THE BEST JUST GOT BETTER

SOPHOS INTERCEPT X

NOW WITH EDR

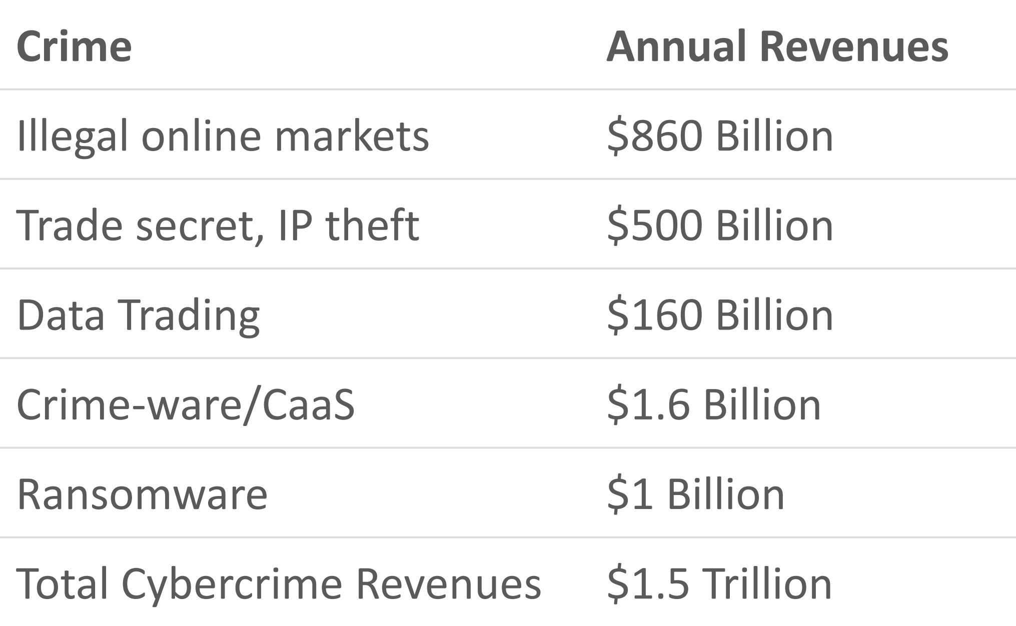
- Dean Shroll - Director Sales Engineering, Central
- Ryan Archer - Director Sales Engineering, East

SOPHOS

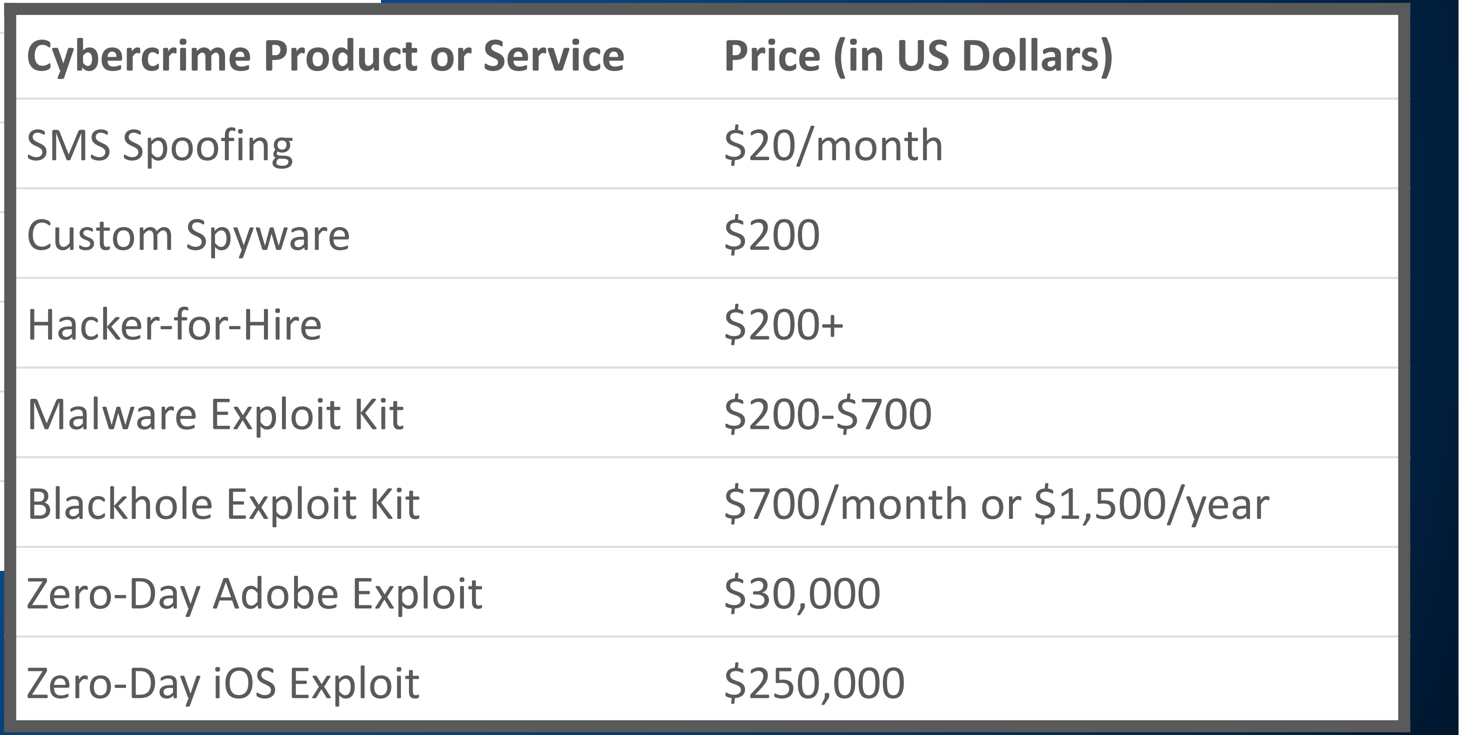
Deconstructing the Threat landscape

Cyber Crime Revenues

Cybercrime will generate at least $1.5 trillion this year



Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware/CaaS	$1.6 Billion
Ransomware	$1 Billion
Total Cybercrime Revenues	$1.5 Trillion



