COMP2216 Principles of Cyber Security 2023/24

Coursework on Cyber-Attack Analysis

Student ID: 33461104.

Task 1 – Kill Chain-based Analysis

Reconnaissance Phase #1

The initial intrusion method remains uncertain; however, the attackers were believed to be scanning the Internet for vulnerable Customer Relationship Management (CRM) systems to infiltrate due to knowledge of an RCE vulnerability. An assumption is that as they scanned for networks with this vulnerability, they came across SecProv's internal network, whereby the CRM system connected their internal network to the Internet, distinct from the one exploited to access the local file-sharing application in GovVault's internal network, installed on machine hosting services.

Weaponisation Phase #1

It is believed that the attackers developed the RCE vulnerability to penetrate the CRM system by crafting arbitrary executable commands towards the targeted machine hosting service. Moreover, they would simultaneously prepare for their Command and Control (C&C) infrastructure to maintain persistence, such as the downloader script, since the initial intrusion was four months to upload the malicious update to SecProv's internal code repository.

Delivery Phase #1

As SecProv provides machine hosting services such as the CRM system over the Internet, the attackers can deliver crafted arbitrary executable commands such as the downloader script via this medium. An assumption is that these commands were delivered via the Internet either through the HTTP/HTTPS protocols using ports 80 for HTTP or port 443 for HTTPS. This is because CRM systems typically involve web-based interfaces accessible using a browser through these protocols. However, due to sensitive data in CRM systems, HTTPS is more likely to be used.

Exploitation Phase #1

The attackers successfully exploited the CRM system using the RCE vulnerability by sending these executable commands, which executed the downloader script. This successful exploitation is suspected to have led to the downloader script on the same machine the forensic team discovered. An assumption is that the crafted commands were sent to the machine and created the downloader script found on the same system.

Installation Phase #1

The downloader script which downloaded the backdoor on the CRM machine is assumed to be installed from these remote executable commands using the RCE vulnerability. Therefore, to gain persistence, the attackers modified the operating system registry keys so that the backdoor remained active in the CRM system whenever the system booted up.

Command and Control Phase #1

The attackers established a communication channel through the backdoor, which was installed using the downloader script for the CRM system. The backdoor would allow them a remote connection to the machine. An assumption is that the attackers would send remote instructions to the CRM system to scan the entire internal network for existing devices vulnerable to further exploitation, and this information would go back to the attackers so they could pivot in SecProv's internal network.

Reconnaissance Phase #2

It is assumed that the attackers scanned SecProv's internal network from the CRM system. By doing this, they identified a developer's device with unusual Remote Desktop Service (RDP) protocol configurations, whereby notifications and logging have been disabled. These configurations are essential for the attackers as they would mitigate their chances of being detected in the network since any notifications of changes or unusual logins would alert the developer, which would cause the attackers to be detected.

Weaponisation Phase #2

The forensic team assumes the attackers breached the developer's workstation via the poorly secured RDP service. The RDP service is a probable cause as there could have been some implementation of a brute-force attack (such as a list of common default credentials) since the workstation credentials were weak and susceptible. It is also probable that they were preparing the C&C infrastructure.

Delivery Phase #2

The exact delivery is not explicitly mentioned. However, the attackers likely used a dictionary attack in SecProv's internal network with common default credentials to deliver the brute-force attack on the RDP service towards the developer's workstation. The brute-force attack likely ran on port 3389, the default RDP port number.

Exploitation Phase #2

The assumed brute force attack exploited the developer's workstation when a password guess was a successful login (via brute force attack using the list of common default credentials), giving access to the developer's machine through the RDP service. The password was weak enough for brute force exploitation.

Installation Phase #2

No other information is available that the attackers tried to gain persistence within the workstation. It may not also be relevant as they gained persistence in the first iteration. However, they may have installed a backdoor and modified the operating system registry keys, so the backdoor ran every time the system restarted, similar to the CRM system. This is because this is how they gained persistence within the CRM system and would consistently deploy similar techniques. It may also be the case that the attackers disabled the notifications and logging themselves as opposed to finding it in that configuration.

