Sophos Day Barcelona

7 Marzo 2019

Ricardo Maté
Country Manager Iberia

@ricardomatesal

SEE THE FUTURE
SOPHOS DISCOVER

CCN-CERT: Ciberamenazas y tendencias 2018

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

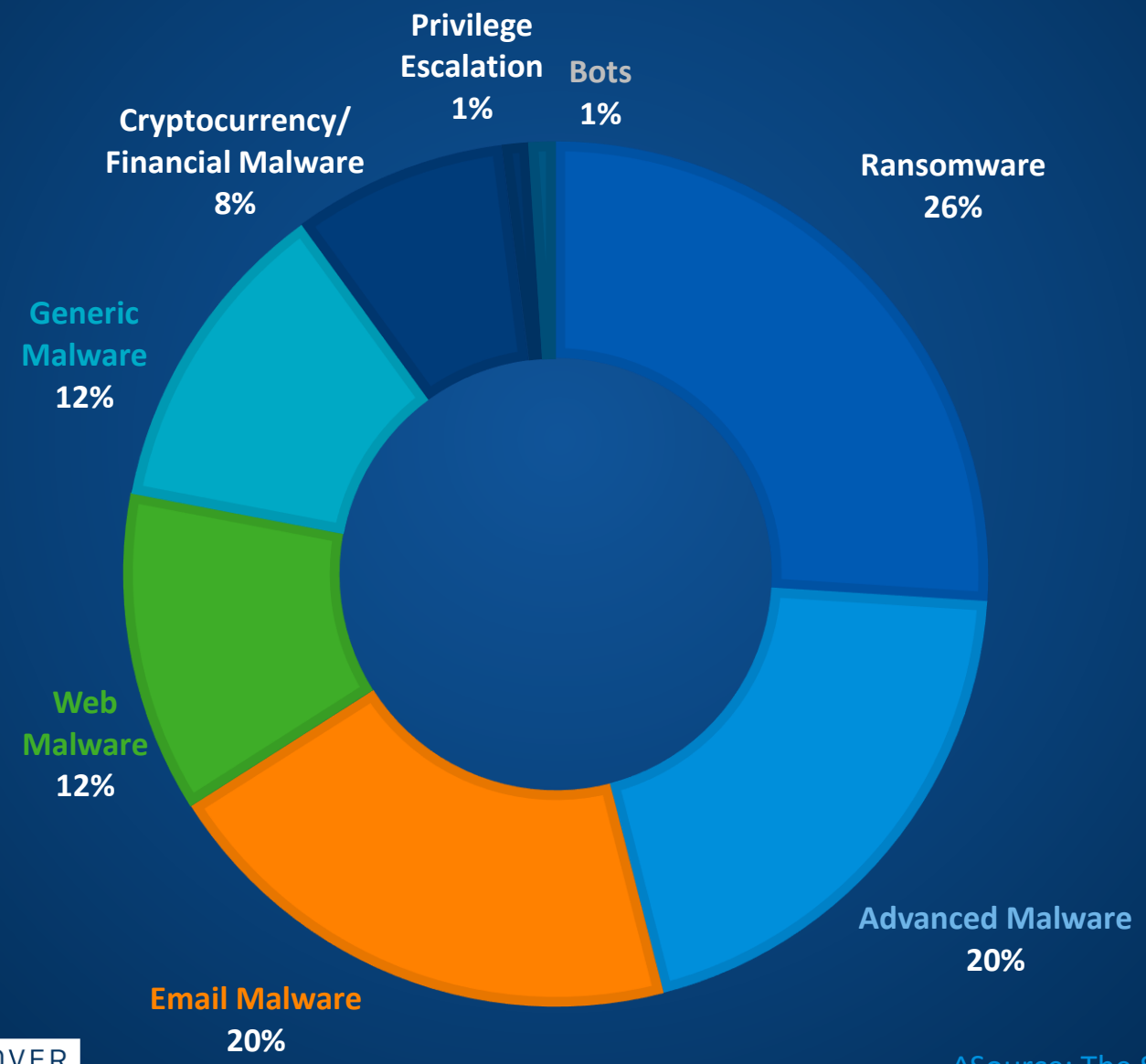
UN ATAQUE DE TIPO 'RANSOMWARE'

Puerto de BCN, Maersk... Una oleada de ciberataques 'estratégicos' golpea Cataluña

El puerto de Barcelona, Maersk y varias empresas de la Ciudad Condal han sufrido potentes ciberataques de tipo 'ransomware'. Y todos han coincidido justo en el mismo periodo de tiempo

Vista del puerto de Barcelona. (EFE)

