

DarkCloud Infostealer Being Distributed via Spam Emails

By ATCP

Published: 2023-05-16 · Archived: 2026-04-05 22:51:41 UTC



AhnLab Security Emergency response Center (ASEC) has recently discovered the DarkCloud malware being distributed via spam email. DarkCloud is an Infostealer that steals account credentials saved on infected systems, and the threat actor installed ClipBanker alongside DarkCloud.

1. Distribution Method

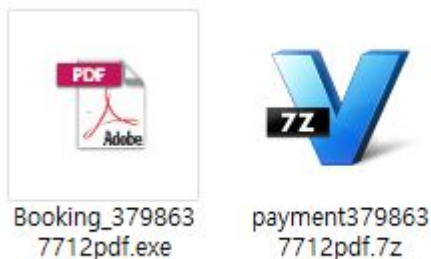
The threat actor sent the following email to induce users to download and execute the attachment.



Good Morning,
We were instructed by your costumer this morning to transfer this payment =o your company account.
Kindly confirm the swift payment copy attached.
Best Regards



The contents of this email prompt users to check the attached copy of the payment statement sent to the company account. When the attachment is uncompressed, normal users are likely to execute the contained malware as it is disguised with a PDF icon.



The file attached to the email is a dropper that is responsible for generating and executing DarkCloud and ClipBanker. If a user downloads the attached file in the email and executes it after decompressing, various account credentials present on the infected system can be stolen. Additionally, if the user copies a cryptocurrency wallet address to their clipboard, there is a risk of it being replaced with the threat actor’s address, resulting in funds being sent to the threat actor’s wallet during transactions.

2. Malware Attachment

The file attached to the email is a dropper that first copies itself to the %APPDATA%\Zwldpcobpfq\Gdktnpm.exe path before registering itself to the Run key so that it can operate even after reboots. Afterward, it generates and executes two individual malware in the %TEMP% path.

2.1. ClipBanker

“Lilgghom.exe”, which is the first malware generated and executed, is the ClipBanker. ClipBanker resides on the system and, when the user copies a Bitcoin or Ethereum cryptocurrency wallet address, it replaces it with the threat actor’s wallet address. A coin wallet address normally has a certain form, but it is difficult to memorize as the string is long and complicated. Hence, users are likely to copy and paste the address when using it. Should the

wallet address change at this stage, users who want to deposit money to a certain wallet may end up depositing it to a different wallet because the address is changed to that of the attacker’s wallet.

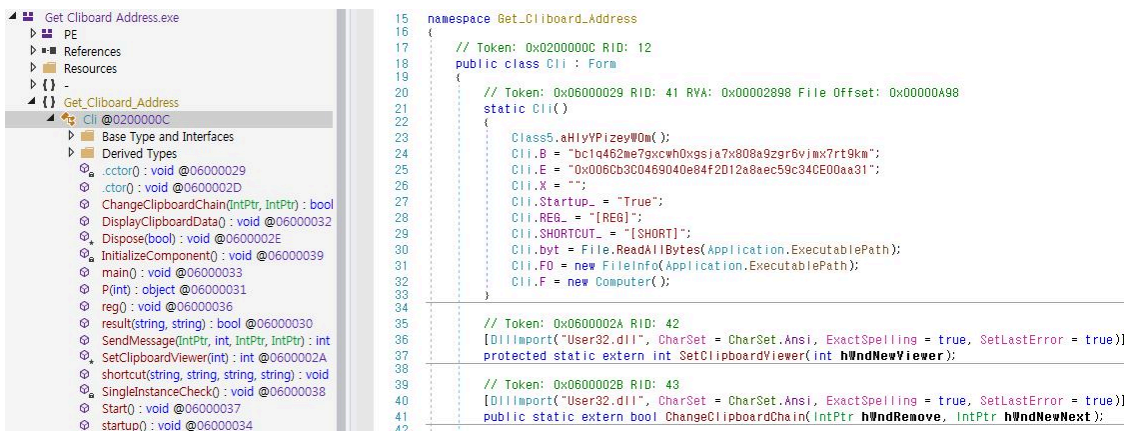
The ClipBanker used in the attack was created under the name “Get Cliboard Address.exe” and monitors the clipboard. When an entry that matches the following regular expressions is saved, it is changed to the wallet address defined by the threat actor.

- Bitcoin: “(?<!\w)[a-zA-Z0-9]{34}(?!\\w)”
- Ethereum: “(?<!\w)0x[a-zA-Z0-9]{40}(?!\\w)”
- Monero: “(?<!\w)[a-zA-Z0-9]{95}(?!\\w)”

Additionally, “Get Cliboard Address.exe” supports various features according to its configuration.