Cybercrime Product or Service	Price (in US Dollars)
SMS Spoofing	$20/month
Custom Spyware	$200
Hacker-for-Hire	$200+
Malware Exploit Kit	$200-$700
Blackhole Exploit Kit	$700/month or $1,500/year
Zero-Day Adobe Exploit	$30,000
Zero-Day iOS Exploit	$250,000

https://www.thesslstore.com/blog/2018-cybercrime-statistics/

Continued rapid growth in new malware

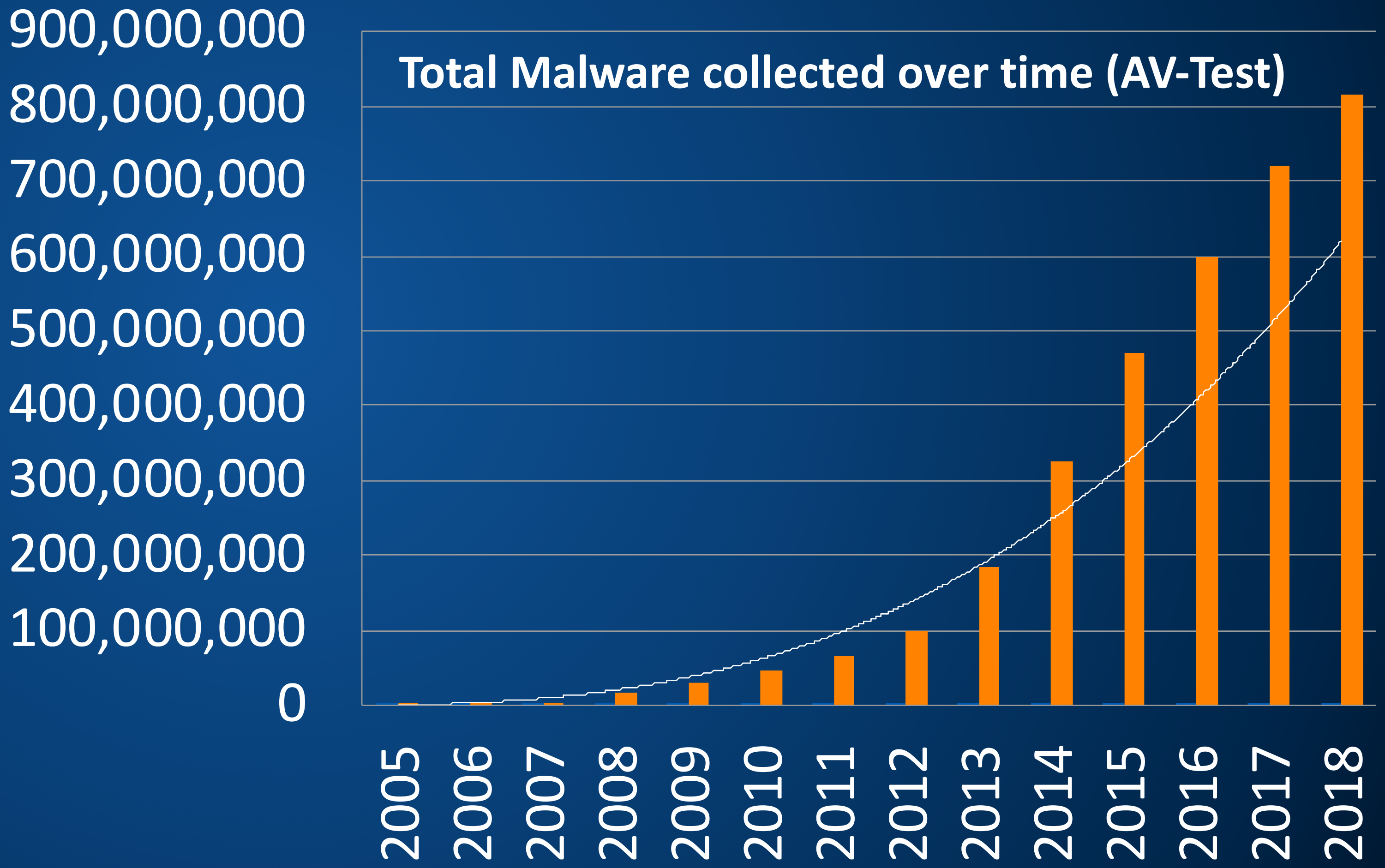
By the end of 2019 over 1 Billion unique malware samples will exist

The Volume of malware is staggering

1990’s - Signature based Anti-Virus

- 1-1 map of ‘checksums’ to malware
- String Scanning

Requires a Victim to report the malware so a new signature can be built

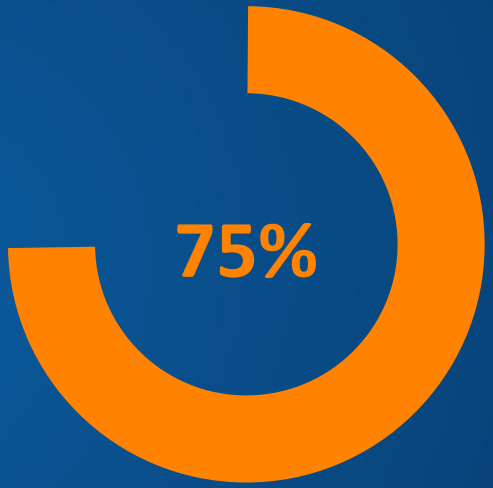

Total Malware collected over time (AV-Test)

SOPHOS

The age of single-use disposable malware

400,000

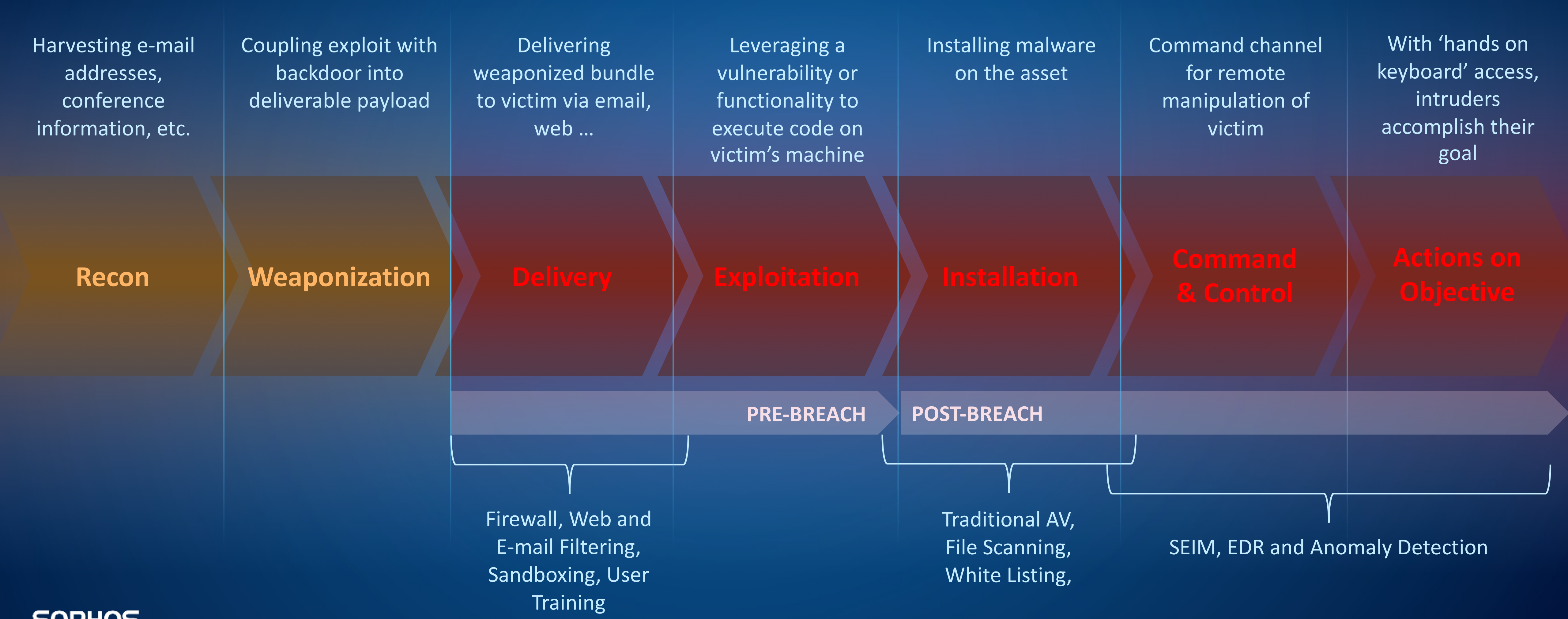
Sophos Labs receives and processes **400,000** previously unseen malware samples each day.



