TX Assessment Report

Information: Security & Society
INF10101
Coursework 2

Matric Number: 40136554

Date: 02/04/2017
Word count: 1990

Contents

1 List of Figures

2 Introduction

DeKamp Ltd is a company that provides serviced offices to small businesses in Edinburgh. The software is provided by TX, which has been selected as a solution provider by DeKamp. However, DeKamp has doubts about the company and have requested an appraisal of TX to determine the security of TX systems.

This report is drafted by an unbiased third-party and the goal is to analyse the threats that TX may be subjected to by hackers with malicious intent.

Many organisations contain sensitive information that hackers may find very valuable, whether they be competitors, those looking to disrupt the organisation or unsophisticated hackers looking for a challenge or amusement.

This report will assess TX's vulnerabilities and risks, as well as identifying the most significant threat to the organisation. The report will then break down the threat into its attack model, and how to address the attack (i.e. the defence model).

3 Threat Modelling, Vulnerability Assessment and Risk Management

A Vulnerability Assessment and a Risk Management is required before creating an attack or defence model is carried out. There is a relationship between threat modelling, vulnerability assessment and risk management that must be kept in mind upon launching an attack.

3.1 Threat Modelling

Threat modelling describes the architecture of a threat that an attacker may use to attack a system. It looks at what an attacker may hope to gain from an attack, and how they may plan their exploit, as well as their capabilities and intent.

There are several modelling methodologies that can be used to assist in threat modelling, such as Microsoft's STRIDE.

Spoofing Identify –	Hiding a user's identity
Tampering with Data –	Illegal modification of data
Repudiation –	Denial or rejection of an immoral action
Information Disclosure -	Disclosing information to an unauthorised party
Denial of Service -	Denying service to valid users
Elevation of Privilege -	Gain authorised access.

Figure 1. Microsoft's STRIDE System.(Microsoft, 2005)

Vulnerability takes place by analysing the system and its components to assess the severity and opportunity of the system's faults.
Risk Management is the process of assessing the risk of launching an attack on an organisation.

4 Modelling an Attack

4.1 Choice of Scenario

One of the most significant threats to TX is Infrastructure Advanced Persistent Threat (APT). Infrastructure APT is a continuous and targeted attack that primarily targets organisations such as TX. (Musa, 2014)

Most attacks aim for vulnerable targets and target victims indiscriminately, and may be willing to give up if they encounter too much resistance. However, APT attacks are different. They are not only well-resourced, capable and sophisticated, they are also persistent against their chosen targets. (Ltd, 2011)

Infrastructure APT is often performed by a criminal syndicate targeting a specific organisation, often for financial gain, disrupt a competitor or access user's personal data. (Dell, 2014) The emphasis on Infrastructure APT is that attacks are prolonged and persistent – the attacks often take a long time, as the attackers carefully research and make careful moves.

The Cuckoo's Egg (Stoll, 1989) is a non-fiction novel written by Clifford Stoll. It details a first-hand account of the hunt for a computer hacker who broke into a computer at the Lawrence Berkeley National Laboratory, CA. The hacker, Markus Hess, had been selling stolen information from the library to the Soviet KGB. Hess uses Infrastructure APT over a long period of time to gain access to the libraries resources. This is the earliest example of an APT attack.

4.2 Attack Model

When attempting to counter an Infrastructure APT attack, it is very beneficial to take a “Know Thine Enemy” approach. That is to say - the more one knows about the attacker’s motives, plans and attack patterns - the better equipped they are to defend their system. (Moran & Haq, 2013)

4.2.1 Threat Actors

The actors of the threat are almost always external. It is not uncommon for the actor to be a competitor who are aiming to cripple the organisation. They often spend a large amount of time planning their attack, and thoroughly research the company and its infrastructure, looking for vulnerabilities.

There are some examples of TX staff members having access to information that may be worrying to have in the wrong hands. For example, managers have access to resource reports that can contain sensitive information. Administrators also have access to a lot of sensitive information that could be very valuable to a competitor.

APT targets are almost always very serious. Those who partake in APT attacks are often very sophisticated, persistent and capable. They are often part of a criminal syndicate, with large-scale goals of financial gain or information access.

