

Intercept X & Sophos Central

Mauro Pisoni
Senior Sales Engineer

14 Giugno 2019

SOPHOS DISCOVER 2019
EVOLVE

SOPHOS
INTERCEPT



NOW WITH
EDR

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.



The Ever-Evolving Threat Landscape

SOPHOS

Email

zxc@ @

like like

email

Password

password

[22:20

Search

Done.

[22:20

```

0 Array
1 (
2   [id] => 1394644334
3   [luser] => zxc
4   [domain] => .126.com
5   [password] => 123456789
6 )
7
8 1 Array
9 (
10  [id] => 1394644335
11  [luser] => zxc
12  [domain] => .163.com
13  [password] => 5060789
14 )
15
16 2 Array
17 (
18  [id] => 1394644336
19  [luser] => zxc
20  [domain] => .163.com
21  [password] => a53231323
22 )
23
24 3 Array
25 (
26  [id] => 1394644337
27  [luser] => zxc
28  [domain] => .onen.pl
29  [password] => 123456
30 )

```

SOP
EY

';--have i been pwned?

Check if you have an account that has been compromised in a data breach



Generate secure, unique passwords for every account

[Learn more at 1Password.com](https://1password.com)

[Why 1Password?](#)

359

pwned websites

7,840,611,051

pwned accounts

92,986

pastes

113,418,023

paste accounts

359

pwned websites

7,840,611,051

pwned accounts











92,986

pastes











113,418,023

paste accounts

Largest breaches

-  772,904,991 [Collection #1 accounts](#)
-  763,117,241 [Verifications.io accounts](#)
-  711,477,622 [Onliner Spambot accounts](#)
-  593,427,119 [Exploit.In accounts](#)
-  457,962,538 [Anti Public Combo List accounts](#)
-  393,430,309 [River City Media Spam List accounts](#)
-  359,420,698 [MySpace accounts](#)
-  234,842,089 [NetEase accounts](#)
-  164,611,595 [LinkedIn accounts](#)
-  161,749,950 [Dubsmash accounts](#)

Recently added breaches

-  DataCamp 760,561 [DataCamp accounts](#)
-  808,330 [Knuddels accounts](#)
-  52,623 [Demon Forums accounts](#)
-  871,190 [Everybody Edits accounts](#)
-  3,073,409 [Intelimost accounts](#)
-  11,657,763 [Whitepages accounts](#)
-  14,867,999 [500px accounts](#)
-  3,830,916 [Bookmate accounts](#)
-  28,510,459 [HauteLook accounts](#)
-  15,025,407 [8fit accounts](#)

500,000

new malware
per day

75%

only seen
once

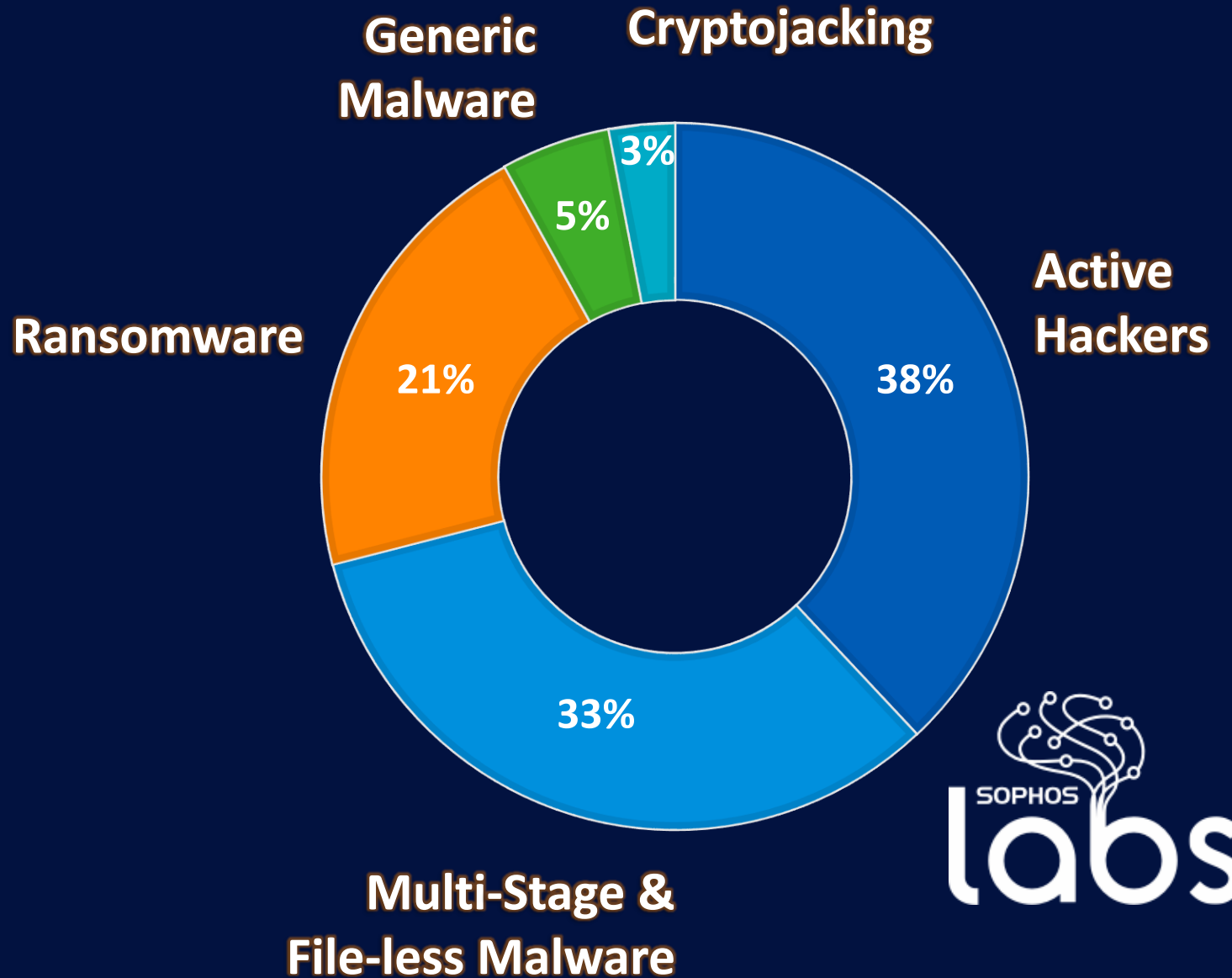


SOPHOS
labs

53%
orgs hit by
ransomware

*Source: State of Endpoint Protection Study 2018

1/3
paid the ransom



Vulnerabilities Waiting to Be Exploited

Software Vulnerabilities Reported by Year



■ low ■ medium ■ high

Up to Feb 2019

A Recent Threat

EMOTET



The image is a highly detailed, fractal-like composition in shades of brown and gold. At the center is a skull, with its eye sockets and nasal cavity rendered in deep shadow. Above the skull is a glowing, golden cross-like symbol with a circular top, resembling a caduceus or a similar medical or alchemical symbol. The background is filled with intricate, repeating patterns of spirals, floral motifs, and geometric shapes, creating a sense of depth and complexity. The overall aesthetic is reminiscent of ancient Egyptian art or a highly detailed woodcut.

