Name : Selly Amelia Putri (2141762142)

Class : SIB 4C (16)

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?

%appdata% - Around 26.5% of all malware infections are found in this location.

%temp% - This is another common location where malware hides.

%cache% - The cache folder is also often used by malware to hide itself.

%windir% - The Windows directory is also a common hiding place for malware.

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?

Based on the findings of the 2020 Webroot Threat Report, key trends in ransomware include:

1. More targeted attacks on high-value and more vulnerable targets.

2. Threat actors are using reconnaissance techniques to identify targets that are more likely to be vulnerable.

3. While the number of attacks is decreasing, their impact is becoming more dangerous.

Ransomware implementations are becoming more sophisticated.

4. Focus on specific sectors such as transportation, healthcare, education, and SMEs.

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?

Based on findings in recent reports, some of the current trends in phishing attacks include:

1. Increased use of AI and machine learning to create more convincing and personalized phishing content.

2. The rise of highly realistic audio and video phishing deepfakes.

3. Leveraging social media platforms to impersonate and distribute phishing content.

4. Increased use of smishing (SMS phishing) attacks targeting mobile devices.

5. Use of QR codes in emails and documents to hide malicious links ("quishing").

6. More targeted and sophisticated phishing attacks, such as spear phishing.

7. Increased use of vishing (voice phishing) attacks that combine email and phone calls.

8. Exploitation of cloud services and communication apps like Microsoft Teams to distribute phishing.

9. Leverage of Phishing-as-a-Service (PhaaS) that makes it easier to launch phishing campaigns.

10. Attacks that follow public news trends or new product launches to increase credibility.

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?

Based on findings in the Webroot Threat Report 2020, Android is more vulnerable to security issues for several reasons:

1. Android devices come with 100-400 pre-installed apps, which are potentially vulnerabilities.

2. These pre-installed apps are known to threat actors as commonly installed apps, making them attractive targets for attack.

3. Trojans and malware accounted for 91.8% of threats on Android, indicating a high prevalence of malware targeting this platform.

4. Android's open-source nature makes it easier for attackers to find and exploit vulnerabilities.

5. The fragmentation of the Android ecosystem, with many different versions and devices, makes it more difficult to distribute security updates evenly.

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 that provides a range of security products and services for homes and businesses. Some key points about Webroot:

1. Founded in 1997 in Boulder, Colorado, USA.

2. It is the largest privately held cybersecurity company based in the US, operating globally in North America, EMEA, and APAC.

3. In 2019, Webroot and its parent company Carbonite were acquired by OpenText, a global leader in Enterprise Information Management.

4. Webroot is a pioneer in leveraging the cloud and artificial intelligence to stop zero-day threats in real-time.

5. Their core products include endpoint protection, network protection, and security awareness training solutions.

6. Webroot uses a cloud-based platform with advanced machine learning to analyze and protect against cyberthreats.

7. The company has made several strategic acquisitions to strengthen their cybersecurity capabilities, including BrightCloud and Prevx.

8. Webroot provides threat intelligence services used by leading companies such as Cisco, F5 Networks, and Citrix.

Overall, Webroot is a key player in the cybersecurity industry that focuses on innovation and cloud-based protection for a wide range of users.

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.

According to FireEye's findings, the two most common malware families used by threat actors targeting the healthcare and health insurance industries are WITCHCOVEN and XtremeRAT.

WITCHCOVEN

WITCHCOVEN is used by 49% of threat actors in the industry. This malware is a profiling script used to gather detailed information about target systems. The actors modify certain websites to direct visitors to the WITCHCOVEN script, which then footprints the target computer system and organization.

XtremeRAT

XtremeRAT is used by 32% of threat actors. This is a Remote Access Trojan (RAT) that has a variety of malicious capabilities:

1. Uploading and downloading files from an infected system
2. Interacting with the Windows registry
3. Manipulating processes and services running on the system
4. Capturing screenshots of the victim's computer
5. Recording audio and video via microphone or webcam
6. Keylogging

XtremeRAT has been used in attacks on financial institutions, telecommunications companies, gaming companies, the IT sector, and the energy and utilities sector. This malware was also used in attacks on the Israeli and Syrian governments in 2012.

Both of these malware pose a serious threat to the healthcare and health insurance industries, as they can be used to steal sensitive data and disrupt system operations.

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 FireEye's findings for the energy industry, the two most common malware families used by threat actors are SOGU and ADDTEMP.

SOGU

SOGU is a backdoor used by 41% of threat actors in the energy industry. This malware has quite sophisticated capabilities, including:

1. Uploading and downloading files
2. Accessing the file system
3. Manipulating the Windows registry
4. Changing system configurations
5. Providing remote shell access

What makes SOGU special is its use of a custom protocol to provide graphical control and control (C2) access to the infected system's desktop. This allows attackers to interact with the target system as if they were physically sitting in front of it.

ADDTEMP

ADDTEMP is used by 20% of threat actors in the energy industry. While more detailed information is limited compared to SOGU, ADDTEMP is also a dangerous malware designed to provide unauthorized access to target systems.

These two malwares demonstrate that threat actors targeting the energy industry are using sophisticated and effective tools to gain and maintain access to critical systems. This emphasizes the importance of strong cybersecurity in the energy sector, given the potentially significant impact of disruptions to energy infrastructure.

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.

Based on information available on the CISA website, the four identified Nation State Cyber Threats are:

1. China (People's Republic of China)

2. Russia

3. North Korea

4. Iran

These four nations are considered the primary sources of nation state cyber threats to the United States and its critical infrastructure. CISA provides specific information and guidance to help U.S. organizations and critical infrastructure protect themselves from state-sponsored cyber activity.

