VERSION 1.0 / 26-02-2022

Threat Intelligence Report

# Hunting Recent QakBot Malware

Zayed AlJaberi

26- 02 - 2022

https://www.linkedin.com/in/zayedaljaberi

## QAKBOT THEN

QAKBOT, first observed in 2007, is a known malware to be used by multiple threat actor groups for keylogging and stealing online banking credentials to serve access to human-operated ransomware attacks.

Initial versions of QAKBOT targeted financial data, so it was classified as a banking trojan, but more recent versions have acted as a **delivery mechanism** for “second stage” malware. Specifically, QAKBOT seems to lead to targeted attacks involving data theft **(exfiltration)** and **ransomware**.

## QAKBOT NOW

Nowadays, We have identified a significant increase number of QakBot malware that is being spread across the globe.

Cybereason provides their analysis of an attack that involved **compromising an Exchange server** by exploiting one of the **ProxyShell vulnerabilities** and then using **email threads** obtained from the server to send **phishing emails** containing **malicious links**.

It is not required that your organization’s exchange server be vulnerable for this attack to succeed, as these groups can leverage **“Email threads” from compromised exchange** instances **owned by other organizations** to send out **“Phishing Emails.”**

A global view of QAKBOT activity from March 25, 2021 to October 25, 2021 as seen from Trend Micro Smart Protection Network (SPN)

Many other threat intelligence advisories and reports have shared hundreds of IOCs related to the recent QakBot Campaign. However, the ongoing increase of the IOCs will make it hard for the cyber security team in an enterprise to keep track and block all of them. We find this cannot be practical anymore.

Coming across several advisories, we can see that this campaign uses specific **TTPs** that we can follow and leverage in our environment to take a proactive approach and more efficient security in place.

This report will cover only the **first four techniques** of the malware stages of recent QakBot Malware, mapping it with **MITRE ATT&CK** and hunting queries on **Microsoft Defender ATP**.
I have also added hunting queries of previous **TTPs** mentioned in the [red canary threat report 2021] related to QakBot Malware to have better coverage in our detection for this exercise.

