**Cybersecurity Threat Landscape (Part II - Report Analysis)**

Answer the below questions using the reports provided. You may have to do some independent scouring to find the answers to each question.

**Group Member Names:**

Source: *Symantec Internet Security Threat Report (Volume 23)*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 1 | This report highlights five key themes in 2017. Describe each of them. | There was a sharp rise in coin-mining attacks in which cyber criminals use coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency.  There was a spike in software supply chain attacks, where attackers inject malware implants into the supply chain to infiltrate unsuspecting organizations, with a 200 percent increase in these attacks in 2017.  Ransomware profitability in 2016 led to a crowded market with overpriced ransom demands. In 2017, the ransomware “market” made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity.  Overall targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering. However, the use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past.  Threats in the mobile space continue to grow year- over-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016. And last year, there were an average of 24,000 malicious mobile applications blocked each day. |
| 2 | What exactly is the Eternalblue exploit? Why was it so significant in 2017? | It was significant because the exploit was included in a number of big attacks in 2017, most notably the WannaCry and Petya/NotPetya attacks. |
| 3 | WannaCry and Petya/NotPetya: What are they? What is their significance? How did they spread? What were their implications? | Both of these were ransomware cyber attacks that used the EternalBlue exploit to spread quickly in a short amount of time.  Within hours of its release, WannaCry had infected hundreds of thousands of computers worldwide. While WannaCry caught the world’s attention and caused a significant amount of disruption, from a financial perspective it was a flop, both because the attackers botched the implementation of the payment system and because of a killswitch in the malware that was quickly identified by a security researcher.   Petya/NotPetya also used the EternalBlue exploit to spread itself, but also incorporated other Server Message Block (SMB) network spreading techniques, which meant it could spread across organizations to computers that had been patched against EternalBlue. The attack was designed to mainly affect organizations in Ukraine. The initial infections were spread through a Trojanized version of M.E.doc, a tax and accounting software package that is widely used in Ukraine. The attackers managed to compromise the M.E.doc website and upload a Trojanized version of a software update. Once installed on one computer within an organization, Petya/ NotPetya would begin attempting to spread itself to other computers on the network, building a list of IP addresses and using EternalBlue and other SMB spreading techniques to infect them. It did spread to external IP addresses, but only those that were in some way connected to the infected orga- nization.  The net effect was that Petya/NotPetya was highly targeted against Ukraine and deeply disruptive, because it wiped all infected computers. The timing of the attack also appeared designed to cause maximum disruption, coming on June 27, the day before Ukraine’s Constitution Day, a national holiday. |
| 4 | On average, how much is the average ransom amount requested in a Ransomware attack? | The average value of a ransomware demand fell to $522 in 2017, following a peak of $1,071 in 2016. |
| 6 | When it comes to targeted attacks, what is the number one infection vector? What is the number two infection vector? How do each of these work? | Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of groups. Spear phishing relies on duping the recipient into opening an attachment or following a malicious link and its popularity illustrates how often the person sitting behind a computer can be the weakest link in an organization’s security.  The next most popular infection vector is watering holes, websites which have been compromised by the attacker, usually without the knowledge of the website’s owner. Attackers will often compromise a website that is likely to be visited by intended targets. For example, if their target is in the aviation sector, they may compromise an aviation forum. |
| 7 | According to the report, Zero Day reports continue to fall out of favor. Why is this the case and what are the security implications? | By using Living off the Land tactics, attackers use whatever tools are on hand, such as legitimate networking administration software and OS features.  This allows attacks to fly under the radar making them more appealing to attackers because it becomes harder to attribute attacks to them. |
