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.	1. **Cyber crime threat landscape**: is the statistics of how cyber crime is formulated from a timeline. In this since 2015 through 2017 the numbers of cyber crime threats has dropped due to the blockage of downloaders. This entitles that the level of protection has increased in its security system. 2. **Targeted Attacks by Numbers**: targeted attacks are the work of organized groups. The majority of these groups are state sponsored (although there is a small number of private operators) and they're usually driven by a small number of motivations: intelligence gathering, disruption, sabotage, or financial 3. **Ransomeware more than just Cyber Crime:** Ransomware is no longer just the preserve of the cyber criminal. Attackers are using a combination of malware and penetration testing tools to steal credentials, map the organization's network, and compromise many more computers, including file, application, and email servers 4. **Infecting the Software Supply Chain**: There was at least one large software update supply chain attack reported every month in 2017. Implanting a piece of malware into an otherwise legitimate software package at its usual distribution location; this can occur during production at the software vendor, at a third- party storage location, or through redirection. 5. **Mobile Threat Landscape**: Attackers have developed new methods of infection and tricks to remain on compromised devices as long as possible. They've also come up with a variety of means of generating revenue from devices, from ransomware to cryptocurrency mining

2	What exactly is the Eternalblue exploit? Why was it so significant in 2017?	Uses town know vulnerabilities in Windows to turn the ransomware into a worm, capable of spreading itself to any unpatched computers on the victim’s network and other vulnerable computers connected to the internet. **Significance**: **MAY 2017** WannaCry uses leaked EternalBlue exploit to spread globally in hours “Phonywall” fake ransomware used to cover-up targeted attack in SE Asia Disk-wiping malware disguised as ransomware in attacks on Ukraine **JUN 2017** Petya/NotPetya outbreak, mainly affecting Ukraine **OCT 2017** BadRabbit outbreak, mainly affecting Russia

3	WannaCry and Petya/NotPetya: What are they? What is their significance? How did they spread? What were their implications?	**WannaCry** : is a threat composed of two main parts, a worm module and a ransomware module. The ransomware module is spread by a companion worm module. The worm module uses the Microsoft Windows SMB Server Remote Code Execution Vulnerability (CVE-2017-0144) and the Microsoft Windows SMB Server Remote Code Execution Vulnerability (CVE-2017-0145) to spread. **Petya/NotPetya :** is a Trojan horse that encrypts files on the compromised computer. **Significance:** They disguise as Ransomware and once infected they traverse through the network and going across other computers that are vulnerable and connected to the internet. **Implications:** lowing down devices, overheating batteries and in some cases, rendering devices also financial implication to an organization for getting billed for the cloud cpu.
4	On average, how much is the average ransom amount requested in a Ransomware attack?	$522 in 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?	The number one infection vector is Spear phishing emails. The number two is the watering-hole websites. the attackers used a combination of malware and penetration testing tools to steal credentials, map the organization’s network, and compromise many more computers, including file, application, and email servers. The true purpose of the attack was data theft and, over the course of the intervening five months, the attackers managed to steal thousands of files from the organization. When they were finished, the intruders attempted to cover their tracks, deploying the fake ransomware to wipe the disks of infected computers.
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?	**Fall out of Favor**: the zero-day vulnerabilities they were using would have required a lot of time and skill to acquire on their own and they were most likely bought instead. **Security Implication**: Zero days like those cost a lot of money, which means they must have been earning a lot.

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?	**% Android users** : only 20% user are on the newest major version. **iOS Devices on Newest Major Version**: 77.3% **Discrepancy**: Over the years Android users are not keeping up to date with the latest major version of the OS or due to lack of the compatibilities older devices have to update. This exposes the network to be insecure. For iOS has issues that are vulnerable in terms of rooting the device to unlock its full potential control over the device, but may open doors for network breach or even lead to ransomeware request. **Security Implication**: a network threat may be something such as a malicious man-in-the-middle (MitM) style 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?	**Service for DDoS for 1 hour** = $5 - $20 **Credit Score Repair** = $50 **Generate Fake ID** = $10 - $600 **Online Presence** = $500 **Hack Gmail** = $0.1 - $5 **Security Implication** = Attackers will no doubt have noticed how effective both threats were. EternalBlue’s usefulness may be exhausted at this stage since most organizations will have patched, but there are other techniques that can be used. Petya/NotPetya employed other SMB spreading techniques using legitimate tools, such as PsExec and Windows Management Instrumentation Command-line (WMIC), to spread to network shares using stolen credentials.

10	What is the difference between a vulnerability and an attack? Provide an example of each mentioned in this report.	**Vulnerability** : the attacker uses spam, phishing, and or email malware trends/ The attackers behind the Zealot campaign sought to exploit vulnerabilities in order to install a Monero miner on unpatched machines. **Attack** : Symantec has found that overall targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering.
11	What exactly was the CCleaner Incident? What was the significance? How many people were affected? How did it occur?	**CCleaner** : the attack affected a total of 2.27M computers between August 15, 2017 and September 15, 2017 and used the popular PC cleaning software CCleaner version 5.33.6162 as a distribution vehicle. **Affected** : 2.27 million computers **How it occurred**: analysis of the data from the CnC server has proven that this was an APT (Advanced Persistent Threat) programmed to deliver the 2nd stage payload to select users.
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.	attacker replacing a legitimate software update with a malicious version in order to distribute it quickly. Any user applying the software update will automatically have their computer infected and will give the attacker a foothold on their network. It is not only desktop computers, the same applies to IoT devices and industrial controller components
13	How are DDoS attacks used in conjunction with Ransomware?	Basically the attackers would use Ransomeware as a decoy.

