February 1, 2024

Stately Taurus Continued – New Information on Cyberespionage Attacks against Myanmar Military Junta

On January 23rd, CSIRT-CTI published a blogpost describing a pair of campaigns believed to be launched by Stately Taurus (alias Bronze President, Camaro Dragon, Earth Preta, Mustang Panda, Red Delta, TEMP.Hex and Luminous Moth) against the Myanmar military junta. Subsequently, additional observations were made by Palo Alto Networks's Unit 42, suggesting that the ubiquity of the campaigns targeting Myanmar may have been more extensive than originally delineated. In a joint effort with Unit 42, CSIRT-CTI continued its Stately Taurus investigation to uncover and describe five additional campaigns likely to be run against targeted entities in Myanmar.

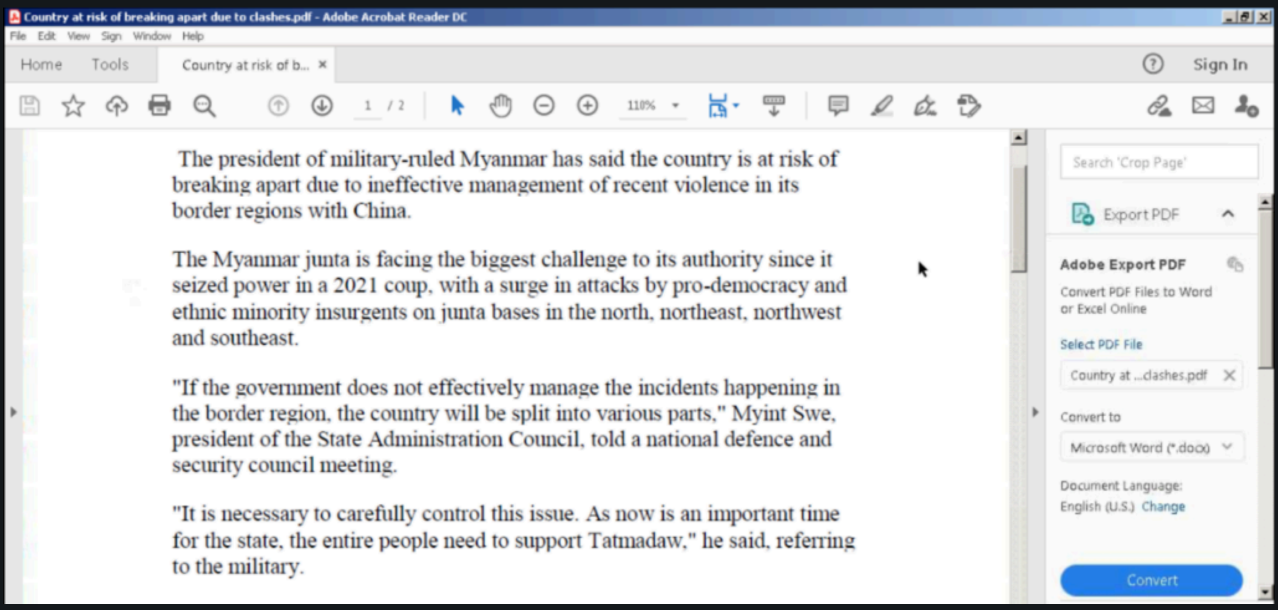
All newly discovered campaigns have taken place in between the originally discussed campaigns on November 9th, 2023 and January 17th, 2024. Employment of previously seen techniques such as DLL Search Order Hijacking and leveraging publicly documented malware such as PUBLOAD show a consistent intrusion set. However, deviations like the use of Cobalt Strike beacons and infostealers showcase variability in modus operandi. Key Indicators of Compromise (IOCs) involve IP addresses, standard magic bytes, autorun keys and created directories, with the certificate Common Name "WIN-9JJA076EVSS" consistently associated with C2 servers the malware communicates with. While attribution to Stately Taurus is made with confidence, it is advised to monitor adequately, as the mentioned variability might affect the effectiveness of rule-based detection using the disclosed IOCs.

For the previous two campaigns, see CSIRT-CTI's previous blog.

Campaign #3 – Shan(north) – 11-09-2023.zip

On November 11th, 2023, a ZIP-archive with the name *Shan(north) – 11-09-2023.zip* was created and uploaded to VirusTotal by an entity in Myanmar. It contains a lure document referencing the conflict between the Myanmar military junta and *pro-democracy and ethnic minority insurgents* in the North and Southeast of the country. While the spreading of lure documents is a tactic that was previously seen in Stately Taurus campaigns such as documented by Cisco Talos, this is the only campaign in this set with a PDF file.

