Saptang Labs

Targeting Weak links in the CIIs Chain: Qbot's new tactics in Ransomware Era.

Executive Summary

Sophos Labs reported recently [1]that high incidence of ransomware attacks is in India. Over 68% of respondents from India said that they were hit by ransomware. The recent spate of publicly disclosed attacks only confirms the trend. We investigated how this new wave of attacks on the infrastructure are being carried out. Our threat research team observed re-orientation of the BOTNETs - oldest threat actors. Old malspam oriented Botnets are making themselves relevant in the ransomware era. They now employ improved and sophisticated techniques and appear to care about geographies. Their core objective appears to breach and identify meaty targets for ransomware attacks.

This is a dangerous trend for cyberspace. Hostile state actors and organised crime gangs had limited leads to penetrate CIIs. Botnets with their widespread reach can offer better leads. This dangerous development could be behind the sudden rise in attacks on the CIIs in India. This sudden shift could also have two more additional reasons.

(a) There is an increased enforcement activity against cybercrime groups in the developed countries. This led to the taking down of the larger botnets. Consequently, large botnet operators are migrating into new jurisdictions such as India.
(b) Pandemic created by the Wuhan virus (Covid-19) is a major force in this shift. It moved many CIIs to open their network for WFH. It also spawned many new CIIs who are rapidly scaling up with limited focus on cyber security. Consequently, large botnet operators are finding cyberspace attractive for their operations.

We observed an old BOTNET Qbot activity in India. It is recently connected with ransomware groups such as REVIL/Sodinokibi. Botnet has undergone total transformation. Its new campaign titled **Biden52** appears to be significantly focussed on India. As a part of the campaign, emails were targeted on breaching one of the port clearing agents. It is a common trend by the Qbot to hijack or pretend internal email threads. We see that email threads that were hijacked have a relation to a critical port in India. The malware that was enclosed as an attachment is more sophisticated than seen before in Qbot campaigns. Full analysis of the attachment is enclosed.

Target was one of the top clearing agents at JNPT. They are part of a regular trusted group for interaction by port authorities. This relationship is attempted to be exploited by the threat actors. There could be network level integration between the ports and clearing agents. This

[1] https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

CONTACT: SALES@SAPTANGLABS.COM

is new modus targeting the supply chain of entities related to a very important port operator in India. However, we don't have an indicator as to whether the attack was successful or not.

It may be noted that there was a previous attack on Maersk Terminal of JNPT in June 2017. Attack in 2017 disrupted port operations (container terminal) for days. History of a successful disruption makes port infrastructure an attractive proposition to ransomware operators. Detailed technical report is enclosed and it may be noted that this is a live campaign. This new trend requires a comprehensive policy response from the Government and Boards. They should ensure that their security is not put at risk due to the vendor's weak security posture. We are only as strong as our weakest link.

Saptang Labs

We are a young cyber security start-up from India with a strong R&D focus. We would continue to track and study specific threats to Indian cyber space. If you are interested in collaborating with us or working with us or reaching out, please feel free to email us tushar@saptanglabs.com

Qbot: Introduction

The decade old Qbot has been known as Qakbot, Pinkslip bot since 2008. Qbot is a continuously evolving Trojan that started as a banking trojan capable of stealing banking credentials, browser data, and other financial information but has been expanding its capabilities to become a persistent threat for Organizations. Unlike typical financially motivated Banking Trojans, Qbot doesn't just stop with banking information but creates a botnet of infected machines to distribute Ransomware, utilizing the harvested information to propagate the campaign.

The capabilities of Qbot Trojan include:

- Remote Command & Control over infected machines
- Exfiltrate financial and banking information
- Hijack victim's email threads to propagate the campaign
- Botnet for dropping Ransomware and Trojans.

The group uses evolving Techniques Tactics and Procedures (TTPs), anti-analysis features, and constantly changing delivery methods from the use of VBS scripts with XML4 Macros in Excel Software to drop payload from the malicious Excel file.

Qbot: Biden 52 Campaign

Our research in this report covers the Qbot with special focus on targeting of Indian cyber space. Multiple security companies including the Checkpoint have covered emerging trends in the operations of the organised cybercrime groups. We believe that recent crackdown and seizing of the Emotet botnet resulted in Qbot playing a bigger role acting as a botnet to deploy Trojans and Ransomware including Prolock ransomware and Egregor ransomware.

