Qakbot Resurges, Spreads through VBS Files

Insights and Analysis by Erika Mendoza, Ian Lagrazon, and Gilbert Sison
Additional Analysis by Miguel Ang, Monte De Jesus, Jesus Titular, Catherine Loveria

Through managed detection and response (MDR), we found that a lot of threats come from inbound emails. These messages usually contain phishing links, malicious attachments, or instructions. However, in our daily investigation of email metadata, we often detect threats not just in inbound emails, but even in the users' own sent items folder. This involves an unwitting user, a possibly compromised account, and harmful messages carrying threats. In one such incident, we have been able to correlate email compromise with the intent to spread Qakbot-related email messages.

We have seen events that point to the resurgence of Qakbot, a multi-component, information-stealing threat first discovered in 2007. Feedback from our sensors indicates that Qakbot detections increased overall. A notable rise in detections of a particular Qakbot sample (detected by Trend Micro as Backdoor.Win32.QBOT.SMTH) was also witnessed in early April. Note that we used a partial and inexhaustive list of indicators for this analysis.

Background of detections for all Qakbot variants

From January to the third week of May this year, we had a total of 3,893 unique Qakbot detections. We've seen a spike in January with over 1,400, which mellowed down in February and March. It climbed back in April with over 1,000. Data for May is also quite high at 679, considering that the month has not ended yet.

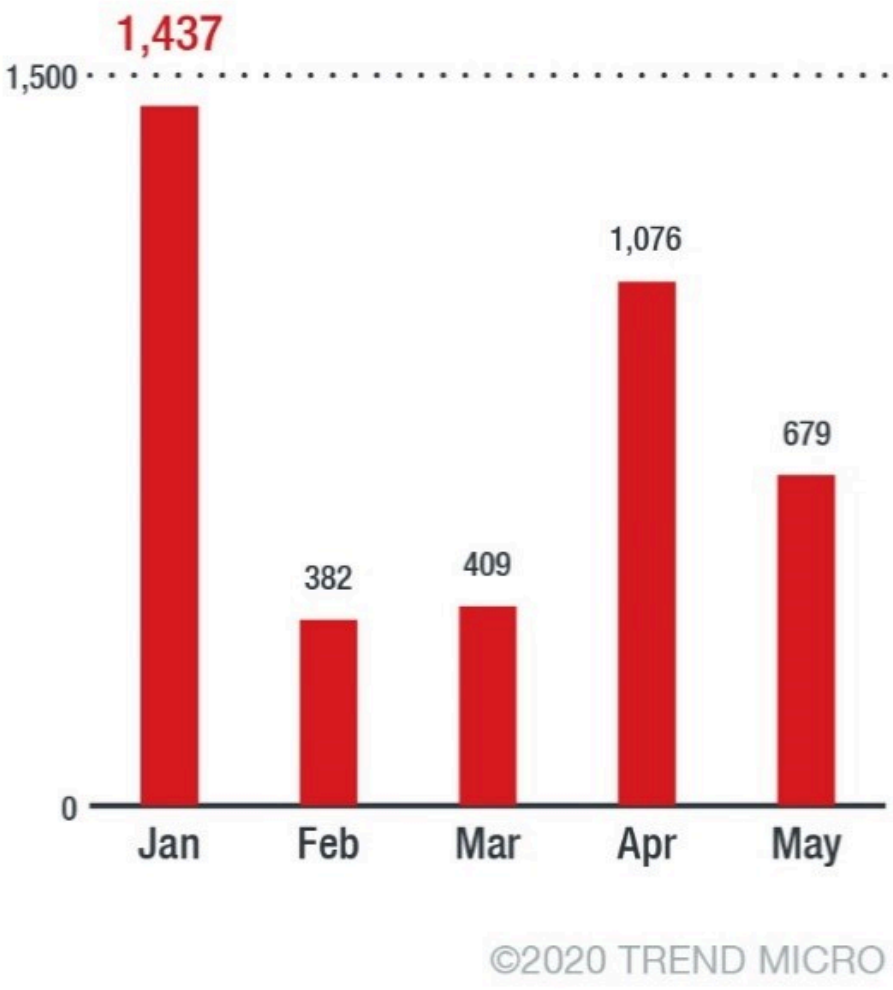


Figure 1. Unique Qakbot detections from January to May 2020

Among the specified and known industries, healthcare was the most affected with 256 unique detections from the same period, followed by manufacturing and government with 161 and 60, respectively. These three consistently appeared on the top of the list in most months.

