COMP2216 Principles of Cyber Security 2022/23

Coursework on Cyber-Attack Analysis

Student ID: gdi1u21@soton.ac.uk

Task 1 – Kill Chain-based Analysis

Introduction:

A Kill Chain-based analysis is a framework for describing the evolution of cyberattacks, starting from the initial Reconnaissance phase and ending with data extraction or various objectives. This breakdown of an attack provides a more in-depth analysis of different attacker profiles and potential vulnerabilities which when leveraged, will prevent future attacks.

In the analysis of the first task, there will be presented three iterations, all of which are ordered chronologically corresponding to a cyberattack targeting the internal repository of an organization called ElectroSmart and a government website. The initial iteration contains a social engineering campaign, launched by the adversary with the purpose of stealing the account credentials of a developer, working for the organization. The succeeding, second iteration is primarily determined by the attacker's attempts to penetrate the internal repository of the targeted company and subsequently upload a malicious driver update. The third, final and most crucial iteration involves a Distributed Denial of Service (DDoS) attack on the government website using infected with malware smartphones.
The second task identified three potential cyber actors as the likely perpetrators of the attack: a cybercriminal working for nation-state, a nation-state, and a hacktivist. The cybercriminal may be motivated by financial gain, while the hacktivist may be motivated by raising awareness, promoting a cause, or protesting an alleged injustice. The nation-state may be motivated by political, financial, military gain, espionage, or propaganda goals.
The detailed exploration of every iteration of the attack and the mapping to attack chain stages provides a more in-depth understanding of the procedures and vulnerabilities on the company's security level by following a specific construction.

First iteration: Social Engineering campaign containing phishing email

Reconnaissance Phase

The first iteration of the Reconnaissance phase is retrieved by a social engineering campaign conducted by the adversary, associated with detecting vulnerability inside the internal repository of a smartphone camera producer and intending at hijacking developers' credentials. It is a result of a previous in-depth analysis of the company's modus operandi in gathering information about employees' activities and is deployed by using social engineering techniques for acquiring data – an essential part of launching a successful phishing attack. Overall, this phase demonstrates the commitment of the attacker to identifying vulnerabilities, especially trust and curiosity to gather personally susceptible information.

Weaponization Phase

The initial adversary's action during the Weaponization phase of the first iteration is producing a phishing email together with a fake website, which undoubtedly represents malicious weapons. The attacker doesn't utilise spearfishing within an email for reviewing the work-from-home policy. However, his purpose is to use these weapons to extract personal account details. The development process of malicious software is not explicitly defined but there exist numerous methods for development, such as relying on open-source tools or building them from scratch. After acquiring the victim's personal login information, the attacker needs to carefully consider his succeeding step.

Delivery Phase

The source or equivalently - the adversary, hidden behind a mock email address produces the delivery phase in the first iteration by sending a phishing email to the destination which might be the inbox of the targeted developer. The delivered message avoids using expressions recognized by spam filtering. The purposeful similarity to the authentic organisation's website further prevents possible sceptical assumptions made by the victim.

Exploitation Phase

In the course of the exploitation phase, the adversary successfully takes advantage of social engineering techniques and convinces the victim of the legitimacy of the hyperlink contained in the phishing email. Therefore, the attacker accomplishes extraction of the personal account details of the developer. Such persuasion plays a critical role in the cyber-attack and covers a hazardous action with the potential unmasking of the adversary's motivations and aims.

Installation Phase

After completing the previous stages, during the "Install" phase of the first iteration, an attacker was able to obtain an employee's login information without successfully connecting to ElectroSmart's virtual private network (VPN). The attacker assumed that the employee's credentials would not be changed due to suspicion, potentially allowing him continued access to the network. However, it is not specified if the adversary has not considered such a scenario and somehow implemented prevention of it. Regardless of such further reflection, the attacker establishes persistence, mainly through email's efficient masking.

