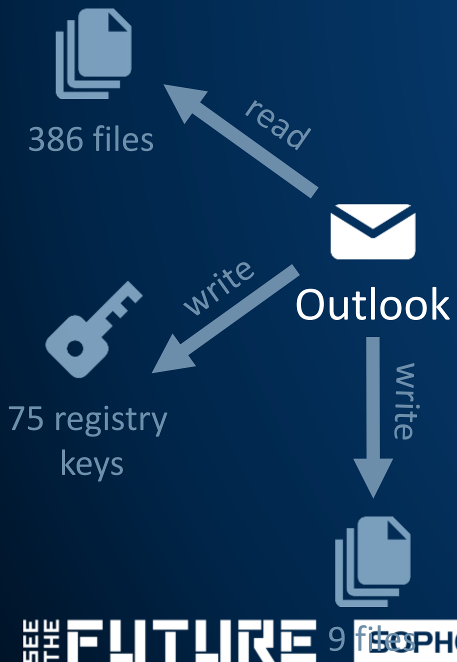
new payload executables every day

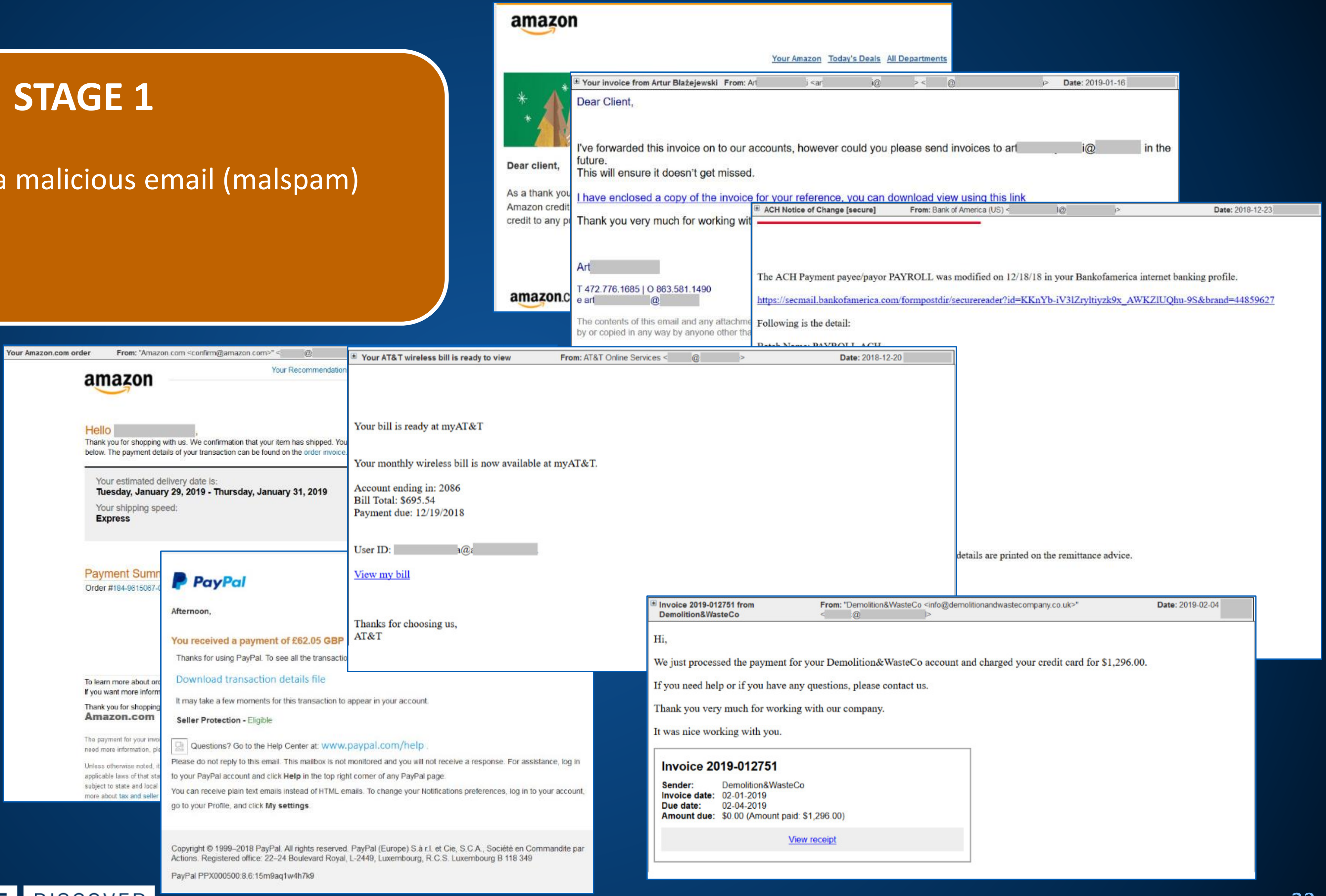


# of unique Emotet payload executables seen by SophosLabs

STAGE 1

User received a malicious email (malspam)





amazon

Your Amazon Today's Deals All Departments

Dear client,

As a thank you
Amazon credit
credit to any p

amazon.c

Your invoice from Artur Błażejewski **From:** Art[redacted]i <ar[redacted]i@[redacted]> <[redacted]@[redacted]> **Date:** 2019-01-16 [redacted]

Dear Client,

I've forwarded this invoice on to our accounts, however could you please send invoices to art[redacted]i@[redacted] in the future.
This will ensure it doesn't get missed.

I have enclosed a copy of the invoice for your reference, you can download view using this link

Thank you very much for working wit

Art[redacted]

T 472.776.1685 | O 863.581.1490
e art[redacted]@[redacted]

The contents of this email and any attachme
by or copied in any way by anyone other tha

ACH Notice of Change [secure] **From:** Bank of America (US) <[redacted]l@[redacted]> **Date:** 2018-12-23 [redacted]

The ACH Payment payee/payor PAYROLL was modified on 12/18/18 in your Bankofamerica internet banking profile.

https://secmail.bankofamerica.com/formpostdir/securereader?id=KKnYb-iV3lZryltiyzk9x_AWKZlUQhu-9S&brand=44859627

Following is the detail:

details are printed on the remittance advice.

Your Amazon.com order **From:** "Amazon.com <confirm@amazon.com>" <[redacted]@[redacted]

amazon

Your Recommendation

Hello [redacted],
Thank you for shopping with us. We confirmation that your item has shipped. You
below. The payment details of your transaction can be found on the order invoice.

Your estimated delivery date is:
Tuesday, January 29, 2019 - Thursday, January 31, 2019
Your shipping speed:
Express

Payment Summ
Order #184-9615067-

To learn more about ord
If you want more inform

Thank you for shopping
Amazon.com

The payment for your invoi
need more information, ple

Unless otherwise noted, it
applicable laws of that sta
subject to state and local
more about tax and seller

Your AT&T wireless bill is ready to view **From:** AT&T Online Services <[redacted]@[redacted]> **Date:** 2018-12-20 [redacted]

Your bill is ready at myAT&T

Your monthly wireless bill is now available at myAT&T.

