Endpoint Protection : Last line of defense?

First TC Noumea, New Caledonia 10 Sept 2018

Raja Azrina Raja Othman Independent Information Security Advisor

MSc Information Security & Computer Crime BSc Computer Engineering Co-founder of MyCERT Date: 10 Sept 2018

OVERVIEW

UNDERSTANDING ENDPOINT SECURITY AND THE BIG PICTURE

- Rapid development in security technology requires understanding on how the many solutions work together, not against each other.
- Good understanding of technology allows better design and implementation when:
 - Integrating Security Controls in a new infrastructure, or
 - Incorporating new or optimizing existing security controls in response to recent threats.
- Understanding the role of **Endpoint Security Controls** as the last line of defense.

CYBER SECURITY IS A CEO, NOT CIO ISSUE THE BUSINESS IMPACT OF CYBER CRIME IS OVERWHELMING

Cyber threats are a material risk to your business

200+DAYS

Median number of days attackers are present on a victims network **before detection**

Source Microsoft Advanced Threat Analytics \$3 trillion

Impact of loss of productivity and growth by 2020

Source : McKinsey Risk and Responsibility in Hyperconnected World Report 2014

\$4 MILLION

Average **cost of a data breach** (up 29% since 2013) [383 Org in 12 countries]

Source : 2016 Ponemon Institute Cost of Data Breach Study

50%

Attacks are fast, efficient, and easier to implement

of those who open phishing messages, click attachments within the first hour

Source Microsoft Advanced Threat Analytics

IRSTTC NEW CALEDONIA

CHANGES IN CYBER THREAT ?

MALWARE | SELF PROPAGATE | DISRUPT | PERSISTENT

Blaster Worm Discovered: August 11, 2003

- Propagates via network (network worm)
- Scans and connect on TCP port 135
- **Exploit** MS Windows DCOM RPC Interface Buffer Overrun Vulnerability.
- Date trigger payload that launches DDoS SYN flood against windowsupdate.com
- Sends large amount of data sufficient to overrun the buffer
- Gain shell on TCP port 4444 **backdoor**
- Invoke 'tftp.exe' download
- System to reboot in order to launch

Created by an 18-year-old from Minnesota, sentenced to 18mo prison term.

Wannacry Ransomware Discovered: May 12, 2017

- Propagates via network (network worm)
- Scans and exploit SMB protocol
- Eternal Blue exploit
- Install backdoors (Double Pulsar)
- Encrypting data and demanding ransom payments in Bitcoin
- Includes Kill switch (prevented infected computers from spreading WannaCry further).
- Affected more than 200,000 computers across 150 countries (manufacturing plants, hospitals)
- System reboot/bluescreen on certain platform.

Created by a North Korean computer programmer, claimed to be state-sponsored attack.

DOJ Charges North Korean in Sony Hack, Wanna Cry Attack (September 6, 2018)

The US Department of Justice (DOJ) has charged Park Jin Hyok, a North Korean computer programmer, in the 2014 attack against Sony Pictures, a 2016 theft from Bangladesh Bank, and the 2017 Wanna Cry malware attack. The complaint alleges that Park carried out the attack against Sony Pictures on behalf of the North Korean government; it also links Park to the Lazarus Group, which is believed to be involved in the Wanna Cry attack and a Bangladesh Bank theft.

