# Nama : Mochammad Aldo Rizky

# NIM : 2141762002

# Kelas : SIB 4C

# 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?

Malware typically hides in several key locations on a Windows PC, including:

1. %appdata% - 26.5% of all infections are found here.
2. %temp% - Temporary files can be a hiding place for malware.
3. %cache% - Cached files may also harbor malicious software.
4. %windir% - The Windows directory can contain infected system files.

**Answers will vary. 26.5% 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?

Some trends in ransomware include targeting higher value and weaker targets more frequently. Threat actors are increasingly using reconnaissance techniques to identify targets that are more likely to be vulnerable, allowing them to maximize the impact of their attacks. This shift in strategy emphasizes the importance of robust security measures for organizations.

**Answers will vary. 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?

Current trends in phishing attacks include:

1. Conversation Hijacking: Hackers often gain access to a person's email and respond within existing legitimate conversations, attaching a malicious payload that can evade email filtering.
2. Increased Use of HTTPS: Many phishing sites now use HTTPS, making them appear more legitimate and increasing the difficulty of detection.
3. Timely Targeting: Phishing attacks are often timed to coincide with public news events, such as the launch of new products (e.g., iPhones), making them more relevant and convincing.
4. Impersonation of Trusted Brands: Attackers frequently impersonate well-known companies like DocuSign and Steam, creating challenges for digital document signing and automatic game updates.

**Answers will vary. 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?

Android devices are often more susceptible to security issues for several reasons:

1. Pre-installed Apps: Many Android devices come with 100 to 400 pre-installed apps, some of which may have vulnerabilities. These apps are familiar to threat actors and can be prime targets for attacks.
2. Open Ecosystem: The Android platform allows for a wide range of apps from various sources, including third-party app stores. This openness increases the likelihood of malicious software being installed.
3. Fragmentation: The diverse range of Android devices and operating system versions leads to inconsistent security updates. Many users do not receive timely updates, leaving devices vulnerable.
4. User Behavior: Users may not practice safe browsing habits or may download apps without verifying their security, increasing the risk of exposure to threats.
5. Lack of Stringent App Review: The Google Play Store has a less rigorous app review process compared to other platforms, making it easier for malicious apps to be published..

**Answers will vary. 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.

**Webroot is a cybersecurity company founded in 1997 and headquartered in Colorado, USA. It specializes in cloud-based security solutions, including antivirus software, internet security, and endpoint protection. Webroot is known for its advanced threat intelligence and real-time protection, leveraging machine learning to detect and respond to cyber threats quickly. The company primarily serves both home users and businesses, offering solutions that protect against malware, phishing, and other online threats. Webroot's focus on lightweight, efficient products has made it popular among users looking for seamless security without sacrificing system performance. In 2019, Webroot was acquired by Carbonite, a data protection company, expanding its reach and capabilities in the cybersecurity space.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.

Based on the findings from the FireEye threat intelligence report for the healthcare and health insurance industry, the two most commonly used malware families identified are WITCHCOVEN and XtremeRAT.

WITCHCOVEN

WITCHCOVEN is a sophisticated malware family often utilized by threat actors to perform reconnaissance and maintain persistence within targeted systems. It is designed to footprint networks and gather sensitive information from compromised systems. Its capabilities may include stealing credentials, exfiltrating data, and facilitating further attacks by providing backdoor access to the attackers.

XtremeRAT

XtremeRAT is a remote access tool (RAT) that allows attackers to gain control over infected systems. It enables various malicious activities, such as uploading and downloading files, manipulating the Windows registry, controlling processes and services, and capturing sensitive data, including keystrokes and screenshots. This makes it particularly dangerous for the healthcare industry, where sensitive patient data is at risk.

Both malware families illustrate the growing threats to healthcare cybersecurity, emphasizing the need for robust protective measures in the sector..

