Stopping the Threat at the Door

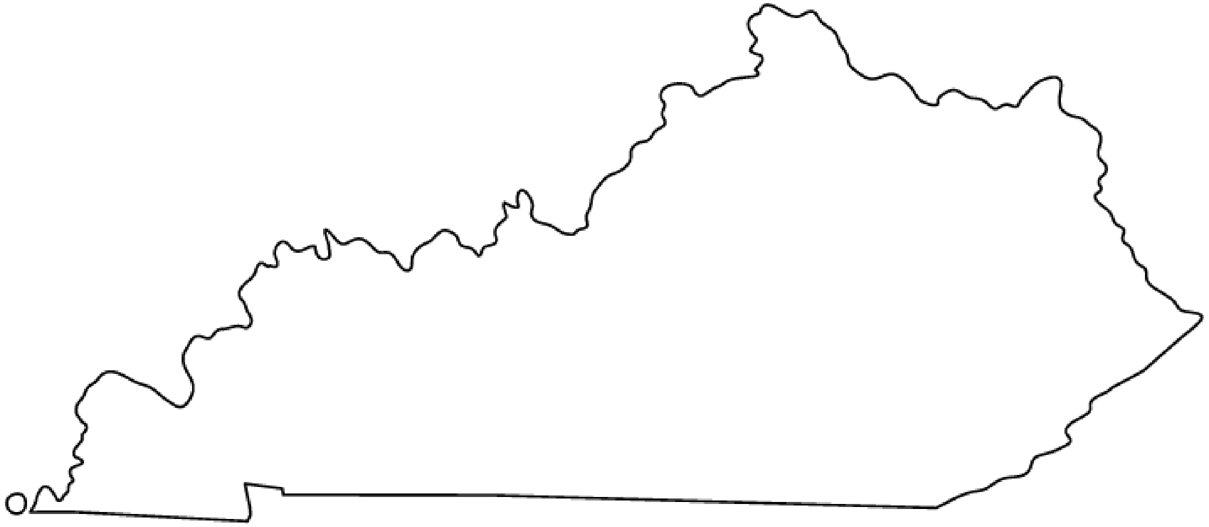
Matt Pannebaker

Sales Engineer – Ohio and Kentucky

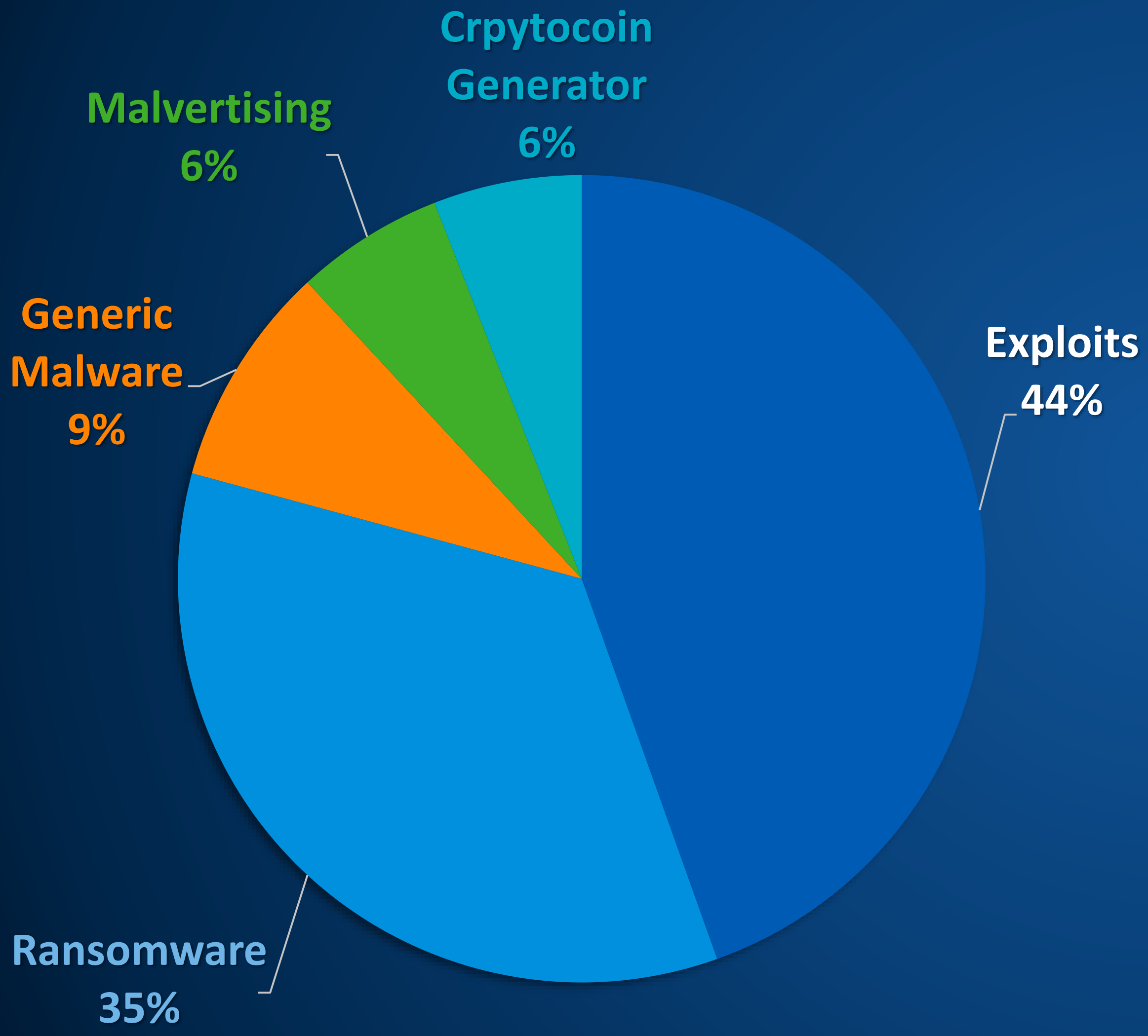
Today

SOPHOS

home



Top Threats in the US



Phishing

- 93% of phishing emails have a ransomware payload (CSO Online)

Exploits

- **Industrialized attacks**
- Flash, Downloader, JS redirect, Malvertising

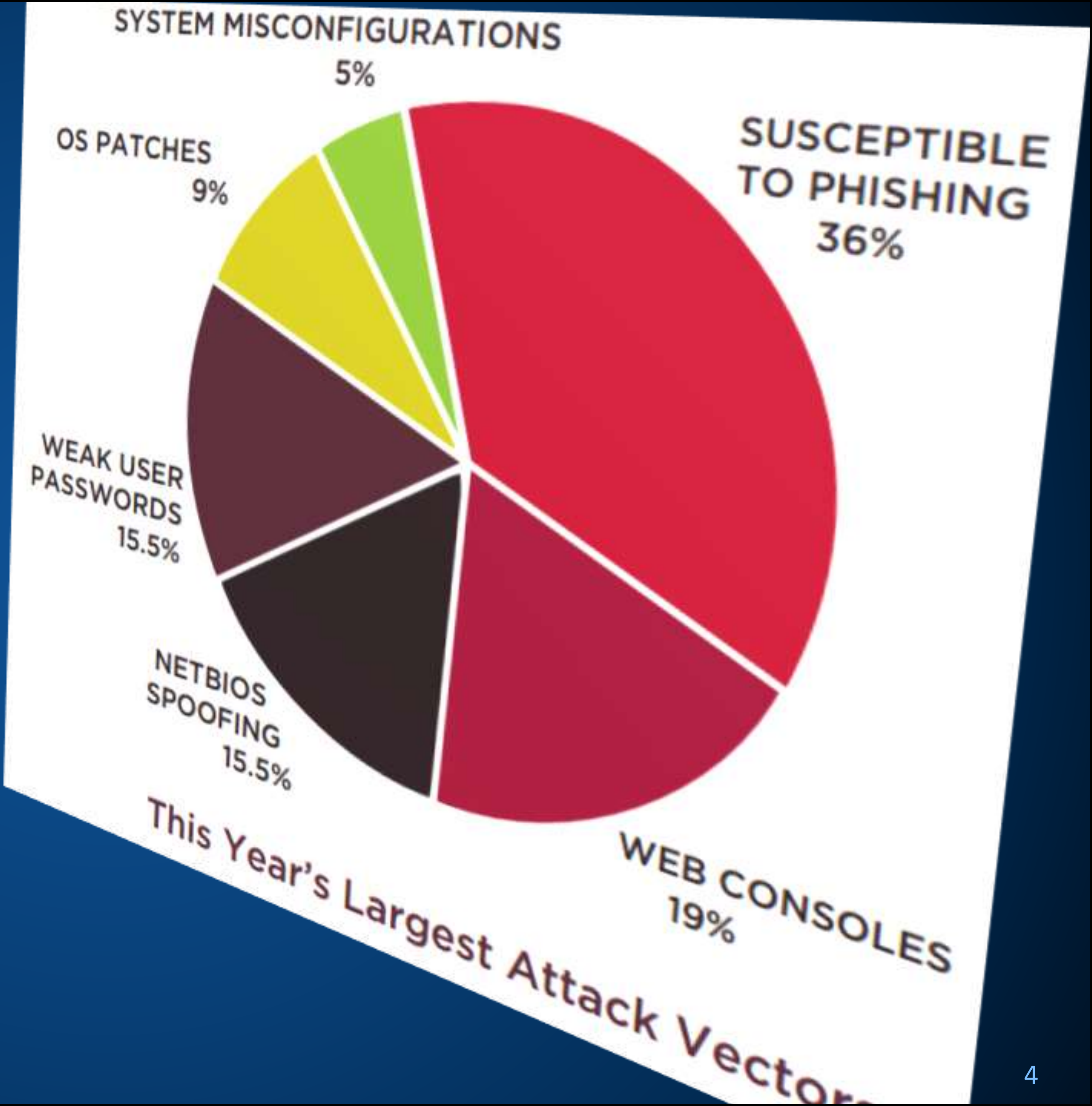
Ransomware

- Dropper, Phish, Shortcut, Doc Macro
- Successful attacker can earn up to **$394,000 in a single month**