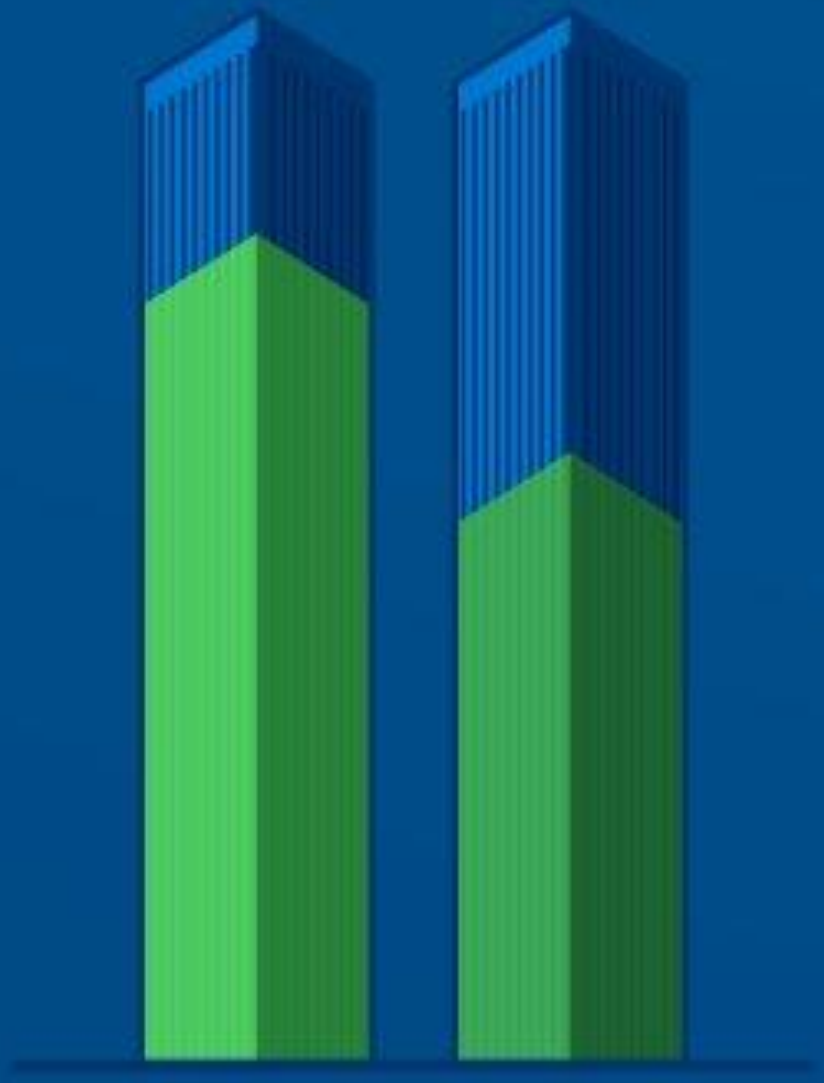
Panorama de amenazas actual



^Source: The State of Endpoint Security Today Survey

77%

of organizations were running **up-to-date** endpoint security at the time of the attack



54%

of organizations **do not** have specific anti-ransomware protection in place

Social Engineering – “Timo del CEO”

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.

Entre enero de 2015 y diciembre de 2016, los ataques BEC aumentaron un 2.370%. Europa Press

EMPRESAS

Qué es el 'fraude del CEO' y cómo evitarlo

Se estima que los ataques 'Business Email Corporate' costarán a las empresas 9.000 millones en 2018.

24 enero, 2018 - 16:32

Inicio / Seguridad / ¡Cuidado con el timo del CEO en las empresas!

¡Cuidado con el timo del CEO en las empresas!

3 julio, 2018 Seguridad
Comentarios desactivadosen ¡Cuidado con el timo del CEO en las empresas! 678 Views

El 93% de las Brechas de Seguridad provienen de algún ataque de Phishing

SOPHOS

Inside Matrix And Emotet:

