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

****TASK 1****

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.

****QUESTION 1****

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

****ANSWER****

85 percent of threats hide in one of four locations: %temp%, %appdata%, %cache%, and %windir%, with more than half of threats (54.4%) on business PCs hiding in %temp% folders. This risk can be easily mitigated by setting a Windows policy to disallow programs from running from the temp directory.

QUESTION 2

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

ANSWER

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.

QUESTION 3

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

ANSWER

One of the trends is evolution of phishing known as 'hijacked email reply chains'. A hacker gains access to a person's email and takes over a legitimate conversation, then forwards it to one of that person's friends or colleagues with a malicious payload attached. The email is likely to get through any email filtering, and the recipient is likely to open it, since the conversation details are convincing— because they are real. However, opening the file could result in infection with Emotet or another banking Trojan, such as Ursnif/Gozi

Also, there is biggest difference in phishing than before as it's increasing number of HTTPS phishing sites.

QUESTION 4

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

ANSWER

Since the average Android device comes with between 100 and 400 apps pre-installed, the potential for security holes remains high. These apps are known to threat actors as commonly installed and, therefore, are likely targets.

QUESTION 5

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

ANSWER

Webroot, an OpenText company, was the first to harness the cloud and artificial intelligence to stop zero-day threats in real time. Webroot secures businesses and individuals worldwide with threat intelligence and protection for endpoints and networks. It provides a range of security products and services for home and business.

TASK 2

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.

QUESTION 1

Based on the FIREEYE findings identify the two most commonly used malware families by threat actors for this industry.

Briefly describe the malware.

ANSWER

1. Ryuk

- **Type:** Ransomware
- **Description:** Originally deployed via phishing or remote access tools, Ryuk encrypts critical systems and demands ransom for decryption. Frequently used in targeted attacks against hospitals and health insurers.

2. Cobalt Strike

- **Type:** Post-exploitation toolkit
- **Description:** A legitimate penetration-testing tool repurposed by threat actors for credential theft, lateral movement, and deployment of additional payloads. Its modular framework makes it a favorite for stealthy persistence.

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 2

Describe the malware.

ANSWER

1. Triton (Trisis)

- **Type:** Industrial control systems (ICS) malware

- **Description:** Designed to specifically target and disable Schneider Electric Triconex safety instrumented systems—capable of triggering shutdowns, safety failures, or even physical disasters

2. Havex

- **Type:** Remote Access Trojan (RAT)
- **Description:** Associated with Russia's "Energetic Bear" group, Havex infiltrates energy and industrial networks via watering-hole attacks and injects payloads like Karagany for espionage, credential theft, and command execution

****TASK 3****

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.

****QUESTION 1****

Identify the four accused Nation State Cyber Threats.

****ANSWER****

- China Threat Overview and Advisories
- Iran Threat Overview and Advisories
- North Korea Threat Overview and Advisories
- Russia Threat Overview and Advisories

****QUESTION 2****

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

****ANSWER****

CISA, the National Security Agency (NSA), and Federal Bureau of Investigation (FBI) have confirmed that the PRC state-sponsored cyber actors known as Volt Typhoon have compromised the IT environments of multiple critical infrastructure organizations.

CISA, NSA, and FBI assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to operational technology assets to disrupt functions.

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 3****

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

****ANSWER****

Wing FTP Server

- **Timestamp:** July 14, 2025
- **Issue:** CVE-2025-47812 — improper neutralization of null byte vulnerability
- **Update Summary:** A flaw in Wing FTP Server allows attackers to inject arbitrary Lua code into user session files, potentially enabling execution of system commands with ROOT or SYSTEM privileges. Organizations are advised to follow vendor guidance to mitigate or disable the product if patches are unavailable

Citrix NetScaler ADC & Gateway

- **Timestamp:** July 10, 2025
- **Issue:** CVE-2025-5777 — out-of-bounds read vulnerability
- **Update Summary:** An input validation flaw affecting NetScaler Gateway (used for VPN/RDP) exposes the system to memory over-read attacks. CISA recommends applying vendor-supplied patches or discontinuing use where mitigations are not feasible

TASK 4

Reflection Questions

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

   ANSWER

- Increased phishing attacks
- Unsecured home networks
- Lack of endpoint security
- Use of personal (unpatched) device

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

   ANSWER

   ADDTEMP malware, also known as "fileless malware" or "in-memory malware", is a type of malicious software that doesn't rely on creating or modifying files on a system to execute its malicious actions. Instead, it operates directly within the computer's memory, making it harder to detect and remove using traditional antivirus or anti-malware solutions.

   It can be delivered through spear phishing.

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

   ANSWER

- Cisco (Annual Cybersecurity Report)
- IBM (X-Force Threat Intelligence Index)
- TrendMicro
- FireEye/Mandiant Threat Reports

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

   ANSWER

   Phishing and credential theft were the most common attack vectors (Verizon DBIR 2021)

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

   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.