The University of Queensland Malware Overview

Peter Stewart
CISSP CCIE R&S

August 2017

SOPHOS

What we will cover today

- *What is Malware*
- *The Malware Challenge*
- *Motivation of a Malware Author*
- *Who's making all the Malware*
- *Malware Trends and Delivery Systems*
- *How to protect your devices*
- *The Future of Malware Detection*

SOPHOS

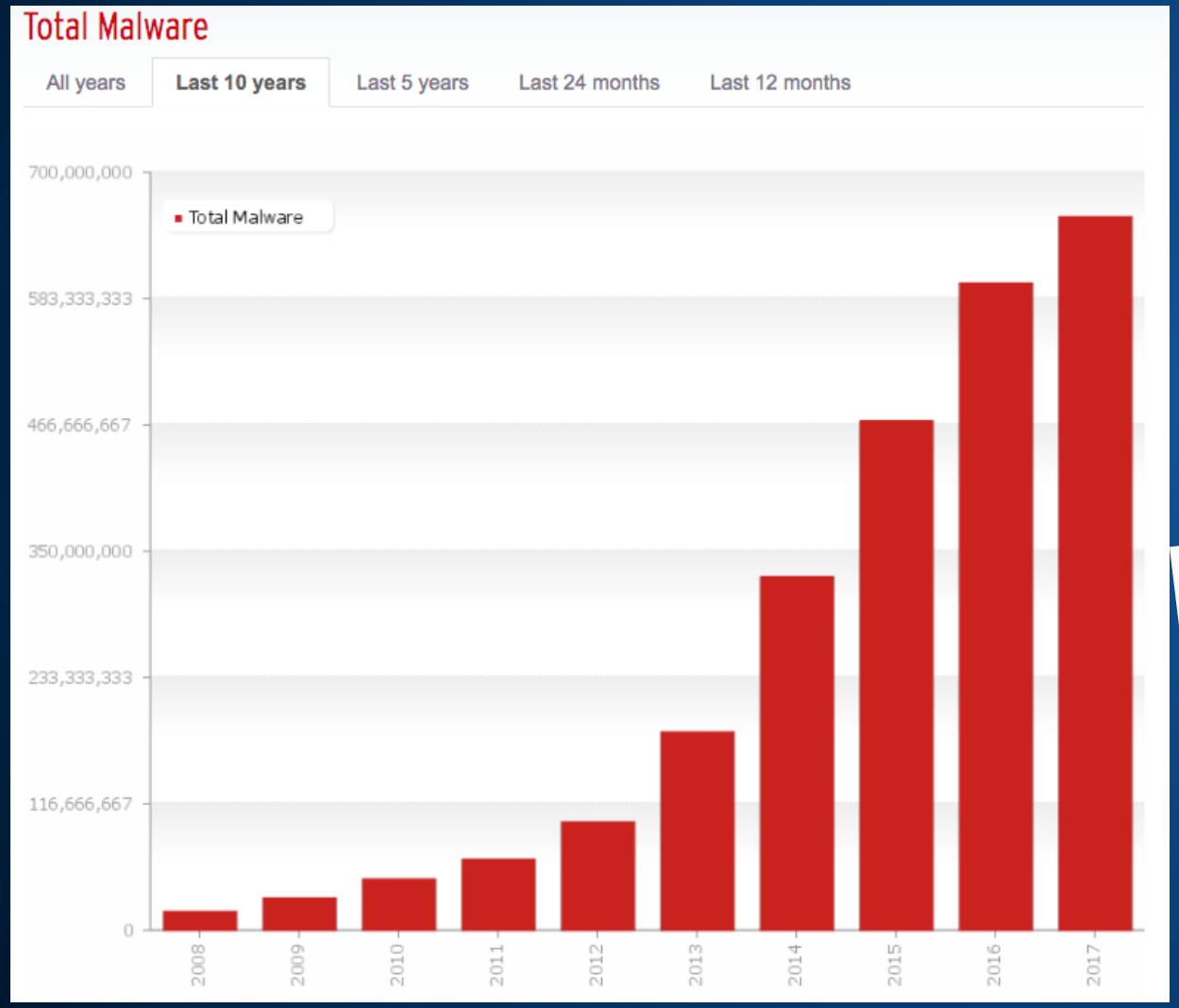
What is Malware

Catch-all term for any sort of software designed with malicious intent.