| 8 | What percentage of Android users are on the newest major version? What percentage of iOS devices are on the newest major version? Why is there a discrepancy? What are the security implications of this? | Only 20 percent of Android devices are running the newest major version and only 2.3 percent are on the latest minor release.  For iOS,  approximately 77.3 percent of iOS devices using the latest version, and 26.5 percent using the latest minor version. iOS updates are rolled out much more quickly as they are not dependent on a carrier making the updates available for their devices on their network.  This can make Android devices more vulnerable to attack. |
| 9 | In the underground economy, how much might it cost you to have someone conduct a DDoS attack for 1 hour? How much would it cost to have someone “repair” your credit score? How much would it cost to generate a fake ID? How much would it cost to mess up a person’s online presence? How much would it cost to hack a Gmail account? What are the security implications? | DDoS Attack for an hour- $5-20  “Repair” credit score- $50  Fake id- $10-600  Mess up a person’s online presence- $500  Hack a gmail account- $.1-5  The implications are that because these costs are relatively cheap, there is a higher likelihood of them occurring |
| 10 | What is the difference between a vulnerability and an attack? Provide an example of each mentioned in this report. | A vulnerability is a flaw or weakness in a system or computer that can make it open to an attack.  An attack then is a security threat that involves an attempt to remove, destroy, or change information without permission or access. Petya/NotPetya is an example of an attack  In a direct compromise scenario, the attacker switches the update package with a modified malicious version. The simplest way to achieve this is by compromising the web server where the update packages are hosted—for example, through a vulnerability in the content management tool. |
| 11 | What exactly was the CCleaner Incident? What was the significance? How many people were affected? How did it occur? | In August 2017, a popular system clean-up tool called CCleaner was targeted by supply chain attackers. An unknown group of attackers gained access to the company’s development environment, which allowed them to create and distribute a malicious version of the tool through the update process.  The success of the campaign was aided by the fact that the attackers were able to sign the Trojanized update with the manufacturer’s official digital signature. Between August 15 and September 12, the compromised version, CCleaner v5.33.6162, and the cloud version were distributed to customers. According to figures from Avast, the modified version was downloaded 2.27 million times |
| 12 | What does the report mean when it says: “Attackers typically use software update supply chain attacks to infiltrate well-protected organizations?” Provide an example. | Hijacking software updates is a popular alternative as it gets harder to find exploitable zero-day vulnerabilities and other traditional infection vectors. Supply chain attacks usually involve hijacking software updates with the attacker replacing a legitimate software update with a malicious version in order to distribute it quickly and surreptitiously to intended targets. Any user applying the software update will automatically have their computer infected and will give the attacker a foothold on their network.  The CCleaner incident was an example of this. |
| 13 | How are DDoS attacks used in conjunction with Ransomware? | DDoS attacks can knock an organization offline and systems admins will be busy trying to step this attack and get the organization back online. This means that they will be too distracted and busy to notice other suspicious activity that could indicate that a targeted attack is on its way. Similarly, hackers can use ransomware attacks as a decoy for more targeted attacks that are also on their way. |
| 14 | Talk about Butterfly, Dragonfly, and Turla from the Analyst stories. What made these groups interesting to the analysts? | Butterfly is a targeted attack group that doesn’t appear to be affiliated to any country and were instead involved in corporate espionage, presumably for financial gain. Over the course of a few years, they compromised a range of major corporations, such as Twitter™, Facebook™, Apple®, and Microsoft®. But they’ve disappeared completely for now, but they had some of the best operational security.  Dragonfly is an attack group that has  been targeting critical infrastructure and has been compromising energy companies since at least 2011. As time goes on, they’ve begun to use more off-the-shelf tools and Living off the Land tactics, meaning it’s become harder to attribute attacks to them. They’re focused on getting and maintaining access to energy networks and gathering information on how they operate. We know they have the ability to cause serious disruption to energy networks, but so far they’ve never opted to go that far. The danger is that they could, at a time of their choosing. Of all the groups we’ve looked at, they’re probably the ones that have come closest to crossing the line between intelligence gathering and something more hostile, like sabotage.  Turla was an attack group that used a lot of sophisticated tools and tricks; tracing the development of their tool kit indicated this was a large, well organized group that had money to back their operations. There was obviously a lot of skilled work involved by different people to develop each component. |
