COMP2216 Principles of Cyber Security 2022/23

Coursework on Cyber-Attack Analysis

Student ID: gdi1u21@soton.ac.uk

# Task 1 – Kill Chain-based Analysis

Based on the information provided, it is not explicitly clear which phase(s) belong to the first iteration and which belong to the second. However, assuming the first iteration includes the attack on the government website and the subsequent investigation, it is likely that the Delivery phase in this iteration refers to the delivery of the DDoS attack to the government website.

Overall, the weaponization phases of this attack involved the development of sophisticated malware and social engineering techniques to spread the malware and gain access to the internal repository and employees' personal login credentials. The attack demonstrates the need for organizations to prioritize cybersecurity measures and educate their employees about the risks of social engineering attacks.

The Actions on Objective (AOO) phase is the stage where the attacker takes action to achieve their goals. In this case, the attacker's objective was to render a government website unavailable through a DDoS attack. The AOO phase involved several steps, which are as follows:

## Reconnaissance Phase

[*What information did the attacker require to gather? How? Max 100 words*]

Following the attack description, the first iteration of the Reconnaissance phase is retrieved by the social engineering campaign conducted by the adversary and intending at hijacking developers’ credentials. It is a result of the previous in-depth analysis of company’s internal processes gathering information about employees’ activities and deploying 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 into manipulating vulnerabilities, especially trust and curiosity with the purpose of gaining personal susceptible information.

## Reconnaissance Phase

[*What information did the attacker require to gather? How? Max 100 words*]

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. However, 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.

## Reconnaissance Phase

[*What information did the attacker require to gather? How? Max 100 words*]

The Reconnaissance phase of the third iteration is determined while closely observing the actions of ElectroSmart’s development team, for which the adversary dedicates several months while aiming to determine a way of establishment and integration of 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

[*What cyber weapons or tools were required? How did the attacker obtain them? Max 100 words*]

The initial action of the attacker is allocating several months for closely observing the ElectroSmart’s developers’ actions with the purpose of determining potential exposures and a way for embedding the malicious software inside the camera driver update. It is developed so that one may communicate with a remote server using HTTPS 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.

## Weaponization Phase

[*What cyber weapons or tools were required? How did the attacker obtain them? Max 100 words*]

During the Weaponisation phase of the second iteration, the adversary penetrates ElectroSmart’s internal repository by utilising various tools and techniques such as malware, social engineering procedures for gathering access to the webpage, and delivers 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 not specified but the complex nature indicates the possession of significant resources and expertise.

## Weaponization Phase

[*What cyber weapons or tools were required? How did the attacker obtain them? Max 100 words*]

In the third iteration, the adversary produces a phishing email together with a fake website, which undoubtedly represents malicious weapons. The attacker’s purpose is to use these weapons to extract personal account details. The development process of the malicious software is not explicitly defined but there exist numerous methods for developing them, such as relying on open-source tools or building them from scratch. After acquiring the victim’s personal login information, the attacker has access to the organisation’s software and network.

## Delivery Phase

[*How did the attacker deliver the cyber weapon(s) to the intended target? What were the source and destination of the communication? What communication means were used? Max 100 words*]

The first iteration is preserved by the delivery of the DDoS attack and establishment of a communication supplier such as a botnet consisting of a network of smartphones implanted with malware installed on the camera driver, connected to a remote server with HTTPS, recording and inspecting for an appropriate webpage and time to attack. By establishing such communication, the adversary succeeds in infiltrating the network and overwhelming it with new requests, resulting in disruption of the normal internet traffic and workflow of the government webpage.

## Delivery Phase

[*How did the attacker deliver the cyber weapon(s) to the intended target? What were the source and destination of the communication? What communication means were used? Max 100 words*]

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 malicious software into the driver code and send the updated version to a company’s repository for generating new drivers. The adversary succeeds in infiltrating and overwhelming the network with new requests, resulting in the disruption of normal traffic and workflow of the government webpage. The means of communication are secure, yet not clearly defined.