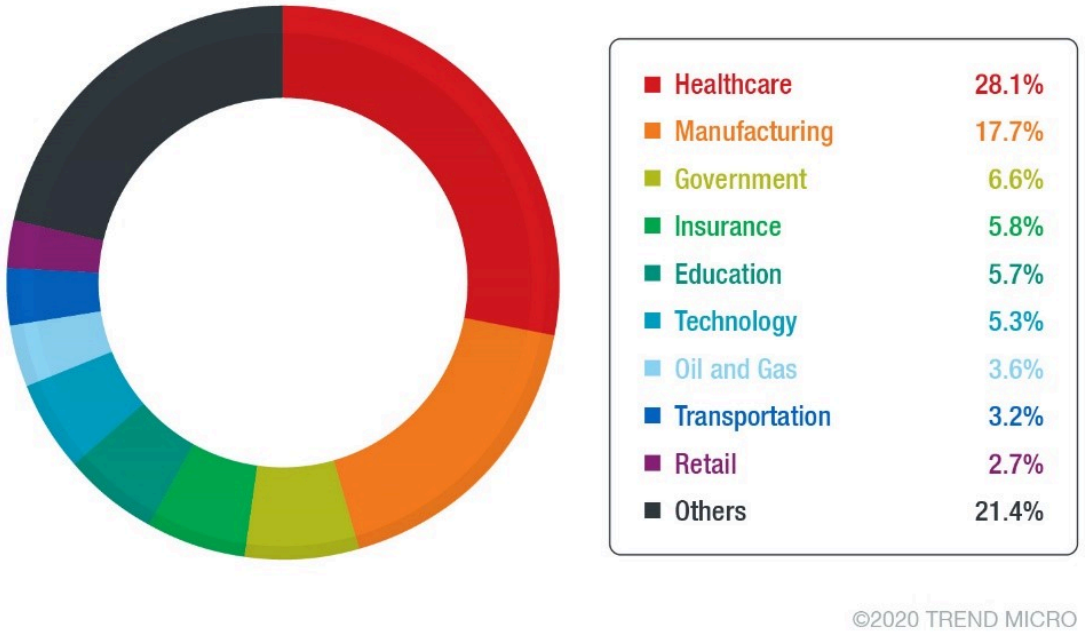


Figure 2. Top industries for unique Qakbot detections from January to May 2020

In terms of the countries of affected users, Thailand had the most unique detections at 939, with most detected in January. China followed closely with 908, while the US was third at 688. China and the US have been consistently in the top three for all months. In January, Thailand had the highest number of unique detections while the United States was mostly affected in April. In May, we see a surge in number from Germany.

