Matanbuchus Loader Resurfaces

blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/

June 23, 2022

Malware Variant Delivering Cobalt Strike Beacons via Spam Campaigns

Researchers discovered that Matanbuchus, a malware loader, was available on Russian-speaking cybercrime forums for a rental price of $2500 from February 2021.

Recently, Cyble Research Labs came across a Twitter post where a researcher observed this malware spreading through spam campaigns. Additionally, it downloads Cobalt Strike Beacons as payloads in compromised systems. Figure 1 shows the infection chain of the Matanbuchus malware.

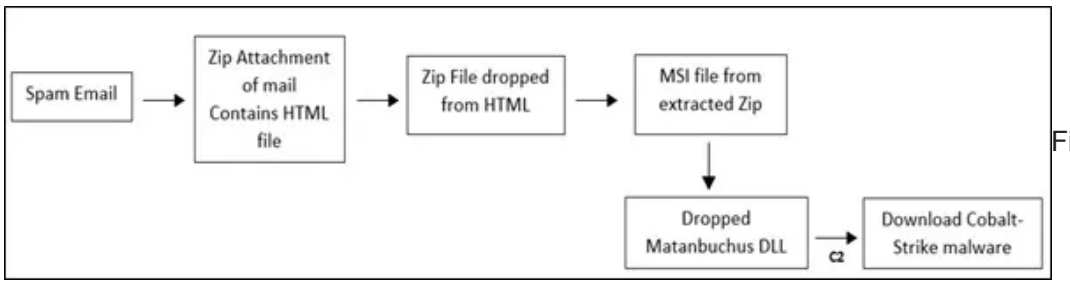

Figure 1 – Infection Chain of Matanbuchus

The Matanbuchus infection starts through spam emails containing a ZIP attachment. This ZIP attachment contains an HTML file.

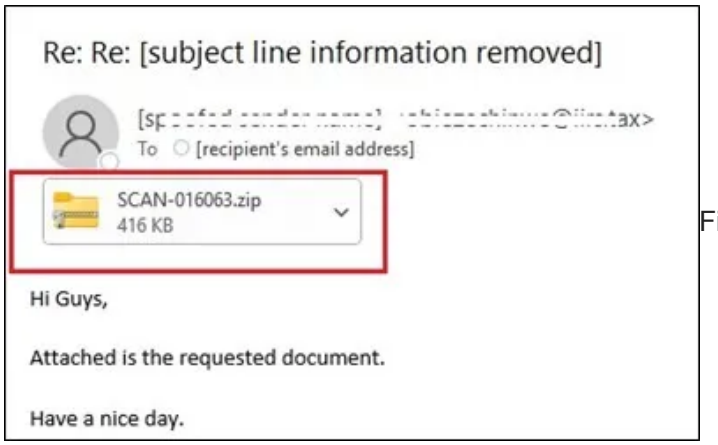

Figure 2 – Spam Email with ZIP Attachment

Upon executing the HTML file, it decodes the base64 content embedded in the file and drops a ZIP file in the *Downloads* folder.

However, there is a code present in the HTML file which shows that the ZIP file is in the *OneDrive* location, as shown below.

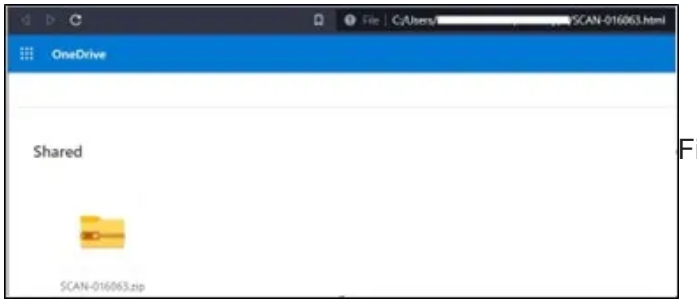

Figure 3 – ZIP Attachment in HTML Page

The ZIP file contains an MSI installer file. After extraction, it shows a fake error message upon the execution of the MSI file, as shown below.

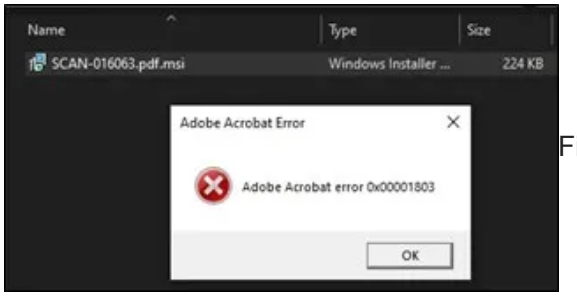

Figure 4 – Adobe Fake Error Message

However, in the background, the MSI installer drops a Dynamic Link Library (DLL) and VBS file in the following locations.