How they work and how to defend

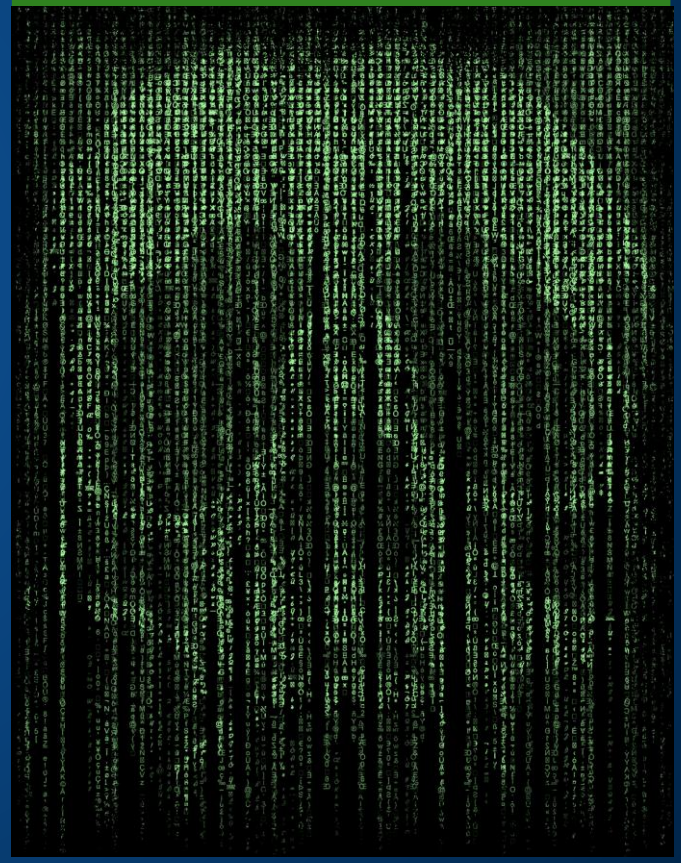
SEE THE FUTURE

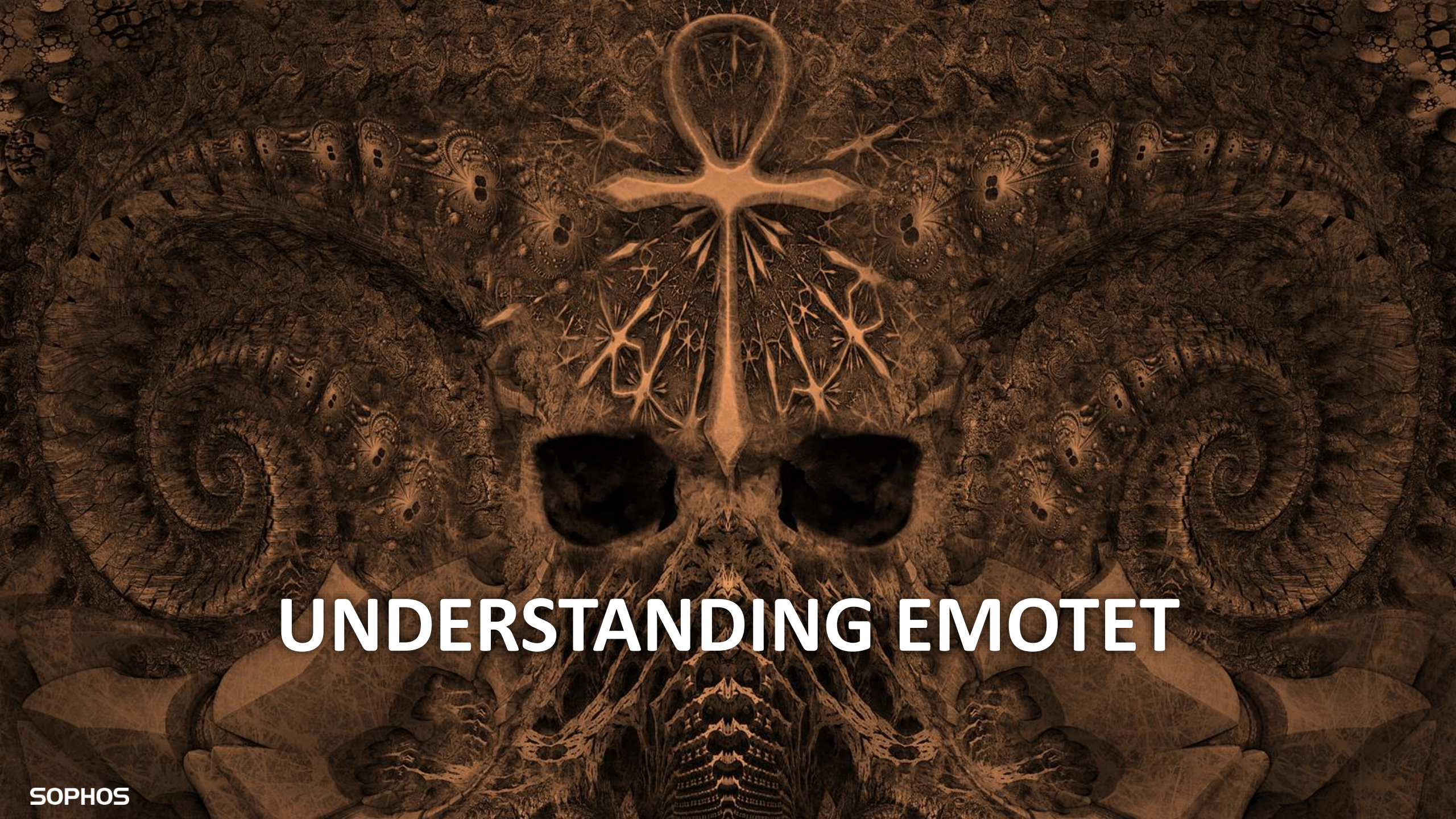
SOPHOS DISCOVER

Two Recent Examples

EMOTET

MATRIX





UNDERSTANDING EMOTET

SOPHOS

EMOTET

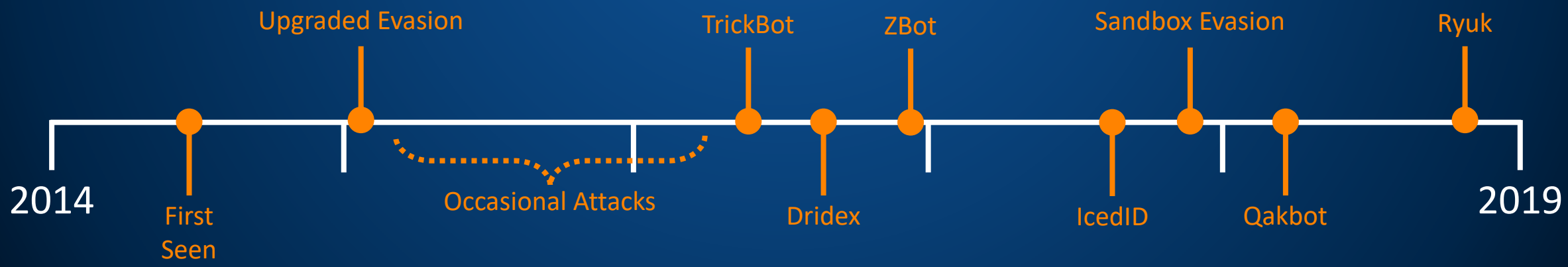
"Amongst the most costly and destructive threats to U.S. businesses right now"