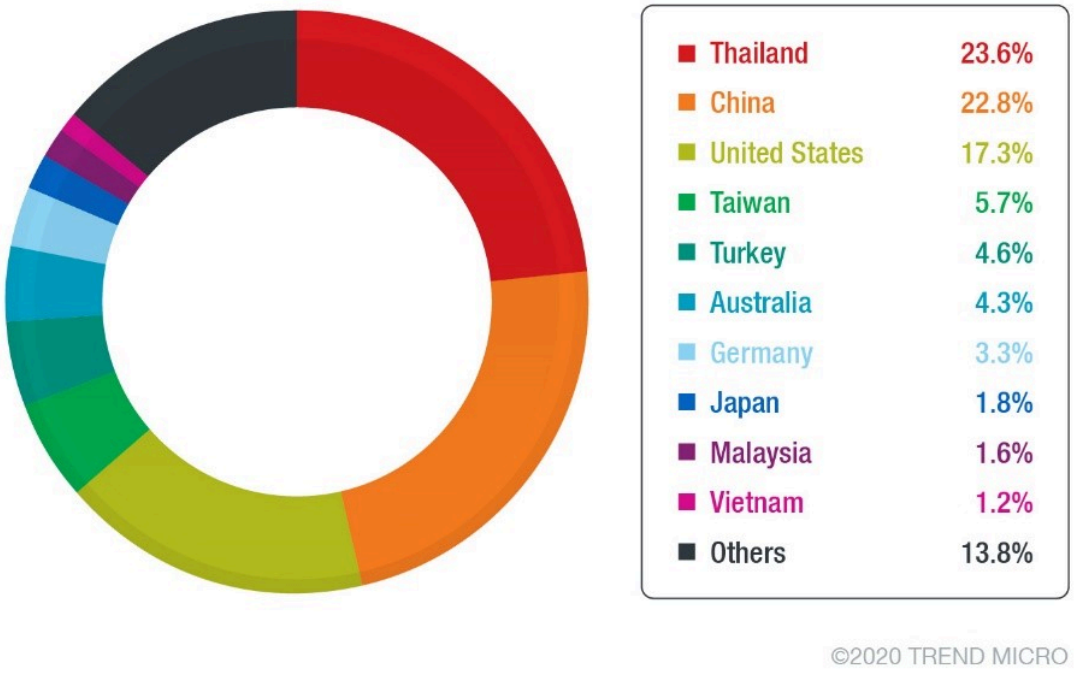


Figure 3. Top countries for unique Qakbot detections from January to May 2020

Detections for Backdoor.Win32.QBOT.SMTH Qakbot variant

After inactivity since the beginning of this year, unique detections for Backdoor.Win32.QBOT.SMTH trickled in since April 9. Among 434 unique detections, the highest came within the period of April 19-23. April 22 had the highest number at 91.

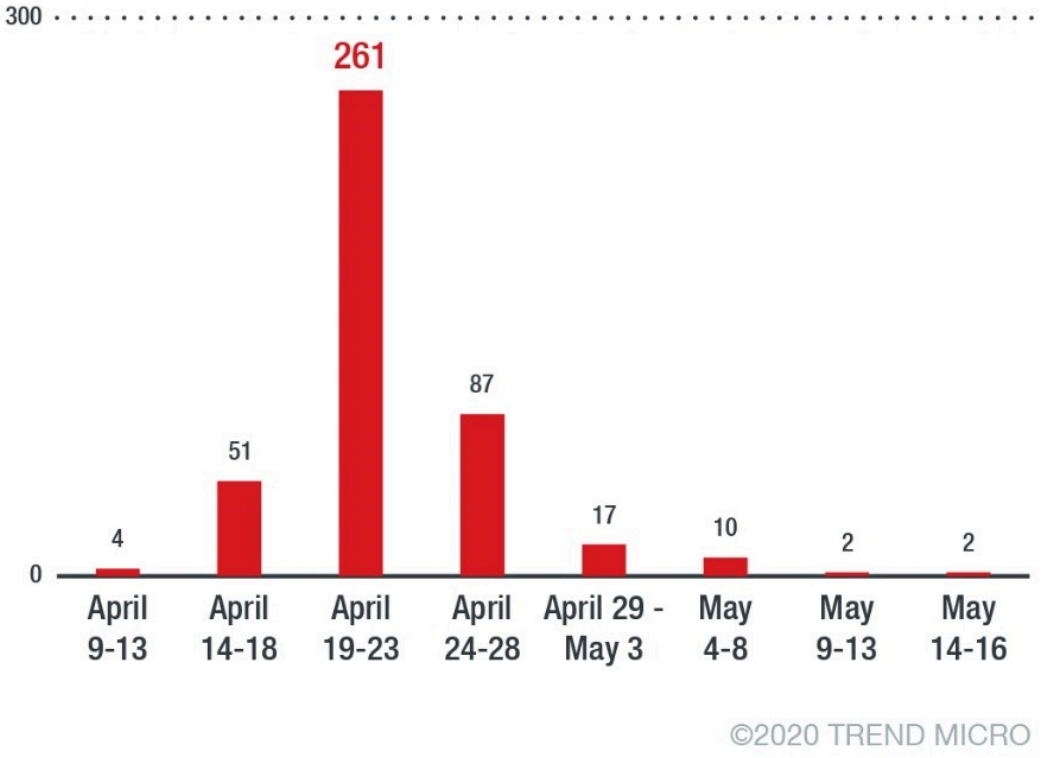


Figure 4. Unique detections of the Qakbot variant from April 21 to May 16, 2020

Among users with specified and known industries, the rise had been observed mostly in the healthcare sector with 141 unique detections.