Modus-operandi

The current modus operandi is to compromise an email account and hijack an email thread to reply to conversations with organizations, making use of the benign email conversation to persuade the victims into downloading the attached zip file and opening the extracted XLSM file. A better understanding of the campaign can be achieved with the below image:

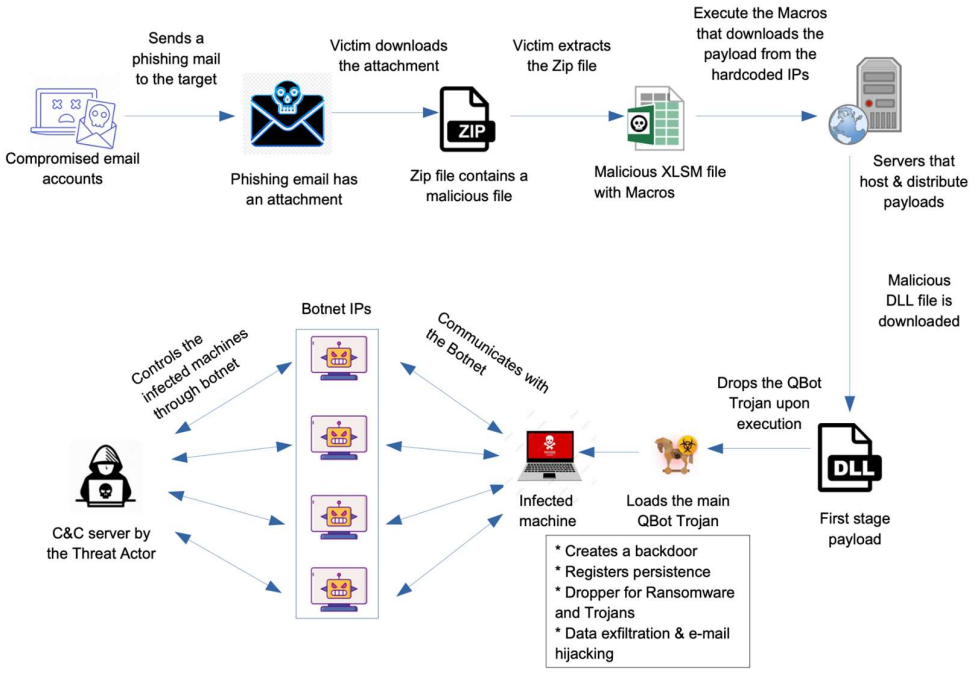


Figure.1: *Modus Operandi of the Qbot Campaign*

Attack Vector

The contents of the malicious emails are greatly socially engineered to not raise any suspicion and the strategy of hijacking email threads clearly has a greater probability of success since the malicious email is from a trusted source.