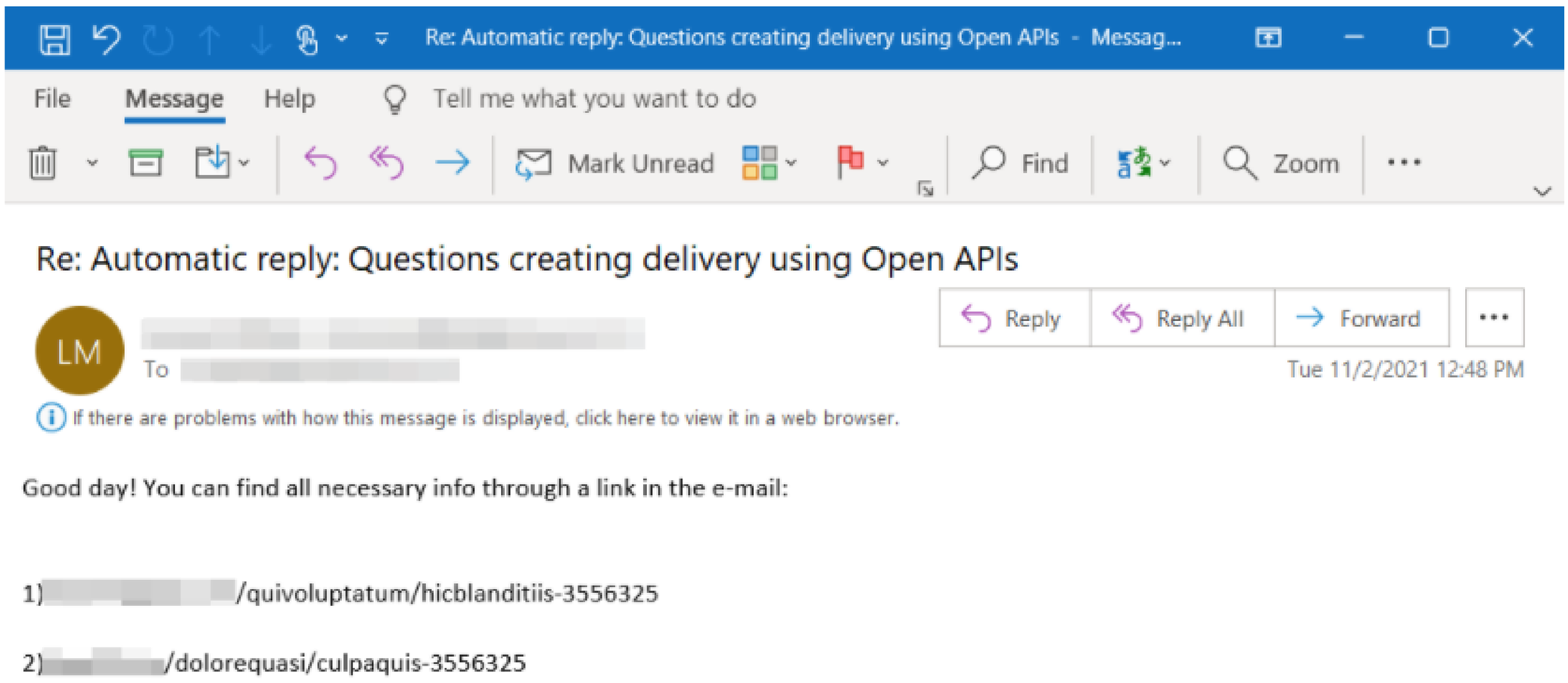
## EMAIL DELIVERY

**Technique/Sub-Technique**: Phishing, Spear phishing Link - T1566.002
**Technique/Sub-Technique**: User Execution, Malicious Link- T1204.001

Qakbot is delivered via one of three **email** methods: **malicious links**, malicious attachments, or, more recently, embedded images. The links used have been categorized as; ; **compromised sites**, **file share sites,** or **newly seen domains.**

Earlier this year, we began to observe abuse of **OneDrive** and mail with **un/clickable links** to **download the malicious Excel document**.

Screenshot from Microsoft Security Blog