MALicious softWARE

SOPHOS

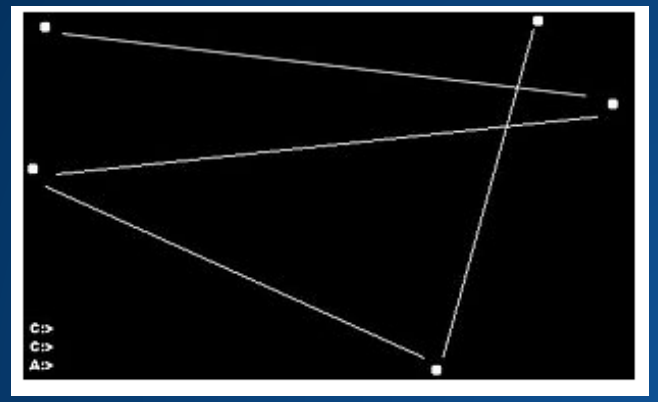
The Malware Challenge



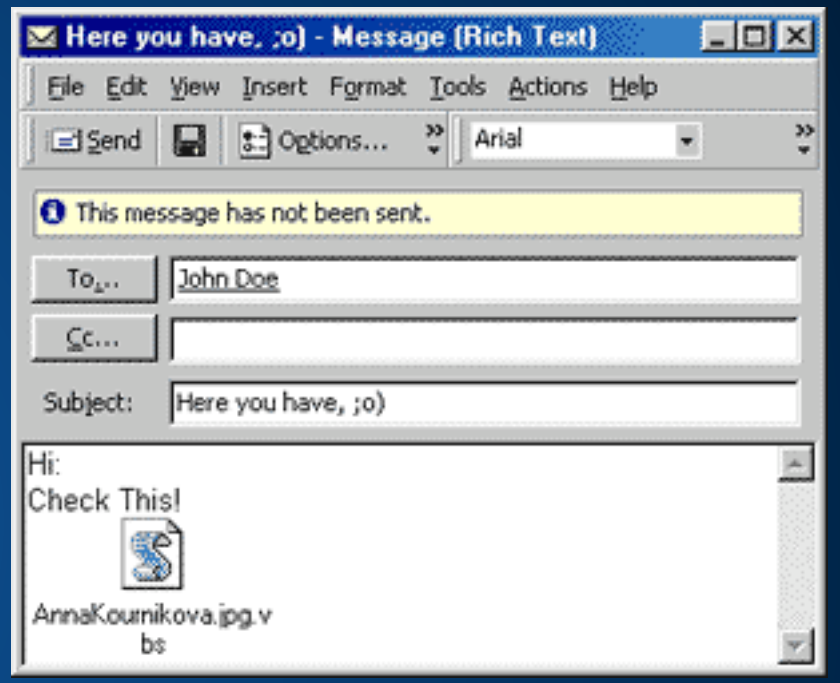
SOPHOS

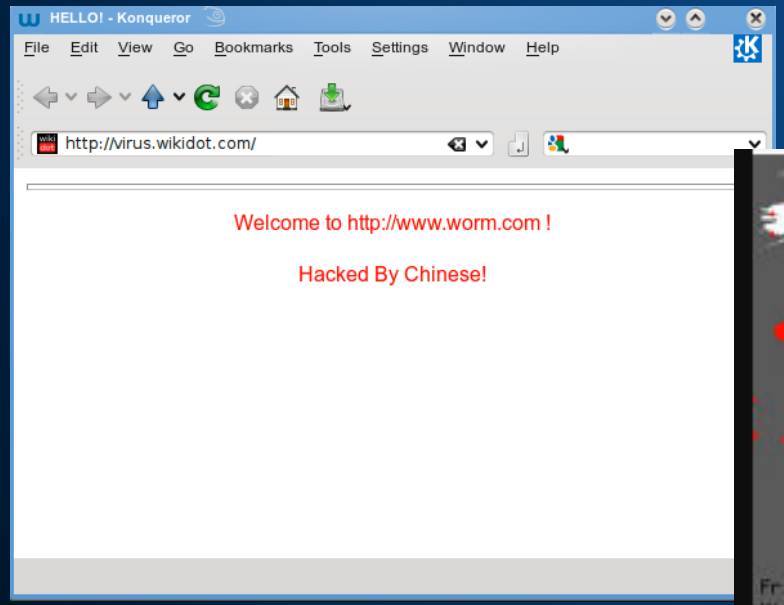
Motivations of a Malware Author

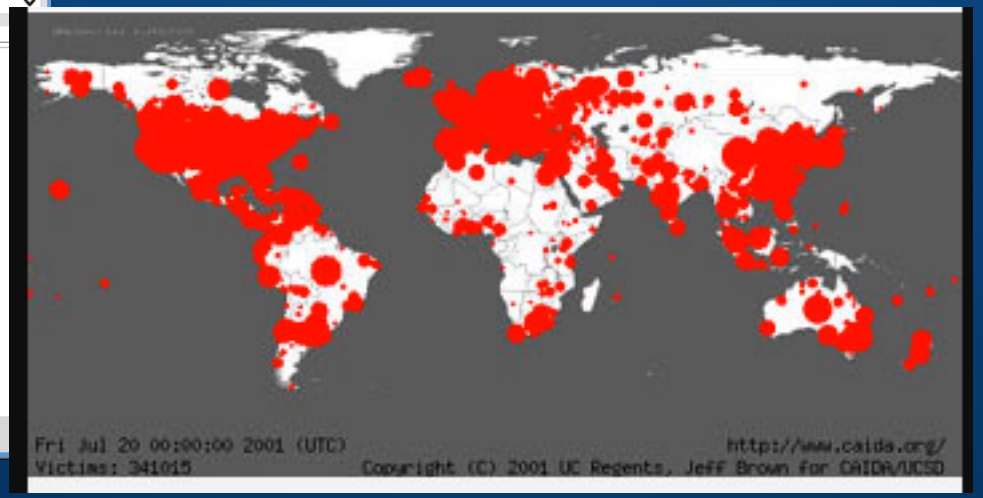
Ping-Pong virus



The Anna Kournikova worm







Code Red Worm

SOPHOS

Motivations of a Malware Author

South Korean Company Agrees To Pay Hackers $1.5 Million Bitcoin Ransom To Unlock Its Files