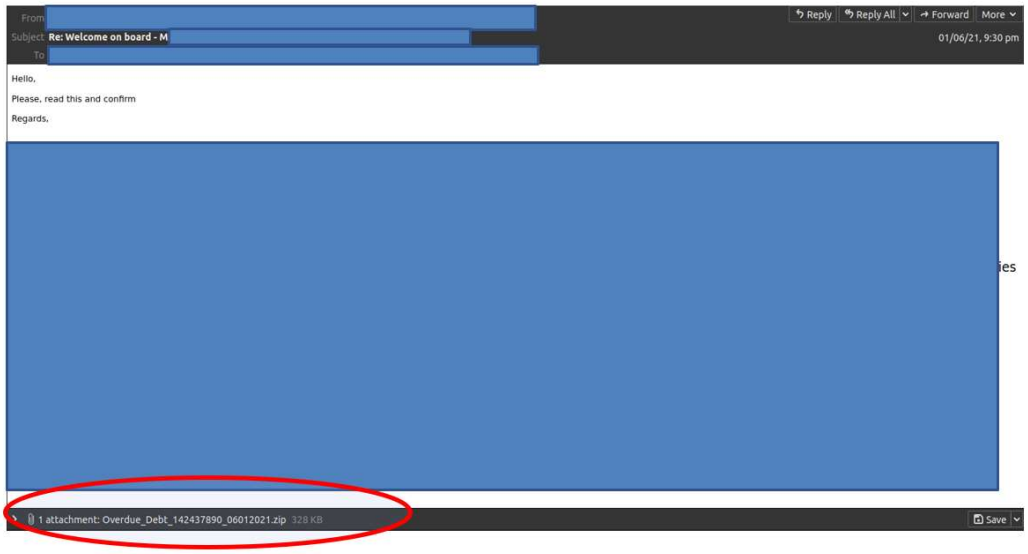


Figure 14

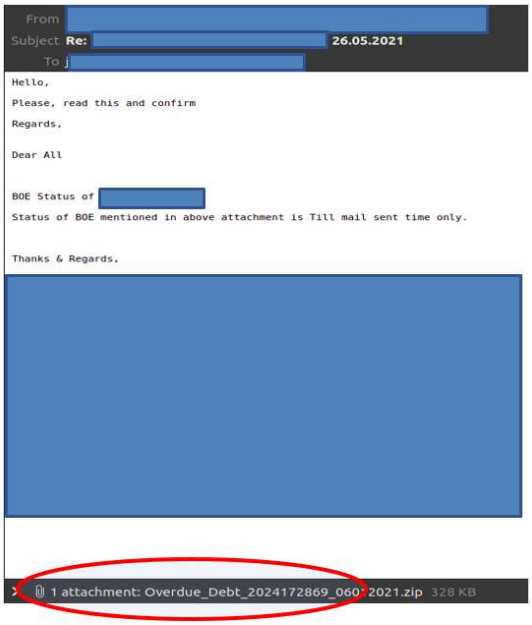


Figure 15

Figure 16

Figures.14,15,16: *Screenshots of the e-mails received by the target organizations*

From: [redacted]
To:
Subject: Re: RE: Please go through the attached invoice & packing List, we want to export it Kenya
Date: 01.06.2021 22:15:24 (+0530)
Attachments: Overdue_Debt_1577895391_06012021.zip (0 pages)

Hello,

Please look at the file attached. It must be interesting

Thank you.

Figure.2: *Screenshot of an email containing the malicious zip file*

The attachment contains a zip file[2] that contains a XLSM file as shown below:

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compr
essed size: 335485, uncompressed size: 343693, name: Overdue_Debt_1577895391_06
012021.xlsm
335671        0x51F37         End of Zip archive, footer length: 22
```

Figure.3: *Binwalk analysis of the zip file*

The extracted XLSM file[3] is meant to be opened using Microsoft Office, displays the below content:

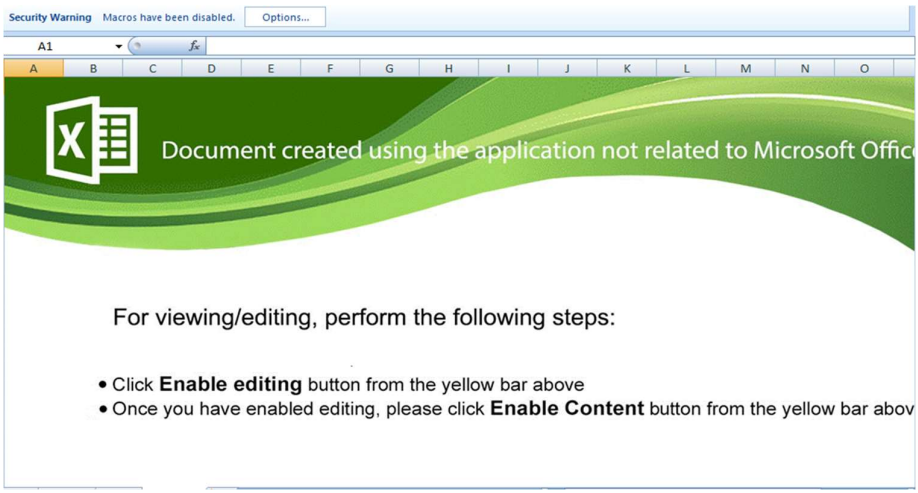


Figure.4: *Screenshot of the malicious excel file as seen from above*

[2] **Hash:** d9d964ab0dc7792c81df8f2b0fc08b532d73dc56eb98452e1ceb42933d69b6b3

[3] **Hash**: cf20e03d8b89cd17eb76f7f28db5d514baed57996d078aa21296acc15477de10

Microsoft disables Macros by default for such Security reasons which doesn't let the code run by just opening the file. The malicious actors, therefore, convince the target to explicitly enable the Macros as seen in the screenshot above. An **XLSM** file is a macro-enabled spreadsheet created by Microsoft Excel, analyzing it using the open-source tool developed by **@decalage2** gave the below result:

Indicator	Value	Risk	Description
File format	MS Excel 2007+ Macro-Enabled Workbook (.xlsm)	info	
Container format	OpenXML	info	Container type
Encrypted	False	none	The file is not encrypted
VBA Macros	No	none	This file does not contain VBA macros.
XLM Macros	Yes	Medium	This file contains XLM macros. Use olevba to analyse them.
External Relationships	0	none	External relationships such as remote templates, remote OLE objects, etc

Figure.5: *Oleid view of XLSM file showing the presence of XLM macros in it*

Unlike recently seen versions of QBot that make use of VBA Macros, this campaign adapted to XLM Macros as shown in the above screenshot. The XLSM file is made up of XML files that can be deobfuscated using the Open-Source tool developed by **@DissectMalware**.

The XML file **"Content_Types.xml"** described the initial structure of the XLSM file and following up with **"xl/workbook.xml"**, the details of the sheets is displayed as below:

"<Override PartName="/xl/workbook.xml" ContentType="application/vnd.ms-excel.sheet.macroEnabled.main+xml"/>"