75% of the malicious files SophosLabs detects are found only within a single organization.

2018 Threat Space Change – Kill Chain Compression

- (Cyber Kill Chain)



Harvesting e-mail addresses, conference information, etc.

Recon

Coupling exploit with backdoor into deliverable payload

Weaponization

Delivering weaponized bundle to victim via email, web …

Delivery

Leveraging a vulnerability or functionality to execute code on victim's machine

Exploitation

Installing malware on the asset

Installation

Command channel for remote manipulation of victim

Command & Control

With 'hands on keyboard' access, intruders accomplish their goal

Actions on Objective

PRE-BREACH

POST-BREACH

Firewall, Web and E-mail Filtering, Sandboxing, User Training

Traditional AV, File Scanning, White Listing,

SEIM, EDR and Anomaly Detection

Emotet

“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.”

Source:

US CERT

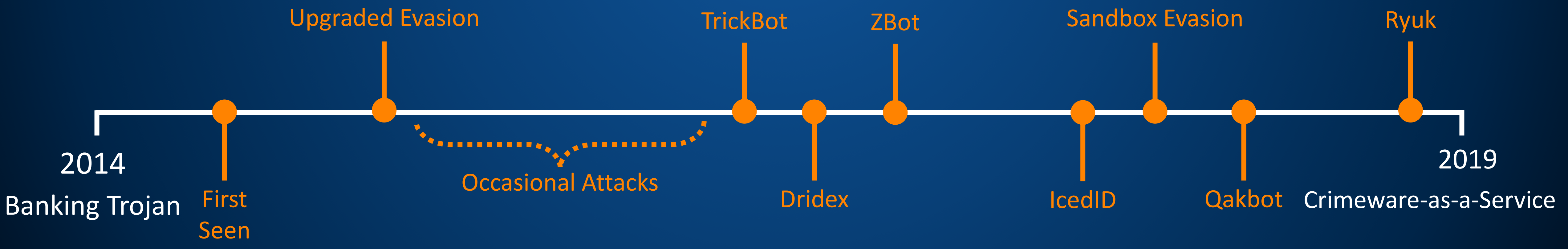
https://www.us-cert.gov/ncas/alerts/TA18-201A