UNDERSTANDING EMOTET

EMOTET

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

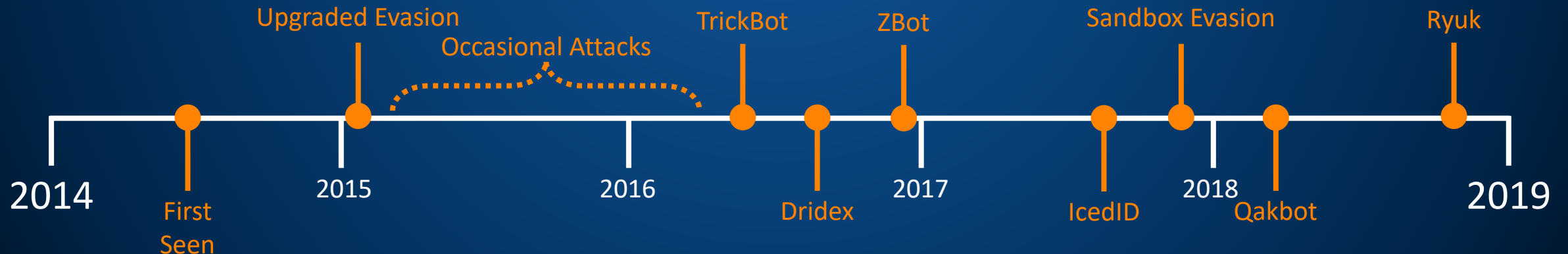
U.S. Department of Homeland Security, 2018

Trojan that silently steals
victims' banking credentials

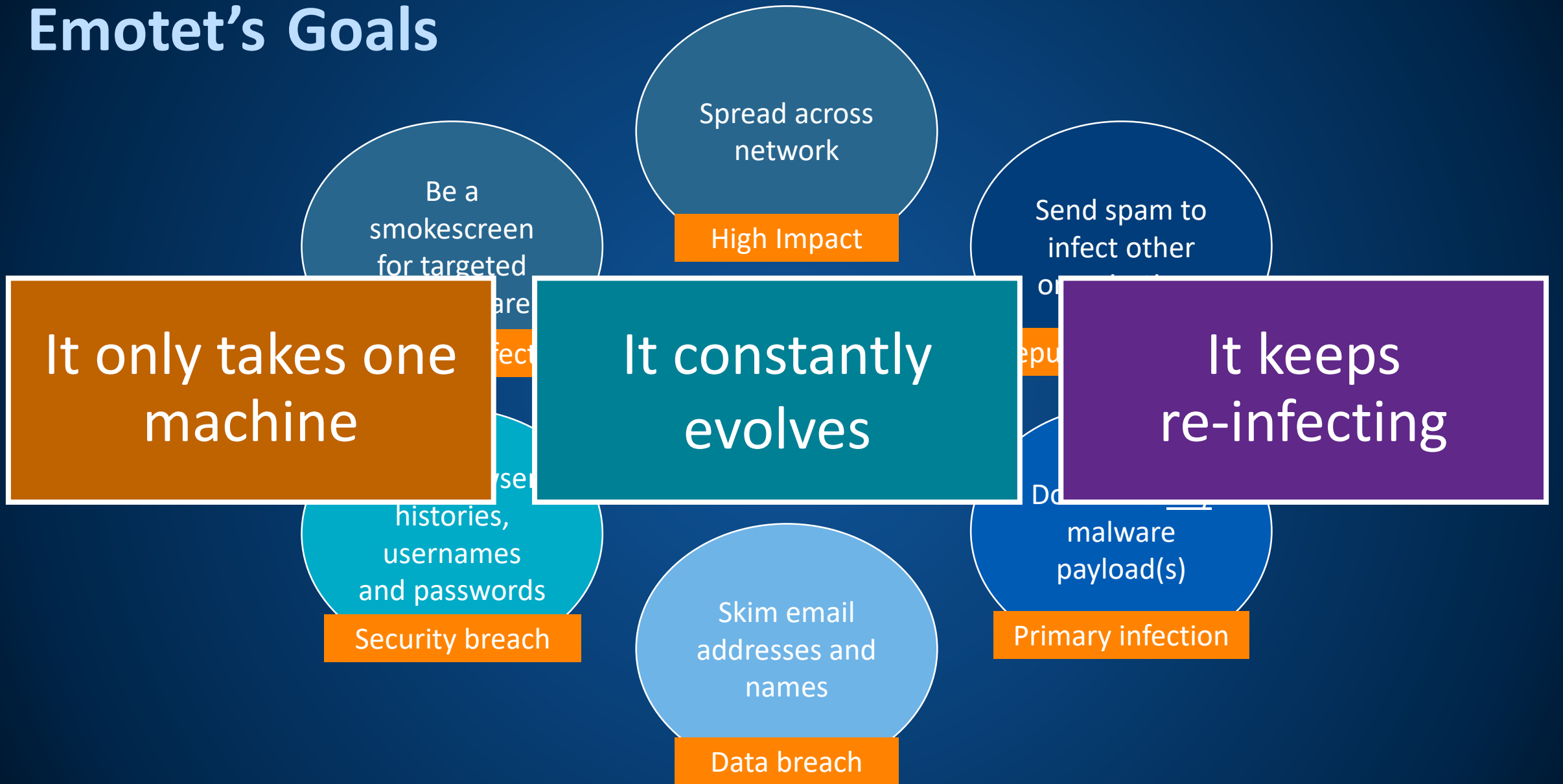


Constant evolution

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



Emotet's Goals





CISA
CYBER+INFRASTRUCTURE



HOME

ABOUT US

ALERTS AND TIPS

RESOURCES

C³ VP

Alert (TA18-201A)

[More Alerts](#)

Emotet Malware

Original release date: July 20, 2018



Print

Systems Affected

Network Systems

Overview

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.

This joint Technical Alert (TA) is the result of Multi State Information Sharing & Analysis Center (MS-ISAC) analytic efforts, in coordination with the Department of

, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be one of the most destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.

Report (TA) is the result of Multi-State Information Sharing & Analysis Center (MS-ISAC) analytic efforts, in coordination with the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC).