| 15 | Describe each of the three most common techniques used in lateral movement. | Stolen credentials were the most commonly seen lateral movement technique employed. Attackers often use hacking software tools to obtain credentials from a compromised computer and then use them to attempt to log into other computers on the network.  “Pass the hash” is where where attackers steal and reuse the underlying hashed version of a password. Then without cracking it, they can use it to authentic themselves on other computers or servers.  Exploiting open network shares is another technique. |
| 16 | What was the most common username and password attempted by hackers trying to penetrate IoT devices? | The most common username in 2017 was “root”  The most common password in 2017 was “password” |
| 17 | At one point in the report, the authors are quoted as saying: “No need to compromise the software vendor if you own the software.” What is meant by this message? Describe the specific case referenced in this passage. | Instead of having to compromise the software vendor, the attacker can just buy the rights to the software package and through that send a malicious update to the existing user base.  This is a lot easier than attacking the software vendor. |
| 18 | Describe how coiminer attacks typically work. What is the difference between file-based coin mining and browser-based coin mining. What are the security implications for each? | Files and scripts are run on a person’s computer to carry out coin mining. The problem is when people aren’t aware that their computers are being used to mine cryptocurrency.  File-based coin mining involves downloading and running an executable file on your computer. Browser-based coin mining, which saw the biggest jump in prevalence in 2017, takes place inside a web browser and is implemented using scripting languages. |
| 19 | How much of an increase was there in IoT attacks between 2016 and 2017? | There was a 600 percent increase in overall IoT attacks in 2017 |
| 20 | According to researchers, what are the three motivations for using ransomware? Describe each of them and an example named ransomware that utilized each. | By far the most prevalent motive is intelligence gathering, with 90 percent of groups being wholly or partly involved in it. Intelligence gathering can include information stealing, spying, and surveillance.   * Dragonfly engages in attacks for intelligence gathering   Disruption is still a distant second to intelligence gathering. By their very nature, they draw a lot of attention. The exposure makes it more difficult for groups to carry out further attacks, since their tools and techniques will have been thoroughly investigated and as a result organizations are likely to bolster their defenses. Disruptive attacks are also regarded as being far more hostile and aggressive than intelligence gathering and anyone mounting them will risk reprisals. In most cases, particularly when sabotage is involved, they are used sparingly and usually appear calibrated to send a message to the intended target.   * The Lazarus group has done a number of very public disruptive attacks; e.g. the 2014 Sony Pictures™ attack which saw large amounts of information, including unreleased films, being stolen and computers wiped by malware.   The third category of motive we’ve seen is financial, seen in just over nine percent of groups. Again, this isn’t too surprising. Most targeted attack groups are state sponsored, meaning they have the resources of an entire country behind them. They don’t need money. Or, to be precise, they don’t need any more money.   * Lazarus group was also involved in the $81 million theft from the Bangladesh central bank in 2016, |

Source: *Verizon* *2018 Data Breach Investigations Report (11th Edition)*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 21 | According to the report, what is the difference between a breach and an incident? | An incident is a security event that compromises the integrity, confidentiality or availability of an information asset.  A breach is an incident that results in the confirmed disclosure— not just potential exposure—of data to an unauthorized party. |
| 22 | On average what is the average time interval that takes place to compromise a breached system? What is the average time interval that it takes to discover and contain a breach? | When breaches are successful, the time to compromise continues to be very short. While we cannot determine how much time is spent in intelligence gathering or other adversary preparations, the time from first action in an event chain to initial compromise of an asset is most often measured in seconds or minutes  However, discovery time is likelier to be weeks or months. The discovery time is also very dependent on the type of attack, with payment card compromises often discovered based on the fraudulent use of the stolen data (typically weeks or months) as opposed to a stolen laptop which is discovered when the victim realizes they have been burglarized. |