Command and Control Phase

After the employee enters his credentials as required when proceeding with reviewing the new remote work policy, provides the adversary with the private information by directly sending it to him and supplies him with access to the internal organisation's repository, the single action left for the adversary during the first iteration is establishing communication between him and the company's software so that he can upload a malware inside it. Nevertheless, the Command and Control phase cannot be identified within this iteration since the attacker logs in presenting himself as a developer.

Actions on Objective Phase

The first iteration of the Actions on Objective phase is not present since the adversary is facilitated with access to the internal storage of ElectroSmart's webpage. Furthermore, he is capable of executing further actions which allow him to gather persistence within the network and not get revealed. However, it is a crucial part in terms of proceeding with the following

iteration and successfully executing the attack.

Second iteration: Uploading a malicious driver update

Reconnaissance Phase

Throughout the Reconnaissance phase of the second iteration, the adversary gathers data directly connected with the developers and their ways of accessing the company's software. There aren't any concrete and clear methods specified but potential ones include social engineering attacks, open-source intelligence research or a comprehensive scan of the external-facing organization systems and websites. Moreover, preceding observation and surveillance for determining potential vulnerabilities and possible targets for the attack is highly possible. The adversary's observation of the company's network infrastructure and security protocols could have led to the discovery of susceptible vulnerabilities.

Weaponization Phase

During the Weaponisation phase of the second iteration, the attacker tackles the development of malicious software inside a camera driver update which is responsible for the subsequent communication server established between the adversary and a botnet sending data and is developed for creating records of the virus and occasionally scan for instructions as regards targeting the desired website and setting an ideal timeframe to conduct the attack. The developers of ElectroSmart are potentially using similar coding approaches and manners when building a camera update. There might have been masking which would ensure the validity of the phishing email and the trustworthiness of the victim.

Delivery Phase

In the Delivery phase of the second iteration, the attacker locates and leverages vulnerabilities and successfully inserts malware in the camera driver. Afterwards, he aims to inject the source of communication in this phase, which is the malicious software into the driver code and send the updated version to the company's repository for generating new drivers, which appears to be the destination of the transmission. The concrete modes of communication are not specified but leave the notion of the presence of secure channels, used for data transfers.

Exploitation Phase

In terms of the exploitation phase within the second iteration, the adversary exploits the workflow of the targeted driver update so that he ensures easiness when implementing the malware to the repository together with securing the highest possible standard. Furthermore, such processes contribute towards taking full control when launching the malicious driver update, consequently uploading the update into the internal repository, analyzing the potential distribution over thousands of phones, and resulting in a successful execution of the cyber-attack and delivery of the desired malicious software.

Installation Phase

The Installation phase in the second iteration is initialized by trying to determine a way of spreading the infectious source code used as a replacement to the authentic, importing malicious software inside the camera driver and subsequently pushing the updates into the internal repository. Furthermore, after gaining persistence within these operations, the single action left to be executed is uploading a malware-containing driver version to the internal

repository, triggering the new driver installed on mobile phones which mounts the camera. This sequence of activities grants the attacker with full access to the company's software and ends up the attack successfully.

Command and Control Phase

In the Command and Control phase during the second iteration, the attacker acquires access to the internal repository of ElectroSmart and embeds a malicious driver update for spreading the virus whenever a smartphone installs the update. The adversary also establishes a botnet which uses HTTPS protocols for establishing communication between the installed malware and the smartphones in such a manner that he is capable of stealing personal login information for uploading the malicious driver update in the repository. The succeeding operation is awaiting further instructions regarding which website to attack and the timing of the attack.

Actions on Objective Phase

The actions within the second iteration are determined by the development and deployment of the malware which is spread amongst smartphones through a malicious update of a prominent camera brand called ElectroSmart. The objectives are established in a way that the malware remains hidden but repeatedly interconnects with a remote server and determines a suitable time and place for executing the attack. For successful incorporation of the malware inside the camera driver, the adversary allocates several months of surveilling the target. If the victim perceives the potential impact and possible mitigation, the outcome could have been different.