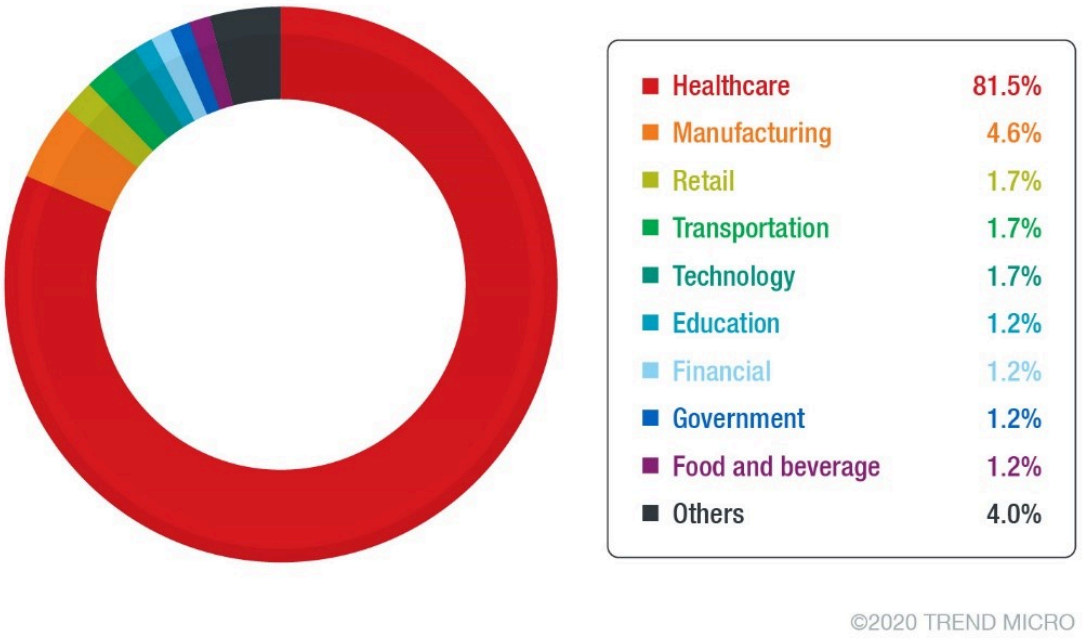


Figure 5. Industries with unique detections of the Qakbot variant

233 or almost half of the recorded unique detections have been seen affecting users from the US. Australia and China follow with 95 and 30, respectively.