U.S. Department for Homeland Security, 2018

Trojan that silently steals victims' banking credentials

Constant evolution

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



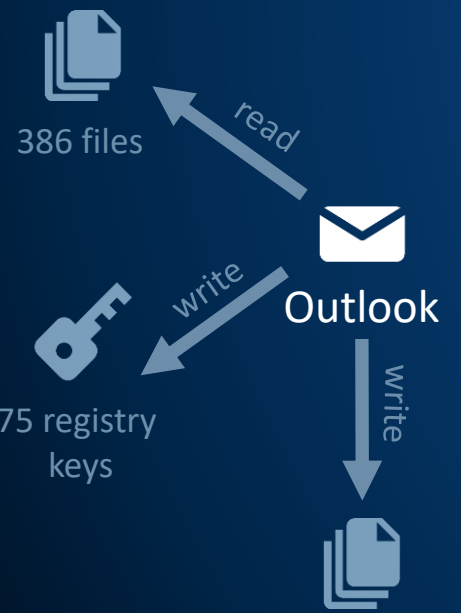
Emotet payloads change constantly

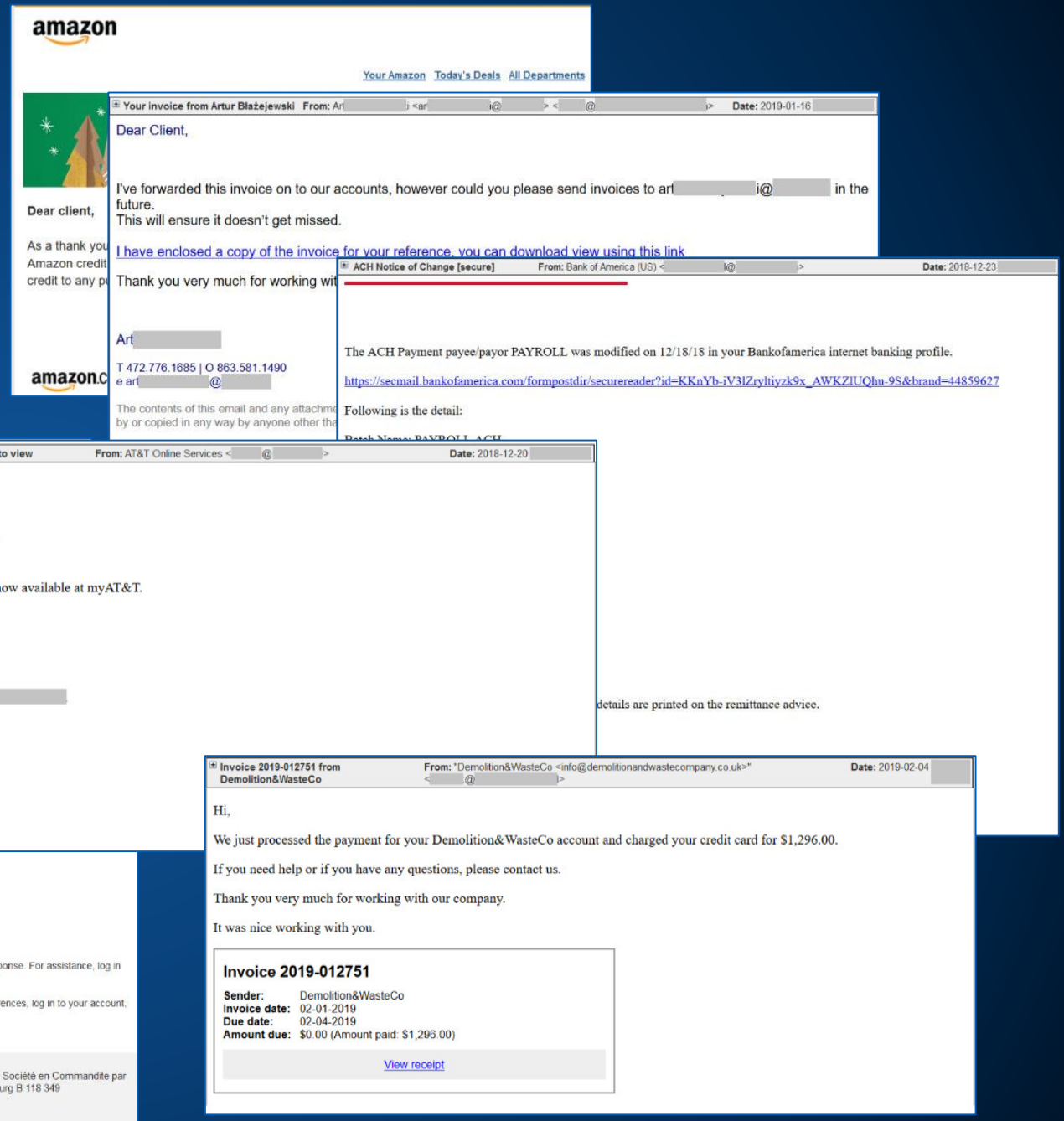
