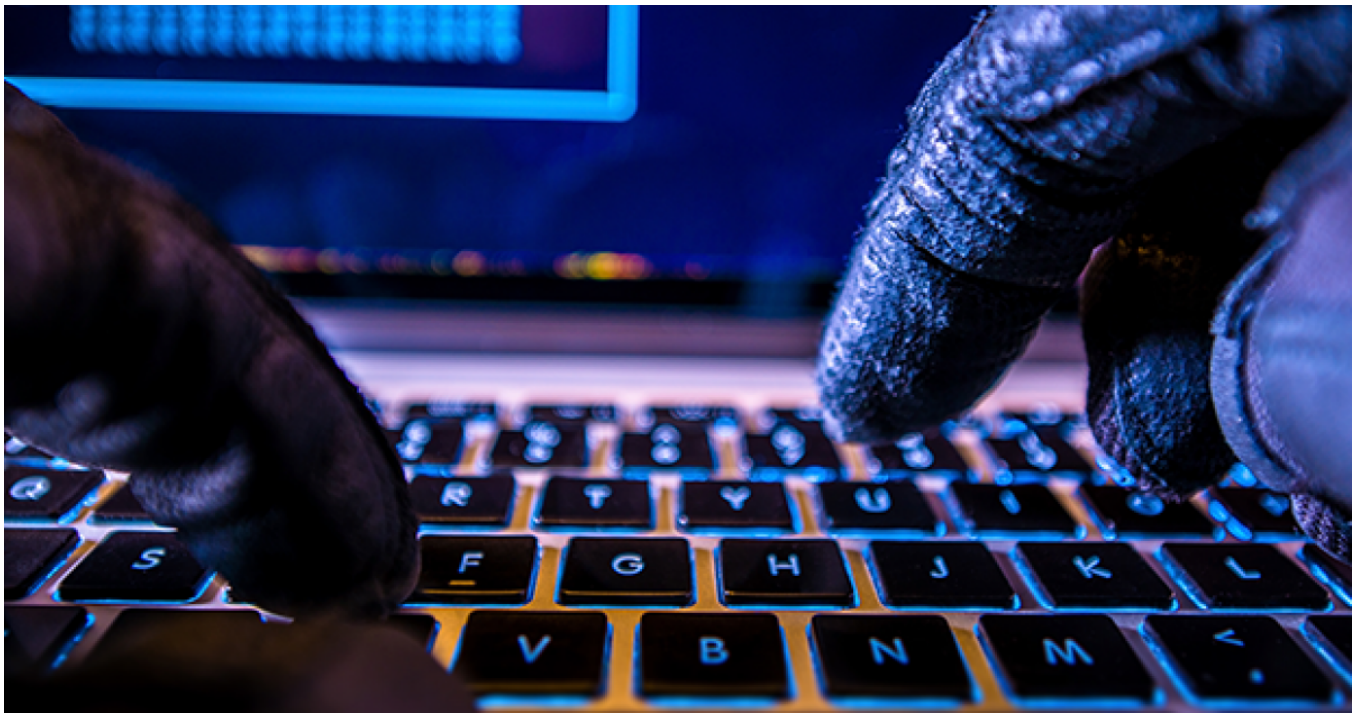
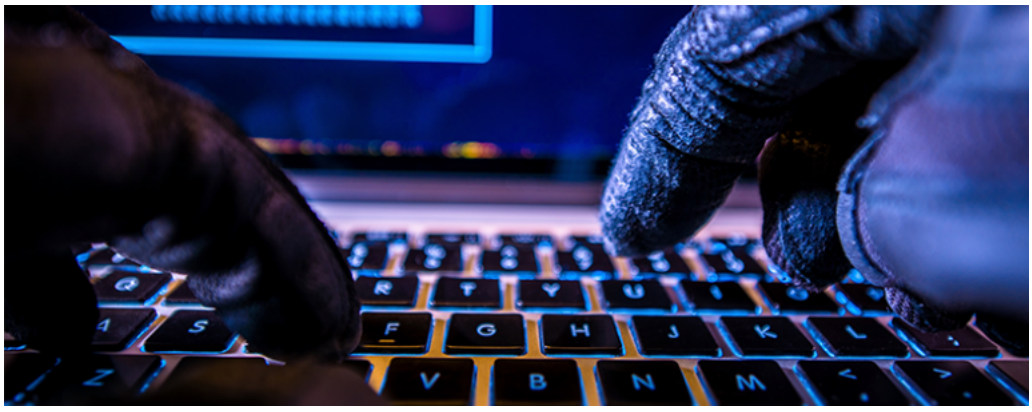
TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader

proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader

November 23, 2020



Blog
Threat Insight
TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader



November 23, 2020 The Proofpoint Threat Research Team

Executive Summary

Following the Chinese National Day holiday in September, Proofpoint researchers observed a resumption of activity by the APT actor TA416. Historic campaigns by this actor have also been publicly attributed to “Mustang Panda” and “RedDelta”. This new activity appears to be a continuation of previously reported campaigns that have targeted entities associated with diplomatic relations between the Vatican and the Chinese Communist Party, as well as entities in Myanmar. The targeting of organizations conducting diplomacy in Africa has also been observed. Proofpoint researchers have identified updates to the actor’s toolset which is used to deliver PlugX malware payloads. Specifically, researchers identified a new Golang variant of TA416’s PlugX malware loader and identified consistent usage of PlugX malware in targeted campaigns. As this group continues to be publicly reported on by security researchers, they exemplify a persistence in the modification of their toolset to frustrate analysis and evade detection. While baseline changes to their payloads do not greatly increase the difficulty of attributing TA416 campaigns, they do make automated detection and execution of malware components independent from the infection chain more challenging for researchers. This may represent efforts by the group to continue their pursuit of espionage objectives while maintaining an embattled toolset and staying out of the daily Twitter conversation popular amongst threat researchers.

Renewed Phishing Activity

After nearly a month of inactivity following publications by threat researchers, Proofpoint analysts have identified limited signs of renewed phishing activity that can be attributed to the Chinese APT group TA416 (also referred to as Mustang Panda and RedDelta) [1]. Recorded Future researchers have previously noted historic periods of dormancy following disclosure of TA416’s targeted campaigns.[2] This most recent period of inactivity encompassed September 16, 2020 through October 10, 2020. Notably this time period included the Chinese National holiday referred to as National Day and the following unofficial vacation period “Golden Week”. The resumption of phishing activity by TA416 included a continued use of social engineering lures referencing the provisional agreement recently renewed between the Vatican Holy See and the Chinese Communist Party “CCP”.[3] Additionally, spoofed email header from fields were observed that appear to imitate journalists from the Union of Catholic Asia News. This confluence of themed social engineering content suggests a continued focus on matters pertaining to the evolving relationship between the Catholic Church and the “CCP”.

PlugX Malware Analysis

Proofpoint researchers identified two RAR archives which serve as PlugX malware droppers. One of these files was found to be a self-extracting RAR archive. For the purposes of this analysis the self-extracting archive file AdobelmdyU.exe|930b7a798e3279b7460e30ce2f3a2deccbc252f3ca213cb022f5b7e6a25a0867 was examined. The initial delivery vector for these RAR archives could not be identified. However, historically TA416 has been observed including Google Drive and Dropbox URLs within phishing emails that deliver archives containing PlugX malware and related components. Once the RAR archive is extracted four files are installed on the host and the portable executable Adobelm.exe is executed. The installed files include:

Adobelm.exe|0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681

A legitimate Adobe executable used in the DLL Side-Loading of Hex.dll.

Adobehelp.exe|e3e3c28f7a96906e6c30f56e8e6b013e42b5113967d6fb054c32885501dfd1b7

An unused binary that has been previously observed in malicious RAR archives linked to TA416.

hex.dll|235752f22f1a21e18e0833fc26e1cdb4834a56ee53ec7acb8a402129329c0cdd

A Golang binary which decrypts and loads adobeupdate.dat (the PlugX payload).

adobeupdate.dat|afa06df5a2c33dc0bdf80bbe09dade421b3e8b5990a56246e0d7053d5668d91

The encrypted PlugX malware payload.