Account ending in: 2086
Bill Total: $695.54
Payment due: 12/19/2018

User ID: [redacted]a@a[redacted].

View my bill

Thanks for choosing us,
AT&T

PayPal

Afternoon,

You received a payment of £62.05 GBP

Thanks for using PayPal. To see all the transactio

Download transaction details file

It may take a few moments for this transaction to appear in your account.

Seller Protection - Eligible

Questions? Go to the Help Center at: www.paypal.com/help .

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click **Help** in the top right corner of any PayPal page.

You can receive plain text emails instead of HTML emails. To change your Notifications preferences, log in to your account, go to your Profile, and click **My settings**.

Copyright © 1999–2018 PayPal. All rights reserved. PayPal (Europe) S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Registered office: 22–24 Boulevard Royal, L-2449, Luxembourg, R.C.S. Luxembourg B 118 349

PayPal PPX000500:8.6:15m9aq1w4h7k9

Invoice 2019-012751 from Demolition&WasteCo **From:** "Demolition&WasteCo <info@demolitionandwastecompany.co.uk>" <[redacted]@[redacted]> **Date:** 2019-02-04 [redacted]

Hi,

We just processed the payment for your Demolition&WasteCo account and charged your credit card for $1,296.00.

If you need help or if you have any questions, please contact us.

Thank you very much for working with our company.

It was nice working with you.

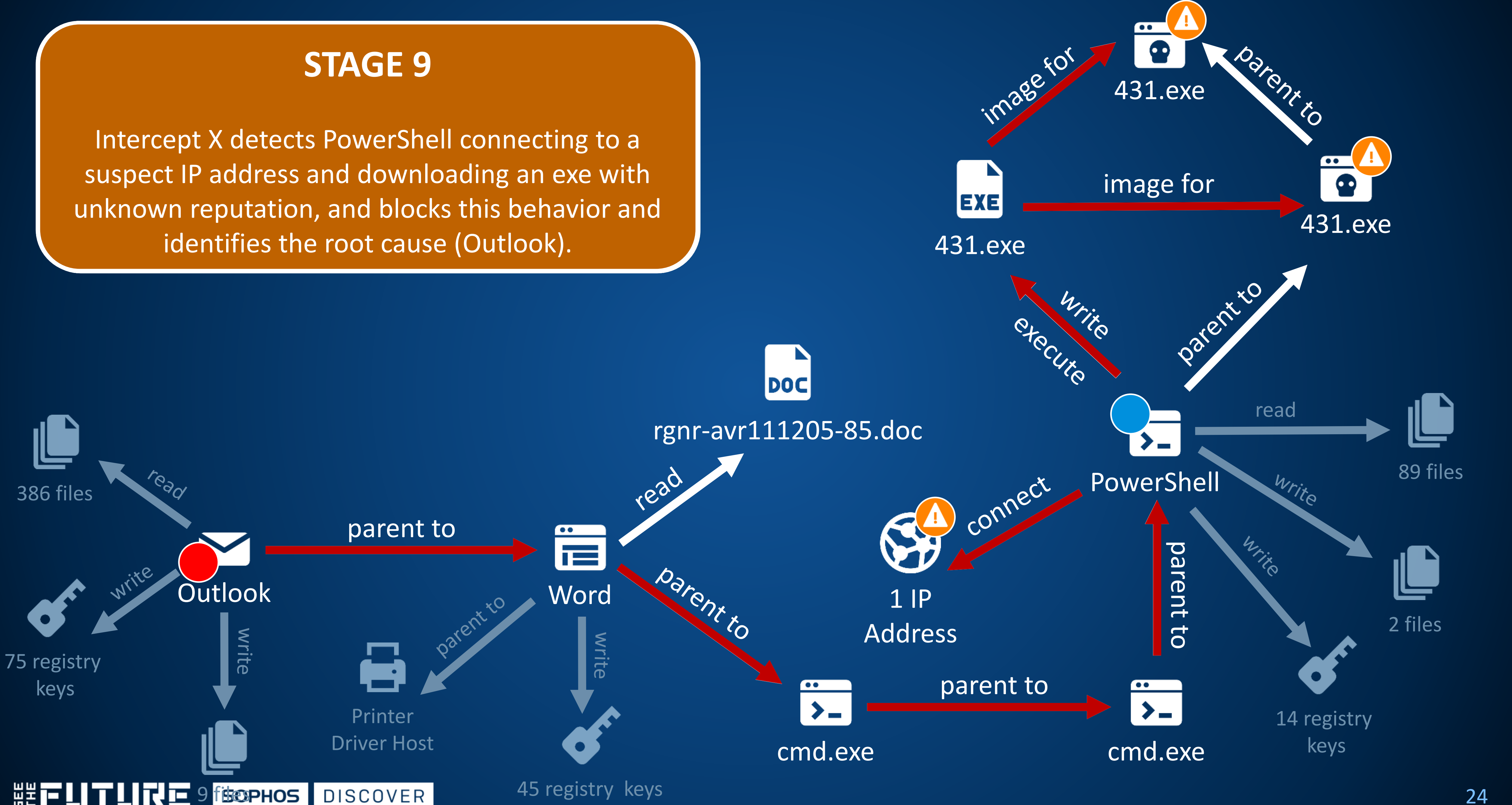
Invoice 2019-012751

Sender: Demolition&WasteCo
Invoice date: 02-01-2019
Due date: 02-04-2019
Amount due: $0.00 (Amount paid: $1,296.00)