FIRST TC NEW CALEDONIA

RECENT INCIDENTS/VULNERABILITY HIT ENDPOINTS

RANSOMWARE | HARDWARE LEVEL VULNERABILITY

	Wana Decrypt0r 2.0
	Ooops, your files have been encrypted!
	What Happened to My Computer? Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Payment will be raised on	Can I Recover My Files?
5/16/2017 00:47:55	Sure. We guarantee that you can recover all your files safely and easily. But you have
Time Left 02:23:57:37	not to enough time. You can decrypt some of your files for free. Try now by clicking <decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.</decrypt>
Your files will be lost on	We will have free events for users who are so poor that they couldn't pay in 6 months.
5/20/2017 00:47:55	How Do I Pay? Payment is accepted in Bitcoin only. For more information, click <about bitcoin="">.</about>
Time Left 06:23:57:37	Please check the current price of Bitcoin and buy some bitcoins. For more information, click <how bitcoins="" buy="" to="">. And send the correct amount to the address specified in this window. After your payment, click <check payment="">. Best time to check: 9.00am - 11.00am</check></how>
Albourt billionin Hores to beau billionins?	Send \$300 worth of bitcoin to this address: 12197DPgwueZ9NyMgw519p7AA8isjr65Mw
Contact Us	Check Payment Decrypt

May 2017 - Wannacry Ransomware

on became victim of the PETYN RINSOMERRET.

The barddisks of your computer have been encrypted with an willtary grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

 Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
 Usit one of the following pages with the Tor Browser:

. Enter your personal decryption code there:

(6) Find the second se Second sec

If you already purchased your key, please enter it below.

June 2017 -NotPetya

BAD RABBIT

If you access this page your compute has been encrypted. Enter the ppeared personal key in the fiel below. If succeed, you'll be provide with a bitcoin account to transfe agment. The current price is on the right.

Once we receive your payment you'll got a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

 \checkmark

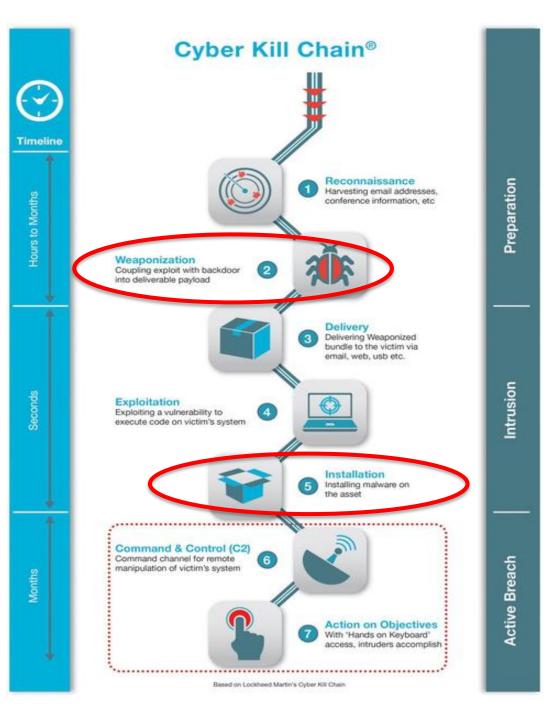
Price for decryption:

Oct 2017 – Bad Rabbit



Jan 2018 – Meltdown and Spectre Kernel memory vulnerability allow memory exploit at hardware level