Top Threats

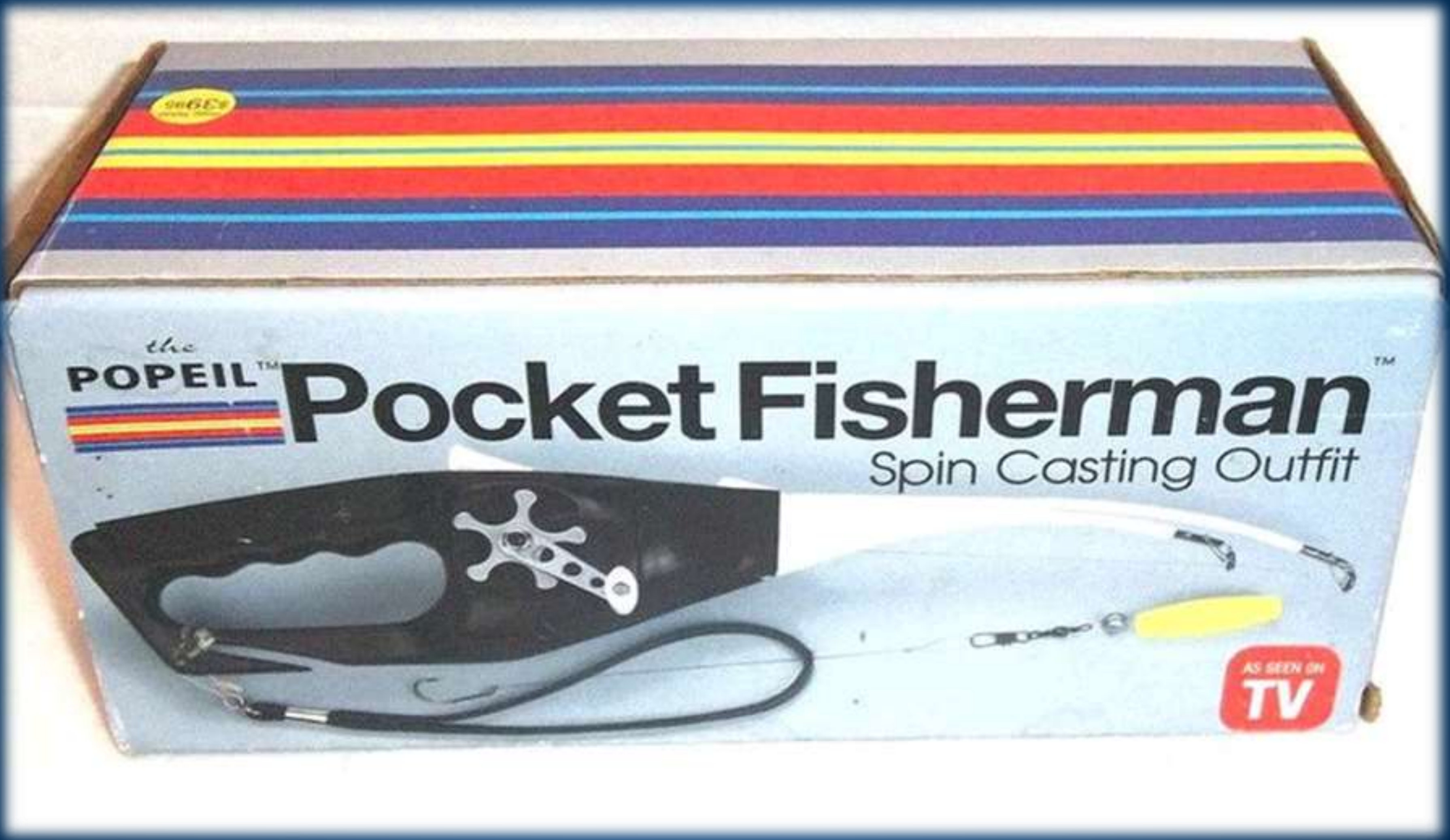
Secure State

Cleveland, Ohio

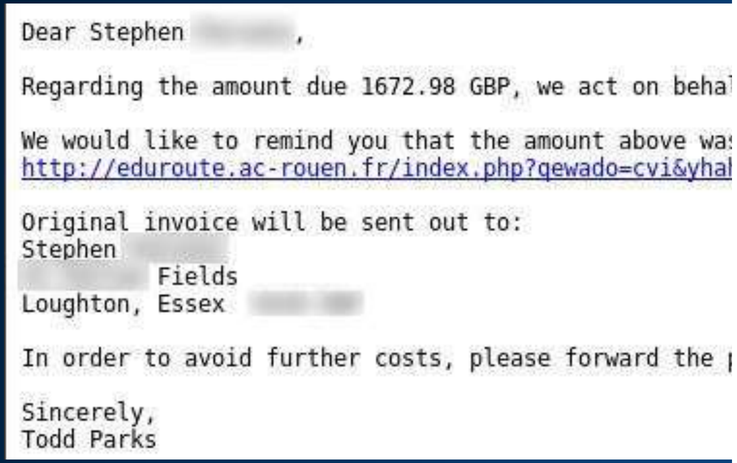


SOPHOS

HD Fishing


the
POPEIL™
Pocket Fisherman™
Spin Casting Outfit
AS SEEN ON
TV

HD Phishing



Dear Stephen [redacted],

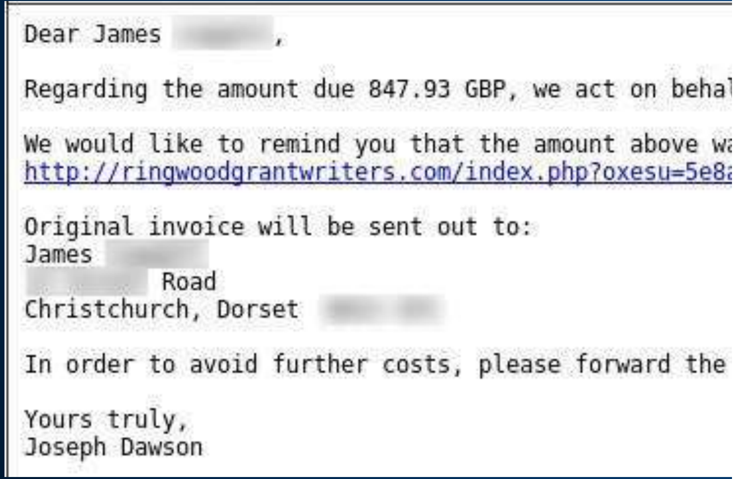
Regarding the amount due 1672.98 GBP, we act on behal

We would like to remind you that the amount above was
http://eduroute.ac-rouen.fr/index.php?qewado=cvi&yhal

Original invoice will be sent out to:
Stephen [redacted]
[redacted] Fields
Loughton, Essex [redacted]

In order to avoid further costs, please forward the

Sincerely,
Todd Parks



Dear James [redacted],

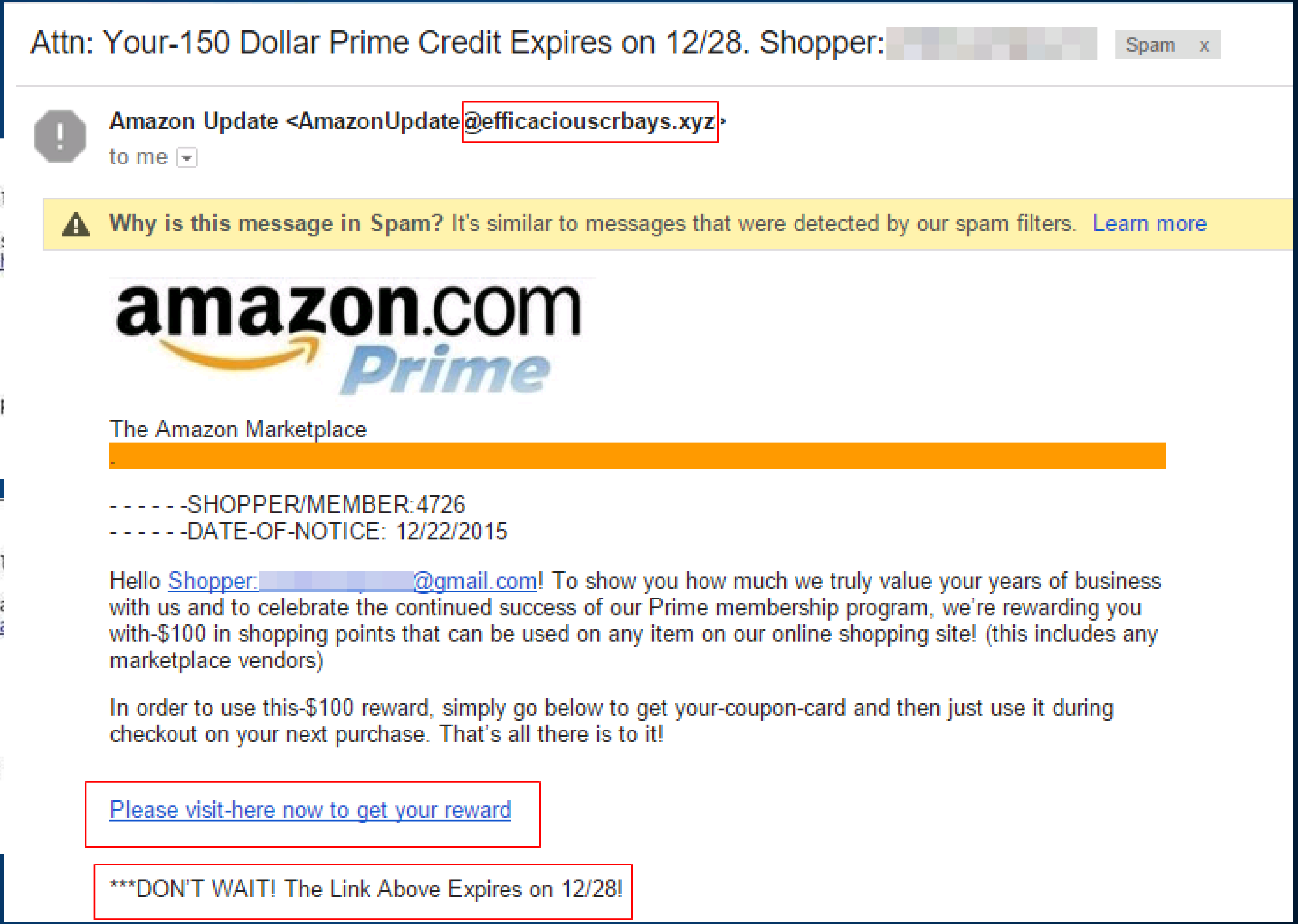
Regarding the amount due 847.93 GBP, we act on behal

We would like to remind you that the amount above wa
http://ringwoodgrantwriters.com/index.php?oxesu=5e8

Original invoice will be sent out to:
James [redacted]
[redacted] Road
Christchurch, Dorset [redacted]

In order to avoid further costs, please forward the

Yours truly,
Joseph Dawson



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted]

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>
to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

The Amazon Marketplace

- - - - - -SHOPPER/MEMBER:4726
- - - - - -DATE-OF-NOTICE: 12/22/2015

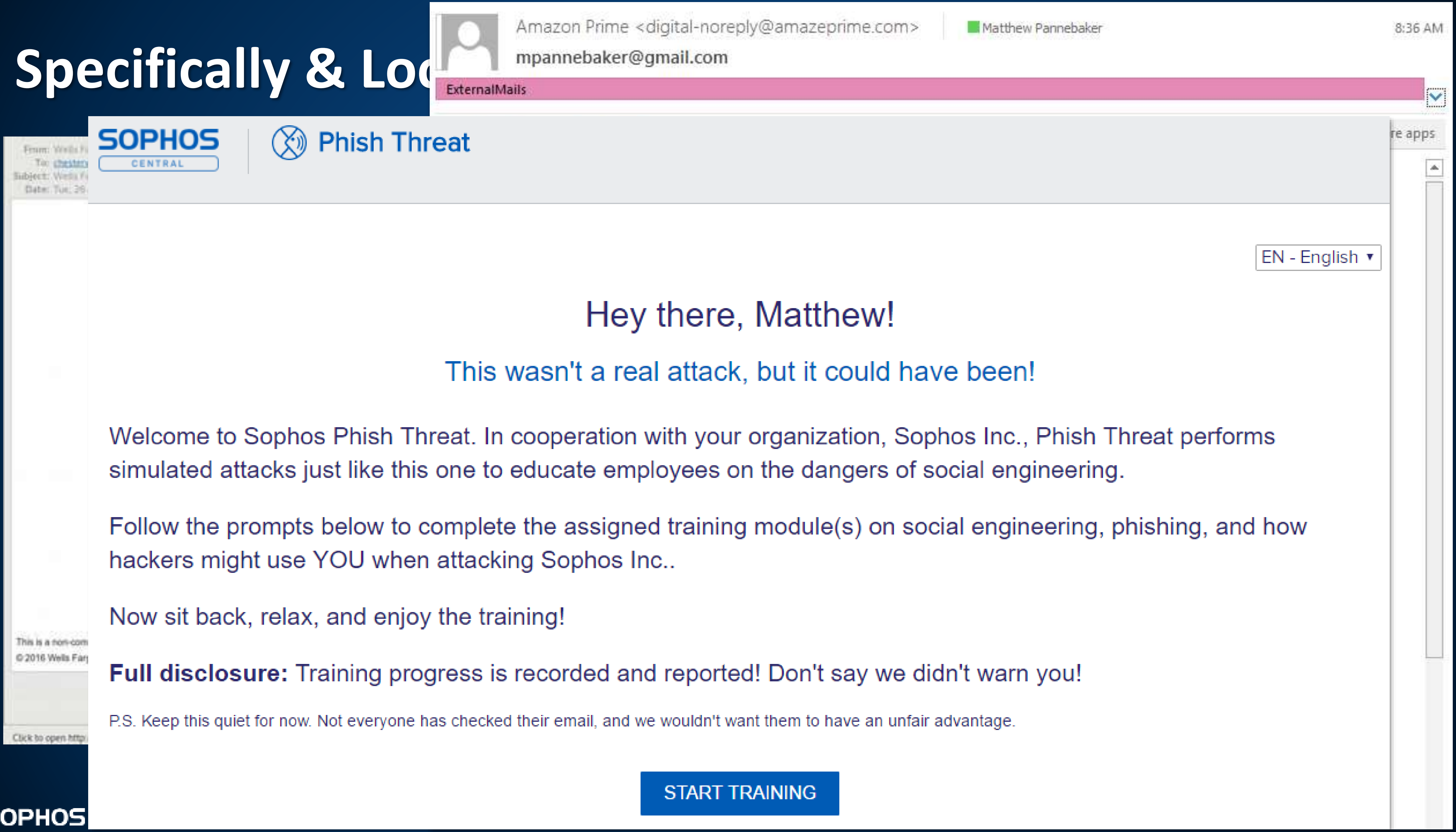
Hello Shopper:[redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

Specifically & Loc



Amazon Prime <digital-noreply@amazeprime.com> | Matthew Pannebaker 8:36 AM

mpannebaker@gmail.com

ExternalMails

From: Wells F
To: chester
Subject: Wells F
Date: Tue, 29

This is a non-com
© 2016 Wells Farg

Click to open http

Hey there, Matthew!

This wasn't a real attack, but it could have been!

Welcome to Sophos Phish Threat. In cooperation with your organization, Sophos Inc., Phish Threat performs simulated attacks just like this one to educate employees on the dangers of social engineering.

Follow the prompts below to complete the assigned training module(s) on social engineering, phishing, and how hackers might use YOU when attacking Sophos Inc..

Now sit back, relax, and enjoy the training!

Full disclosure: Training progress is recorded and reported! Don't say we didn't warn you!

P.S. Keep this quiet for now. Not everyone has checked their email, and we wouldn't want them to have an unfair advantage.

Tail-tell signs of Phishing…

It just doesn’t look right

Generic salutations

Requests for sensitive data

Specific information on you

Scare tactics

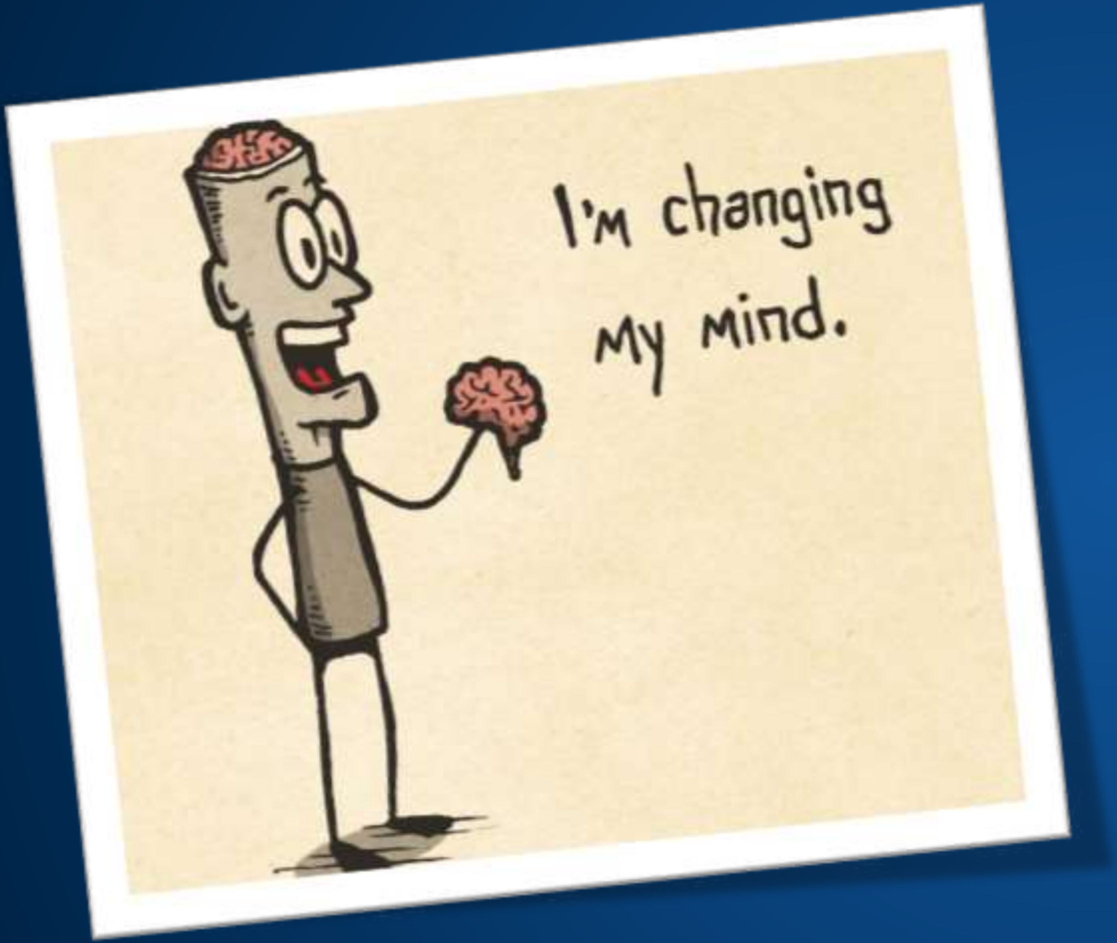
Poor grammar or spelling

Sense of urgency

“You’ve won the grand prize!”