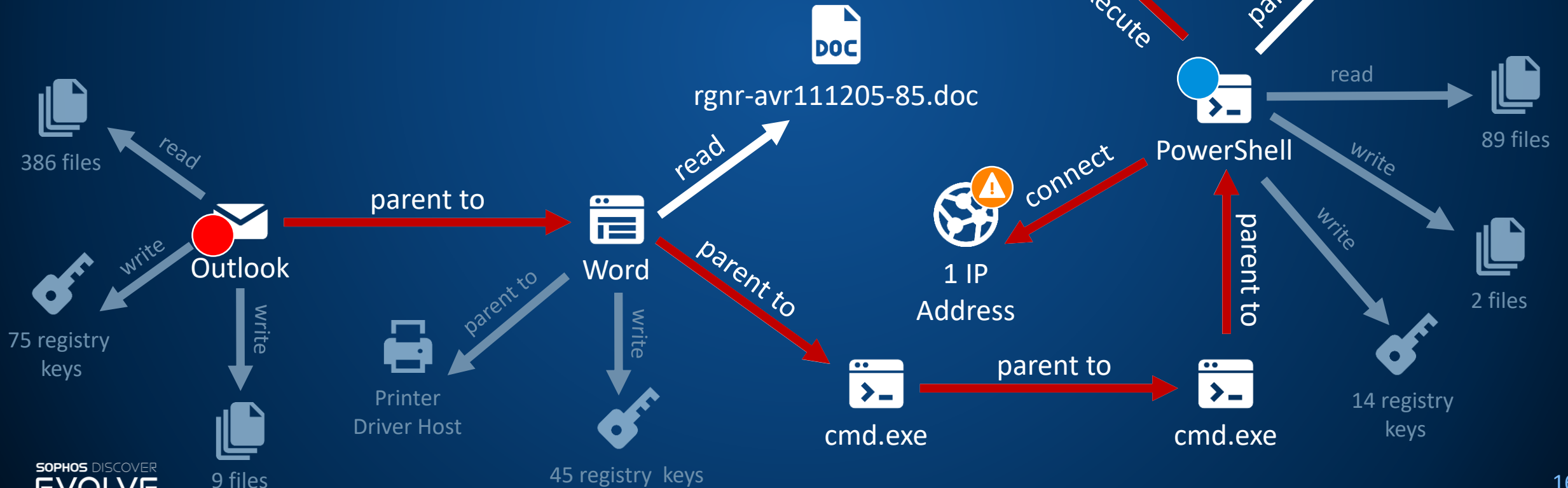
Emotet is among the most costly and destructive malware affecting SLTT governments. Its worm-like features result in rapidly spreading infections that are difficult to combat. Emotet infections have cost SLTT governments up to \$1 million per incident to remediate.

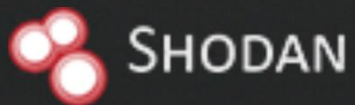
, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Additionally, Emotet is designed to evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys, scheduled tasks, and Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine-aware and can operate within a virtual environment.

Emotet is often spread through malspam (emails containing malicious attachments or links) that uses branding familiar to the recipient; it has even been used to impersonate well-known companies. As of July 2018, the most recent campaigns imitate PayPal receipts, shipping notifications, or “past-due” invoices purportedly from a company. An infection occurs when a user opens or clicks the malicious download link, PDF, or macro-enabled Microsoft Word document included in the email. Once installed, Emotet establishes persistence and attempts to propagate the local networks through incorporated spreader modules.

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).





os:windows port:3389



Explore

Downloads

Reports

Pricing

Enterprise Access

My Account



Exploits



Maps



Images



Share Search



Download Results



Create Report

TOTAL RESULTS

14,627

TOP COUNTRIES



United States	7,603
Netherlands	2,413
China	1,122
Germany	687
United Kingdom	518

34.254.91.126

ec2-34-254-91-126.eu-west-1.compute.amazonaws.com

Windows 7 or 8

Amazon Data Services Ireland Limited

Added on 2019-04-11 02:18:44 GMT



Ireland, Dublin

cloud

self-signed

SSL Certificate

Issued By:

|- Common Name: WIN-RLF3S1DUO0H

Issued To:

|- Common Name: WIN-RLF3S1DUO0H

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

os:windows port:3389

Search



Total Results:14,628



Top Countries



US	7,604
NL	2,413
CN	1,122
DE	687
GB	518

Top Organizations

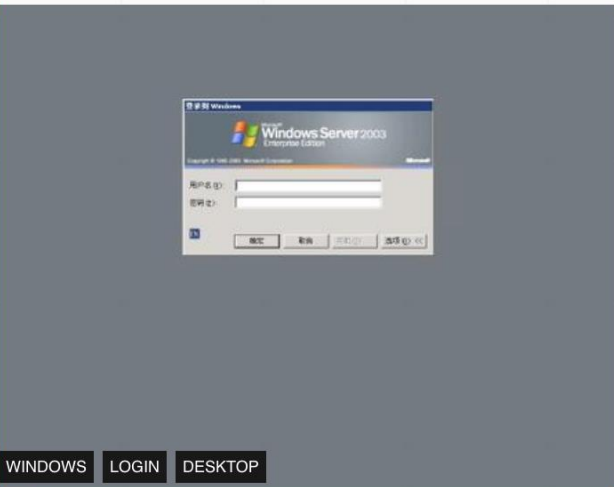


Microsoft Azure	4,138
China Unicom Beijing	573
Enzu	515
Psychz Networks	498
Amazon.com	433





WINDOWS LOGIN DESKTOP Windows Server 2008 R2 Standard Edition



WINDOWS LOGIN DESKTOP



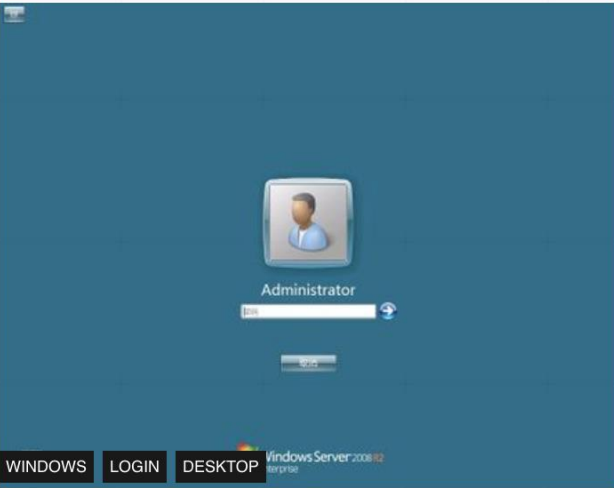
WINDOWS LOGIN DESKTOP Windows 7 Professional



WINDOWS LOGIN DESKTOP



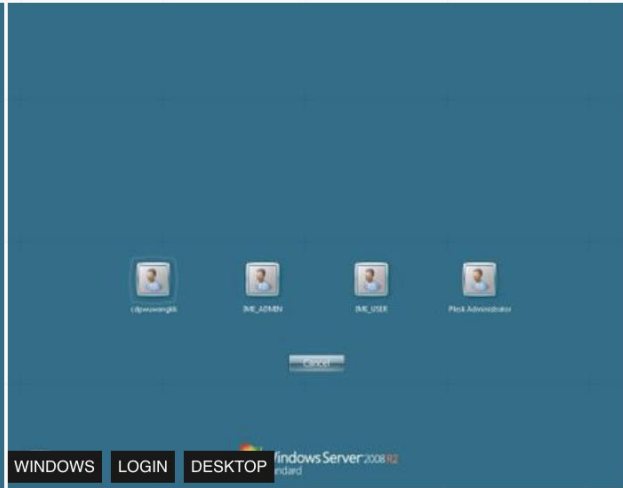
WINDOWS LOGIN DESKTOP Windows Server 2008 R2 Standard Edition



