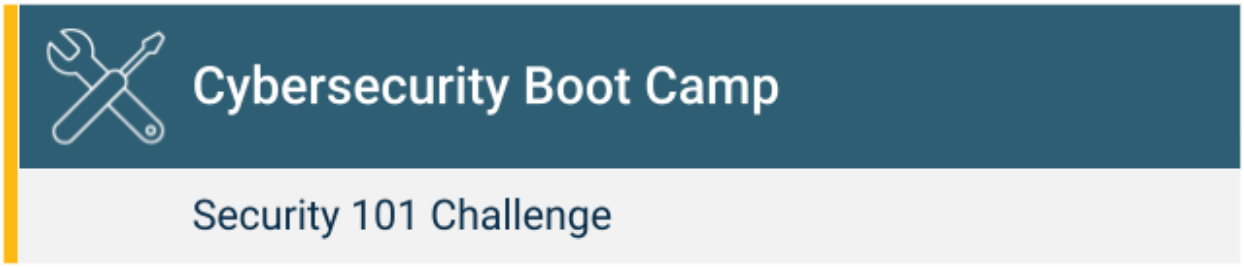

Cybersecurity Threat Landscape

Part 1: 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 on):

---

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

```
According to the Crowdstrike 2021 Global Threat report, the most common
ransomware family utilized against the healthcare industry was “Maze”.
```

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

```
During the pandemic, hackers were able to take advantage of the fear and
uncertainty surrounding Covid-19. Several types of pandemic related phishing
scams arose from this.

a) During the pandemic, governments began handing out stimulus cheques. As
people began receiving them, they began to boast about it on social media
platforms. However, because most governments staggered these payments, not
everyone received their money at the same time. This led people who had not
received their cheques to wonder about the status of theirs. Phishing emails
claiming to be official government portals were deployed in order to get
people to fill out personal information for the purpose of checking the
status of their stimulus money.
```

```
b) Fraudulent stores offering personal protection equipment (PPE) used phishing emails to prey on the rising fear and concerns for personal safety. Furthemore, these emails boasted free shipping to people who were in lockdown and unable to shop in person. These false storefronts would include covid-19 stats and updates to store policy in order to further convince targets that they were real.

c) Fake CDC (center for disease control) emails acting as donation portals for covid-19 relief efforts.
```

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

```
According to the 2021 Crowdstrike report, the Industrial and Engineering sectors were most heavily targeted by ransomware based attacks.
```

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

```
WICKED PANDA is a Chinese state sponsored adversary with a focus on espionage, surveillance and the theft of intellectual property, mainly within the telecom sector. They gain access to systems by exploiting software vulnerabilities in order to deploy Malware such as Cobalt Strike and Meterpreter. They are well funded and resilient.
```

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

```
OUTLAW SPIDER first employed the tactic of deploying ransomware for the purpose of data extortion combined with a dedicated DLS to conduct extortion operations in 2019.
```

6. What is an access broker?

```
Access brokers specialize in selling backend access information for both corporate and government sites. Levels of offered access range from full admin control to basic login credentials. These brokers are generally used by Big Game Hunters and other ransomware based attackers through criminal forums or private channels. Attackers save a lot of time determining their targets as the access broker provides that for them, allowing them to operate more efficiently.
```

7. Explain a credential-based attack.

```
User account credentials are harvested through either an exploit or
phishing. The adversary can then use the obtained login credentials to gain
access to more sensitive data as the target usually has an elevated level of
access in their company or organization. From here, the adversary can
escalate their access privileges and completely take over a domain and
access information on all users within it.
```

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

```
TWISTED SPIDER was the first actor to heavily embrace data extortion tactics
starting in 2020. This sparked a shift from threats targeting something like
point of sale systems to Big Game Hunting and data extortion. This also led
to the rise of network access brokers as more and more adversaries began
shifting to BGH and required backdoor access to their targets.
```

9. What is a DLS?

```
DLS is short for Dedicated Leak Site. These are websites where ransomware
actors leak or threaten to leak the data they have stolen if the target does
not pay the required ransom.
```

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

```
79% of intrusions were committed by eCriminals in 2020.
```

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

```
With the explosion of BGH attacks in 2020, WIZARD SPIDER saw itself as the
most prolific actor on this stage. So it is no surprise that they were the
most reported adversary in this year. With a wide range of tools at their
disposal and strong relationships with other threat actors, WIZARD SPIDER is
a formidable threat in the eCrime world.
```

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

```
Both of these adversaries utilized the less popular technique of deploying
Linux based ransomware that attacked ESXi hosts, or virtual servers. This
enabled them to quickly encrypt large amounts of data being hosted on said
servers for the purpose of ransom. Because these ESXi hosts had no backend
protection against ransomware, it made them extremely vulnerable to attack.
```

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

```
Enablers offer Malware/Ransomware as a service. They sell malware to
adversaries for use in their various attacks. They work closely with BGH and
access brokers to help facilitate eCrime.
```