## Delivery Phase

[*How did the attacker deliver the cyber weapon(s) to the intended target? What were the source and destination of the communication? What communication means were used? Max 100 words*]

The source or equivalently - the adversary, produces the delivery phase in the third iteration by sending a phishing email to the targeted developer – the destination. The delivered message includes a hyperlink to a fake website and requires the victim to express an opinion and review the recently adopted remote work policy. The purposeful similarity to the authentic organisation’s website tricks the employee to enter his personal account details.

## Exploitation Phase

[*How were cyber weapons activated or used? Max 100 words*]

In terms of the exploitation phase within the first iteration, the adversary dedicates several months to close observation of the developer’s actions so that the familiarity with the target and therefore the easiness when implementing the malicious driver update to the repository is on the highest possible standard. The succeeding extraction of credentials by utilizing social engineering methods, contributes towards taking full control when launching the malicious driver update and consequently uploading the update into the internal repository. All these actions result in the successful execution of the cyber-attack and delivery of the desired malicious software.   
  
The process allows the distributor to install the malicious driver update into users’ mobile phones in a way, equivalent to an ordinary update installation process, which exploits the developers’ full reliability on the company’s software and the legitimacy of the upgrade procedure. By taking advantage of this reliance, the adversary successfully executes an attack and delivers a malicious cyber weapon.

## Exploitation Phase

[*How were cyber weapons activated or used? Max 100 words*]

In conformity with the former analysis in the second iteration of the exploitation phase, the attacker successfully launches and executes the embedded malicious driver update into the internal repository aiming to infect as many mobile phones as possible with the malware. These devices repeatedly scanned for information concerning vulnerabilities of the website and therefore plan an appropriate timeframe in which to execute the DDoS attack which leaves the webpage unavailable for several hours. The smartphones appear to operate identically to bots in the botnet developed by the adversary and used when performing the attack.

## Exploitation Phase

[*How were cyber weapons activated or used? Max 100 words*]

In the course of the exploitation phase, part of the third iteration, the adversary successfully takes advantage of techniques used in similar social engineering attacks and convinces the victim of the legitimacy of the hyperlink contained in the phishing email. Therefore, the attacker extracts the personal account details of the developer, which allows him to access the internal software repository of ElectroSmart’s website. By utilising the information, extracted within the first iteration and located in the reserved area, the attacker is capable of completing the cyber-attack fully, leaving the website unavailable for several hours.

## Installation Phase

[*How did the attacker gain persistence inside the target? Max 100 words*]

The Installation phase in the first iteration is initialized by allocating several months during which the adversary observes developers’ actions and tries to determine a way of developing and importing malicious software inside the camera driver and subsequently push 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 company’s software and ends up the attack successfully.

## Installation Phase

[*How did the attacker gain persistence inside the target? Max 100 words*]

Succeeding the implementation of the malicious software within the camera driver, in the Installation phase of the second iteration, the malware establishes 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, 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.

## Installation Phase

[*How did the attacker gain persistence inside the target? Max 100 words*]  
During the Installation phase of the third iteration, the adversary sends a hijacking email with a hyper link to one of the ElectroSmart’s developers, which requests him to review the recently adopted remote work policy. This link navigates the employee to a fake website, which cannot be differentiated from the authentic one and asks for his personal credentials. After providing the attacker with them, he supplys him with access to the internal software repository of ElectroSmart’s webpage and the Virtual Private Network (VPN), used by organisation’s employees when they work remotely. The persistence is mainly established through email’s efficient masking.

## Command and Control Phase

[*What communication channel did the attacker use to control the cyber weapons installed inside the target or to get access to the target? How was the connection established? Max 100 words*]

In the process of the Command and Control phase in the first iteration, the adversary utilizes 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.

## Command and Control Phase

[*What communication channel did the attacker use to control the cyber weapons installed inside the target or to get access to the target? How was the connection established? Max 100 words*]

In 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. Adversary also uses HTTPS protocols for establishing communication between the installed malware and the injected smartphones in such a manner that he is capable of stealing personal login information for uploading the malicious driver update in repository. The adversary might have political motives since the attack is not publicly stated and is performed near an important national election resulting in turmoil and anger among people.