WINDOWS LOGIN DESKTOP Windows Server 2008 R2 Enterprise Edition



WINDOWS LOGIN DESKTOP Windows Small Business Server 2008



WINDOWS LOGIN DESKTOP Windows Server 2008 R2 Standard Edition



Modern Cyber Attacks

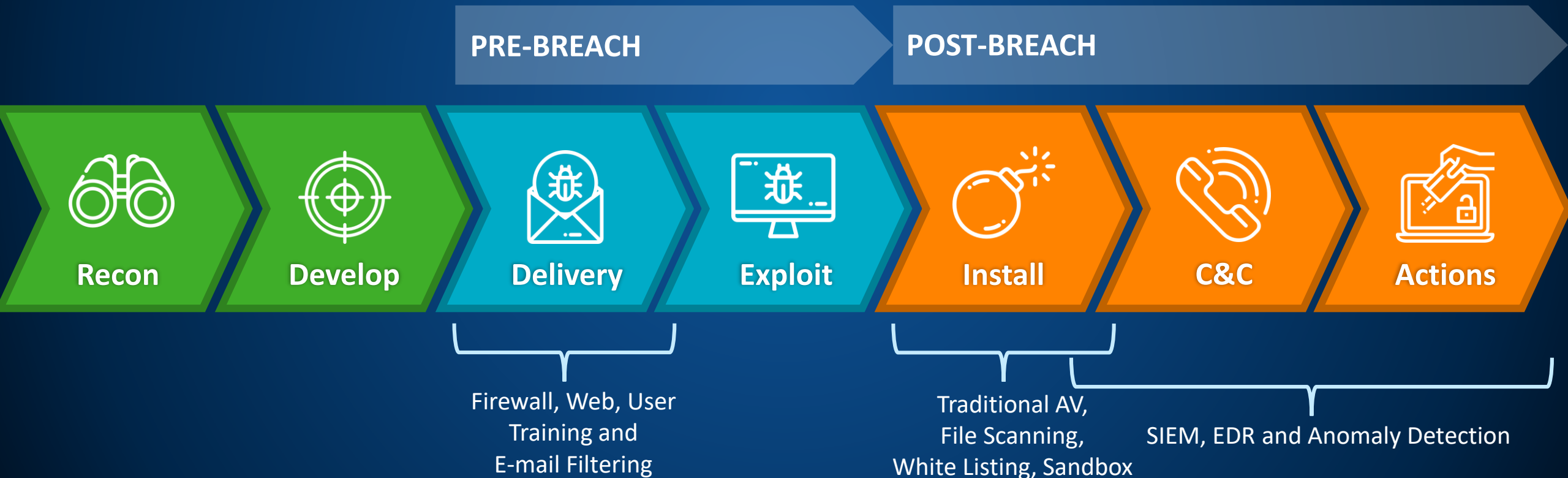
SOPHOS

Anatomy of an Attack – The Cyber Kill Chain



Anatomy of an Attack

Cyber Kill Chain



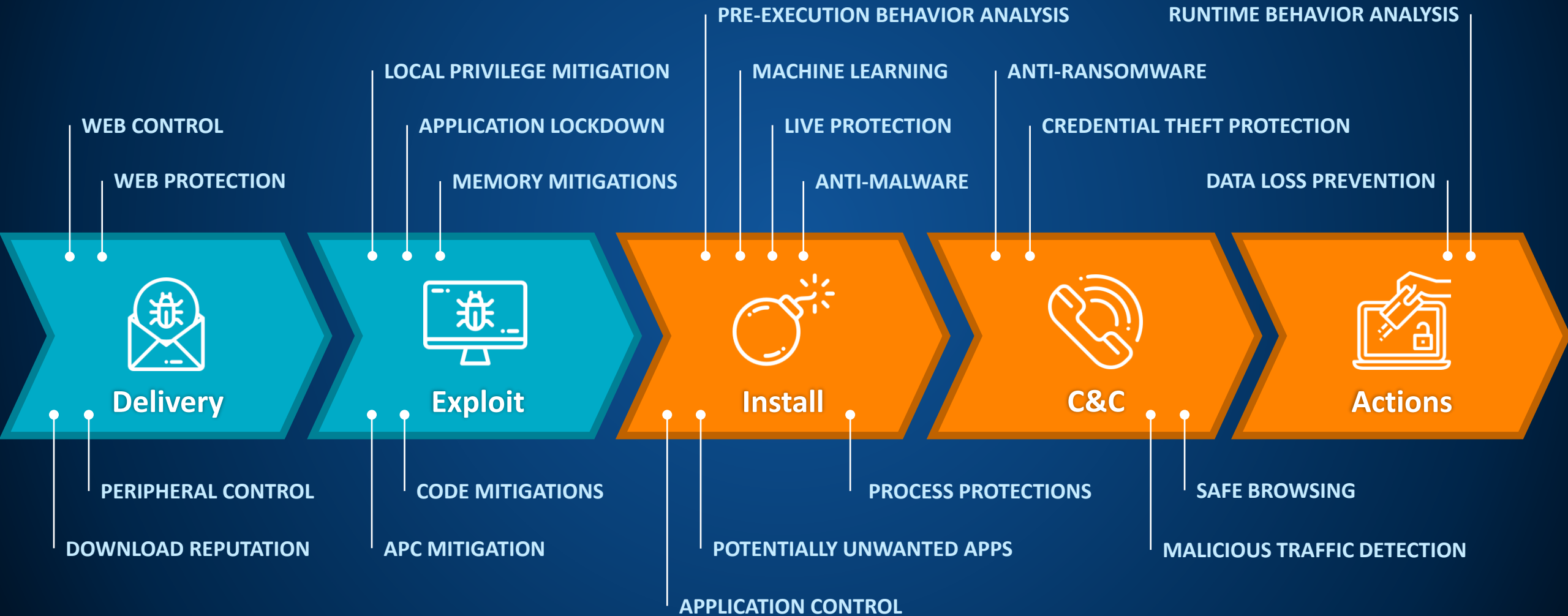
Layered Defense

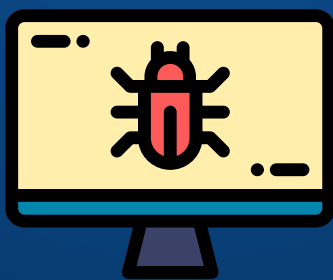
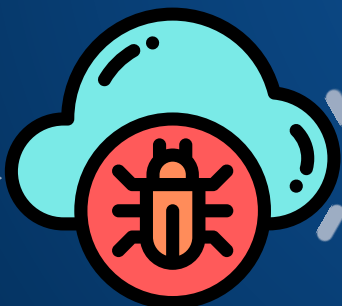
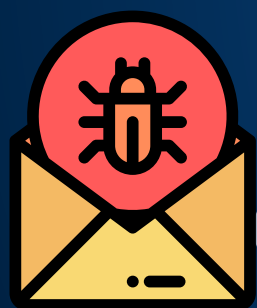
Intercept X Advanced with EDR

SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Threat Cases
Sophos Clean M with SafeStore

DETECT & RESPOND
AI Expert Insights
Cross-Estate Hunting
SophosLabs Threat Intelligence







SOPHOS

INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

Modern Attack Solution – Intercept X

Unknown Threats

Protect Against the Unknown

- Deep Learning Behavior Model
- Signatureless Exploit Prevention
- Malicious and Benign identification
- Tiny Footprint & Low False Positives

~~UNKNOWN
THREATS~~

*No User / Performance Impact
No File Scanning
No Signatures*

Crypto-Ransomware

Stop Ransomware

- Behavioral Based Conviction
- Blocks Encryption and Boot Attacks
- Automatically Reverts Affected Files
- Identifies Source of Attack

~~CRYPTO
RANSOMWARE~~

*Prevent Ransomware Attacks
Roll-Back Changes
Attack Chain Analysis*

Real-Time Attacks

Deny the Hacker

- Protects against Real-Time Breaches
- Stops Credential Harvesting Attacks
- Prevents Persistence Techniques
- Blocks APC and Process Attacks

~~EVASIVE
HACKER~~

*Prevent 'Land and Expand'
Protect Login Credentials
Expose Hackers in plain sight*

SOPHOS
INTERCEPT



NOW WITH
EDR

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

BENIGN

BENIGN

THE
GAP

THE GAP

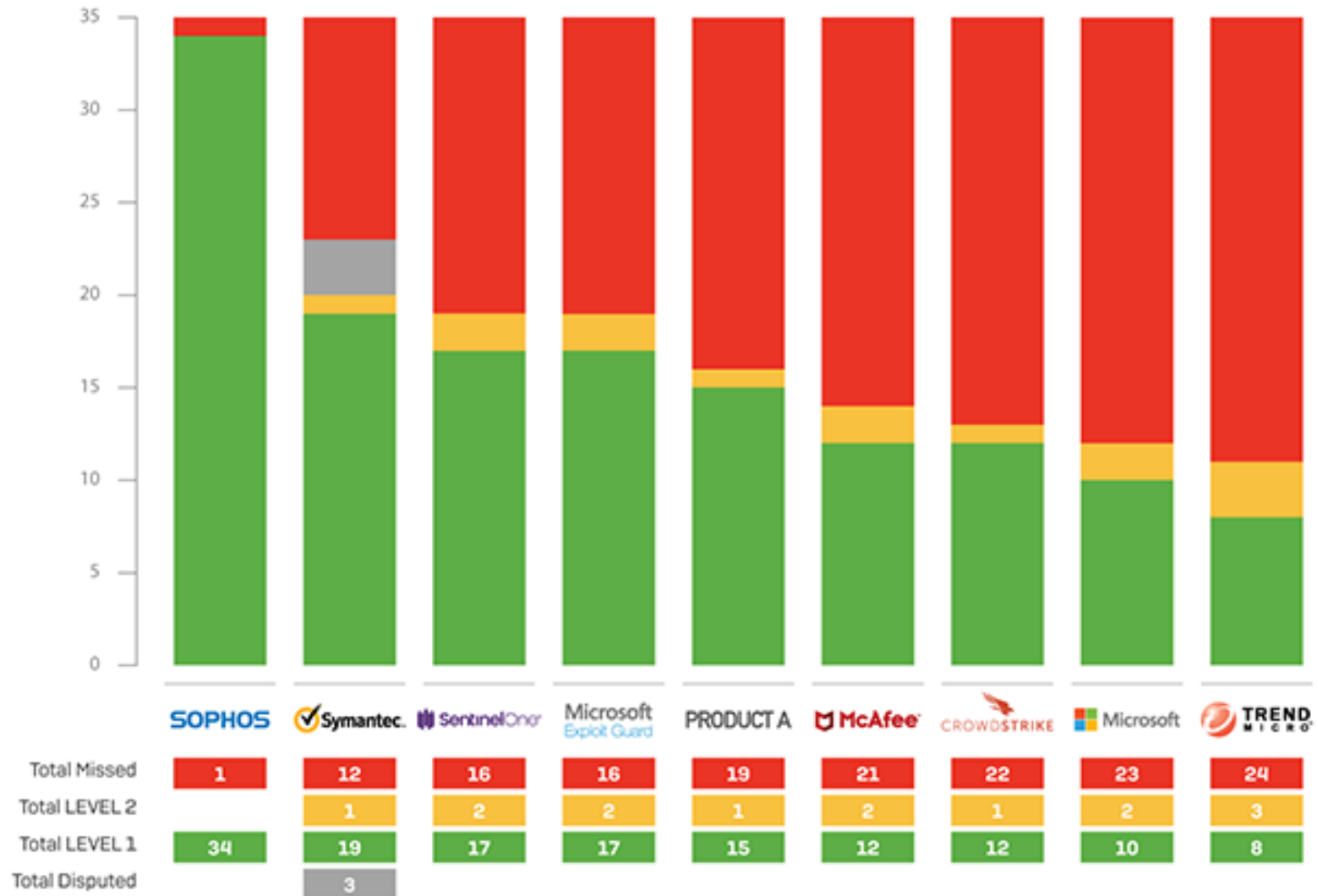
MALICIOUS

MALICIOUS

“Traditional”
EDR

SOPHOS
INTERCEPT
NOW WITH EDR

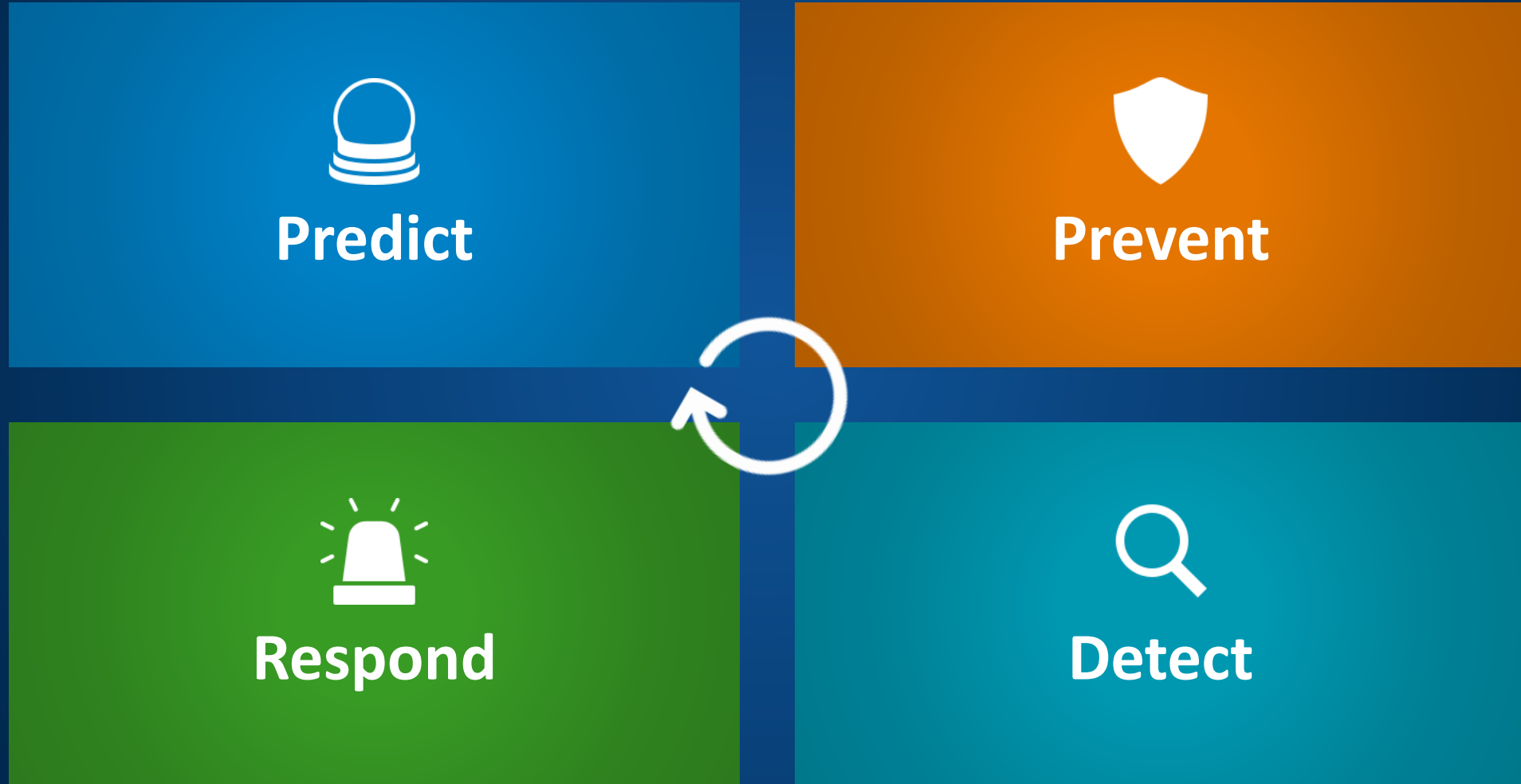
Exploit Protection Test Results



Best protection and lowest TCO in the industry



Adaptive Security Architecture



What is EDR?

It's **not** a switch you flick on or a dial you set and forget about.



It is a **process** of using a multiple features/tools to **detect** potential threats and **respond** to them.

EDR is something you **do**.

BANK
\$£€



Synchronized Security



◀◀ REW

BANK
\$£€



Endpoint Detection
& Response

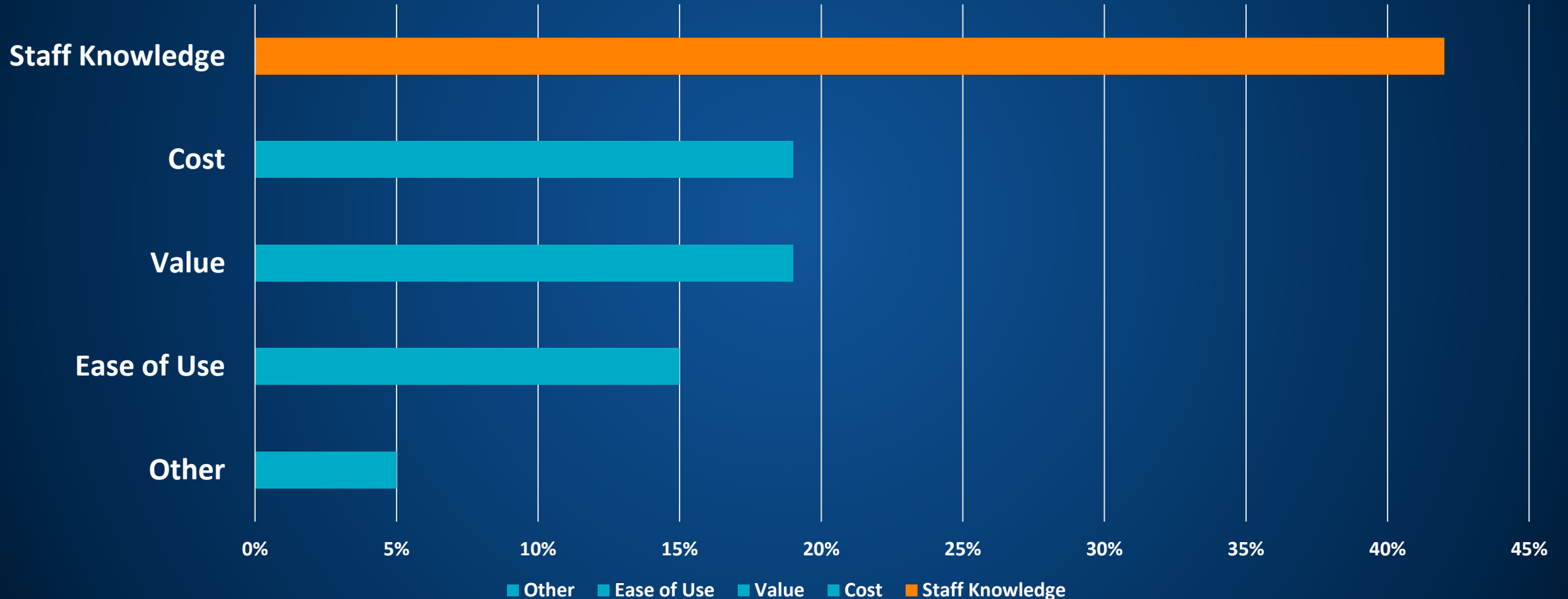


Sophos Labs
Threat