### Microsoft Defender ATP| Advanced Hunting Query:

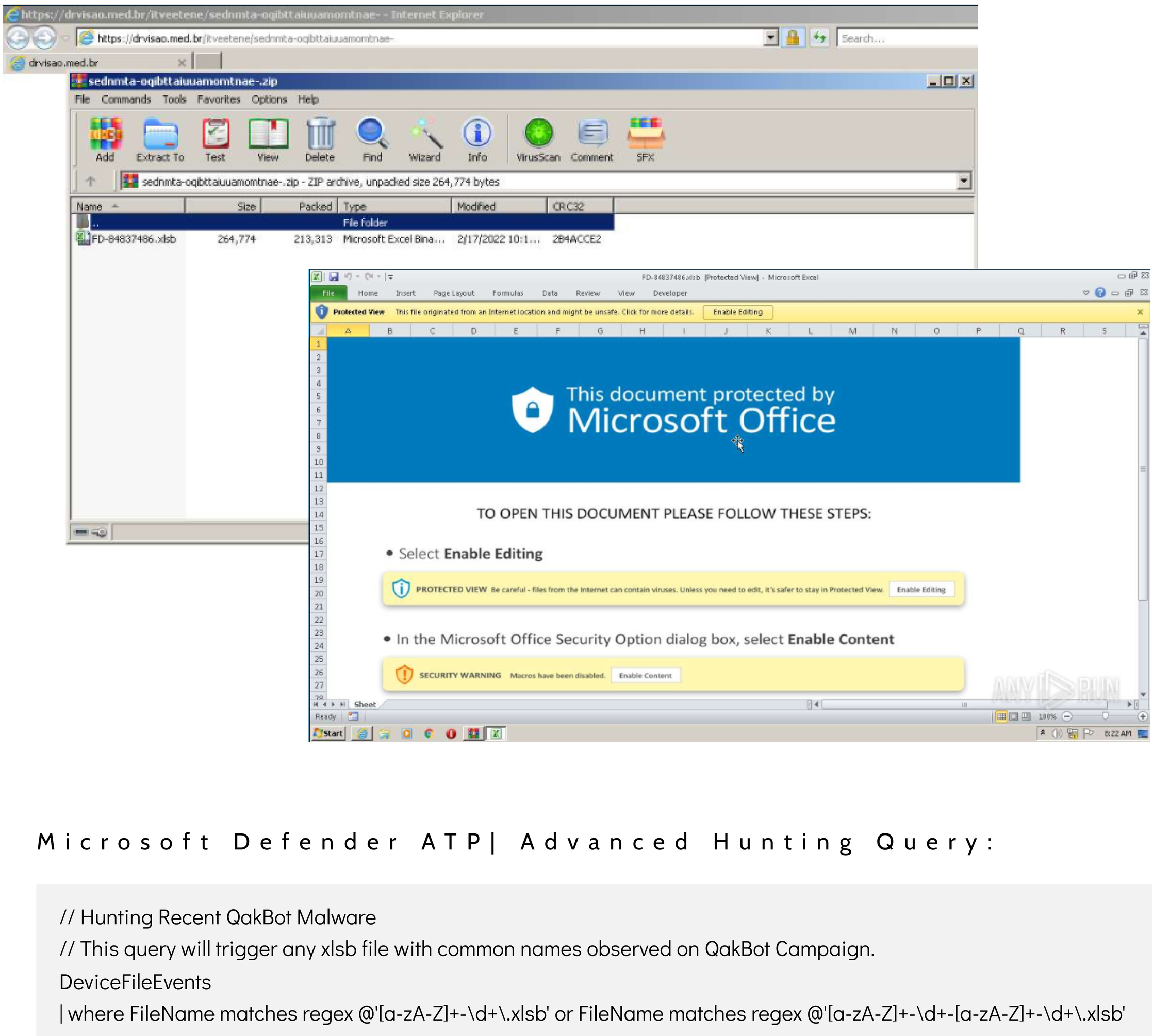
```
// Hunting Recent QakBot Malware
// This query will give you visibilty of accessed URLs from recieved emails, you can run bulk scan across Virustotal,Talos,Sitereview...etc to identify the once classified as malicious/suspicous (Note: Validate all the onedrive links)
DeviceNetworkEvents
| where InitiatingProcessParentFileName has "OUTLOOK" or InitiatingProcessParentFileName has "Mail"
| where InitiatingProcessFileName has_any ('chrome','firefox','msedge','opera','safari','brave')
| where isnotnull (RemoteUrl)
| summarize count() by RemoteUrl
```