Dell Cameron
Jun 21, 2017, 7:00am · Filed to: cybersecurity

Share

WannaCry Ransom Bitcoins Withdrawn from Online Wallets

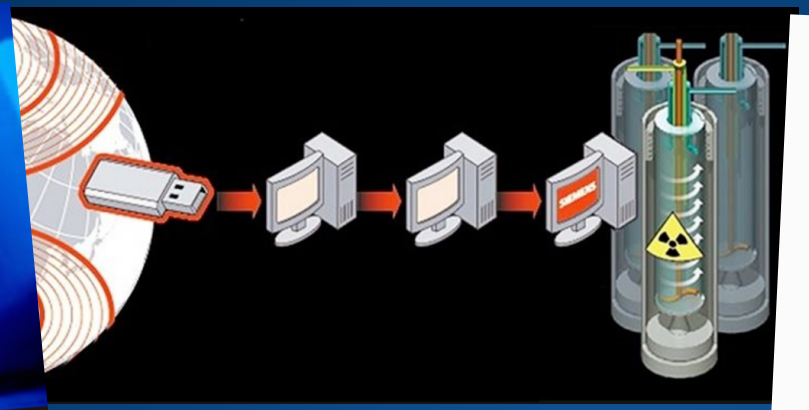
More than $140,000 in digital currency paid by WannaCry victims has been removed from online wallets.

Latest ransomware twist: A demand for $250,000

Following last week's NotPetya outbreak, a new ransom note demands bitcoin in exchange for a security key that decrypts locked files.

SOPHOS

Motivations of a Malware Author



Security

US officials confirm Stuxnet was a joint US-Israeli op

Well, sure ... so why are you telling us, Mr President?

By John Leyden 1 Jun 2012 at 15:14

Country	Share of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

Motivations of a Malware Author

US-CERT issues North Korean cyberattack patch warning

15 JUN 2017 7

Vulnerability

China blamed after ASIO blueprints stolen in major cyber attack on Canberra HQ

Updated 28 May 2013, 7:51am

TOP 5 COUNTRIES WITH OFFENSIVE CYBER CAPABILITIES

F-Secure Life, Threats & Hacks

1. The United States
2. Israel
3. Russia
4. China
5. Iran/North Korea

Who's Making all the Malware

'Paunch', Blackhole exploit kit creator and Gang arrested in Russia

Saturday, December 07, 2013 Mohit Kumar

Who's Making all the Malware

Cybercrime Inc: How hacking gangs are modeling themselves on big business

Franchises, resellers, customer service, collaboration tools, and training -- professional hacking organizations are now operating like any other business.

By Danny Palmer | September 1, 2016 -- 15:56 GMT (01:56 AEST) | Topic: Cyberwar and the Future of Cybersecurity

FBI: Cybercrime Gang Stole $1.2 Million via Bank Malware

Prosecutors Announce Guilty Plea as Part of Ongoing Investigation

Mathew J. Schwartz (euroinfosec) · February 6, 2017 0 Comments

IaaS (Infrastructure-as-a-Service) - Amazon Web Services (AWS), Microsoft Azure

PaaS (Platform-as-a-Service) - Salesforce.com Force.com, Google App Engine

SaaS (Software-as-a-Service) - Google Apps, Microsoft Office 365

CaaS (Crimeware-as-a-Service)