- *C:\Users\<Admin>\AppData\Local\AdobeFontPack\main.dll*
- *C:\Users\<Admin>\AppData\Local\AdobeFontPack\notify.vbs*

The malware uses the VBS file to show fake error messages.

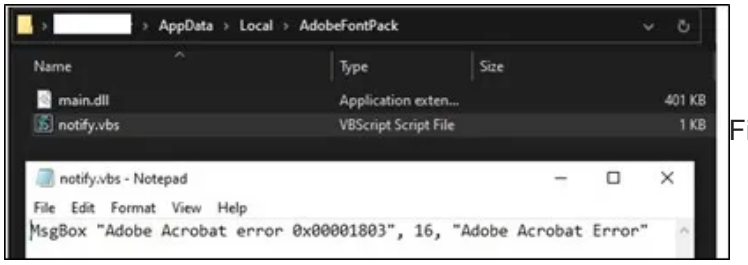

Figure 5 – Dropped DLL and VBS files

Additionally, the malware downloads another DLL file with an NLS extension from ***https[:]//telemetrysystemcollection[.]com*** in the below location. *C:\Users\<Admin>\AppData\Local\x86\<4-digit Hex Value>.nls*

The downloaded file is a copy of main.dll, which is another way to get the latest version of this malware from the remote server.

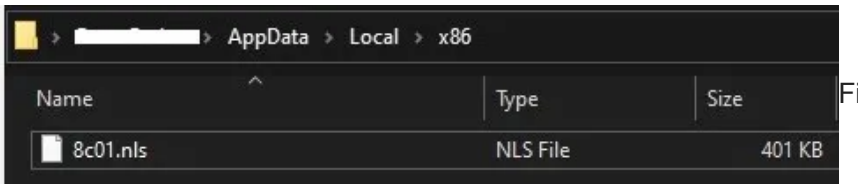

Figure 6 – Dropped Copy of Malware DLL File with .nls Extension

After dropping the DLL files, the MSI file launches *regsvr32.exe* and loads the malicious *main.dll* file to download the actual Matanbuchus malware.

The below figure shows the process chain of the MSI file.

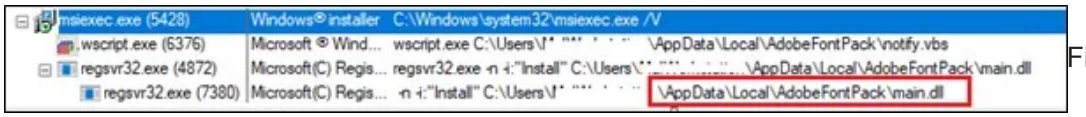

Figure 7 – Process Chain

Technical Analysis

We have taken the below sample hash for analysis :
(SHA256), ***14debc481aa0a26d3a0bdeed0e56b3ae9e301220f2606aae624d57a9d0617d6f***

We found that the malicious binary is a 32-bit DLL file based on static analysis.

The main function of dropped DLL files (*main.dll*) is to act as a loader and download the actual Matanbuchus DLL from the C&C server.

Before downloading the DLL file , it calls APIs such as *IsProcessorFeaturePresent(), GetSystemTimeAsFileTime() , IsDebuggerPresent(), QueryPerformanceCounter()* and *cpuid* to ensure that the malware is not running under a controlled environment such as VMware, Sandbox, etc.

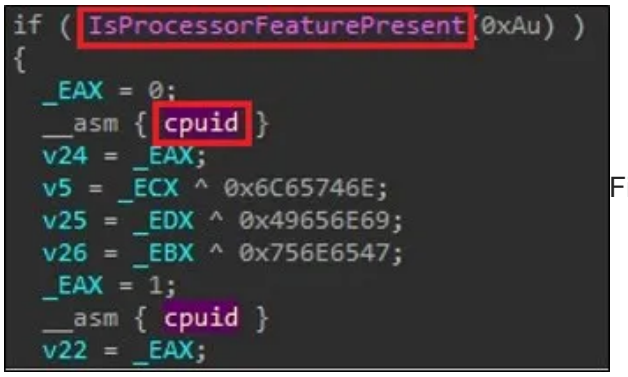

Figure 8 – Anti-debug Check

The malware executes an export function called *HackCheck()*, which runs a decryption loop on encrypted strings and prints the output using the *OutputDebugStringA()* API. The below figure shows the encrypted string and decryption code.