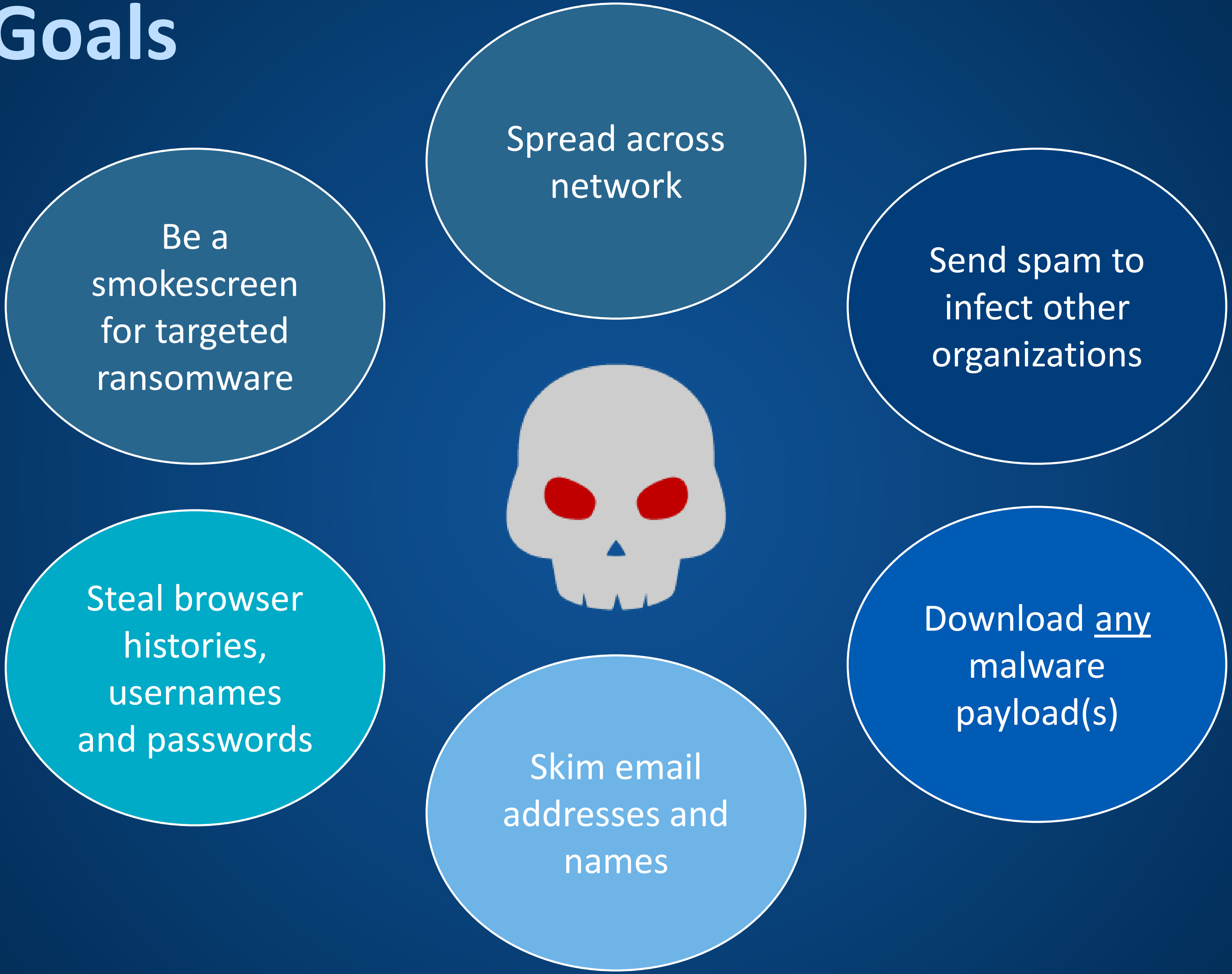
View receipt

STAGE 9

Intercept X detects PowerShell connecting to a suspect IP address and downloading an exe with unknown reputation, and blocks this behavior and identifies the root cause (Outlook).



Emotet's Goals



Spread across network

Be a smokescreen for targeted ransomware

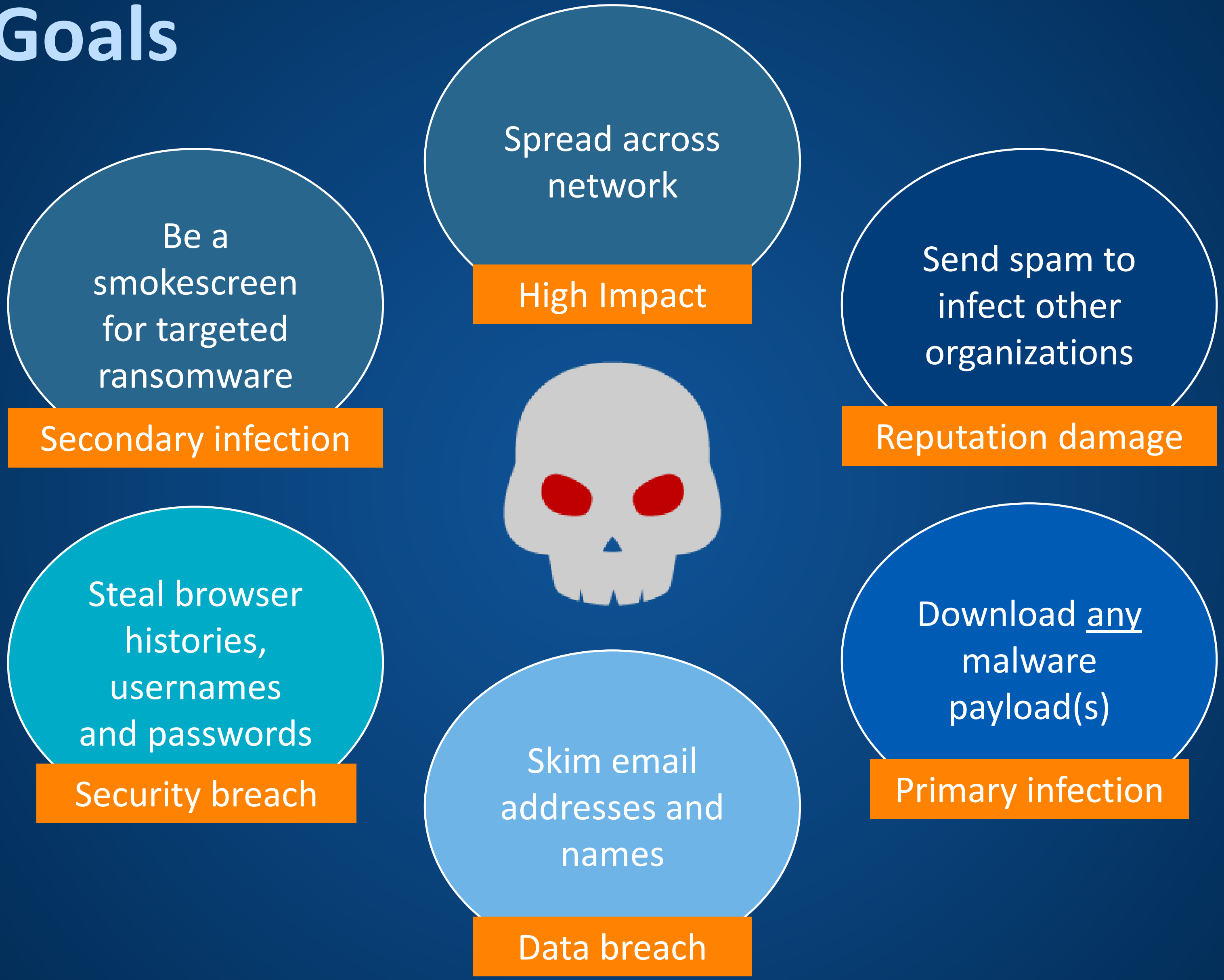
Send spam to infect other organizations

Steal browser histories, usernames and passwords

Skim email addresses and names

Download any malware payload(s)