SOPHOS

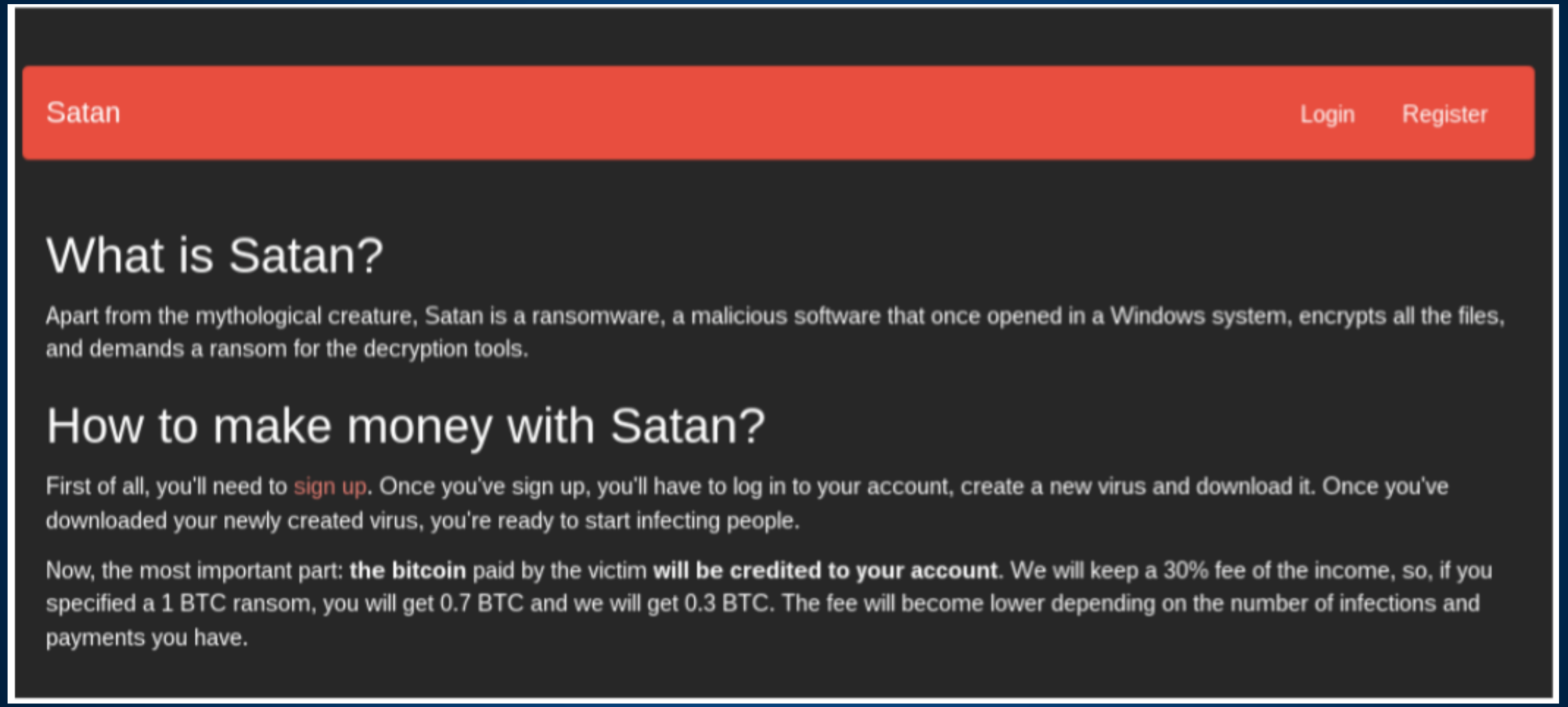
Who's Making all the Malware

Crimeware-as-a-Service (CaaS)

	Bitcoin	USD
Custom Ransomware (CTB-Locker)	2	$1,239.62
24 Hour DDoS	0.743	$460.52
Social Media Hacking, Per Account	0.104	$64.46