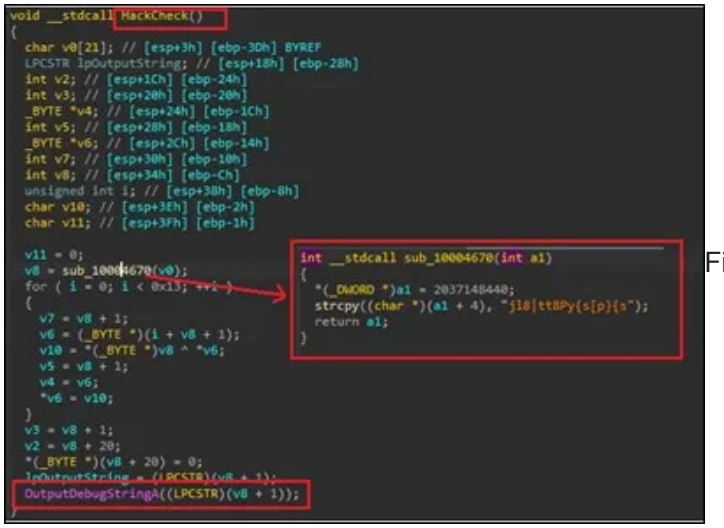

Figure 9 – HackCheck Function

To establish persistence, the malware creates a scheduled task to run the *8c01.nls* file with a specific function by using the following command line.

> *%windir%\system32\regsvr32.exe -n -i:"UpdateCheck" "C:\Users\<Admin>\AppData\Local\x86\8c01.nls"*

This scheduled task checks the malware version and downloads the latest version from the remote server every 60 seconds.

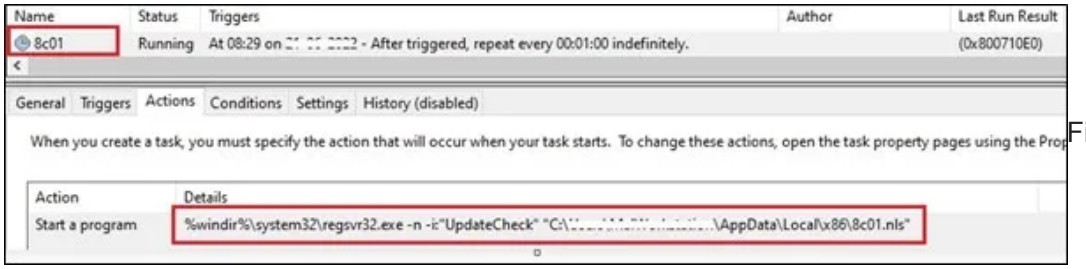

Figure 10 – Scheduled Task Entry for Persistence

Then, the malware connects to the below URL and receives this base64-encoded response:

> *"hxxp://telemetrysystemcollection[.]com/m8YYdu/mCQ2U9/home.aspx"*

The malware decodes the base64 content, an XOR encrypted binary that will be decrypted using a hardcoded key *FuHZu4rQgn3eqLZ6FB48Deybj49xEUCtDTAmF*.

The decrypted content is the actual Matanbuchus malware that will be mapped into the same process and executed using the export function *DllRegisterServer*.

The below figure shows the URL, XOR key, and export function names during runtime.

Figure 11 – URL and XOR key to download Actual Matanbuchus DLL

The below figure shows the hardcoded strings related to Matanbuchus present in the memory of *regsvr32.exe*. This indicates that the actual payload is loaded and executed in the memory without ever dropping it on the disk.

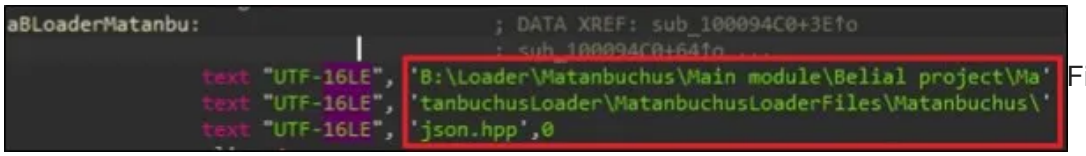

Figure 12 – Hardcoded Matanbuchus Strings

The Matanbuchus payload is responsible for executing other exe payloads as well as loading and executing shellcodes and malicious DLL files.

