CHAPTER 7

Adversary Infrastructure

We previously identified the nature of the threat; however, many organizations will need a deeper understanding of the resources the threat will employ to compromise them. Depending on the threat, they may use their own resources, or they could bring in an entire criminal ecosystem. This ecosystem is available on demand and can provide a criminal, who has minimal technical expertise, with world-class talent.

For this chapter, we specifically use the term adversary. The reason is that threats can be malignant or malicious threats and an adversary is specifically a malicious threat with the intent of Computer Network Attack (CNA) or Computer Network Exploitation (CNE). To exercise proaction, you need to fully understand what resources are available to target you by a given threat. Again, some threats rely solely on their own skills and tools. However, the more capable threats make use of a criminal ecosystem that makes them significantly more potent than they would otherwise be, creating significantly more risk to your organization.

Although it is impossible to list every threat, this chapter identifies the computer criminal ecosystem. This ecosystem allows individuals to specialize in a specific criminal function.

In many ways, the person who will actually target you can be considered a general contractor. When you renovate a house, a general contractor will run the project. The contractor will bring in plumbers, electricians, roofers, etc.; will buy the carpets, kitchen fixtures, etc.; and will do the work, but will rely on suppliers and specialized laborers to complete the projects.

Consider the threat who actually commits the crime to be the general contractor for the crime. The remainder of this chapter discusses the resources available to the threat to commit the crime.

Advanced Persistent Security. http://dx.doi.org/10.1016/B978-0-12-809316-0.00007-5

HIGHLY SOPHISTICATED ADVERSARY INFRASTRUCTURE

When you consider the types of adversaries that you face, the most potent are nation-states, organized crime gangs, drug cartels, and potentially some of the more sophisticated computer crime gangs. These organizations have a great deal of money, have a large number of people, and can create their own exploitation infrastructure. They do not have to rely on anonymous resources from the dark web, but have created their own highly refined exploitation ecosystem. These entities are who you would consider an advanced persistent threat (APT).

This does not mean that they will rely solely on their own ecosystem. As previously described, Russia apparently enlisted Russian computer criminals to launch a distributed denial of service (DDOS) attack against Georgian assets to coincide with the Russian invasion of Georgia. China sometimes enlists, or at least encourages, independent Chinese hackers to cause general damage to another nation. An example of this occurred when the United States accidentally bombed the Chinese embassy in Serbia in 1999 and the Chinese patriots tried hacking random US-related systems.

It is also important to note that the level of sophistication of an adversary is not necessarily determined by the sophistication of the individual attacks used, but by the methodologies, effectiveness, and efficiency of the overall operations. APTs might begin an attack with an extremely simple exploit. However, once they are in, they proceed methodically, covertly, efficiently, and effectively.

This section identifies the infrastructure that these entities create and foster. It provides for highly effective attacks that are also very efficient. These organizations typically attempt to keep their CNE and preparation of the battlefield as surreptitious as possible. They also plan to make their CNA as devastating as possible. This infrastructure allows for hacking at will.

Research and Development

The more a threat understands technology, the more effective it will be at CNA and CNE. Highly sophisticated threats will maintain their own research and development (R&D) efforts to actively study technologies and find vulnerabilities in them. Once the vulnerabilities are discovered, they will develop attack tools to automate the exploitation of the vulnerabilities.

By constantly examining technologies, they systematize computer hacking. When new technologies begin to be used, or even when they are in development, researchers will begin to study the technologies to find vulnerabilities. Some nation-states might even attempt to embed vulnerabilities into products. Such was the case with Juniper Networks, as reported in December 2015 that

a malicious party found a way to embed a malicious code in the software baseline. The US government banned the sale of Huawei products to its customers, as it was believed the Chinese government had backdoors installed in the products. Products from Checkpoint, an Israeli company, were also banned for sale to the US government customers, as Checkpoint would not allow a review of its software.

