Cybersecurity Boot Camp

Security 101 Challenge

Cybersecurity Threat Landscape

Part I: Crowdstrike 2021 Global Threat Report

For Part 1 of your homework assignment, use the *Crowdstrike 2021 Global Threat Report* along with independent research to answer the following questions. (Remember to make a copy of this document to work in.)

---

1. What was the dominant ransomware family that impacted the healthcare industry in 2020?

The dominant ransomware family was TWISTED SPIDER using *Maze*. Another family to take note of is WICKED SPIDER using *Conti* and *Ryuk*. *Ryuk* surged during Q4 of 2020 which coincided with the flu and cold season which is where the ransomware campaigns would have the most impact (even in a non-pandemic year).

2. Describe three different pandemic-related eCrime Phishing themes.

Why these pandemic related themes could have/were so successful is that they played on almost all of the exploitable human emotions which are greed, curiosity, fear, and desire to help.
One of the pandemic-related eCrime Phishing themes was “financial assistance or government stimulus packages”. This was very apparent because so many people were out of work at the time and that was their only source of income. This played on the greed, curiosity, and fear emotions.
Another theme was “impersonation of medical bodies” such as WHO and the CDC. People seeing these names in an email or message would have immediately

brought them comfort on the information being given. This could have exploited curiosity, fear, or desire to help emotions.
A third theme that was used was “exploitation of individuals looking for details on disease tracking, testing, and treatment”. Everyone was worried about when the vaccine was coming out and what they should do to be safer. So any information on those topics would have been an easy way to exploit people’s interest. This would have exploited curiosity and fear emotions mostly.

3. Which industry was targeted with the highest number of ransomware-associated data extortion operations?

The industry with the highest number of ransomware-associated data extortion operations was the industrial and engineering sector with 229 incidents. The manufacturing sector was a close second with 228 incidents. *note that the manufacturing sector takes an extra hit when this happens because of the disruption on day-to-day operations. Companies will be unable to meet production demands.*

4. What is WICKED PANDA? Where do they originate from?

WICKED PANDA is one of China’s most prolific adversaries that is currently being tracked by CrowdStrike Intelligence. As all of the cyber actors in China, they are some of the most prolific state-sponsored actors on the planet. WICKED PANDA’s main target groups are academic, manufacturing, government, telecommunications, and computer gaming. WICKED PANDA uses *Cobalt Strike* and *Meterpreter* malware families to deploy their software. A prime example of this state-sponsorship was back in September 2020. U.S. DOJ found individuals that worked with WICKED PANDA operations and were operating illicit for-profit cyber operations against video game firms. They did this for years without being punished because they were also supporting state-directed intelligence requirements.

5. Which ransomware actor was the first observed using data extortion in a ransomware campaign?

The ransomware actor that was first observed using data extortion was OUTLAW SPIDER.

6. What is an access broker?

Access brokers are threat actors that have gained access to organizations, ranging from corporations and government entities, and will sell this access to criminal malware operators. These brokers can be very beneficial to the criminal operators because they save them the need to identify targets and gain access. This allows for quicker malware deployment and higher potential for monetization. Common data that the access broker will sell are the IP addresses, endpoint URLs, login credentials, screenshots of desktop, cookies, and browser autofill history. This can all be used to gain initial access to the target system.

7. Explain a credential-based attack.

A credential-based attack is when the attacker steals “credential to gain access, bypass an organization’s security measures, and steal critical data” (What is a Credential-Based Attack? - Palo Alto Networks). Common examples of this are brute forcing, password spraying, and credential stuffing. Attackers often use phishing emails to gain access to credentials. This places a big emphasis on security awareness training for employees, especially during this remote service and privilege day and age.

8. Who is credited for the heavy adoption of data extortion in ransomware campaigns?

While OUTLAW SPIDER was the first observed to use this technique, TWISTED SPIDER has been credited as being the catalyst of the heavy adoption of data extortion in ransomware campaigns.

9. What is a DLS?

A DLS is a dedicated leak site, in terms of cybersecurity in this context. Big Game Hunters (BGHs) use these with their data extortion techniques. Two of the most active BGH adversaries with DLSs are TWISTED SPIDER with ~500 and WIZARD SPIDER with ~200.

10. According to Crowdstrike Falcon OverWatch, what percentage of intrusions came from eCrime intrusions in 2020?

In 2020, eCrime intrusions accounted for 79% of intrusions, which is up 10% from 2019.