```
<sheet name="Sheet" sheetId="2" r:id="rId1"/>
<sheet name="Sheet1" sheetId="13" r:id="rId2"/>
<sheet name="Sheet2" sheetId="14" r:id="rId3"/>
<sheet name="Pervi" sheetId="3" state="hidden" r:id="rId4"/>
<sheet name="Pervi2" sheetId="4" state="hidden" r:id="rId5"/>
<sheet name="sobr" sheetId="5" state="hidden" r:id="rId6"/>
<sheet name="sobr1" sheetId="6" state="hidden" r:id="rId7"/>
<sheet name="sobr2" sheetId="7" state="hidden" r:id="rId8"/>
<sheet name="sobr3" sheetId="8" state="hidden" r:id="rId9"/>
<sheet name="zap1" sheetId="9" state="hidden" r:id="rId10"/>
<sheet name="zap2" sheetId="10" state="hidden" r:id="rId11"/>
<sheet name="zap3" sheetId="11" state="hidden" r:id="rId12"/>
<sheet name="osn" sheetId="12" state="hidden" r:id="rId13"/>
```

Figure.6: *Hidden sheets in the XLSM file*

The above results show that there are multiple sheets but most of which are hidden and not displayed to the victim as shown below:

Figure.7: *Sheets visible to the victim*

Saptang Labs

Once the victim enables Macros following the **"Enable Editing"**, the auto-execution functionality starts working dynamically.

Figure.8: *XLMDeobsufucator output for the XLSM file*

The above screenshot depicts the call from URLmon.dll to URLDownloadFileToA to download files from three IPs:

- 190.14.37[.]113
- 101.99.95[.]206
- 51.195.38[.]41

The above IPs are used to host and distribute the **1st stage payloads** that are downloaded, renamed to **"Post.storg"**, and executed with the command:

"regsv32.exe -s ..\Post.storg"

The 1st stage payload is a malicious **DLL** file and dynamically loads the final Qbot Trojan payload into memory using DLL injection techniques.

Analysing the Dropper:

The dropped .dat(renamed to Post.storg) file[4] is compiled with Borland Delphi Compiler and has import functions such as **VirtualAlloc(), LoadLibrary(), WriteFile(),** and **RegQueryValue()** all of which are commonly observed in malwares while doing DLL injection and Registry tampering.