Emotet’s Goals



Spread across network

High Impact

Be a smokescreen for targeted ransomware

Secondary infection

Send spam to infect other organizations

Reputation damage

Steal browser histories, usernames and passwords

Security breach

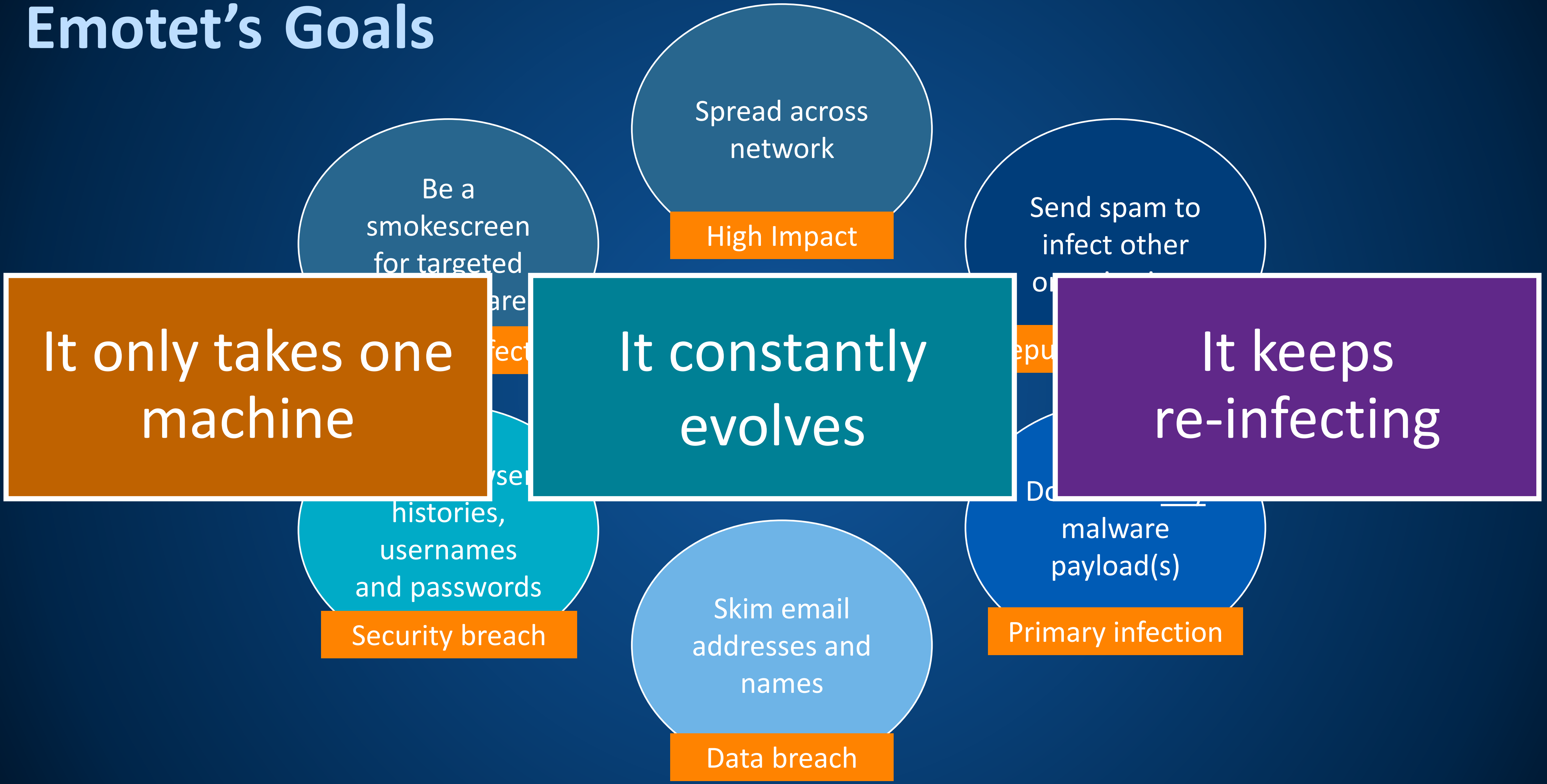
Download <u>any</u> malware payload(s)

Primary infection

Skim email addresses and names

Data breach

Emotet’s Goals



Spread across network

High Impact

Be a smokescreen for targeted

are

fect

Send spam to infect other

or

epu

It only takes one machine

It constantly evolves

It keeps re-infecting

ser

histories, usernames and passwords

Security breach

Skim email addresses and names

Data breach

Do

malware payload(s)

Primary infection

1. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-1-the-spam-lure/

2. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-2-the-malicious-attachment-and-killchain/

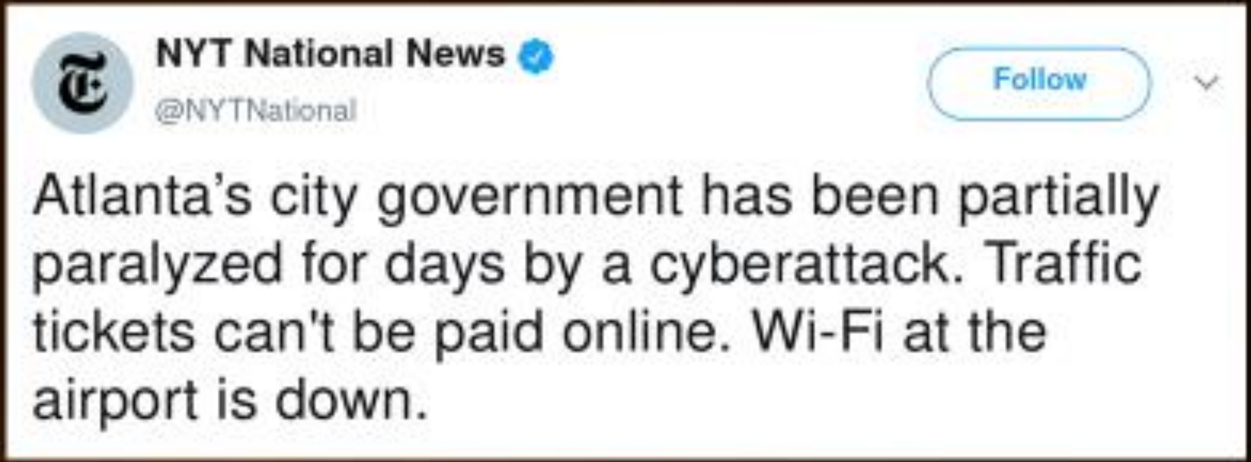
3. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-3-the-emotet-executable/

4. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-4-command-and-control/

5. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-5-a-delivery-vehicle-for-more-malware/