300
new payload executables every day

# of unique Emotet payload executables seen by SophosLabs

STAGE 1

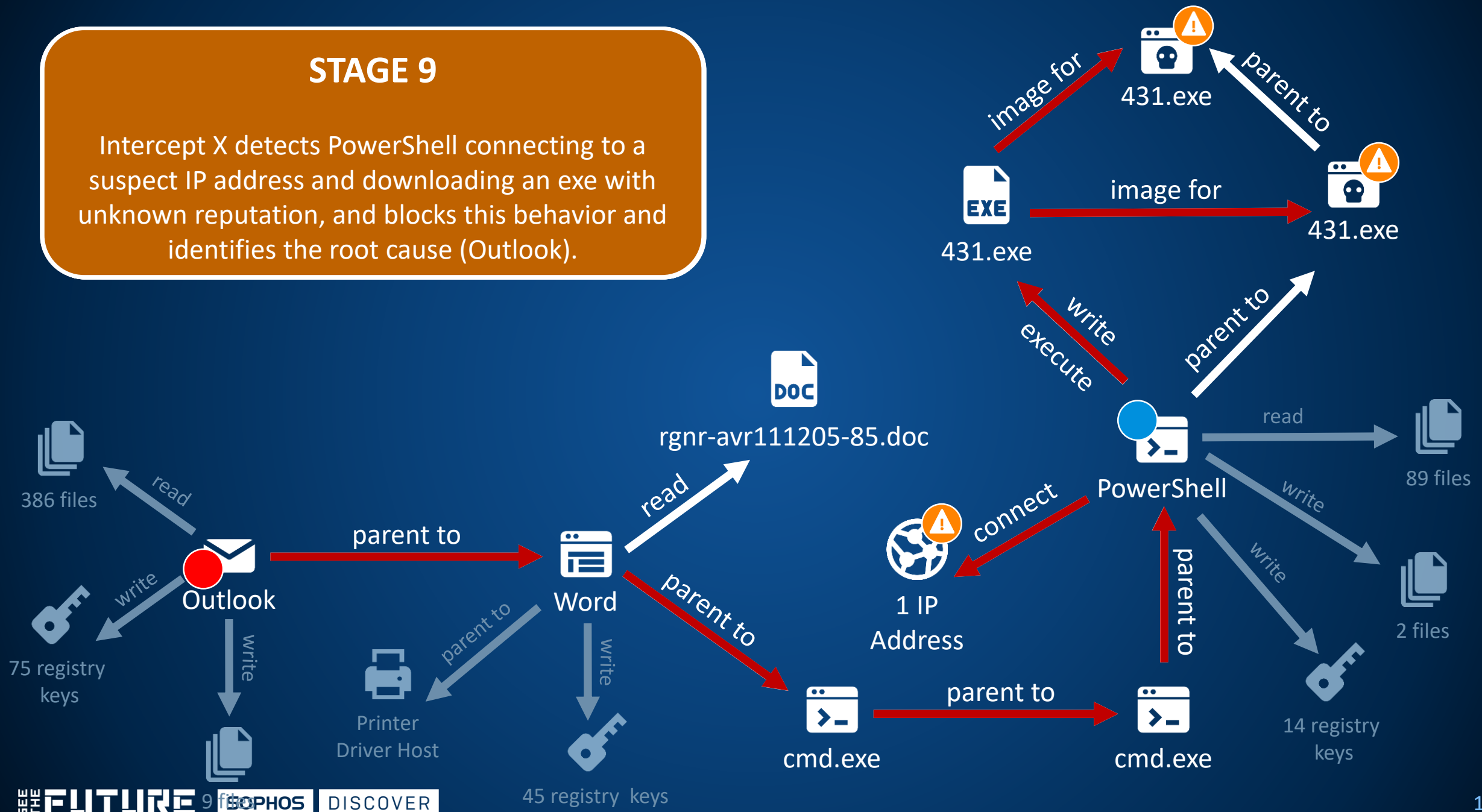
User received a malicious email (malspam)





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

Download any malware payload(s)