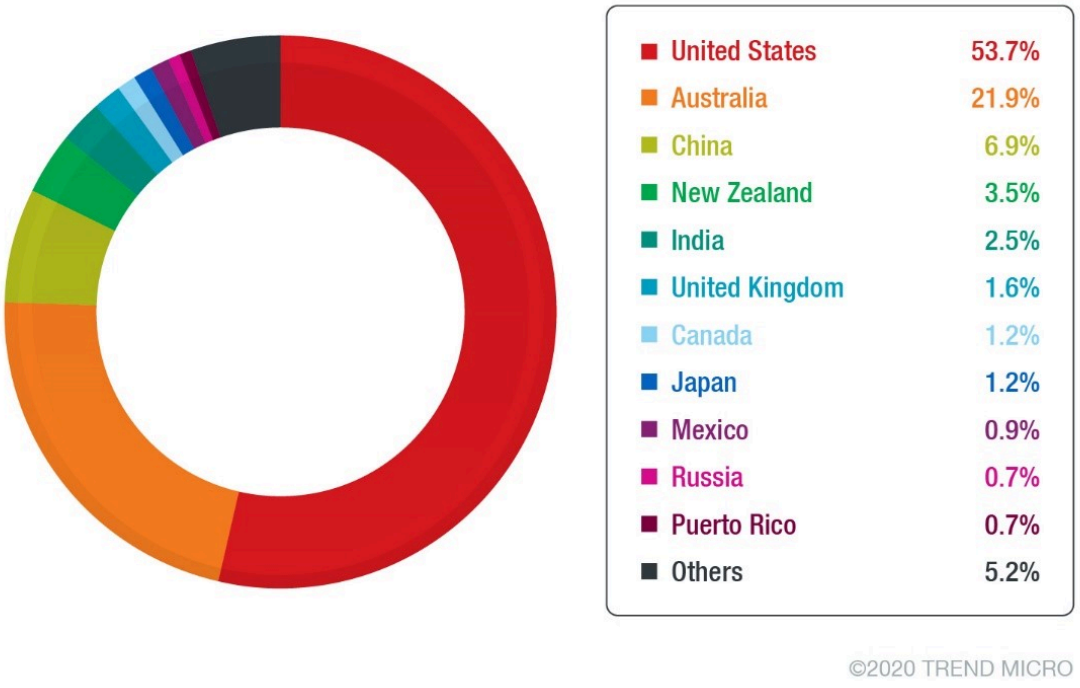


Figure 6. Top countries with unique detections of the Qakbot variant

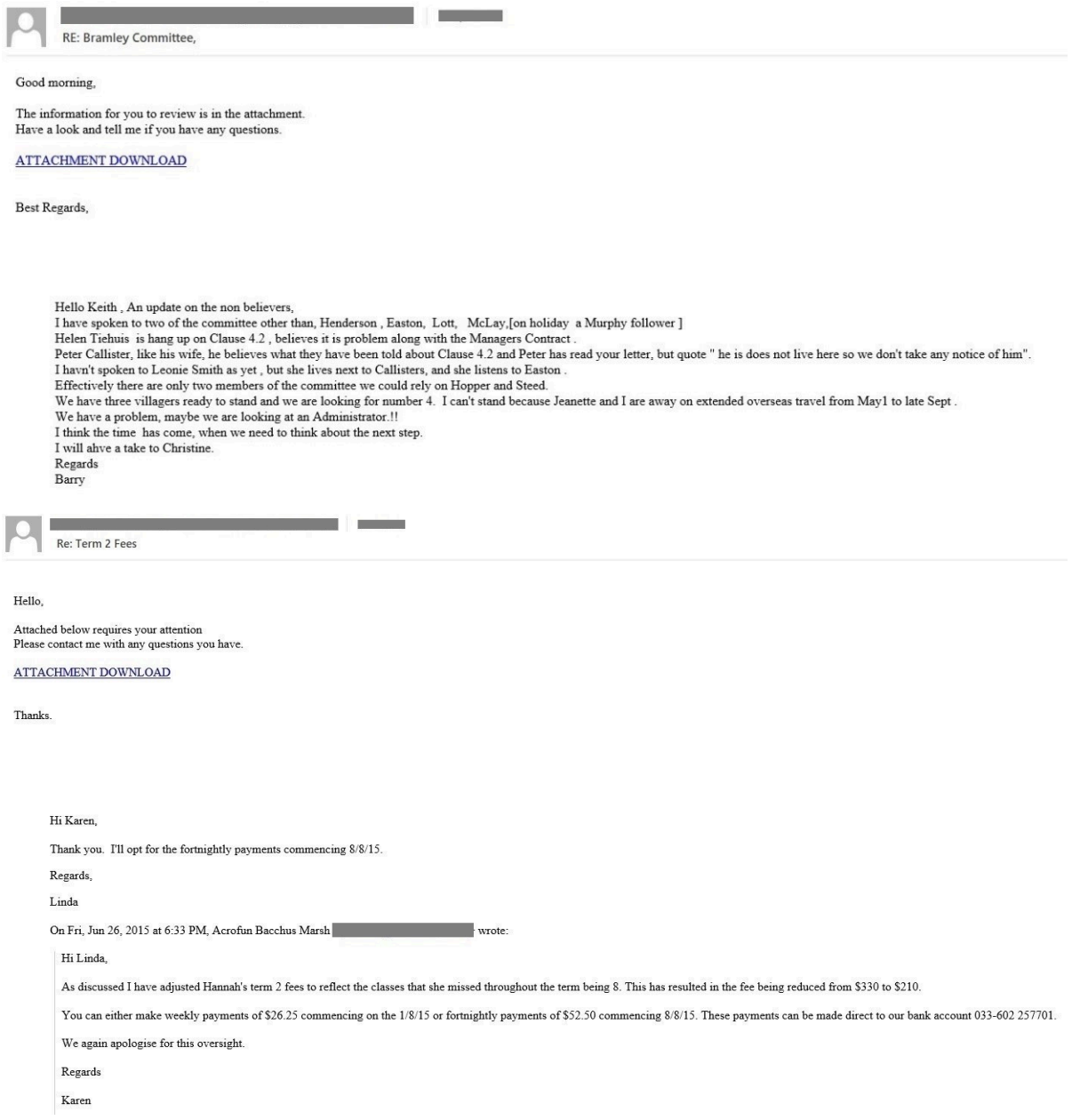
The malware has been known to proliferate through network shares, removable drives, or software vulnerabilities. The recent instances we have observed were spread through emails with malicious links. Clicking the link leads to the download

of a zip containing a VBS file (detected as Trojan.VBS.QAKBOT.SM) that then downloads a malicious executable file (detected by Trend Micro as Backdoor.Win32.QBOT.SMTH).

The new samples are similar to older variants in terms of behavior and encryption. Like its earlier versions, it maintains persistence by creating an auto-run registry and scheduled task.

Proliferation and Behavior of the Qakbot Variant

This Qakbot variant spreads via emails with malicious links pointing to compromised websites hosting the Qakbot malware. The emails look like old forwarded messages that pose as replies to relevant business-related email threads. Often, the sender's name and email address don't match.