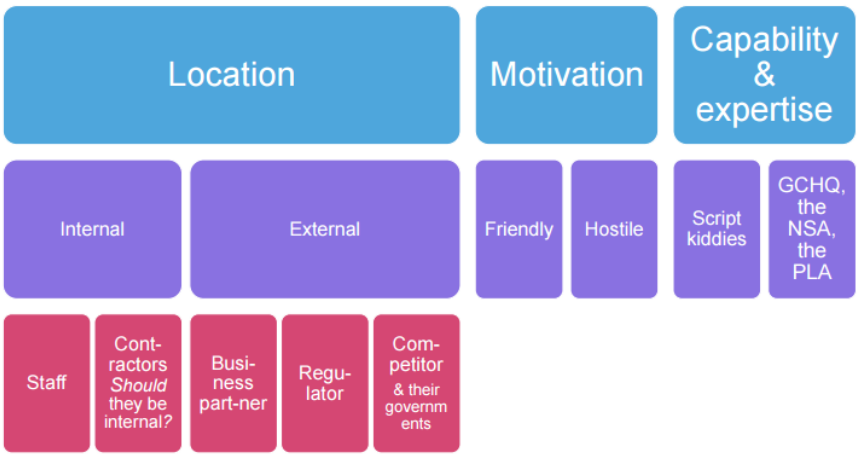

Figure 2. Threat Actors

4.2.2 Attack Model

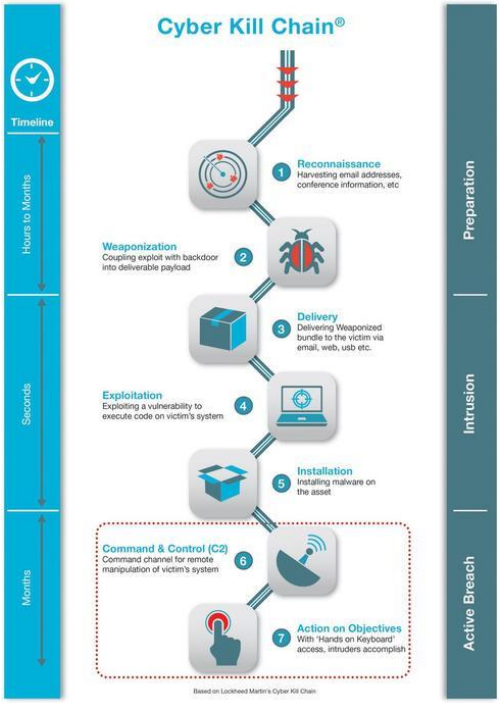

Figure 3. The Kill Chain (Engel, 2014)

4.2.2.1 Reconnaissance

Reconnaissance is the first stage of an Infrastructure APT attack. The objective is to gather as much information as possible on the company, this can be done through e-mail harvesting, reviewing the organisation's web and media presence or looking at their job postings. (Pernet, 2014)

Through this information, a malicious hacker could gain a very valuable insight into the organisation's security. Has the company been involved in a data leak or exploit? Are they in need of security experts? Is the organisation associated with any software partners? How many employees does the organisation have? (Pernet, 2014) This information can be gathered through research of a company without even breaking the law, and a lot of it could prove very valuable to a hacker.

In the case of TX and DeKamp, it is not particularly difficult to discover that DeKamp is using TX as a service provider, this relationship is one example of where hackers can gain valuable information.

Information gained through the reconnaissance stage is refined and the APT team can review the vulnerabilities of the organisation more clearly. The APT team may choose to fully commit to the organisation at this stage if they have not already.

4.2.2.2 Weaponisation

Upon reaching a satisfactory level of information, the attackers may start building their exploit against their chosen target. This exploit is crafted with the target in mind, and aims to attack the target at its most vulnerable points. (Meyers, 2013)

Note that the target does not receive anything at this point of the attack.

TX may be particularly susceptible to a data breach. A lot of data is available to employees that include things like call records, traffic and subscribers. Therefore, it is feasible that a competitor may aim to gain access to this information, with the intent of distributing it to their own organisation or to the public in order to cripple the organisation and its reputation.

