Nama : Moh. Samsul HadiKelas :
SIB-4C
No : 06
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 :

26.5% of all infections on PCs are found in the %appdata% directory. Other common locations include %temp%, %cache%, and %windir%, where malware can hide to avoid detection.

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

Ransomware attacks are increasingly aimed at high-value and more vulnerable targets. Attackers are conducting reconnaissance to identify and exploit weaknesses, focusing on organizations that may lack strong security measures.

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

Phishing tactics have evolved to exploit ongoing email conversations by embedding malicious payloads that can evade email filters. Additionally, the use of HTTPS on phishing sites has risen, making attacks appear more legitimate. Attackers often target trending topics or recent product releases, such as new devices or services (e.g., iPhone, DocuSign, and Steam updates).

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

Android devices often come pre-installed with 100 to 400 apps, many of which have known vulnerabilities. Because these apps are commonly found on Android devices, they are familiar targets for attackers.

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

Webroot is a cybersecurity company that offers security products and services for both personal and business use. Their focus is on providing protection against various digital threats through advanced security solutions.

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.

WITCHCOVEN (49% prevalence): Threat actors use WITCHCOVEN to conduct reconnaissance on computer systems and organizations, allowing them to map out system infrastructure and identify potential weaknesses.

XtremeRAT (32% prevalence): XtremeRAT is a remote access tool (RAT) that enables attackers to upload and download files, interact with the Windows registry, manipulate processes and services, and capture sensitive data. It allows full access to and control over compromised systems.

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.

SOGU (41% prevalence): SOGU is a backdoor malware that grants attackers remote access to a compromised system, enabling them to upload and download files, access the filesystem, registry, and configuration, and even run a remote shell. It communicates with command-and-control (C2) servers using a custom protocol that allows graphical access to the system's desktop.

ADDTEMP (20% prevalence): ADDTEMP allows attackers to create temporary files and manipulate system functions for further exploitation. It enables persistent access and can manipulate system resources for various malicious purposes, including exfiltrating data or executing commands remotely.

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 accused Nation State Cyber Threat actors include **China**, **Russia**, **North Korea**, and **Iran**.

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

Example Advisory for China: One advisory issued for China details cyber activities aimed at targeting the U.S. critical infrastructure sectors. The advisory warns of sophisticated malware campaigns used to compromise telecommunications and financial organizations. This advisory emphasizes the importance of maintaining robust security practices and applying patches to minimize 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.

Software Company: Apple

Timestamp: September 21, 2021

Description: Apple issued updates for iOS 15, iPadOS, watchOS, and macOS to address multiple security vulnerabilities. The update includes essential patches to improve security in various Apple products and protect users from potential exploitation.

Reflection Questions

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

   With the shift to remote learning and working, organizations face increased phishing attacks through email, SMS, and video conferencing platforms. Attackers exploit these communication channels to deliver malicious links or attachments. There is also an increased risk of unsecured home networks, which may lack the security measures of on-site networks, making it easier for attackers to target remote users.

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

   ADDTEMP malware is also known as **Desert Falcon** and **Arid Viper**. It is commonly delivered through **spear-phishing attacks**, where attackers use carefully crafted emails to target specific individuals or organizations, tricking them into downloading the malware.

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

   Companies that produced cybersecurity reports in 2020 include **Cisco**, **TrendMicro**, and **Check Point**,

along with several other cybersecurity organizations that analyze and report on emerging threats and trends.

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

   For example, in 2019, a common type of exploit involved unpatched vulnerabilities in applications and operating systems, leading to ransomware attacks and data breaches.

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

   These reports are valuable because they provide insights into emerging cybersecurity threats and trends, helping professionals prepare for and mitigate risks. However, it's essential to consider the source of the information. Some reports may be biased if produced by companies promoting their security products. Additionally, cybersecurity is a rapidly evolving field, so these reports may quickly become outdated. Professionals should also reference more recent sources, such as the CVE database, for the latest threat intelligence