First reported in 2014

EMOTET

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

U.S. Department for Homeland Security, 2018


2014
Banking Trojan

First Seen

Upgraded Evasion

Occasional Attacks

TrickBot

Dridex

ZBot

IcedID

Sandbox Evasion

Qakbot

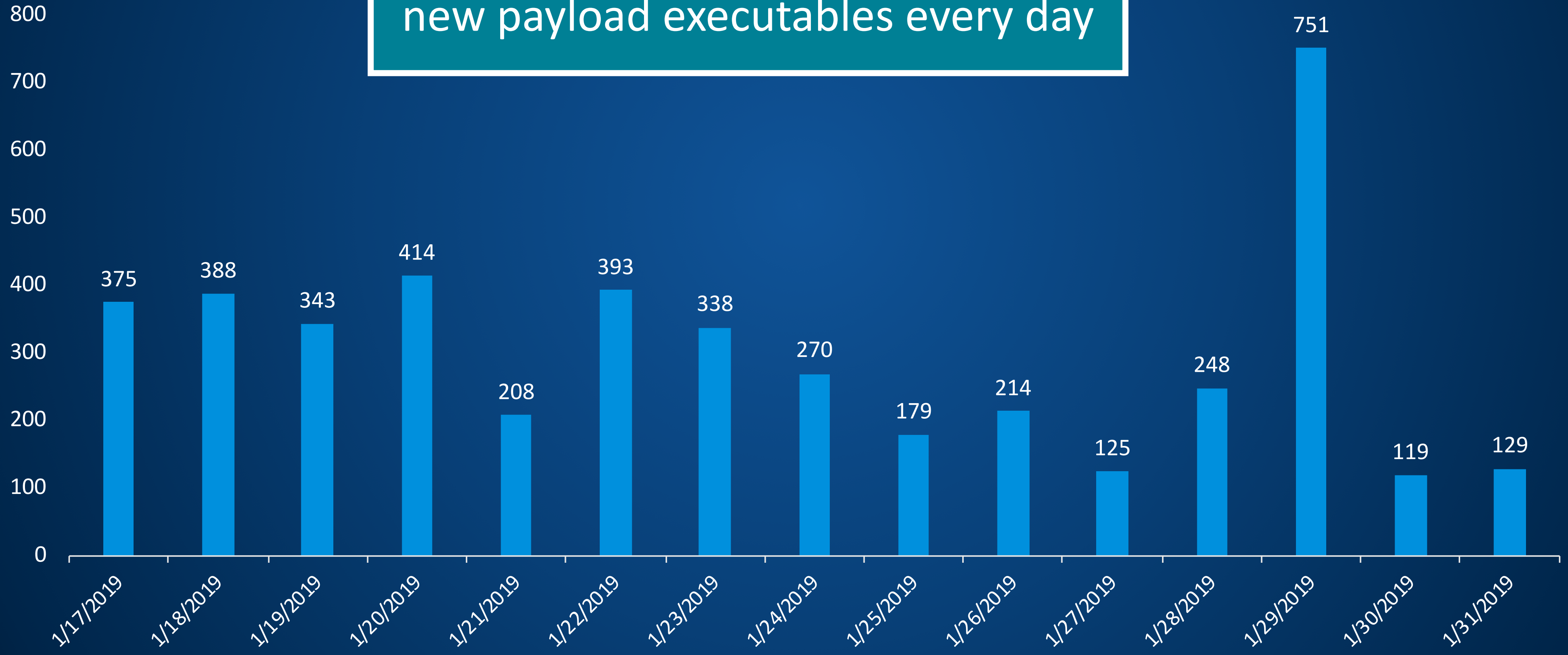
Ryuk

2019
Crimeware-as-a-Service

Emotet payloads change constantly

300

new payload executables every day

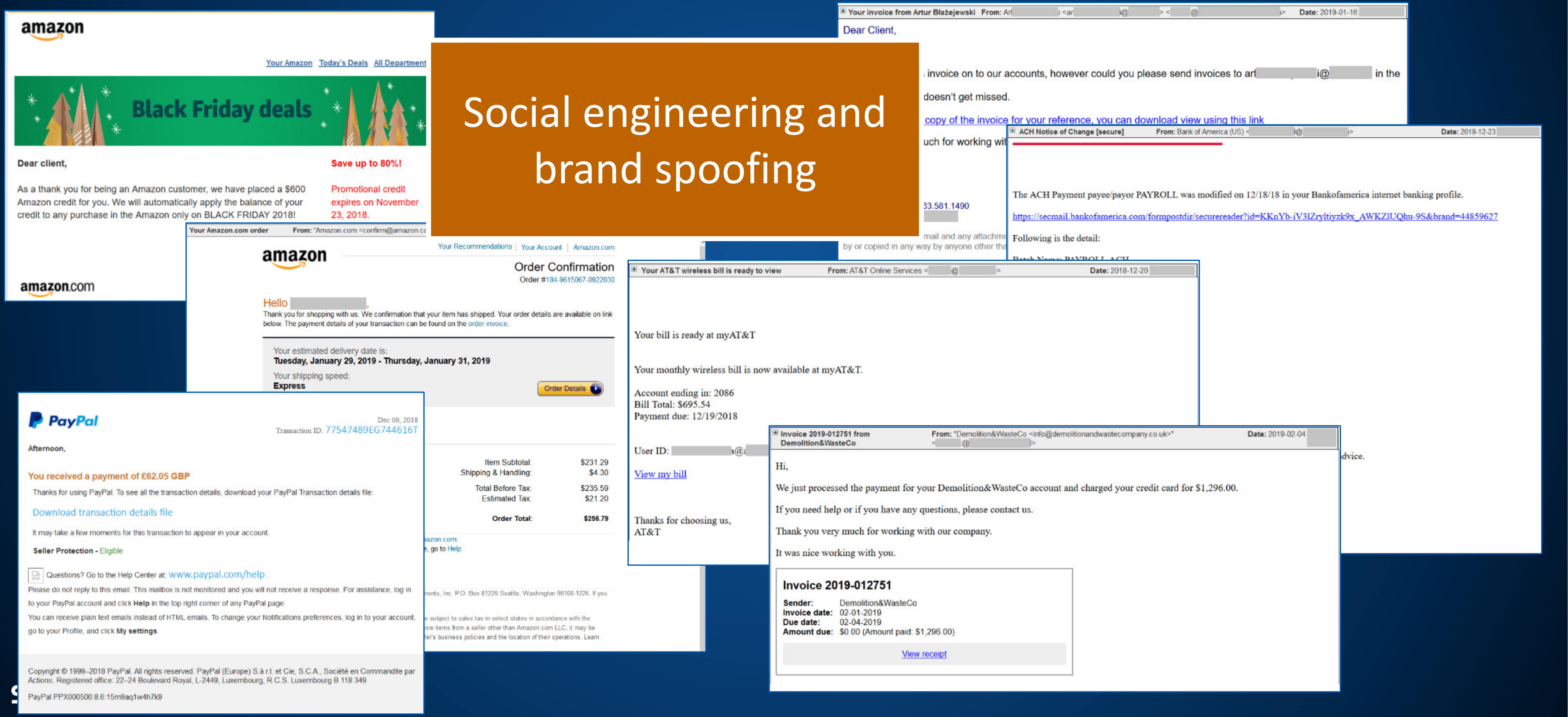


# of unique Emotet payload executables seen by SophosLabs

SOPHOS

Usually Starts with Spam

Social engineering and brand spoofing



amazon

Your Amazon | Today's Deals | All Department

Dear client,

Save up to 80%!

As a thank you for being an Amazon customer, we have placed a $600 Amazon credit for you. We will automatically apply the balance of your credit to any purchase in the Amazon only on BLACK FRIDAY 2018!

Promotional credit expires on November 23, 2018.

amazon.com

Your Amazon.com order **From:** "Amazon.com <confirm@amazon.cc

amazon

Your Recommendations | Your Account | Amazon.com

Order Confirmation

Order #184-9615067-0922030

Hello [redacted],

Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link 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

Order Details

Item Subtotal:	$231.29
Shipping & Handling:	$4.30
Total Before Tax:	$235.59
Estimated Tax:	$21.20
Order Total:	**$256.79**

nazon.com.
e, go to Help

nents, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you

e subject to sales tax in select states in accordance with the
ore items from a seller other than Amazon.com LLC, it may be
ller's business policies and the location of their operations. Learn

PayPal

Dec 06, 2018
Transaction ID: 77547489EG744616T

Afternoon,

You received a payment of £62.05 GBP

Thanks for using PayPal. To see all the transaction details, download your PayPal Transaction details file:

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

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

Dear Client,

invoice on to our accounts, however could you please send invoices to art[redacted]i@[redacted] in the

doesn't get missed.

copy of the invoice for your reference, you can download view using this link

uch for working wit

63.581.1490
[redacted]

mail 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:

Batch Name: PAYROLL_ACH

dvice.

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@[redacted]

View my bill

Thanks for choosing us,
AT&T

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

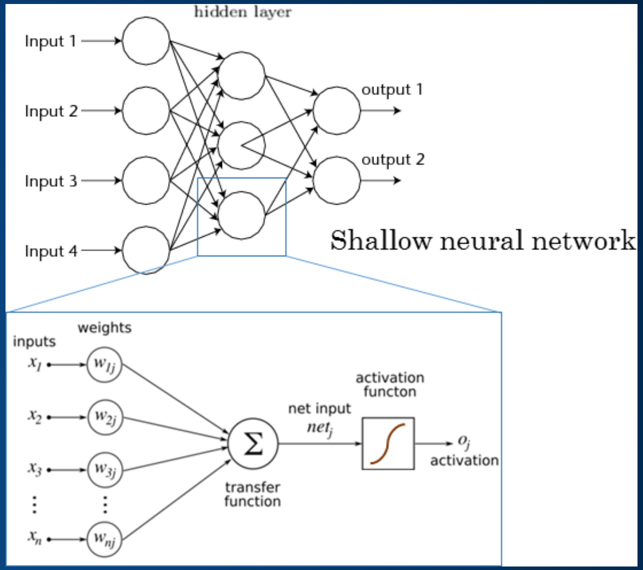
Sender:	Demolition&WasteCo
Invoice date:	02-01-2019
Due date:	02-04-2019
Amount due:	$0.00 (Amount paid: $1,296.00)

