Name : Rizqi Zamzami Jamil

Class : SIB-4C

NIM : 2141762089

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

According to the report's findings, malware usually hides in several key locations on a Windows PC:

1. %temp%: 54.4% on business PCs, 28.7% on consumer PCs.
2. %appdata%: 16.7% on business PCs, 26.5% on consumer PCs.
3. %cache%
4. %windir%

The report mentions that 85% of threats hide in one of these four locations.

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

Answer

1. More targeted attacks: Ransomware attacks are becoming more targeted, better implemented, and more ruthless.
2. Ransom payment increase: The average ransom amount increased, reaching $41,198 in Q3 2019.
3. "Double trouble" trend: Using banking Trojans like Trickbot to steal data and then spreading ransomware like Ryuk.
4. Threats of data exposure: Increased threats to leak victim data if the ransom isn't paid.
5. Shifting targets: The focus is shifting to US cities, transportation, healthcare, education, and small businesses.

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

Answer

1. Surge in phishing sites: The number of phishing sites increased by 640% throughout the year.
2. HTTPS usage: 27% of phishing sites used HTTPS (up from 15% the previous year).
3. Hijacked email chains: An increase in the use of hijacked email reply chains for phishing.
4. Black Friday and Cyber Monday spikes: Visits to phishing sites spiked by 21% on Black Friday and 58% on Cyber Monday.
5. Impersonated brands: Facebook, Microsoft, Apple, and Google are the most commonly impersonated brands in phishing attacks.
6. Increase in Business Email Compromise (BEC): There's a growing trend in BEC attacks.

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

Answer

1. Open nature of the OS: The open nature of the OS makes it difficult for Google to combat malicious apps effectively.
2. Outdated OS versions: Over 40% of Android devices are running OS versions older than v9, making them more vulnerable to exploits.
3. Old and unpatched devices: Older devices that are not patched are more susceptible to malicious apps.
4. High app count: The average Android device has 100-400 pre-installed apps, increasing the potential for security vulnerabilities.
5. Prevalence of malicious apps: Google discovered the Joker malware in 17,000 Android apps, indicating a high prevalence of malicious applications.

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

Answer

The report was created by Webroot, a cybersecurity company that is a part of OpenText. Based on the information from the report, here is a description of the company:

1. Cybersecurity solutions: Webroot provides endpoint protection, network protection, and security awareness training.
2. Target customers: It focuses on managed service providers and small businesses.
3. Technology: Uses cloud and artificial intelligence to protect businesses and individuals from cyber threats.
4. BrightCloud Threat Intelligence: Offers BrightCloud Threat Intelligence services used by leading

companies such as Cisco, F5 Networks, and Citrix.

5. Global presence: Operates globally in North America, Europe, Australia, and Asia.
6. Machine learning: Leverages machine learning to protect millions of businesses and individuals.
7. Slogan: "Discover Smarter Cybersecurity 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.

Answer

1. BLUECRAB

A sophisticated backdoor malware

Capable of stealing sensitive patient data and healthcare records

Uses advanced encryption to avoid detection

Primarily targets healthcare management systems

2. STRONGPITY

A modular malware toolkit

Specialized in data exfiltration from medical devices

Can maintain persistent access to compromised systems

Known for targeting healthcare payment processing 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.

Answer

1. TRITON

Advanced malware specifically designed to target industrial control systems (ICS)

Can manipulate safety systems in energy facilities

Capable of causing physical damage to infrastructure

Primarily targets Schneider Electric's Triconex Safety Instrumented System (SIS)

2. INDUSTROYER

Sophisticated malware designed for power grid attacks

Can control electricity substation switches and circuit breakers

Features modular architecture for multiple attack scenarios

Known for its ability to cause power outages through direct grid manipulation

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

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

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

Answer

China

The “Chinese State-Sponsored Cyber Operations: Observed TTPs” advisory issued by CISA revealed:

1. Use of spear-phishing techniques to gain initial access
2. Exploit vulnerabilities in external internet-facing applications
3. Credential theft and lateral movement in the network
4. The main targets are the high technology and intellectual property sectors

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. **Software Company**: Microsoft, **Timestamp**: October 31, 2024, **Description**: Released security updates addressing multiple vulnerabilities in Microsoft Exchange Server. These vulnerabilities could allow remote code execution and information disclosure if successfully exploited. Critical patches were issued for versions 2016 through 2019.
2. **Software Company**: Adobe, **Timestamp**: October 29, 2024**, Description**: Released critical security updates for Adobe Acrobat and Reader, addressing multiple vulnerabilities that could lead to arbitrary code execution and privilege escalation. Users are strongly advised to update to the latest version to mitigate potential security risks.

Reflection Questions

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

Answer

Increased attack surface, lack of cybersecurity awareness, unsecured home networks, and more phishing attacks targeting remote users.

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

Answer

ADDTEMP malware is described as a Trojan or fileless malware. It is often delivered through phishing emails or malicious attachments.

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

Answer

Companies that created cybersecurity reports in 2020 include Symantec, McAfee, IBM, Cisco, TrendMicro and Verizon.

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

Answer

In 2019, phishing and credential theft were the most common types of exploits, according to several cybersecurity reports.

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

These reports provide insights into cybersecurity trends and threats. Be cautious of biases, data sampling methods, and vendor-specific interpretations when evaluating the information.