| 23 | What are the two main varieties of social attacks? Define them. | Phishing is the crafting of a message that is sent typically via email and is designed to influence the recipient to “take the bait” via a simple mouse click. That bait is most often a malicious attachment but can also be a link to a page that will request credentials or drop malware.  Pretexting is the creation of a false narrative to obtain information or influence behavior.  While there is a level of pretext to phishing attacks, we use pretexting for social attacks that include a level of dialogue or back and forth (and this certainly is the case when the pretexting is over the phone), but also if a specific persona was used by the attacker. |
| 24 | What percentage of malware is spread via email? What percentage is spread via the web at large? | 92.4% of malware is spread through email, while 6.3% is spread through the web. |
| 25 | What percentage of people in a given phishing campaign click it? What do the authors mean when they say: “The vampire only needs one person to let them in?” | Most people never click phishing emails. On average 4%2 of people in any given phishing campaign will click it.  Phishing is the initial entry point into an organization’s network and systems, so even if only 4% click on a phishing email, that entry point will allow an attacker to attack other parts of the system and organization. |
| 26 | What are the primary motivators in phishing attacks? | Motives for phishing are split between financial (59%) and espionage (41%). Phishing is often used as the lead action of an attack and is followed by malware installation and other actions that ultimately lead to exfiltration of data. |
| 27 | Provide some characteristics of ransomware | * It is a style of malware and the most prevalent variety of malicious code in 2018. It can be used in completely opportunistic attacks affecting individuals’ home computers as well as targeted strikes against organizations. It can be deployed across numerous devices in organizations to inflict bigger impacts and thus command bigger ransoms. It can be attempted with little risk or cost to the adversary involved. It can be successful with no reliance on having to monetize stolen data |
| 28 | Define botnet. According to this report, what are two ways that botnet attacks can occur. | DEFINE Botnets can affect you in two different ways. The first way, you never even see the bot. Instead, your users download the bot, it steals their credentials, and then uses them to log in to your systems. The aforementioned bounty of data provided through botnet takedowns represents this case. This attack primarily targeted banking organizations (91%) though Information (5%) and Professional Services organizations (2%) were victims as well.  The second way organizations are affected involves compromised hosts within your network acting as foot soldiers in a botnet |
| 29 | Define a DDOS attack.  What is the median length of a DDOS attack? | It is any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service. Most companies that do suffer a DDoS normally aren’t under attack that long each year—the median is three days. |
| 30 | Who are the most common threat actors targeting the public sector? What varieties of attacks are most commonly used? | External state-affiliated threat actors account for over half of all breaches. Phishing attacks, installations and subsequent uses of backdoors or C2 channels are front and center in espionage related breaches.  Cyber-Espionage, Privilege Misuse, Everything Else, Web Applications, and Miscellaneous Errors represent 92% of breaches |
| 31 | What is the top action category with regards to incidents? What is the top action category with regards to breaches? | DoS hacking is the top action category with regards to incidents.  Use of stolen credentials (also hacking) is the top action category with regards to breaches. |
| 32 | Who are the top external actors with regards to breaches? Who are the top internal actor varieties? | Organized crime actors are the top external actors with regards to breaches.  System admins are the top internal actors with regards to breaches. |
| 33 | What top two forms (file types) does malware typically take according to this report? | JavaScript (.js) (32%) and Visual Basic Script (.vbs) (21%) are the top two file types. |

Source: *Akamai State of the Internet / Security Q4 2017 Report*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 34 | In the opening passage of the report, Chris Kubeka highlights his desire to “put away the fire extinguisher,” what does she mean by this? | With the rise of the internet of things and a record number of people and devices connected to the internet, there is a larger more vulnerable attack surface, because many devices lack basic security and privacy safeguards. This has led to an increasing number of attacks and so instead of trying to just extinguish them one by one, it’s critical that we avoid these reactionary approaches and think about a more holistic and proactive approach to security. |
