Cybersecurity Threat Landscape
(Part II - Report Analysis)

Group Member Name: Vittal Siddaiah

Source: Symantec Internet Security Threat Report Volume 24 - February 2019

#	Question	Answer
1	The 2018 Year In Review portion of the report highlights eight key themes. Describe each of them.	**Formjacking** – The use of JavaScript to steal payment data from e-commerce sites. Symantec showed 4,800+ unique websites were compromised via formjacking every month in 2018. **Cryptojacking** – Is the use on computing resources from compromised systems to mine crypto-currencies. While the use of Cryptojacking has fallen, it remains popular due to ease of entry and minimal overhead. **Ransomware** – Is the encrypting of a victim's data and requiring payment to recover the data. While down overall 20% focus has changed from consumers to enterprises which showed a 12% increase. **Living off the Land & Supply Chain Attacks** – LotL is when attackers identify the processes that a business uses, then they focus on that as an attack vector. If a company is using PowerShell to conduct day to day business operations, then attackers would also use PowerShell scripts to "fly under the radar" and act maliciously. **Targeted Attacks** – Focus on key and vulnerable employees of companies to get access into an organization. This usually comes in the form of Spear phishing. **Cloud** – Issues in securing cloud services provide unique challenges. Because cloud servers share the same memory pool on a server, poorly secured cloud databases, could allow for one attack to affect more than just one company. **IoT** – The Internet of Things has provided an entire new surface of attacks. New technologies such as smart light bulbs, or voice assistants, introduce different attack vectors in a home or company. **Election Interference** – Misinformation, bots spamming social media, and fake websites, could point misinformed voters to a specific candidates agenda.
2		Formjacking is the process of injecting malicious JavaScript to be able to get end user's payment information, etc. In the Ticketmaster

	What if Formjacking and how was it introduced and used in the breach of TicketMaster	incident a third-party chatbot service was used to load the malicious code into the web browser of Ticketmaster site customers to get their payment data.
3	The Executive Summary starts out: "Like flies to honey, miscreants swarm to the latest exploits that promise quick bucks with minimal effort. Ransomware and cryptojacking had their day; now it's formjacking's turn." You work in a large enterprise and your boss reads this and says we no longer have to worry about Ransomware. Using the full report, explain why that statement is in error and clarify the current trends.	While it is true that Ransomware is down 20%, its focus has shifted from consumers to enterprises and the rate of ransomware infections in enterprise has increased by 12%. Ransomware can disrupt our systems, cost us money, cause loss of data and business interruption.
4	What is Emotet? Provide details of how much it is used and what makes it so dangerous.	Emotet is a financial trojan (worm) that jumped from 4% to 16% of the financial trojans from 2017 to 2018. What makes Emotet so dangerous is that it is a self-propagating but does not use remote vulnerabilities but instead moves laterally across a network by finding/brute forcing passwords.

5	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 65 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 accounting for 23%, 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 online gaming sector, they may compromise a game forum.
6	What is the main purpose of these targeted attacks?	96% of the groups primary motivation is intelligence gathering.

7	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 and what choices might it make for an enterprise environment?	Only 23.7% of Android users are on the latest major version but of those only 5.1% of Android users are on the latest minor version (meaning only 5.1% have the latest patched version). The leaves 18.6% without the very latest, but over 75% of Android users on a previous version of the phone's operating system. 48.6% of iPhone users have moved to the latest major version and an additional 29.7% on the very latest, leaving only 21.7% on older iOS systems. These statistics leave Android devices more vulnerable to attacks than iOS devices. Enterprise administrators may want to restrict BYOD (Bring Your Own Device) to iOS to reduce the risk, this is also supported by the number of Jailbroken or Rooted mobile device rate.
8	What IoT device has increased in being compromised in 2018 detail that changes.	Cameras increased from 3.5% in 2017 to 15% of the attacks in 2018.
9	What are the top three usernames and passwords used on IoT devices?	root, admin, enable are the top three user names and 123456, [BLANK], and system are the top three passwords
10	What is the top attack vector for IoT devices?	Telnet is the main protocol used to attack IoT devices, account for 91% of the attacks.
11	Seeing the trend, postulate what the trend will be for 2019 and what type of IoT devices may become more prominent?	With the large rise in the use of home IoT security such as the Ring Doorbell, attacks on these systems will increase as well as other home IoT devices. Bad actors can use to gain access inside a users home network and to monitor when they are home or not to advance physical theft.

12	What type of email attachment represents nearly half on the malicious attachments and how has that changed since 2017?	Office files (.doc) and this is representing 48% of malicious email attachments. And is up from only 5% in 2017.
13	What are the top three industries effected by malicious emails?	1) Mining 2) Agriculture, Forestry, & Fishing 3) Public Administration
14	Are users in small or larger organizations more likely to be targeted, explain the numbers?	Users in small (1-500 employees) were at higher risk with 1 in 6 and 500-1000 having a 1 in 4 rate of receiving malicious email verses 1 in 11 in large corporations. That was an outlier in the data with companies from 1501-2500 having 1 in 4. Then looking at the malicious email rate, 1 in 323 emails were malicious in companies 1-250 with large companies only having 1 in 556 be malicious.

