Winda Umi Fatimatus Sa'diyah

SIB – 4C / 2141762055

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?

- 26,5% dari semua infeksi di PC ditemukan di `%appdata%`. Lokasi umum lainnya adalah `%temp%`, `%cache%`, dan `%windir%`.

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

- Ransomware semakin sering menargetkan target yang bernilai tinggi dan lebih rentan. Pelaku ancaman menggunakan teknik pengintaian (reconnaissance) untuk mengidentifikasi target yang lebih

mungkin terkena serangan, seperti sektor kesehatan atau keuangan yang memiliki sistem pertahanan yang lebih lemah.

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

- Serangan phishing menjadi lebih canggih, sering kali menyamar sebagai merek terkenal atau entitas terpercaya. Serangan ini biasanya menggunakan taktik rekayasa sosial untuk menipu pengguna agar mengklik tautan berbahaya atau memberikan informasi pribadi.

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

- Perangkat Android lebih rentan karena sering kali menggunakan sistem operasi yang usang dan tidak mendapatkan pembaruan keamanan secara tepat waktu. Selain itu, sifat terbuka dari ekosistem Android memungkinkan adanya toko aplikasi pihak ketiga yang dapat menghosting aplikasi berbahaya.

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

- Webroot adalah perusahaan keamanan siber yang menyediakan solusi keamanan berbasis cloud. Mereka berfokus pada perlindungan endpoint, intelijen ancaman, dan keamanan jaringan untuk bisnis dan konsumen. Webroot menggunakan pembelajaran mesin dan AI untuk membantu mendeteksi dan mencegah ancaman siber.

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.

- Yang paling umum digunakan yaitu:
  1. **Ryuk** - Ransomware yang digunakan untuk mengenkripsi data sensitif dan meminta tebusan.
  2. **TrickBot** - Trojan perbankan yang mengumpulkan kredensial dan informasi keuangan, sering digunakan sebagai tahap awal serangan ransomware seperti Ryuk.

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.

- Yang paling umum digunakan yaitu:

1. **Industroyer** - Malware yang dirancang khusus untuk menyerang sistem kontrol industri (ICS), menyebabkan gangguan signifikan pada sektor energi.
2. **BlackEnergy** - Trojan yang digunakan untuk spionase siber dan sabotase, sering kali menargetkan infrastruktur energi untuk mengganggu layanan.

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.

- Empat negara yang dituduh menjadi ancaman siber:
  1. Rusia
  2. China
  3. Korea Utara
  4. Iran

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

- **Rusia**: Salah satu peringatan yang dikeluarkan melibatkan aktor siber yang disponsori negara Rusia yang menargetkan rantai pasokan dan infrastruktur penting, memanfaatkan kerentanan pada produk perangkat lunak untuk mendapatkan akses tanpa izin dan menyebarkan malware destruktif.

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.

- Contoh berdasarkan halaman CISA:

- Perusahaan: Microsoft
- **Cap Waktu:** 10 November 2020
- **Deskripsi Pembaruan:** Microsoft mengeluarkan pembaruan keamanan yang memperbaiki berbagai kerentanan dalam perangkat lunak mereka, termasuk kelemahan eksekusi kode jarak jauh yang kritis di Windows, Office, dan browser Edge. Kerentanan ini dapat memungkinkan penyerang mengambil alih sistem yang terpengaruh.

Reflection Questions

1. What are some cybersecurity challenges with schools and companies moving towards remote learning and working?
   - Tantangan utama termasuk mengamankan perangkat pribadi, memastikan akses aman ke jaringan perusahaan, dan melindungi data sensitif dari serangan phishing dan ransomware. Lingkungan kerja jarak jauh juga mungkin kurang memiliki kebijakan keamanan yang kuat, sehingga meningkatkan risiko serangan siber..
2. What are two terms used to describe ADDTEMP malware and how is it delivered?
   - Malware ADDTEMP sering dikaitkan dengan keluarga malware **Emotet** dan **TrickBot**, yang biasanya disebarkan melalui email phishing dengan lampiran berbahaya atau tautan yang mengunduh malware ke sistem korban..
3. Search the web and locate other annual cybersecurity reports for 2020. What companies or organizations created the reports?
   - Beberapa perusahaan yang membuat laporan keamanan siber pada tahun 2020 termasuk:
     1. Symantec
     2. McAfee
     3. Kaspersky
     4. Cisco
     5. CrowdStrike
4. Locate a cybersecurity report for another year. What was the most common type of exploit for that year?
   - Pada tahun 2019, **jenis eksploitasi yang paling umum** adalah **pencurian kredensial** dan **ransomware**. Penyerang sering menggunakan phishing dan kerentanan pada protokol remote desktop (RDP) untuk mendapatkan akses ke jaringan.
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 memberikan wawasan berharga tentang ancaman yang muncul, metode serangan, dan strategi pertahanan, yang membantu organisasi memperkuat postur keamanan sibernya. Namun, penting untuk mempertimbangkan bias atau keterbatasan dari laporan-laporan ini, terutama jika dibuat oleh perusahaan yang mungkin memiliki kepentingan komersial dalam mempromosikan solusi keamanan tertentu.

End of document