View receipt

For example - Deep learning neural network

Faster

- Deep learning detections in 20-100miliseconds per file
- Traditional ML 100-500 milliseconds per file

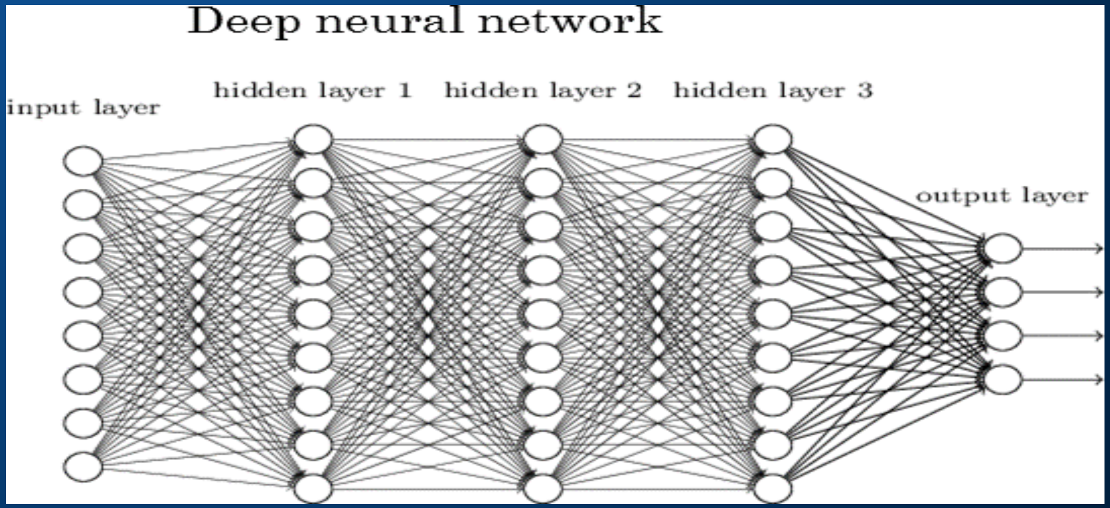


Smaller

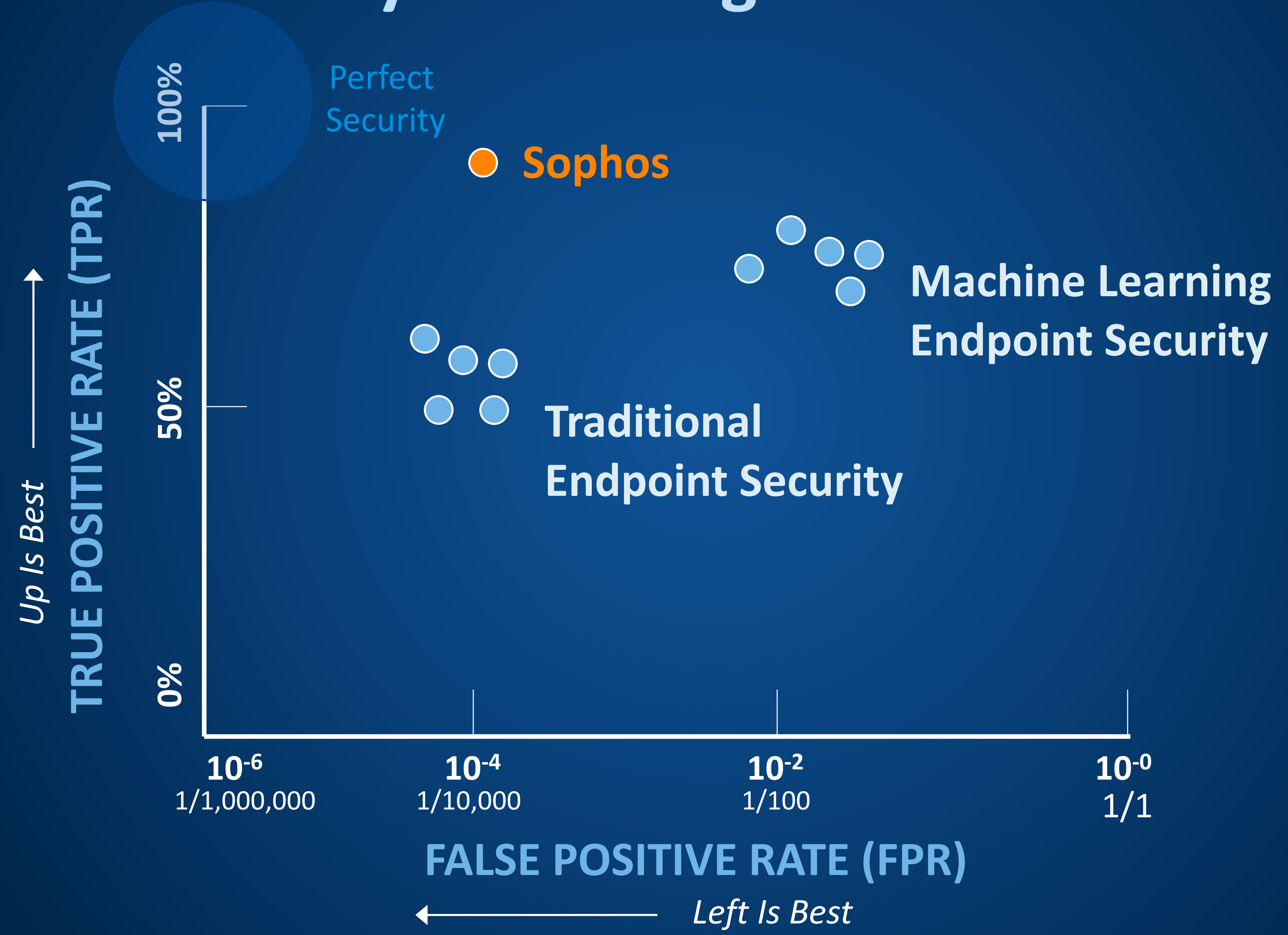
- Deep learning models are about 10-20 MB
- Traditional ML models can get huge 500 MB-10 GB

Smarter

- Deep learning provide proven higher detection rates that improves with more data
- Traditional ML has Lower detection rates and diminishing returns with more data

