Rossi Dea Agatha
SIB 4C – 2141762112

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% dari semua infeksi pada PC ditemukan di %appdata%. Lokasi umum lainnya termasuk %temp%, %cache%, dan %windir%.ype**

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

- **Ransomware semakin diarahkan ke target bernilai tinggi dan lebih rentan. Aktor ancaman menggunakan pengintaian untuk mengidentifikasi target yang lebih mungkin rentan terhadap serangan.**

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

- **Peretas mendapatkan akses ke email seseorang dan melanjutkan percakapan yang sudah ada dengan lampiran berbahaya yang mungkin lolos dari filter email. Penggunaan HTTPS pada**

situs phishing meningkat, dan pelaku sering kali meniru perusahaan sah seperti DocuSign dan Steam. Serangan phishing juga mengikuti berita publik, seperti peluncuran produk populer (misalnya, iPhone).Type

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

- **Perangkat Android sering kali dilengkapi dengan 100-400 aplikasi yang sudah terinstal sebelumnya, yang banyak di antaranya rentan terhadap serangan. Aplikasi-aplikasi umum ini menjadi target ancaman yang diketahui oleh aktor jahat.**

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

- **Webroot adalah perusahaan keamanan siber yang menawarkan berbagai produk dan layanan keamanan untuk penggunaan pribadi dan bisnis. Mereka fokus menyediakan solusi seperti perangkat lunak antivirus, intelijen ancaman, dan perlindungan dari malware.**

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%): Malware yang digunakan untuk footprinting sistem, sering dikaitkan dengan ancaman persisten tingkat lanjut (APT).**
- **XtremeRAT (32%): Alat akses jarak jauh (Remote Access Tool/RAT) yang digunakan untuk memanipulasi file, berinteraksi dengan registri Windows, dan mengumpulkan data dari sistem yang terinfeksi.**

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%): Sebuah malware backdoor yang dapat mengunggah/mengunduh file, mengakses sistem file, memanipulasi registri Windows, dan memberikan akses shell jarak jauh.**
- **ADDTEMP (20%): Dikirim melalui spear phishing, juga dikenal sebagai Desert Falcon atau Arid Viper, dan memungkinkan kontrol jarak jauh atas sistem yang terinfeksi.**

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.

- **China, Rusia, Korea Utara, dan Iran.**

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

- **Korea Utara: Sebuah penasihat mungkin menyoroti serangan terhadap institusi keuangan yang menggunakan Lazarus Group, yang dikenal dengan malware perbankan dan pencurian cryptocurrency.**

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.

- **Contoh 1 :**
  - **Perusahaan : Apple**
  - **Tanggal : 21 September 2021**
  - **Deskripsi : Apple merilis pembaruan untuk iOS 15, watchOS, dan produk lainnya, merekomendasikan pengguna untuk menginstal patch keamanan terbaru guna melindungi dari kerentanan yang diketahui.**

- **Contoh 2 :**
  - **Perusahaan : Adobe**
  - **Tanggal : 14 September 2021**
  - **Deskripsi : Adobe mengeluarkan patch keamanan untuk Photoshop Elements dan Acrobat, yang memperbaiki beberapa kerentanan pada produk perangkat lunaknya.**

Reflection Questions

1. What are some cybersecurity challenges with schools and companies moving towards remote learning and working?
   - **Peningkatan serangan phishing yang menargetkan email, pesan teks, dan konferensi video.**
   - **Kurangnya infrastruktur yang aman untuk akses jarak jauh ke data dan sumber daya sensitif.**

2. What are two terms used to describe ADDTEMP malware and how is it delivered?
    - **Desert Falcon dan Arid Viper. Dikirim melalui serangan spear phishing.**
3. Search the web and locate other annual cybersecurity reports for 2020. What companies or organizations created the reports?
    - **Cisco, TrendMicro, dan Check Point adalah beberapa perusahaan yang menawarkan laporan keamanan siber.**
4. Locate a cybersecurity report for another year. What was the most common type of exploit for that year?
    - **Jenis eksploitasi yang paling umum bervariasi, tetapi buffer overflow dan injeksi SQL merupakan masalah besar di tahun 2019, menurut laporan perusahaan seperti Symantec.**
5. How are these reports valuable, and what do you need to be careful of when accepting the information that is presented in them?
    - **Laporan ini sangat berguna untuk mengikuti ancaman yang muncul dan menginformasikan strategi pertahanan. Namun, penting untuk memverifikasi sumber laporan guna memastikan kredibilitasnya, karena beberapa perusahaan mungkin memiliki motivasi yang bias, seperti mempromosikan produk mereka sendiri. Selain itu, laporan tersebut mungkin menjadi usang dengan cepat, sehingga penting untuk memeriksa data terbaru.**