“Verify your account.”

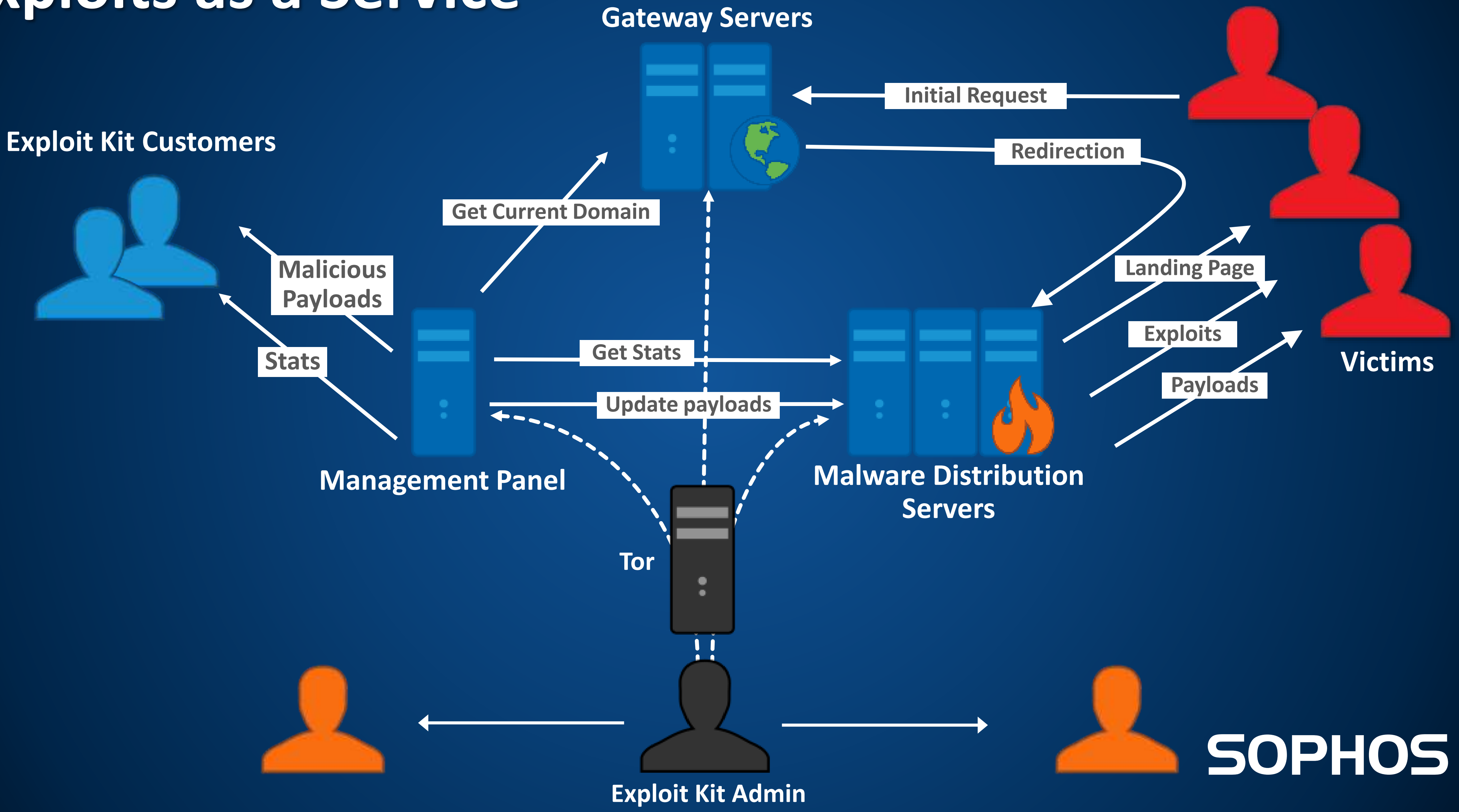
Cybersquatting



Changing our minds about the how's and why's of hackers & malware…

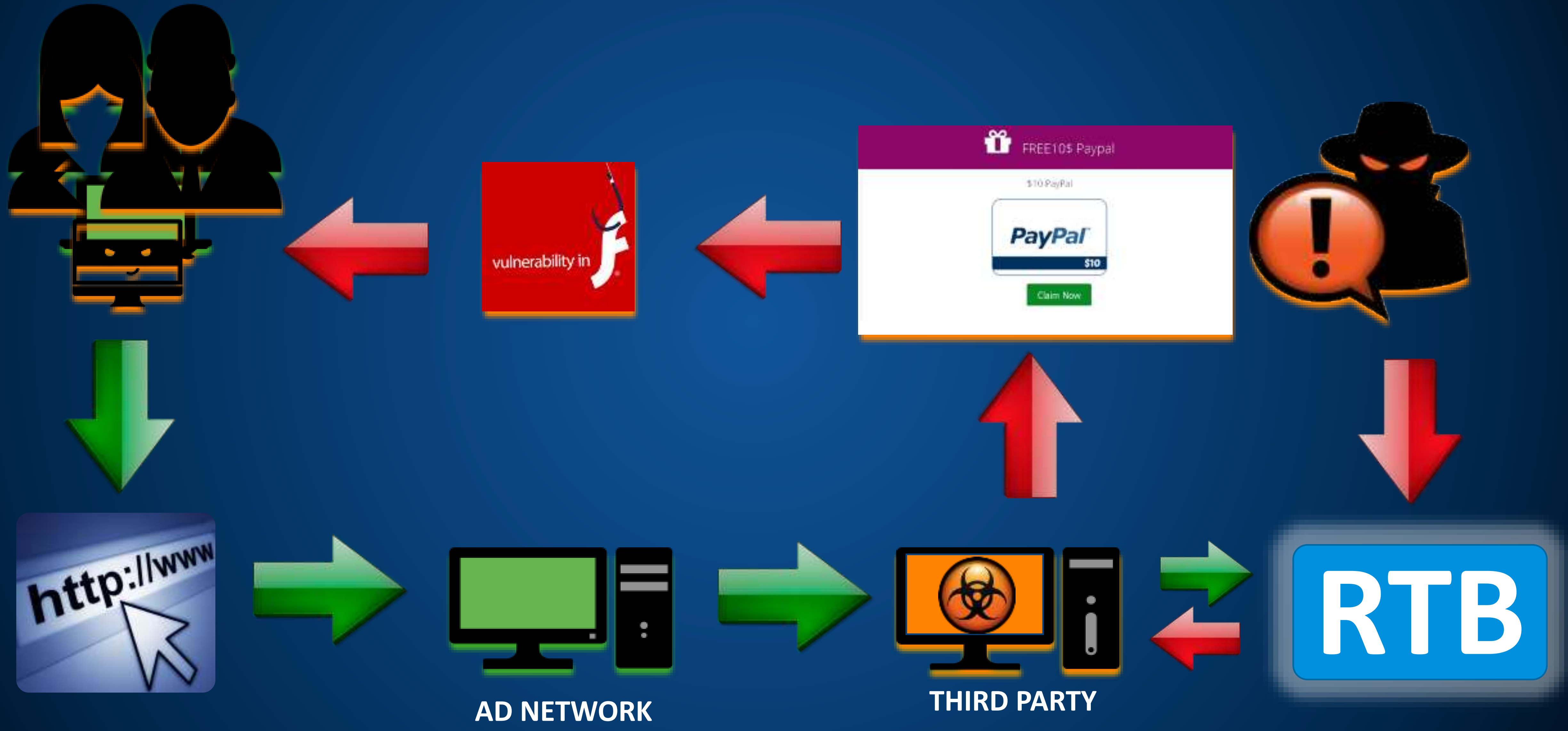
Pavel Vrublevsky

Exploits as a Service



SOPHOS

Malvertising Threat Chain



AD NETWORK

THIRD PARTY

RTB

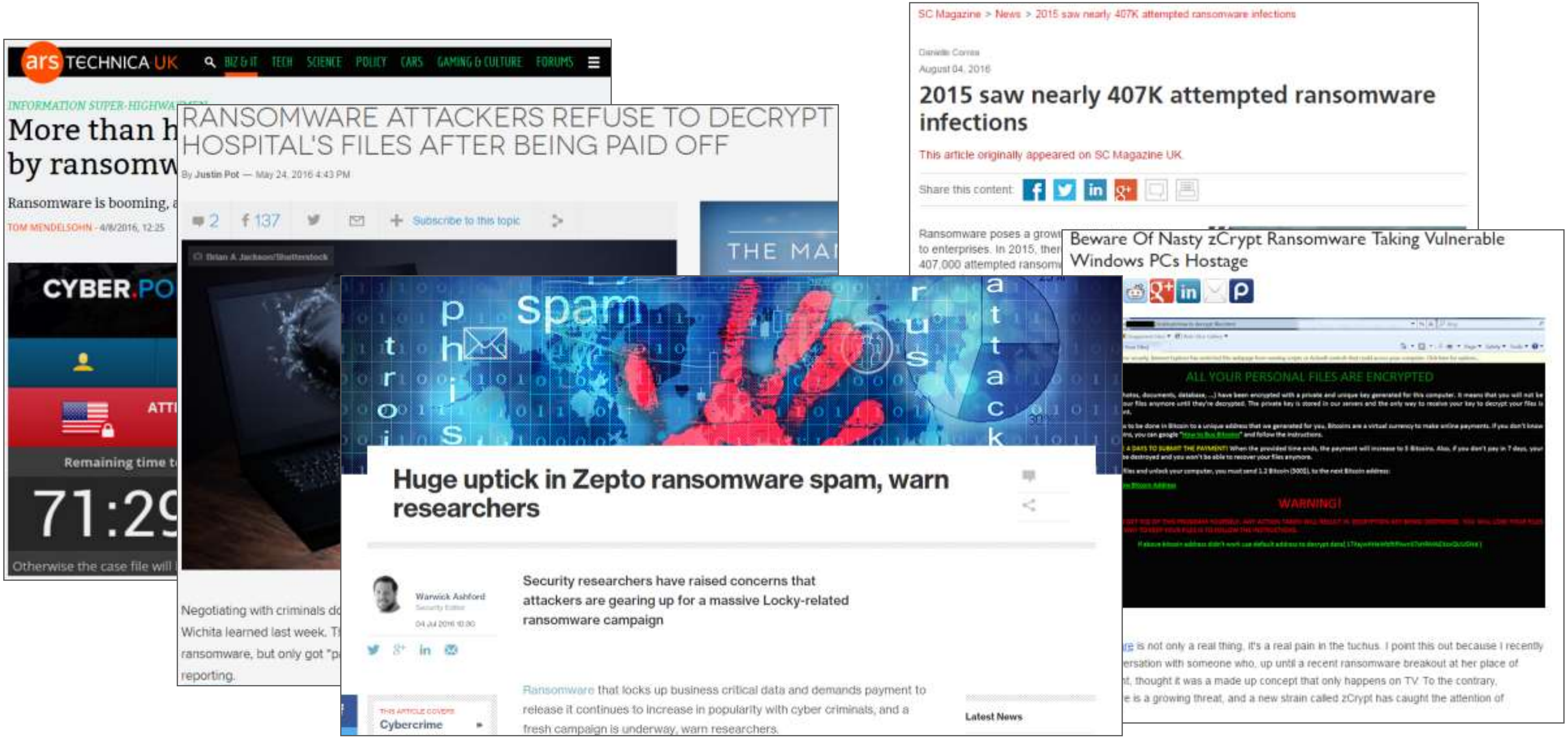
No site is immune…

Forbes
The New York Times
BBC
London Stock Exchange
Disney
facebook
THE HUFFINGTON POST
theguardian
Aol.
Spotify
YAHOO!
TMZ.com
the Atlantic
Zillow

Who Likes Extortion?

Hey, Calvin, it's gonna cost you 50 cents to be my friend today.

Ransomware Is Hitting the Headlines…



ars TECHNICA UK
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

INFORMATION SUPER-HIGHWA

More than h
by ransomw

Ransomware is booming, a

TOM MENDELSOHN - 4/8/2016, 12:25

CYBER.PO
ATT
Remaining time t
71:29
Otherwise the case file will

RANSOMWARE ATTACKERS REFUSE TO DECRYPT HOSPITAL'S FILES AFTER BEING PAID OFF

By Justin Pot — May 24, 2016 4:43 PM

2 137 + Subscribe to this topic
Brian A Jackson/Shutterstock
THE MA

Negotiating with criminals d
Wichita learned last week. T
ransomware, but only got "p
reporting.

SC Magazine > News > 2015 saw nearly 407K attempted ransomware infections

Danielle Correa
August 04, 2016

2015 saw nearly 407K attempted ransomware infections

This article originally appeared on SC Magazine UK.

Share this content:

Ransomware poses a growi
to enterprises. In 2015, ther
407,000 attempted ransom

Beware Of Nasty zCrypt Ransomware Taking Vulnerable Windows PCs Hostage

ALL YOUR PERSONAL FILES ARE ENCRYPTED

hotos, documents, database, ...) have been encrypted with a private and unique key generated for this computer. It means that you will not be
our files anymore until they're decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is
nt.

s to be done in Bitcoin to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know
ins, you can google "How to Buy Bitcoins" and follow the instructions.

4 DAYS TO SUBMIT THE PAYMENT! When the provided time ends, the payment will increase to 5 Bitcoins. Also, if you don't pay in 7 days, your
be destroyed and you won't be able to recover your files anymore.

files and unlock your computer, you must send 1.2 Bitcoin (500$), to the next Bitcoin address:

WARNING!