UNDERSTANDING MATRIX

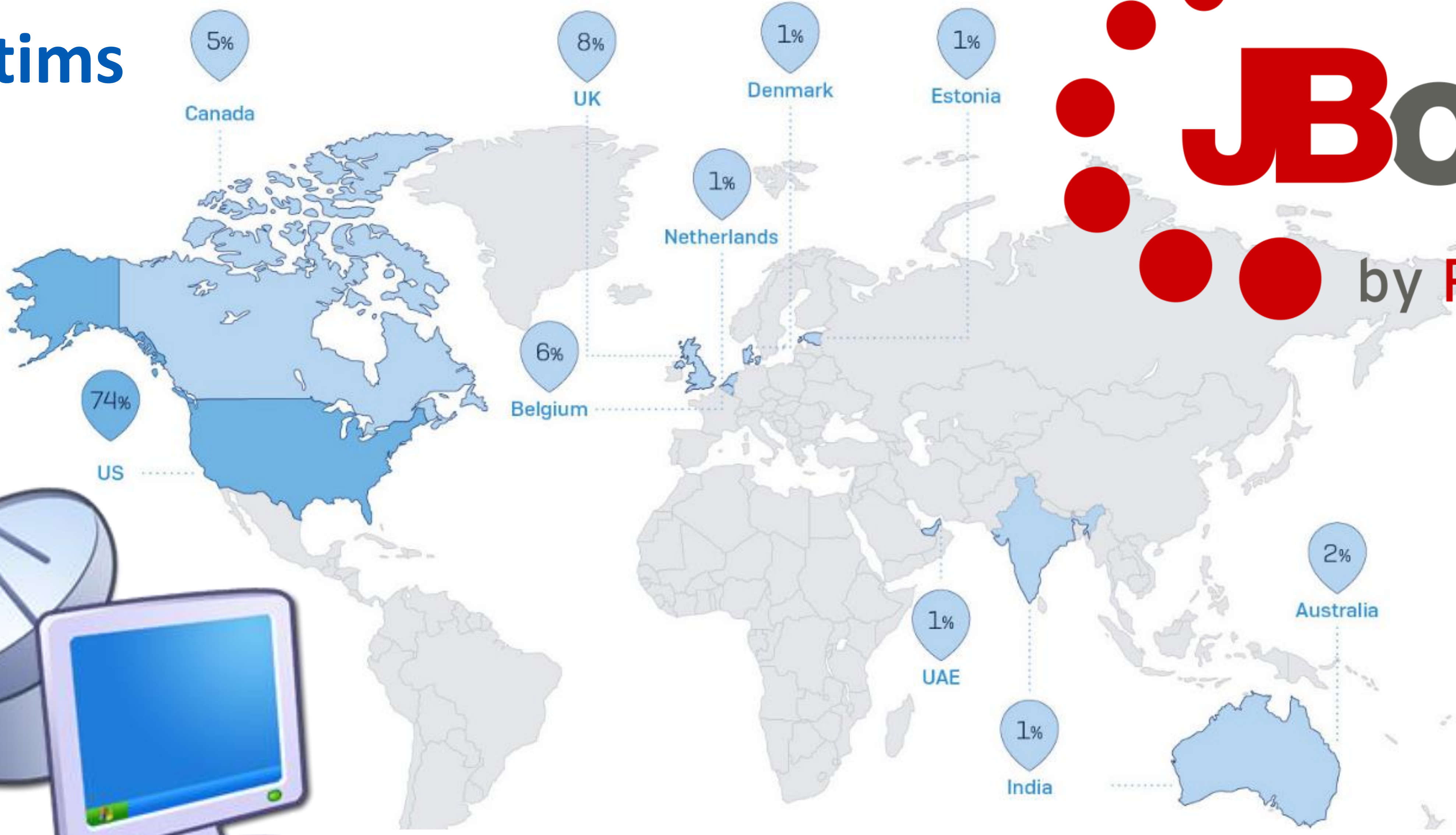
SamSam



NYT National News
@NYTNational

Atlanta's city government has been partially paralyzed for days by a cyberattack. Traffic tickets can't be paid online. Wi-Fi at the airport is down.

