Adaptive Security

Innovix Symposium 2017

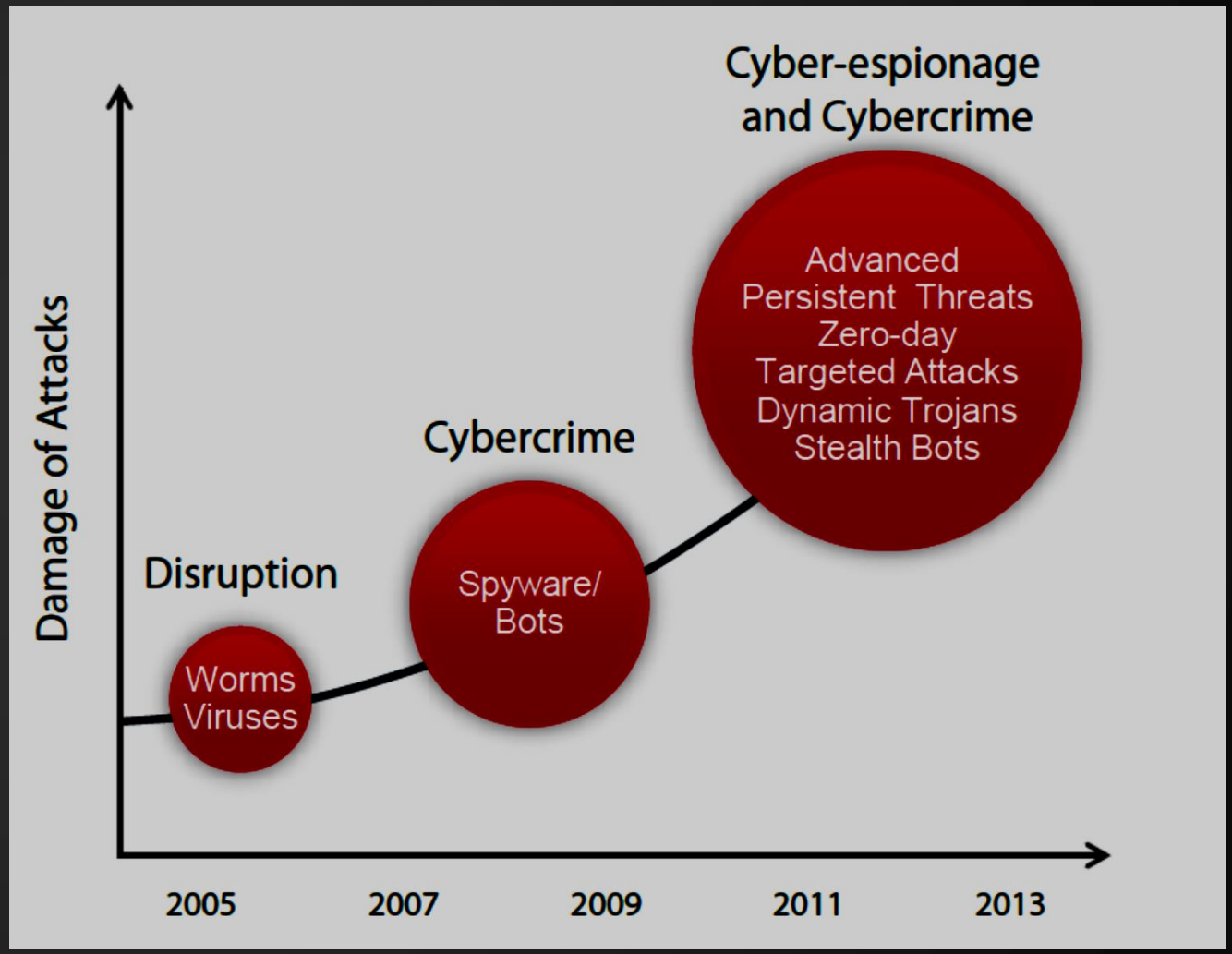
Roy Low (HP Inc)

Today's topics

1. What's happening in the Cyberworld?
2. Where are the threats and COST in Cyberworld?
3. Why Singapore has to stay vigilant in Cyber Wellness?
4. How to Protect your client EndPoint Device. Introducing Device, Identity and Data
5. HP Studios presents THE WOLF (Healthcare), THE HUNT CONTINUES
6. Call to Action

CYBER ATTACKS AND MOTIVES ARE EVOLVING – What's Happening

- **The reward is high – e.g. in Feb 2016, Hackers attempted to steal $1B via compromised SWIFT credentials of bank employees[1]**
- **Malware is readily available & getting increasingly sophisticated**
- **Increasingly, the PC is the entry point for attacks**
- The TAM is large - standardization of PC architecture makes the opportunity of breaches larger
- Companies don't want to publicly admit to security breaches