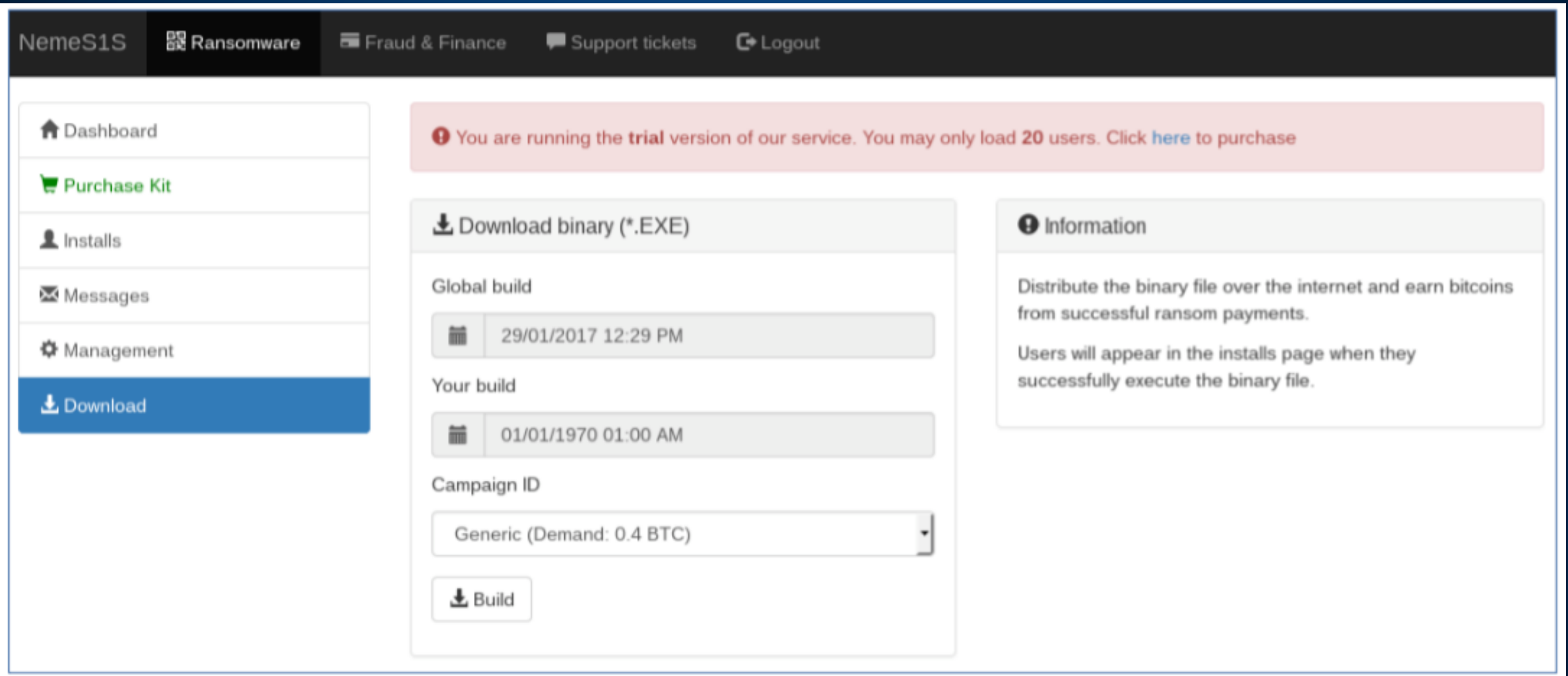
SOPHOS

Who's Making all the Malware



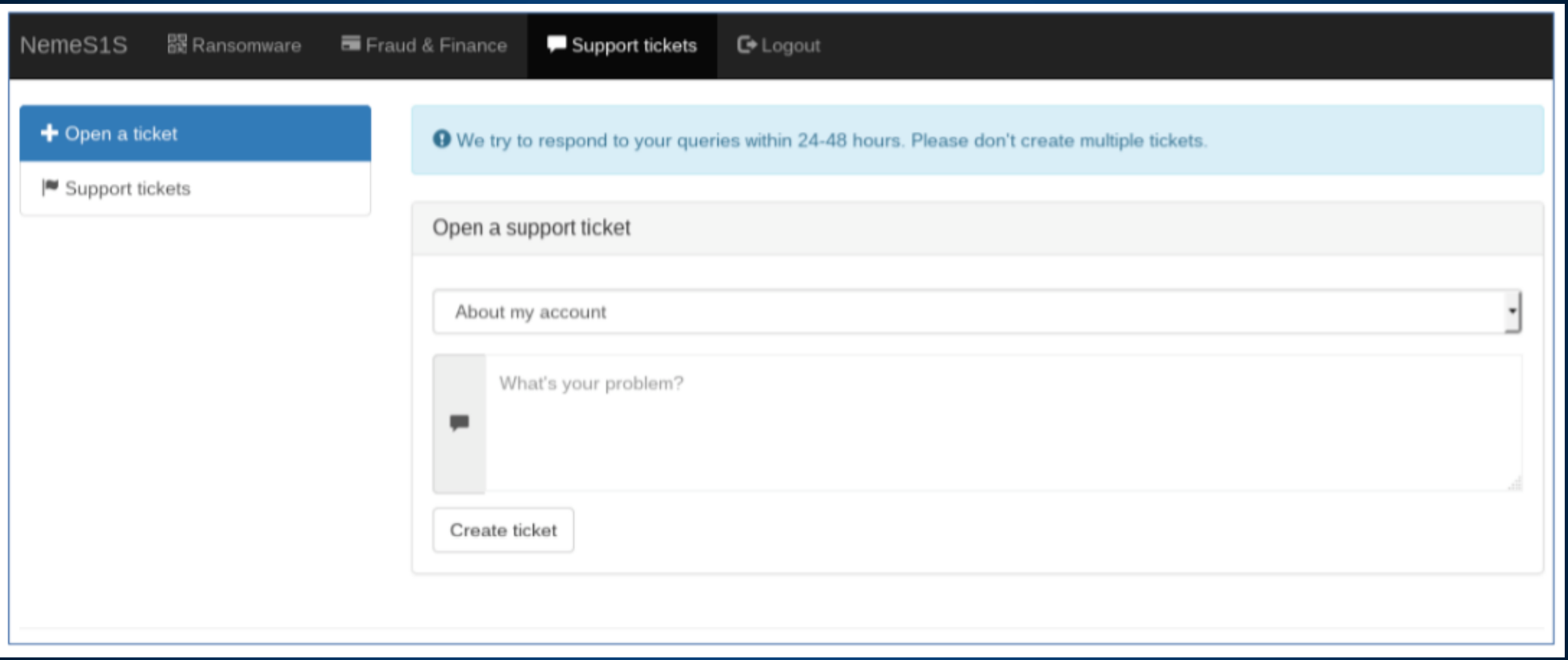
SOPHOS

Who's Making all the Malware



SOPHOS

Who's Making all the Malware



SOPHOS

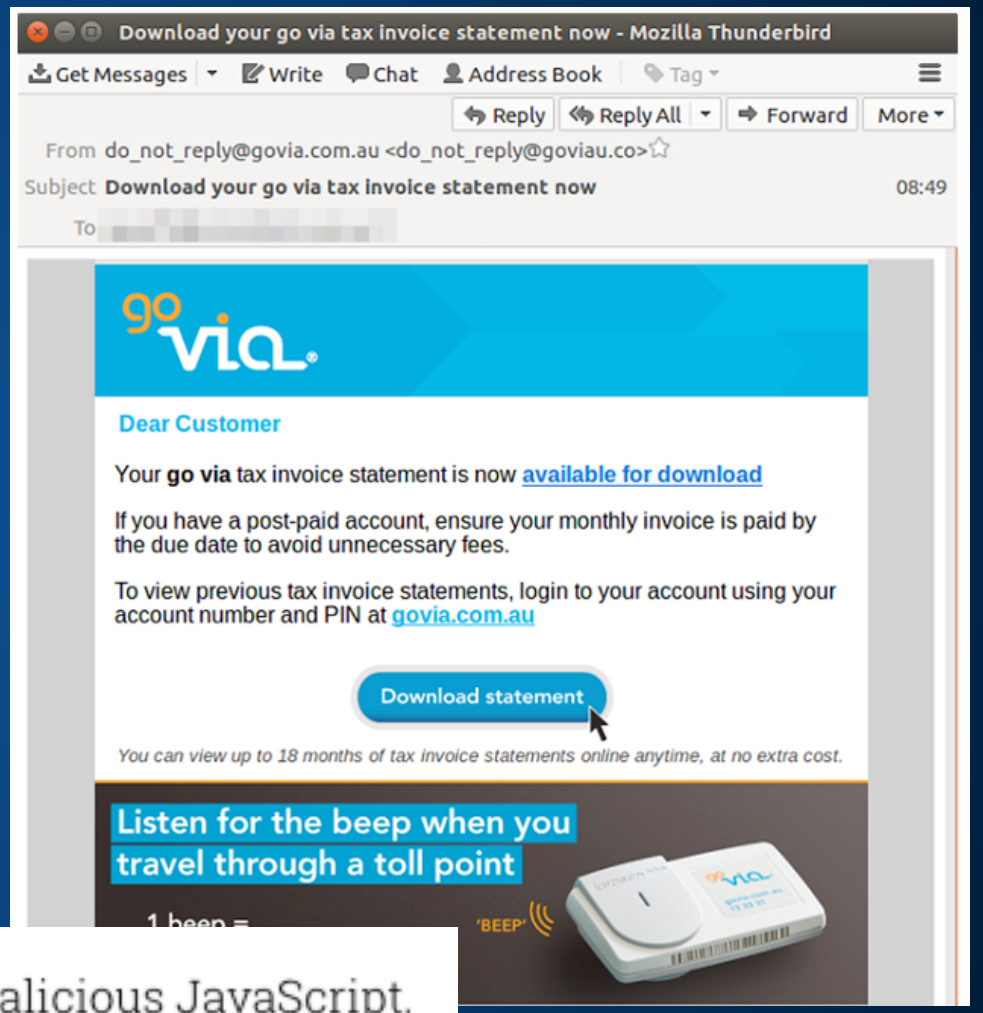
Malware Trends and Delivery Systems

Malicious Websites and Drive-by-downloads

Malvertising

Man-in-the-middle (MitM) Attack