The PDF file contains some metadata. This metadata shows the author, which is set to FBI, the website the document was generated on and the dates of creation and modification, showing that the document was created on November 10th, 2023. This is a day before creation of the ZIP-file.


Country at risk of breaking apart due to clashes.pdf - Adobe Acrobat Reader DC
File Edit View Sign Window Help
Home Tools Country at risk of b...
Sign In
1 / 2
110%
Search 'Crop Page'
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
Country at ...clashes.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert

The president of military-ruled Myanmar has said the country is at risk of breaking apart due to ineffective management of recent violence in its border regions with China.

The Myanmar junta is facing the biggest challenge to its authority since it seized power in a 2021 coup, with a surge in attacks by pro-democracy and ethnic minority insurgents on junta bases in the north, northeast, northwest and southeast.

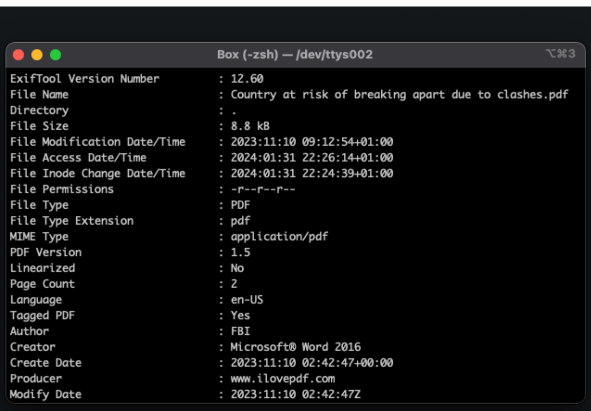
"If the government does not effectively manage the incidents happening in the border region, the country will be split into various parts," Myint Swe, president of the State Administration Council, told a national defence and security council meeting.

"It is necessary to carefully control this issue. As now is an important time for the state, the entire people need to support Tatmadaw," he said, referring to the military.

Figure 1: Lure PDF describing the ongoing crisis in Myanmar

Aside from the PDF, the ZIP-file contains another three files. Two of these are benign executables with the names *Country at risk of breaking apart due to clashes.exe* and *Report – 11-09-23.exe*, which are both copies of the legitimate executable *KeyScrambler.exe*, which was originally signed by QFX Software Corporation. Both executables leverage the previously-seen DLL Search Order Hijacking technique

(T1574.002) to side-load a malicious DLL with the name *KeyScramblerIE.dll*.



```
Box (-zsh) — /dev/ttys002
ExifTool Version Number         : 12.60
File Name                       : Country at risk of breaking apart due to clashes.pdf
Directory                       : .
File Size                       : 8.8 kB
File Modification Date/Time     : 2023:11:10 09:12:54+01:00
File Access Date/Time           : 2024:01:31 22:26:14+01:00
File Inode Change Date/Time     : 2024:01:31 22:24:39+01:00
File Permissions                : -r--r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 2
Language                        : en-US
Tagged PDF                      : Yes
Author                          : FBI
Creator                         : Microsoft® Word 2016
Create Date                     : 2023:11:10 02:42:47+00:00
Producer                        : www.ilovepdf.com
Modify Date                     : 2023:11:10 02:42:47Z
```

Figure 2: Metadata of the lure PDF

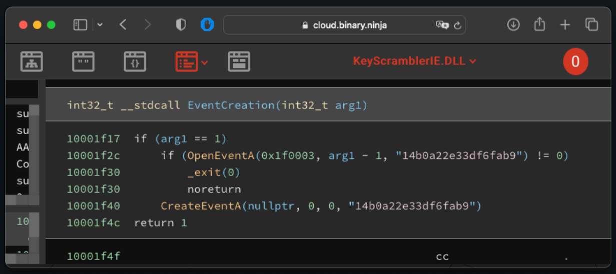
This DLL has a few interesting aspects. It connects with FakeTLS to `45.121.146[.]113` for C2 similar to the documented behaviour in the previous blog and with the same certificate Common Name `WIN-9JJA076EVSS`. This IP address was previously seen in Unit 42's report on Stately Taurus's SolidPDFCreator campaigns assessed to be ran against the Philippines. As documented by Lab52, the DLL uses the same magic bytes (`17 03 03`) for communicating the payload, displaying typical PUBLOAD traits. Before moving the executable and malicious DLL to a newly created directory `%ProgramData%\QFXSoftware`, however, the malware proceeds to read a set of directories with potentially sensitive data. This indicates that this sample could have an infostealer aspect to it. Exfiltration behavior of this threat group has previously been discussed by Avast, where they describe that Stately Taurus was suspected of exfiltrating sensitive documents, recordings and email dumps. This substantiates the theory of an infostealer in this sample, as the following directories were read for all local users:

