NAMA : Wiraswanti Rismanda Putri

NO : 20

KELAS : SIB-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 realtime. 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: **Biasanya 26,5% dari semua infeksi pada PC ditemukan di %appdata%. Lokasi umum lainnya adalah %temp%, %cache%, dan %windir%.**

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

Answer: **Ransomware cenderung menyasar target yang memiliki nilai tinggi dan tingkat pertahanan yang lebih lemah. Para pelaku ancaman melakukan pengintaian untuk menemukan target yang lebih rentan.**

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

Answer: **Peretas dapat memperoleh akses ke email seseorang dan melanjutkan percakapan yang sah dengan menyertakan lampiran berbahaya. Lampiran ini mampu melewati filter email. Penggunaan HTTPS di situs phishing juga semakin meningkat. Serangan phishing sering kali memanfaatkan berita terkini, seperti peluncuran produk baru (seperti iPhone). Meniru perusahaan-perusahaan baru seperti DocuSign dan Steam menimbulkan tantangan baru dalam penandatanganan dokumen digital dan pembaruan otomatis untuk game.**

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

Answer: **Perangkat Android lebih rentan terhadap masalah keamanan karena beberapa faktor, salah satunya adalah fragmentasi sistem operasi. Android digunakan oleh berbagai produsen dengan beragam**

versi OS, sehingga pembaruan keamanan sering kali tidak merata di seluruh perangkat. Selain itu, perangkat Android biasanya sudah terinstal dengan ratusan aplikasi yang bisa memiliki celah keamanan. Aplikasi-aplikasi ini diketahui oleh para peretas sebagai target potensial karena sering diinstal pada banyak perangkat. Ditambah lagi, Android memiliki ekosistem yang lebih terbuka dibandingkan iOS, yang memudahkan pengguna untuk mengunduh aplikasi dari sumber yang tidak resmi, meningkatkan risiko keamanan.

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

Answer: **Webroot adalah perusahaan keamanan siber yang menyediakan berbagai produk dan layanan keamanan untuk rumah dan bisnis.**

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: **Berdasarkan temuan FIREEYE, malware WITCHCOVEN dan XtremeRAT adalah yang paling umum digunakan oleh aktor ancaman, masing-masing sebesar 49% dan 32%. WITCHCOVEN digunakan untuk melacak sistem komputer dan organisasi, memungkinkan penyerang memantau aktivitas serta mencuri informasi. Sementara itu, XtremeRAT adalah alat akses jarak jauh (RAT) yang memungkinkan pengunggahan dan pengunduhan file, manipulasi registri Windows, proses, layanan, dan menangkap 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.

Answer: **Berdasarkan temuan FIREEYE, dua malware yang paling umum digunakan oleh pelaku ancaman dalam industri ini adalah SOGU dan ADDTEMP, dengan masing-masing penggunaan sebesar 41% dan 20%. SOGU adalah pintu belakang (backdoor) yang memungkinkan pengunggahan dan pengunduhan file, serta memberikan akses ke sistem berkas, registri, konfigurasi, dan shell jarak jauh. Malware ini menggunakan protokol khusus untuk menyediakan akses grafis ke desktop sistem yang terinfeksi melalui Command and Control (C2). ADDTEMP adalah malware yang digunakan oleh pelaku ancaman untuk tujuan serupa, namun dengan cara dan tingkat akses yang berbeda.**

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: **Tiongkok, Rusia, Korea Utara, dan Iran**

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

Answer: **Tiongkok: Salah satu nasihat yang telah dikeluarkan terkait aktivitas siber dari Tiongkok adalah mengenai ancaman Advanced Persistent Threat (APT) grup yang didukung negara, seperti APT40 atau APT10. Nasihat ini menyoroti serangan yang menargetkan infrastruktur penting seperti sektor kesehatan, teknologi, dan telekomunikasi. Pemerintah sering kali mengingatkan perusahaan dan lembaga untuk meningkatkan sistem keamanan mereka, menggunakan autentikasi multifaktor, serta memperbarui perangkat lunak guna melindungi dari serangan siber yang mencuri kekayaan intelektual dan data sensitif.**

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: **Perusahaan Adobe pada 14 September 2021. Adobe merilis pembaruan keamanan untuk beberapa produk mereka, termasuk Adobe Photoshop Elements dan Adobe Acrobat. Pembaruan ini memperbaiki kerentanan kritis yang dapat dieksploitasi untuk menjalankan kode berbahaya pada sistem yang terpengaruh. Pengguna disarankan untuk mengunduh dan menginstal pembaruan segera untuk melindungi sistem mereka dari potensi serangan.**

Reflection Questions

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

   Answer: **Peningkatan serangan phishing melalui email, pesan teks, dan konferensi video, kesulitan dalam memantau dan mengamankan data sensitif karena akses jarak jauh, kurangnya keamanan jaringan rumah yang dapat membuka akses ke serangan ransomware dan malware**

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

   Answer: **Desert Falcon dan Arid Viper adalah dua alias yang digunakan untuk menggambarkan malware ADDTEMP. Penyebarannya melalui Spear Phishing, di mana target menerima email yang tampaknya sah tetapi berisi file atau tautan berbahaya.**

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

   Answer: **Beberapa perusahaan yang membuat laporan keamanan siber tahunan 2020 adalah Cisco, TrendMicro, dan Check Point. Banyak perusahaan lain seperti Symantec dan FireEye juga menerbitkan laporan.**

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

   Answer: **Pada 2020 beberapa jenis eksploitasi yang umum termasuk ransomware, serangan phishing, dan exploiting vulnerabilities dalam perangkat lunak yang tidak diperbarui atau sudah usang.**

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: **Perlu memperhatikan siapa yang membuat laporan dan apakah mereka memiliki kepentingan komersial dalam menjual solusi keamanan. Evaluasi relevansi laporan, karena ancaman siber terus berkembang dan informasi dalam laporan bisa cepat usang. Sumber informasi terbaru seperti CVE (Common Vulnerabilities and Exposures) sangat penting untuk diikuti.**