Victims

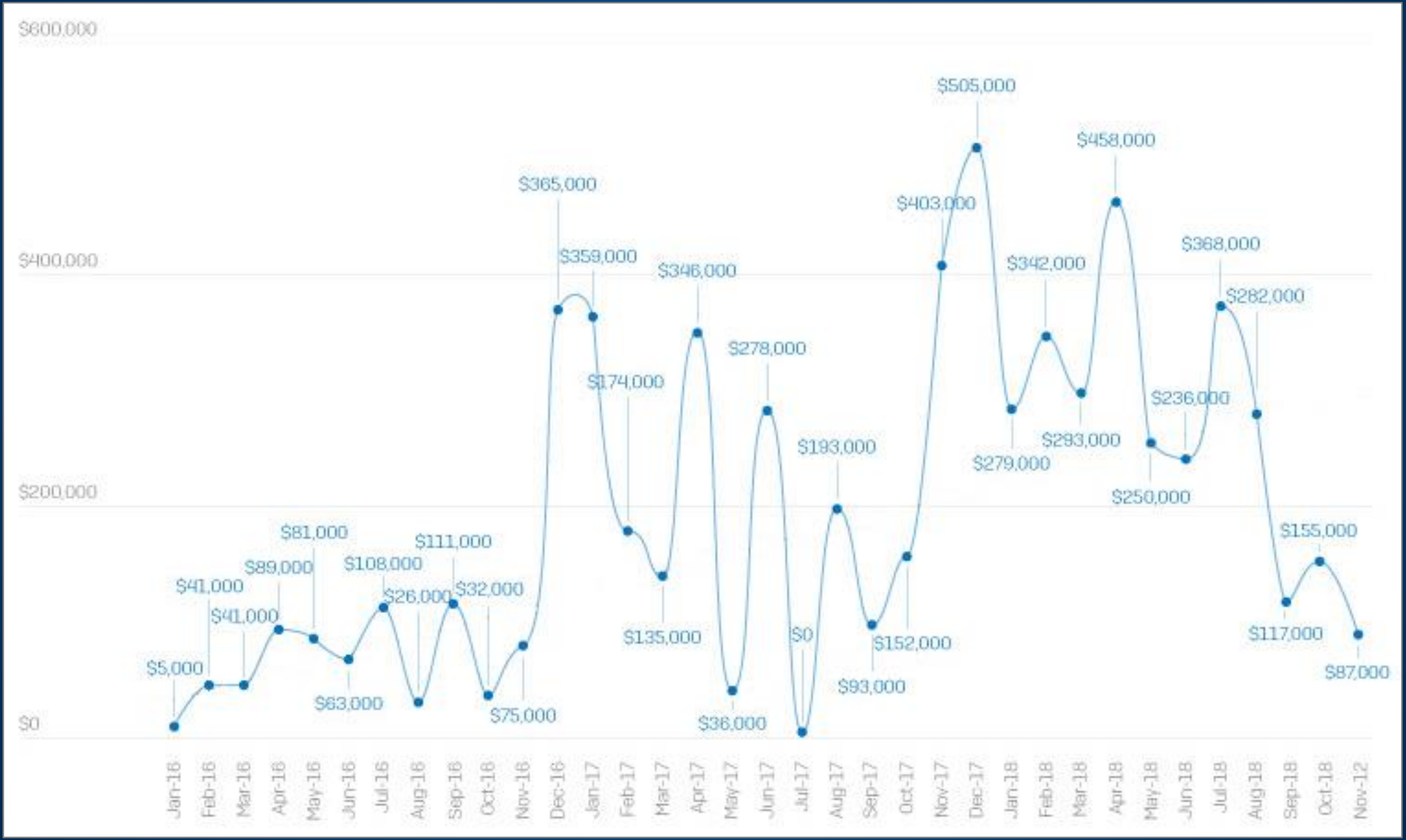


JBoss® by Red Hat

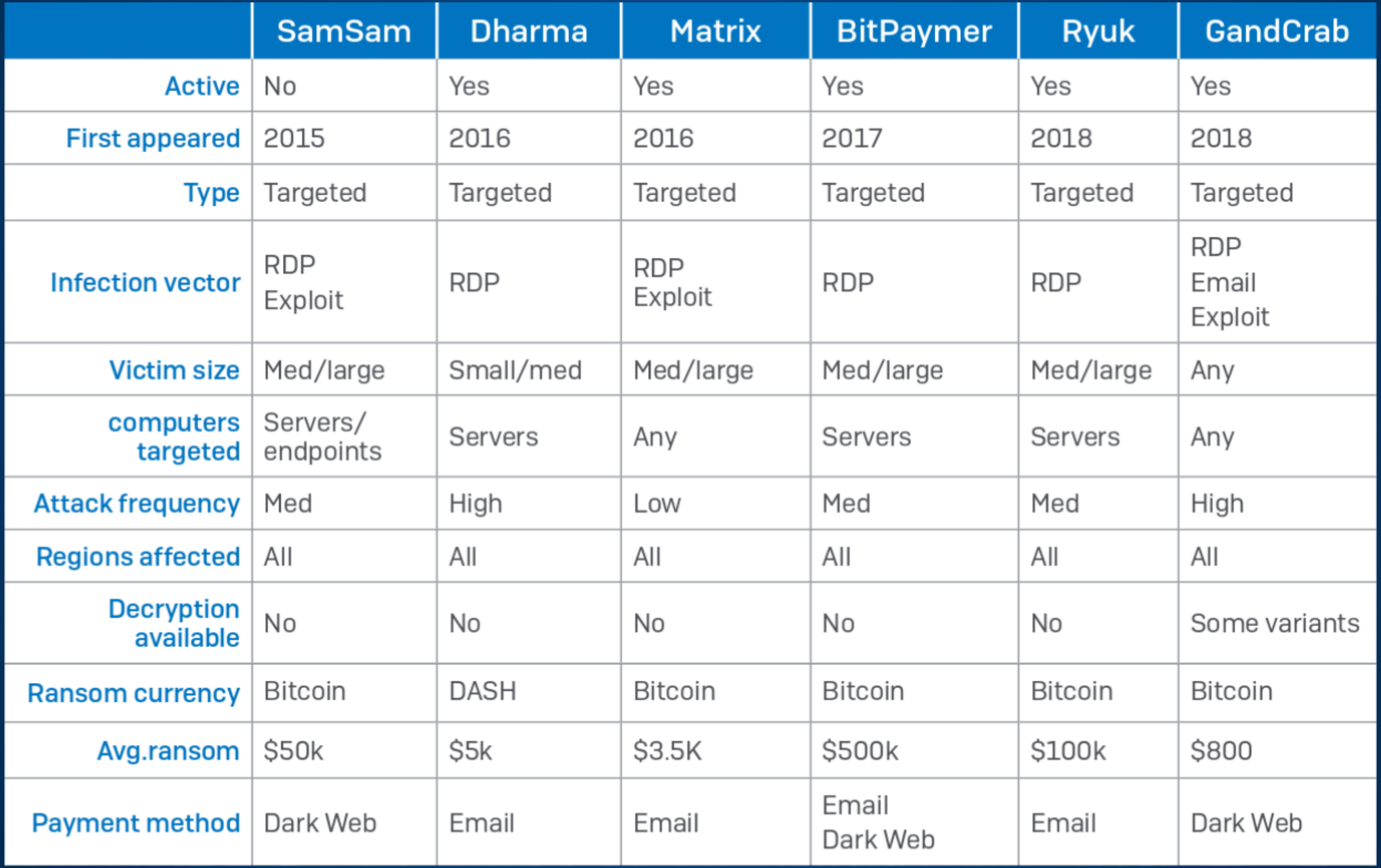
```
psexec -accepteula -s \\machine-name cmd.exe /c if exist
C:\windows\system32\g04inst.bat start /b g04inst.bat <PASSWORD>
```

SamSam ransom payments - $6.7 million USD

January 2016 - November 2018



Copy cats



	SamSam	Dharma	Matrix	BitPaymer	Ryuk	GandCrab
Active	No	Yes	Yes	Yes	Yes	Yes
First appeared	2015	2016	2016	2017	2018	2018
Type	Targeted	Targeted	Targeted	Targeted	Targeted	Targeted
Infection vector	RDP Exploit	RDP	RDP Exploit	RDP	RDP	RDP Email Exploit
Victim size	Med/large	Small/med	Med/large	Med/large	Med/large	Any
computers targeted	Servers/ endpoints	Servers	Any	Servers	Servers	Any
Attack frequency	Med	High	Low	Med	Med	High
Regions affected	All	All	All	All	All	All
Decryption available	No	No	No	No	No	Some variants
Ransom currency	Bitcoin	DASH	Bitcoin	Bitcoin	Bitcoin	Bitcoin
Avg.ransom	$50k	$5k	$3.5K	$500k	$100k	$800
Payment method	Dark Web	Email	Email	Email Dark Web	Email	Dark Web