Skim email addresses and names

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

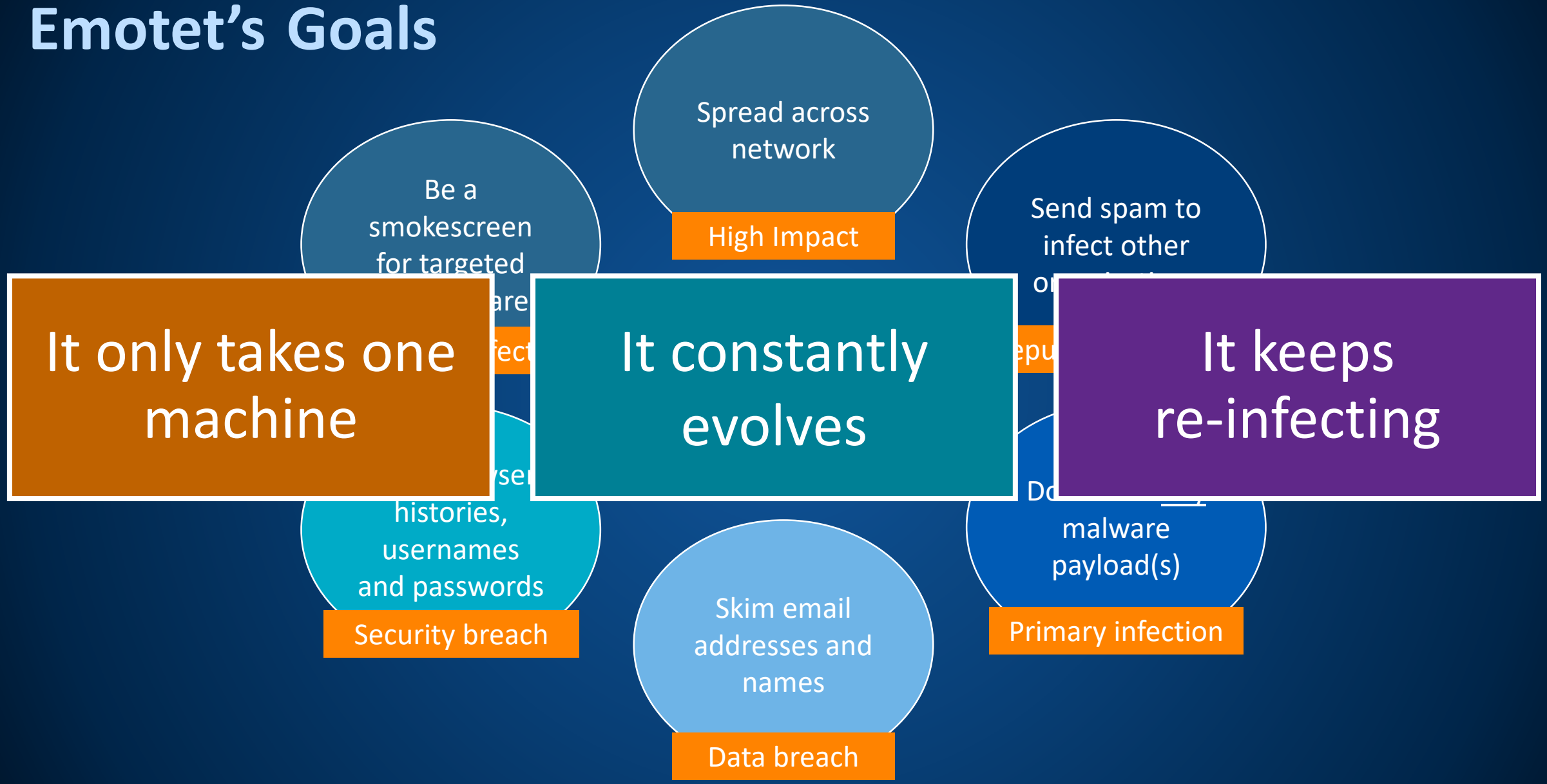
Skim email addresses and names

Data breach

Download any malware payload(s)