Intelligence



Staff knowledge is the largest barrier to EDR adoption

Top reasons why organization does not have EDR



Security Analysis

Prioritized threat indicators and threat hunting

Suspicious Executables

[Suspicious Executable History](#)

Search



All categories

Executed or not

	First Seen	File name	SHA	Category	Threat score	Endpoints affected
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R02FJHU.exe	575316f0fa...	PUA	92	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R03B930.exe	05ec4f1727...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R03F6G7.exe	f4102513ed...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R06XM4W.exe	3e381dac00...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R07C607.exe	8be459816d...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R07EE4D.exe	26611d888c...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R07S7X0.exe	677e61cb8a...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R095ULR.exe	94fbd8fa22...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R09AT12.exe	dcd699674e...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R09K5US.exe	33389b7c44...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R09K8UR.exe	c928261ef9...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R0AHKRU.exe	6a8e3388bf...	PUA	90	1
<input type="checkbox"/>	Oct 25, 2018 3:...	\$R0DB7RV.exe	12a1dae840...	PUA	90	1

Threat Intelligence Analysis

Access on-demand threat intelligence curated by SophosLabs



Search

Clean and block

[What does this do?](#)

Process details : recipeaddictstool.exe

Process details

Report summary

Machine learning analysis

File properties

File breakdown

Reputation at time case was created:

Uncertain



Known bad reputation

Known good reputation

Detection status: Not detected at time case was created

You should investigate this item to determine whether it is harmful.