Source: *The Evolution of Cyber Attacks, FireEye*

Security Imperative and today's threat

$9.5M

is the average total cost of breach[1]

200%

increase in attacks targeting notebooks & desktops[2]

81%

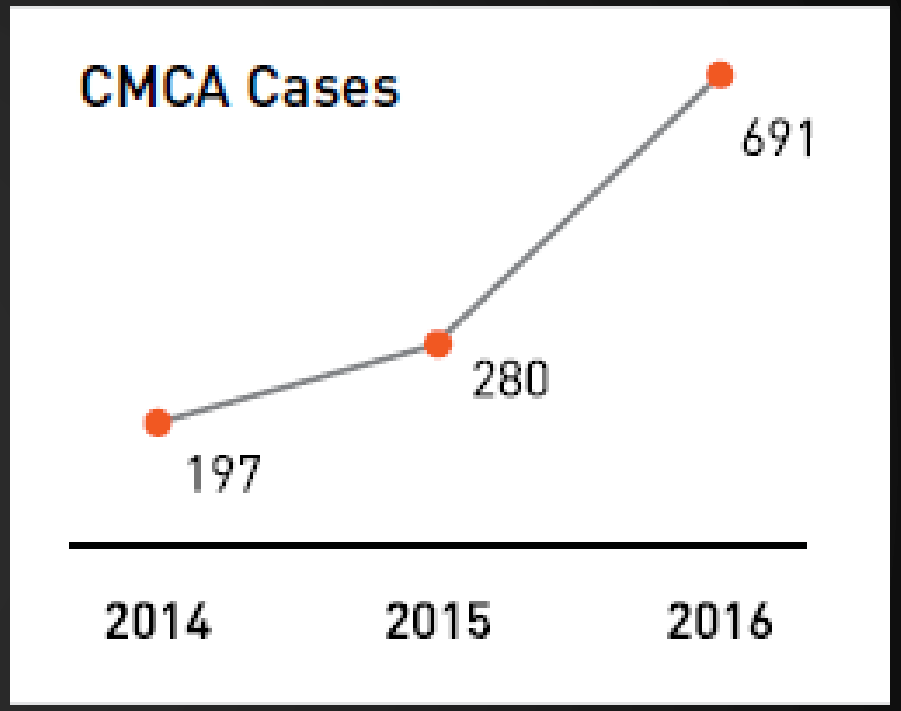
cite insecure web browsers as a primary attack vector[3]

every **40** seconds

a business was attacked with ransomware in Q3' 2016[4]

CYBER ATTACKS IN SINGAPORE ARE INCREASING

- **Under the Computer Misuse and Cybersecurity Act (CMCA) more than double year on year to 2016, 691 cases reported**
- **Ransomware, online and banking accounts constituting the top categories**
- **Some reports noted that there may be as many as 550 ransomware- related attacks every day in Singapore**
- **Nearly 1,800 website defacement were detected**
- **Attackers sought personal data that could be trade in underground market**



Source: *Singapore Cyber Landscape 2016*

COMMITTEE ON THE FUTURE ECONOMY 2017

Strategy 4: Build strong digital capabilities

37. Digitalisation is creating new industries as well as transforming many existing ones, such as finance, advanced manufacturing and healthcare. Digitalisation also offers businesses, small and big, an effective means of reaching global markets. Building on our Smart Nation vision, we can tap on the economic opportunities offered by the digital economy. To do so, we must promote the adoption of digital technologies across all sectors of the economy. In addition, we must build strong capabilities in digital technologies, in particular data analytics and cybersecurity, which can be applied flexibly across sectors. Data will be an increasingly important source of comparative advantage and we need to improve our ability to use it productively in the economy.

Source: Report of The Committe on the Future Economy

Do you agree?

"Cyber Wellness helps in Productivity."

Singapore Cyber Landscape 2016 Report

David Koh, Chief Executive Cyber Security Agency of Singapore

"Singapore similarly faced such threats. Our high level of connectivity comes with a corresponding level of vulnerability…… "

Source: Singapore Cyber Landscape 2016

Summary:

- Cyber threats are here!
- Singapore is not spared, be prepared!
- Protect your client end point device!