4.2.2.3 Delivery

The Delivery stage is where the hackers attempt to transfer the malware to the victim. They will use information gathered in the research stage to plan out the most efficient method of getting the malware into the victim's system.

The payload is often transmitted using e-mail, websites or through USB sticks. (Meyers, 2013)

For example, the APT team may have learned that employees at TX have a tendency to open and run software from unfamiliar e-mails, or employees may insert a USB stick that they found into their PC that can be ran automatically. Other techniques may also be used, such as Spear Phishing, social engineering or water-holing to accomplish the transmission of the payload. (Engel, 2014)

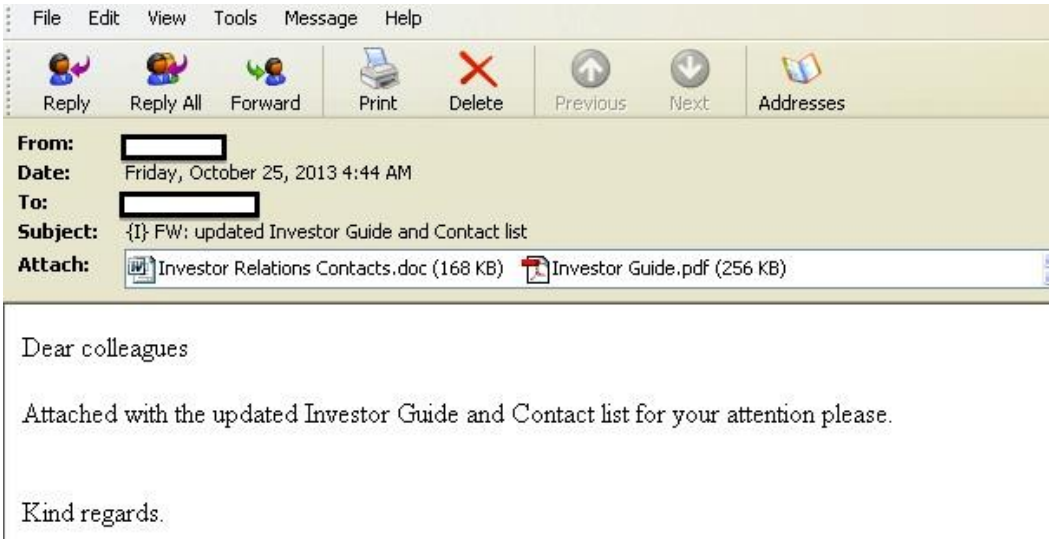

Figure 4. Example of spear phishing.

4.2.2.4 Exploitation

The exploitation stage is where the malware is triggered. The hackers may make use of a zero-day, which means that they exploit a vulnerability that the organisation is not aware of. The results of a zero-day attack can be devastating, as the victim has no time to implement a fix or even mitigate the attack before it happens. (What is a Zero-Day Vulnerability?, n.d.)

Once the malware has been executed, it can then begin to install itself onto the system and begin to wreak havoc.

4.2.2.5 Installation

Upon execution, the malware often aims to create an access point such as a backdoor that allows the hackers to gain access to the system, even if the exploit is patched. (Engel, 2014)

The objective of the installation stage is to create an access point, and exploit the vulnerability to make it as difficult for the organisation to retaliate or even know about the infection.

4.2.2.6 Command-and-Control

The attackers creates a channel that allows them to remotely access the victim's system, and enables them to accomplish the tasks that they set out to accomplish. (Engel, 2014)

The attackers may use several tools such as shells or information collectors through this channels that allows them to sift through information and interact with compromised resources. (Dell, 2014)

4.2.2.7 Actions on Objectives

At this stage, the attackers have accomplished their goal of gaining access to the system, and their goal is to now act on the objectives that they initially set out on. (Engel, 2014) For example, if the goal was to find subscriber information on TX. They may use a tool set up in the command-and-control stage to transfer this information to the attacker on a regular basis. (Dell, 2014)

The time of the stage is indefinite, and the hackers will stay on this stage until they are satisfied with the information they have received, or until they are caught.

