EE379K Enterprise Network Security Lab 3 Report

Student: Brian Cheung bc32427
Professor: Mohit Tiwari
TA: Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

October 21, 2019

Part 1 - APT Campaign Questions

Exercise Set 1

1. Dwell time is the number of days from when an attacker first compromises the victim to when the attacker is finally detected. The decrease in median dwell time over the past year can be attributed to the improvement of "internal hunting capabilities" and "enhanced network, endpoint and cloud-service provider visibility." [1]

2. Advanced Persistent Threat (APT) groups are "generally focused on espionage activities."

    - APT37 ("Reaper") - Active since 2012, APT37 primarily targets organizations in South Korea, but have recently started targeting Japan, Vietnam, and the Middle East in order to gain intelligence for North Korea's military, political, and economic interests.
    - APT38 - APT38 uses destructive malware to steal hundreds of millions of dollars from financial institutions. This group is linked to North Korean espionage operators.
    - APT39 - APT 39 is an Iranian cyber espionage group primarily targeting the Middle East. It targets the telecommunications sector, travel industry and supporting IT firms, and the high-tech industry in order to monitor and track specific individuals and collect customer data for strategic purposes related to national priorities.
    - APT40 ("Periscope") - APT40 is a Chinese espionage group that targets Southeast Asian countries that are important to China's "Belt and Road Initiative". The group takes large amounts of information from organizations in the engineering, transportation, and defense sectors related to maritime technologies.

3. The known methods of initial compromise for APT37 include phishing operations and strategic web compromise. Specifically, APT37 sent a reunification-themed email that contained a weaponized HWP attachment. This spearphishing attachment is a form of social engineering that relies on the victim to execute the attachment which compromises the victim's system. "Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments." [2] APT37 also used social networking and cloud platforms like Twitter, AOL, and Dropbox to relay commands to compromise

the victim's systems. Analyzing network data for abnormal data flows and unexpected protocol behaviors may be useful in detecting such attacks. [3]

4. A lack of investigation on infected systems may cause the victim to overlook the the possibility of a larger breach. After detection of malware on a system, it is important to understand that the piece of malware may have stemmed from a lateral movement from another system in the environment, and not just a new isolated attack. This understanding would encourage the victim to run a more thorough investigation to detect the breach. A poorly timed remediation may actually hurt the victim even further. If an attacker has had long term access to the victim, the attacker may likely have many different ways to evade eradication methods. As a result of a poorly time remediation, the victim could fail to eradicate the attacker and even complicate the investigation further prolonging the investigation and remediation process. This mistake can be avoided by conducting regular reviews of incident response plans, use cases, and playbooks in addition to properly handling and storing evidence in incident respons plans. Organizations should also develop guidelines and procedures for analyzing threats ion addition to erradication and remediation plans.

Exercise Set 2

5. According to MITRE [3], the Web Service attack is a Command and Control and Defense Evasion tactic. Since this attack often uses common services that the victim is already using and web service providers often us SSL/TSL encryption, attackers can easily hide under the "expected noise" and extra level of protection.

6. Web services commonly used in a Web Service attack: 1

7. Social networking platforms like Twitter, cloud storage services like Dropbox, and Github are often used in a Web Service attack. These services allow attackers to post content embedded with malicious domains or IP addresses that infect victims. A victim may be able to detect the malicious intent through abnormal data flows and suspicious activitywhen accessing content on these services.

Web Service	Examples
Social Networking	10
Cloud Storage	9
Github	7
Google Services	7
Pastebin	5
Blogs	3
Downloader	1

Table 1: Table of web services commonly used in a Web Service attack.

Exercise Set 3

Part 2 - Fuzzing

Part 3 - Exploitation

Conclusion

References

[1] F. Mandiant, "M-Trends 2019 Report," 2019.

[2] MITRE, "Spearphishing Attachment."

[3] MITRE, "Web Service."