Nama : Yusufa Haidar

Kelas : SIB – 4C

No : 21

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?

According to the findings in the 2020 Webroot Threat Report, malware on Windows PCs typically hides in four main locations: %temp%, %appdata%, %cache%, and %windir%. Specifically, 26.5% of infections are found in the %appdata% folder, while more than half of the threats (54.4%) affecting business PCs are located in the %temp% folder.

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?

According to the findings in the 2020 Webroot Threat Report, several significant trends were observed in ransomware attacks:

1. **Increased Frequency of Ransomware Attacks**: Ransomware infections continued to rise, particularly targeting small and medium-sized businesses (SMBs). Attackers preferred these smaller organizations due to their limited resources to defend against and recover from attacks, making them more likely to pay the ransom.
2. **Larger Ransom Demands**: The financial demands from ransomware attacks escalated, with average ransom payments more than doubling between 2019 and 2020. Attackers leveraged this for substantial financial gain, demanding sums that smaller businesses found increasingly difficult to manage.
3. **Advanced Ransomware Techniques**: Attackers deployed more sophisticated methods to evade detection and penetrate defenses, such as using social engineering tactics and exploiting system vulnerabilities. The ability of ransomware to avoid traditional detection mechanisms posed a growing challenge.
4. **Geographically Diverse Targets**: Ransomware attacks were observed across a variety of regions and industries, with sectors like manufacturing, public administration, and healthcare particularly vulnerable to infection

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?

The 2020 Webroot Threat Report highlights several significant trends in phishing attacks. The report found a 640% increase in phishing attempts in 2019, with one in four malicious URLs hosted on otherwise non-malicious domains. Notably, cybercriminals commonly impersonated major brands like Facebook, Microsoft, Apple, Google, PayPal, and Dropbox in their phishing campaigns.

Phishing attackers also targeted specific types of websites, with cryptocurrency exchanges (55%), gaming platforms (50%), web email services (40%), financial institutions (40%), and payment services (32%) being among the most impersonated. These trends demonstrate that phishing continues to evolve, with attackers focusing on exploiting popular services and platforms to deceive users and steal credentials

Answers will vary. The ability of a hacker to gain access to a personâ€™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?

According to the 2020 Webroot Threat Report, Android devices are more susceptible to security issues for several reasons:

1. **Open Ecosystem**: Android’s open-source nature allows users to download apps from various third-party sources, which increases the risk of downloading malicious software compared to platforms like iOS, which have stricter app store policies.
2. **Trojans and Malware**: The report indicates that Trojans and other malware accounted for 91.8% of Android threats, highlighting that malicious apps are a primary vector for infections on these devices(

3. **Inconsistent Updates**: Many Android devices do not receive timely security patches, especially those running older versions of the operating system. This delay leaves vulnerabilities unpatched for extended periods, making it easier for attackers to exploit security flaws.
4. **Device Fragmentation**: The large number of different Android devices, each with varying hardware and software configurations, complicates the rollout of security updates, leading to many unprotected devices remaining in use.

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.

The 2020 Webroot Threat Report was created by **Webroot**, a cybersecurity company that focuses on providing protection against internet-based threats. Founded in 1997 and headquartered in Broomfield, Colorado, Webroot is best known for its cloud-based threat intelligence services and endpoint protection solutions.

Key points about Webroot:

1. **Cloud-Based Security Solutions**: Webroot offers services like endpoint protection, network security, and threat intelligence, which leverage cloud-based architecture. This allows the company to provide real-time protection against malware, phishing, ransomware, and other threats.
2. **Acquisition by OpenText**: In 2019, Webroot was acquired by **OpenText**, a Canadian enterprise information management company. This acquisition strengthened OpenText's cybersecurity portfolio by integrating Webroot's threat intelligence into its wider enterprise solutions.
3. **Machine Learning and Automation**: Webroot utilizes advanced machine learning algorithms to analyze vast amounts of threat data. By collecting and analyzing information from billions of URLs, domains, IP addresses, and files, Webroot helps detect and prevent cyberattacks.
4. **Consumer and Business Focus**: Webroot caters to both consumers and businesses, providing solutions for personal devices as well as more complex systems for small and medium-sized enterprises (SMEs). It is particularly well-regarded for its user-friendly antivirus software for personal use.

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 FireEye's findings for the healthcare and health insurance industry, two of the most commonly used malware families by threat actors are **WITCHCOVEN** and **XtremeRAT**.