Network Activities

The Matanbuchus payload connects to C&C server ***hxxp://collectiontelemetrysystem[.]com/cAUtfkUDaptk/ZRSeiy/requets/index.php*** and sends the base64-encoded POST request.

The decoded base64 content is in JSON, as shown in Figure 13.

The JSON values are encrypted using the RC4 key and encoded using base64. These will further be decrypted on the server-side. This gives the TA victim details such as MAC address, computer name, etc.

Figure 13 – POST Request to C&C Server

Finally, Matanbuchus malware downloads two Cobalt Strike Beacons from the C&C servers.

First Cobalt-Strike Beacon:

The malware first downloads a file "*cob23_443.txt*" from ***hxxp://144.208.127[.]245/cob23_443.txt***. This is a hexadecimal binary file that will further be converted to ASCII characters and then downloads Cobalt Strike Beacons from ***hxxps://extic[.]icu/empower/type.tiff***.

The below figure shows the network communication which downloads the first Cobalt Strike Beacon.

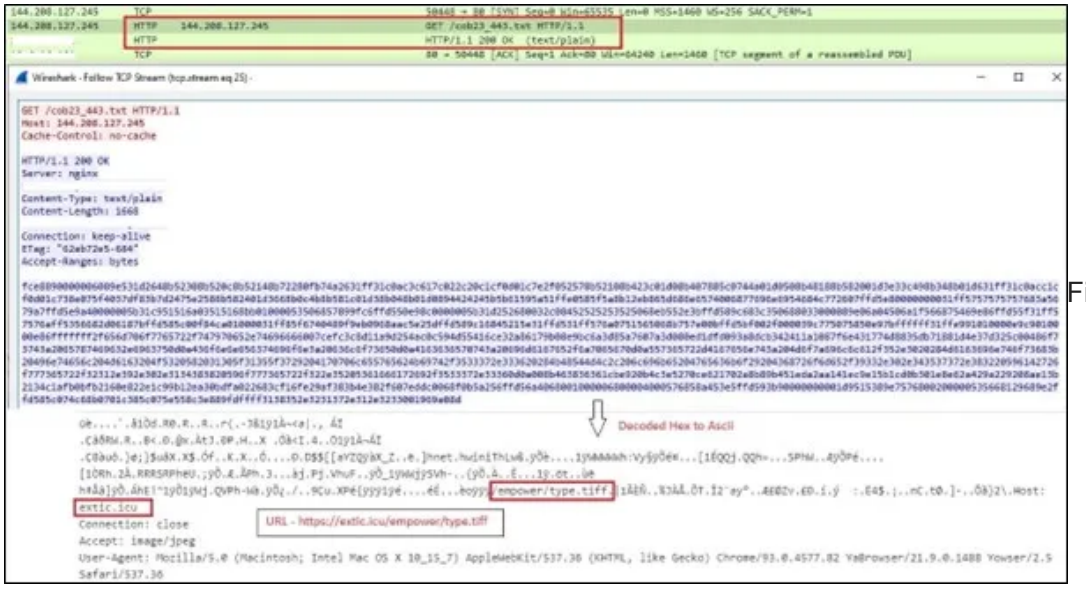

Figure 14 – C&C details of First Cobalt-Strike Payload

Second Cobalt-Strike Beacon:

After downloading the first beacon, Matanbuchus downloads a second Cobalt Strike DLL file named "*cob_220_443.dll*" from another URL:

hxxp://144.208.127[.]245/cob_220_443.dll

The below figure shows the network communication that downloads the second Cobalt Strike Beacon.

Figure 15 – C&C details of Second Cobalt-Strike Payload

C&C Commands

The Matanbuchus malware executes the following C&C commands.

- *Running exe*
- *Starting the exe with parameters*
- *High start exe*
- *RunDll32 & Execute*
- *Regsvr32 & Execute*
- *Run CMD in memory*
- *Run PS in memory*
- *MemLoadDllMain || MemLoadExe*
- *MemLoadShellCode*
- *MemLoadShellCode #2*
- *Running dll in memory #2 (DllRegisterServer)*
- *Running dll in memory #3 (DllInstall(Install))*
- *Running dll in memory #3 (DllInstall(Unstall))*
- *Crypt update & Bots upgrade*
- *Uninstall*

Conclusion

Threat Actors use various techniques to deploy their malicious payloads into the victim's system. In this case, we observed the TAs used Matanbuchus malware loader to deliver Cobalt Strike Beacons.