In the first case of its kind, it was documented that a Swiss cryptographic company, Crypto AG, provided the National Security Agency (NSA) with a backdoor in its products for more than three decades. The previously mentioned Equation Group reportedly intercepted products shipped to certain customers and embedded backdoors into the equipment's firmware. The Snowden leaks indicated that NSA was able to infiltrate email systems throughout the world. All these cases are just what has been discovered and publicized. It is highly likely that there are many more compromises of commercial products that have not been discovered and/or disclosed.

Although these are operational espionage efforts, the extent of these compromises indicated that there were tremendous R&D efforts in place. One of the documents that Snowden leaked was essentially a catalog of attack tools created by the NSA Tailored Access Operations (TAO) office and available to the intelligence community. The tools allowed for the interception of cell phone calls and automated computer hacking, among other tools that automated or initiated attacks. The R&D is conducted by on-staff security researchers, who are extremely skilled and well-resourced. The TAO is essentially NSA's team of security researchers. Other US intelligence agencies, as well as multiple organizations in most nation-states, and all other APTs maintain their own teams of security researchers.

APTs will also make use of the resources available to less skilled and resourced hackers. They will monitor the dark web, hacker forums, etc. for any information that may help with their attacks. Although random hackers may not have as much resources available to them, given their sheer numbers, it is likely that they will find new zero-day attacks. They might already have information that the APT is interested in collecting. Also as mentioned, APT actors might make use of random hackers and the general hacking infrastructure to obfuscate their own actions.

Collection Management

Collection management is a formal process and a key function in all major CNE and potentially CNA efforts. Collection management is the tasking and coordination of intelligence efforts. The collection management team receives requirements from some authority. The assumption is that the authority has some strategic goal that has been passed on to them.

If we are talking about the US intelligence efforts, the director of National Intelligence sets the collection tasking requirements. These requirements do not necessarily say, "Hack this country," but they are to the effect, we need to know information on a specific subject. These requirements are then delegated to the intelligence agencies that are most likely to be able to satisfy the need for the information. Assuming it involves some level of hacking, it is passed to the collection management team that then initiates the process. You can assume that the previous description of the tasking process applies to all APTs.

Once the collection manager has the requirements, he/she passes the targeting information to the breach team. The breach team establishes a foothold on the system and ideally hacks enough systems within the targeted organization to provide a firm foundation for collection efforts. It has to pass on the information to the collection team and/or back to the collection manager.

The collection manager then ensures that the collection team is aware of the collection requirements. The collection team then gets whatever data it can and passes it back to the collection manager. The collection manager then has to evaluate whether the requirements have been satisfied. Ideally the collection manager also determines if there has been any information discovered that was not expected, but valuable. If so, the collection manager passes that information back to the tasking elements, along with the information requested.

The collection management team will then be informed as to whether or not the requirements were actually satisfied.

Breach Team

An APT breach team will have a wide variety of hacking skills. Its job is to infiltrate the targeted organization to establish a foothold in the target and ideally create an infrastructure inside the target that allows for easy movement on the part of the collection team. It will likely have specialists for different technologies and can call on the specialists required to compromise the target.

The breach team will either have its own security researchers available or have ready access to its organization's security research group. This allows the breach team to rapidly exploit a target, and if they run into a problem or a new technology, it facilitates rapidly overcoming the issue.

When the breach team learns that there is a requirement, it will perform research and reconnaissance on the targeted organization. It will determine the technologies in place and the potential points of entry. This reconnaissance also includes reconnaissance of employees and others with access to the targeted organization. It will perform LinkedIn searches, among other searches, to determine who might be the most fruitful to spear phishing attacks. Once it identifies a person or other entry point, it will research the best way to target them.

The reconnaissance can be incredibly thorough and extensive. In the widely reported breach of the RSA Security company, in which the Chinese attackers infiltrated RSA Security to steal the source codes to their SecurID security product, the attackers identified people who worked in the human resources department and sent them a spear phishing email that appeared to come from Beyond.com, a company that deals with recruiting new employees. The attackers attached a spreadsheet that supposedly contained potential recruits, but actually contained a flash file that contained a zero-day vulnerability. When a single user clicked on the file, it gave the attackers the ability to install a backdoor program that they then used to compromise the rest of the network.