If above bitcoin address didn't work use default address to decrypt data[[illegible]]

e is not only a real thing, it's a real pain in the tuchus. I point this out because I recently
ersation with someone who, up until a recent ransomware breakout at her place of
t, thought it was a made up concept that only happens on TV. To the contrary,
e is a growing threat, and a new strain called zCrypt has caught the attention of

Huge uptick in Zepto ransomware spam, warn researchers

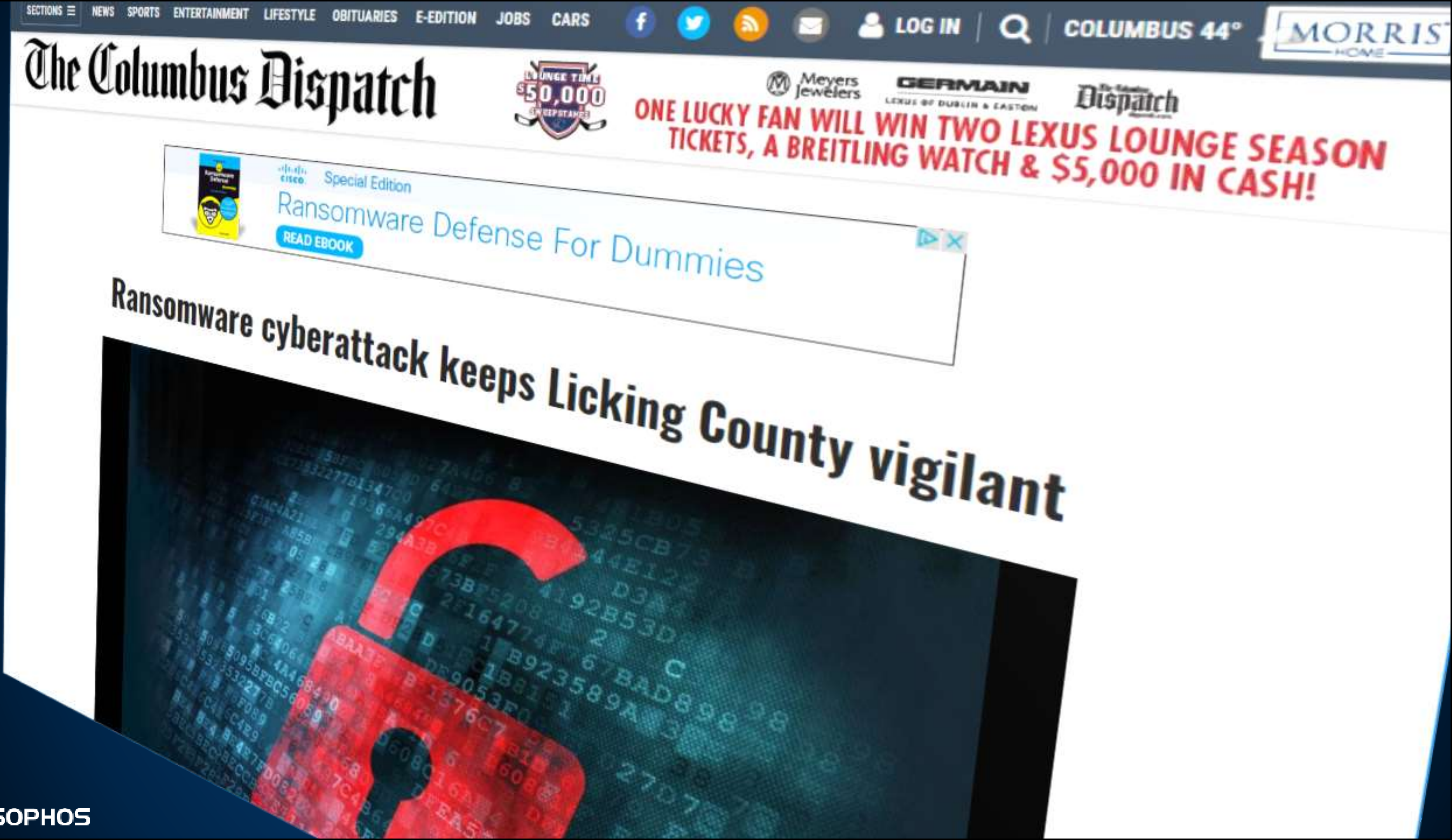
Warwick Ashford
Security Editor
04 Jul 2016 10:30

Security researchers have raised concerns that attackers are gearing up for a massive Locky-related ransomware campaign

THIS ARTICLE COVERS
Cybercrime

Ransomware that locks up business critical data and demands payment to release it continues to increase in popularity with cyber criminals, and a fresh campaign is underway, warn researchers.

Latest News



The Columbus Dispatch

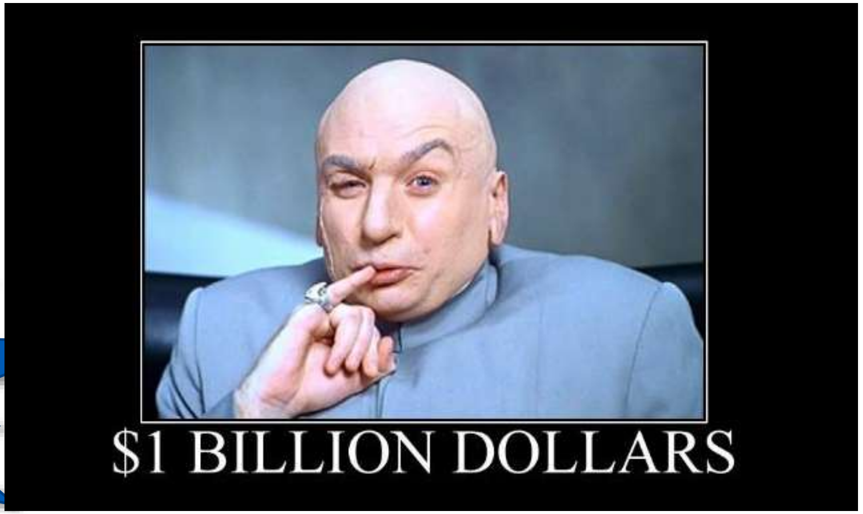
Ransomware cyberattack keeps Licking County vigilant

…And Keeps Growing…

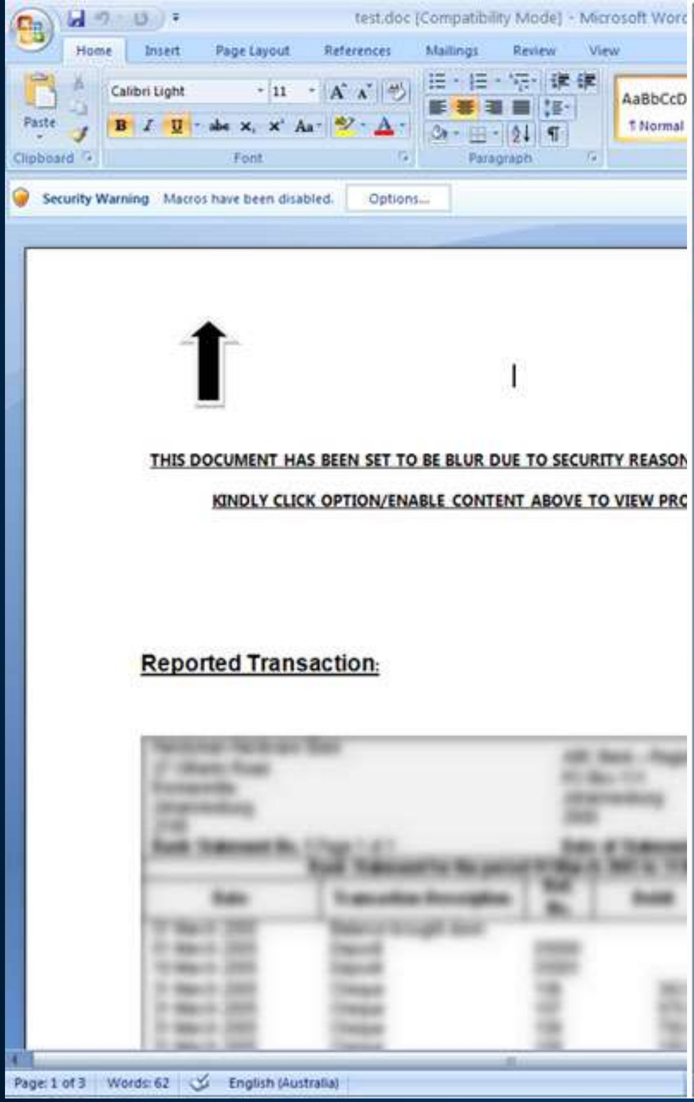
- Estimated to be a **$1 Billion** a year industry by the end of 2016 (FBI)

- Criminals are dedicated and professional – even setting up **customer care teams** to secure payment

Precast Concrete ~12bn



Document malware



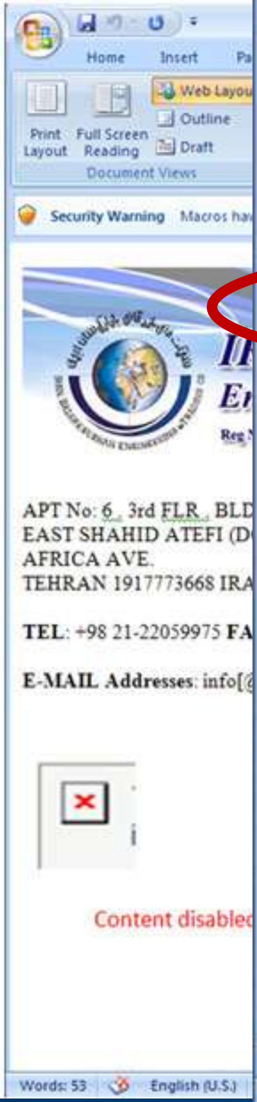
Security Warning Macros have been disabled. Options...

THIS DOCUMENT HAS BEEN SET TO BE BLUR DUE TO SECURITY REASON

KINDLY CLICK OPTION/ENABLE CONTENT ABOVE TO VIEW PRC

Reported Transaction:

Page: 1 of 3 Words: 62 English (Australia)



Security Warning Macros ha

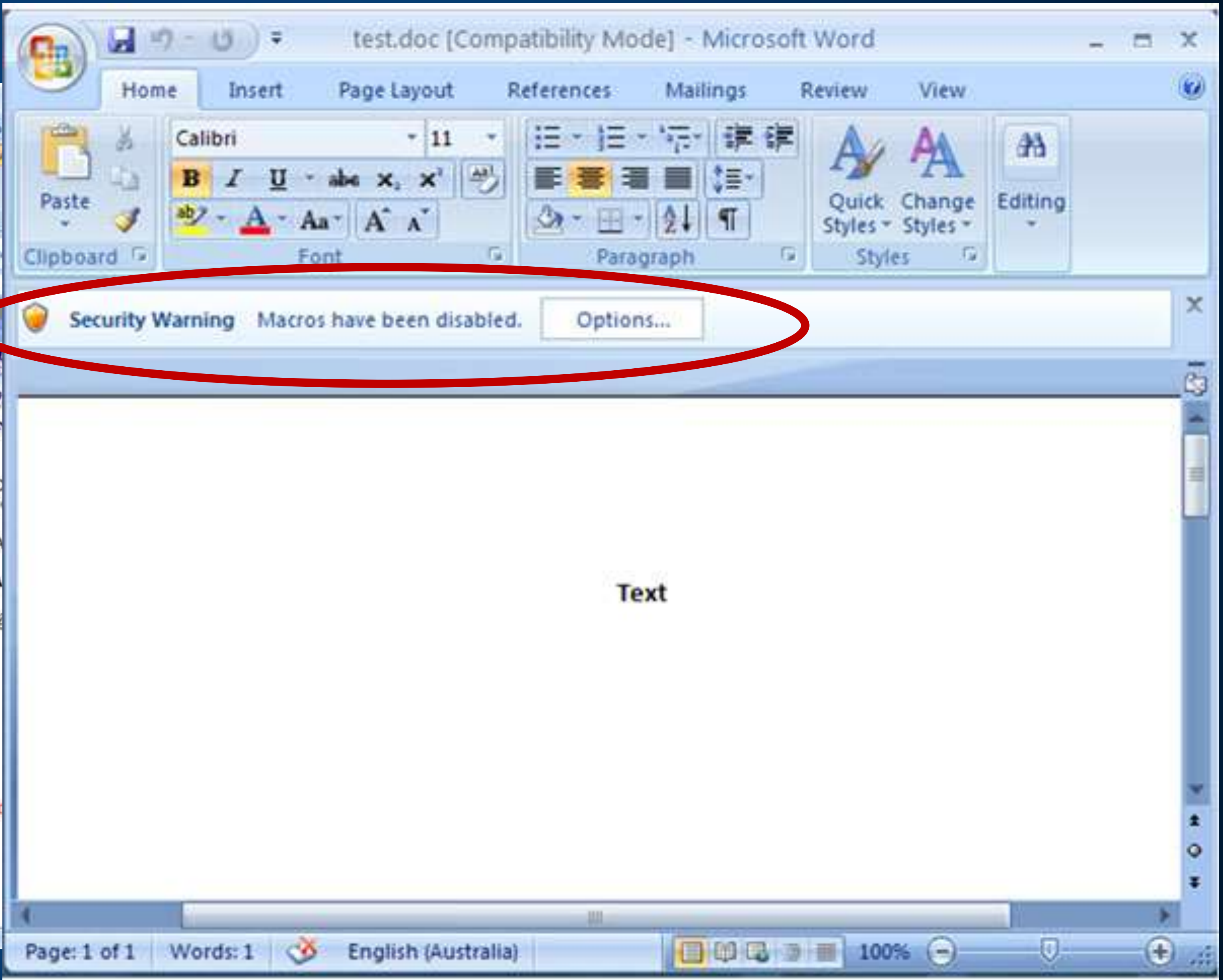
APT No: 6, 3rd FLR, BLD
EAST SHAHID ATEFI (D
AFRICA AVE.
TEHRAN 1917773668 IRA

TEL: +98 21-22059975 FA

E-MAIL Addresses: info[@

Content disabled

Words: 53 English (U.S.)