Cyble Research Labs will closely monitor the Matanbuchus malware group and other TAs and analyze them to better understand their motivations and TTPs.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Avoid downloading files from unknown websites.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.

- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solution on the employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204 T1059	User Execution Command and Scripting Interpreter
Persistence	T1053	Scheduled Task/Job
Defence Evasion	T1497	Virtualization/Sandbox Evasion
Lateral Movement	T1021	Remote Services
CNC	T1071	Application Layer Protocol

Indicator Of Compromise (IOCs)

Indicators	Indicator Type	Description
5698e2786aafbda7e252d89829250112 2521a69b98265e08c30f1d175f29865801e2aa15 d19ebb3abfbef6365accb6368973b8d10779cbf80a72fd28c8f2b9dd223ac288	MD5 SHA1 Sha256	Spam email
41049c329659e51ccca47c13b8021c14 50dd607fb2147457fb5978a591e9d2f46b412d24 72426e6b8ea42012675c07bf9a2895bcd7eae15c82343b4b71aece29d96a7b22	MD5 SHA1 Sha256	Email Attachment ZIP file
3e757306c45b710d739a802fbd1fb69f 60c1dc0b885ac77b8f670b636c8d404654362354 d0e2e92ec9d3921dc73b962354c7708f06a1a34cce67e8b67af4581adfc7aaad	MD5 SHA1 Sha256	HTML file
f177b0ec8a79756f45f8cf0fb9b99c07 1b18d12dc5c14e68b271164ff63647a6d2eb090d 63242d49d842cdf699b0ec04ad7bba8867080f8337d3e0ec7e768d10573142b3	MD5 SHA1 Sha256	ZIP file from HTML
ff82937564ff59eb6207f079cdc8e43d 7cfe0a71c4a2508a1af80e640ec8b1b034edb604 face46e6593206867da39e47001f134a00385898a36b8142a21ad54954682666	MD5 SHA1 Sha256	MSI file
8cb8cf84ab20159702e6803cd6ce364a 05103f90540f3e8a9599e9f1ab6a11c791aec393 14debc481aa0a26d3a0bdeed0e56b3ae9e301220f2606aae624d57a9d0617d6f	MD5 SHA1 Sha256	DLL file
0308aa2c8dab8a69de41f5d16679bb9b c6827bf44a433ff086e787653361859d6f6e2fb3 0a7e8fd68575db5f84c18b9a26e4058323d1357e2a29a5b12278e4bfa6939489	MD5 SHA1 Sha256	VBS file

8cb8cf84ab20159702e6803cd6ce364a 05103f90540f3e8a9599e9f1ab6a11c791aec393 14debc481aa0a26d3a0bdeed0e56b3ae9e301220f2606aae624d57a9d0617d6f	MD5 SHA1 Sha256	NLS file
314a641ee6ef932f4c561388bd539090 f20a688766f3c7105b64a6342277879d751de6f3 1e9aaf1375d9f7403644b4bea2c6fe679579bf61945ba6bdb54cc7cd7b728211	MD5 SHA1 Sha256	1st Cobalt Strike Payload
40d5b499d9213f44ca786d56b6e10907 73b17544d1e42dc12d4af1d19343e2c7456a4a0b 80e3212beed371025ba8c3eb32bea41de85d856941506f2a5255377069449c95	MD5 SHA1 Sha256	2nd Cobalt Strike Payload
97fc6726f396c4b86bc84ca97e787637 ad6e5024a0be6f69370e7a0482a2baa27c4a25be a5b06297d86aee3c261df7415a4fa873f38bd5573523178000d89a8d5fd64b9a	MD5 SHA1 Sha256	XORed file
8fc15b030254c0d49f18d06c696d6986 75f62f4d419b921bc081b5e8387665ac3cffd0d7 bd68ecd681b844232f050c21c1ea914590351ef64e889d8ef37ea63bd9e2a2ec	MD5 SHA1 Sha256	DLL file from XORed file
hxxp://telemetrysystemcollection[.]com/m8YYdu/mCQ2U9/home.aspx	URL	Matanbuchus traffic
hxxps://extic[.]icu/empower/type.tiff	URL	1st Cobalt Strike URL

References

https://isc.sans.edu/forums/diary/Malspam+pushes+Matanbuchus+malware+leads+to+Cobalt+Strike/28752/