Third iteration: Executing a DDoS attack on the government website

Reconnaissance Phase

The Reconnaissance phase of the third iteration is determined with close observation of the actions of ElectroSmart's development team while aiming to determine a way of establishing and integrating the malware into the camera driver. Such procedures indicate a collection of perceptions concerning the organization's activities, access control mechanisms and infrastructure, constituting a fundamental part of the Reconnaissance phase. Generally, the phase was extensive but essential for further stages of the attack.

Weaponization Phase

In the Weaponization phase of the third iteration, the adversary penetrates ElectroSmart's internal repository by utilising various tools and techniques such as malware, and social engineering procedures for gathering access to the webpage and delivering the malicious driver update into the repository, where it is intended to be used for generating the new driver. The exact way of acquiring the required tools and cyber is not specified but the complex nature indicates the possession of significant resources and expertise.

Delivery Phase

The third iteration is preserved by the delivery of the DDoS attack within the targeted network of smartphones and implanting them with malware installed in the camera driver of a popular camera, connected to a remote server with HTTPS, recording and inspecting for an appropriate webpage and time to attack. The successful delivery of this attack corresponds to the final import done by the adversary. Henceforth the attacker has no physical actions left and solely waits for the succeeding infiltration of the government webpage.

Exploitation Phase

In conformity with the former analysis in the third iteration of the exploitation phase, the attacker further researches the ideal time, to begin with, the penetration of the webpage. There is also a potential further analysis of the workflow of the smartphones, their processes and ways of accessing and scanning for information concerning vulnerabilities of the website which all result in planning an appropriate timeframe for executing a DDoS attack on the targeted website. The smartphones appear to operate identically to bots in the botnet developed by the adversary and used when performing the attack.

Installation Phase

Succeeding the implementation of the malicious software within the camera driver, in the Installation phase of the third iteration, the malware establishes a connection with a remote server and does regular scans looking for vulnerabilities and timeframes, convenient for performing the attack. Persistence is accomplished as soon as a mobile phone has the new driver update installed, and the malicious software is injected inside it, allowing further exploitation. The malware is designed to be persistent and remain hidden from the user, making it difficult to detect or remove.

Command and Control Phase

In the process of the Command and Control phase in the third iteration, the adversary utilises infected with malware smartphones in order to execute a DDoS attack on a government webpage. Furthermore, he adopts a communication channel over HTTPS protocols through which the infected with malicious software mobile phones are connected to a remote server. The protocol potentially encrypts the traffic in such a way that it prevents detection of the attack, makes any observation or interception challenging and reduces the chances of discovering the adversary.

Actions on Objective Phase

Ultimately, throughout the Actions on Objective phase in the third iteration and succeeding in the acquisition of malfunction of the internal government webpage, the adversary disrupts the national election, causing significant damage to it. There is a possibility of successful execution as a consequence of executing a TCP SYN or DNS amplification attack. However, such assumptions require a legally supporting thesis. The desired aim to leave the website unreachable for several hours is accomplished. Furthermore, by preserving any identity, the adversary keeps anonymity and therefore the attack is not publicly claimed by anyone.

Task 2 – Attacker Analysis

Cyber Actor Profile #1: *Cybercriminal working for Nation state*

Attack Strategy

The attack strategy exhibited in the description of the cyberattack corresponds to the profile of a Cybercriminal which typically employs DDoS attacks and utilises various techniques including social engineering and malware distribution. Such attack requires both technical and social skills, as well as vast intelligence to carry it out. The adversary's use of infected smartphones and integration of malware is evidence of a meticulous and well-organised crime. The overall sophistication of the attack implies a skilled and knowledgeable attacker seeking out a profit, possibly acquired by ransom, data theft and others. Motives match typical motives of cybercriminals working for nation state.