MATRIX

Pivoting from automated to manual attacks on highly vulnerable targets

Brute Force

Hackers brute force Windows computers with RDP exposed to the internet

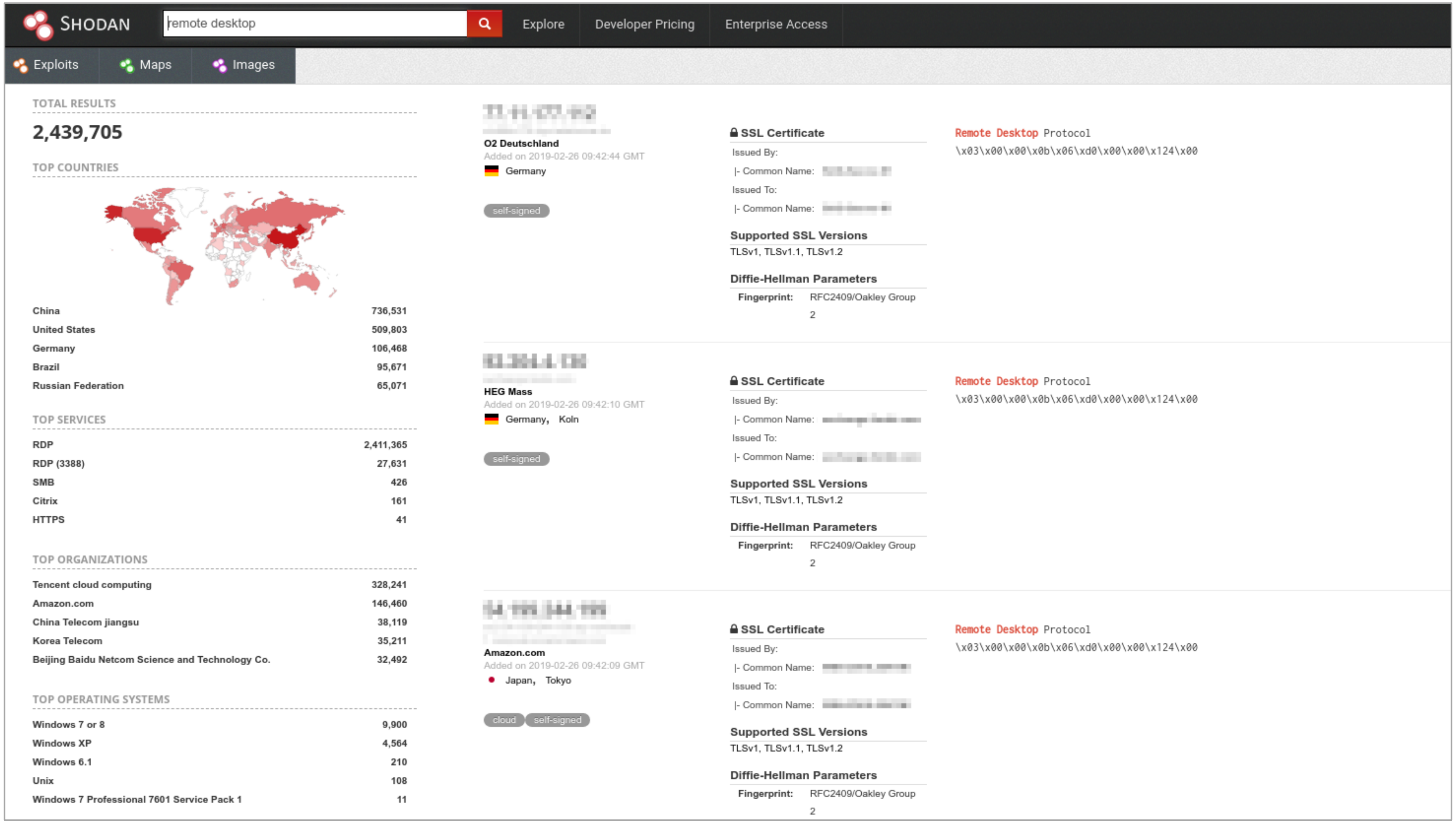
Spread

Once inside, the hackers spread to sensitive parts of the network

Ransom

Deploy ransomware to encrypt data, leaving behind only an email address to contact

RDP (Remote Desktop Pwnage)



TOTAL RESULTS

2,439,705

TOP COUNTRIES

China	736,531
United States	509,803
Germany	106,468
Brazil	95,671
Russian Federation	65,071

TOP SERVICES

RDP	2,411,365
RDP (3388)	27,631
SMB	426
Citrix	161
HTTPS	41

TOP ORGANIZATIONS

Tencent cloud computing	328,241
Amazon.com	146,460
China Telecom jiangsu	38,119
Korea Telecom	35,211
Beijing Baidu Netcom Science and Technology Co.	32,492

TOP OPERATING SYSTEMS

Windows 7 or 8	9,900
Windows XP	4,564
Windows 6.1	210
Unix	108
Windows 7 Professional 7601 Service Pack 1	11

[redacted]

O2 Deutschland

Added on 2019-02-26 09:42:44 GMT

Germany

self-signed

SSL Certificate

Issued By:

|- Common Name: [redacted]

Issued To:

|- Common Name: [redacted]

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

[redacted]

HEG Mass

Added on 2019-02-26 09:42:10 GMT

Germany, Koln

self-signed

SSL Certificate

Issued By:

|- Common Name: [redacted]

Issued To:

|- Common Name: [redacted]

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

[redacted]

Amazon.com

Added on 2019-02-26 09:42:09 GMT

Japan, Tokyo

cloud self-signed

SSL Certificate

Issued By:

|- Common Name: [redacted]

Issued To:

|- Common Name: [redacted]

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

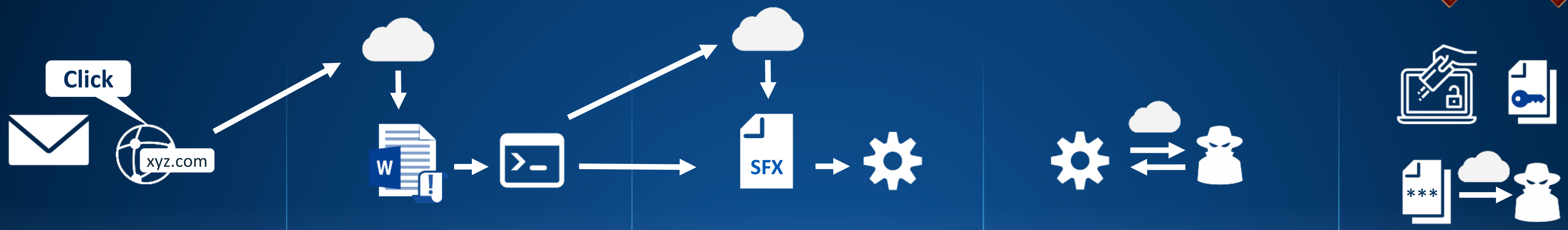
Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group 2