Primary infection

Emotet's Goals



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
Follow

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

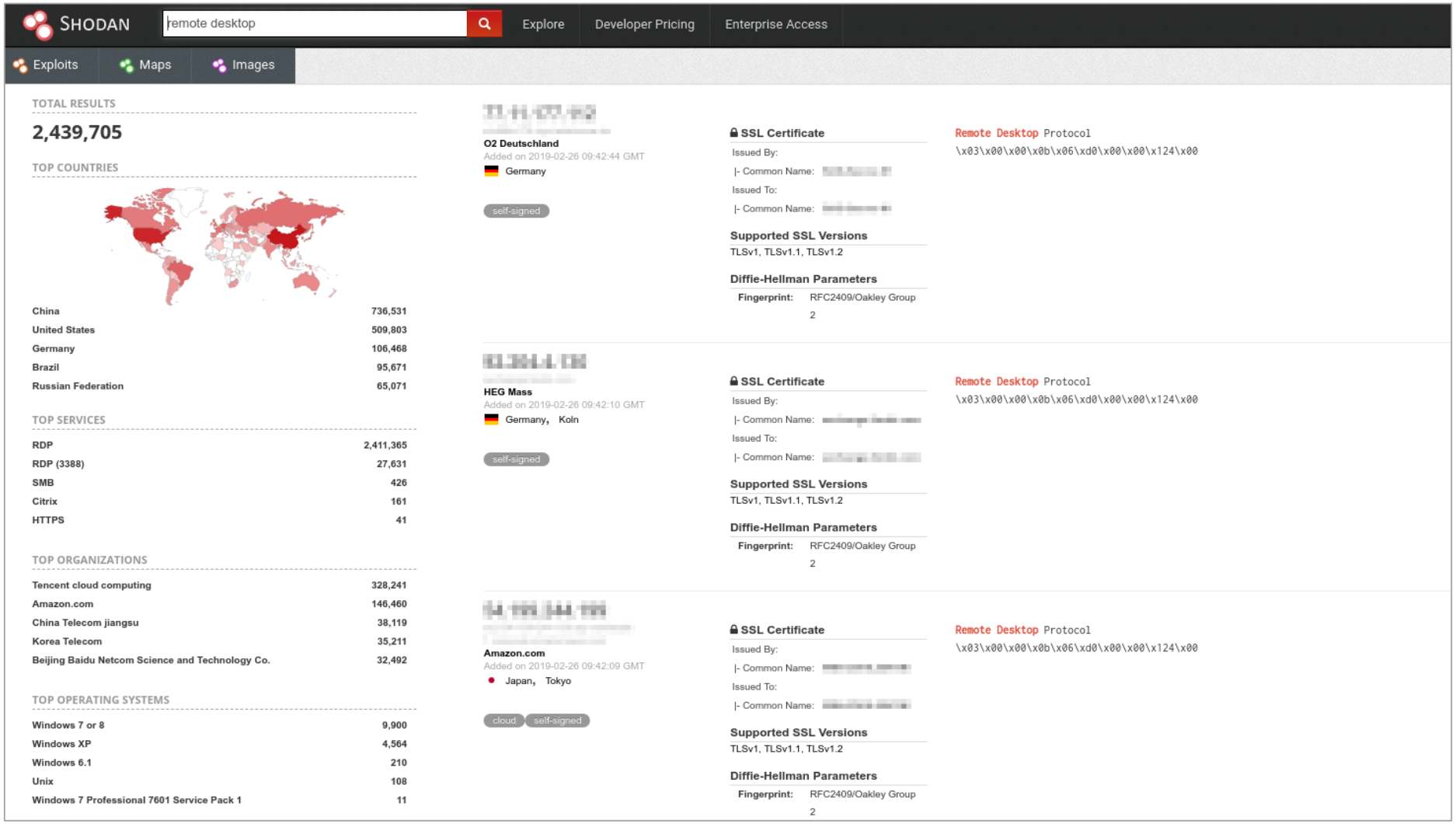
Spread

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

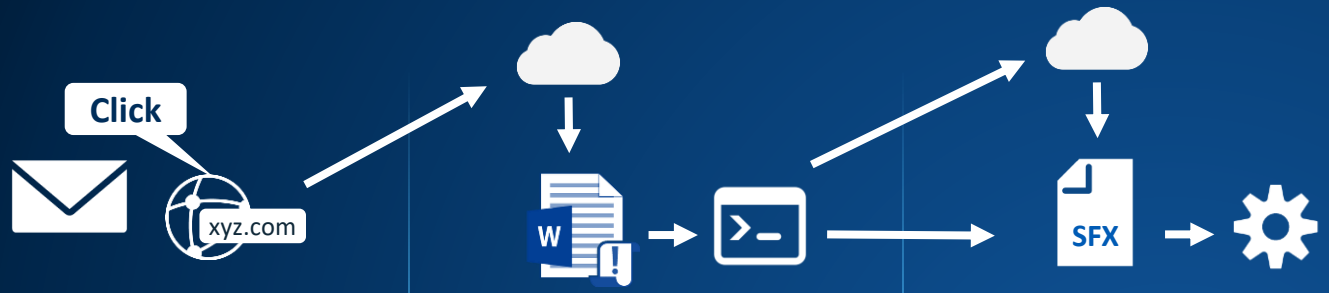
RDP (Remote Desktop Pwnage)



DEFENDING AGAINST EMOTET AND MATRIX WITH SOPHOS

Emotet Attack Chain

SOPHOS INTERCEPT X



Delivery	Exploitation	Installation	Command & Control	Actions on Objective
WEB PROTECTION	ANTI –EXPLOIT (CODE/MEMORY/APC) MITIGATIONS	DEEP LEARNING	MALICIOUS TRAFFIC DETECTION	ANTI-RANSOMWARE
EMAIL PROTECTION	APPLICATION LOCKDOWN	HIPS		CREDENTIAL THEFT PROTECTION
SANDSTORM	LOCAL PRIVILEGE MITIGATION			RUNTIME HIPS
	APPLICATION CONTROL			THREAT CASE (RCA) & EDR

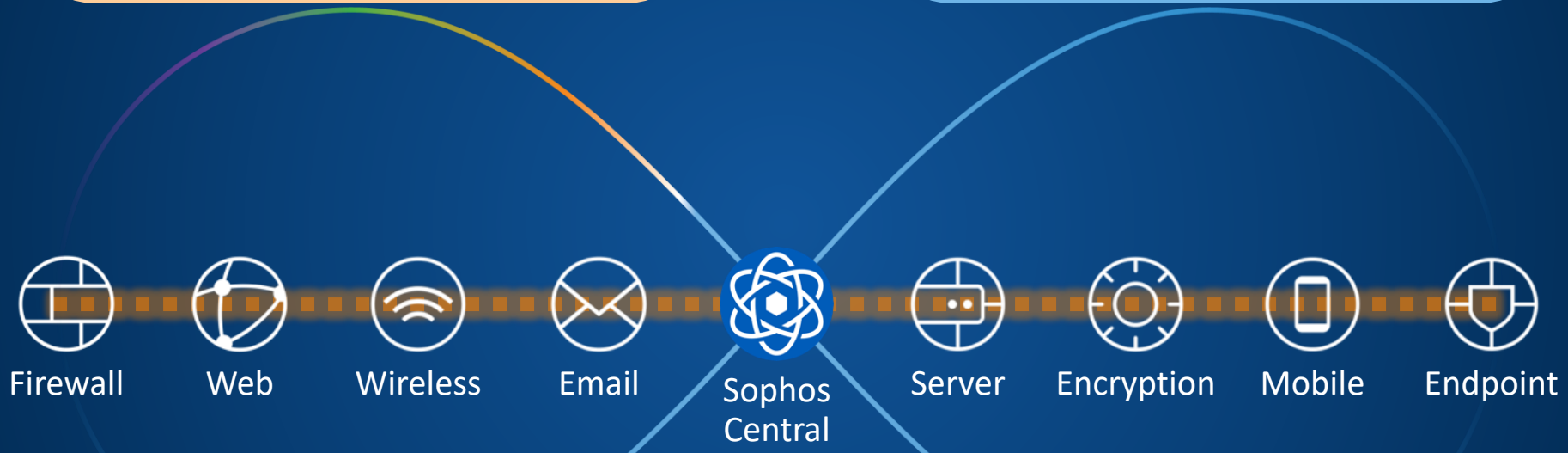
Los datos de Cybersecurity Ventures señalan que habrá 3.5 millones de puestos de especialistas en ciberseguridad sin cubrir para el año 2021.