1. C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\<user>\extensions.cache
2. C:\Users\Admin\AppData\Roaming\Thunderbird\Profiles\
3. C:\Users\Admin\AppData\Roaming\Flock\Browser\Profiles\

After reading these directories, the DLL and executable are moved to the new directory `%ProgramData%\QFXSoftware` and the typical autorun key is created for the executable in its new location with a command-line argument to detect reruns.

```
\REGISTRY\USER\S-1-5-21-1807954202-4137445701-3669982446-1000\Software\Microsoft\Windows\CurrentVersion\Run\AKkeydobe = "C:\\ProgramData\\QFXSoftware\\Report - 11-09-23.exe STLQFXSoftware"
```

Interestingly and seemingly undocumented is the use of Windows event objects. Without further reference of event creation, the DLL creates an event object with the name *14b0a22e33df6fab9*. When decoding this to Traditional Chinese with UTF-16BE (1201), this results in ㄴ戰愲㉥㌳摦㙦慢, translating to *the battle is slow*. The DLL contains several strings that can be decoded like this.



```
int32_t __stdcall EventCreation(int32_t arg1)

10001f17  if (arg1 == 1)
10001f2c      if (OpenEventA(0x1f0003, arg1 - 1, "14b0a22e33df6fab9") != 0)
10001f30          _exit(0)
10001f30          noreturn
10001f40      CreateEventA(nullptr, 0, 0, "14b0a22e33df6fab9")
10001f4c  return 1

10001f4f                                              cc
```

Figure 3: Function creating a Windows Event Object with an UTF-16 encoded string *the battle is slow*

String	Encoding	Decoded	Value
14b0a22e33df6fab9	UTF-16BE	ㄴ戰愲㉥㌳㧓㙫慢	The battle is slow
243503098e6d85bd3367b2e25e144954e88d9a0b	UTF-16LE	伕匭㌰㤰攸搶㔸擄㌳嬠㉢㉥攵叄㤴仔幰搸㤭戰	The battle between the two
n9243503098e6d85bd3367b2e25e144954e88d9a0b	UTF-16LE	伕匭㌰㤰攸搶㔸擄㌳嬠㉢㉥攵叄㤴仔幰搸㤭戰	The battle between the two
bd3367b2e25e144954e88d9a0b	UTF-16LE	擄㌳嬠㉢㉥攵叄㤴仔幰搸㤭戰	The battle
3503098e6d85bd3367b2e25e144954e88d9a0b	UTF-16LE	匭㌰㤰攸搶㔸擄㌳嬠㉢㉥攵叄㤴仔幰搸㤭戰	The battle between

Campaign #4 – Talking Points for China.zip

The next sample was created on December 12th, 2023 and uploaded to VirusTotal from Myanmar. It was named *Talking Points for China.zip* and contains the same executable as in the previous campaign by QFX Software Corporation and a malicious DLL with the names *Talking Points for China.exe* and *KeyScramblerIE.exe*. The sample connects with FakeTLS to an unresponsive C2 server at `61.4.102[.]75` and uses the same magic bytes as the earlier samples to indicate the payload (`17 03 03`).

Execution of this malware aligns very much with the well-documented and earlier discussed PUBLOAD malware. It checks whether there is a command-line argument available andmoves the DLL and the executable to a new directory in `%ProgramData%/QFXSoftwarePubKey`. The malware then reads the same directories as shown in the previous campaign with the potential goal of data exfiltration. Moreover, while the same type of UTF-16LE and BE strings are available, these do not seem to form sentences in the same manner.

Figure 4: Talking Points for China.zip content

Campaign #5 – 01-05-2024.zip

The next campaign was observed to be created on January 5th, 2024 and looks significantly different from the rest of the campaigns. However, at the core of this sample, it is still assessed to be a PUBLOAD sample. When unpacked, the zip file shows three files – *01-05-2024.PIF*, *ZipDLL.dll* and *zero.offers*. The PIF-file is a normal and benign executable originally signed by CAM UnZip Software and both the DLL-file as *zero.offers* are malicious. The first steps of execution of the DLL-file align with the other campaigns by copying the executable, DLL and *zero.offers* file to %ProgramData%\CAMDevelopment though it changes the name of the executable to *UnZipCAM.exe*. After doing so, it attempts to load the *zero.offers* file by decrypting it into a Cobalt Strike Beacon loader, which Cisco Talos describes to be a known alternative to PlugX used by Stately Taurus. It does so by printing a series of debug strings for every byte in the file and performing a bitwise XOR operation on that byte with `0x60` as the key.

