Nama : Sasmita Rachmawati

Absen : 15

Lab - Evaluate Cybersecurity Reports

Objectives

Part 1: Research Cyber Security Intelligence Reports

Part 2: Research Cyber Security Intelligence Based on Industry

Part 3: Research Cyber Security Threat Intelligence in Real Time

Background / Scenario

In the last two years, schools and universities have implemented remote learning. Even companies have adopted a hybrid workspace. What are some of the additional cyber security risks to moving on-line? What are the new trends in ransomware? Most organizations lack the trained personal to keep up the cyber threat landscape in real-time. As a result, some companies rely on cybersecurity threat intelligence reports to help them better understand and prevent cyber threats.

There are a number of companies and government agencies that offer near real-time, high-quality cyber threat information. Access to this data may require you to register on their website or pay a subscription fee. Some data is OpenSource INTelligence (OSINT) and can be accessed from publicly available information sources.

The focus of this lab is to research a few freely available cybersecurity intelligence reports.

Required Resources

- Device with internet access

Instructions

Part 1: Research Cyber Security Intelligence Report

Some companies are using machine learning and artificial intelligence to help collect and identify and defend against cyber threats.

Step 1: Identify findings of the Webroot Threat Report

Use an internet browser to search **webroot threat report final 2020 pdf.** Scroll past any advertising and open the document **2020 Webroot Threat Report_US_FINAL.pdf** and review their findings.

Questions:

Based on their findings, where does malware typically hide on a Windows PC?

- **Answer : For consumer PCs, 26.5% of all infections are found in %appdata% folder. 85% of threats hide in 1 of 4 locatio: %temp%, %appdata%, %cache% and %windir%.**

Based on their findings, what are some trends in ransomware?

1. **More Recon -> Attackers are focusing their efforts on learning about a company and its infrastructure, including critical servers and backup location**
2. **Rising Ransom Costs -> These figures are reported by Coveware, a company specifically set up to help ransomware victims pay their ransom. The average ransom amount is increasing, in 2019, it reached $41198 up from $36,395 in Q1.**
3. **Higher Stakes -> A recent trend in ransomware is to not just steal or lock an organization's data but to threaten the victim with leaking or otherwise abusing the data.**
4. **Shifting Targets -> 2019 saw an epidemic of ransomware attacks on US cities, as well as systematic attacks on favored targets, such as transportation, healthcare, education and SMBs.**

Based on their findings, what are the current trends in Phishing attacks?

1. **Email Hacking: Hackers continue legitimate email conversations by attaching malicious payloads that can evade email filters.**
2. **HTTPS Usage: More phishing sites now use HTTPS, making them appear secure and harder to detect.**
3. **Phishing Trends: Phishing attacks follow public news, such as new product launches (iPhone), to exploit potential victims.**
4. **Impersonation of New Companies: Companies like DocuSign and Steam are being targeted, presenting challenges for digital signatures and automatic updates.**

Based on their findings, why are Android devices more susceptible to security issues?

1. **Vulnerable Apps on Android: Android devices come pre-installed with 100 to 400 apps. These apps are often overlooked in terms of security updates or scrutiny by both users and developers, making them more vulnerable to cyberattacks.**
2. **Threat Targeting: These pre-installed apps often have extensive permissions on the device, and if they contain security flaws, hackers can exploit these vulnerabilities to steal data or gain unauthorized access. Because these apps are so commonly installed, they become attractive targets for attackers.**

Investigate the organization that created the report. Describe the company.

Webroot is a cybersecurity company that offers a variety of security products and services for home and business use. They focus on protecting devices from cyber threats like malware, ransomware, and phishing attacks with cloud-based solutions that are lightweight and fast.

Part 2: Research Cyber Security Intelligence Based on Industry

Some companies produce threat intelligence reports based on industry. In this part of the lab, you will investigate these industry-oriented reports.

Research an Intelligence Report Based on Industry.

a. Use an internet browser to search **FIREEYE cyber security**.

b. Click on the link to the FIREEYE home page.

c. From the FIREEYE home page menu click **Resources**.

d. From the menu select **Threat Intelligence Reports by Industry.**

e. Select the **Healthcare and Health Insurance** industry and download their report.

Based on the FIREEYE findings identify the two most commonly used malware families by threat actors for this industry.

Question:

Briefly describe the malware.