Email Phishing



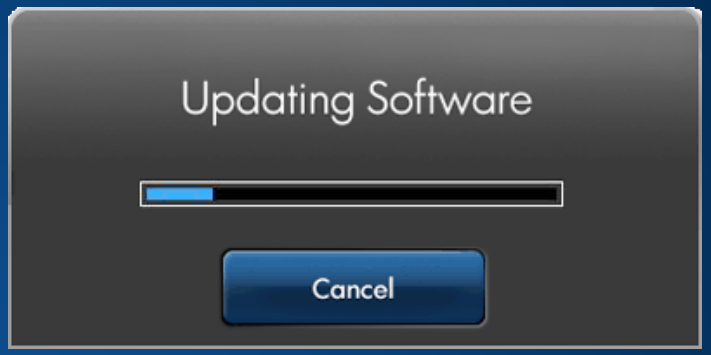
Clicking the 'Download statement' button runs a malicious JavaScript.

SOPHOS

How to Protect Your Devices

Update your OS

Update your Applications



By JONATHAN BERR / MONEYWATCH / May 16, 2017, 5:00 AM

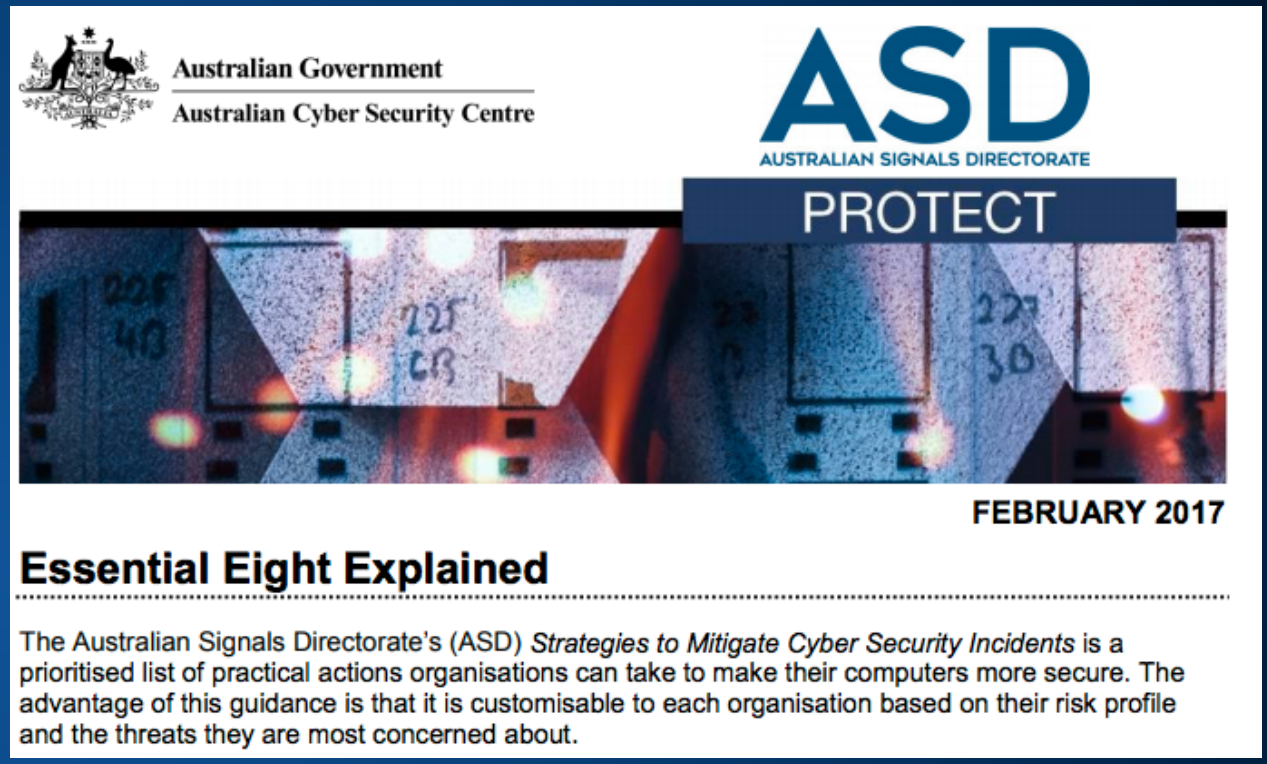
"WannaCry" ransomware attack losses could reach $4 billion