## Command and Control Phase

[*What communication channel did the attacker use to control the cyber weapons installed inside the target or to get access to the target? How was the connection established? Max 100 words*]

Throughout Command and Control phase of the third iteration, the adversary launches a social engineering attack to steal personal login information of an ElectroSmart’s developer. The initial step is sending a phishing email with a link, navigating to a fake website in the same manner as authentic one. After the employee enters his credentials as required when proceeding with reviewing the new remote work policy, the private information is directly sent to the attacker who uploads a malware inside company’s internal repository. The attack proceeds successfully and the malware is installed on smartphones which mount the camera sold by ElectroSmart.

## Actions on Objective Phase

[*What did the attackers do to achieve their goals? Max 100 words*]

The initial procedure of the Actions on Objective phase within the first iteration is the development and deployment of the malware which is spread amongst smartphones through a malicious update of a prominent camera brand called ElectroSmart. The malicious software is established in a way that it remains hidden but repeatedly interconnects with a remote server and determines a suitable time and place for executing the attack. In order to work out a procedure which will result in a successful incorporation of the malware inside the camera driver, the adversary allocates several months of surveilling the target.

## Actions on Objective Phase

[*What did the attackers do to achieve their goals? Max 100 words*]

The succeeding step of the Actions on Objective phase is the obtainment of access to the internal ElectroSmart’s storage by utilizing social engineering procedure to hijack the data of an employee with access to the internal storage who receives a phishing email navigating to a fraudulent website, looking in exactly same way as the original company webpage. The fake website expects the developer to preview the recently adopted remote work style by firstly providing his personal account details, which afterwards are stolen in order to enter the policy page and provide the adversary with access to the inner repository.

## Actions on Objective Phase

[*What did the attackers do to achieve their goals? Max 100 words*]

Ultimately, throughout the Actions on Objective phase in the second iteration and succeeding the acquisition of access to the internal software repository, the adversary injects the malicious software inside the camera driver update source code. This results in spreading the malware on every phone which installs the update of the sold by ElectroSmart camera. Furthermore, by launching the DDoS attack, the infected smartphones distribute the malware to the government website and leave it unreachable for several hours. By preserving any identity, the adversary keeps anonymity and therefore the attack is not publicly claimed by anyone.

# Task 2 – Attacker Analysis

[*Up to 3 cyber actor profiles (or combinations of cyber actor profiles)*]

**Cyber Actor Profile #1:** *Cybercriminal*

## Attack Strategy

*(Discuss why the chosen profile is compatible with this attack by focusing on the attack vectors and techniques used, the level of sophistication of the attack and the level of technical/social skills required.*)

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. This attack demonstrates high level of sophistication, requiring both technical and social skills, as well as vast intelligence to carry it out. 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 for profit. The motives match the typical motives of cybercriminal – financial gain or personal enrichment.

## Motivations

*(Discuss why the objective of this attack fits the usual motivations of the selected profile.)*

The objectives of this attack are consistent with typical motives of Cybercriminals, including financial profit and individual aggrandizement. Cyber criminals often possess advanced software development skills and engage in crimes for personal gain. The DDoS attack is carried out in a well- organised and coordinated manner, suggesting potential involvement of an organized criminal group. However, security of critical infrastructure is often compromised by prioritising financial considerations, such as cost- effectiveness and functionality, over security measures. Therefore, it is likely that the adversary is motivated by the financial gain, derived from disrupting the government website during an important national election.

**Cyber Actor Profile #2:** *Hacktivist*

Attack Strategy

*(Discuss why the chosen profile is compatible with this attack by focusing on the attack vectors and techniques used, the level of sophistication of the attack and the level of technical/social skills required.*)  
The description of the cyber attacker’s profile as an Hacktivist is a plausible scenario considering the involvement in politically or socially oriented hacking procedures and 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 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

*(Discuss why the objective of this attack fits the usual motivations of the selected profile.)*

*The motivation for this attack is consistent with a hacktivist threat scenario 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 hacktivist are non-violent – publishing or stealing confidential data and damaging targeted webpages. 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

*(Discuss why the chosen profile is compatible with this attack by focusing on the attack vectors and techniques used, the level of sophistication of the attack and the level of technical/social skills required.*)

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 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 behavior and psychology. Furthermore, such factors are in alignment with characteristics, typically associated with a nation state actor.

Motivations

*(Discuss why the objective of this attack fits the usual motivations of the selected profile.)*

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 a 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 as processes, common for nation-state actors.