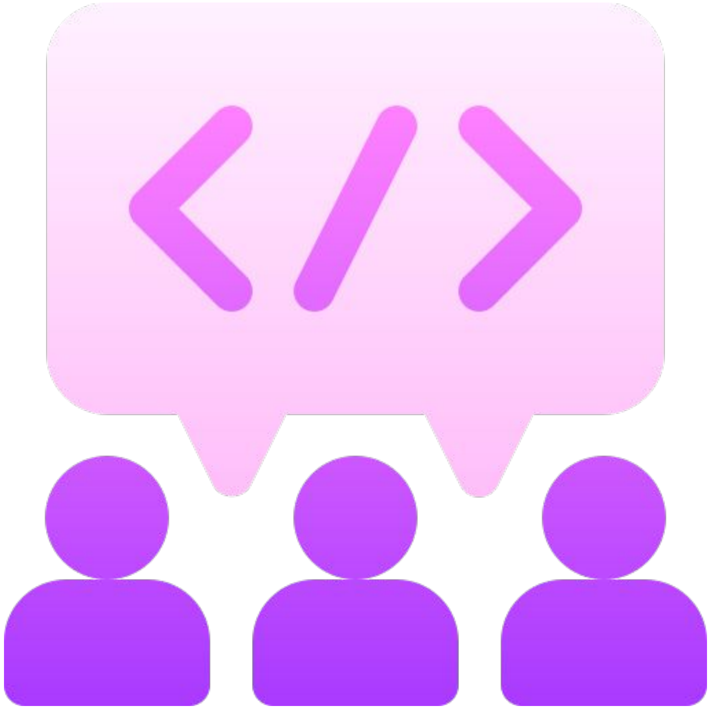
CODEPATH*ORG

Data Dig Presentation: **Excel Macro Pushes Lokibot**

Introductions (Group 17)

- **Emran Habib (He/him)**
  demran235@gmail.com
- **Niles Buchanan (He/him)**
  nilesbuchanan2000@gmail.com
- **Dheeraj Kumar (He/him)**
  dheeraj.narsani@outlook.com
- **Wenhao Xue (He/him)**
  whx3223@gmail.com
- **Areeb Ehsan (He/him)**
  areebehsan16@gmail.com



Data Dig Group 1

Dataset: “EXCEL SPREADSHEET MACRO PUSHES LOKIBOT” from Malware-traffic-analysis.net

Playbook: The NIST Computer Security Incident Handling Guide (Special Publication 800-61, Revision 2)