11. Who was the most reported criminal adversary of 2020?

```
WIZARD SPIDER was the most reported criminal adversary of 2020, which now
makes it two years in a row.
```

12. Explain how SPRITE SPIDER and CARBON SPIDER impacted virtualization infrastructures.

```
SPRITE SPIDER (operators of Defray777) and CARBON SPIDER (operators of
DarkSide) deploy ransomware for Linux on ESXi hosts during BGH operations.
ESXi is a hypervisor that manages multiple virtual machines, things that run
virtualizations. These hosts also do not have the sufficient endpoint
protection software to help prevent ransomware attacks. SPRITE SPIDER  used
administrator credentials to hack into the vCenter web interface. Since they
deployed their ransomware onto the ESXi hosts, they were able to encrypt
multiple systems at once. This in turn helped improve the speed of BGH
operations.
Note that CARBON SPIDER recently made a huge change and shifted from
focusing on narrow campaigns, like POS devices, to broad campaigns and BGH
operations. This follows the trend of adversaries going from targeted eCrime
to focus on BGH.
```

13. What role does an Enabler play in an eCrime ecosystem?

```
Enablers play a big part in an eCrime ecosystem. They provide criminal
adversaries with capabilities and access that they may not have. They
specialize in certain areas to be able to sell initial access to these
criminal actors. BGH adversaries are not averse to working with these
Enablers to help make their operation more efficient.
```

14. What are the three parts of the eCrime ecosystem that CrowdStrike highlighted in their report?

```
The three parts of the eCrime ecosystem are Services, Distribution, and
Monetization.
```

15. What is the name of the malicious code used to exploit a vulnerability in the SolarWinds Orion IT management software?

```
The malicious code used against SolarWinds Orion IT management software was SUNBURST. This code used source code naming conventions wherever it was implemented which made it harder to detect.
```

Part 2: Akamai Security Year in Review 2020

In this part, you should primarily use the *Akamai Security Year in Review 2020* and *Akamai State of the Internet / Security* along with independent research to answer the following questions.

---

1. What was the most vulnerable and targeted element of the gaming industry between October 2019 to September 2020?

```
The most vulnerable and targeted element of the gaming industry between that time frame is its players. The variables of the human element always make it the hardest to control and secure.
```

2. From October 2019 to September 2020, which month did the financial services industry have the most daily web application attacks?

```
The month that saw the most daily web application attacks was in December 2019. There were close to 90-95 million total attacks, with 46,961,855 million of those being FinServ attacks.
```

3. What percentage of phishing kits monitored by Akamai were active for only 20 days or less?

```
From the phishing kits monitored by Akamai, more than 60% of them were only active for 20 days or less. This highlights the quick lifecycle of these devices and kits.
```

4. What is credential stuffing?

```
Credential stuffing is when attackers use already compromised user credentials and use them in other services to try to breach the system. This is usually done by bots for automation and scale. This is similar to brute
```

force attacks, besides the fact that brute force attacks try to guess with no context, so their success rate is much lower.
Multi-Factor Authentication is a great way to combat credential stuffing.

5. Approximately how many of the gaming industry players have experienced their accounts being compromised? How many of them are worried about it?

In the most recent report, there were roughly 55 million gaming logins during the month of September 2020. More than half of the frequency players have experienced their account being compromised, so around 22.5 million. But only one-fifth of them were worried about it, so around 11 million.

6. What is a three-question quiz phishing attack?

A three-question quiz phishing attack is when the scammer will imitate a known, trusted brand and give the victim a quiz with questions about the brand. These questions are related to the brand but with the aim of tricking the victims into giving away personal information. A common way this happens is that the victim will be presented a “prize” that they won after completing the quiz. This is usually where the victim will share their personal information and the scammer will receive it.

7. Explain how Prolexic Routed defends organizations against DDoS attacks.

Prolexic Routed defends organizations from DDoS attacks but finding and stopping them before they happen. They do this by filtering network traffic through the Akamai security operations center (SOC) which will detect and stop attacks before they happen. This allows for only “clean” network traffic to proceed to the targeted organization. Like mentioned before, the Prolexic Routed model is a great thing because it detects and stops attacks before they even happen.

8. What day between October 2019 to September 2020 had the highest Daily Logins associated with Daily Credential Abuse Attempts?

The day that had the highest Daily Logins associated with Daily Credential Abuse Attempts was August 17, 2020 with a total of 365,181,101 malicious login attempts.