Configuration	Description	Data
B	Bitcoin wallet address to change	bc1q462me7gxcwh0xgsja7x808a9zgr6vjmx7rt9km
E	Ethereum wallet address to change	0x006Cb3C0469040e84f2D12a8aec59c34CE00aa31
X	Monero wallet address to change	N/A
Startup	Copy to the Startup folder	True
REG	Register to the Run key	False
SHORTCUT	Create a shortcut in the Startup folder	False

Table 1. Configurations provided by ClipBanker



2.2. DarkCloud

The malware “Ckplomlg.exe” that is generated and executed next functions as an Infostealer, responsible for collecting and stealing various user credentials stored on the infected system. Different from the other malware that have recently been in distribution, this malware was developed with the VB6 language.

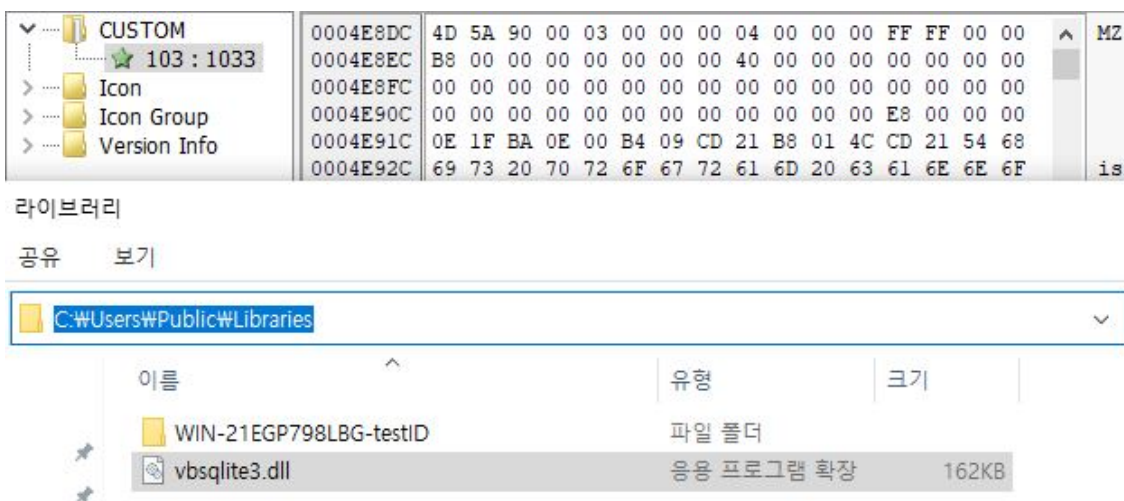
Like the average Infostealer, DarkCloud steals the account credentials of users that have been saved on web browsers, FTP, and email clients. It is also similar to other Infostealers like AgentTesla and SnakeKeylogger as it uses SMTP or the Telegram API to send the collected information to the C&C server.

Additionally, the DarkCloud being analyzed in this post cannot be logged into as the threat actor’s SMTP account credentials were changed. However, the presence of the AgentTesla malware using the same email account in the past suggests that the threat actor may have used not only DarkCloud but also the AgentTesla Infostealer in their spam email attack campaigns.

- **Host:** logxtai[.]shop
- **User:** sender-a3@logxtai[.]shop
- **Password:** f9;2H%A)IpgE
- **Receiver:** ambulancelog@logxtai[.]shop

```
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXN1cm5hbWU6
c2VuZGVyLWEzQGxvZ3h0YWkuc2hvcA==
334 UGFzc3dvcmQ6
Zjk7Mkg1QS1JcGdF
535 Incorrect authentication data
421 server197.web-hosting.com lost input connection
```

DarkCloud has “vbsqlite3.dll” within its resources section which is necessary for collecting account credentials, and it is generated and loaded in the “%PUBLIC%\Libraries” path while DarkCloud is running.