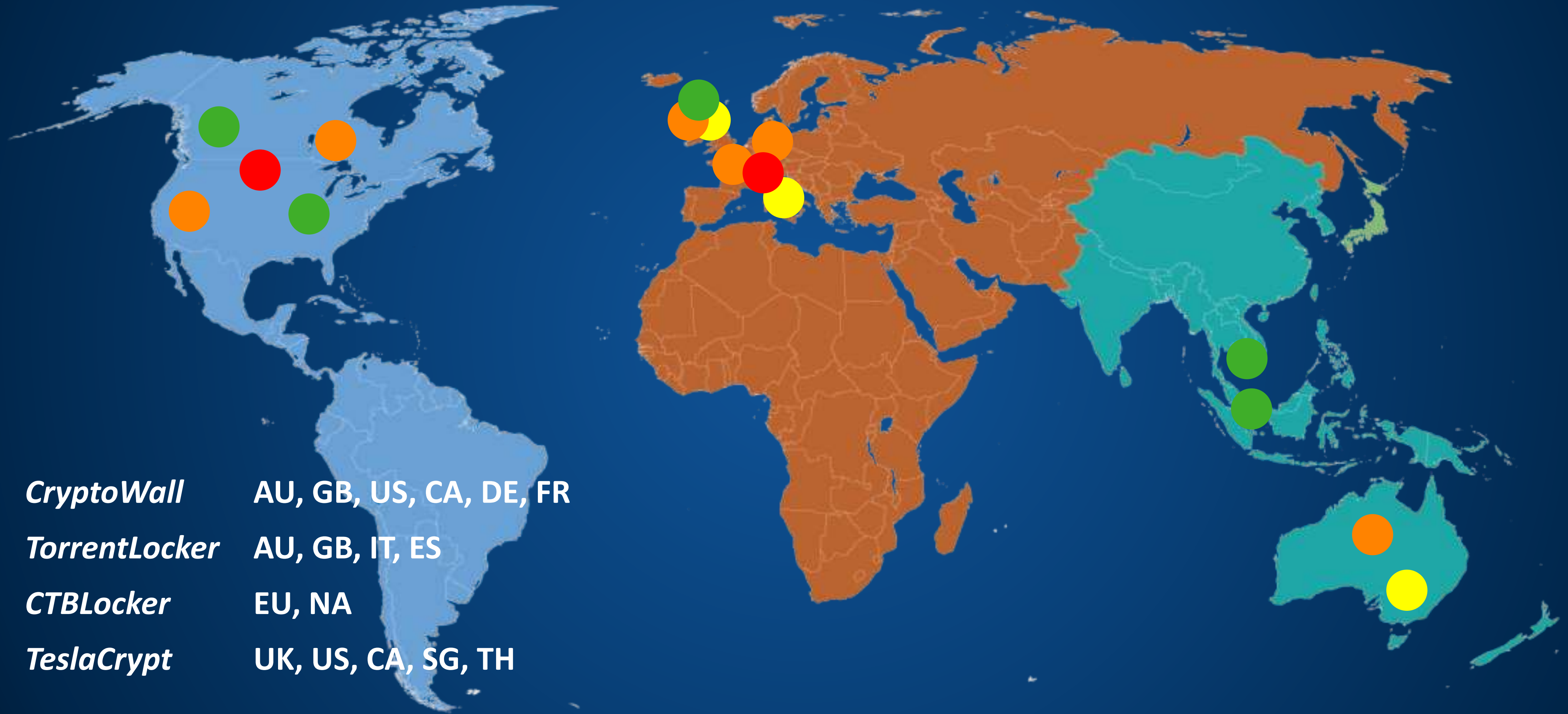


Security Warning Macros have been disabled. Options...

Text

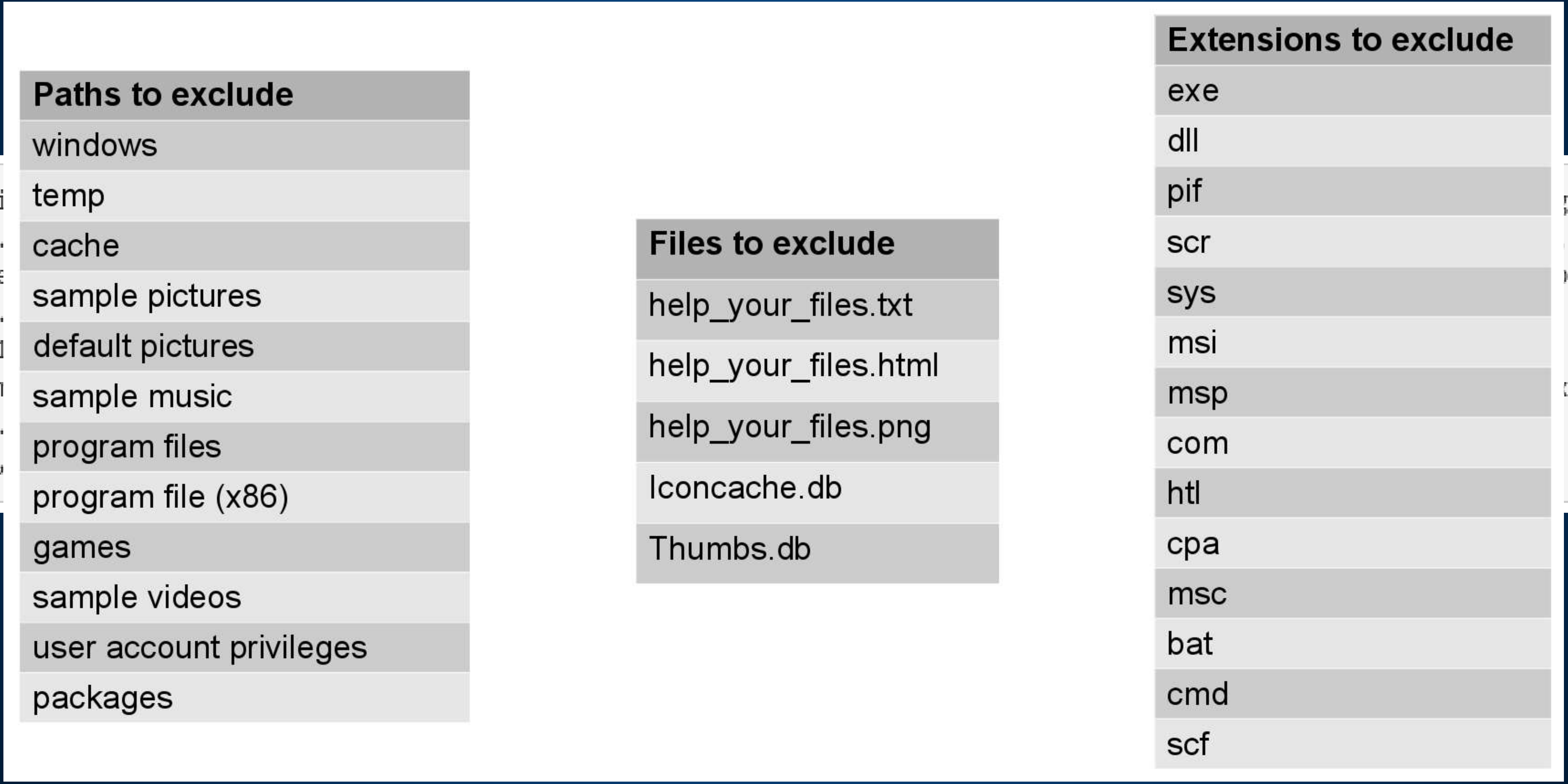
Page: 1 of 1 Words: 1 English (Australia) 100%

Ransomware Prevalence



🟠	*CryptoWall*	AU, GB, US, CA, DE, FR
🟡	*TorrentLocker*	AU, GB, IT, ES
🔴	*CTBLocker*	EU, NA
🟢	*TeslaCrypt*	UK, US, CA, SG, TH

Targeted Ransomware



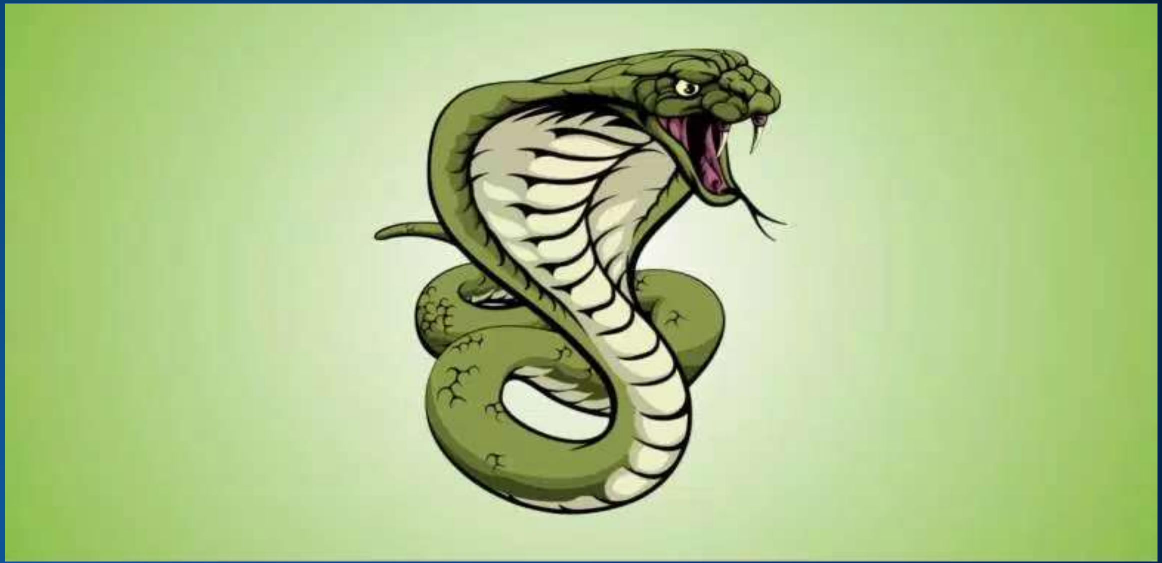
Paths to exclude
windows
temp
cache
sample pictures
default pictures
sample music
program files
program file (x86)
games
sample videos
user account privileges
packages

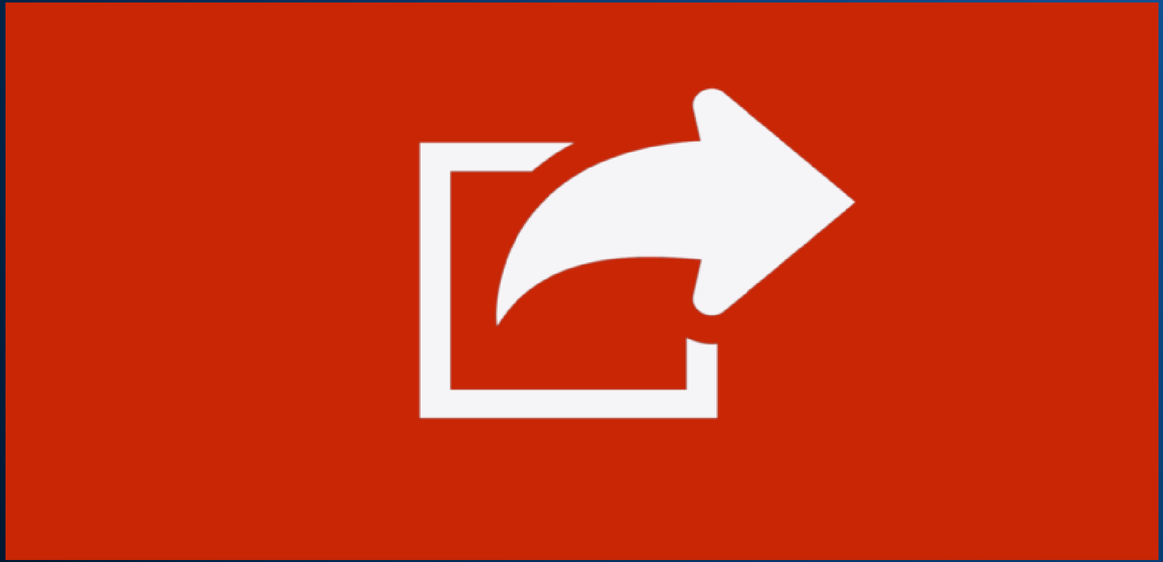
Files to exclude
help_your_files.txt
help_your_files.html
help_your_files.png
Iconcache.db
Thumbs.db

