**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. | 2017 provided us with another reminder that digital security threats can come from new and unexpected sources. Coin-mining attacks explode. With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coin miners to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency.; A spike in software supply chain attacks. An increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting organizations. The Petya/Not Petya (Ransom. Petya) outbreak was the most notable example.; Ransomware business  experiences market correction the ransomware “market” made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity.; Drop in zero days can’t halt the rise in targeted attacks Symantec has found that overall targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering.; Mobile malware continues to surge Threats in the mobile space continue to grow year over-year. The number of new mobile malware variants increased by 54 percent in 2017. |
| 2 | What exactly is the Eternalblue exploit? Why was it so significant in 2017? | Eternalblue is a cyberattack exploit developed by the U.S. National Security Agency (NSA) according to testimony by former NSA employees. It was leaked by the Shadow Brokers hacker group in April 2017 and was used as part WannaCry ransomware attack in May 2017. |
| 3 | WannaCry and Petya/NotPetya: What are they? What is their significance? How did they spread? What were their implications? | WannaCry and Petya/ NotPetya attacks, dominated the ransomware landscape in 2017 but they were not “typical” ransomware attacks, and don’t represent the overall trend for ransomware. Petya/NotPetya was not a real ransomware, it was a destructive wiper that masqueraded as ransomware.  Like WannaCry, Petya/NotPetya also used the EternalBlue exploit to spread itself. |
| 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. In part this may be affected by the volatility in cryptocurrency values towards the end of 2017. |
| 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 is the number one infection vector employed by 71 percent of organized groups in 2017. 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? | One tactic we’ve frequently seen used over the years to infect the victims of targeted attacks is the exploitation of zero-day vulnerabilities, software vulnerabilities which were previously unknown and unpatched. However, in the past few years, usage of zero days seems to have declined and this appears to be borne out by our analysis. Only 27 percent of the groups we’ve investigated have been known to use zero-day vulnerabilities at any point in the past. There was a time when zero days were a valuable and powerful tool for targeted attack groups. But attackers have begun to eschew them in favor of less conspicuous tactics, namely “living off the land” by using whatever tools are on hand, such as legitimate network administration software and operating system features. |
| 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? | Of Android users, only 20 percent of devices are running the newest major version. The story is a little different for iOS™, as we see 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, often with bespoke changes required before doing so. Interestingly, although this figure is higher on iOS than for Android, the number is in decline since 2016, when 79.4 percent of iOS devices were patched to the latest major version, and 24 percent were at the latest minor release. |
| 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 service, short duration <1-hour, medium protected targets cost is $5-20.  Credit score repair cost is $50. Messing up people’s online presence cost is $500. The cost for Fake ID, driver license, and passport is from $10 – 600. The cost to hack a Gmail account is from $0.1 – 5. |
| 10 | What is the difference between a vulnerability and an attack? Provide an example of each mentioned in this report. | Put simply, vulnerabilities are a weakness in software systems, while exploits are attacks made to take advantage of vulnerabilities. |
| 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. Our telemetry shows that most downloads happened in the U.S., followed by Germany. |
| 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. | It is especially common for targeted attack groups to search for the weakest link in the chain. By spreading malware through an already established distribution channel, attackers can compromise a large volume of computers in a short period of time, especially if the compromised software has an automated update mechanism.  All this, without the need for an exploit that can be used for network propagation. Example: Infiltration of well-protected organizations by leveraging a trusted channel |
| 13 | How are DDoS attacks used in conjunction with Ransomware? | Plenty of cases in the past where attackers have employed DDoS attacks to cover up intrusions. However, in 2015 the use of ransomware as a decoy by a targeted attack group was something completely new. All of that quickly changed and by 2017 it was no longer an outlier. Several targeted attack groups had discovered ransomware. They put it to a range of uses but, in almost every case, it was used to devastating effect. DDoS attacks, using ransomware as a decoy had a similar effect, sowing confusion among the victims and delaying an effective response. |
| 14 | Talk about Butterfly, Dragonfly, and Turla from the Analyst stories. What made these groups interesting to the analysts? | Gavin O’Gorman said that Butterfly was one of the few targeted attack groups who didn’t appear to be affiliated to any country and were instead involved in corporate espionage, presumably for financial gain. Their operational security was some of the best we’ve seen. For example, they ran command and control servers on encrypted virtual machines on compromised servers. Stephen Doherty said that Dragonfly has been targeting critical infrastructure. At a time when these kinds of attacks were unthinkable, at least until Stuxnet surfaced. But now there’s several groups doing it. Dragonfly has been compromising energy companies since at least 2011. They’ve probably the ones that have come closest to crossing the line between intelligence gathering and something more hostile, like sabotage. Alan Neville said Turla used a lot of tools and tricks that I hadn’t seen before and really demonstrated the level of sophistication at which these groups operate. Even 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.  They were one of the first groups to use system fingerprinting techniques, whereby they analyzed visitors to watering holes and collected enough information to determine if the potential victim was of interest to the group, and if so, were able to determine the best exploit to deliver in order to gain a foothold within their target’s organization. |
| 15 | Describe each of the three most common techniques used in lateral movement. | Open Share is exploiting open network shares, which was used by just over four percent of groups.  Pass the Hash is where attackers steal and reuse the underlying hashed version of a password and, without cracking it, can use it to authentic themselves on other computers or servers—was used by just under six percent of groups.  Stolen Credentials is 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. |
| 16 | What was the most common username and password attempted by hackers trying to penetrate IoT devices? | most common username in 2016 & 17 was Root and for password in 2016 was admin for 2017 system |