## USER EXECUTION

**Technique/Sub-Technique**: User Execution, Malicious File - T1204.002

Once the user visits the malicious site, a **zip (contain .xlsb)** or direct **xlsb file** will be downloaded. We have analyzed several numbers of QakBot and we can observe they used **a common filename pattern** e.g., MJ-1005546.xlsb.

Screenshot from AnyRun



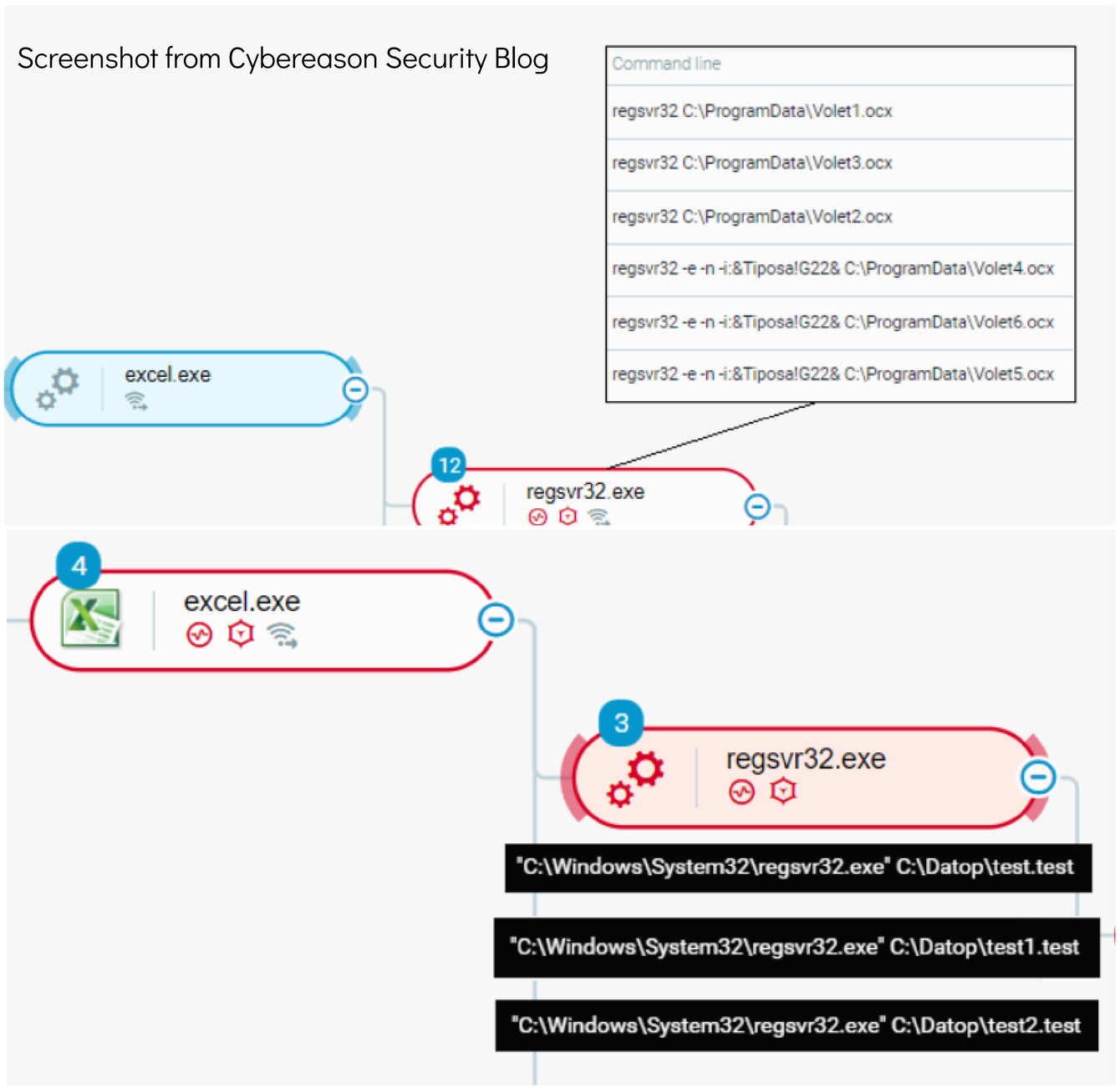

### Microsoft Defender ATP| Advanced Hunting Query:

```
// Hunting Recent QakBot Malware
// This query will trigger any xlsb file with common names observed on QakBot Campaign.
DeviceFileEvents
| where FileName matches regex @'[a-zA-Z]+-\d+\.xlsb' or FileName matches regex @'[a-zA-Z]+-\d+-[a-zA-Z]+-\d+\.xlsb'
```

## DEFENSE EVASION

**Technique/Sub-Technique**: Signed Binary Proxy Execution, Regsvr32 - T1218.010 / Rundll32 - T1218.011

This technique is observed once the user clicks on **"Enable Content"**, in this report we are cover the **spawn of Regsrv32**. two types of files being created ***.ocx** or ***.test**. Gratefully, these files have pattern in common is first numeric in each file (e.g. **tel1.ocx, tel2.ocx, tel3.ocx**) or (**tel.test, tel1.test, tel2.test**).




### Microsoft Defender ATP| Advanced Hunting Query:

```
// Hunting Recent QakBot Malware
// This query will trigger if the user successfully enabled the content of the xlsb macro excel file. This query includes some inputs from Red Canary 2021 QakBot Threat Report. If you see results with filenames new1.ocx, new2.ocx OR new.test , new1.test. initiate  Isolation of the endpoint and involve the IR team.
search in (DeviceImageLoadEvents, DeviceEvents)
(DeviceName == DeviceName)
| where InitiatingProcessParentFileName has_any ("EXCEL", "WORD", "OUTLOOK", "POWERPNT", "ONENOTE", "mobsync")
| where InitiatingProcessFileName has_any ("regsvr32.exe", "rundll32.exe", "schtasks.exe") or * contains "esentutl.exe"
| where InitiatingProcessCommandLine !has "cryptext.dll"
| where InitiatingProcessCommandLine !has "ndfapi.dll"
| where InitiatingProcessCommandLine !has "srchadmin.dll"
```

# Summary

In conclusion, this report has focused on **the first four techniques** currently being used, with proper **data sources of the logs ingested and parsed correctly.** Building **use-case** or **custom detection** will be partially enough to detect and mitigate this risk. We should be aware that **TTPs might be changed** during the coming time.

# IOC Collection

URLHaus

https://urlhaus.abuse.ch/browse/tag/qbot/

https://urlhaus.abuse.ch/browse/tag/Quakbot/

https://urlhaus.abuse.ch/browse/tag/Qakbot/

Github - executemalware

https://github.com/executemalware/Malware-IOCs

# Reference

Sans DFIR Threat Hunting Summit  - Hunting Malicious Office Macros

https://youtu.be/soF5iyeeWDg

UNIVERSAL RULE CONVERTER FOR VARIOUS SIEM, EDR, AND NTDR FORMATS

https://uncoder.io/

Cybereason - THREAT ANALYSIS REPORT: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot

https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot

Qakbot Continues to Abuse OneDrive in Mid-February

https://assets.sentinelone.com/wt-reports/?lb-mode=overlay

Microsoft - A closer look at Qakbot’s latest building blocks (and how to knock them down)

https://www.microsoft.com/security/blog/2021/12/09/a-closer-look-at-qakbots-latest-building-blocks-and-how-to-knock-them-down/

The Prelude to Ransomware: A Look into Current QAKBOT Capabilities and Global Activities

https://documents.trendmicro.com/assets/pdf/Technical-Brief---The-Prelude-to-Ransomware-A-Look-into-Current-QAKBOT-Capabilities-and-Activity.pdf