SOPHOSLABS Threat Intelligence

Current report created: Sep 25, 2018 7:32 PM

Request Latest Intelligence

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. [Learn More](#)

Path:

c:\users\martynroberts\downloads\recipeaddictstool new 25 09 2018\recipeaddictstool.exe

Name:

recipeaddictstool.exe

Process ID:

592

SHA-256:

5e147d105b93a01b0f756f2afd2f44a8a27914c42d948c0e3051a2db3657c453

Start Time:

Sep 26, 2018 2:49 AM

Malware Analysis

Analyzing files using Deep Learning

> Search for item Clean and block
What does this do?

Process details: dropper.exe

Process details Report Summary **Machine learning analysis** File properties File breakdown

SOPHOS LABS Threat Intelligence Current report created: Jun 06 2018 12.45pm

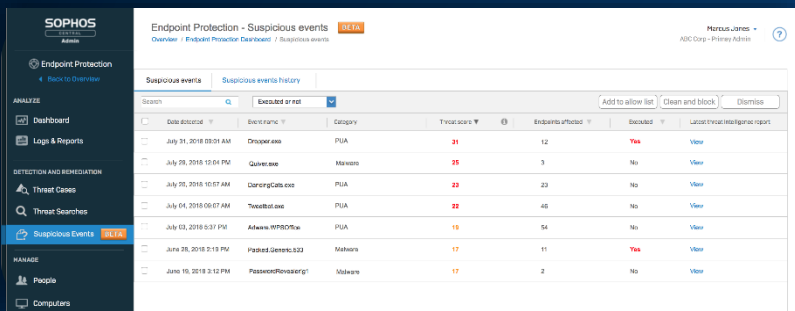
Attributes ⓘ **87% suspicious** Over 52 million known good and 61 million know bad items analysed

Attribute of Dropper.exe	Seen in: Known bad files	Known good files
ⓘ Not signed	4.3 Million	1.0 Million
ⓘ Unknown packs	500 K	205 K
ⓘ Tiny code section	1.0 Million	1.0 Million
ⓘ No icon	2.1 Million	980K
ⓘ Uses encryption	86K	2 K

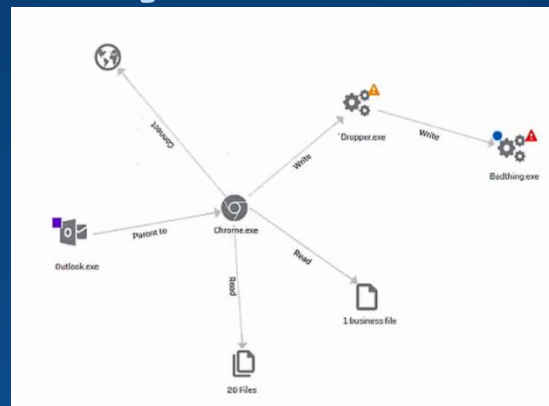
Code similarity ⓘ **82% suspicious** Over 52 million known good and 61 million know bad items analysed

File	Similarity
⚙️ Dropper.exe	99%
❗ x69.exe	96%
✅ TradeStationForms.exe	95%
❗ ioquake3.x86_64.exe	89%
❗ X1ServiceHost.exe	85%
✅ miaa.exe	

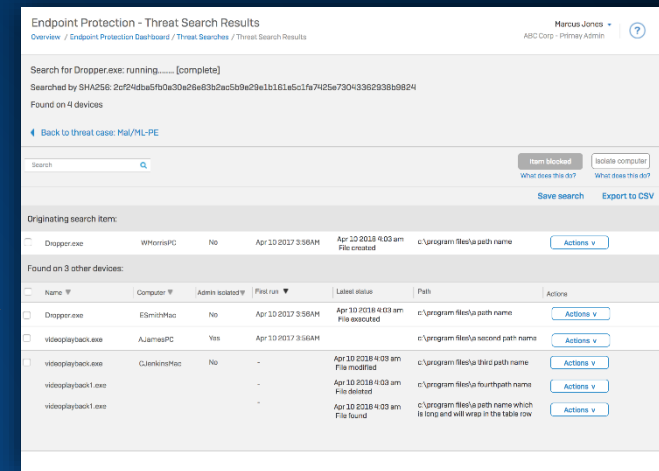
Day in the Life of an Analyst



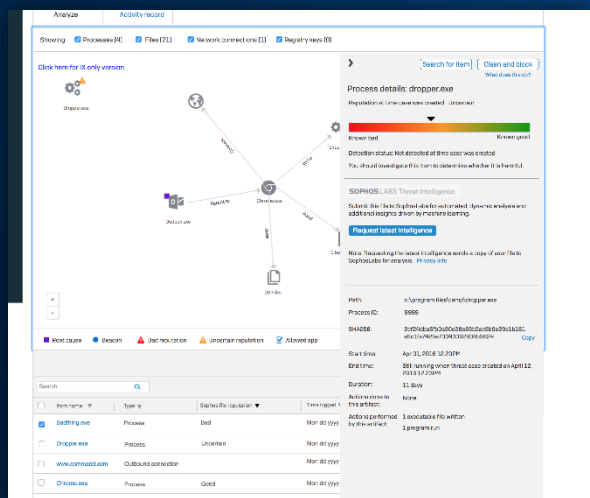
Identifies top incident as Dropper.exe via Threat Indicators*



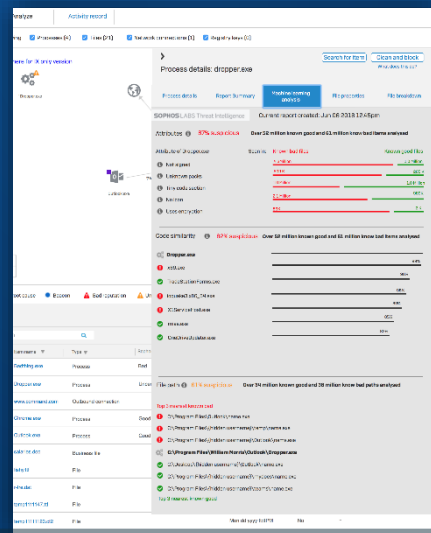
Sees Dropper.exe distributed malware (which was blocked)



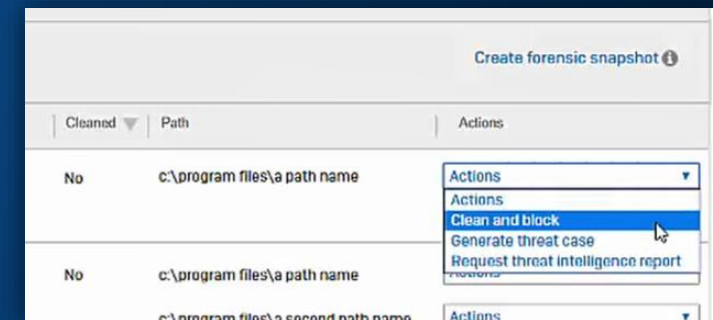
Determines where else Dropper.exe exists