**Answers should include using WITCHCOVEN at 49 % and XtremeRAT at 32 %. class=AnswerGray>Threat actors use it to footprint computer systems and organizations. XtremeRAT is remote access tool (RAT) that can upload and download files, interact with the Windows registry, manipulate processes and services, and capture 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.

Describe the malware.

Based on the findings from the FireEye threat intelligence report for the energy industry, the two most commonly used malware families identified are SOGU and ADDTEMP.

SOGU

SOGU is a backdoor malware family that is utilized by threat actors to gain unauthorized access to compromised systems. It allows attackers to upload and download files, access the filesystem, manipulate the Windows registry, and execute remote commands through a shell. SOGU employs a custom protocol to provide command-and-control (C2) functionality, offering graphical access to the system's desktop. This capability makes it particularly versatile for conducting further malicious activities within targeted environments.

ADDTEMP

ADDTEMP is another malware variant commonly used in the energy sector. It primarily functions as a remote access tool, enabling threat actors to establish persistent connections to infected systems. Its features typically include the ability to execute commands, manipulate files, and gather sensitive information. ADDTEMP is often leveraged in attacks targeting industrial control systems, posing significant risks to critical infrastructure.

Both malware families highlight the cybersecurity challenges faced by the energy industry, underscoring the need for effective defenses against advanced persistent threats.here.

**Answers will vary but should include SOGU at 41% and ADDTEMP at 20%. 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.

Identify the four accused Nation State Cyber Threats.

The four accused nation state cyber threat actors identified by the Cybersecurity and Infrastructure Security Agency (CISA) are:

China

Russia

North Korea

Iran

**Answers should include Nation State Cyber Threats actors from China, Russia, North Korea, and Iran.**

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

Advisory for Russia

One advisory issued regarding cyber threats from Russia focuses on the activities of advanced persistent threat (APT) groups, particularly APT28 (also known as Fancy Bear). This advisory highlights the group's targeting of political organizations, critical infrastructure, and elections.

CISA has warned that APT28 employs various tactics, techniques, and procedures (TTPs), including spear phishing campaigns and the exploitation of software vulnerabilities to gain initial access. The advisory emphasizes the importance of organizations implementing robust security measures, such as regular software updates, enhanced email filtering, and user training to recognize phishing attempts. Additionally, it recommends monitoring for indicators of compromise (IOCs) associated with APT28 to detect and respond to potential intrusions effectively.

This advisory reflects ongoing concerns about Russian cyber activities, especially in relation to election security and geopolitical tensions.

**Answers will vary. References for numerous threats are describe for the accused threat actor nation states.**

## 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.

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

Cybersecurity Updates

Apple

Timestamp: September 21, 2021

Description: An update was released for a series of Apple software products, including Safari, iOS 15, and watchOS. This update included important security patches addressing vulnerabilities that could potentially allow attackers to exploit the systems. Users were strongly advised to update their devices to ensure they had the latest protections against emerging threats.

Adobe

Timestamp: September 14, 2021

Description: Adobe released security updates for several of its products, including Photoshop Elements and Acrobat. These updates addressed critical vulnerabilities that could lead to unauthorized access and exploitation of user data. Users were recommended to apply these updates promptly to safeguard their systems from potential cyber threats.

These updates reflect the ongoing efforts by software companies to enhance security and protect users from evolving cyber threats..

**Answers will vary but should include the most current cyber threat information. For example, an update was released on September 21, 2021 on a series of Apple software products including Safer, iOS 15, and watchOS. It is recommended to update the products to include the most recent security patches. On September 14, 2021, Adobe released security updates for a number of their products including Photoshop Elements and Acrobat.**

## Reflection Questions

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

. Some cybersecurity challenges associated with schools and companies moving towards remote learning and working include:

Increased Phishing Attacks: With more reliance on email, messaging apps, and video conferencing, there has been a rise in phishing attempts targeting students and employees. Attackers often impersonate legitimate sources to steal credentials or deliver malware.