1. **WITCHCOVEN** (used in 49% of attacks) is primarily employed by threat actors to footprint computer systems and organizations, gathering information about the environment for further malicious actions.
2. **XtremeRAT** (used in 32% of attacks) is a Remote Access Tool (RAT) that allows attackers to remotely control infected systems. It can perform a variety of actions, including uploading and downloading files, interacting with the Windows registry, managing processes, and even capturing sensitive data.

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 recent FireEye findings and other sources, two commonly used malware families targeting the energy sector are *PIPEDREAM* and *Black Basta*.

1. **PIPEDREAM**: This highly advanced malware is designed to target industrial control systems (ICS) and operational technology (OT) networks, particularly in the energy industry. It can infiltrate Schneider Electric and Omron controllers, taking advantage of their native functionality, which makes it difficult to detect. PIPEDREAM is modular, allowing it to conduct reconnaissance, upload malicious configurations, and modify device parameters to cause disruption. It is believed to have been developed by a state actor with the intent to disrupt critical energy infrastructure
2. **Black Basta**: This ransomware group has emerged as a key player in attacks on the energy sector. Believed to be a splinter group of the defunct Conti ransomware syndicate, Black Basta specializes in "big game hunting," targeting large corporations and critical infrastructure. Their tactics include stealing sensitive data before encrypting systems to demand ransoms. The group has evolved over time, releasing updated versions of their ransomware to increase effectiveness

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 main accused Nation State Cyber Threats identified by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) are:

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

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 CISA regarding **Russia** is **Advisory AA22-011A**, titled *"Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure."* This advisory, released jointly by CISA, the FBI, and the National Security Agency (NSA), warns of increased Russian state-sponsored cyber activities targeting U.S. critical infrastructure sectors. These activities are believed to be part of broader geopolitical strategies.

The advisory highlights the use of **advanced persistent threat (APT)** tactics, such as spear-phishing, exploiting known vulnerabilities, and leveraging sophisticated malware like *Triton* or *NotPetya*. It emphasizes the need for organizations to implement strong security practices, including patch management, multi-factor authentication, and network segmentation to mitigate risks.

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.

a. Cisco IOS and IOS XE Software Updates:

- **Company Name**: Cisco
- **Timestamp**: September 26, 2024
- **Update Description**: Cisco released a Semiannual Security Advisory that addresses multiple vulnerabilities in IOS and IOS XE software. These vulnerabilities could potentially be exploited by cyber threat actors to take control of affected systems. Users and administrators are encouraged to review and apply the necessary updates detailed in the advisory.

b. Cisco Webex Updates:

- **Company Name**: Cisco
- **Timestamp**: September 24, 2024
- **Update Description**: Cisco also announced updates for Webex products to fix various vulnerabilities, enhancing the overall security and stability of the platform. Specific details about the vulnerabilities and their impact are outlined in the advisory.

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?

   a) Increased Attack Surface

   b) Unsecured Networks

   c) Phishing and Social Engineering

   d) Device Security

   e) Data Loss Prevention

   f) Compliance Challenges

   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?

   ADDTEMP malware is commonly referred to by two terms: **Sogu** and **PlugX**. These terms describe a modular remote access tool (RAT) that has been widely utilized for espionage, particularly by Chinese threat actors. ADDTEMP is characterized by its sophisticated capabilities, including encrypted communication, rootkit technology, and anti-analysis features that help it avoid detection by conventional security measures

   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?

   a) Verizon

   b) Cisco

   c) TrendMicro

   d) ENISA

   e) IBM

   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?

   For the year 2021, one of the most notable exploits was the **Apache Log4j vulnerability**, also known as **Log4Shell** (CVE-2021-44228). This critical vulnerability was revealed in December 2021 and posed a significant risk as it allowed attackers to execute arbitrary code remotely on affected systems. The severity of this vulnerability earned it a CVSS score of 10, indicating a critical level of risk. It was particularly dangerous because the Log4j library is widely used across many applications and services globally, making it a prime target for exploitation

   Another significant exploit that year was the **Microsoft Exchange vulnerabilities** known as **ProxyLogon**, which involved a chain of vulnerabilities (CVE-2021-26857, CVE-2021-26855, CVE-2021-26858, and CVE-2021-27065). These allowed attackers to bypass authentication and gain administrative privileges on Exchange servers, which led to the widespread deployment of web shells for further malicious activities

   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?

   Reasons on why is it valuable :

   a) Insight into Threat Landscape

   b) Trend Analysis

   c) Benchmarking

   d) Awareness and Education

   Points to consider when accepting the findings :

   a) Bias and Motivation

   b) Data Sources

   c) Context

   d) Temporal Relevance

   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.