KEAMANAN SISTEM INFORMASI

Lab – Evaluate Cybersecurity Reports

Praktikan

[2141762149]

[ANISNA HILWA NADHIFAH]

[SISTEM INFORMASI BISNIS – 4C]

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?

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?

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?

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?

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.

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.

Answers should include using WITCHCOVEN at 49 % and XtremeRAT at 32 %. 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. Briefly describe the malware.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.

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.
Identify the four accused Nation State Cyber Threats.

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.

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.

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

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?

   a. Increased Phishing Attacks: With the rise of remote communication tools like email and video conferencing, there has been a notable increase in phishing attacks targeting both students and employees. Cybercriminals are using tactics that exploit the urgency and uncertainty associated with remote setups, often impersonating legitimate institutions or colleagues to steal sensitive information

   b. Insecure Networks: Many individuals access remote learning and work systems from home networks, which may not have the same level of security as corporate or educational environments. This exposure can lead to vulnerabilities, making it easier for attackers to intercept data or gain unauthorized access to systems

   c. Unsecured Devices: The use of personal devices for remote work and learning increases the risk of malware infections and data breaches. Many personal devices lack the necessary security measures, such as updated antivirus software or firewalls, that are typically in place for corporate devices .

   d. Data Privacy Concerns: Remote learning and working often involve the use of third-party platforms that may collect and store personal data. This raises concerns about how data is handled and whether it is adequately protected against breaches .

   e. Lack of Cybersecurity Awareness: The rapid transition to remote environments has left many users unprepared for the associated risks. Without proper training and awareness programs, employees and students may fall victim to social engineering attacks or mishandle sensitive information .

   f. Increased Use of Collaboration Tools: Platforms like Zoom, Microsoft Teams, and others have

become essential for remote communication. However, they have also become targets for cyberattacks, including "Zoom bombing" and unauthorized access to meetings, which can compromise user privacy and data.

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

ADDTEMP malware, also known as Desert Falcon and Arid Viper, is a type of cyber threat primarily associated with espionage activities. This malware is typically delivered through spear phishing attacks, where targeted emails are used to trick recipients into downloading malicious payloads.

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

In 2020, several companies and organizations published annual cybersecurity reports highlighting various security trends and threats. Here are some notable sources:

1. Cisco: Their report covers various aspects of cybersecurity threats, focusing on the evolving tactics of cybercriminals and the impact of remote work due to the pandemic.
2. Trend Micro: Their "2020 Annual Cybersecurity Report" discusses the rise in ransomware attacks, particularly targeting industries like government, banking, healthcare, and education. The report emphasizes the increased activity of ransomware families like WannaCry and Egregor
3. Check Point Software: They released a report detailing the most prevalent cyber threats, including an increase in attacks against remote working environments and various sectors affected during the COVID-19 pandemic.
4. Symantec (Broadcom): Their annual report highlights trends in malware, phishing attacks, and the overall landscape of cybersecurity threats faced by organizations worldwide.

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

In 2021, the most common type of exploit reported in cybersecurity incidents was unauthorized access, which accounted for approximately 41.5% of all disclosed breaches. This was followed by ransomware attacks, which contributed to about 24.5% of incidents. This marked a significant increase in the prevalence of ransomware compared to previous years.
These trends reflect a broader focus by malicious actors on exploiting vulnerabilities to gain unauthorized access to systems, often leading to data breaches and significant financial implications for affected organizations. The rise in ransomware attacks is particularly concerning, as these incidents often involve attackers holding systems hostage and demanding payments to restore access
BleepingComputer Audit Analytics

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

Reports on cybersecurity threats are invaluable for several reasons:

1. Emerging Threat Awareness: They provide insights into new and evolving threats, helping cybersecurity professionals stay informed about tactics, techniques, and procedures (TTPs) used by cybercriminals. This awareness is crucial for developing effective defense strategies VarInsights
2. Trend Analysis: By compiling and analyzing data from various incidents, these reports can highlight trends in cybercrime, such as increasing attack vectors or vulnerabilities that need addressing. This information is critical for prioritizing security measures and resource allocation Open Text Corporation
3. Benchmarking and Compliance: Organizations can use these reports to benchmark their security practices against industry standards. This can aid in compliance with regulations and help identify areas needing improvement Open Text Corporation Options When Accepting Information from Reports

While these reports are useful, there are important considerations:

- Source Credibility: Evaluate the credibility of the report's publisher. Some organizations may have commercial interests, such as promoting their security products, which could lead to biased reporting. Reports from independent research organizations or academic institutions may provide more objective insights .
- Ti Cyber threats evolve rapidly, so it’s essential to ensure that the information is current. Older reports may not reflect the latest threat landscape, making it vital to consult more recent sources like the National Vulnerability Database (NVD) or the Common Vulnerabilities and Exposures (CVE) list
- Open Text Corporation e cautious of reports that generalize findings without providing context or specifics. Attack methods can vary significantly across different industries and regions, so insights may not be universally applicable.