Figure 5: Decrypting Cobalt Strike Beacon with key `0x60` while spamming debug strings

Extracting the Beacon configuration from the resulting file using Didier Stevens's analytics suite indicates that the C2 address for this sample is `45.154.24[.]14`. It uses the User-Agent `Mozilla/5.0 (compatible; mobile! telephone; https://mobile.bing.com/search)`. The Beacon configuration indicates a Cobalt Strike watermark/license-id of 100000. This is a relatively well-known watermark.

Lastly, the function responsible for the creation of Windows event objects is present in this sample as well, creating an event object with the name `JeffreyEpsteindocumentsunsealed`. This event object, however, does have an additional reference in the binary and shows a function that checks the presence of the event object in the system before creating the directory in `%ProgramData%`, moving the files there and creating an autorun key. If it is present, this is indication of achieved persistence and the function will return. Notable is therefore also that this sample does not come with a command-line argument in the autorun key and does not check for those.

Figure 6: Event Object-based conditional must be met before creating the new directory and autorun key

Campaign #6 – Message to the SAC Office.zip

This package named *Message to the SAC Office.zip* was created on January 11th and uploaded on January 15th 2024 to VirusTotal from Myanmar. It is probable that the title references the State Administration Council (SAC), which currently governs Myanmar. Extraction of the ZIP-file shows that it is similar to campaign #5 and contains the earlier-discovered benign executable signed by CAM UnZip software in a folder called *Adviser office*. The files are named *01-11-2023 you _PDF_.pif* and *ZipDLL.dll*. Upon execution of the PIF-file, the malicious DLL is side-loaded again similar to PUBLOAD and attempts to connect to the same C2 server as campaign #5 (`45.154.24[.]14`) using the known magic bytes In contrast to campaign #5, this sample does not attempt to stage Cobalt Strike. Similar to campaign #1, this DLL returns to spoofing the Host headers in HTTP traffic to communicate with the C2 server, spoofing the URLs `http://wpstatic.microsoft.com` and `http://www.download.wndowsupdate.com`.

To do so, it uses the familiar magic bytes `17 03 03` and verifies the presence of any known event objects before creating two directories, one at `C:\Users\Admin\Documents\CAM Development\` and in `%ProgramData%\UnZipCAM\`. In the former, it places an encrypted INI-file named `CUZ.ini`. This INI-file is likely to contain the last execution date combined with a victim ID, according to Avast. Verifying the presence of known event objects is done in the same way as before, though this time the event object is named `ChrisSanders`. Moreover, a routine seems to be added that prints `Start…Code_techspence` before starting the function.

Figure 7: Event Object conditional with the name `ChrisSanders` shows creation of autorun key and `techspence` routine

Campaign #7 – meeting

process.zip

The last observed campaign was created on January 16th and uploaded to VirusTotal on the same day from Myanmar. This is again a ZIP-file with a DLL-file to side-load and a benign executable signed by Silhouette Research & Technology Ltd with the original filename `permissions.exe`. The executable is disguised as a Microsoft Word file with a replaced icon and is named *meeting process .exe* (the space is repeated multiple times to hide the extension) and the DLL is called `RBGUIFramework.dll`. The DLL creates a file called `preferences.ini` in `C:\Users\Public\` that is possibly similar to the previously found INI-file due to the size. It connects to a C2 server on `103.249.84[.]137` with the characterizing magic bytes present and Common Name `WIN-9JJA076EVSS`.

After the verification for present command-line arguments, it creates a directory at *C:\Users\Public\Libraries* and moves the files in this directory. It then creates an autorun key with the name *WindowsOfficeDoc,* including the command line argument.

Figure 8: Executable is disguised as a Microsoft Office document, hiding the .EXE extension

```
\REGISTRY\USER\S-1-5-21-656384163-554681555-2882430073-1000\Software\Microsoft\Windo
ws\CurrentVersion\Run\WindowsOfficeDoc = "C:\\Users\\Public\\Libraries\\meeting proc
ess .exe WindowsDoc"
```

Assessing Campaign Similarity

There is a great deal of similarity between the tactics and flow of execution between these campaigns. All campaigns leverage DLL Search Order Hijacking to stage malware in a near-identical way scattered across six different C2 servers for the seven campaigns. As mentioned, a significant portion of the campaigns comes from the same AS, running a certificate with the common name `WIN-9JJA076EVSS`. While the Tactics, Techniques and Procedures (TTP) within these campaigns are nearly identical with a few different variants, it is valuable information to what extent the binaries are similar as this might influence the effectiveness of rule-based detection of this threat group. Below, two similarity matrices for strings and imports based on the Jaccard similarity index are displayed.