Extensions to exclude
exe
dll
pif
scr
sys
msi
msp
com
htl
cpa
msc
bat
cmd
scf

SOPHOS

Malware with fancy names: Fantom, Mamba & Odin



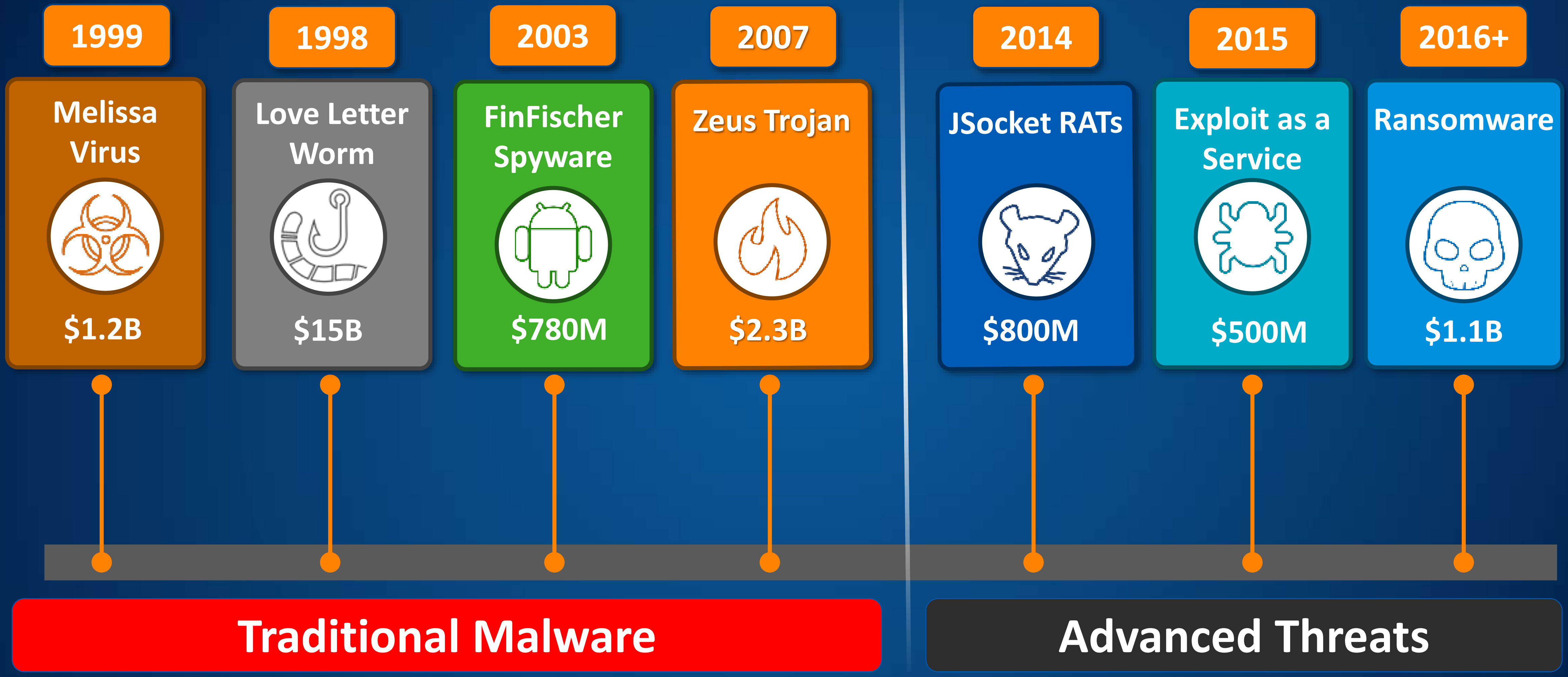


SOPHOS

Evolution of your industry…

The Evolution of Threats

From Malware to Exploits



1999
Melissa Virus
$1.2B

1998
Love Letter Worm
$15B

2003
FinFischer Spyware
$780M

2007
Zeus Trojan
$2.3B

2014
JSocket RATs
$800M

2015
Exploit as a Service
$500M

2016+
Ransomware
$1.1B

Traditional Malware

Advanced Threats

SOPHOS

The Evolution of Security

From Anti-Malware to Anti-Exploit

Virus

Worm

Spyware

Trojan

RATs

Exploit Kits

Ransomware

Exposure Prevention

URL Blocking
Web/App/Dev Ctrl
Download Rep

Pre-Exec Analytics

Generic Matching
Heuristics
Core Rules

File Scanning

Known Malware
Malware Bits

Run-Time

Behavior
Analytics
Runtime
Behavior

Exploit Detection

Technique
Identification

Traditional Malware

Advanced Threats

*Intercept*ing Ne*X*t Gen Threats…

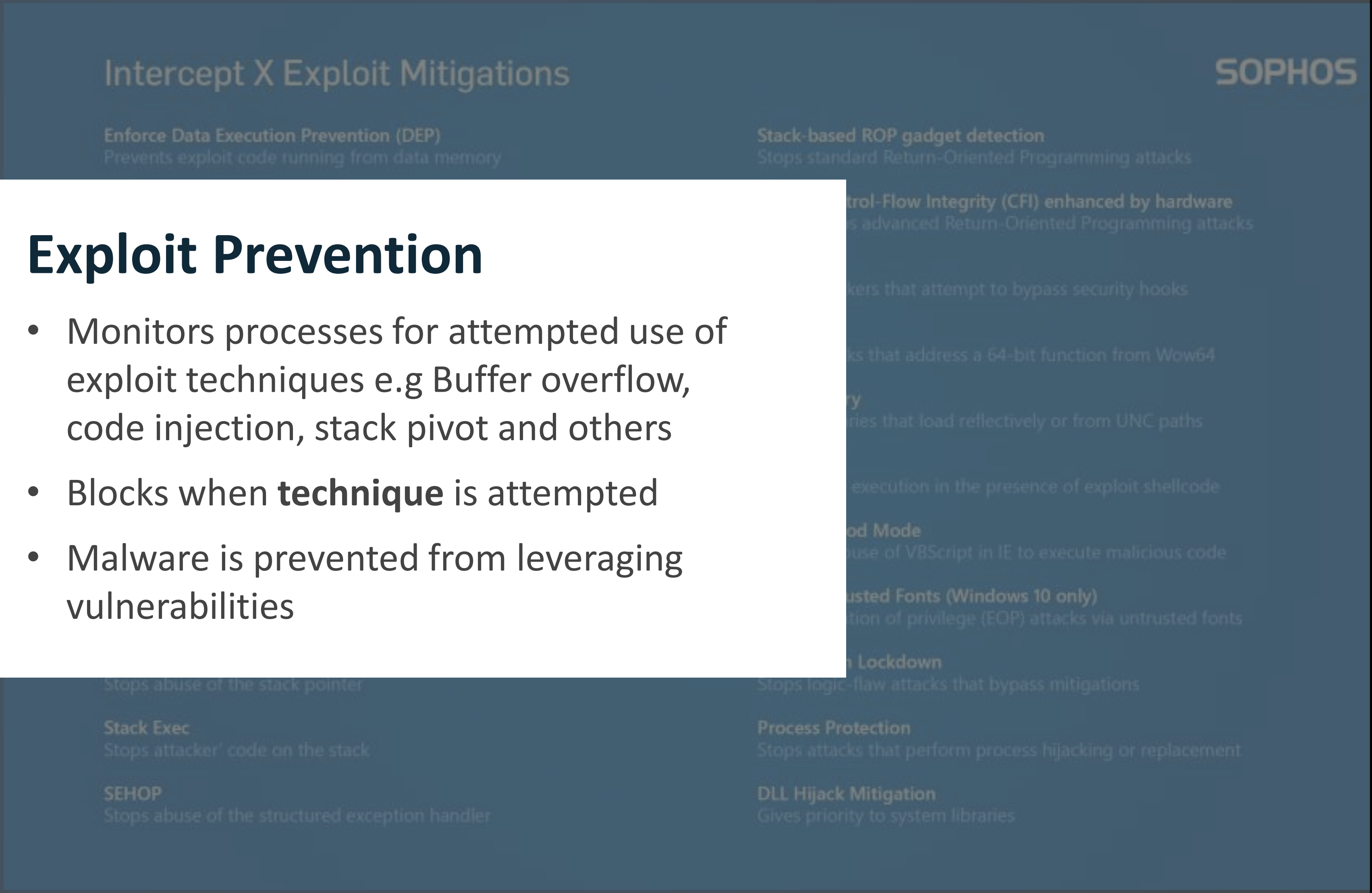
Introducing…

Intercepting Exploits

Malware techniques
10's of new malware sub-techniques every year
New malware each year
100,000,000+

Exploit Prevention

- Monitors processes for attempted use of exploit techniques e.g Buffer overflow, code injection, stack pivot and others
- Blocks when **technique** is attempted
- Malware is prevented from leveraging vulnerabilities



Intercept X Exploit Mitigations

Enforce Data Execution Prevention (DEP)
Prevents exploit code running from data memory

Stops abuse of the stack pointer

Stack Exec
Stops attacker' code on the stack

SEHOP
Stops abuse of the structured exception handler

Stack-based ROP gadget detection
Stops standard Return-Oriented Programming attacks

trol-Flow Integrity (CFI) enhanced by hardware
s advanced Return-Oriented Programming attacks

kers that attempt to bypass security hooks

ks that address a 64-bit function from Wow64

ry
ries that load reflectively or from UNC paths

execution in the presence of exploit shellcode

od Mode
use of VBScript in IE to execute malicious code

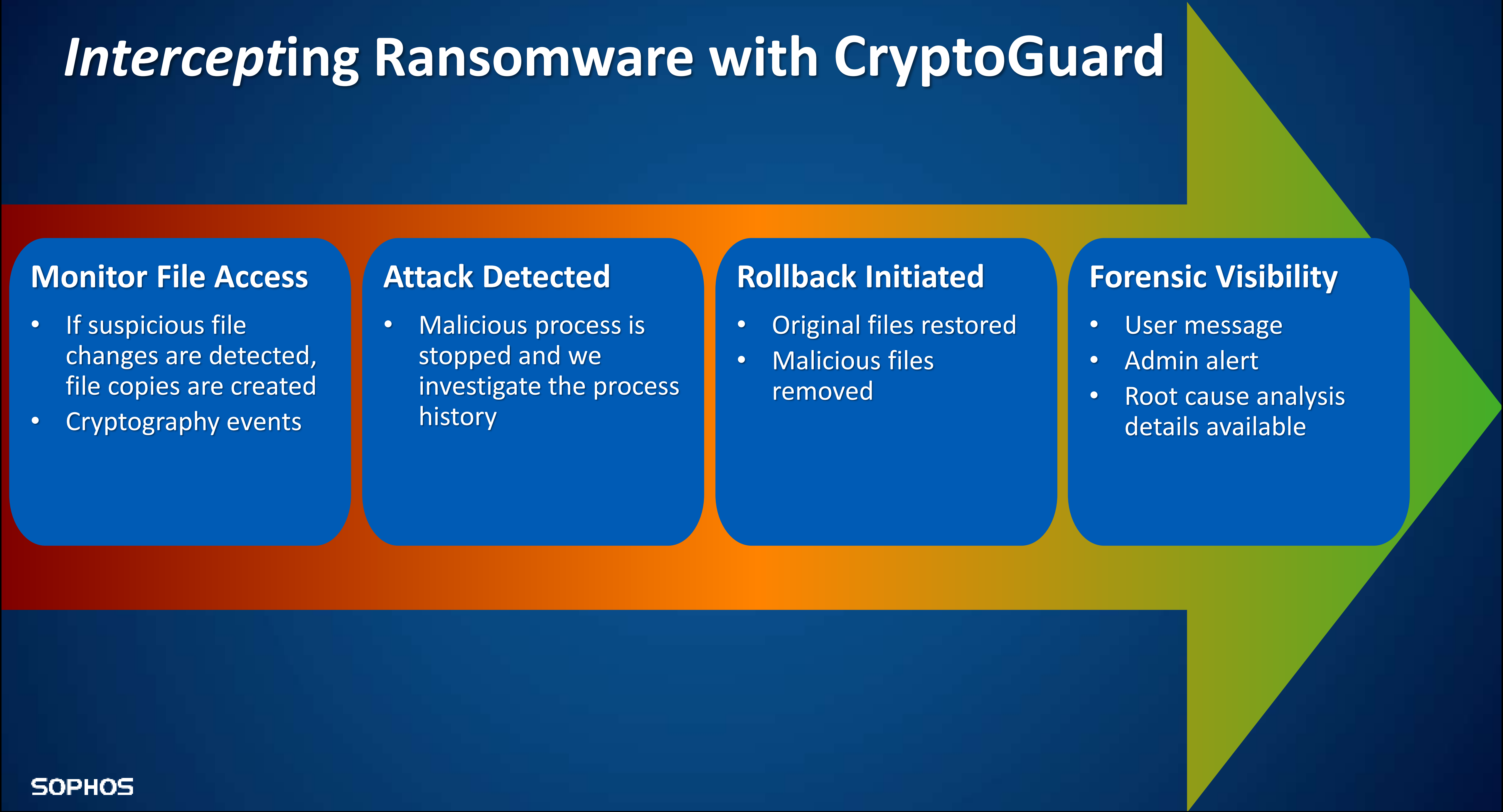
usted Fonts (Windows 10 only)
tion of privilege (EOP) attacks via untrusted fonts

n Lockdown
Stops logic-flaw attacks that bypass mitigations

Process Protection
Stops attacks that perform process hijacking or replacement

DLL Hijack Mitigation
Gives priority to system libraries

Intercepting Ransomware with CryptoGuard



Monitor File Access

- If suspicious file changes are detected, file copies are created
- Cryptography events

Attack Detected

- Malicious process is stopped and we investigate the process history

Rollback Initiated

- Original files restored
- Malicious files removed

Forensic Visibility

- User message
- Admin alert
- Root cause analysis details available

Sophos Clean

Malware Removal. Forensic-Level Cleanup. Second Opinion

Removes Threats

- Deep System Inspection
- Removes Malware Remnants
- Full Quarantine / Removal
- Effective Breach Remediation

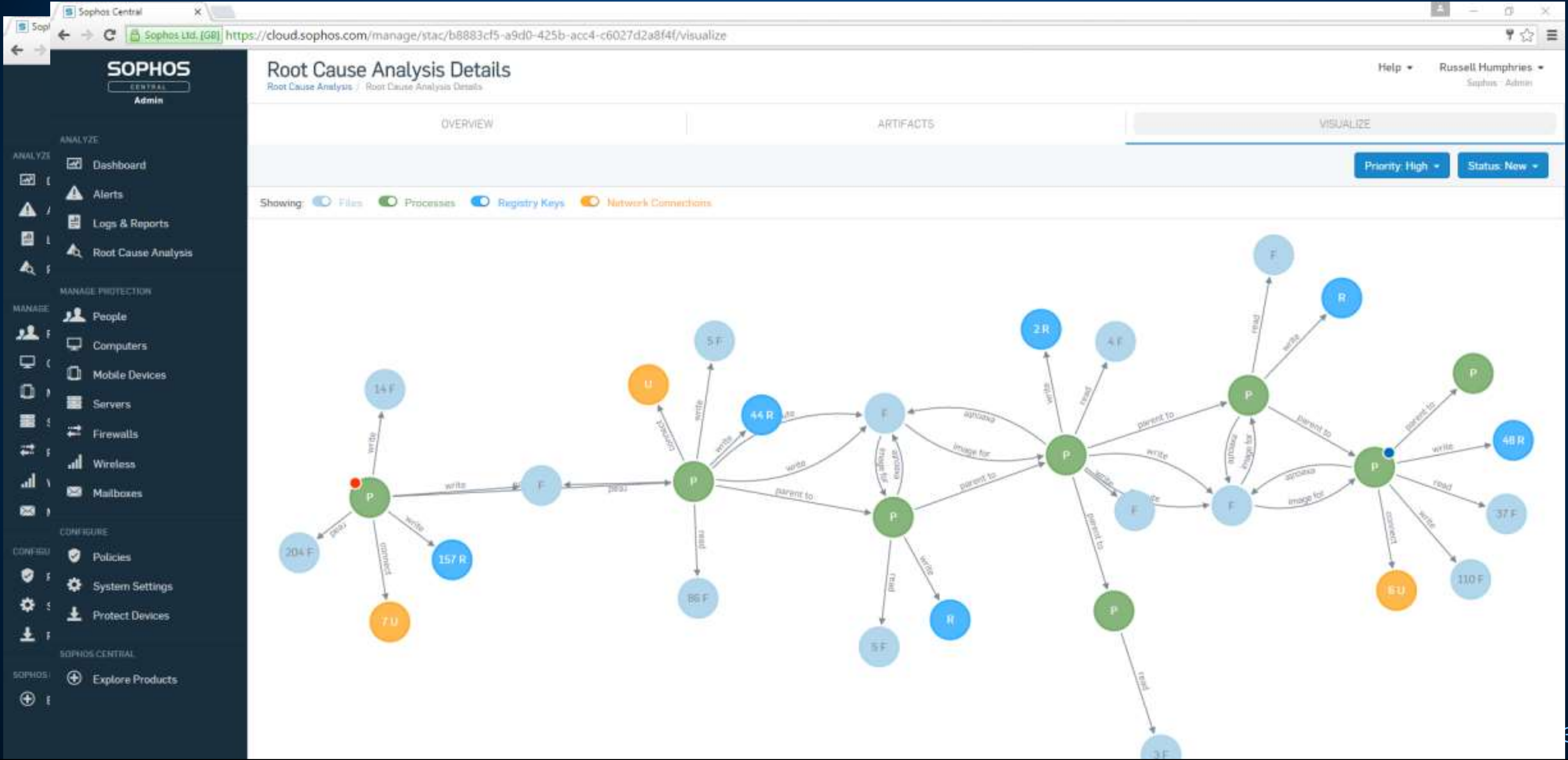
On-Demand Assessment

- Identifies Risky Files / Processes
- Constantly Refreshed Database
- Provides Additional Confidence
- Command-Line Capable

- 100% Automated with Intercept X
- Also available as a standalone Forensic Clean Utility and On-Premise Managed AV

Root Cause Analytics

Understanding the Who, What, When, Where, Why and How



SOPHOS

Why Should You Worry About Your Mobile Devices?

