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.

Questions:

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

Type your answers here.

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?

Type your answers here.

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?

Type your answers here.

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?

Type your answers here.

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.

Type your answers here.

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.

Question:

Briefly describe the malware.

Type your answers here.

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.

Question:

Describe the malware.

Type your answers 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.

Questions:

Identify the four accused Nation State Cyber Threats.

Type your answers here.

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.

Type your answers here.

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.

Question:

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

Type your answers here.

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?

   Type your answers here.

   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?

   Type your answers here.

   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?

   Type your answers here.

   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?

   Type your answers here.

   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?

   Type your answers here.

   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.

End of document