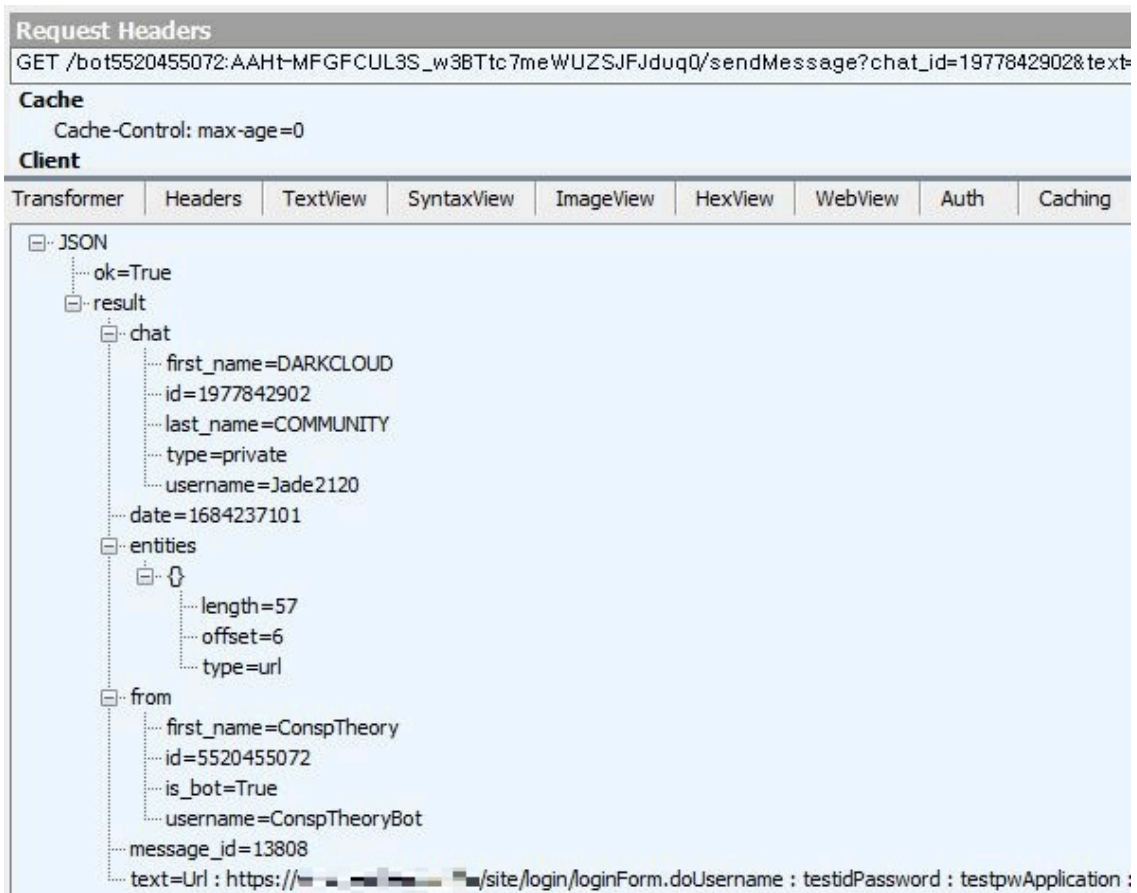
Account credential information is exfiltrated from Chromium and Firefox-based web browsers, email clients such as Outlook, ThunderBird, and FoxMail, and FTP client programs such as CoreFTP and WinSCP. Of course, a variety of other user information can be stolen besides these such as credit card information stored on browsers.

The image shows a debugger window with assembly code on the left and a hex dump on the right. The assembly code includes instructions such as MOV, LEA, CALL, and PUSH. The hex dump shows the ASCII string "ELECT name on card expiration year".

The stolen information is stored in a folder generated within the “%PUBLIC%\Libraries” path. As shown below, “DARKCLOUD” can be confirmed on the signature string of the stolen information.

The image shows a Windows file explorer window displaying a folder named "WIN-21EGP798LBG-testID". The folder contains files like "LogboondoggledMOzzGvNquOYfwZSItLqXBzHXvyvoYwtMrjVLzdzQZfitroot", "WebData", and "WIN-21EGP798LBG-testID.txt". A preview window is open for "WIN-21EGP798LBG-testID.txt", showing a URL, username, password, application, and a signature string "====DARKCLOUD===== ".

The DarkCloud being analyzed here uses both the SMTP protocol and the Telegram API when exfiltrating the collected information.



3. Conclusion

Users must practice strict caution when handling attachments in emails from unknown sources or executables downloaded from the web. It is advised to download products including utility programs and games from their official websites.

Users should also apply the latest patch for operating systems and programs such as internet browsers, and update V3 to the latest version to prevent malware infection in advance.

File Detection

- Trojan/Win.Generic.C5416010 (2023.04.21.01)
- Trojan/Win.Generic.R578585 (2023.05.16.02)
- Malware/Win32.RL_Generic.C4250411 (2020.12.04.01)

Behavior Detection

- Infostealer/MDP.Behavior.M1965

MD5

7c4f98ca98139d4519dc1975069b1e9f

9441cbed94f0fd5b20999d8e2424ce4

991a8bd00693269536d91b4797b7b42b

Additional IOCs are available on AhnLab TIP.

URL

[https://api.telegram.org/bot5520455072\[:AAHt-MFGFCUL3S_w3BTtc7meWUZSJFJduq0/sendMessage](https://api.telegram.org/bot5520455072[:AAHt-MFGFCUL3S_w3BTtc7meWUZSJFJduq0/sendMessage)

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/53128/>