2x

Data breaches involving
smar
more t
2015 [1]

15%

of large organizations
had a security or
each involving
r tablets in 2015 [1]

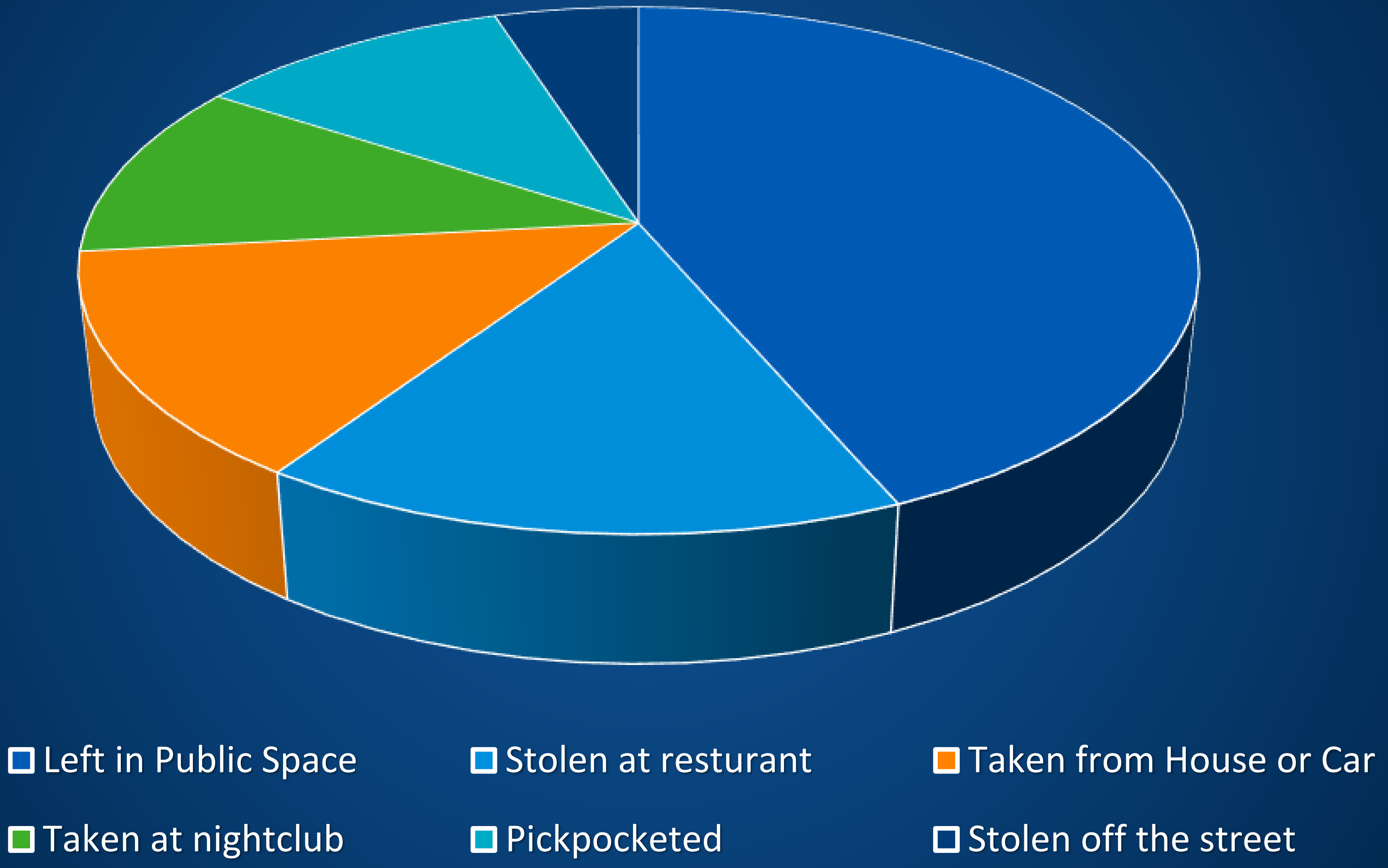
More than **200,000** phones are left in London Taxis each year!

Not managing mobile devices means flying blind, with **zero visibility**

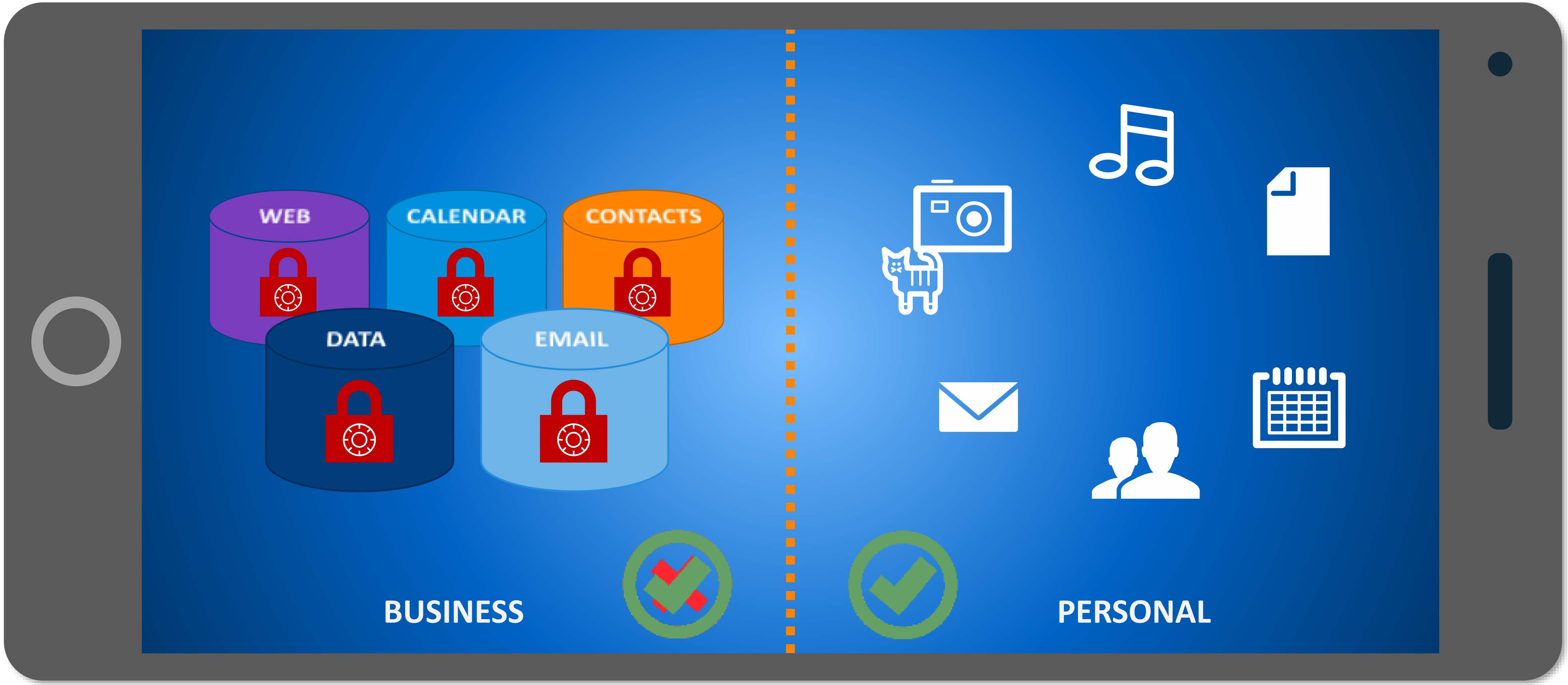
Users find a way to access business resources on **unsecured** devices

[1] HM Gov't, Information Security Breaches Survey 2015

How Mobile Devices are Lost



Containers – Separate Business and Personal Data



Should you worry about mobile malware?

SOPHOS

Potentially Unwanted Apps (PUA) vs Malware

PUA

Not entirely honest about its intentions

Often misuses your resources, leaves you with hidden costs

“Gateway drug”

Malware

A **weapon**, *not* a fun tool, or a prank

Steals your data for money

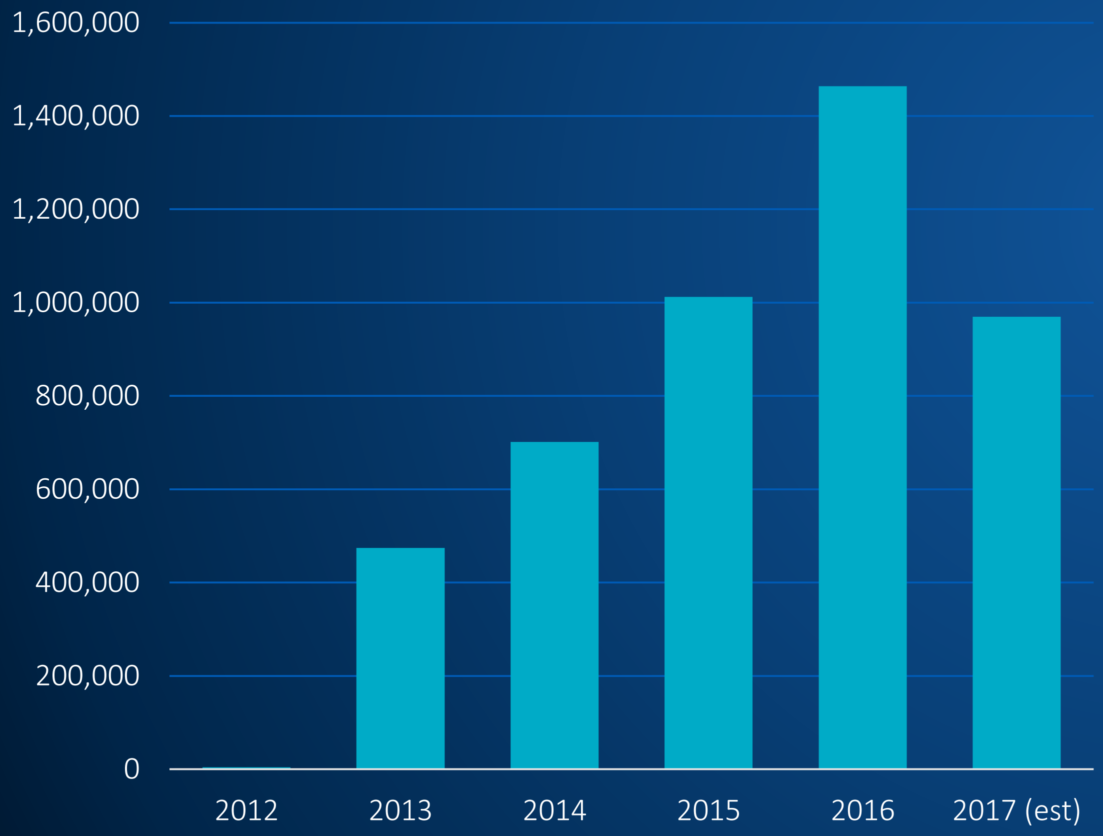
Accesses data or resources with the intent to do harm