Tools: Wireshark, NetworkMiner, VirusTotal, Catalyst

About the Dataset

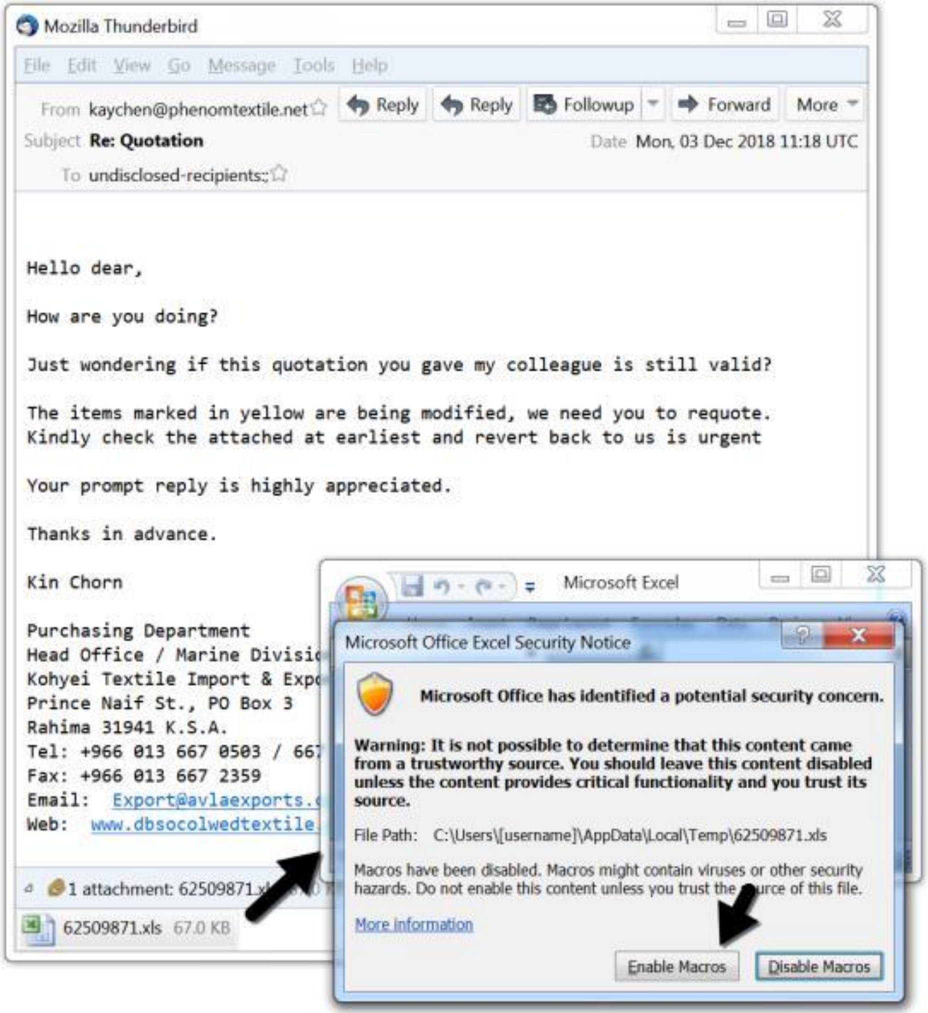
- **Where does the data come from? What kind of devices / technologies does it target?**
- This data was found in malicious spam emails. This is a malicious macro for an Excel spreadsheet. The macro downloads a Lokibot, a credential stealer, called Xehmigm.exe. The Windows registry is also updated to keep this LokiBot persistent.
- **What are 3 things you expect to find when you analyze the data (hypothesis)?**

Knowing what we coincidentally learned about LokiBot from the Threat Intelligence lab, I expect LokiBot to steal credentials from infected machines

I expect a macro to download a file from a website without the user's realization

I expect the malware to be hidden as a normal-looking program

Source: https://isc.sans.edu/diary/Malspam+pushing+Lokibot+malware/24372



From kaychen@phenomtextile.net

Subject **Re: Quotation**

Date Mon, 03 Dec 2018 11:18 UTC

To undisclosed-recipients:;

```
Hello dear,

How are you doing?

Just wondering if this quotation you gave my colleague is still valid?

The items marked in yellow are being modified, we need you to requote.
Kindly check the attached at earliest and revert back to us is urgent

Your prompt reply is highly appreciated.

Thanks in advance.

Kin Chorn

Purchasing Department
Head Office / Marine Divisio
Kohyei Textile Import & Expo
Prince Naif St., PO Box 3
Rahima 31941 K.S.A.
Tel: +966 013 667 0503 / 667
Fax: +966 013 667 2359
Email:  Export@avlaexports.c
Web:  www.dbsocolwedtextile.
```

1 attachment: 62509871.xl

62509871.xls 67.0 KB

Microsoft Office has identified a potential security concern.

Warning: It is not possible to determine that this content came from a trustworthy source. You should leave this content disabled unless the content provides critical functionality and you trust its source.

File Path: C:\Users\[username]\AppData\Local\Temp\62509871.xls

Macros have been disabled. Macros might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.

More information

About the Playbook

- There are several good reasons that led our team to choose the The NIST Computer Security Incident Handling Guide. One of the reasons being that this **playbook was standardized by the NIST**, known for their reliability and reputation.
  This playbook is incredibly in-depth and covers the entire procedure for incident response (**covers all IR steps, future practices, emphasis on defining organizational structures, roles, and responsibilities**).
  Another reason we chose this playbook is because this playbook is **aligned with many NIST compliance requirements.**

- Tools Used: Wireshark, NetworkMiner, VirusTotal - read traffic to find infection, see downloaded files and suspicious connections, see exfiltrated data, and analyze malware by following TCP stream data and exporting objects (files)

Monitoring Sources

The most common types monitoring sources used were email logs, and network logs.