14	Talk about Butterfly, Dragonfly, and Turla from the Analyst stories. What made these groups interesting to the analysts?	**Butterfly**: were targeted attack groups not affiliated with any country but corporate espionage for financial gain. **Dragonfly:** They've been mainly targeting critical infrastructures such as compromising energy companies since 2011. **Turla**: hey 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.	**Pass the Hash**: "Pass the hash"—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 **Stolen Credentials**: 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. **Open Share:** attacker exploiting open network shares.
16	What was the most common username and password attempted by hackers trying to penetrate IoT devices?	**Username**: Root **Password**: 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.	The attacker bought the rights to the software package and then sent a malicious update to the existing user base.

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?	**Coinminer Attacks**: cyber criminals are using coin-miners to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency File Base: involves downloading and running an executable file on your computer Brower-base: 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?	600%
20	According to researchers, what are the three motivations for using ransomware? Describe each of them and an example named ransomware that utilized each.	• Financial — coin mining attack utilizing the users infected computer processing unit to mine the coins in return to collect the value in cryptocurrency for their pleasure • Disruption — disruptive attacks, most notably the 2014 Sony PicturesTM attack which saw large amounts of information, including unreleased films, being stolen and computers wiped by malware. • Intelligent gathering — Intelligence gathering can include information stealing, spying, and surveillance. In most cases, particularly when sabotage is involved, they are used sparingly and usually appear calibrated to send a message to the intended target.

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?	Breach : when private information or credentials are accessed without permission Incident: when an attack that occur in a certain timeline that uses a legitimate resource to fool the users to update or download in return being able to get to the users credentials and infecting millions of people and or computers
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?	Breached system — Seconds to Days Contain a breach — Weeks to Months
23	What are the two main varieties of social attacks? Define them.	Tailgating — when one person is physically following another person to enter a building to gain access. Spear-phishing — well-crafted email, sent to an unsuspecting staff member is the most likely source of compromise and can be the trigger to a potentially serious security breach
24	What percentage of malware is spread via email? What percentage is spread via the web at large?	32.4% in Ireland 14.5% spreader malware via websites
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?”	4% People didn’t click the phishing campaign — The actor is best left outside the walls
26	What are the primary motivators in phishing attacks?	Basically to steal the credentials of someone that has the permission to upload new binaries
27	Provide some characteristics of ransomware	Some of the characteristics of a ransomware is wiping the users hard disk and encrypting the files that the attackers got a hold of and demanding a lump sum in return to giving access back to the user with the decryption key.

28	Define botnet. According to this report, what are two ways that botnet attacks can occur.	— deployed via spam campaigns sent out by the Emotet botnet — as well as stealing information from infected devices, the malware is also capable of adding infected devices to the botnet.
29	Define a DDOS attack. What is the median length of a DDOS attack?	DDoS attacks can knock an organization offline, meaning that its systems admins will be busy trying to stem the DDoS attack and may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway.
30	Who are the most common threat actors targeting the public sector? What varieties of attacks are most commonly used?	Denial of Service is the most common threat actors targeting the public sector. Use of stolen credentials is most commonly used.
31	What is the top action category with regards to incidents? What is the top action category with regards to breaches?	— money would be the top action regards to incidents — hacking would be the top action regards to breaches.
32	Who are the top external actors with regards to breaches? Who are the top internal actor varieties?	Top external actors = organized crime Top internal actor = System admin
33	What top two forms (file types) does malware typically take according to this report?	Js Vbs

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?	She’s referring to putting away the fire extinguisher pertaining to not allowing the systems to take over the controls, but having the humans continue to work on the process.

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?	Infrastructure is the most common attack vectors Q3 - 22% Q4 - 30%
36	What is the Mirai botnet? How does it work? What event triggered the Mirai botnet's extended longevity?	Mirai botnet is utilizing default account credentials in order to breach devices. Because the of the high amount of IPs that were infected by the Mirai and also newly discovered botnets in other country triggered the extended life of the botnet.
37	Why do the nations of Egypt and Brazil appear so prominently in the botnet attack report?	Egypt and Brazil had the highest newly discovered vulnerable devices pertaining to active Mirai botnet IPs in 2016 & 2017
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?	The two most common web attacks in 2017 is the SQLi and Local File Inclusion. Because organization never took their time to protect their sites.
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?	Credential Abuse attack = Retail, Hotel & Tech and High Tech Retail — 36% malicious attempts High Tech — 57% malicious attempts
40	What are APIs and why do the authors of Akamai believe that they are subject to increased threats in 2018?	APIs is the Cryptocurrency Exchange. The authors of Akamai think that the increase threat of unsecured API of users will be the undetected activity by the attackers within the cryptocurrency exchange inverting users to use the infected cryptocurrency exchange.