EXECUTIVE SUMMARY

COMMON CYBER THREATS IN SINGAPORE

Prevalent cyber threats observed in Singapore's cyberspace[2] in 2016 were defacements, phishing, ransomware, and compromised Command & Control (C&C) Servers, the last being potential launch-pads for other cyber-attacks, such as DDoS. A snapshot of these common cyber threats is as follows:

Ransomware:

It is one of the biggest cybersecurity threats to businesses and individuals today. Some reports noted that there may be as many as 550 ransomware-related attacks every day in Singapore. However, many cases may go unreported. Some people may decide to reformat their affected computer, and companies may not want to report it to protect their corporate reputation. CSA received 19 reports of ransomware cases from individuals and SMEs in 2016. Cerber, CryptoLocker and Locky were among the types of ransomware reported. As ransomware attacks grew in 2016, SingCERT issued an advisory in May 2016 to warn the public of such dangers and provided precautionary measures to be adopted.

Defacements:

Nearly 1,800 website defacements were detected in Singapore in 2016, with the majority being websites of SMEs from a range of businesses such as interior design and manufacturing. The perpetrators included hacktivists keen to promote a certain ideology, and whose attacks were observed across other countries as well. One in 10 defaced websites was hosted on servers running outdated operating systems, which may have resulted in them being vulnerable to such attacks.

C&C Servers & DDoS:

More than 60 C&C servers were detected. It is not immediately apparent who might have set them up, what they intended to do with these servers, and if any damage was done. Whenever a new C&C server is detected, SingCERT will inform the respective Web hosting providers to rectify the issue. Potentially, C&C servers could be used to control botnets – a network of compromised computers ¬– that in turn could be mobilised for DDoS attacks. The thousands of IoT devices marshalled for DDoS attacks in the USA in October 2016 may hint of similar threats to come. DDoS ransom threats were also observed in Singapore's cyberspace, believed to be carried out by cyber criminal groups.

Phishing:

More than 2,500 phishing URLs were detected in 2016, with the Banking & Finance sector appearing to be the most spoofed (31 per cent of all observed phishing URLs). Among online services, PayPal was spoofed most often in phishing campaigns. CSA also observed that file-hosting service providers were popular targets as hackers could easily harvest user credentials from there. Some Government institutions were also spoofed, as attackers sought personal data such as passport numbers that could be traded in underground markets.

THE WORLD'S MOST SECURE & MANAGEABLE PCs[2]

2017 BEST PRODUCT ENDPOINT SECURITY SOLUTION CDM

CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

HP Sure Start Gen3 BIOS Protection

HP Multi-Factor Authenticate for identity

HP Sure View Integrated Privacy Screen

HP Sure Click browsing security solution

HP Manageability Integration Kit

EliteBook 800 G4

EliteBook x360

EliteDesk 800 G3

HP ELITE PCs WITH INTEL® 7TH GENERATION PROCESSORS

HP security features available with HP Elite devices

HP SURE START GEN3[1]

Self-Heals BIOS from

Malware, Rootkits, Corruption

in less than a minute!

Now with

Runtime Intrusion Detection

BIOS Configuration & Policy Protection

Microsoft® SCCM Integration

Customer Benefits

Minimize Downtime

Increase Security

Simplify Management

HP SURE START GEN3[1]

&

Bromium®

HP Sure Click

Browsing Security Solution

HP Sure Click provides hardware-enforced security for web browsers,
protecting your PC from websites infected with malware, ransomware or viruses[5].

web-download for the HP EliteBook x360 G2 on www.hp.com/go/clientmanagement and supports Microsoft® Internet Explorer and Chromium™

How to make Web Browsing more secure?

Educate End User

Requires developing, conducting training, and consumes user's time.

Human error & mistakes will continue happening.

White & Black Lists

Requires regular maintenance of the lists.

Can significantly limit end user productivity.