Motivations

The objectives of this attack are consistent with typical motives of Cybercriminals working for nation state, including sabotaging, causing disturbance, and resulting in frustration close to an important national election. The DDoS attack is carried out in a well-organised and coordinated manner, suggesting the potential involvement of Nation state. Moreover, such processes require time and funds, inaccessible for an ordinary cyber attacker. Therefore, it is likely that the adversary is hired and supported from nation state which want to sabotage the opposition, cause disruption, and possibly win the elections.

Cyber Actor Profile #2: *Hacktivist*

Attack Strategy

The description of the cyber attacker's profile as a Hacktivist is a plausible scenario considering the involvement in politically or socially oriented hacking procedures and the desire of disrupting the already established workflow of the organization by seeking attention. The various attack vectors allow gathering data and access to the targeted victim based on multiple evidence sources and executed using attack and deception techniques. The purpose of tackling the website's software is to reveal some of the vulnerabilities concerning the security practices of the organization. Nevertheless, the complexity and sophistication of the attack indicate the experience and level of technical skills used.

Motivations

The motivation for this attack is consistent with hacktivist threat scenarios where an adversary's final objective is spreading awareness of a present problem, promoting a particular cause or protesting against perceived injustice. The usual methods utilized by hacktivists are non-violent – publishing or stealing confidential data and damaging targeted web pages. However, the hacktivist's proficiency varies on skill level as they can be anything between novices and experienced developers who can achieve their goals without sufficient funds or criminal objectives Nevertheless, they do not aim directly at illegal actions or sabotage but promoting own ideological or ethical agendas instead.

Cyber Actor Profile #3: *Nation State*

Attack Strategy

The chosen Nation State as a cyber actor is consistent with the attack's description due to the complexity and sophistication, which requires significant resources and time to execute. Targeting a government website prior to a national election indicates potential political motivation. The attack includes several months of reconnaissance and surveillance of the targeted company, suggesting a significant level of technical expertise and knowledge concerning the company's internal processes. Furthermore, by utilizing social engineering techniques, the adversary demonstrates a profound knowledge of human behaviour and psychology. Furthermore, such factors are in alignment with characteristics, typically associated with a nation-state actor.

Motivations

A nation-state is a sophisticated adversary that can use various cyberattack techniques for achieving strategic objectives such as political, financial, or military gains, espionage or propaganda. The adversary targets a government website prior to a national election with the purpose of disrupting crucial operations, requiring substantial technical and social skills. The attacker demonstrates proficiency inherent in a nation-state cyber actor who has access to advanced resources and capabilities. The ultimate goal can be manipulating elections, gathering intelligence, or causing chaos and mistrust within the population, all of which are considered processes, common for nation-state actors.

Conclusion:

To summarise, this cyber attack is a pure example of a challenging, time-consuming, well-planned and established, followed promptly step-by-step attempt, which leads to the desired outcome of rendering a government website unavailable for several hours. The adversary-either a Cybercriminal, Hacktivist or Nation state dedicates a substantial amount of finance and time which results in infiltrating the internal repository of a prominent camera brand called ElectroSmart and importing malware in a widely used driver update, later downloaded from thousands of smartphones. The succeeding DDoS attack leaves the government website unreachable for several hours and therefore provokes anger and uproar among citizens close to an important national election.

Furthermore, the attack underlines the poor security practices and protection of the software supply chain. The victim, who is one of ElectroSmart's developers, is blackmailed since he is not aware of security best practices.

Future prevention of similar attacks requires a comprehensive approach, mainly concerning the security practices of organisations and the regular monitoring of networks for suspicious activities. Moreover, policymakers can improve government regulations for better prevention of exploitable vulnerabilities.

Ultimately, the impact on citizens and the wider community can be a financial loss, mistrust in government services or emotional burden and one mitigation of such impacts is investing in possible measures.