In other cases, the Chinese hackers targeted US defense contractors. They assumed that the contractors would be interested in the agenda for an upcoming conference specific to people in the defense industry. The message appeared to contain the updated agenda for the conference. The attachment was a PDF file containing a zero-day attack for PDF readers.

Clearly the breach team has to have a thorough understanding of the target's language, culture, and business environment. Although the quality of attacks varies, APTs typically have extensive resources ensuring the success of spear phishing messages, and are able to rapidly exploit the technologies.

After establishing a foothold inside the target organization, they will identify other systems that can be used to stage attacks by the collection team. This may involve dozens of other systems. They need to identify the protections in place and how to bypass them, as well as to perform a general mapping of the target's network. All the information is compiled and provided to the collection team.

It is also possible that the breach team will set up a network for long-term compromise. In this case, the breach team will install malware throughout the target network. The malware will establish a large distributed system that constantly detects if there are any modifications to the network. The breach team will also install malware on critical servers, such as email servers, and personal computers of key executives, so that it can constantly monitor the data and services on those systems.

Collection Team

The collection team will receive the requirements from the collection management team, as well as the information regarding the preparation of the target from the breach team. Although it might not need as much hacking knowledge as the breach team, it does need to understand the technologies in place, so that it can navigate the network quickly. It also needs to understand the languages in use.

The collection team will scour the network for the required information. It might have a broad collection requirement, which means that it should collect as much information as possible. To support its efforts, it will use a variety of search programs, scripts that allow for mass downloads of information, and tools that provide data transfer channels, among a variety of other utilities. When it finds information of potential interest, it will typically send the data to an exfiltration server. An exfiltration server is one of the compromised servers that is compromised for the specific intent of the temporary storage of data. The breach team will likely create a hidden directory on the intended exfiltration servers, which allows the collection team to capture as much information as possible without sending out constant streams of data, which could be more easily detected. Instead, the exfiltration servers will store the collected data until a point in time when data transfer is less likely to be detected, and it will be transmitted via a covert channel. A covert channel is a nontraditional communications path. For example, it is typical to send data via ftp or other file transfer and command protocols, but they are visible. If you have the appropriate skills or tools, you can modify other Internet protocols, such as the Domain Name System (DNS), to transmit data or commands. You can make a data file look like a video file and transfer sensitive data out in a way that appears to be otherwise insignificant.

As required, the collection team may attempt to clean up all signs of the breach after the collection has been completed. In many cases, the collected data might be rendered worthless if the compromise is detected. For example, if the United States learns of a secret communications mechanism between Chinese warships, and the Chinese learn about it, the Chinese may stop using that communications channel, preventing the United States from exploiting those communications in the future.

DEEP/DARK WEB

The deep web and dark web are the subjects of a great deal of mystery. They are constantly mentioned in news stories, movies, and TV crime series. *CSI: Cyber* and other hyped-up TV shows love to mention the deep and dark webs as immediately explaining how there is a criminal underbelly of the Internet that cannot be tracked. The reality is obviously less sensational.

Although there is no universal definition for the deep and dark webs, we will use the generally accepted definitions. The deep web is that portion of the Internet that is not searchable through the traditional search engines. There is typically no nefarious intent for the lack of searchability. Some content cannot be indexed by Google, Yahoo, Bing, or other search engines. For example, some websites require people to pay for content. Some Web pages are dynamic and might generate content from databases that are searched before the criteria for

the search is provided. Some sites intend that they will be accessible through The Onion Router (Tor), which is discussed later, and some content may be intended to be hidden and be part of the dark web.

In case of adversaries that you will likely deal with, you need to understand that if you have information or services that are essentially on the deep web, whether you knew it or not, an adversary might target data that you believed was confidential. Many content companies lose their competitive edge if their information is compromised. An example of this is porn sites. Although the typical sites are part of the deep web, some less scrupulous site owners have attempted to pay hackers to steal information off the site. Piracy in the industry is a significant problem. Clearly there are other industries that have similar issues.