1. March 14, 2017, Microsoft issued security bulletin MS17-010
2. May 12, 2017 (Two months later) WannaCry used NSA exploit EternalBlue vulnerability to spread

SOPHOS

How to Protect Your Devices

- Patching operating systems
- Patch Applications
- Restrict administrative privileges
- Application Whitelisting
- Multi-factor authentication
- Disable untrusted Microsoft Office macros
- User application hardening
- Daily backup of important data



* Important to know when dealing with government departments or business that work with the government.

SOPHOS

Current Types of Traditional Malware Protection

- Anti-Virus Scanning (Using Signatures of known Malware)
- Application Blacklisting (Blocking Unused/Unwanted Applications)
- Application Whitelisting (Allowing only whitelisted applications to run)
- Peripheral Control (Blocking the use of USB's, Bluetooth, Wireless Bridging)
- Blacklist URL (Blocking an Endpoint from going to known bad webpages)
- Host Intrusion Prevention System (Malicious traffic detection, Suspicious file detection)

* Different Security vendors could do one or more of the above

SOPHOS

The Future of Malware Detection

Issue: Targeted Malware created for a single use. How do you catch something you have never seen before?

Answer: Anti-Ransomware (Stopping files from being encrypted (Bad Encryption))

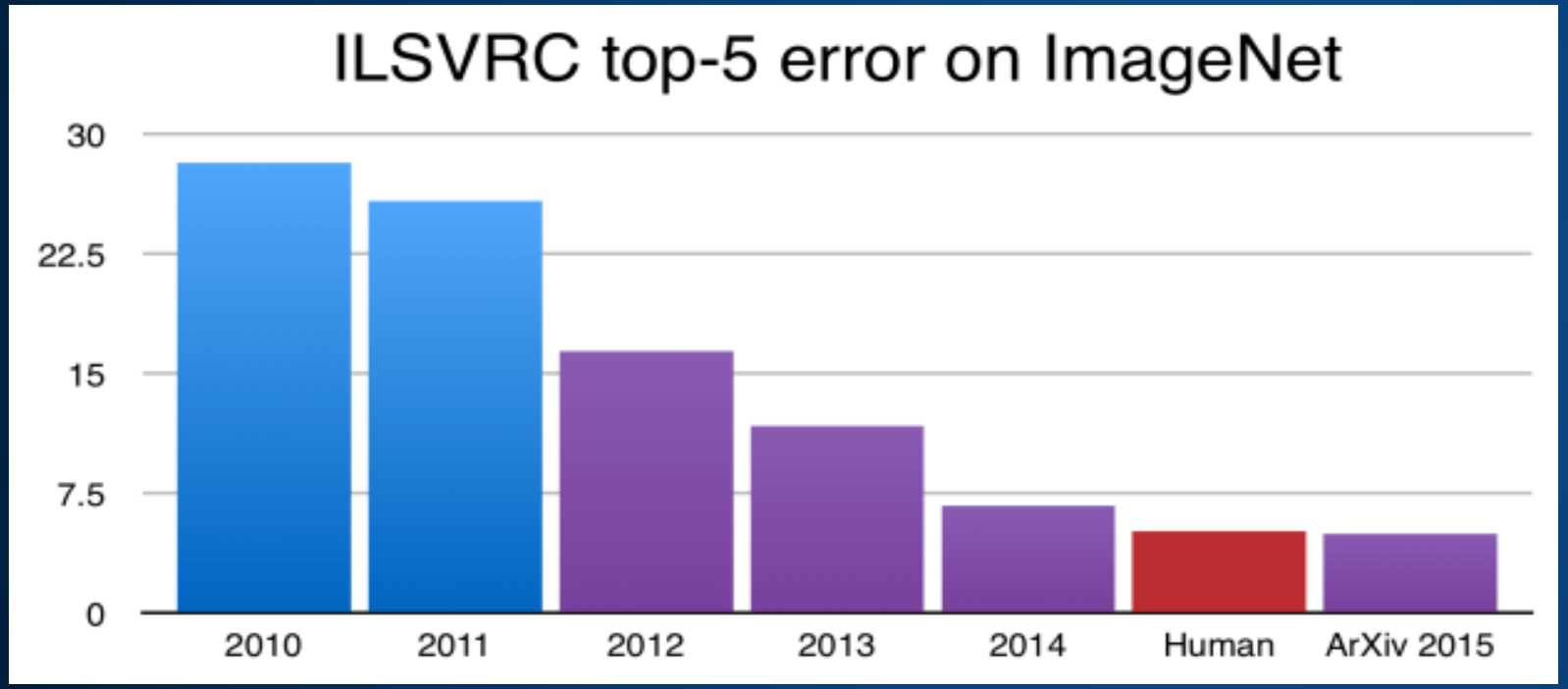
Anti-Exploit (Blocking processes using known exploits eg: Buffer Overflow's)