You pay for what you get…

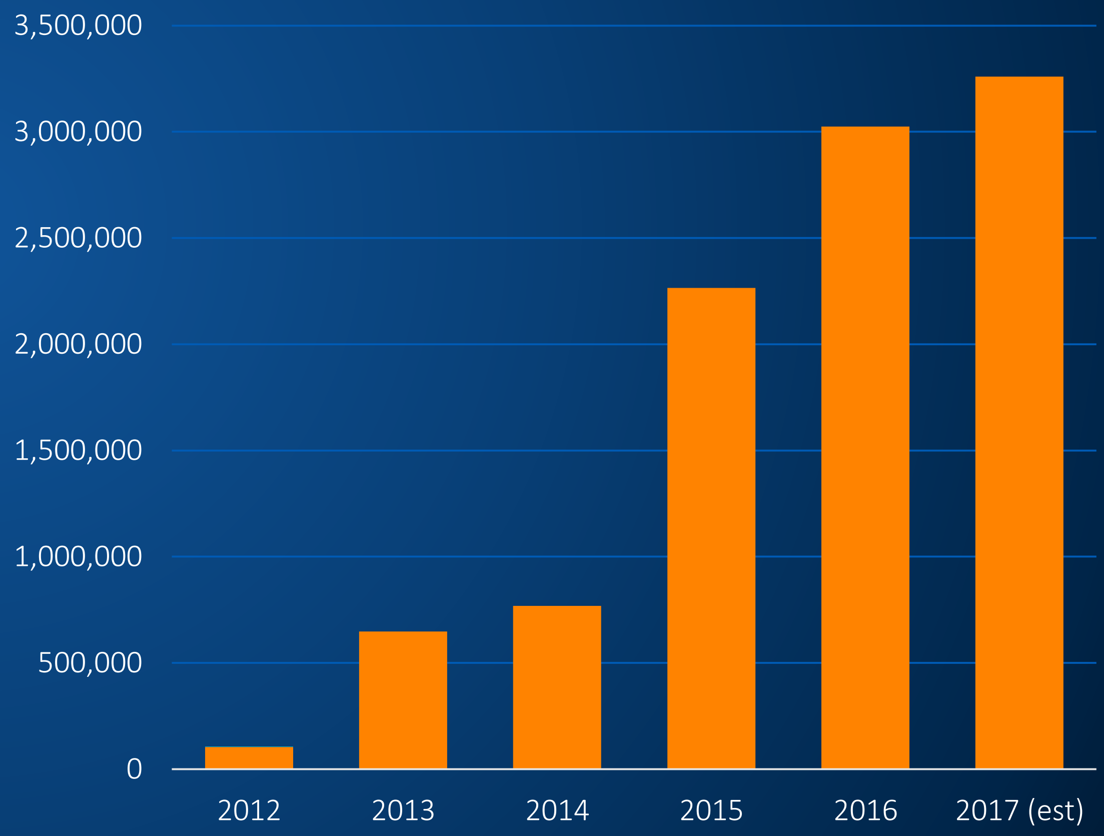
IMAGINARY

Mobile Threats Are Real…

Potentially Unwanted Applications



Android Malware

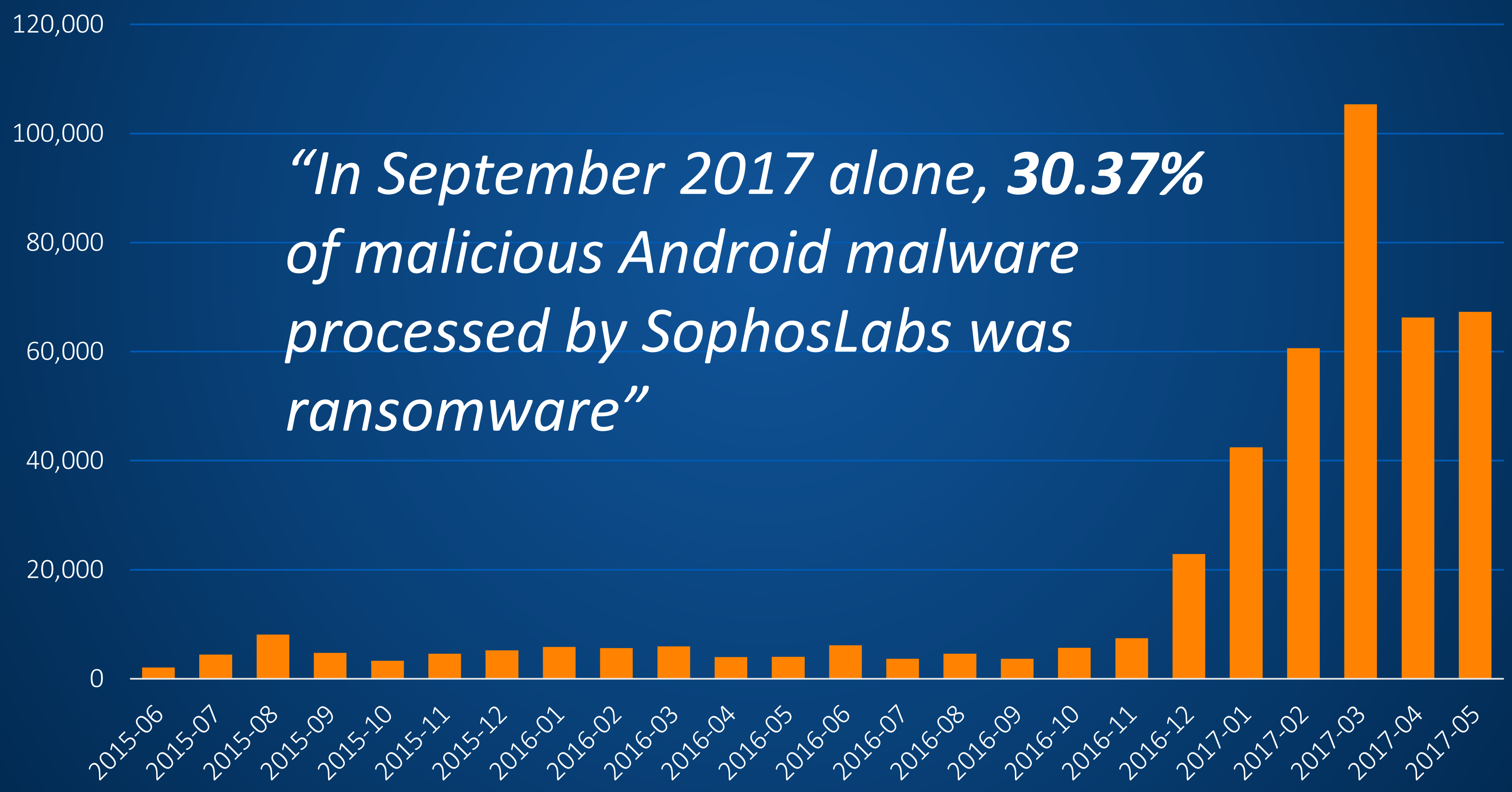


SOPHOS

Source: SophosLabs, 2017

What about ransomware?

Android ransomware 2015-2017



*"In September 2017 alone, **30.37%** of malicious Android malware processed by SophosLabs was ransomware"*

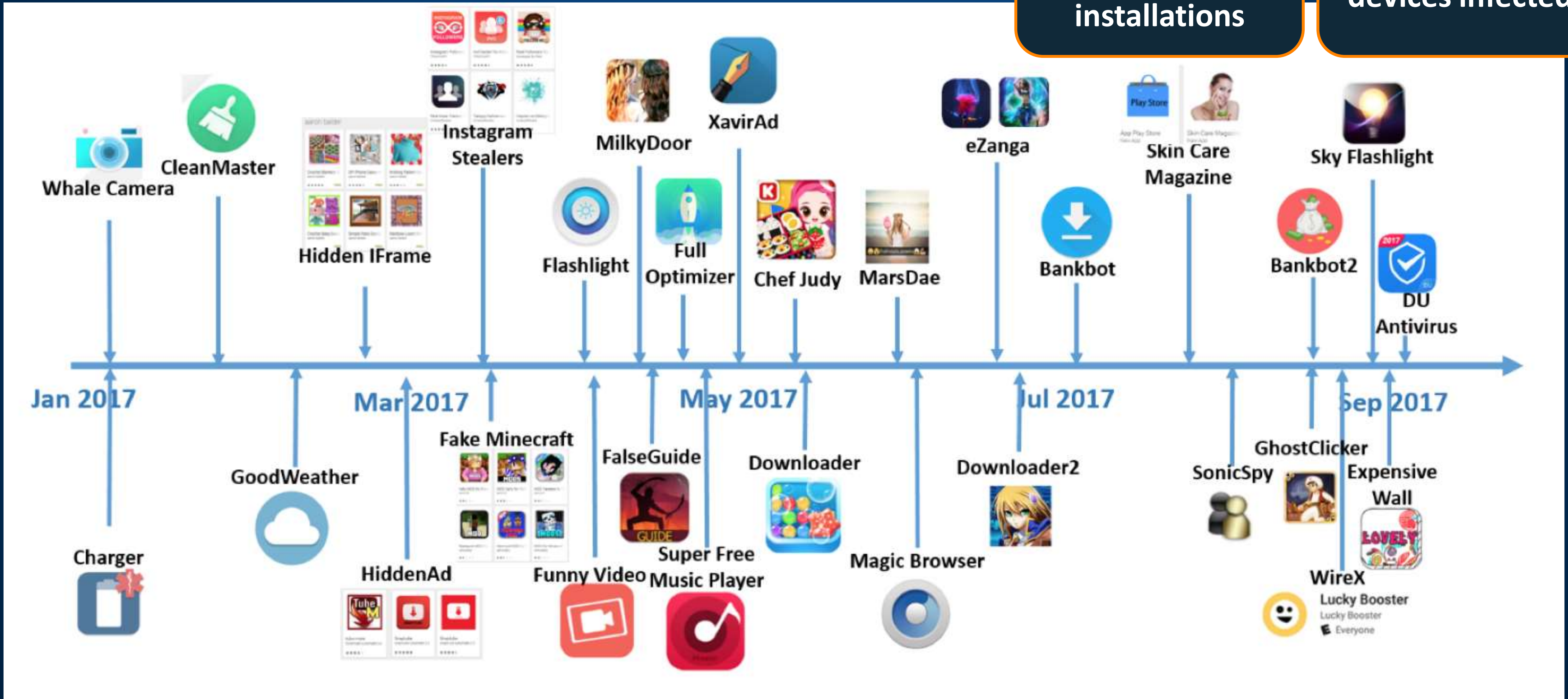
SOPHOS

Source: SophosLabs, 2017

Threats on Google Play Doubled

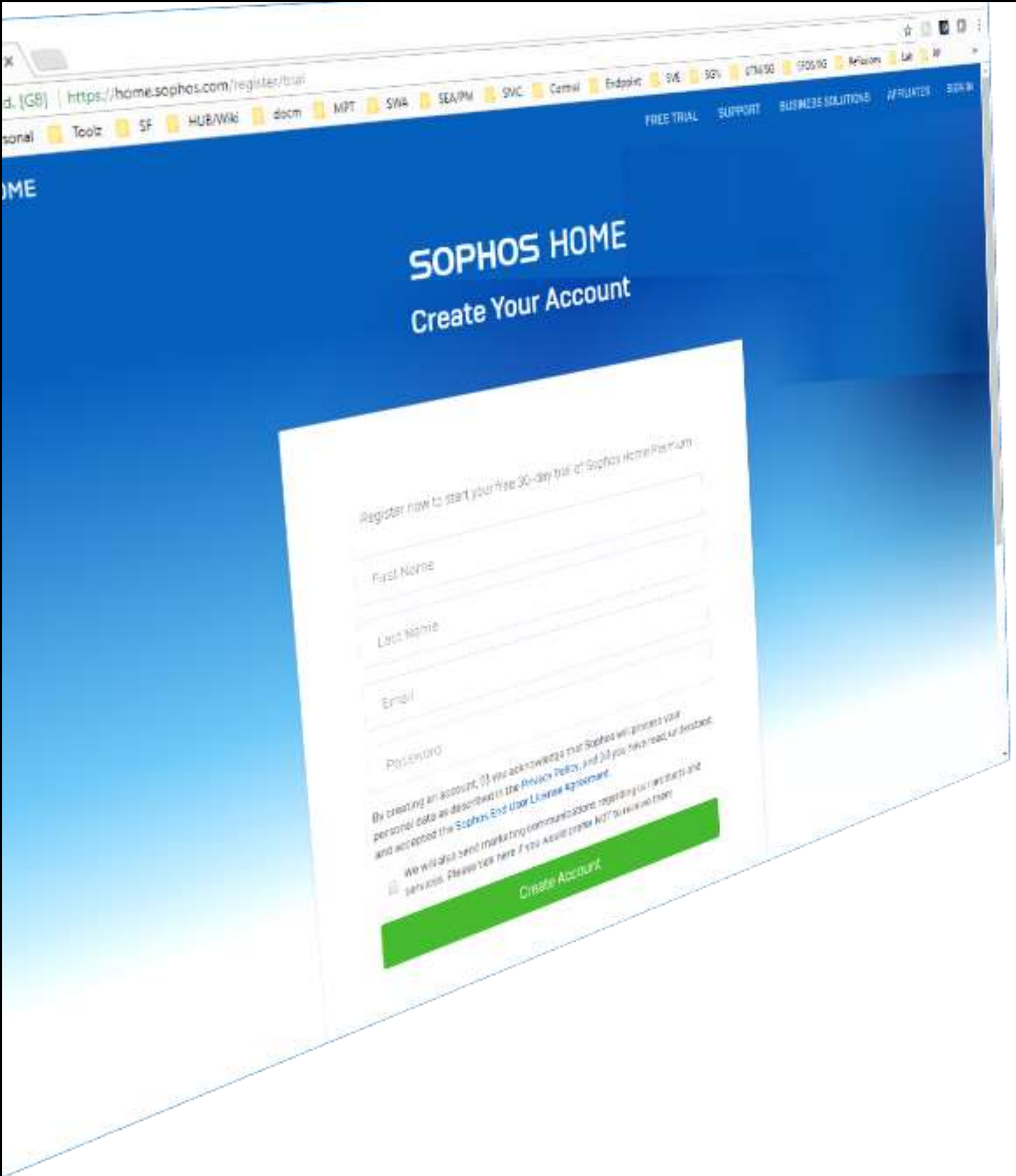
Many apps with 100,000-500,000 installations

Millions of devices infected



Sophos Security Best Practices and Recommendations

- Run an anti-malware app – **Sophos Mobile Security for Android** is **FREE**, or can be **managed** in Sophos Central
- Stick to the **official app stores**, not perfect but…
- Avoid low reputation apps – **think before installing**
- Make sure your device's OS is up to date (if you can…)
- If in doubt about your network, use VPN or use cellular/mobile data
- Manage your mobile devices with **Sophos Mobile**
- Configure Mobile Management for Security
  - Jailbreak/Rooting detection
  - Version check/enforce upgrades
  - Restrict devices and remove unneeded features if possible



SOPHOS HOME

Create Your Account

Register now to start your free 30-day trial of Sophos Home Premium.

First Name

Last Name

Email

Password

By creating an account, (1) you acknowledge that Sophos will process your personal data as described in the Privacy Policy, and (2) you have read, understood and accepted the Sophos End User License Agreement.

□ We will also send marketing communications regarding our products and services. Please tick here if you would prefer NOT to receive them.

Create Account

Sophos Home

home.sophos.com

Manage 10 Windows / Mac Computers

Same Great Sophos Engine

Web Content Filtering

naked security by SOPHOS

Award-winning computer security news

SOPHOS

Security made simple.

Thank You