Each of these nations has different characteristics and objectives for cyber attacks, but all are considered serious threats to U.S. national cybersecurity. CISA works with a variety of government and private sector partners to monitor, analyze, and provide guidance on threats from these four nation state actors.

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.

One notable advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA) concerns Iranian-based cyber actors. The advisory is titled **“Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations.”**

Description of the Advisory :

This joint advisory, released by CISA, the FBI, and the Department of Defense Cyber Crime Center (DC3), aims to alert network defenders about ongoing threats from a group of Iranian cyber actors known as Pioneer Kitten, Parisite, Rubidium , and Lemon Sandstorm. These groups have been actively targeting U.S. organizations across various sectors, including education, finance, healthcare, and defense, as well as local government entities.

The advisory highlights that these Iranian cyber actors are not only involved in ransomware attacks but also engage in computer network exploitation (CNE) activities to support the Iranian government's objectives. The advisory emphasizes the need for organizations to review and implement specific mitigations to reduce the likelihood and impact of ransomware incidents.

CISA encourages critical infrastructure organizations to take proactive measures in response to this advisory, which includes reviewing their cybersecurity posture and ensuring robust defenses against such threats. The timing of this advisory aligns with ongoing research and reports on Iranian cyber threats, underscoring the importance of vigilance in cybersecurity practices.

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.

1. Adobe Photoshop Elements

- Timestamp: September 14, 2021

- Update: Adobe has released a security update for Photoshop Elements. This update resolves a critical vulnerability that could lead to arbitrary code execution in the context of the current user. This vulnerability could be exploited if an attacker successfully gains access to an infected system.

2. Adobe Acrobat

- Timestamp: September 14, 2021

- Update: Adobe has also released a security update for Acrobat. This update resolves a vulnerability that could lead to arbitrary code execution in the context of the current user. This vulnerability could be exploited if an attacker successfully gains access to an infected system.

Both of these updates are critical to download and install to avoid vulnerabilities that could be exploited by an attacker.

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?

The shift towards remote learning and working has introduced several cybersecurity challenges for both schools and companies. Here are some of the key issues:

1. Increased Phishing Attacks: - With the rise of remote communication tools such as email, texting, and video conferencing, there has been a notable increase in phishing attempts. Cybercriminals exploit the vulnerabilities of remote work by sending deceptive emails or messages that impersonate trusted sources to obtain sensitive information from users.

2. Malware and Ransomware Threats: - Schools and organizations have become prime targets for malware and ransomware attacks. Cyber actors are increasingly deploying ransomware to encrypt data and demand payment for its release. This not only disrupts educational activities but also threatens the confidentiality of sensitive data, including student records.

3. Unsecured Networks: - Many students and employees access online platforms from home or public networks that lack robust security measures. This exposes their devices to potential cyber threats, making it easier for attackers to infiltrate systems.

4. Disruption of Online Learning Environments: - Uninvited users have disrupted virtual classrooms by harassing students or displaying inappropriate content during live sessions. This not only affects the learning experience but also raises concerns about safety and privacy in online educational settings.

5. Data Privacy Concerns: - The transition to online learning involves collecting and storing vast amounts of personal data, which makes educational platforms attractive targets for hackers. Data breaches can lead to identity theft and financial fraud, impacting both students and institutions.

6. Cyberbullying and Mental Health Risks: - The lack of supervision in remote settings can lead to increased incidents of cyberbullying among students. Additionally, without adequate monitoring, signs of self-harm or distress may go unnoticed, posing risks to students' mental health.

7. Endpoint Security Vulnerabilities: - With employees using personal devices for work, ensuring endpoint security has become crucial. Devices that are not thoroughly protected can serve as entry points for cyber threats.

8. Trust Erosion: - Frequent security breaches can erode trust in remote learning platforms among students, parents, and educators. Maintaining a secure environment is essential for fostering confidence in these systems.

These challenges highlight the need for robust cybersecurity measures tailored to the unique risks associated with remote learning and working environments. Organizations must prioritize training, implement strong security protocols, and continuously monitor their systems to mitigate these threats 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. It may be delivered via Spear Phishing attacks, where targeted emails containing malicious attachments or links are sent to victims to infect their systems.

   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?

   Companies and organizations that created annual cybersecurity reports for 2020 include:

   - Cisco
   - TrendMicro
   - Check Point
   - Symantec
   - Palo Alto Networks
   - IBM Security
   - Kaspersky
   - McAfee
   - FireEye
   - Verizon (Data Breach Investigations Report)

   Many of these organizations regularly publish detailed reports on the evolving cyber threat landscape.

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

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

   A cybersecurity report from 2021 indicates that the most common type of exploit that year was ransomware attacks. Ransomware surged globally as cybercriminals increasingly targeted organizations to encrypt their data and demand payment for its release. Other significant exploits included phishing and vulnerabilities in remote access tools due to the rise of remote work during the COVID-19 pandemic.

   Answers will vary.

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

   The reports are very valuable because they provide crucial insights that help cybersecurity professionals stay informed about emerging threats, attack patterns, and vulnerabilities. However, it's important to evaluate these reports critically, considering:

   1. Bias: Some reports are produced by companies with vested interests, potentially promoting their products or services.
   2. Relevance: Reports can quickly become outdated, as new threats emerge constantly. It's important to consult more up-to-date sources, such as the CVE (Common Vulnerabilities and Exposures) database, to stay current.

   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.