Syahira Azizah Rendra Putri

SIB – 4C / 18

2141762059

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.

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

Answer :

of all infections on PCs are found in %appdata%. Other common locations are %temp%, %cache%, and %windir%

Based on their findings, what are some trends in ransomware? Type your answers here.

Answer :

Ransomware is more often directed towards higher value and weaker targets. Threat actors are using reconnaissance to identify targets that are more likely to be vulnerable.

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

Answer :

The ability of a hacker to gain access to a person's email continues with an existing legitimate conversation with a malicious payload attached. The payload may evade any email filtering. The use of HTTPS on phishing sites has increased. Phishing attacks seem to follow the public news about a company or release of a new product (I-Phone). Impersonating new companies, including DocuSign and Steam, offers new challenges for digital document signing and automatic updates for games.

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

Answer :

Based on their findings, Android devices come pre-installed with between 100 to 400 apps that could be vulnerable. These apps are known to threat actors as commonly installed and, therefore, are likely targets.

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

Answer :

Webroot is a cybersecurity company that provides a range of security products and services for home and business.

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.

Briefly describe the malware.

Jawab :

Based on FIREEYE's findings, the two most common malware families in the healthcare industry are WITCHCOVEN (49%) and XtremeRAT (32%).

- WITCHCOVEN is used for reconnaissance, helping attackers map systems and networks.

- XtremeRAT is a remote access tool that allows attackers to control systems, manipulate files, and capture data.

Both are used to target healthcare organizations for sensitive data.

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.

Jawab :

SOGU is a backdoor can upload and download files and provide access the filesystem, registry, configuration, and remote shell among others. It uses a custom protocol to provide C2 graphical access to the system desktop.

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.

- China
- Russia
- Iran

- North korea

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

- Rusia

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.

Jawab :

- **Apple Security Updates:** Apple consistently releases security updates for its devices to address vulnerabilities in iOS, macOS, and other software. Notably, recent updates for iOS, iPadOS, and macOS (such as iOS 15.1 and macOS 12 Monterey) include critical security patches that address flaws potentially exploitable by attackers for unauthorized access or data breaches. Users should regularly update their Apple devices to benefit from the latest protections.
- **Adobe Security Updates:** Adobe routinely issues updates for its products to secure them against cyber threats. On recent dates, updates were rolled out for Photoshop, Acrobat, and Creative Cloud applications. These updates mitigate vulnerabilities that could allow remote code execution or unauthorized system access. Regularly updating Adobe software is crucial for avoiding potential exploitation.

Reflection Questions

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

Jawab :

- **Increased Exposure to Phishing and Social Engineering Attacks**
  With more users relying on emails, messages, and virtual collaboration tools, cybercriminals exploit this reliance by crafting phishing schemes and impersonation attempts to gain sensitive information.

- **Insufficient Home Network Security**
  Employees and students often connect from personal or unprotected networks, which may lack robust firewalls, intrusion detection systems, or encryption standards found in organizational networks, making them easier targets.

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

   Jawab :

   - **Backdoor**: ADDTEMP functions as a backdoor, allowing attackers remote access to the infected system. Through this, they can execute commands, steal data, and maintain persistence without the user's knowledge.
   - **Remote Access Trojan (RAT)**: It's often categorized as a Remote Access Trojan because it grants attackers remote control over the infected machine, enabling them to manipulate files, install other malware, and monitor user activity.

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

   Jawab :

   Several companies and organizations published annual cybersecurity reports in 2020. Notable examples include:

- **Cisco** released its "2020 Data Privacy Benchmark Study," which focused on data privacy and security concerns.
- **IBM** produced its "X-Force Threat Intelligence Index 2020," which analyzed various cyber threats and industry-specific risks.
- **Trend Micro** released "A Constant State of Flux," highlighting major attacks and vulnerabilities throughout 2020

  Trend Micro

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

   Jawab :

   In the 2021 cybersecurity landscape, the **most common exploit was phishing**. Phishing attacks increased significantly, often leveraging pandemic-related themes to deceive users into clicking malicious links or providing personal information. Other notable threats included ransomware, with variants like **Ryuk and Egregor** targeting critical infrastructure in sectors such as healthcare and finance

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

   Jawab :

These reports provide essential insights into evolving threats, vulnerabilities, and cybersecurity best practices, helping organizations to strengthen defenses and anticipate potential risks. However, it's important to:

- **Consider Vendor Bias**: Reports from security vendors may emphasize threats that align with the products or services they offer.
- **Verify Across Multiple Sources**: Comparing information across different reports can provide a more balanced view.
- **Focus on Relevance**: Some insights may be general; assess which trends apply specifically to your sector or organization for more actionable information.

These reports serve as valuable tools but should be used alongside other security intelligence to create a comprehensive understanding of cyber threats.