Email logs: the purpose is to identify malicious emails and understand the delivery method of the Lokibot malware, often distributed through phishing emails with malicious macros. Action:Analyzing logs from email servers for indicators of phishing attempts, or links leading to Lokibot.

Network logs: Identifying unusual network traffic patterns associated with Lokibot, including communication with command and control servers. Action: Inspecting logs for outbound/inbound connections, analyzing traffic patterns, and looking for connections to known malicious IP addresses.

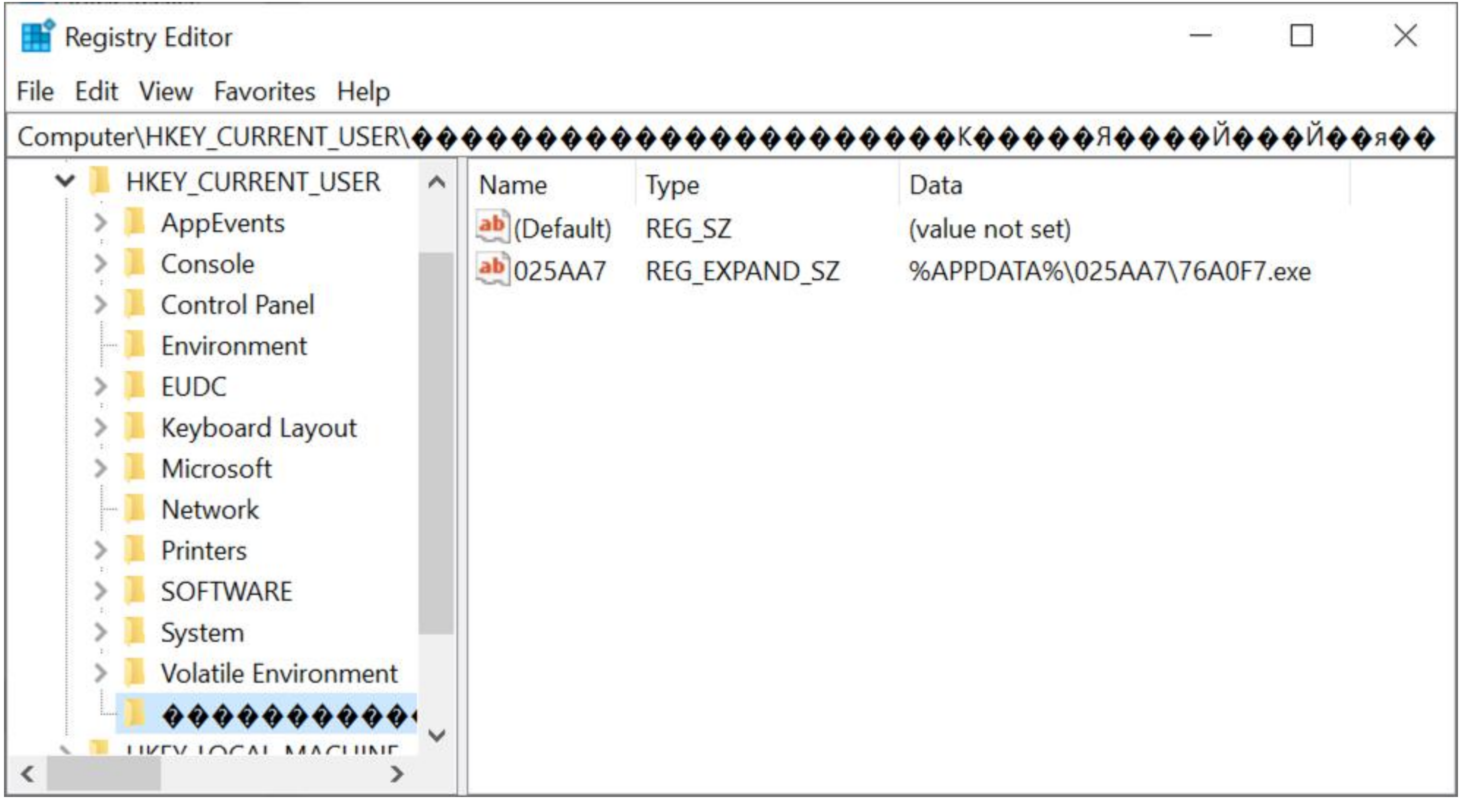
Impact Analysis

- **What was the impact of the incident? What was the severity?**
- LokiBot establishes persistence by creating and modifying files in user directories which makes it challenging to trace it. Primarily, it targets Microsoft Office files and creates executable files with random names (eg: 76A0F7.exe).
- It poses a high severity threat because of its persistent nature and credential theft capability.

- **Were other systems or applications affected?**
- LokiBot malware makes various changes to the registry keys associated with Windows applications such as Internet Explorer, Microsoft Edge.
- One interesting thing that stood off was the presence of a French text, “*Interdire (Bloquer) un CD/DVD sur votre ordinateur* “ which refers that LokiBot is interfering with the hardware component of the system which are the CD/DVD drives and trying to potentially restrict access to it.