9. What day between October 2019 to September 2020 had the highest gaming attacks associated with Daily Web Application Attacks?

```
The day that had the highest gaming attacks associated with Daily Web
Application Attacks was July 11, 2020 with a total of 14,631,618 attacks.
After further research, this could be related to the COVID-19 pandemic since
there was an insane 340% increase in attacks on web applications in the
gaming industry in 2020.
```

10. What day between October 2019 to September 2020 had the highest media attacks associated with Daily Web Application Attacks?

```
The day that had the highest media attacks associated with Daily Web
Application Attacks was August 20, 2020 with a total of 5,150,760 attacks.
```

Part 3: Verizon Data Breaches Investigation Report

In this part, use the *Verizon Data Breaches Investigation Report* plus independent research to answer the following questions.

---

1. What is the difference between an incident and a breach?

```
Although an incident and a breach are related to one another, they cannot be
synonymously used. An incident is where an event occurs that is not “normal”
with regular operations. Some examples of an incident are spam emails, a
DDoS, brute force attack enabling network access, or a malware infection.
Incidents are usually categorized on how severe they are to the
organization. A breach is when there is “unauthorized access to an
organization’s network, data, applications, or devices” (McCourt, 2021). A
breach can be seen as a specific kind of incident that is usually seen as a
severe incident.
Data breaches are usually disclosed to the public, whereas incidents are not
required to be (depends on the severity of the specific incident).
```

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?

Between the time range of 2016-2020, the average percentage of breaches perpetrated by outside actors was around 70-75%. There was a slight increase from ~70% to ~80% from 2019 into 2020.
Within the same time frame, the average percentage of breaches perpetrated by internal actors was around 20-30%. There was a slight decrease from 2019 to 2020, in accordance with the rise of external actors.

3. What percentage of breaches were perpetrated by organized crime?

The percentage of breaches that were perpetrated by organized crime was around 80%. Organized crime is the main category for actors as the next two categories, “Other” and “Unaffiliated”, are both around 5-15%.

4. What percentage of breaches were financially motivated?

The percentage of breaches that were financially motivated from the time range of 2016-2020 had an average of around 80%. There has been a generally linear increase to this percentage from 2016 (~70%) to 2020 (~90%). This rise in financially motivated breaches have of course decreased the “espionage” and “other” category motives for breaches.

5. Define the following (additional research may be required outside of the report):

Denial of service: This is a type of cyber attack where hackers/criminals prevent the intended/legitimate user from accessing the computer itself or the network. It is done by using a single Internet connection and one IP address to send continuous requests to the target server to overload the server’s bandwidth. This will exhaust the RAM and CPU of the computer. The most common and harder to detect type of DoS attack is a distributed denial-of-service (DDoS) attack. This type of attack is done using multiple connected devices attacking the same target server which is why it is so much harder to detect and stop.

Command control: Command and control cyber attacks (also known as C2 or C&C) are very dangerous and can compromise an entire network. This is done by the attacker infecting a computer’s network through phishing, security holes, or other malicious software. After this connection is done the attacker has full control and the commands of the infected computer and can install additional software. Typically the attacker can then infect more computers on that same network, thus creating a botnet. Attackers can accomplish things like DDoS, data theft, and shutdowns and reboots of the systems.

Backdoor: A backdoor cyber attack is a type of attack that bypasses the computer's and/or network's authentication system without being detected. This authentication system is usually the conventional username and password process. The attacker gains access to the computer's files and system without needing authentication.

Keylogger: A keylogger is a type of spyware that will monitor and track the infected user's keystrokes. This allows the attackers to record anything the victim types on their keyboard. Things that the attacker usually looks for are their passwords, account numbers, and credit card information. Advanced keyloggers can even do more than just track your keyboard inputs. Things like tracking activity with files, record screenshots, and record activity throughout the computer's functions can be done.

6. What remains one of the most sought-after data types for hackers?

Credentials still remain one of the most sought-after data types for hackers making up around 60% of the type of data attacked. Credentials are usually the username and password of the targeted network that the attackers want. Credential data type is followed by Personal data which makes up around 40% of the data types.

7. What was the percentage of breaches involving phishing?

The percentage of breaches involving phishing was 36% in this year, which is up from 25% from the last. The rise in this percentage is due in part to the COVID-19 phishing campaigns with everyone staying at home with the national orders in effect. Phishing has been the top action variety in breaches for the past two years.