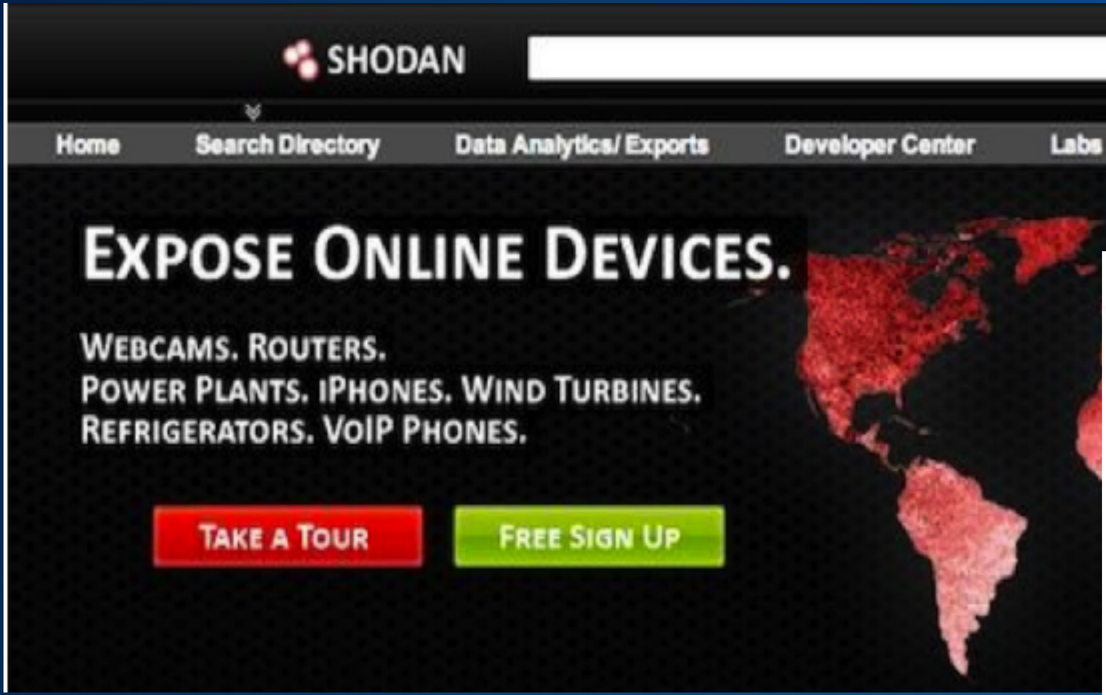


Predictive Security: Detecting Unknown Malware



Source: SophosLabs analysis of malware found in the wild

So how did they steal my RDP password?

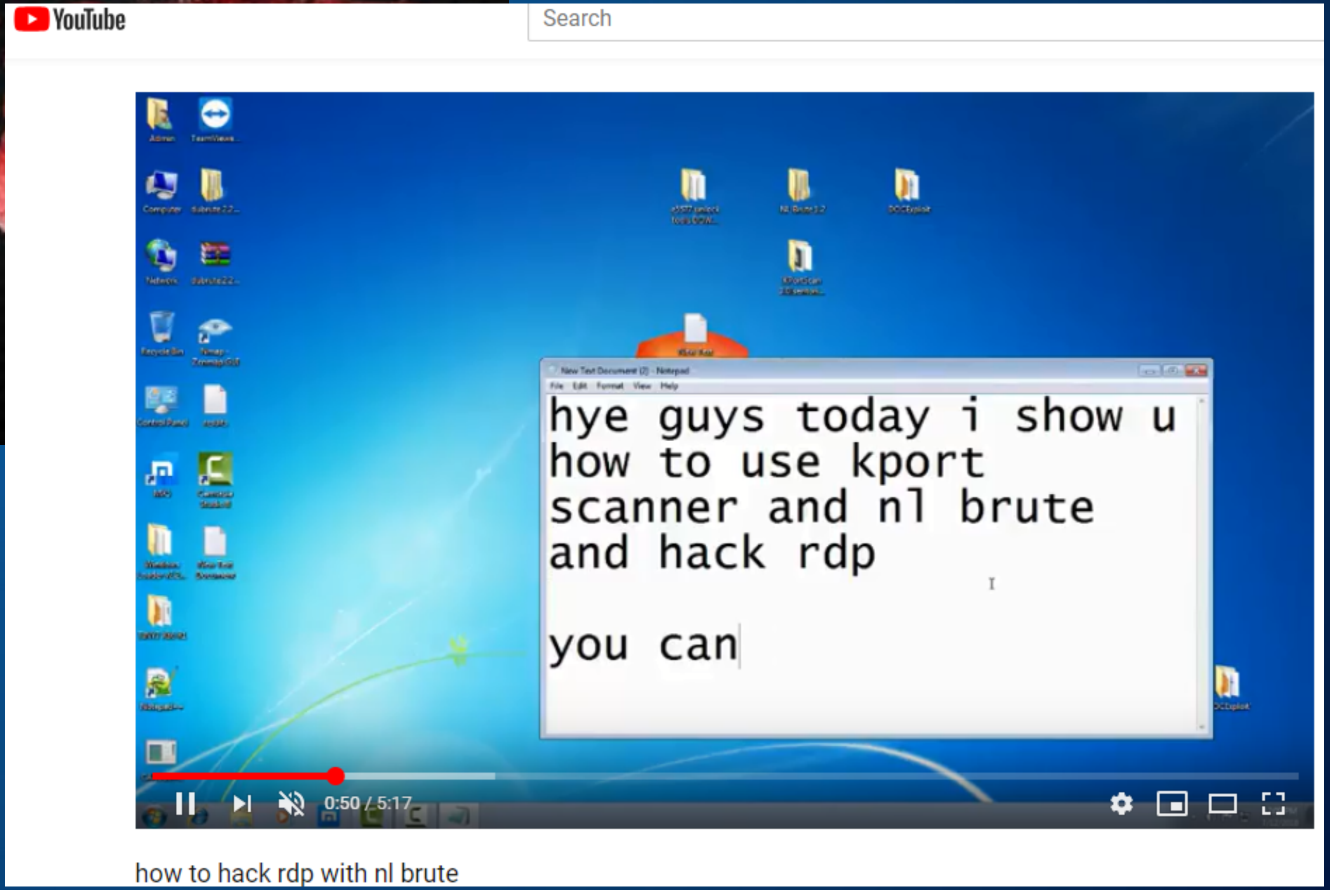


EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

Search the internet for devices that allow RDP authentication

Follow the online video demos on how to brute force RDP with NLBrute



```
hye guys today i show u
how to use kport
scanner and nl brute
and hack rdp

you can
```

how to hack rdp with nl brute

Now that you have an RDP password what

Anonymity

- Use the compromised device for other crimes
- Setup decoys on the device to delay investigators

SPAM Platform

- You have a server under your control, use it to send your spam campaign

Simple data theft

- You have full access, so see if they have anything of value on the box

Harvest more credentials

- Setup a key logger and wait for the user to do something interesting like log into a bank account

Crypto mining

- Start harvesting cryptocurrency using their CPU, electricity and cooling

Deploy ransomware

- As admin uninstall the AV
- Check if you can move laterally to get more boxes
- Encrypt and post the ransom note
- Wait for payment

Endpoint Detection and Response

Why do I need Endpoint Detection and Response?

