Guest Lecture 5

Speaker: Mel Masterson, AirBnB

This lecture on threat intelligence will be interactive, and each student will have to sign-up for a 3-4 minute assignment. Please pick your assignment from the list.

Assignments

https://cyware.com/news/new-version-of-trickbot-trojan-targets-windows-defender-9a4cc9e4
Thanhthanh
What is Trickbot and what does it do?

- Trickbot is banking Trojan that uses either the Registry settings or the Set-MpPreference Powershell command to set Windows Defender preferences; it has 12 ways of disabling Windows Defender and Microsoft Defender ATP. It performs privilege escalation so that it can get more access to system privileges. Then it loads the “core” component by injecting a DLL, which downloads modules that are designed to steal information from the communication layer, and perform other tasks.

What operating system does it affect?

- It affects the Windows OS.

How can you detect it?

- Most reputable malware-removal software will be able to detect Trickbot and remove the malware.

https://isc.sans.edu/diary/Targeted+Phishing+Attacks+in+the+Financial+Industry%3A+Fire-3+Phishing+Kit/25188
OSCAR
What is the type of attack?

- The type of attack was a phishing attack with the aim to “collect e-mail credentials for business-email-compromise (BEC) attacks.”

Who is being targeted?

- Usually financial companies. In this instance it was a home loans company.

What do the attackers try to get from their victims?

- They attempt to gain access to emails, as well as payment information

What does the attacker do once they have the victims password?

- Either read the victim’s emails, or use it to add a “forward” address.

Is there a way to reduce this type of attack?

- Phishing attacks can be very intricate at times. In this situation the attacker made a mistake, which allowed the analyst to get a hold of the email creating the attack, and the phishing kit used (Fire-3).

https://www.theverge.com/2019/7/31/20748886/capital-one-breach-hack-thompson-security-data
-WENDY
What company was compromised?
What happened?
How did the company discover they had been compromised?
What is the name of the person who was arrested?
Where did they work previously? What was their title?
How many customers were affected?

https://blog.knowbe4.com/iranian-hacker-group-apt34-use-new-tonedeaf-malware-over-linkedin-in-latest-phishing-campaign
SABRINA W.
What type of attack is this? (A linkedIn phishing campaign)
How is the attack executed?
Who is believed to be responsible for this attack technique?
What is APT?
What industries are targeted in this malware campaign?

https://www.alienvault.com/blogs/labs-research/newly-identified-strongpity-operations
Finn
What is the malware campaign known as StrongPity? *Malware used to control compromised computers, hiding in malicious versions of WinBox and WinRAR installers.*
When was it first reported? *October 2016*
Is it still spreading now? How? *It hides in malicious versions of legitimate installers, that work as normal while quietly installing StrongPity.* (Read the section "Technical Details" and tell us about what it does)
How can it be detected? (Alert on the domains it beacons out to or by alerting on the file it drops `wintcsr.exe`)

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
OSCAR
Tell us about the WannaCry malware attack
- The attack was made possible using an exploit named EternalBlue, which was developed by the NSA.

What kind of malware was used? (ransomware)
- The malware used was ransomware crypto worm

What is ransomware?

- A malware that threatens victims with deleting or publishing their data, unless a ransom is paid, usually in bitcoin as it is untraceable.

What operating system was targeted?

- Microsoft Windows operating system

How many computers are believed to have been affected?

- More than 200,000, in over 150 countries

What was the "kill switch" that stopped the spread?

- The kill switch involved registering the domain name found in the malware. This slowed down the spread of the attack, as it only encrypted machines that couldn't connect to that domain.

Who was responsible for publishing the kill switch?

- Marcus Hutchins accidentally discovered it hard coded in the malware

https://www.technadu.com/kpot-stealer-version-2-0-new-features/67140/
https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal

Finn

What is KPOT Stealer? *Malware stealing account information and other sensitive data by intercepting various sources*

What is the attack vector? *An exploit in RTF documents attached to emails* (in other words, how does it reach the victim?) i.e. via email

What vulnerability does it target? *CVE-2017-11882*

What operating system is susceptible? *Windows*

How can you be protected from this? *Don't download things or click links in unsolicited emails*

https://blog.malwarebytes.com/threat-analysis/2019/02/the-advanced-persistent-threat-files-apt1/

What is APT?

APT is an acronym for Advanced Persistent Threat.

Who is APT1?

APT1Different parties have identified APT1 as People's Liberation Army Unit 61398

Where are they from?

They are famous for authoring the hacking tool mimikatz. Can tell us what mimikatz does?

https://community.riskiq.com/

Sign up for a free account on RiskIQ and tell the class what types of things you see.

https://community.riskiq.com/projects/b36fc143-4414-828b-bfe7-2e2fbc7b41b0

Tell us about this threat actor.

Who is APT34?

Where are they based??

Who do they target?

https://en.wikipedia.org/wiki/Indicator_of_compromise
https://digitalguardian.com/blog/what-are-indicators-compromise
SABRINA W.
What is an IOC?
Give us some examples of IOC's
How can you use IOC's to improve detection and response?

https://securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html
-WENDY
What is cyber espionage?
Tell us about #8 (the obama attack)
http://investigations.nb