Registry Update

Source: https://isc.sans.edu/diary/Malspam+pushing+Lokibot+malware/24372



Computer\HKEY_CURRENT_USER\�����������������������К�����Я����Й���Й��я��

Name	Type	Data
(Default)	REG_SZ	(value not set)
025AA7	REG_EXPAND_SZ	%APPDATA%\025AA7\76A0F7.exe

Incident Response

- **What happened when you followed the playbook to "respond" to the incident?**

- Unusual patterns in HTTP traffic were detected through Wireshark and NetworkMiner logs, leading to the identification of a threat involving the download of a Lokibot-infected Excel spreadsheet. In response, the affected system was immediately disconnected from the network, and the malicious file was isolated and quarantined to prevent further damage.
- **Discuss the relevant data and monitoring sources that were used to identify the incident.**

- The incident was identified through careful inspection of Wireshark and NetworkMiner logs, with a focus on HTTP traffic analysis. The focus is on detecting patterns that indicate malicious file transfers and interactions with suspicious IP addresses.

- **What were the tactics, techniques, and procedures (TTPs) used? Did you identify any indicators of compromise (IOCs)?**

1. Phishing and Malware Delivery:

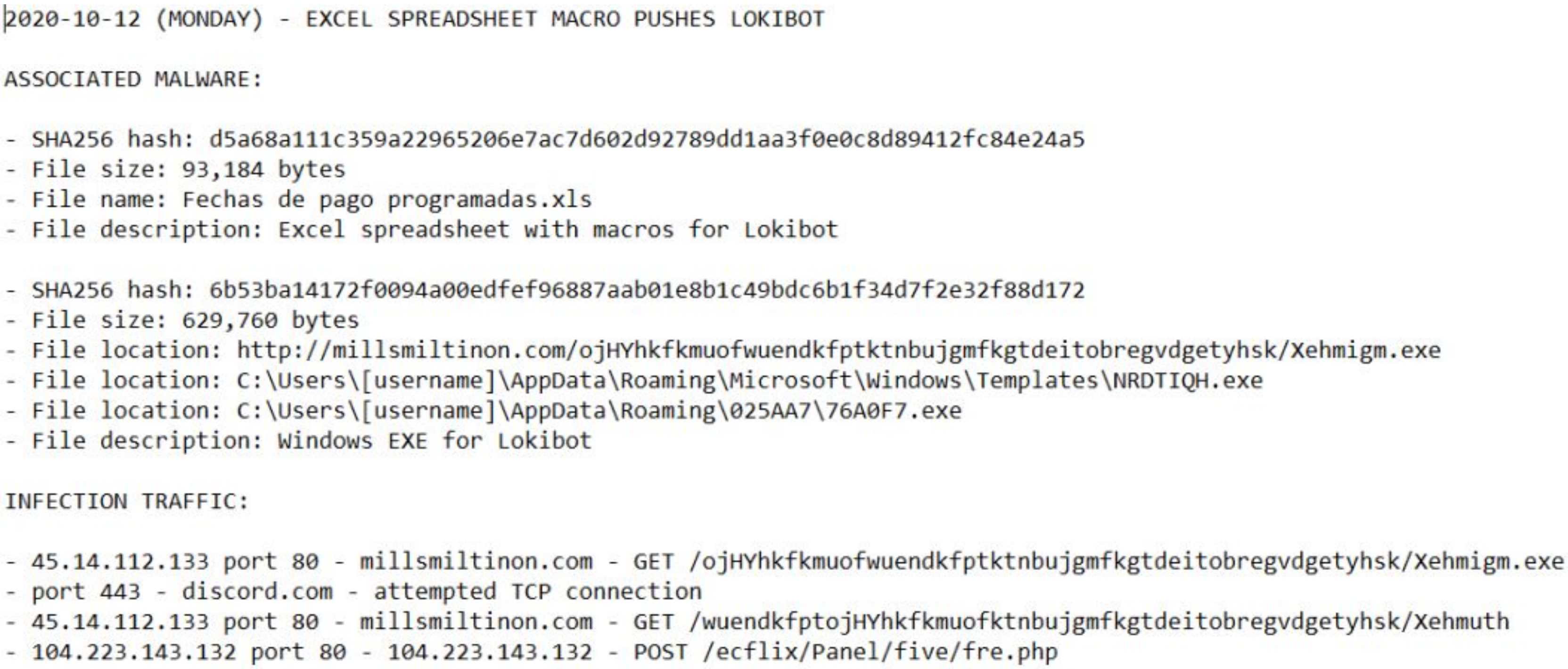
   Threat actors employed a phishing campaign using an Excel spreadsheet to download and execute Lokibot.