FIRST TC NEW CALEDONIA

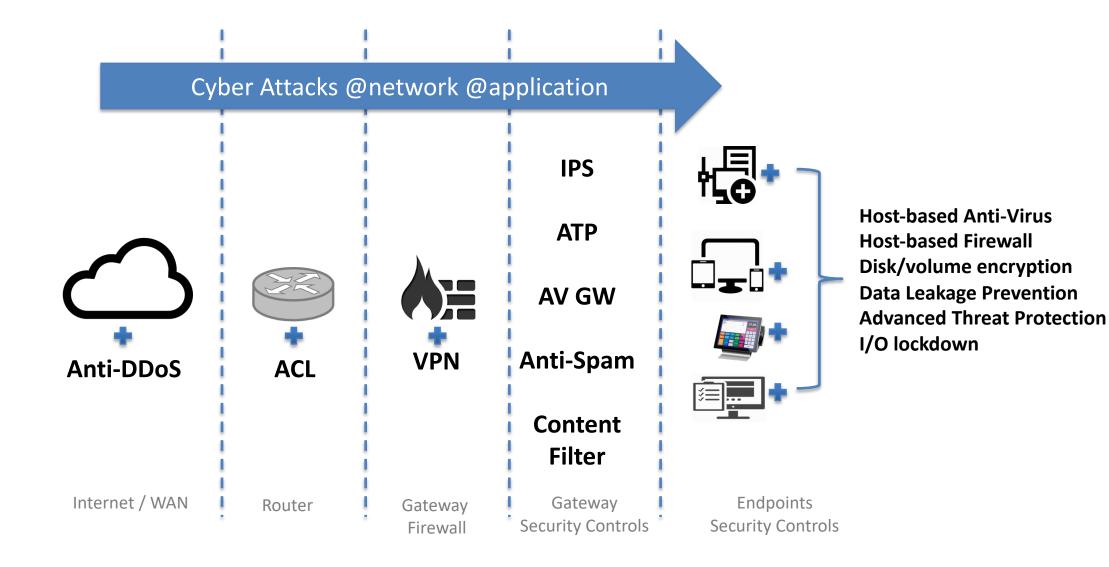


ANATOMY OF A HACK AND WHAT'S AT STAKE

Objective of compromise:

- To **steal** information, credentials.
- To **weaponize** a compromised host as launching pad, man in the middle.
- To **ransom** the victim.
- To gain unauthorized use of computing resources – crypto mining, spam relay, malware hosting

MULTI-LEVEL SUBVERSION TO ULTIMATELY TARGET ENDPOINTS



BLACKLISTING | WHITELISTING | LEARNING

Blacklist: allows everyone access except those listed in the blacklist



Whitelist: denies everyone access except those listed in the whitelist



Blacklisting Technology

- Block/Blacklist selected
 files/applications/URL/domain/content based on
 certain known fact/signature.
- IPS, Firewall, Content Filter, DLP, Anti Malware

Whitelisting Technology

- Application Whitelist Allow installation of only selected files/application based on certain known criteria that is set as policy.
- Network Traffic Whitelist Access Control List

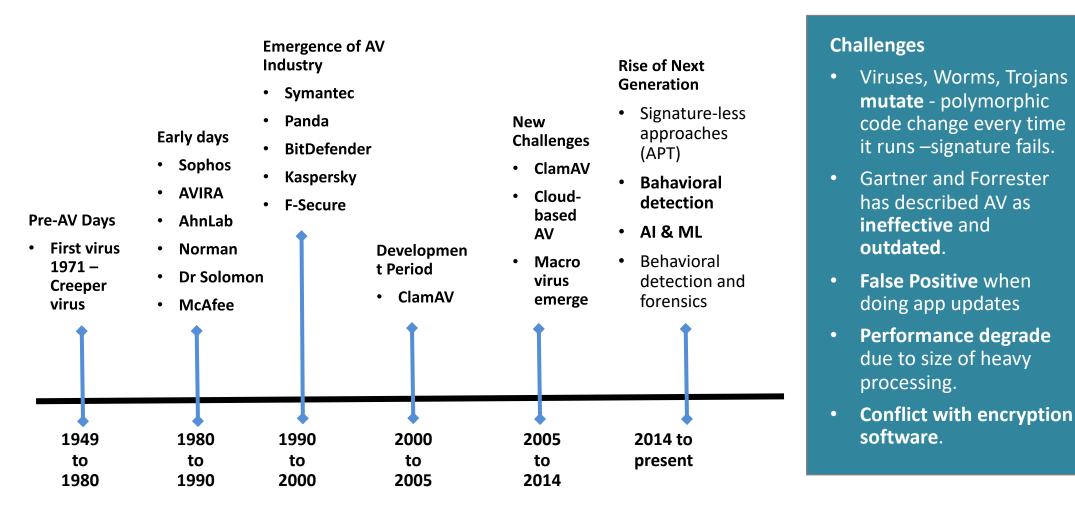
Learning Technology

- Conduct analysis to determine anomaly, based on algorithms such as behavioral, heuristic, Artificial Intelligence, Machine Learning and more
- Example: Anti-spam, ATP, Anti-DDoS