Command and Control Phase #2

The attackers established a communication channel on the developer's workstation. It is possible that the attackers established communication through the RDP service using the password they guessed to access the workstation. The attackers could send commands to identify the developer's permissions and access to applications, such as SecProv's internal code repository, to upload the malicious SecMon software update later.

Reconnaissance Phase #3

To infiltrate further, the attackers would have identified or known that the developer's workstation had full access privileges to SecMon's internal code repository. They would have made this discovery by identifying what applications the developer's workstation had access to and relaying that information to the attackers for later use.

Weaponisation Phase #3

The attackers developed a backdoor using the developer's access to SecMon to pivot from SecProv's internal network to GovVault's internal network. This backdoor, later injected into SecProv's internal code repository through a software update, would allow them to prepare for the C&C deployment into the GovVault network.

Delivery Phase #3

The attackers delivered the backdoor by injecting it into SecMon's application using the full access privileges of the developer's workstation. This delivery allowed the attackers to gain a foothold in GovVault's internal network because GovVault installed a software update of SecMon from SecProv containing the attacker's backdoor. This injection was possible because SecMon was a pre-existing application for GovVault before it was infiltrated by the attackers internally in SecProv's network.

Exploitation Phase #3

The backdoor was successfully exploited when GovVault updated their SecMon software and executed the malicious backdoor injection after the update, giving attackers access to

GovVault's internal network through a remote connection. As SecMon is their security monitoring service, other software would typically not detect that the security software had vulnerabilities within itself. This approach would minimise the detection of backdoors unless other intrusion software recognised the malware.

Installation Phase #3

As the backdoor is within the security software that GovVault uses, the attackers gained persistence by having remote access to their network because the pre-existing application was downloaded and executed. An assumption is that the software remains active because the network requires SecMon's security. No other information was available.

Command and Control Phase #3

The attackers established a communication channel to GovVault's internal network through the security application SecMon using their C&C infrastructure. An assumption is that they would send remote instructions to SecMon to scan the new network for devices to pivot further and relay this information back to the attackers so that they can infiltrate further.

Reconnaissance Phase #4

An assumption is that the attackers in GovVault's network scanned the network for further vulnerable devices and found knowledge of an RCE vulnerability in a version of a local file-sharing application. This vulnerability means they found a way to bypass the exemplary security configuration and access control policies in the local file-sharing application.

Weaponisation Phase #4

The attacker's exploit for the vulnerability used specially crafted packets that triggered a buffer overflow condition when processed. The attackers also prepared the C&C infrastructure when this vulnerability became activated later.

Delivery Phase #4

Although not explicitly mentioned, the specially crafted packets are believed to have been delivered to the local file-sharing application through SecMon using remote commands in the GovVault internal network. No other information is available as to which protocols were explicitly used.

Exploitation Phase #4

When the specially crafted packets are delivered and processed to the local file-sharing application, upon processing, a buffer overflow condition triggers, leading to the application's successful exploitation of the RCE vulnerability. This successful exploitation allows attackers to execute arbitrary code with system-level privileges.

Installation Phase #4

An assumption is that the attackers did not gain persistence as no other information was available. It may also not be relevant as they already gained persistence by injecting the backdoor into the SecMon application. Instead, they may have sent arbitrary code commands with system-level privileges and exploited the RCE vulnerability each time a new connection was created from the attackers to the local file-sharing application.

Command and Control Phase #4

An assumption is that the attackers already established a communication channel by injecting a backdoor into the SecMon application in GovVault's internal network. The attackers were likely to send commands remotely, allowing them to view and download any valuable information on the local file-sharing application, such as the top-secret documents they later exposed to the public a few months afterwards.

Actions on Objective Phase #4

The attackers stole unauthorised access to confidential documents by exfiltrating the data from the local file-sharing application to achieve their goals. Although it is not made explicit where the stolen documents went, it's assumed that they went to computers via the Internet that they could access and later share with the public about the recent government misconduct.