2. File-Based IOCs:

   Identified malicious Excel file: SHA256 hash "d5a68a111c359a22965206e7ac7d602d92789dd1aa3f0e0c8d89412fc84e24a5."

3. Network Traffic to Malicious IP Addresses:

   Observed HTTP traffic to "45[.]14[.]112[.]133" for downloading Lokibot.



```
2020-10-12 (MONDAY) - EXCEL SPREADSHEET MACRO PUSHES LOKIBOT

ASSOCIATED MALWARE:

- SHA256 hash: d5a68a111c359a22965206e7ac7d602d92789dd1aa3f0e0c8d89412fc84e24a5
- File size: 93,184 bytes
- File name: Fechas de pago programadas.xls
- File description: Excel spreadsheet with macros for Lokibot

- SHA256 hash: 6b53ba14172f0094a00edfef96887aab01e8b1c49bdc6b1f34d7f2e32f88d172
- File size: 629,760 bytes
- File location: http://millsmiltinon.com/ojHYhkfkmuofwuendkfptktnbujgmfkgtdeitobregvdgetyhsk/Xehmigm.exe
- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Templates\NRDTIQH.exe
- File location: C:\Users\[username]\AppData\Roaming\025AA7\76A0F7.exe
- File description: Windows EXE for Lokibot

INFECTION TRAFFIC:

- 45.14.112.133 port 80 - millsmiltinon.com - GET /ojHYhkfkmuofwuendkfptktnbujgmfkgtdeitobregvdgetyhsk/Xehmigm.exe
- port 443 - discord.com - attempted TCP connection
- 45.14.112.133 port 80 - millsmiltinon.com - GET /wuendkfptojHYhkfkmuofktnbujgmfkgtdeitobregvdgetyhsk/Xehmuth
- 104.223.143.132 port 80 - 104.223.143.132 - POST /ecflix/Panel/five/fre.php
```

Source: https://www.malware-traffic-analysis.net/2020/10/12/index.html

Remediation

- Areas of weakness: Lack of user education, weak email and spam filtering, enabled macros settings, weak antivirus (endpoint security), and weak access control settings.
- Recommended remediation: **Scanning and removal**, utilize **backups**, apply **patches**, security awareness **training**, update **email filter and firewall rules**, **disable macros** for MS Office, **upgrade endpoint security** services, **stricter access controls**, aggregate and send **audit logs** to SIEM**,** set up **SIEM alerts**, **change passwords**, **continue monitoring the system**, and continue **documenting** and learning.