Hardware-Enforced Isolation

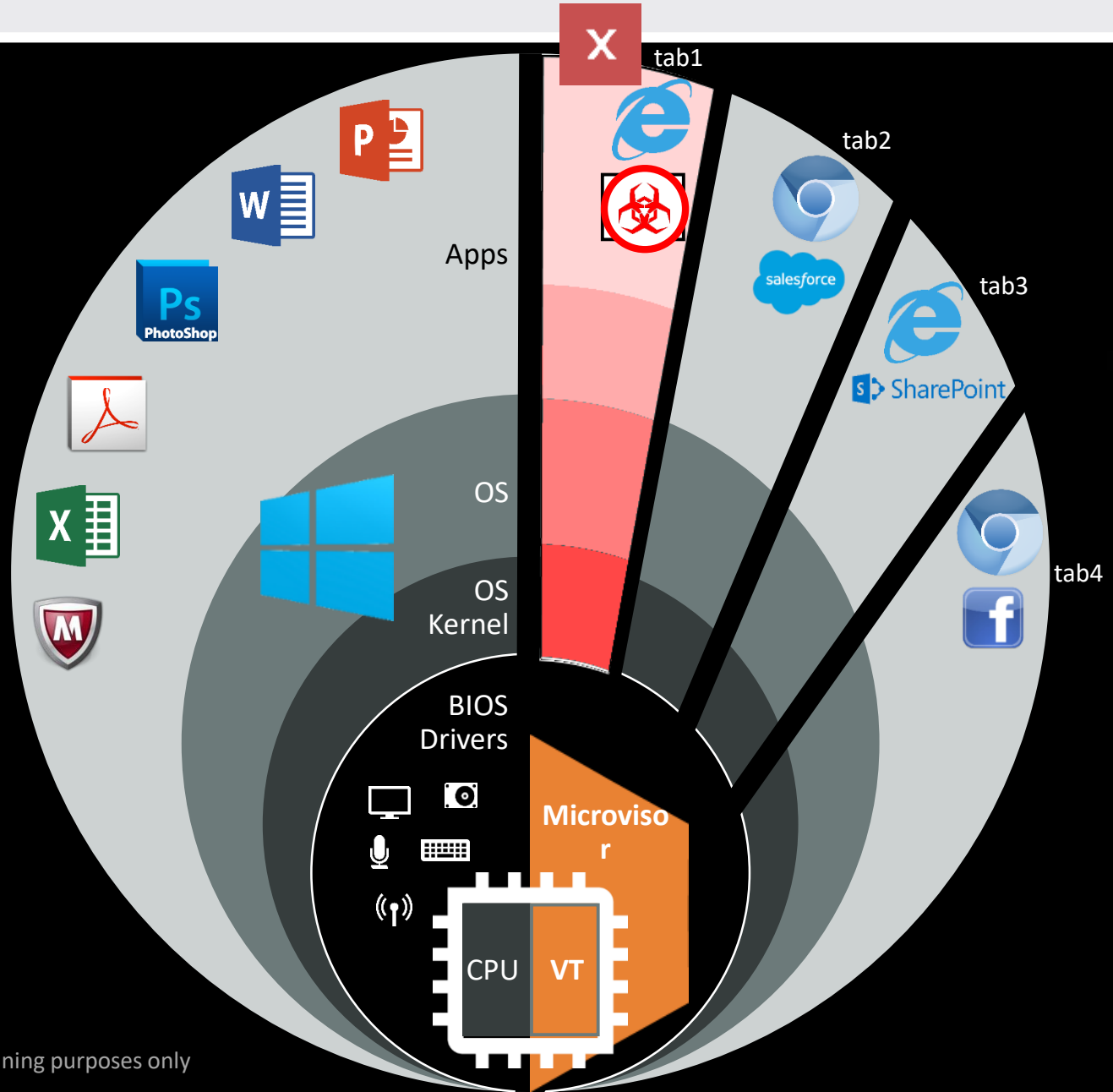
Isolates each Web Browser Tab through virtualization. Once a Tab is closed whatever happens within it is discarded.

Users browse without worrying about malicious links & web sites.

HP Sure Click – how it works

81%

say web-borne malware can be undetectable[3]



HP Sure Click

Each web browser **tab** is opened automatically in a CPU-isolated Micro Virtual Machine

Malware impacting one tab has NO impact on any other tab, app or the OS

Just close the tab & the malware's gone

HP Sure Click

HP SURE VIEW

WORLD'S ONLY INTEGRATED PC PRIVACY SCREEN[1]

Built in electronic privacy screen prevents visual hacking

Simple as pressing F2

Visual protection starts when others are 35° from the center

Viewed at an angle, it reduces up to 95% of the visible light

9 out of 10 attempt to steal sensitive business information using only visual means were successful[8]

HP Sure View

Security Video – The Hunt Continues Healthcare

https://www.youtube.com/embed/FqibWHfn_Yc?start=0&end=236

Security Video – The Hunt Continues Part 1 & 2

Call to Action

- Learn more about HP Secure feature
http://www8.hp.com/us/en/campaign/computersecurity/

- Use HP Security Awareness Campaign video, as your entry point for client discussion

- Share HP Studios with your client
  - The Wolf (FSI): The Hunt (FSI) - https://www.youtube.com/watch?v=U3QXMMV-Srs
  - The Wolf (Healthcare): The Hunt Continues - https://www.youtube.com/watch?v=FqibWHfn_Yc
  - Rivolta: Inside the Mind of Canada's Most Notorious Hacker - https://www.youtube.com/watch?v=ia-BtKzx0So

- Nothing is SAFE, if they are isn't HP Secure. Protect your client endpoint device with HP latest range of Desktop, Notebook, Mobility, Workstation and Printers.

THANK YOU