ANTI MALWARE EVOLVED INTO ENDPOINT PROTECTION

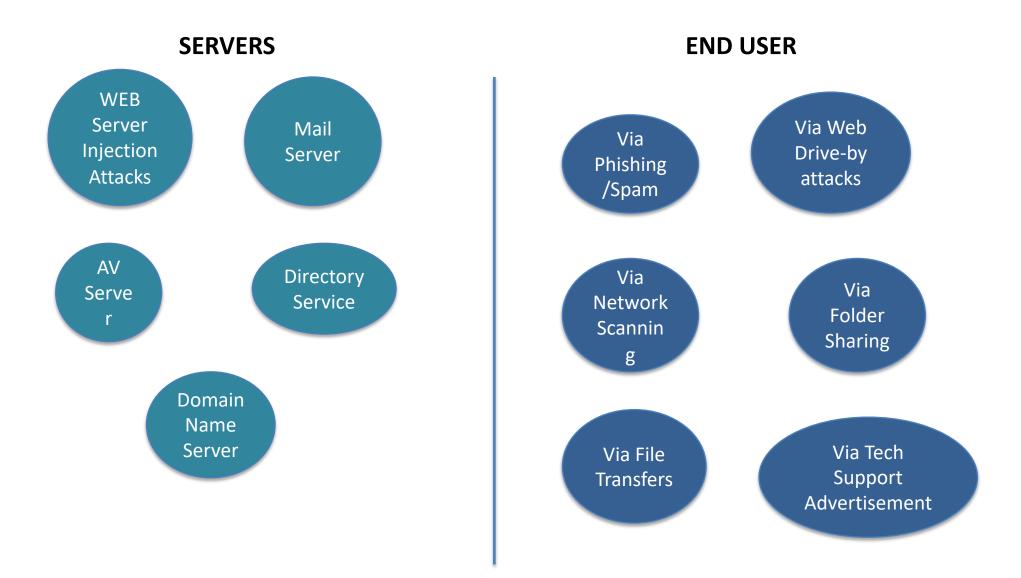
DETECTING THE KNOWN AND UNKNOWN (ZERO-DAY)

The anti malware technology had over decades relied on **signature based detection**. The next generation Endpoint Protection includes **Behavioral Detection**, Artificial Intelligence (AI) and Machine Learning (ML). These require heavy processing. Most desktops in critical sector are running End of Life systems.



ENDPOINT TARGETS

INTERNET FACING SERVERS | END USER COMPUTERS



FIRST TC NEW CALEDONIA

METHODS OF APPLICATION WHITELISTING

- Critical systems require only limited function to conduct daily operations and should operate based on trusted applications.
- Implementing Top 4* security controls at endpoints will mitigate at least 85% of the intrusion techniques. Application whitelisting is one of the Top 4 controls.

Methods used by most application whitelist solution:

- File Hash maintaining hash of the whitelisted files
- **Digital Certificates** trust certain publishers of software. Most software vendors digitally sign their applications. This digital signature can be used by many whitelisting vendors to automatically approve software from a specific vendor into the whitelist.
- **Trusted updaters** e.g. predefined accounts, processes or network locations which are automatically trusted. Automatic trust means that an application can be installed and automatically added to the enterprise whitelist.
- Monitoring mode | Incident Response This provides visibility into the executables which are running on end user systems and can be used to detect, confirm and respond to attacks.

*TOP 4 STRATEGIES TO MITIGATE TARGETED CYBER INTRUSIONS: MANDATORY REQUIREMENT EXPLAINED by Australian Signals Directorate (ASD) assesses that https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

BRINGING IT ALL TOGETHER TOWARDS EFFECTIVE SECURITY CONTROLS AGAINST PAST, CURRENT AND EMERGING THREATS

- Make security controls work together, not against each other.
- Don't just settle Measure effectiveness of Endpoint controls and make improvements.

Thank you