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

DEFENDING AGAINST EMOTET AND MATRIX WITH SOPHOS

Emotet Attack Chain



Delivery

WEB PROTECTION

EMAIL PROTECTION

SANDSTORM

Exploitation

ANTI –EXPLOIT (CODE/MEMORY/APC) MITIGATIONS

APPLICATION LOCKDOWN

LOCAL PRIVILEGE MITIGATION

APPLICATION CONTROL

Installation

DEEP LEARNING

HIPS

Command & Control

MALICIOUS TRAFFIC DETECTION

Actions on Objective

ANTI-RANSOMWARE

CREDENTIAL THEFT PROTECTION

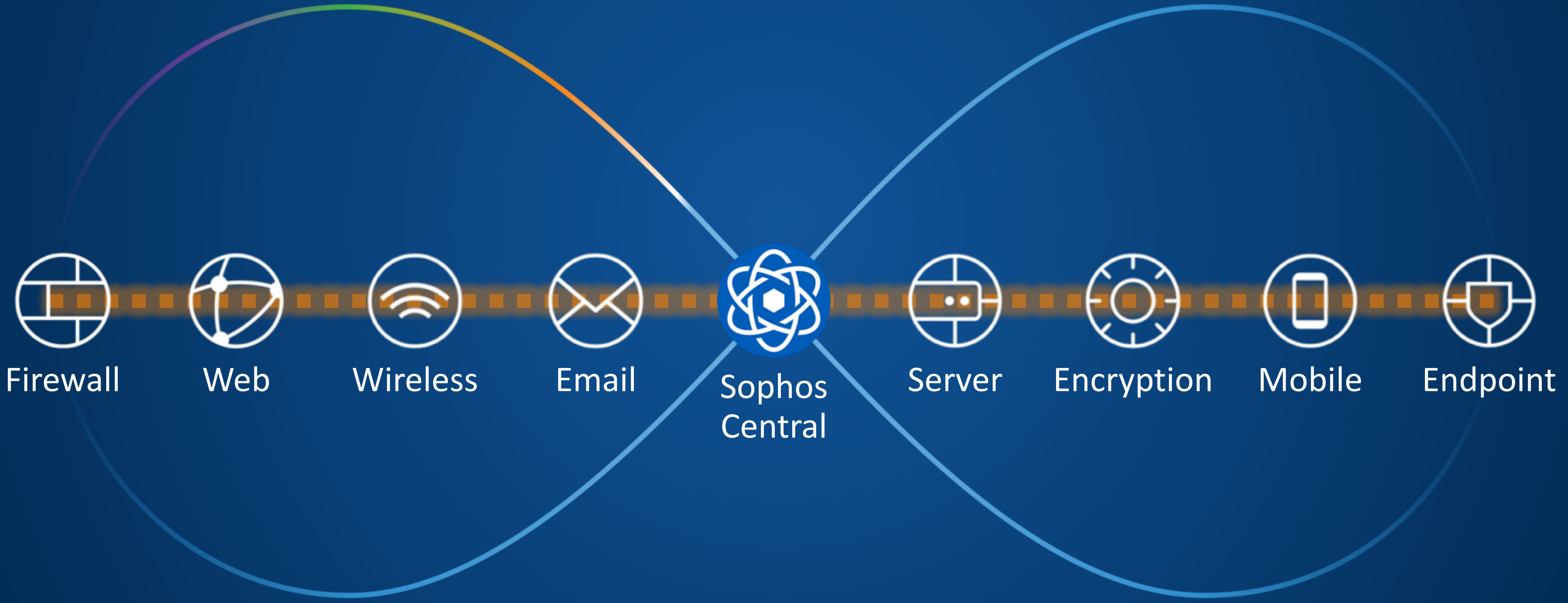
RUNTIME HIPS

THREAT CASE (RCA) & EDR

Seguridad Sincronizada = Seguridad Next-Gen

Sencilla

Robusta



Firewall

Web

Wireless

Email

Sophos Central

Server

Encryption

Mobile

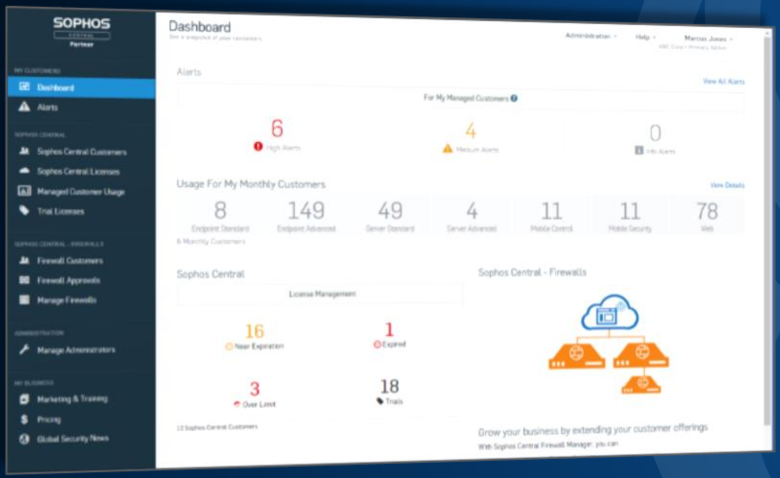
Endpoint

Respuesta automática

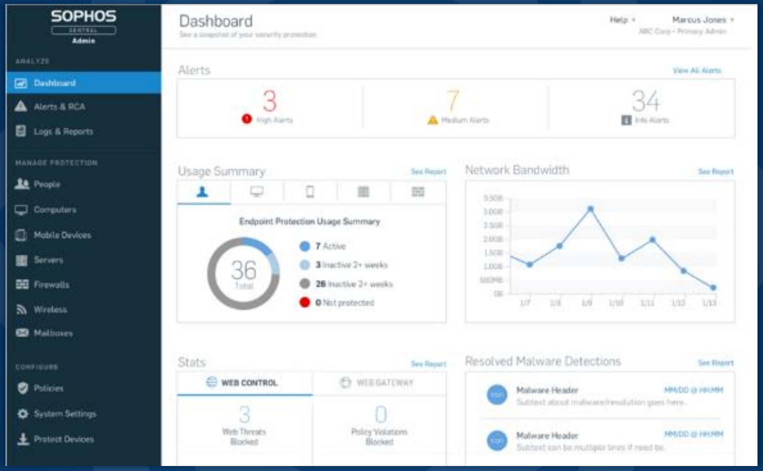
Proactiva

Gestion Centralizada: “Cibersecurity Made Simple”

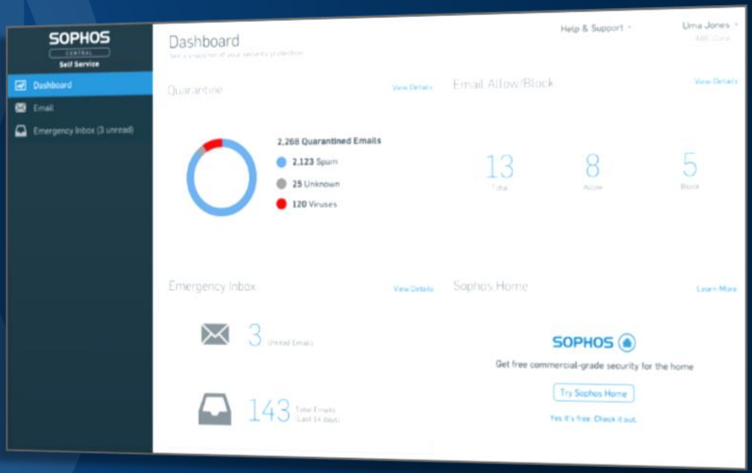
Partner Dashboard



Admin



Self Service



Reconocimiento como Lider por el Mercado/Analistas

SE Labs AAA APR-JUN 2018 ENTERPRISE ENDPOINT PROTECTION

AAA RATED

Enterprise Protection

SE Labs AAA APR-JUN 2018 SMALL BUSINESS ENDPOINT PROTECTION

AAA RATED

Small Business Protection

MRG Effitas EFFICACY ASSESSMENT & ASSURANCE

#1

Malware Protection

NSS LABS

#1

Advanced Endpoint Protection

#1

TCO

Gartner.

LEADER

FORRESTER®

LEADER

325.000 Clientes: **10.000 nuevos por Trimestre**

Iberia: **Crecimiento >20%,** 27 empleados, 9.000 Clientes, >1.500 nuevos

Adquisiciones recientes

DarkBytes

A SOPHOS Company

AVID Secure

A SOPHOS Company