Source: *Akamai – State of the Internet / Security Volume 5, Special Media Edition*
Credential Stuffing: Attacks and Economics

#	Question	Answer
15	What is credential stuffing? What are other names this is known by?	Credential stuffing is the systematic attempt to use know id/password pairs from one site on another. (many others). With the goal to find sites where the end-user had used those same credentials on a different site. Credential Reuse; Validation Attacks; Account Takeovers
16	According to the report, what industries are being targeted and why?	Gaming companies and the entertainment industry because these tend to be susceptible accounts and have real value. Be it in-game currency or the ability to trade or sell items, to the account itself.
17	How many of these attacks have been detected and what were the peaks during 2018?	30 Billion attacks in 2018 were detected, with peaks of 252,176,323 on June 8, 2018; 285,983,922 on October 24, 2018 and 287,168,120 on October 27, 2018.
18	Where were the 620 million passwords/usernames referenced in the report obtained from?	Some 617 million online account details stolen from 16 hacked websites Dubsmash (162 million), MyFitnessPal (151 million), MyHeritage (92 million), ShareThis (41 million), HauteLook (28 million), Animoto (25 million), EyeEm (22 million), 8fit (20 million), Whitepages (18 million), Fotolog (16 million), 500px (15 million), Armor Games (11 million), BookMate (8 million), CoffeeMeetsBagel (6 million), Artsy (1 million), and DataCamp (700,000). https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/
19	What is an AIO? What is one of the AIO referenced in the report and how much does it cost?	AIO is All-in-one and is an application to automate account takeovers. SNIPR - $20; STORM - $52.
20	What is the cost to purchase a compromised account? What if those credentials no longer work? What does that imply about the seller?	At minimum $3.25. Credentials that don't work at the time of sale, are replaced with another set of credentials at no charge. This implies the seller is looking to create "consumer" loyalty and additional (repeat) sales. This is a business savvy enterprise.
21	What are some of the challenges in mitigating the ATO risk?	Account takeovers use a company's normal login processes to validate the credentials. Care has to be taken in blocking these attempts so as to not disrupt normal "good" customer's use of the site.

Source: *Akamai – State of the Internet / Security Volume 5, Issue 1*
DDoS and Application Attacks

#	Question	Answer
22	The report has a guest author article on Mental Health, why is this relevant?	Managing Risk, dealing with live attacks and the pressures of the business leads to increased stress, lack of sleep and other mental health related issues. Learning how to deal with these issues and attending to your mental health help maintain your focus on work while at the same time maintaining your overall health.
23	What situations at work as a Cyber Security Professional might affect your mental health?	Breach Notifications Bomb/Violence threats Overbearing boss Criminal Activity Risk Mitigation Failures
24	Name six common signs of potential mental health issues.	• Excessive worrying or fear • Feeling excessively sad or low • Confused thinking or problems concentrating and learning • Extreme mood changes, including uncontrollable “highs” or feelings of euphoria • Prolonged or strong feelings of irritability or anger • Avoiding friends and social activities • Difficulties understanding or relating to other people • Changes in sleeping habits or feeling tired and low energy • Changes in eating habits such as increased hunger or lack of appetite • Changes in sex drive • Difficulty perceiving reality (delusions/hallucinations) • Inability to perceive changes in one’s own feelings, behavior, or personality • Abuse of substances like alcohol or drugs • Multiple physical ailments without obvious causes • Thoughts of suicide, or suicidal planning • Inability to carry out daily activities or handle daily problems and stress
25	Akamai's research discovered a vulnerability in jQuery. Does this effect all jQuery, explain?	No, the issue was found in the Blueimp’s jQuery File Upload project, but while fixed there, there are many uses (copies) that have not been updated.
26	Why when Akamai found 875,000 requests per second assumed to be a DDOS attack?	Because this was not normal behavior and was such an excessive amount of traffic.
27	Was it an attack? What was the root cause? Was this still a DDOS situation?	No. It was due to poorly tested software (warranty tool) that started “screaming” http requests. Yes, this was still a DDOS situation because that aberrant behavior could have shut down the services to the customer if the traffic had not been diverted.

28	What is a BOT and are they good or bad?	BOT (or robot) is an automated inquiry/request to a website. Most traffic to online business is bot traffic. There are both good Bots, and bad Bots.
29	What are common categories for known bots?	Search Engine Crawlers Web Archives Search Engine Optimization Audience Analytics Site Monitoring Services Content Aggregators Marketing Services Advertisement (could be bad…)
30	Looking at the Job Description in the report, what are the key takeaways?	They are advertising for people to write code that will most likely be used for illegal activities. They are looking for experienced programmers They are specifically trying to and looking for a person who can bypass Akamai and Cloudflare's anti-bot defenses.
31	What are some of the methods used by bad bots to avoid detection?	Spoofing known fingerprint characteristics Modifying cookies Playing back known good cookies Leveraging large numbers (thousands) of IP addresses Modifying client

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

#	Question	Answer
32	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.
33	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.
34	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.
35	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.
36	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 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.
37	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.

38	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
39	Define botnet. According to this report, what are two ways that botnet attacks can occur.	Botnets are groups of Bots working together. 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
40	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.
41	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
42	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.

43	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.
44	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.