Security 101 Homework: Security Reporting

Part I: Symantec

For Part 1 of your homework assignment, you should primarily use the *Symantec Internet Security Threat Report* along with independent research to answer the following questions.

1. **What is formjacking?**  
     
   Formjacking is the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites.
2. **How many websites are compromised each month with formjacking code?**   
   There were 4,818 unique websites that were compromised each month in 2018.
3. **What is Powershell?**

Powershell is a task automation and configuration management framework from Microsoft.

1. **What was the annual percentage increase in malicious Powershell scripts?**  
   The annual percentage increase in malicious Powershell scripts was an 1,000 percent increase in 2018.
2. **What is a coinminer?**

A coinminer is a program that generates cryptocurrency.

1. **How much can data from a single credit card can be sold for?** Data from a single credit card can be sold for $45.
2. **How did Magecart successfully attack Ticketmaster?**

Magecart successfully attacked Ticketmaster by compromising a third-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster’s website, with the aim of harvesting customers’ payment data.

1. **What is one reason why there has been a growth of formjacking?**

One reason why there may have been a growth of formjacking is that the value of cryptocurrency dropped that year.

1. **Cryptojacking dropped by what percentage between January and December 2018?**

Cryptojacking dropped by 52% between January and December in 2018.

1. **If a web page contains a coinmining script, what happens?**

If a web page contains a coinmining script, the computing power will be used to mine for cryptocurrency for as long as the web page is open.

1. **How does an exploit kit work?**

An exploit kit works by gathering information on the victim machine, finds vulnerabilities, and determines the appropriate exploit.

1. **What does the criminal group SamSam specialize in?**

The criminal group SamSam specializes in ransomware.

1. **How many SamSam attacks did Symantec find evidence of in 2018?**

There was evidence of 67 SamSam attacks in 2018.

1. **Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?**

Even though ransomware attacks declined, the one dramatic changes was that enterprises were becoming more infected at an accelerated rate.

1. **In 2018, what was the primary ransomware distribution method?**

In 2018, the primary ransomware distribution method was email campaigns.

1. **What operating systems do most types of ransomware attacks still target?**

The operating system that most types of ransomware attacks target is Windows.

1. **What are “living off the land” attacks? What is the advantage to hackers?**

“Living off the land” attacks are ones that opt for off-the-shelf tools and operating features to conduct attacks. The advantage to hackers is that PowerShell is now a staple for both cyber crime and those being targeted.This means that attackers can now blend into networks and hide among legitimate users.

1. **What is an example of a tool that’s used in “living off the land” attacks?**

Astaroth is an example of a tool that’s used in “living off the land” attacks.

1. **What are zero-day exploits?**

Zero-day exploits are vulnerabilities that are first discovered and have no current fix.

1. **By what percentage did zero-day exploits decline in 2018?**

Zero-day exploits declined from 27 percent to 23 percent.

1. **What are two techniques that worms such as Emotet and Qakbot use?**

The two techniques that worms such a Emotet and Qakbot use are simple techniques. It uses the dumping of passwords from memory or brute-forcing access to network shares to laterally move across a network.

1. **What are supply chain attacks? By how much did they increase in 2018?**

Supply chain attacks are attacks that aim to damage an enterprise by targeting elements in the supply chain that may be less secure. Supply chain attacks increased by 78 percent in 2018.

1. **What challenge do supply chain attacks and living off the land attacks highlight for organizations?**

The challenge that supply chain attacks and living off the land attack highlight for organizations is that attacks are increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.

1. **The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?**

The 20 most active groups tracked by Symantec targeted an average of 55 organizations.

1. **How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?**

There were 49 individuals or organizations that were indicted during 2018. These individuals and organizations were from Russia, China, Iran, and North Korea.

1. **When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?**

When it comes to the increased number of cloud cybersecurity attacks, it shows that poorly configured databases continued to be a weak point for organizations.

1. **What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?**

The implication is that a successful attack on a single physical system could result in data being leaked from several cloud instances.

1. **What are two examples of the above cloud attack?**

Meltdown and Spectre.

1. **Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?**

The two most common infected devices of IoT attacks were routers and connected cameras. They account for 75 and 15 percent of the attacks respectively.

1. **What is the Mirai worm and what does it do?**

The Mirai worm is a worm that infects smart devices that run on ARC processors. It then uses them as bots to launch DDoS attacks.

1. **Why was Mirai the third most common IoT threat in 2018?**

Mirai was the third most common IoT threat in 2018 because it is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection. It also expanded its target scope by going after unpatched Linux servers.

1. **What was unique about VPNFilter with regards to IoT threats?**

VPNFilter was unique because it was the first widespread persistent IoT threat. It can survive a reboot making it very difficult to remove.

1. **What type of attack targeted the Democratic National Committee in 2019?**

The DNC was targeted by an unsuccessful spear-phishing attack.

1. **What were 48% of  malicious email attachments in 2018?**

Office files accounted for 48 percent of malicious email attachments in 2018.

1. **What were the top two malicious email themes in 2018?**

The top email themes in 2018 were Bill and Email delivery failure.

1. **What was the top malicious email attachment type in 2018?**

The top malicious email attachment type was .doc and .dot.

1. **Which country had the highest email phishing rate? Which country had the lowest email phishing rate?**

Saudi Arabia had the highest email phishing rate, while Canada had the lowest email phishing rate.

1. **What is Emotet and how much did it jump in 2018?**

Emotet is a self-propagating malware that jumped up to 16 percent from 4 percent in 2017.

1. **What was the top malware threat of the year? How many of those attacks were blocked?**

The top malware threat of the year was Heur.AdvML.C and there were 43,999,373 attacks blocked.

1. **Malware primarily attacks which type of operating system?**

Malware primarily attacks the Windows operating system.

1. **What was the top coinminer of 2018 and how many of those attacks were blocked?**

The top coinminer of 2018 was JS.Webcoinminer and there 2,380,725 attacks blocked.

1. **What were the top three financial Trojans of 2018?**

The top three financial Trojans of 2018 were: Ramnit, Zbot, and Emotet.

1. **What was the most common avenue of attack in 2018?**

Spear-phishing emails remained the most popular avenue for 2018.

1. **What is destructive malware? By what percent did these attacks increase in 2018?**

Destructive malware is malicious software with the ability to render the affected machines inoperable. It went up 25 percent in 2018.

1. **What was the top user name used in IoT attacks?**

The top user name used in IoT attacks was root.

1. **What was the top password used in IoT attacks?**

The top password used in IoT attacks was 123456.

1. **What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?**

The top three protocols used in IoT attacks were: telnet, http, and https. The top two ports were 23 and 80.

1. **In the underground economy, how much can someone get for the following?**

1. **Stolen or fake identity:**

$.10 - $1.50

1. **Stolen medical records:**

$15 - $20

1. **Hacker for hire:**

$100+

1. **Single credit card with full details:**

$1 - $45

1. **500 social media followers:**

$2 - $6