Machine Learning (Latest and greatest Malware detection)

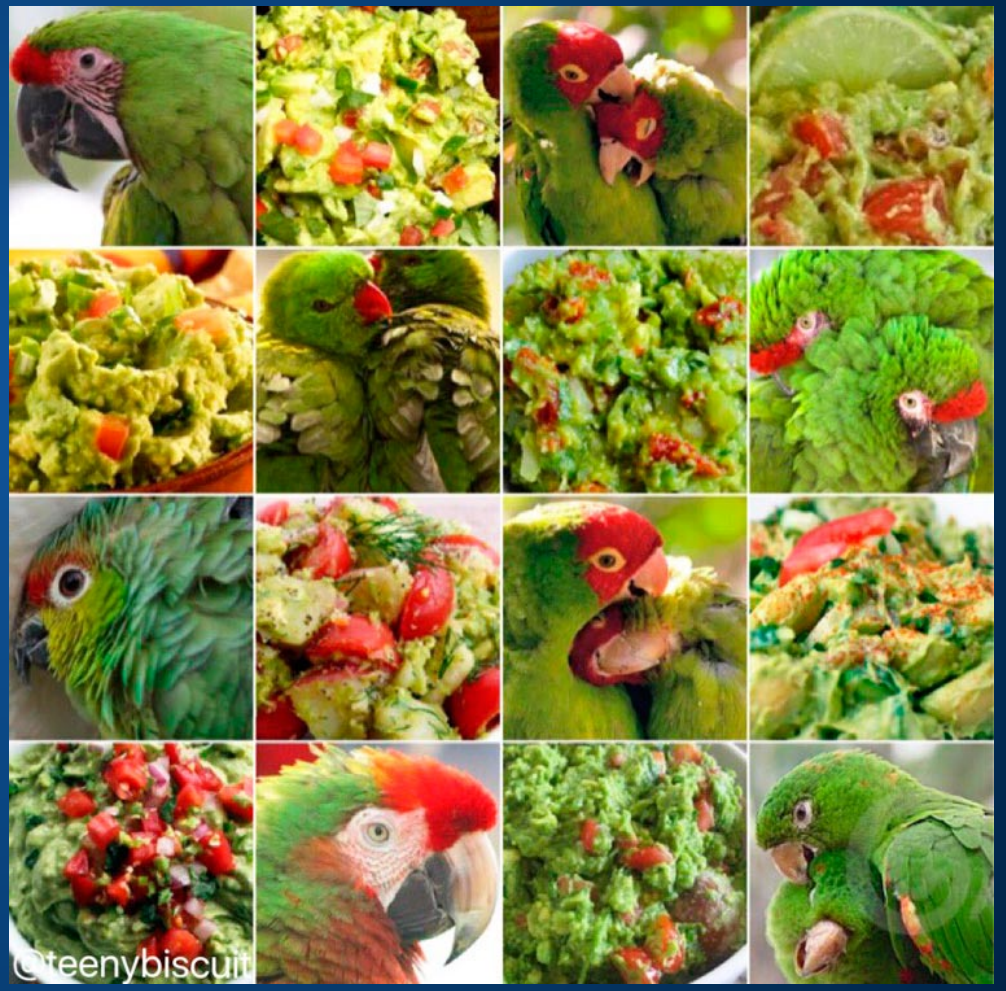
** All of the above "do not" need signatures

SOPHOS

Introducing Machine Learning



What is Machine Learning?



Machine Learning

Sophos Home – Free Anti-Virus

https://home.sophos.com

SOPHOS

Questions

SOPHOS

Things I wish I knew when starting out

Its not what you know, its who you know

1. Join Linkedin and connect with people who have the job you want.
    1. *Look at their job history*
    2. *Ask questions*
2. Join local User Groups
    1. *Meet people in the industry*
    2. *Help organise events*
3. Find a Mentor
    1. *Can help you not make the same mistakes they made*

SOPHOS

SOPHOS

Security made simple.