Figure 9: Similarity Matrix for string similarities between malicious DLLs

Figure 10: Similarity Matrix for import similarities between malicious DLLs

It is to be expected that the binaries do not have very high string similarity. After all, the actual strings in the malware are tailored for their target. However, adding the import similarity matrix shows that most samples have a high similarity in terms of imports. For example, *Analysis of the third meeting of NDSC* and *ASEAN Notes* exhibit a correlation coefficient of 0.96, indicating that they have a very high similarity in terms of imports. Using this matrix to set a threshold, it becomes possible to visualize which samples have a higher degree of similarity than others in this set. This results in the below graph.

What stands out is that when a Jaccard index threshold of 0.7 is handled, two subsets appear. This threshold represents a clear division between samples in the similarity matrices and also represents a significant similarity between samples. In particular the sample DLLs that did not have any variations or additional implementations such as Cobalt Strike or infostealers scored very high in import similarity. The same goes for the Control Flow Graphs resulting from these binaries. The samples can be assessed as related with moderate confidence due to the high similarity in imports, control flow and TTPs.

Figure 11: Sample subsets consisting of similar samples above the 0.7 Jaccard index threshold

Conclusion

In addition to the two campaigns discussed in the previous blog, five additional campaigns have been discovered. All these campaigns have been assessed to be likely related to the Stately Taurus threat group operating on an agenda aligning with Chinese geopolitical interest. We have found multiple variants of the PUBLOAD malware in this research extension of which some variants used Cobalt Strike rather than PlugX and some that contained infostealers. Even though the samples deviate, there are multiple observations that indicate that these campaigns are related. A very strong indicator are the titles, in particular a title referencing the ongoing rebel attacks in Myanmar. Other indicators include known infrastructure IOCs such as certificate Common Names, (shared) IP addresses and a significant portion of shared code that can be related back to previous campaigns. The variability in the samples, however, might affect the ability of security teams to detect this threat group based on IOCs only. Therefore, it is recommended to adequately monitor assets for suspicious activity.

Indicators of Compromise

IOC	Value
C2 address	45.121.146[.]113
C2 address	61.4.102[.]75
C2 address	45.154.24[.]14
C2 address	103.249.84[.]137
Spoofed Host header	wpstatic.microsoft.com
Spoofed Host header	www.download.wndowsupdate.com
Magic Bytes	17 03 03
Certificate Common Name	WIN-9JJA076EVSS
Cobalt Strike User Agent	"Mozilla/5.0 (compatible; mobile! telephone; https://mobile.bing.com/
Shan(north) – 11-09-2023.zip	3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc
Country at risk of breaking apart due to clashes.exe	fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f
Country at risk of breaking apart due to clashes.pdf	879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892ca
Report – 11-09-23.exe	fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f
KeyScramblerIE.dll (Campaign #3)	b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3c
KeyScramblerIE.dll (Campaign #4)	8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a

Talking Points for China.zip	3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473
Talking Points for China.exe	fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f
01-05-2024.zip	fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570ca
01-05-2024.pif	5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda
ZipDLL.dll (Campaign #5)	6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bc
zero.offers	e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236
Message to the SAC Office.zip	536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991
01-11-2023 yyo *PDF*.pif	5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda
ZipDLL.dll (Campaign #6)	6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36
meeting process.zip	edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7
meeting process .exe	01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec9
RBGUIFramework.dll	8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c65310
Malware drop location	%ProgramData%\QFXSoftware
Malware drop location	%ProgramData%\QFXSoftwarePubKey
Malware drop location	%ProgramData%\CAMDevelopment
Malware drop location	%ProgramData%\UnZipCAM
Autorun key	AKkeydobe
Autorun key	WindowsOfficeDoc
Unique string	14b0a22e33df6fab9
Unique string	243503098e6d85bd3367b2e25e144954e88d9a0b
Unique string	n9243503098e6d85bd3367b2e25e144954e88d9a0b
Unique string	bd3367b2e25e144954e88d9a0b3503098e6d85bd3367b2e25
Unique string	144954e88d9a0b
Unique string	JeffreyEpsteindocumentsunsealed
Unique string	ChrisSanders

Tags : APT China Malware

‹ Stately Taurus Targets Myanmar Amidst Concerns over Military Junta’s Handling of Rebel Attacks

About