The first stage payload is responsible for creating persistence in the system and auto-running after every Restart of the system. The final payload is dropped and executed by this payload which is seen in the **"Dump 3"** from the below figure:

The **"Dump 3"** is the main Qbot Trojan payload that is written to a file as **"stager_1.dll"**

[4] **Hash**: 7cf30ffdb463a48d4148aa2aaa5d2cbe54502b9978642136f703c10d712ab33f

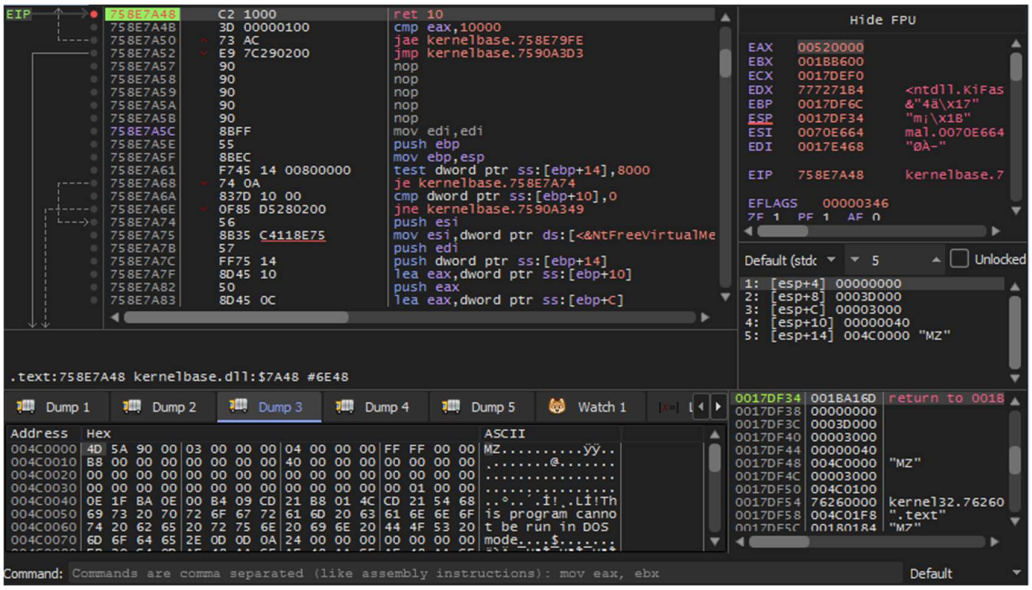


Figure.9: *Dumping the main Qbot Trojan in the Memory*

Analysing the Payload

The main payload[5] is compiled using C/C++ and has a single export function - **"DLLRegisterServer".**

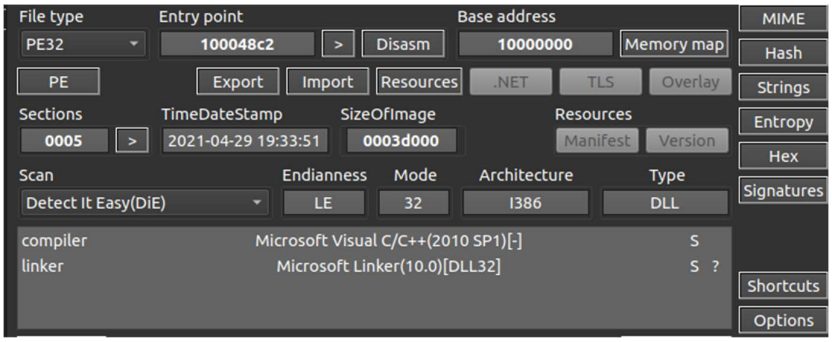


Figure.10: *DIE tool view showing the overview of QBot Trojan*

Analyzing using PE-Bear, the Open-Source tool developed by @hashzerade

Offset	Name	Value	Meaning
36240	Characteris...	0	
36244	TimeDateS...	608ABCC6	Thursday, 29.04.2021 14:03:50 UTC
36248	MajorVersion	0	
3624A	MinorVersion	0	
3624C	Name	37472	stager_1.dll
36250	Base	1	
36254	NumberOf...	1	
36258	NumberOf...	1	

Exported Functions [1 entry]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
36268	1	4407	3747F	DllRegister...	

[5] **Hash:** 855ff14330f4a4e5924fa97b9a51211787f9a9b448250e3db28322563239cd6e

Figure.11: *Exports and Characteristics view for the Qbot Trojan in PE-bear*

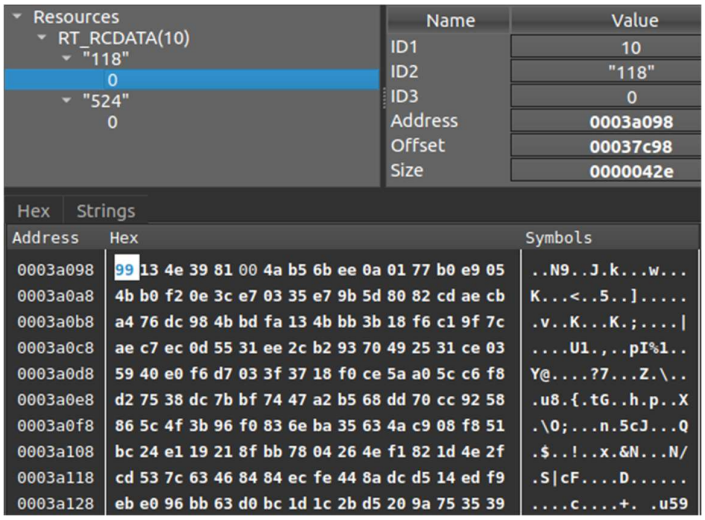


Figure.12: *The. rsrc **section** of the payload contains two indexes: "118" and "524"*

The contents of the indexes are RC4 encrypted ciphertext

- "118" - Command & Control server's IP address and Port information
- "524" - Botnet configuration file

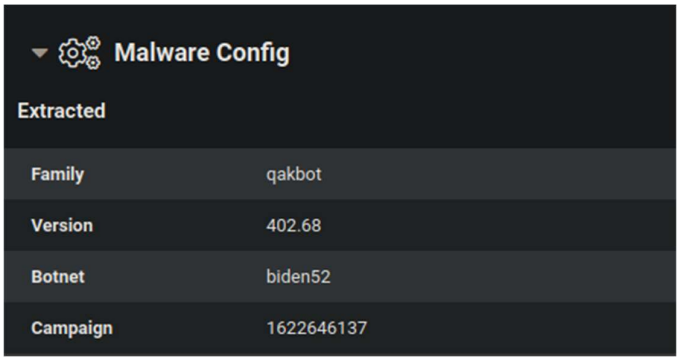
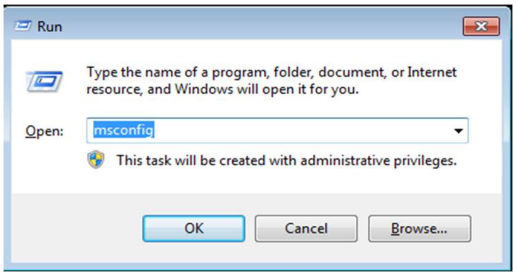


Figure.13: *The Botnet configuration file for biden52*

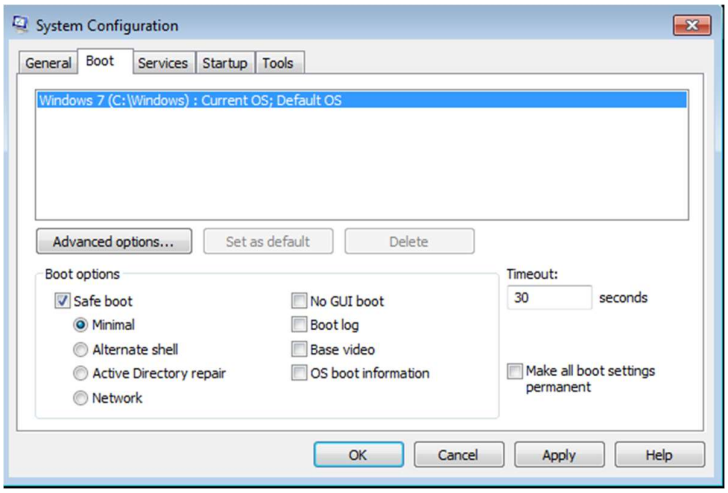
Remediation

Step.1) The infected computer should be booted in Safe Mode by following the below-mentioned steps:

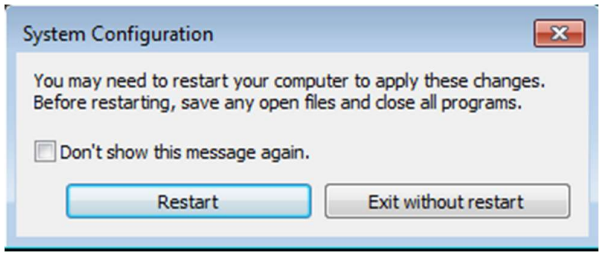