Requests more details from SophosLabs

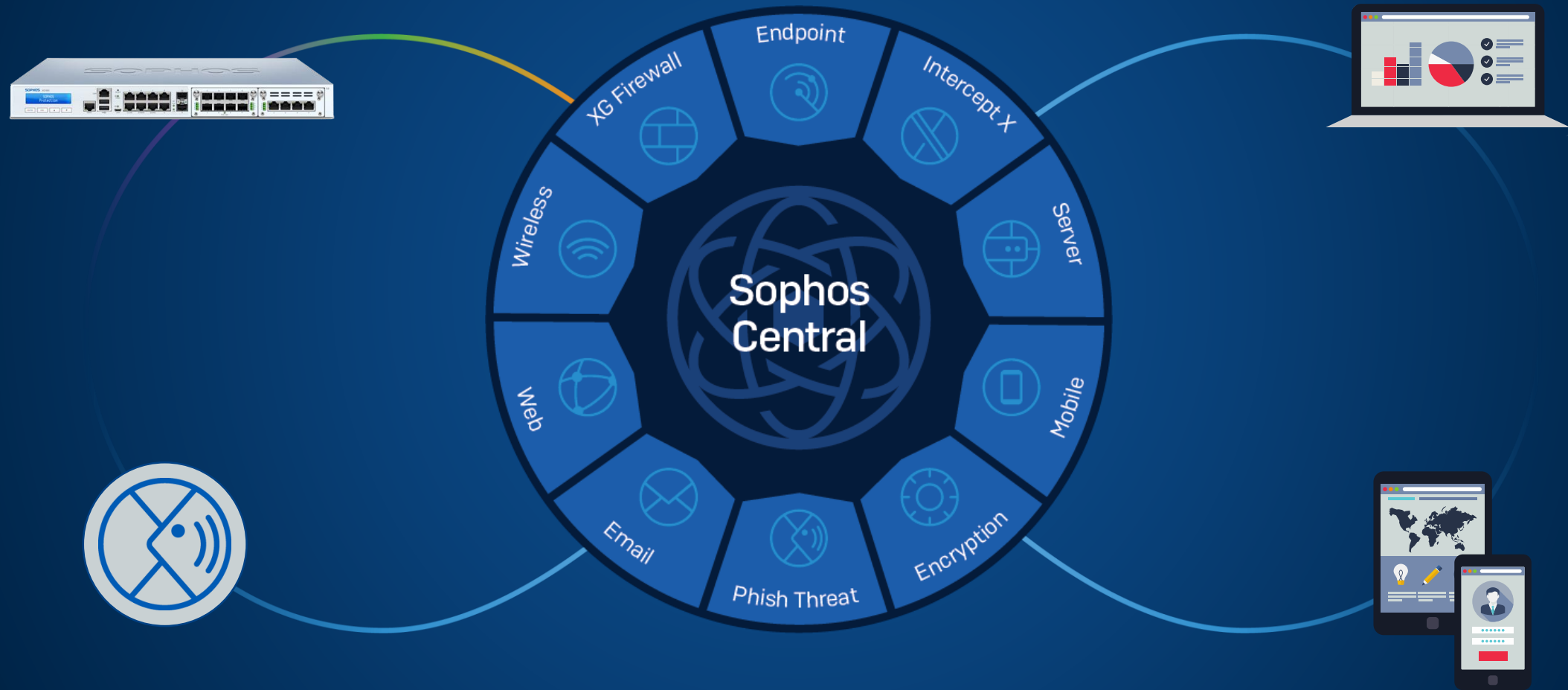


Uses Deep Learning to determine file is malicious



Remediates threat "Clean and block"

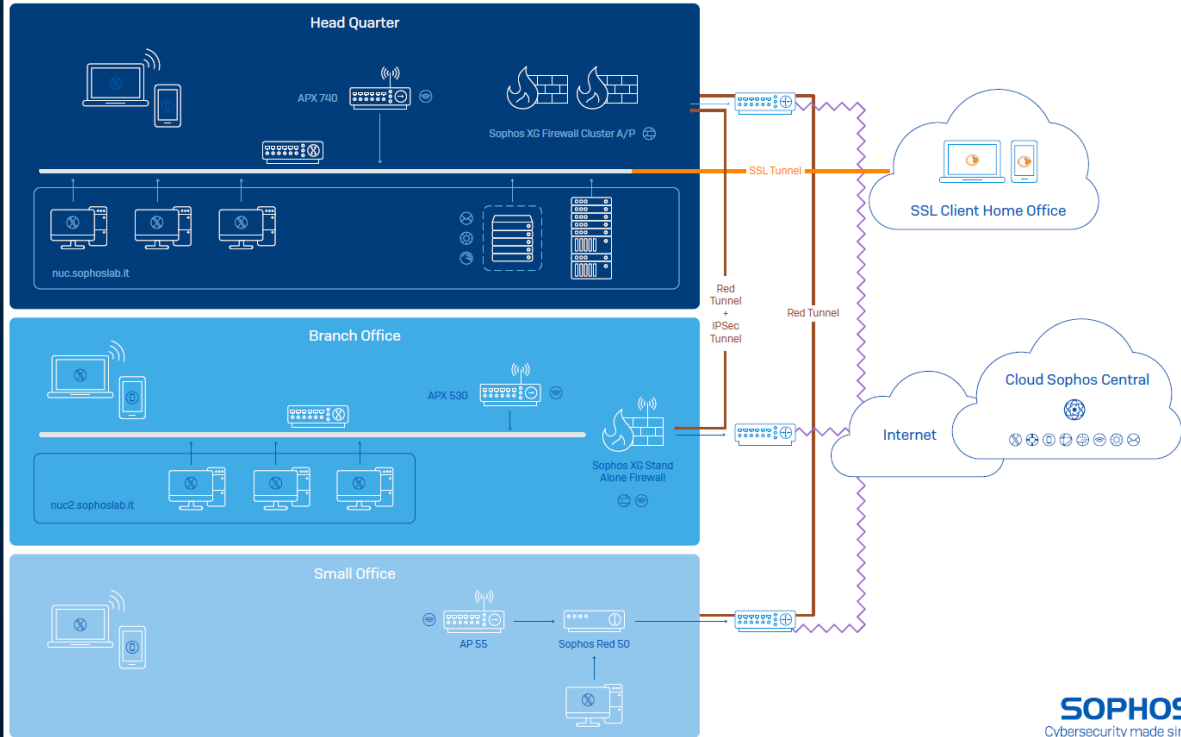
All Managed Through Sophos Central



Demo Room



IT Network Architecture





Demo

