EE379K Enterprise Network Security Lab 3 Report

Student: Sean Wang, szw87
Professor: Mohit Tiwari, Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

October 27, 2019

Part 1 - APT Campaign Questions

Exercise Set 1

1-1. Dwell time is defined as the number of days that an attacker is present in a victim network. In other words, the time in days from the first evidence of compromise to detection. In the last year, the median dwell time has decrerased due to the fact that organizations are getting better at finding compromises internally, as well as the fact that clients have generally been improving data visiblity through better tools, resulting in faster responses. Median as a metric for dwell time can be good when a one number summary is needed, but it leaves out lots of information regarding the scale or complexity of the attacks.

1-2. There are four new APT groups: APT37, APT38, APT39, and APT40. The primary mission of APT37, also known as "Reaper," is to covertly gather intelligence to support North Korea's interests in military, politics, and economics, which is hypothesized due to their targeting of South Korean entities. Similarly, APT38, is a financially motivated group targeting financial institutions in support of the North Korean regime. APT39, on the other hand, is an Iranian cyber espionage group that seems to focus on monitoring, tracking, and surveilling specific people, collecting data to use for national priorities or for future campaigns. APT40, also known as "Periscope," is a Chinese cyber espionage group targeting countries important to China's "Belt and

Road Initiative." They typically target sectors pertaining to engineering, transportation, and defense, especially those that overlap with maritime technology.

1-3. APT37's known methods of initial compromise are phishing and strategic web compromise. Phishing is when the attacker attempts to get sensitive information using a diguise of a trustworthy entity. One such example is spear fishing, which occurs through emails or links. Defense against phishing attacks include using an antivirus to quarantine suspicious files or a system to scan incoming email attachments and remove any malicious ones. Additionaly, users can be trained to watch out for social engineering techniques and suspicious emails and links. On the other hand, strategic web compromises are when an attacker gets access into a system due to a user visiting a compromised website with malicious ads or injected code. One way to prevent this is to use network signatures to identify malware traffic. Additionally, proxies can be used to prevent the use of unauthorized external services through an enforced communication policy.

1-4. Lack of investigation is problematic since it leaves out any information regarding the context of the malware and if a more in-depth analysis is needed. An in-depth analysis reveals much more about the system and the environment of the attack. Defenders can follow a more detailed analysis procedure to reveal much more information about attacks, including but not limited to: where it came from, how it attacked, and why it happened. The specific steps should be reviewed often as attack methods aren't stagnant, so defense against and analysis of attacks shouldn't be either. Poorly timed remediation is also problematic since organizations end up acting too fast to eradicate the attack, leaving some backdoors up in haste. As a result, the attack has not been fully eradicated and there is now no visibility of attacker activity either. Defenders can consider what evidence to keep and have more detailed guidelines so that attacker can be fully shut out.

Exercise Set 2

1-5. The linked behavior, web service, is part of the command and control part of the APT lifecycle. This might be hard for defenders to detect since popular websites and social media can provide a lot of cover for the attack, since there is generally a prior connection to those sites before the compromise. In addition to common services providing noise,

web service providers typically use SSL or TLS encryption, which gives these types of attacks another layer of protection.

1-6. The web services used and number of times they are listed are shown below in Table 1.

Web Service	Examples
Social Networks	8
Github	8
Blogs	7
Cloud Storage	7
Google Apps	7
Pastebin	6
Microsoft TechNet	4
RSS feeds	2
Microsoft OneDrive	2
Forums	1

Table 1: Table of web services used and the number of times listed.

1-7. The most prevalent web services are social networks, such as Twitter and AOL. Github is also a very common web service used in these attacks. To detect when these services are being used for malicious purposes, one can look for suspicious activity through packet capture analysis for communications that do not follow expected behavior. If the data is encrypted, then SSL/TLS inspection is also needed. Another method is to look for patterns, such as an uncommonly excessive amount of data flow or monitoring user activity.

Exercise Set 3

1-8.