1.1) Press “Windows key + R” that opens the Run tool and Enter “msconfig”



1.2) Navigate to the “Boot” tab in the System Configuration tool and click on the checkbox “Safe Boot” and press OK



1.3) Click on the Restart option to boot into safe mode

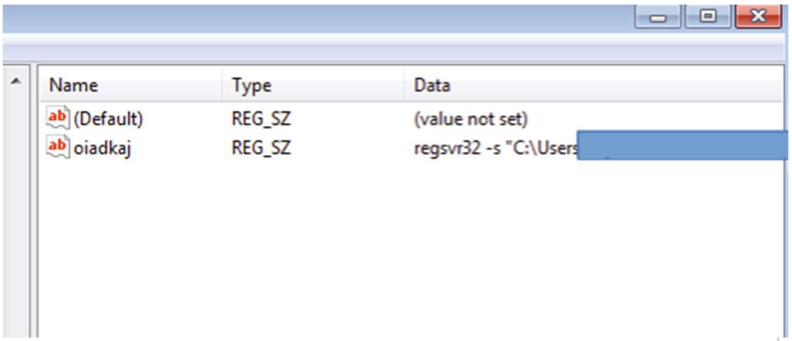


Step.2) In order to defend against the persistence created by the Trojan, the following steps should be followed:

2.1) To create persistence, by auto-execution at startup without user interaction, the Qbot creates a registry key as one of the mentioned below:

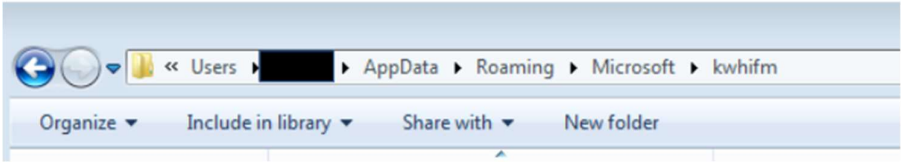
"HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run"
"HKEY_CURRENT_USER\Microsoft\Windows\CurrentVersion\Run"

The name consists of some "random characters" and data contains the command to run the Trojan at startup.



2.2) The trojan is a DLL file that is stored as seen in the above image at:

"C:\Users\{user}\AppData\Roaming\Microsoft\{random name}\{random}.dll



2.3) Navigate to the above-seen location and delete the Trojan and remove the Registry key created by the Qbot Trojan.

Conclusion

This research confirms that all bad actors are now gearing towards targeting perceived low risk and medium to high gain jurisdictions. India figures out among the top of the list. This calls for increasing policy importance to the Critical Information Infrastructure (CII) and its supply chain. It may be noted that defence of the critical information infrastructure is only as strong as its weakest link. We want to thank our intern **Shreesh Roliwal** for his key contribution to this research.

Simple policy advice could be to ensure that the vendors and suppliers of critical information infrastructure should be directed to adhere to the same security standards prescribed for the CIIs. Data about the campaign would be shared with the agencies and fellow cyber researchers. Please feel free to reach out to us at tushar@saptanglabs.com

Saptang Labs

References

To read other coverages of Qbot attacks from the past, refer to the links below:

- https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/
- https://securityaffairs.co/wordpress/117558/cyber-crime/qakbot-latest-release.html
- https://blog.vincss.net/2021/03/re021-qakbot-dangerous-malware-has-been-around-for-more-than-a-decade.html
- https://blog.cyberint.com/qakbot-banking-trojan
- https://n1ght-w0lf.github.io/malware%20analysis/qbot-banking-trojan/

List of Indicators of Compromise (IOCs):

XLSM file Hashes

- cf20e03d8b89cd17eb76f7f28db5d514baed57996d078aa21296acc15477de10
- f202c64f338d6815bde2a4a1a7946e5b037359e3701c1e7f90db31273e0cbf42
- cc9d719a9329627c13d44231374440e156eb7afb3be933d31f6767eafb65f2cd
- eec75f6090d0b4aafba01dc07c5a90a86a3a6221745387db9664511b7f4b83da
- a631dfa6707d85e26337da2e16a6358402a53329610952ff6e5a9f2bef74dca4
- df5037621d597247be2765dcd8e3dbf799c7a4bf051451150b9cc069a1b0b74c
- 01a7ec6f72ae8d9b4d53487763fe0679fe18672b9eefd105e8a72a3bc7c51e05
- 9631385508917c670f57f1225ddb43d8e3bd92f1db74e30fe6ce9841a4a52f1a
- b39cf2cddf259d3f226561747cd1386186fa6bf91e51d5e98071d9a8a1c9145f
- 0162ad73634f616f0dac77e09a032aba720c306efcdfb838ff122763eb02c95d
- d9ec7792072681636567594b980cd574bd0e69956c1ba10ffee41468f1e126d4

IP addresses

184.185.103.157:443	149.28.99.97:2222	86.173.143.211:443
71.187.170.235:443	149.28.99.97:443	47.196.213.73:443
86.220.62.251:2222	149.28.99.97:995	45.46.53.140:2222
75.67.192.125:443	45.63.107.192:995	186.154.175.13:443
96.61.23.88:995	97.69.160.4:2222	70.163.161.79:443
92.96.3.180:2078	83.196.56.65:2222	24.95.61.62:443
72.252.201.69:443	72.240.200.181:2222	78.63.226.32:443
24.152.219.253:995	75.137.47.174:443	195.6.1.154:2222
105.198.236.101:443	188.26.91.212:443	76.168.147.166:993
24.179.77.236:443	68.186.192.69:443	64.121.114.87:443
189.210.115.207:443	140.82.49.12:443	77.27.207.217:995
81.97.154.100:443	24.55.112.61:443	31.4.242.233:995
47.22.148.6:443	90.65.234.26:2222	125.62.192.220:443

Saptang Labs

45.77.115.208:443	24.229.150.54:995	195.12.154.8:443