We want to be very clear that there are pornographic sites with illegal content, such as sites that contain child pornography. These sites would traditionally be in the dark web.

The dark web is that portion of the web that is intended to be anonymous. There are some legal uses for the dark web. Initially, the US intelligence agencies intended to create the dark web to facilitate covert communications, as well as to provide forums for dissidents in totalitarian regimes. Some groups also prefer to communicate anonymously. Some people want to offer services that are legal, but otherwise maintain their anonymity.

The dark web requires that people use specific software to access systems or communicate with each other. If the system wants to support anonymous web access, using the Tor browser might suffice. However, if there is a desire to exchange files or have personal exchanges, a person would need to use specific software.

The dark web can be considered an anonymous Internet with friend-to-friend communications functionality. It allows for private communications between parties known to each other, which is why the Islamic State of Iraq and Syria (ISIS) uses the dark net to communicate with potential recruits.

The dark web also facilitates online markets that are generally used by criminals. Silk Road is a notorious case of an online market for selling illegal drugs. As discussed later, there are markets for leasing botnets, fencing stolen credit card numbers, buying weapons, hiring criminals to perform illegal acts, laundering money, etc.

As previously mentioned, ISIS members use the dark web to communicate with each other and with potential recruits. They provide information to facilitate communications, coordinate potential terrorist attacks, and distribute training materials to launch cyberattacks.

Although law enforcement and intelligence agencies have had some success in infiltrating the dark net, criminals still consider the dark web a reasonably secure mechanism to support their actions.

What is important for a security professional to consider is that the dark web provides resources for people targeting your organization. These resources might be information and software to make their attacks more sophisticated, allowing a person with little technological know-how to launch attacks with much more skill. Malicious parties may also hire attackers to attack you on their behalf, or fence stolen information or other goods through the dark web. The dark web itself is not inherently dangerous to a potential victim, but the resources and capabilities that it provides a would-be adversary with are what that makes it dangerous to the victim.

TOR

Tor is both a software and a network that helps maintain anonymity on the Internet. The average user will interact with Tor through a Tor web browser. The web browser encrypts traffic that you send. It also connects to the Tor network, which randomizes how the web browser connects to the destination. Servers associated with the Tor network facilitate an anonymous connection between the sender and the recipient. The browser will connect to one server and that server transfers the connection to another server. There will be multiple server connections, with none of the intermediate servers knowing the sender and intended recipient.

Tor is a basic tool of Internet anonymity. It is not perfect, but it is reasonably effective for the intended purpose. The average user can use it to browse the traditional World Wide Web. Tor, or similar browsers, is required to use the dark web.

BITCOIN

Bitcoin is a digital asset and a payment system that is used as a form of Internet currency. It allows for anonymous payment from one person to another and is therefore a preferred payment method for criminal actions on the Internet. It is, however, important to note that many traditional businesses are beginning to accept bitcoins.

Bitcoins are unregulated and the value of a bitcoin can fluctuate significantly. However, the anonymity of the transaction makes it a preferred tool for criminal endeavors, especially by Internet-based criminals.

A stereotypic example of bitcoin usage is the use of paying ransoms to unlock ransomware, as will be discussed later. Criminals exchange bitcoins with each

other as payments for services, information, extortion, or any other monetary use. If you want to know how to make your own transactions using bitcoins, the reader is referred to the Internet. For the purpose of this book, it is sufficient to understand that bitcoins have tangible value and are widely used throughout the adversary infrastructure.

BOTNETS

Botnets are essentially a set of Internet-based computers under a common controller. Although the term can include legitimate networks of computers, the overwhelming use of the term is for computers that have been hacked and under the control of criminal hackers.