Unsecured Networks: Many individuals access educational and work resources from home networks that may lack robust security measures, making them vulnerable to attacks.

Device Security: Employees and students often use personal devices for remote access, which may not have the same security protections as corporate or institutional devices. This can lead to vulnerabilities in accessing sensitive information.

Video Conferencing Risks: The use of video conferencing tools has surged, but many platforms have faced security issues such as "Zoombombing," where unauthorized users disrupt meetings, and inadequate privacy settings that expose sensitive information.

Data Privacy Concerns: With increased online activities, there are greater risks related to data privacy, including unauthorized access to personal information and compliance with regulations like FERPA and GDPR.

Lack of Cybersecurity Training: Many students and employees may not have received adequate cybersecurity training, leading to poor security practices and increased susceptibility to attacks.

Cloud Security Issues: As organizations move data and applications to the cloud, they face challenges related to securing cloud environments and managing user access effectively.

**Answers will vary but may include additional phishing towards email, texting, and video conferencing.**

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

Two terms used to describe ADDTEMP malware are Desert Falcon and Arid Viper. This malware is typically delivered via spear phishing attacks, where targeted emails are crafted to trick recipients into downloading malicious attachments or clicking on harmful links. These tactics exploit social engineering techniques to increase the likelihood of successful infection..

**Answers should include that ADDTEMP malware, aka Desert Falcon and Arid Viper, may be delivered via Spear Phishing.**

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

Several companies and organizations released annual cybersecurity reports for 2020, including:

Cisco - Known for its annual Cybersecurity Report, which analyzes trends and threats in the cybersecurity landscape.

Trend Micro - Released their annual Cybersecurity Threat Report, detailing the evolving threat landscape and the impacts of various cyber threats.

Check Point - Provided their annual Cyber Security Report, focusing on trends, attack vectors, and key findings from the previous year.

Verizon - Known for the Data Breach Investigations Report (DBIR), which compiles data on breaches and incidents across various industries.

IBM - Offered their X-Force Threat Intelligence Index, which examines security incidents and highlights emerging threats.

McAfee - Released their Threats Report, providing insights into malware and cyber threat trends.

**Answers will vary. Cisco, TrendMicro, and Check Point offer these reports, as do many other companies and organizations.**

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

   For the 2021 Verizon Data Breach Investigations Report (DBIR), the most common type of exploit identified was social engineering, particularly phishing attacks. This report highlighted how attackers often used deceptive tactics to manipulate individuals into providing sensitive information or credentials, underscoring the importance of employee training and awareness in mitigating these risks. Social engineering remained a prominent method for breaching security across various sectors..

**Answers will vary.**

6. 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 valuable because they offer insights into emerging threats, vulnerabilities, and attack trends, helping cybersecurity professionals to stay informed and enhance their defenses. They can also provide benchmarks for evaluating an organization's security posture compared to industry standards.

However, when accepting the information presented in these reports, it's important to consider:

Source Credibility: Evaluate the organization that produced the report. Some companies may have biases or agendas, such as promoting their products or services, which can influence the data or interpretations presented.

Data Relevance and Timeliness: Reports can become outdated quickly as new threats emerge. It's crucial to cross-reference findings with more current sources, such as the Common Vulnerabilities and Exposures (CVE) database or recent threat intelligence updates.

Context and Scope: Understand the context in which the data was collected. Reports may focus on specific industries or regions, which may not be applicable to all organizations.

Methodology: Scrutinize the methodology used to gather and analyze the data. A lack of transparency in how the data was collected can lead to misinterpretations.

**The reports are very valuable because they provide information that helps cybersecurity professionals to know about emerging threats. It is important to evaluate the reports based on who created them. Some are created by companies that may be trying to sell their products through the reports. In addition, the reports are old. New threats are constantly immerging, so it is important to follow more up-to-date sources of information, such as the CVE.**