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

```
The three elements of the eCrime ecosystem highlighted in this report are:

   a) Services - This includes access brokers, phishing kits, ransomware,
      recruiting, malware services and any other tools or services that
      facilitate eCrime, particularly BGH.
   b) Distribution - this element refers to the distribution of spam emails,
      instant messaging spam and other ways to deliver malware to their
      intended targets.
   c) Monetization - this refers to the avenues eCriminals use to get paid.
      So money laundering services, ransom payments, wire fraud and cashing
      services all fall under this umbrella.
```

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

```
SUNBURST was the name of the malicious code injected into SolarWinds that
allowed the StellarParticle activity cluster to gain access and control of
the supply chain software or C2.
```

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 and September 2020?

```
As with any target in the cyber security world, the most vulnerable element of the gaming industry was its users, or players, in this case.
```

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

```
December 2019 saw the most daily web application attacks on the financial services industry. This is due largely in part to attackers adopting automation.
```

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

```
More than 60% of monitored phishing kits were only active for 20 days or less. Due to the quick life cycle of these packages, we can infer that eCriminals are constantly updating and refining their techniques and kits.
```

4. What is credential stuffing?

```
Credential stuffing is when an attacker obtains stolen login credentials from one platform and then utilizes them to attempt to gain access to other platforms using the same login info.
```

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

```
According to the report, more than 50% of gamers said their accounts had been compromised, yet only 20% were actually worried about it happening to them.
```

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

```
The attacker in this case will send out a phishing email fraudulently posing as a popular or respected brand. The target is prompted to answer 3 quiz
```

```
questions about the brand and then is redirected to a site requesting their
personal information, notably their email, address and age.
```

7. Explain how Prolexic Routed defends organizations against Distributed Denial of Service (DDoS) attacks.

```
Prolexic Routed essentially takes all network traffic, sanitizes the input
and filters the output. This ensures that only clean, legitimate traffic can
proceed. The remaining traffic is then monitored to ensure no further action
is needed. This allows security teams to stop a denial of service attack
before it happens by filtering out all the superfluous traffic to the site.
```

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

```
[Enter answer here]
```

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

```
On October 7, 2019, the highest number of daily web application attacks in
the gaming world was recorded with 85,846,516 attempts in one day.
```

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

August 20, 2020, saw 5,150,760 attacks on media based targets.

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?

```
A security incident is an event that compromises the CIA triad of an asset.
For example, clicking through on a phishing email and infecting your
computer with malware would be an incident since said malware could affect
```

the CIA triad. If we were to push this scenario further and say that data from the compromised system was found on a DLS, we could conclude that this was a breach. The reasoning being that in this instance we have confirmation that the data has been leaked.

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

According to the Verizon report, from 2016-2020, external threat actors were responsible for around 70% of breaches, with that number actually rising between 2019-2020, to 80%. Over that same span of time, internal actors made up roughly 30% of breaches, with that falling to 25% between 2019-2020. As external breaches grew, internal breaches fell, relatively speaking.

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

There are several threat actors to consider in the world of cyber security; script kiddies, nation states, hacktivists or insiders. However, by far, the most prolific threat actor is organized crime. They are financially motivated and are responsible for 80% of breaches.

4. In 2020, what percent of breaches were financially motivated?

Since organized crime accounts for 80% of data breaches, and we know that their main motivation is money, it comes as no surprise that in 2020, roughly 80% of breaches were financially motivated.

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

Denial of service: Denial of Service or DoS/DDos is a type of attack that seeks to disrupt the availability of data on a host server. This is done by overwhelming the host server with excessive false traffic in the hopes that legitimate traffic cannot get through to access the data in question.

Command control:This refers to gaining remote control of a target system by creating a link between the hacker's command center and the target system. Once established, the attacker can steal data, escalate their attack within the compromised system and even attack another system from the compromised one.

Backdoor:A backdoor is a point of access to a system of which the main user is unaware. This affords the attacker discrete access to your system. There are two types of backdoors; hardware based and software based. Physical hardware can be installed by the attacker on the system in question or it can be infected through the use of a malware based backdoor.

Keylogger:This is a type of malicious software that records the keystrokes on an unsuspecting user's system or machine. The idea is that the attacker can observe what keys are being pressed when the victim types sensitive login info or other personal data.The attacker can then record the credentials of the user and utilize them to escalate their attack.

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

Because organized crime makes up 80% of threat actors, and because these actors' main motivation is financial, it makes sense that the most sought after data type for hackers is banking and credit card information.

7. What was the percentage of breaches that involved phishing?

In 2020, 36% of breaches involved phishing. This rose up from 25% in 2019 due to the ramping up of phishing based attacks during the pandemic. Covid-19 offered hackers a powerful pretext to use in phishing emails, preying on people's fear and uncertainty during this time. The main goal of these phishing attacks was to acquire login credentials that could in turn be exploited for financial gain. The deployment of C2 and backdoor malware through phishing emails allowed hackers to conduct a sustained attack on infected systems and provided a jumping off point for further incursions on other systems.