149.28.98.196:443	95.77.223.148:443	71.117.132.169:443
45.77.115.208:2222	122.58.117.81:995	96.21.251.127:2222
144.202.38.185:995	197.45.110.165:995	71.199.192.62:443
45.77.115.208:8443	50.29.166.232:995	70.168.130.172:995
207.246.77.75:8443	71.74.12.34:443	82.12.157.95:995
207.246.77.75:443	27.223.92.142:995	209.210.187.52:995
144.202.38.185:2222	144.139.47.206:443	209.210.187.52:443
45.77.117.108:995	50.244.112.106:443	67.6.12.4:443
149.28.98.196:995	76.25.142.196:443	189.222.59.177:443
149.28.101.90:443	75.118.1.141:443	174.104.22.30:443
149.28.98.196:2222	98.252.118.134:443	142.117.191.18:2222
45.32.211.207:995	98.192.185.86:443	189.146.183.105:443
144.202.38.185:443	67.165.206.193:993	213.60.147.140:443
92.59.35.196:2222	109.12.111.14:443	196.221.207.137:995
207.246.77.75:2222	190.85.91.154:443	108.46.145.30:443
45.77.115.208:995	175.136.38.142:443	187.250.238.164:995
45.77.117.108:443	83.110.108.161:2222	2.7.116.188:2222
149.28.101.90:8443	100.2.123.234:443	195.43.173.70:443
149.28.101.90:2222	105.198.236.99:443	106.250.150.98:443
207.246.116.237:443	81.214.126.173:2222	45.67.231.247:443
207.246.77.75:995	68.204.7.158:443	83.110.103.152:443
45.32.211.207:2222	151.205.102.42:443	83.110.9.71:2222
216.201.162.158:443	149.28.101.90:995	78.97.207.104:443
73.151.236.31:443	207.246.116.237:8443	59.90.246.200:443
173.21.10.71:2222	207.246.116.237:995	80.227.5.69:443
71.41.184.10:3389	45.77.117.108:2222	125.63.101.62:443
136.232.34.70:443	45.32.211.207:443	86.236.77.68:2222
76.94.200.148:995	45.32.211.207:8443	109.106.69.138:2222
71.63.120.101:443	45.77.117.108:8443	84.72.35.226:443
196.151.252.84:443	207.246.116.237:2222	217.133.54.140:32100
202.188.138.162:443	45.63.107.192:2222	197.161.154.132:443
74.68.144.202:443	45.63.107.192:443	89.137.211.239:995
69.58.147.82:2078	172.78.18.142:443	74.222.204.82:995
	96.37.113.36:993	122.148.156.131:995
	24.122.166.173:443	156.223.110.23:443
	73.25.124.140:2222	144.139.166.18:443
	71.163.222.223:443	202.185.166.181:443
	24.139.72.117:443	