The hacker can then use these computers to send out spams or launch DDOS attacks, where the bots of the botnet are commanded to direct large volumes of communication requests to a targeted system. The hacker may also use these bots for data collection, as they can install spyware on the computer to monitor keystrokes, to constantly collect data, to use the system to monitor its network, or as a launch point for other attacks, including the collection of other bots.

Botnets are typically formed through a variety of illicit means. A bot herder may have systems randomly scanning the Internet for systems with unpatched vulnerabilities that allow for remote hacking. If a vulnerable system is found, it is hacked and the botnet software installed. Phishing messages can also lure naive users into downloading malicious software that adds the system to a botnet.

Legitimate websites can be hacked, and visitors to such websites might unknowingly download the malicious software as well. This is a type of "watering hole" attack. In one case, a website operator was contacted by a criminal and offered a commission for every instance of botnet software installed on a computer, after visiting the site. The criminal did not blatantly state that the software installed was illicit, but luckily the website owner was smart enough to realize the real intent and informed the appropriate authorities. In some cases, hackers might set up fake websites just to attract visitors to be duped into downloading the malicious software.

In another demonstration of the criminal infrastructure, a bot herder will pay commission for bots herded into their botnet. This incentivizes random hackers to hack systems throughout the Internet to install the botnet software and claim their commission.

Given the pervasiveness of botnets, it can be expected that almost all companies, universities, and other organizations will have some of their systems herded into a botnet. If an organization does not monitor its systems and networks properly, it could be an unknowing complicit in attacking other organizations.

There are reportedly botnets with more than 1,000,000 bots. Although some bot herders might use the bots for their own malicious purposes, such as the North Korean and Iranian intelligence services, many bot herders will lease their botnet through the dark web. Criminals can lease botnets by the thousands for a fee. Criminals do not have to create their own botnet, as they can lease as much botnets as they need. Botnets are extremely versatile and can be used for a variety of illicit purposes.

RANSOMWARE

Ransomware is a growing form of computer crime that is hitting all types of organizations, including law enforcement. Ransomware is malicious software that once loaded on a victim system encrypts the hard drive and issues a warning that unless a ransom is paid within 24—48 hours, all the data will become unrecoverable. The software then tells the victim to typically send between $250 and $1,000 to the criminal within the allotted period, usually via bitcoin. When the ransom is paid, the criminal will send the victim an alphanumeric sequence to unlock the malware.

The victims typically infect themselves by clicking on a phishing message or downloading the ransomware from an infected or malicious website. The relatively short period allowed to pay the ransom is to discourage the victims from finding alternative methods of decrypting the system. Many victims find that they need more time to figure out how to use bitcoin. In some cases, victims have negotiated with the criminals for lower fees.

Ransomware programs are occasionally hacked by legitimate security experts, and people make a master code to decrypt the systems available, but more frequently, it is impossible to find a solution without paying the ransom. In October 2015, an FBI agent actually stated that victims should just pay the ransom by default, if their systems were locked by ransomware. In April 2015, it was reported that many police departments were forced to pay ransom to computer criminals.

Generally, the criminals do not specifically target a victim. They send out random phishing messages and infect as many sites on the Internet as possible. It is also possible that they pay a commission to any hacker who spreads their software. Ransomware is a growing problem as people tend to leave their systems insecure and behave insecurely on the Internet. As long as people allow untrusted software to be installed on their system and do not maintain a proper antimalware software, ransomware will continue to be a problem.

SECURITY RESEARCHERS

We have discussed security researchers in Chapter 5, but we want to specify that there are security researchers who are also part of the adversary/criminal infrastructure. These people will find zero-day exploits and sell them on the dark web. They might also perform criminal consulting on an as-needed basis.

As previously defined in the discussion of APTs, it is possible that APTs may hire some freelance security researchers on a project-by-project basis. This serves to hide their activities and reserves their exploits for critical occasions.

The exploits created by the security researchers would have different values depending on the technologies being exploited. Clearly there is the potential to make a great deal of money. For the purpose of this book, it is just important to note that this level of skill is available to anyone with enough money to buy it.

