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:

Malware typically hides in the following locations on a Windows PC:

- 26.5% of all infections are found in %appdata%.
- Other common locations include %temp%, %cache%, and %windir%.

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

Answer:

- Ransomware is increasingly targeting higher-value, vulnerable entities.
- Cybercriminals conduct reconnaissance to identify targets more likely to pay.
- There is a rise in "double extortion" tactics, where attackers steal sensitive data in addition to encrypting it, threatening to leak the data unless a ransom is paid.

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

Answer:

- Attackers continue to infiltrate email chains by hijacking ongoing, legitimate conversations and attaching malicious payloads that can bypass traditional email filters.
- The use of HTTPS on phishing websites has increased, making phishing attacks harder to detect.
- Phishing campaigns often mirror high-profile events, such as the launch of new products like the iPhone, to make their attacks more convincing.
- Impersonating companies such as DocuSign and Steam for digital document signing and software updates is a growing challenge.

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

Answer:

- Android devices often come pre-installed with a large number of apps (between 100 to 400), which increases the attack surface.
- These pre-installed apps are known by threat actors, making them common targets for exploitation.
- Android's fragmented ecosystem and delayed security updates contribute to the platform's vulnerability.

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

Answer:

Webroot is a cybersecurity company that specializes in providing protection against malware, phishing, and other cyber threats. The company offers solutions such as endpoint protection, network threat detection, and cybersecurity intelligence services to both individuals and businesses. Webroot leverages machine learning and cloud-based intelligence to deliver real-time protection and threat insights.

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.

Answer:

Healthcare and Health Insurance Industry

Based on FIREEYE's findings, the two most commonly used malware families by threat actors in the healthcare and health insurance industry are:

1. WITCHCOVEN (49%)

   WITCHCOVEN is used to footprint and map computer systems within organizations. It helps threat actors understand the network structure and gather information about vulnerabilities to launch further attacks.

2. XtremeRAT (32%)

   XtremeRAT is a Remote Access Tool (RAT) that provides an attacker with full control over the infected system. It can upload and download files, manipulate the Windows registry, interact with processes and services, and capture sensitive data from the machine. It is often used in targeted attacks to exfiltrate data or maintain long-term access.

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.

Answer:

Energy Industry

Based on FIREEYE's findings, the two most commonly used malware families by threat actors in the energy industry are:

1. SOGU (41%)

   SOGU is a backdoor that provides attackers with remote access to the infected system. It allows the uploading and downloading of files, interaction with the system's filesystem and registry, and access to a remote shell. It uses a custom protocol to enable command-and-control (C2) communication, including graphical access to the system's desktop.

2. ADDTEMP (20%)

   ADDTEMP is a type of malware that allows attackers to execute remote commands, manipulate files, and gain control over the target system. It is commonly used to maintain persistence on a compromised network and facilitate additional malicious activity, such as lateral movement or data exfiltration.

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.

Answer:

The four accused Nation State Cyber Threats identified by CISA are:

- China
- Russia
- North Korea
- Iran

Selected Nation State: Russia

One advisory related to Russia:

- Advisory Title: "Russian State-Sponsored Cyber Actors Exploit Vulnerabilities to Target U.S. Critical Infrastructure"
- Description: This advisory provides information on Russian state-sponsored cyber actors exploiting known vulnerabilities in systems related to U.S. critical infrastructure. It emphasizes the need for organizations to update software and systems to prevent exploitation and highlights specific vulnerabilities used by Russian actors, such as those in VPN systems, to access and disrupt critical operations.

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

Answer:

Two cybersecurity updates regarding software products:

1. Software Company: Apple

   Timestamp: September 21, 2021

   Description: This update focuses on several Apple software products, including iOS 15, iPadOS 15, and watchOS 8. The advisory recommends that users update to the latest versions to address multiple security vulnerabilities that could allow unauthorized access or the execution of arbitrary code. The security patches included in these updates mitigate several critical flaws in Apple's ecosystem.

2. Software Company: Adobe

   Timestamp: September 14, 2021

   Description: Adobe released security updates for a wide range of products, including Photoshop Elements and Acrobat. These updates addressed multiple vulnerabilities that could allow an attacker to take control of an affected system. Users were urged to install the updates immediately to protect against potential exploits of these vulnerabilities.

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.

Answer:

1. Cisco IOS XE Web UI Vulnerabilities
    - Software Company: Cisco
    - Timestamp: January 17, 2023
    - Update Description: This advisory addresses critical vulnerabilities found in Cisco's IOS XE software, which allows unauthorized remote access via the web interface. The issue impacts the security of routers and network infrastructure running the software. Cisco released patches to mitigate these risks and prevent exploitation.
2. Apple macOS, iOS, and watchOS Security Updates
    - Software Company: Apple
    - Timestamp: September 12, 2023
    - Update Description: Apple released security updates for multiple products, including macOS, iOS, and watchOS. These patches address several critical vulnerabilities that could allow arbitrary code execution. Users are advised to update to the latest versions to ensure protection from potential exploits.

Reflection Questions

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

    Answer:

    Schools and companies face increased cybersecurity risks due to the widespread use of personal devices and unsecured networks. Phishing attacks, especially through email and video conferencing tools, have risen significantly. Additionally, the lack of physical security and control over the devices and networks used for remote access makes it easier for cybercriminals to exploit vulnerabilities.

    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?

    Answer:

    ADDTEMP malware, also known as **Desert Falcon** or **Arid Viper**, is commonly delivered through **spear phishing** emails. These emails trick users into clicking malicious links or downloading infected attachments, enabling the malware to infiltrate the system.

    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?

   Answer:

   Several companies and organizations produced cybersecurity reports for 2020, including:

   - Cisco: Annual cybersecurity report focused on network threats.
   - TrendMicro: Provided insights into malware trends and ransomware.
   - Check Point: Issued a report on global cybersecurity threats and vulnerabilities.

   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?

   Answer:

   In 2019, **phishing** and **ransomware** were among the most common exploits, according to reports from cybersecurity firms like Verizon and Symantec. Phishing attacks were often used as a vector for delivering malware or stealing credentials.

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

   Answer:

   Cybersecurity reports are valuable because they provide a comprehensive view of emerging threats and help organizations strengthen their security posture. However, it is important to critically evaluate these reports, considering that some may be biased due to the commercial interests of the companies producing them. Furthermore, as new threats constantly emerge, relying solely on past reports can leave an organization vulnerable. Staying up-to-date with current threat intelligence, such as CVE databases, is crucial.

   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.