Figures 7-8. Sample emails with malicious links that lead to the download of Qakbot

The emails contain URLs that follow noticeable pattern, as seen below:

- {compromised website}/differ/ ...
- {compromised website}/docs_{3 characters}/{numbers} …

- {compromised website}/wp-content/plugins/advanced-ads-genesis/docs_{3 characters}/ …
- {compromised website}/wp-content/themes/calliope/docs_{3 characters}/ …
- {compromised website}/wp-content/themes/mapro/pump/ ...
- {compromised website}/wp-content/uploads/2020/04/evolving/ …

Clicking the link will download a zip file. Like the URLs, the file names follow a particular pattern:

- {numbers}.zip
- Buy-Sell Agreement_{numbers}_{date}.zip
- Judgement_{date}_{numbers}.zip

The more recent spam mails this month use this file name pattern instead:

- EmploymentVerification_{numbers}_{date}.zip
- LoanAgreement_{numbers}_{date}.zip

In one sample we analyzed, the zip file contains a VBS file named NUM_56960.vbs. The size of the file is around 30MB. The large file size helps it evade detection, as file scanners usually skip scanning huge files for performance reasons. This VBS file then downloads the malicious executable file PaintHelper.exe.

Qakbot has anti-analysis and anti-virtual machine checks. It will not continue to execute if any of the following exists in the system:

Analysis Tools

- AvastSvc.exe
- avgcsrva.exe
- avgsvcx.exe
- avp.exe
- bdagent.exe
- ByteFence.exe
- ccSvcHst.exe
- cmdagent.exe
- coreServiceShell.exe
- egui.exe
- ekrn.exe
- fmon.exe
- fshoster32.exe
- isesrv.exe
- mbamgui.exe
- MBAMService.exe
- mcshield.exe
- MsMpEng.exe
- NTRTScan.exe
- PccNTMon.exe
- SAVAdminService.exe
- SavService.exe
- vgcsrvx.exe
- vkise.exe
- vsserv.exe
- vsservppl.exe
- windump.exe

- WRSA.exe

Sandbox

- CWSandbox
- QEMU
- SbieDll.dll
- VBox
- Vmtoolsd.exe
- VMWare

Once it continues, it creates a folder for its components in %AppData%\Microsoft\{random name}\. It then proceeds by copying itself to %AppData%\Microsoft\{random name}\{random}.exe then creates a corresponding auto-run.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

{random} = %APPDATA%\Microsoft\{random name}\{random}.exe

It also creates a scheduled task through the following:

- "C:\Windows\system32\schtasks.exe" /create /tn {8BAD047B-4889-4161-9D32-63F25CBFC779} /tr ""{Malware Path}\{malware name}"" /sc HOURLY /mo 5 /F

Copies of the malware are also placed in other locations:

- %ProgramData%\{random}.exe
- %TEMP%\{random}.exe
- %User%\{random.exe}

After installation, Qakbot injects itself into any of the following processes to remain memory resident.

- explorer.exe
- Iexplore.exe
- Mobsync.exe

It has both domain generation algorithms (DGA) and a couple of hardcoded C&C servers. The DGA routine works by trying to access random IP and port combinations and continues into a POST command once it makes a successful connection.

Its code also suggests a PowerShell routine that allows it to download other components, as also seen in older variants. This means that its routines (other than installation) are loaded through another component, usually downloaded from the C&C server.

Like other malware types, Qakbot is periodically updated, giving it improved propagation techniques in 2011 and a resurgence in 2016. It has also been seen to include Simple Mail Transfer Protocol (SMTP) activities and use Mimikatz. Recently, Qakbot has been seen teaming up with ProLock ransomware.

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.

From their end, users can protect themselves from the new Qakbot samples and other threats spread through emails by following some of these best practices:

- Avoid downloading attachments or clicking on 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 name, 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.

Indicators of Compromise

URL

- hxxps://besthack[.]co/differ/50160153/50160153[.]zip
- hxxps://besthack[.]co/differ/886927[.]zip

File Name	SHA-256	Trend Micro Pattern Detection
NUM_56960.vbs	166442aca7750b45d10cdbdb372dd336a730a3033933a2a0b142d91462017fd2	Trojan.VBS.QAKBOT.SM
Painthelper.exe	b8b7b5df48840b90393a702c994c6fb47b7e40cfe3552533693149d9537eaef5	Backdoor.Win32.QBOT.SM

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