The core assumption is that your endpoint protection has failed to protect and you need someone to hunt for undetected threats, determine the amount of damage done and take action to recover to a known good state

By its nature EDR is an after the fact capability

Something bad is happening, can I discover it and stop it before more damage is done

61% of Surveyed Hackers Took Less than 15 Hours to Obtain Healthcare Data

(NUIX Black Report - https://www.nuix.com/black-report/black-report-2018)

68% of data breaches take months to discover

(Verizon DBIR 2018 - http://www.verizonenterprise.com/verizon-insights-lab/dbir/)

SOPHOS

What are Endpoint Detection and Response Solutions?

Endpoint Data Recorder + Anomaly and Threat Detection + Investigation Tools + Containment and Recovery

Endpoint Data Recorder

Process activity
Memory
Network
File system
Registry

Anomaly and Threat Detection

Threat intel feeds
Confirmed attacks
Suspect executables
Admin hunting

Investigation Tools

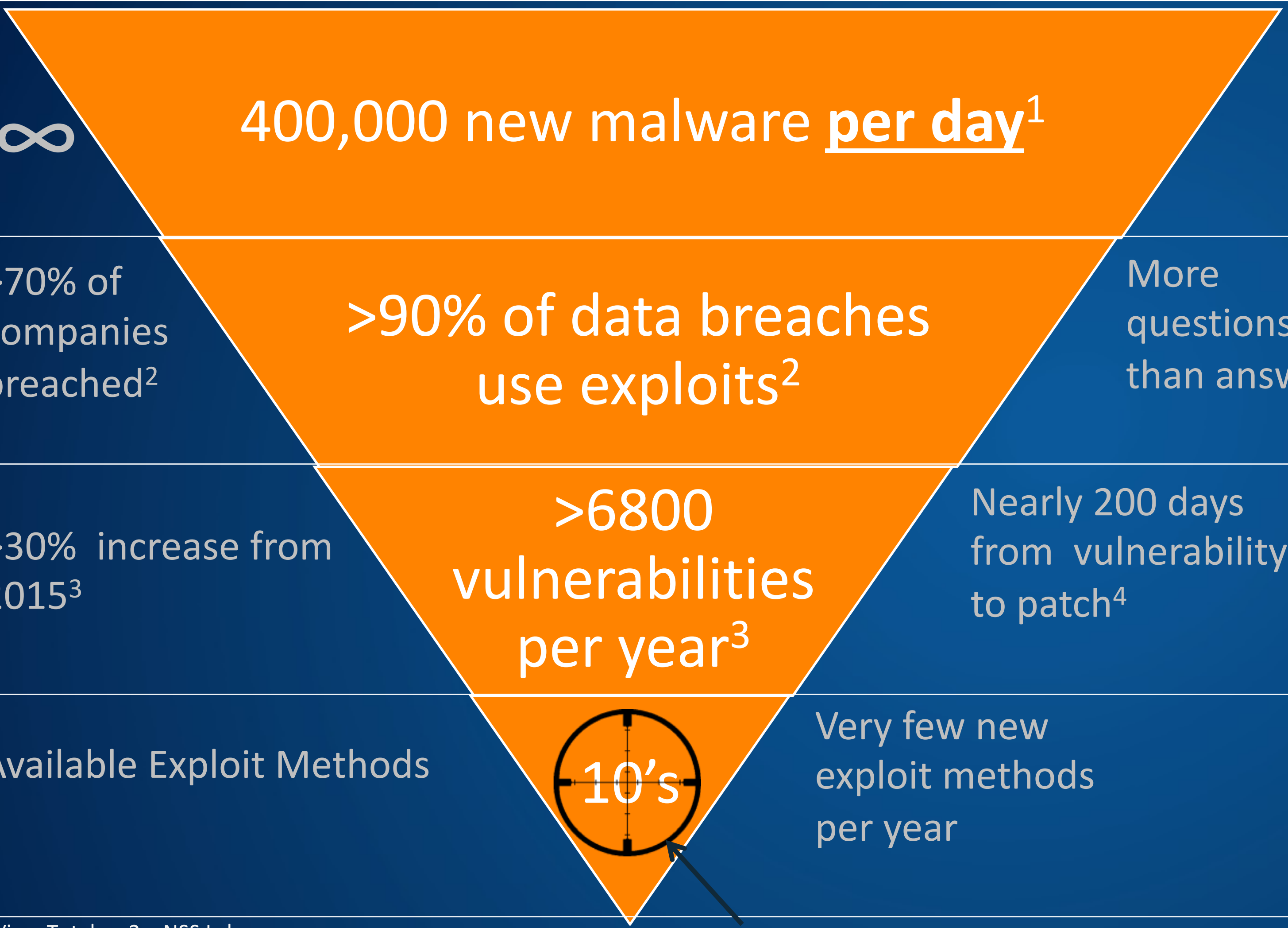
- Situational awareness
  - Who/What/Where/When
  - Assets at risk
  - Scope of attack
- Activity map
- Deep insight
  - File and Device Forensics
  - Reputation

Containment and Recovery

Device Isolation
Quarantine
Removal
Do no harm

Gartner definition - The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record endpoint-system-level behaviors and events (for example user, file, process, registry, memory and network events and store this information either locally on the endpoint or in a centralized database. Databases of known IOCs and behavior analytics techniques are then used to continually search the data to identify early identification of breaches (including insider threats), and to rapidly respond to those attacks. These tools also help with rapid investigation into the scope of attacks, and provide response capability

And how about Exploits



∞

400,000 new malware **per day**[1]

Traditional Anti-Virus

- File Analytics
- Heuristics
- URL Blocking

>70% of companies breached[2]

>90% of data breaches use exploits[2]

More questions than answers

SIEM, EDR, UEBA

- Anomaly Detection
- Security Operations Center
- Forensic breach assessment teams

>30% increase from 2015[3]

>6800 vulnerabilities per year[3]

Nearly 200 days from vulnerability to patch[4]

Patch Management

- Vulnerability Scanning
- Device Management
- Patch testing and deployment

Available Exploit Methods

10's

Very few new exploit methods per year

Anti-Exploit

- Exploit and Ransomware prevention
- Incident Response Report
- Automatic Root Cause Attribution