LEASED OR PURCHASED MALWARE

Zero-day exploits are an example of malware, but there are more examples of attack programs that criminals can purchase to better automate their attacks. The website, TheRealDeal, claims to specialize in the brokering of zero-day exploits in the dark web. Again, criminals do not have to be computer geniuses to execute complex attacks. They can purchase or lease software tools that automate the most complicated attacks possible.

BROKERAGE OR ESCROW OF DATA

Once criminals commit a data theft, they need to be able to profit from it. This requires fencing whatever was stolen. For example, when Target was hacked in 2012, the perpetrator needed a way to profit from the theft. He/she had to fence the credit card numbers. The credit card numbers were apparently distributed via a variety of carder sites that allowed people to specify the criteria for card numbers available for purchase. Criminals were then able to search for the cards that were locally sourced, so that they were less likely to be flagged for fraudulent use.

For example, a criminal in the Chicago region could purchase credit cards that were issued to victims in the Chicago region. This way it was less likely to be considered fraudulent than perhaps a card issued to someone in Arizona being used in Chicago.

Many of these sites claim to provide excellent customer service and guarantees. For example, if you purchase credit cards from some sites, they will substitute any credit cards that are not valid. They even rate the sellers of stolen data. Some

of the more notable criminal marketplaces include ShadowCrew, Russian Business Network (RBN), Carders Market, and Silk Road.

There is a very robust marketplace to fence virtual goods. Although credit cards are clearly a major focus of online distribution, there are other sorts of information that can be of value; for example, bank account information can be useful, personally identifiable information (PII) can be sold for identity theft purposes, and corporate information can be sold to competitors. Healthcare information contains the same information as traditional financial information, but also facilitates medical insurance fraud. Accordingly, attacks against healthcare organization are on the rise.

Some people may ask why would criminals not exploit the stolen information themselves. The answer is twofold. First, a successful crime, such as the Target credit card theft, results in more data stolen than a single criminal can exploit. It is to the criminal's advantage to sell most of the cards, as he/she would never get to take advantage of all the cards. More importantly, it is not the criminal's specialty. The criminal infrastructure allowed the Target hackers to make sufficient money from the criminal aspects that they specialize in.

HACKERS FOR HIRE

Criminals without sufficient technical skill to accomplish their intended acts can hire the talent they need on the dark web. There are many online forums that allow people to scout for the required talent. Clearly it is difficult to ensure that you are dealing with a truly talented individual, as many hackers exaggerate their skills and accomplishments. There is also the risk that some people soliciting hackers may actually be undercover law enforcement agents.

Regarding the potential skill level of would-be hires, some hackers have a reputation. Some sites have a rating system. It is also common for criminal enterprises who recruit hackers to test their skills. If they can pass the tests, they will make formal offers.

Again, this is another example of criminals being able to make use of world-class talent without having the skills organically.

ENCRYPTED APPS

In the November 2015 Paris attacks by ISIS, a great deal of reporting was devoted to the terrorists' use of mobile apps, such as Telegram, to help plan the attacks. Telegram and WhatsApp, among other communications apps, offer encryption and other capabilities to allow for sharing of data that cannot be easily compromised by law enforcement.

Although ISIS is one concern, the reality is that your employees, both good and bad, are going to use mobile apps to your detriment. Adversaries will be able to coordinate their activities against you through easily available applications.

Although our goal is not to make you think that all technologies are against you, it is important to understand that there are some technologies that are apt to be used by your adversaries. You have to understand what they are, so that you can design your security programs most effectively.

SUMMARY

Although this chapter can make adversaries appear to have unlimited resources, and can make you think that all technologies will be used against you, the goal is to help you optimize your risk. You can only do so when you understand the true nature of the resources that may be put against you.

The reality for most readers is that you will only face a small portion of the resources identified here. When you understand the threats you are most likely to face, you can determine which resources your adversary is most likely to use against you. Then you can figure out what countermeasures are most appropriate to implement given your risk.