| 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. | Some attacks where rather than compromising the software vendor, the attacker simply bought the rights to the software package and then sent a malicious update to the existing user base. The case reference is called CCleaner a popular system clean-up tool in August 2017, it 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. |
| 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? | 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 IoT attacks from 2016 to 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. | Using ransomware as a decoy had a similar effect, sowing confusion among the victims and delaying an effective response. the amount of ransomware being distributed has expanded rapidly, making it one of the most common cybercrime threats. Its ubiquity has made it a perfect cover for attacks. It’s now so widespread that admins may not be surprised by a ransomware attack or question an apparent ransomware infection.; Revenue-generating attacks When WannaCry (Ransom. WannaCry) first struck. WannaCry had a massive impact and, had the potential to be hugely profitable.; Ransomware as a disruption tool    the advent of ransomware as a decoy, followed by the appearance of WannaCry has led to the arrival of a third type of attack, namely ransomware as a form of disruption. The first and most notable case of this was Petya/Not Petya (Ransom. Petya). When it emerged, it initially appeared to be a WannaCry copycat. |

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? | Incidents vs. breaches We talk a lot about incidents and breaches, and we use the following definitions: Incident A security event that compromises the integrity, confidentiality or availability of an information asset. Breach 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. The discovery time is likelier to be weeks or months. |
| 23 | What are the two main varieties of social attacks? Define them. | Two main varieties of social attack that are focus on in this section; 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. |
| 24 | What percentage of malware is spread via email? What percentage is spread via the web at large? | Data shows that the most common vectors of malware are via email and malicious websites, so focus your efforts around those factors. Phishing (70% of social attacks) occurs when an attacker sends a communication—usually an email—to an individual attempting to influence them to open an infected file or click on a malicious link. Web Applications, Everything Else, and Miscellaneous Errors represent 92% of breaches within Information |
| 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?” | Unfortunately, on average 4% of people in any given phishing campaign will click it, and the vampire only needs one person to let them in. Meaning they only need one person to open email so they can gain access. |
| 26 | What are the primary motivators in phishing attacks? | first click in most campaigns is 16 minutes.3 Most people who are going to click a phishing email do so in just over an hour. The first report from a savvy user normally comes in around 28 minutes with half of the reports done by 33 minutes. So, you may not catch the first click but you might be able to limit the number of future clickers. |
| 27 | Provide some characteristics of ransomware | Characteristics of ransomware are its unbreakable encryption (can’t decrypt the files on your own); ability to encrypt all kinds of files from documents to pictures, videos, and audio files; scramble your files names so you can’t know data as affected; add a different extension to your files |
| 28 | Define botnet. According to this report, what are two ways that botnet attacks can occur. | A botnet is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks. 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 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? | DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. As far as attack strength, the median size of a DDoS has been getting smaller as time has gone on. The slow reduction in median DDoS size. This year it fell below a gigabit per second. |
| 30 | Who are the most common threat actors targeting the public sector? What varieties of attacks are most commonly used? | Cyberespionage remains a large concern for the public sector, with state-affiliated actors accounting for over half of all breaches. Privilege misuse and error by insiders account for a third of breaches. Threat actors -External (67%), Internal (34%), Partner (2%), Multiple parties (3%) (breaches) |
| 31 | What is the top action category with regards to incidents? What is the top action category with regards to breaches? | Top action varieties regarding incidents are DoS (hacking). Top action varieties regarding breaches are the use of stolen credentials (hacking) |
| 32 | Who are the top external actors with regards to breaches? Who are the top internal actor varieties? | Top external actor varieties in breaches are organized crime. Top internal actor varieties in breaches are system admin. |
| 33 | What top two forms (file types) does malware typically take according to this report? | JavaScript (.js), Visual Basic Script (.vbs), MS Office and PDF10 tend to be the file types found in first-stage malware. |

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? | Have some relief from of dealing with all the high-profile security events that took place and learn from them to develop a greater awareness to assist with future impacts. |
| 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? | Across industry gaming once again shouldered the brunt of overall attack traffic in q4 2017, though it saw a minor reprieve with a 7% drop in attack traffic compared with q3 2017. Nearly 80% of the DDoS attack traffic against gaming companies was directed at their Internet-facing assets. |
| 36 | What is the Mirai botnet? How does it work? What event triggered the Mirai botnet’s extended longevity? | Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or zombies. This network of bots, called a botnet is often used to launch DDoS attacks. At its core, Mirai is a self-propagating worm, that is, it's a malicious program that replicates itself by finding, attacking and infecting vulnerable IoT devices. It is also considered a botnet because the infected devices are controlled via a central set of command and control (C&C) servers. The release and modification of the Mirai code have kept the botnet active |
| 37 | Why do the nations of Egypt and Brazil appear so prominently in the botnet attack report? | One of the interesting things that the change in Mirai code highlights is the geographic distribution of certain devices. Both the initial and secondary attack spikes were driven primarily by devices in Brazil, 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. On the other hand, the Satori variant that surfaced in November has been primarily driven by devices located in Egypt. We don’t know the specific device that was added, but it is most likely a router or other network device heavily used by a service provider unique to Egypt. |
| 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? | Two most common web attacks in 2017 were ISQL injection (SQLi) and Local File Inclusion (LFI). SQLi attacks remained the dominant web attack vector.   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. |
| 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? | Three main types of organizations most affected by credential abuse: airlines, hotels and resorts, and online travel agencies. 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? | Application Programming Interface (API) a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service. Allow applications to communicate with one another. APIs are going to be an increasingly popular attack surface for hackers. 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. |