Malware in Healthcare Industry:

- **WITCHCOVEN (49%): A commonly used malware by threat actors in the healthcare sector, employed for initial reconnaissance or footprinting. It helps attackers map out the organization's systems.**
- **XtremeRAT (32%): This is a Remote Access Tool (RAT) that allows attackers to:**
    - **Upload and download files.**
    - **Manipulate Windows registry, processes, and services.**
    - **Capture sensitive data like user credentials.**
    - **It provides the attacker with significant control over the victim's system.**

f. Return to the Threat Intelligence Reports by Industry page and select the Energy industry. Download the report.

g. Based on the FIREEYE findings identify the two most commonly used malware families by threat actors for this industry.

Question:

Describe the malware.

Malware in Energy Industry:

- **SOGU (41%): A backdoor malware that can upload and download files, access the filesystem, registry, and even provide a remote shell. It uses a custom protocol to give attackers graphical control over the victim's desktop.**
- **ADDTEMP (20%): Also known as Desert Falcon or Arid Viper, this malware is typically delivered via spear phishing. It can manipulate files, processes, and other system functionalities.**

Part 3: Research Cyber Security Threat Intelligence in Real Time

Today, sharing threat intelligence data is becoming more popular. Sharing cyber threat data improves security for everyone. Government agencies and companies have sites which can be used to submit cyber security data, as well as receive the latest cybersecurity activities and alerts.

Step 1: Access the Cybersecurity and Infrastructure Security Agency web site

a. Use an internet browser to search **Department of Homeland Security (DHS): CISA Automated Indicator Sharing**.

b. Click on the **Automated Indicator Sharing | CISA** link.

c. From the Menu options click on CYBERSECURITY. On the CyberSecurity webpage, you should see many Quick Links options. Scroll down the page to the Nation State Cyber Threats section.

Questions:

Identify the four accused Nation State Cyber Threats.

1. **China**
2. **Russia**
3. **North Kora**
4. **Iran**

Select one of the accused Nation States and describe one advisory that has been issued.

- **An advisory might describe ongoing cyber espionage efforts by a specific nation-state targeting sensitive sectors such as healthcare, energy, or government agencies. For example, a North Korean threat might focus on financial institutions, aiming to steal cryptocurrency or disrupt banking operations.**

Step 2: From the CYBERSECURITY|CISA web page download and open the CISA Services Catalog

a. Return to the CYBERSECURITY|CISA web page. Scroll down to the CISA Cybersecurity Services section of the page. Locate and click on the **CISA Services Catalog** link.

b. The CISA catalog provides access to all of the CISA services areas in a single document. Click on the link to download the CISA Services Catalog

c. Next. scroll down to page 18, Index - SERVICES FOR FEDERAL GOVERNMENT STAKEHOLDERS. Under the **Service Name** column locate **Current Cybersecurity Activity**

d. Click on the corresponding Website URL. From this page, document two cybersecurity updates that have been issued regarding software products.

Question:

What is the software company name and timestamp? Briefly describe the update.

Example Software Updates:

- **Apple Security Update (Sept 21, 2021): A series of updates for products like iOS 15 and watchOS, recommending immediate patching to address vulnerabilities.**

- **Adobe Update (Sept 14, 2021): Security updates were released for Photoshop Elements and Acrobat to patch critical vulnerabilities.**

Reflection Questions

1. What are some cybersecurity challenges with schools and companies moving towards remote learning and working?

- **Increased phishing attacks through email, messaging apps, and video conferencing platforms. Cybercriminals target people working remotely with scams exploiting less secure home networks.**

2. What are two terms used to describe ADDTEMP malware and how is it delivered?

- **Also known as Desert Falcon or Arid Viper, this malware is often delivered through spear-phishing emails with malicious attachments or links.**

3. Search the web and locate other annual cybersecurity reports for 2020. What companies or organizations created the reports?

- **Companies like Cisco, TrendMicro, and Check Point produce annual cybersecurity reports, highlighting trends and major threats.**

4. Locate a cybersecurity report for another year. What was the most common type of exploit for that year?

- **Depending on the year, exploits might include vulnerabilities in remote desktop protocols (RDP) or email server vulnerabilities. For example, in 2020, many attacks leveraged vulnerabilities in Microsoft Exchange.**

5. How are these reports valuable, and what do you need to be careful of when accepting the information that is presented in them?

- **These reports are crucial for staying informed about the latest threats. However, it's important to verify the credibility of the report creators, as some companies may use reports to promote their products. Additionally, the information can become outdated quickly, so it's essential to follow ongoing updates from sources like CVE (Common Vulnerabilities and Exposures).**