It should be noted that the "kill-chain" is not necessarily a linear process. The attackers may use alternative methods if they deem it necessary or more effective. Attackers will take the path of least of resistance to ensure that they have the highest success rate as possible. (Dell, 2014)

4.3 Defence Model

Defence can often be treated with a "Protect, Detect, Remediate" Model (Zsscaler, 2014)

Protect

In the early stages of an attack, the best defence is being prepared for a possible attack. An organisation should be aware of the types of attack strategies such as Infrastructure APT or Denial of Service attacks. The organisation should also be careful upon what they release to the public as part of their web or media presence – they should be informational but not exploitable.

TX, or any organisation, should employ white-hat or ethical hackers to evaluate the security of their system. These types of hackers are moral, and only break into systems that they have permission to, they can then find vulnerabilities inside of the system. Rather than exploiting these vulnerabilities,

an ethical hacker can report the faults and work on resolving them (or passing the information to the relevant body).

Organisations should ensure that their employees follow safe procedures when dealing with outside information, such as websites or e-mails. They should be instructed not to download or install unfamiliar files from dubious sources. They should also not plug in USB sticks that they may have found or been given by an unknown person, as the USB could contain malware that has intentionally been given or left to an employee. (Vaas, 2016)

Technicians should have a thorough knowledge of their system, and where vulnerabilities are likely to occur, and being careful of any unfamiliar connections or data transfers.

Detect

In the event of a successful attack, it can be very difficult to close down the breach and prevent the hackers from accessing information. The first step should be to know that there has been an attack – many attacks are stealthy, and often steal information without the organisation even knowing that their data has been breached.

Remediate

Upon discovering an APT attack, alerting and remediating of any damage caused should be top priority, especially considering the seriousness of an APT attack. Preventing loss of any future information should also be addressed. Infected sections should be contained, quarantined and remediated.

5 Discussion and Conclusion

Advanced Persistent Threats (APTs) are one of the most difficult-to-defend attacks. The attackers are very rarely unsophisticated or attacking for amusement or a personal challenge. Rather, the attackers are competent (Advanced), relentless (Persistent) and dangerous (Threat). They are unlikely to back down easily and are amongst the most dangerous hackers.

Attackers often have very powerful tools at their disposal, such as intelligence-gathering, message-intercepting and computer intrusion. They also are far more experienced in hiding their tracks than less advanced attackers, and can therefore be very difficult to pin down.

Attackers also aim to have long-term access to the target and steal information over the course of several months or even years. These attackers specifically target certain organisations, rather than being opportunistic and hoping for vulnerable targets.

The combination of the sophistication and persistence of APT hackers is very threatening to an organisation, and they present one of the stealthiest, most dangerous and imposing threats that an organisation can face.

6 References

Dell. (2014). *Anatomy of an Advanced Persistent Attack (APT).* Retrieved from Secure Works: https://www.secureworks.com/resources/sb-advanced-threat-protection

Engel, G. (2014, November 18th). *Deconstructing The Cyber Kill Chain*. Retrieved from Dark Reading: http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

Ltd, C. F. (2011, June). *Advanced Persistent Threats: A Decade in Review.* Retrieved from Commandfive: http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

Meyers, L. (2013, October 4th). *The practicality of the Cyber Kill Chain approach to security*. Retrieved from CSO online: http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

Moran, N., & Haq, T. (2013, October 31st). *Know Your Enemy: Tracking A Rapidly Evolving APT Actor*. Retrieved from Fire Eye: https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

Musa, S. (2014, March). *Advanced Persistent Threat - APT.* Retrieved from academia: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

Pernet, C. (2014, May 23rd). *APT Kill chain - Part 3: Reconnaissance*. Retrieved from Airbus: http://blog.airbuscybersecurity.com/post/2014/05/APT-Kill-chain-Part-3-%3A-Reconnaissance

Stoll, C. (1989). *The Cuckoo's Egg.* Doubleday.

What is a Zero-Day Vulnerability? (n.d.). Retrieved from PC Tools: http://www.pctools.com/security-news/zero-day-vulnerability/