| 35 | Which industry has consistently shouldered the brunt of DDoS attacks over the last few years? What percentage of DDoS attacks affect them in Q4 and Q3 2017? | The gaming industry has consistently shouldered the brunt of DDoS attacks over the last few years. In Q4 2017 it accounted for 79% of all DDos attacks, and in Q3 2017 it accounted for 86% of attacks. |
| 36 | What is the Mirai botnet? How does it work? What event triggered the Mirai botnet’s extended longevity? | It is tool that was originally created to help a small group of college students who wanted an unfair advantage as a Minecraft hosting provider, but it became one of the most well-known DDoS tools on the Internet. It is responsible for a number of attacks, including one took down a large number of major sites around the world when it caused an outage at Dyn, a provider of dns services.  Mirai’s source code waspublicly released by its author, Anna-sempai. This move ensured Mirai’s longevity by making it possible for hackers around the globe to evolve and modify it for their own use. |
| 37 | Why do the nations of Egypt and Brazil appear so prominently in the botnet attack report? | In the case of Brazil, Mirai attacks were driven primarily by devices there, apparently because a large pool of vulnerable devices had been discovered in that region. According to Akamai’s initial research, a significant part of this pool consisted of Internet-enabled security cameras.   Satori, a Mirai variant, was primarily driven by devices located in Egypt. Though the specific device isn’t known, it is most likely a router or other network device heavily used by a service provider |
| 38 | According to the report, what were the two most common web attacks in 2017? Why do the authors suspect that the first vector is so dominant? | Sql injection (SQLi) attacks remained the dominant web attack vector in q4 2017 and made up 50% of all attacks. SQLi is a well-known and well-understood attack that has remained in the top position over time simply because organizations have not taken the time to protect their sites. Attackers will continue to utilize these vectors to gain access to systems if applications do not take the simple but necessary step of sanitizing data input and output. These types of attacks are easily automated and scalable, looking for any vulnerable system, rather than targeting specific organizations.  Local File Inclusion (lfi) came in second after SQLi attacks on the list of most used attack vectors, with a 36% share of the q4 attacks |
| 39 | Which three industries are most subject to credential abuse attacks? What percentage of login attempts are malicious in the case of these two industries? | Retail organizations saw the largest number of malicious login attempts in November (1 billion), followed closely by Hotel & Travel (968 million) and High Tech (781 million)  Retail organizations saw a total of 2.8 billion login attempts, of which 36% were considered to be malicious. Compared to the cross-industry average of 43%, Retail received relatively few attacks. High Tech companies saw 1.4 billion total login attempts, of which 57% were deemed malicious. The Hotel & Travel industry saw 1.2 billion login attempts in November, and 968 million were attempts that Akamai has judged to be malicious. This means 82% of login attempts at these sites, or more than four out of every five, were malicious! |
| 40 | What are APIs and why do the authors of Akamai believe that they are subject to increased threats in 2018? | API is the acronym for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other. Each time you use an app like Facebook, send an instant message, or check the weather on your phone, you’re using an API. When you use an application on your mobile phone, the application connects to the Internet and sends data to a server. The server then retrieves that data, interprets it, performs the necessary actions and sends it back to your phone. The application then interprets that data and presents you with the information you wanted in a readable way. This is what an API is - all of this happens via API.  Specifically with cryptocurrency attacks, attackers will compromise accounts and the APIs that make the exchanges accessible. The accounts are monitored by their account owners, but in large part the APIs that communicate and control most sites are underprotected.  This leads us to the final prediction of this report for 2018: APIs are going to be an increasingly popular attack surface for hackers. They are more long-term focused than short-term attacks such as DDoS attacks. Akamai has seen growth in this area throughout 2017, and the lack of controls and safeguards most organizations have around their APIs make them tempting targets for people who want to compromise systems without being detected. |