SOPHOS

Seguridad Sincronizada = Seguridad Next-Gen

Sencilla

Robusta

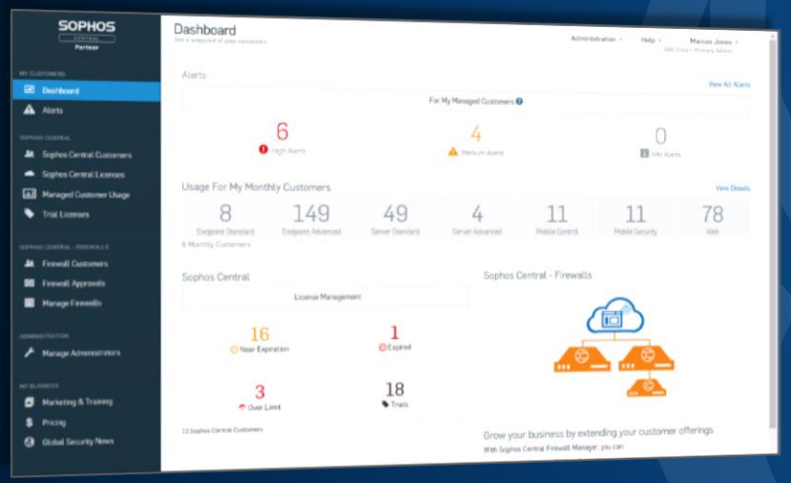


Respuesta automática

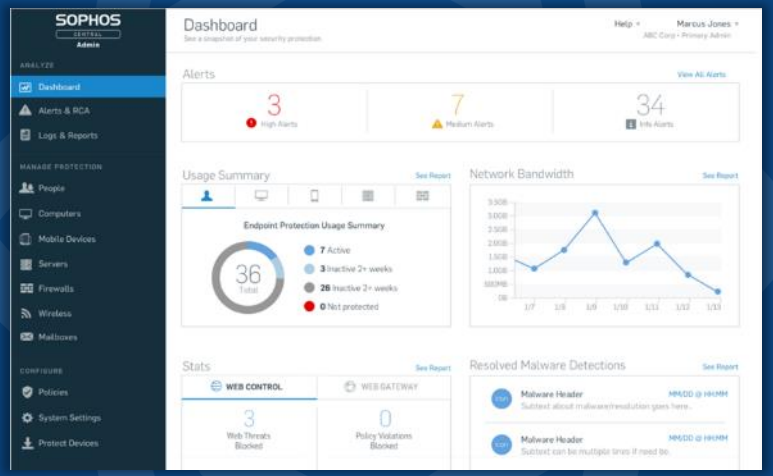
Proactiva

Gestion Centralizada: “Cibersecurity Made Simple”

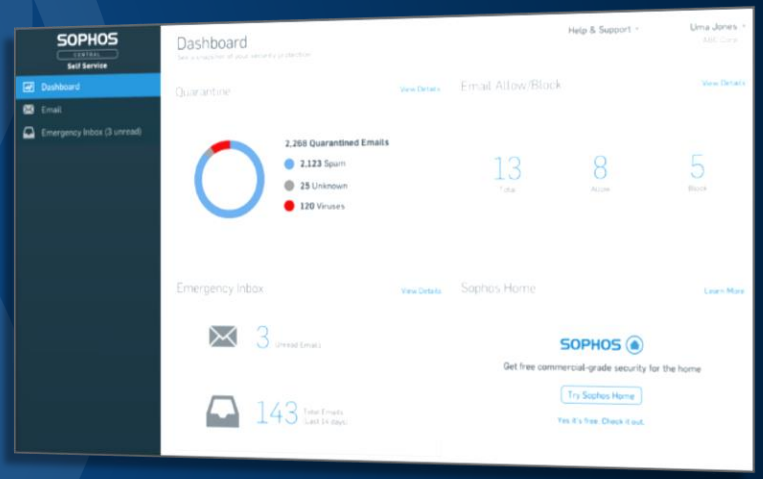
Partner Dashboard



Admin



Self Service



Reconocimiento como Lider por el Mercado/Analistas

AAA RATED

Enterprise 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