Task 2 – Attacker Analysis

Cybercriminal

Motivations

Cybercriminals, which would be perpetrators in this instance, are generally interested in illegal profit. Their typical motivations would not align with the attack's impact of publicly leaking top secret documents because they do not directly achieve any monetary profit from disclosing this information. However, it is possible that they would be cybercriminals if they were paid by someone else to execute this attack, especially if those people who paid the cybercriminals were motivated to publicly disclose the recent government misconduct, such as nation-states or hacktivists, which would be instigators.

Attack Strategy

In terms of attack vectors, some similarities align cybercriminals to this attack. For instance, they injected a backdoor into the SecMon application, a type of malware typical for cybercriminals to deploy. However, it was not explicitly mentioned that any use of social engineering, social media, or botnets was used, which are also commonly used by this type of profile. In contrast, RCE and brute force attack vectors were used instead. Although part of the attack shares techniques with cybercriminals, it needs to be more evident to conclude that cybercriminals were behind the attack due to how sophisticated it was.

Technical Skills

Cybercriminals' technical skill requirements are very abrasive, including money theft, personal document ransom, data breaches, and distributed denial of service (DDoS) attacks. Although a data breach occurred when accessing the local file-sharing application and exfiltrating the top-secret documents, none of the other typical attack strategies aligns with this one. This would mean that although it is possible that it was cybercriminals due to one shared commonality, there needs to be more substantial evidence to conclude it is, especially when the sophistication of this multi-step cyber-attack is beyond the technical skills of cybercriminals.

Nation State

Motivations

Nation States are generally interested in high-quality intelligence, sabotaging activities or critical infrastructures, and subversion, such as a political election. This profile would align if another nation-state instigated the attack on the government agency, as they wanted to encourage conflict within their country and cause sabotage. However, it would not align

with the other interests as no explicit relation exists in this attack. They could either be the instigator or the perpetrator of the attack.

Attack Strategy

The attack vectors are the same as cybercriminals (malware, social engineering, social media, botnets) but more advanced. This would align with this attack as they were persistent by remaining hidden for four months from the initial intrusion to the upload of the malicious update. There is also a malicious nature as they exfiltrated data, but rather than for espionage purposes, it was for widespread chaos. However, advancement is limited, as the exploitation included a known RCE vulnerability rather than zero-day exploits.

Technical Skills

Their typical attacks are more aligned than those of cybercriminals, such as data breaches for top-secret documents and advanced persistent threats (APT). This is because the sophistication of APTs using backdoor injection and the careful strategy of their data breach requires more significant technical skill requirements not seen by cybercriminals or hacktivists. However, it was never explicitly mentioned that any DDoS or Influence Campaigns were used, which misaligns with nation-states.

Hacktivist

Motivations

Hacktivists are generally motivated by political, religious and social ideologies. Their typical motivations are the most aligned compared to cyber criminals or nation-states. This is because their motivations would explain why they want to disclose the recent government misconduct publicly. Having these belief systems has led to these impacts, which happen more closely if the profile of the attacks is that of hacktivists. They could be either a perpetrator (they were involved themselves) or an instigator (they intentionally started it).

Attack Strategy

The attack vectors are the same as cybercriminals but generally less advanced. Given this, the attack vectors of hacktivists would not align with this attack because the backdoor injected into SecMon to infiltrate another network would be considered a sophisticated attack. Additionally, no explicit use of social engineering, social media, or botnets was made, which are attacks typical of hacktivists. However, the injected backdoor is a type of malware, which makes it partially aligned.

Technical Skills

Hacktivists' typical attacks include DDoS, data breaches, and web defacements. Although data breaches have occurred with the local file-sharing application, the other tactics to access top-secret documents do not align with the typical skill requirements of hacktivists, especially if they are less advanced than cyber criminals when this attack is sophisticated in its pivotal and persistent nature.