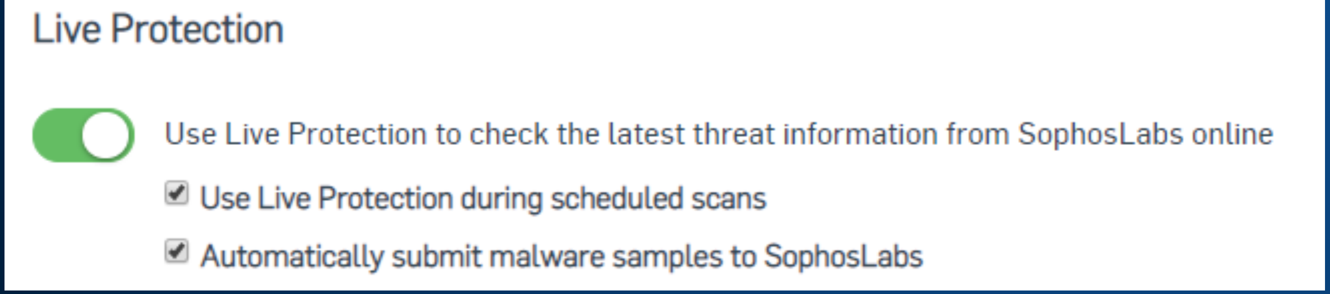
Anti-Exploit – Targets the root of the problem

1 – Virus Total
2 – NSS Labs
3 – Gartner
4 – White Hat Security

SOPHOS

Threat Intelligence Analysis: Threat Intelligence

- Typical EDR products
  - You receive Threat Intel and search the EDR data base for matches
- Intercept X Advanced with EDR
  - Sophos Live Protection
  - Direct search if you still need it

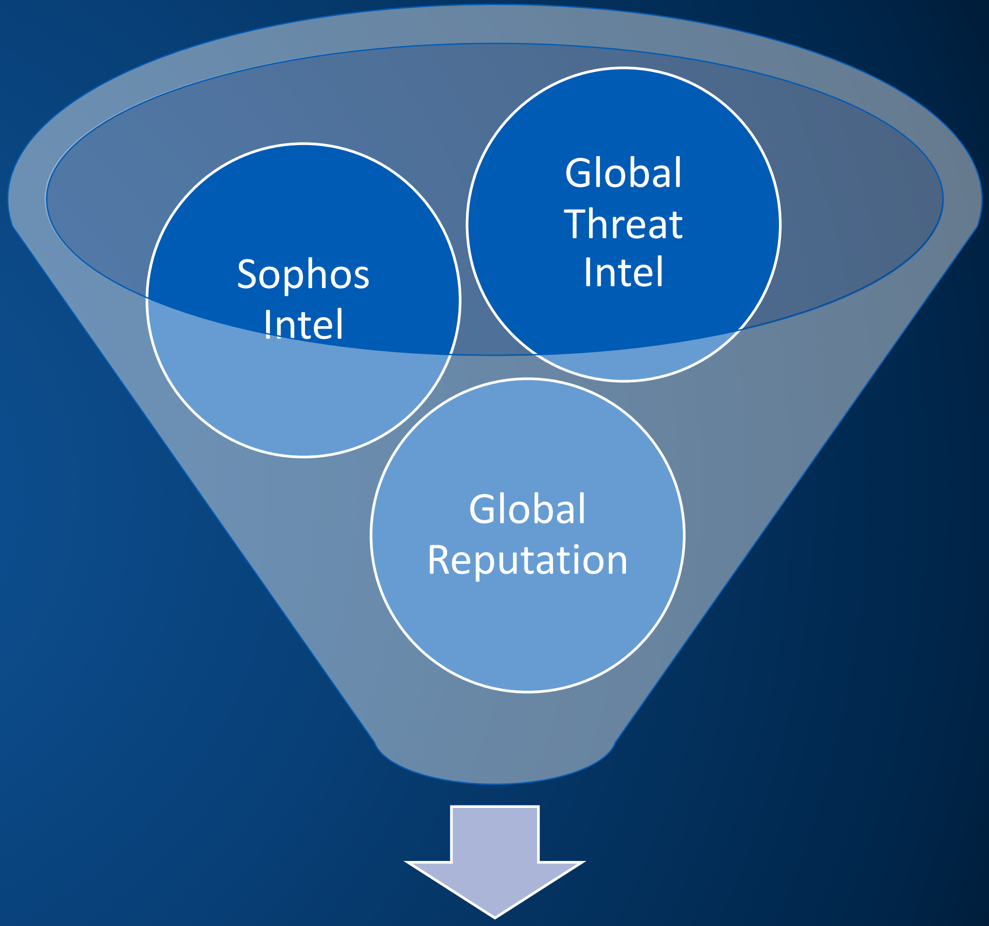


Live Protection

● Use Live Protection to check the latest threat information from SophosLabs online

☑ Use Live Protection during scheduled scans

☑ Automatically submit malware samples to SophosLabs



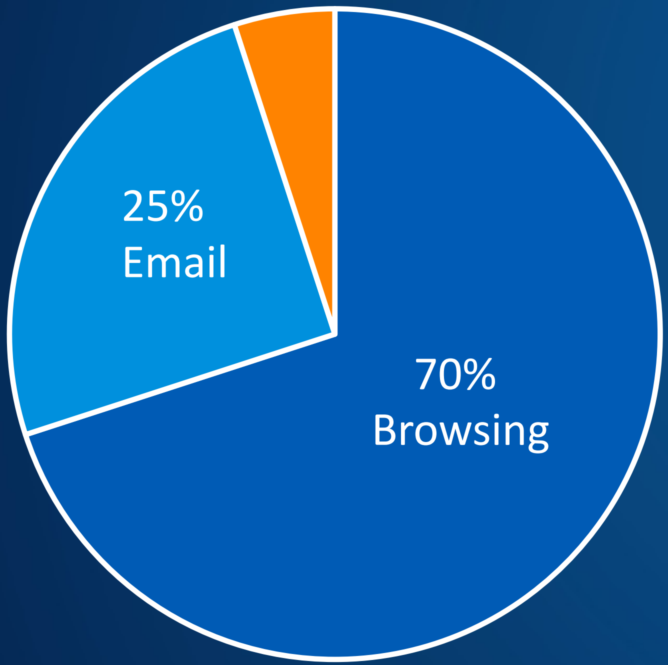
Sophos Live Protect

Threat Vectors, Payloads and Techniques

Infection Vectors

Malicious URLs | Phishing Attacks | Removable Media | Unauthorized Apps

Other 5%



Common Infection Payloads

45% Weaponized Documents

.doc
.xls
.pdf

Non-.exe Malware

- Leverages authorized application to perform malicious activity
- Often uses existing system tools to complete the attack
- May use malformed content to exploit the legitimate application

32% Malicious Executables

.exe Malware

- Frequently packed and obfuscated to avoid traditional signature scans
- May be hidden inside legitimate software
- Often deployed by other malware to establish persistence

15% Malicious Scripts and HTML

Script-based Malware

- Typically Java Script run in the browser
- Includes MSHTA, Powershell, Cmd scripts ect
- Often used to deliver malicious exe or establish connection to C2

Exploit Activity

Exploits (90% of breaches involved an exploit)

Exploits

- Leverages a known or unknown vulnerability to execute code
- Often uses multiple exploit techniques to achieve objective
- May never deploy a file to the device and can stay in runtime memory