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?

Answer Area

Based on the 2020 Webroot Threat Report, malware on Windows PCs typically hides in several key system locations. For consumer PCs, a significant portion of infections (26.5%) are found in the %appdata% folder. In contrast, for business PCs, the threats detected in %appdata% account for 16.7%. Other common hiding spots include %temp%, %cache%, and %windir%, with 85% of threats residing in one of these four locations.

Show Answer

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

Answer Area

Trends in ransomware include:
1. More Reconnaissance: Attackers gather detailed information on targets.
2. Higher Ransom Costs: Average ransom demands are increasing.
3. Double Attacks: Combining data theft (e.g., Trickbot) with ransomware (e.g., Ryuk).
4. Targeting High-Value Victims: Focusing on larger, more lucrative targets.
5. Data Leak Threats: Ransomware now often includes threats to leak stolen data

Show Answer

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

Answer Area

Current trends in phishing attacks include:
- Hackers hijacking legitimate email conversations and attaching malicious payloads that can bypass email filters.
- Increased use of HTTPS on phishing sites, making them appear more trustworthy.
- Phishing campaigns often align with public news or product releases (e.g., iPhone launches).
- Impersonation of emerging companies like DocuSign and Steam, creating new challenges in areas like digital document signing and game updates

Show Answer

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

Answer Area

Android devices are more susceptible to security issues because they often come pre-installed with 100 to 400 apps, which could contain vulnerabilities. These widely installed apps are familiar to threat actors, making them attractive targets.

Show Answer

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

Answer Area

The report you provided, titled 2020 Webroot Threat Report, was created by Webroot, a cybersecurity company. Webroot provides a range of cybersecurity solutions, including endpoint protection, network protection, and security awareness training. The company uses cloud-based and artificial intelligence-driven technology to protect individuals and businesses from various cyber threats. Its services are designed for both individual consumers and managed service providers, with particular emphasis on small and medium-sized businesses (SMBs).

Webroot is a subsidiary of OpenText, a leading global enterprise information management company. They operate globally, with a presence in North America, Europe, Australia, and Asia.

Show Answer

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.

Answer Area

In FireEye's analysis of threats targeting the healthcare and health insurance industries, two prominent malware families were identified: WITCHCOVEN and XtremeRAT.

1. WITCHCOVEN: This malware family is primarily used for tracking and profiling potential targets. It injects malicious code into compromised websites, allowing attackers to gather data about victims' devices, such as computer and browser configurations. This helps attackers deploy tailored exploits against vulnerable systems. WITCHCOVEN is used for long-term reconnaissance and can be highly effective in identifying security gaps for future attacks.

2. XtremeRAT: XtremeRAT is a remote access tool (RAT) that enables attackers to control infected systems remotely. It allows them to upload and download files, manipulate Windows processes, interact with the registry, and even steal sensitive data. This malware is often employed in espionage operations, especially in industries with valuable intellectual property, such as healthcare.

Show Answer

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.

Answer Area

The two most commonly used malware families targeting the energy industry are:

- SOGU(41%): A backdoor that can upload/download files, access the file system, registry, and provide C2 graphical access to the desktop.
- ADDTEMP(20%): Used to create persistence by adding new files to system directories, allowing attackers continued access to the compromised system.

Show Answer

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.

Answer Area

```
The key nation-state cyber threat actors identified by CISA are associated
with the following countries:

1. China: Commonly linked with APT41 (Double Dragon) and APT10 (Stone Panda),
these groups focus on cyber espionage, intellectual property theft, and
infiltration of critical infrastructure.
2. Russia: Known actors include APT28 (Fancy Bear) and APT29 (Cozy Bear),
which are associated with cyber espionage, election interference, and attacks
on critical infrastructure.
3. North Korea: Lazarus Group is the main actor, involved in cyber attacks
for financial gain, ransomware, and espionage.
4. Iran: APT33 (Elfin) and APT34 (OilRig) conduct cyber operations targeting
critical infrastructure and businesses, often for political motives
```

Show Answer

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

Answer Area

```
One advisory issued by CISA focuses on North Korean state-sponsored cyber
actors targeting blockchain companies. The advisory, published in April 2022,
highlights the Lazarus Group, a North Korean advanced persistent threat (APT)
group. This group used the TraderTraitor malware, disguised as cryptocurrency
applications, to infiltrate systems and steal cryptocurrency from blockchain-
related companies. The malware variants, such as Manuscrypt, were designed to
collect system information, execute commands, and download further payloads.
The advisory provides recommendations for mitigating this threat, such as
patching known vulnerabilities and implementing strong cybersecurity protocols
.
```

Show Answer

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.

Answer Area

On September 16, 2024, CISA released a plan to align operational cybersecurity priorities for federal agencies. This announcement was preceded by a joint Public Service Announcement (PSA) from the FBI and CISA on September 12, 2024, which warned that false claims of hacked voter information are likely intended to sow distrust in U.S. elections. Additionally, on September 9, 2024, CISA Director Jen Easterly delivered remarks at the Election Center's 39th Annual National Conference in Detroit.

Show Answer

Reflection Questions

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

Answer Area

As schools and companies shift to remote learning and working, they face several cybersecurity challenges. These include a rise in phishing attacks targeting email, text, and video conferencing platforms, as well as increased risks from unsecured networks. Many users may also struggle with outdated software and lack proper training in cybersecurity best practices, making them more vulnerable to threats. Additionally, handling sensitive data remotely complicates privacy issues, and enforcing security protocols becomes more challenging. Overall, these factors underscore the need for enhanced cybersecurity measures and ongoing education.

Show Answer

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

Answer Area

ADDTEMP malware, also known as Desert Falcon and Arid Viper, is typically delivered through spear phishing attacks. These targeted emails often contain malicious attachments or links that, when interacted with, compromise the victim's system, allowing the malware to be installed and execute its harmful activities.

Show Answer

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

Answer Area

Several companies and organizations published annual cybersecurity reports for 2020, including:
1. Cisco - Known for its annual Cybersecurity Report, which covers various security trends and insights.
2. Trend Micro - Released its Threat Landscape report, detailing emerging threats and attack patterns.
3. Check Point - Provided its annual Cyber Security Report, focusing on global security trends and incidents.
4. Verizon - Published the Data Breach Investigations Report (DBIR), analyzing data breaches across multiple industries.
5. McAfee - Offered its Cybersecurity Threats Report, highlighting key threats and vulnerabilities observed throughout the year.

Show Answer

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

Answer Area

In 2023, some of the most common cybersecurity exploits were centered around vulnerabilities in widely used applications and services. One of the most notable was CVE-2023-38831, a flaw in WinRAR used by attackers for malware delivery. This vulnerability replaced Microsoft Office, which had been a top target in prior years. Another critical vulnerability, CVE-2023-34362, affected the MOVEit Transfer software, allowing SQL injection attacks that enabled data theft

Additionally, the CrowdStrike 2023 Global Threat Report highlighted a sharp increase in cloud exploitation and a growing prevalence of malware-free attacks, which accounted for 71% of incidents. This shift highlights how attackers are increasingly bypassing traditional malware defenses

Show Answer

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 Area

Cybersecurity reports are valuable as they provide insights into current threats and vulnerabilities, helping professionals defend against attacks. However, be cautious as some reports may be biased, especially if created by companies promoting their products. Additionally, reports can quickly become outdated, so it’s important to cross-check with up-to-date sources like the CVE database for the latest threats.

Show Answer

End of document

Show All Answers Clear My Responses