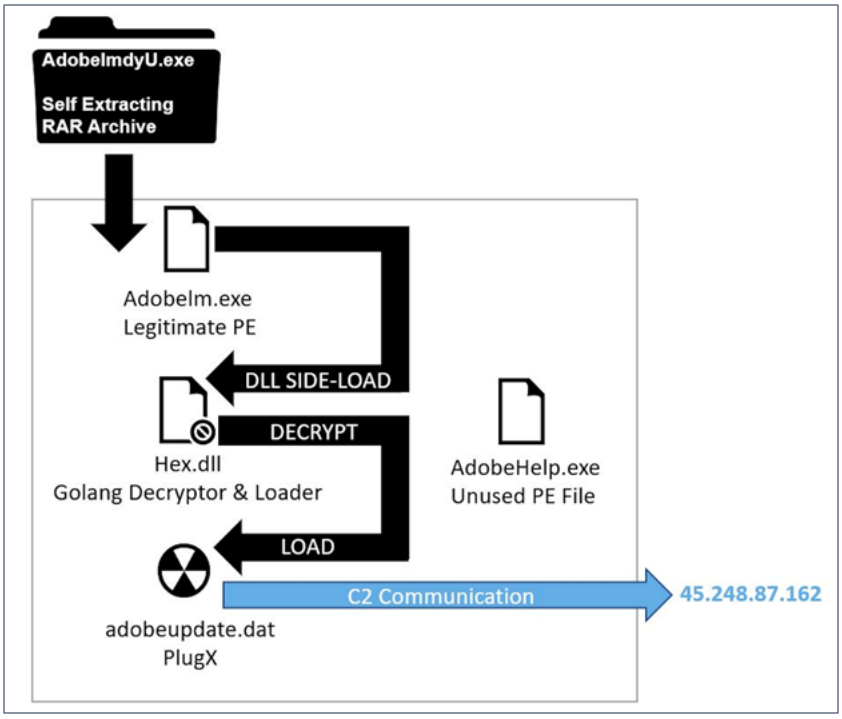


Figure 1: PlugX Malware Execution Diagram

Following RAR extraction, Adobelm.exe, a legitimate PE that is used for the DLL side-loading of hex.dll, is executed. It calls a PE export function of hex.dll named CEFProcessForkHandlerEx. Historically, TA416 campaigns have used the file name hex.dll and the same PE export name to achieve DLL side-loading for a Microsoft Windows PE DLL. These files served as loaders and decryptors of encrypted PlugX malware payloads. The file would read, load, decrypt, and execute the PlugX malware payload (regularly named adobeupdate.dat, as it is in this case).

The PlugX malware loader found in this case was identified as a Golang binary. Proofpoint has not previously observed this file type in use by TA416. Both identified RAR archives were found to drop the same encrypted PlugX malware file and Golang loader samples. The Golang loader has a compilation creation time that dates it to June 24, 2020. However, the command and control infrastructure discussed later in this posting suggests that the PlugX malware payload and Golang loader variant were used after August 24, 2020. Despite the file type of the PlugX loader changing, the functionality remains largely the same. It reads the file adobeupdate.dat, retrieves the XOR key beginning at offset x00 and continues until it reads a null byte. It then decrypts the payload, and finally executes the decrypted adobeupdate.dat. This results in the execution of the PlugX malware payload which ultimately calls out to the command and control IP 45.248.87[.]162. The following registry key is also created during this process which runs at startup establishing the malware's persistence. Notably the sample uses the distinct file installation directory "AdobeImdyU".

Registry Key	Data
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AdobeImdyU	"C:\ProgramData\Adobe\AdobeI 402

Figure 2: PlugX malware Registry Key established for malware persistence.

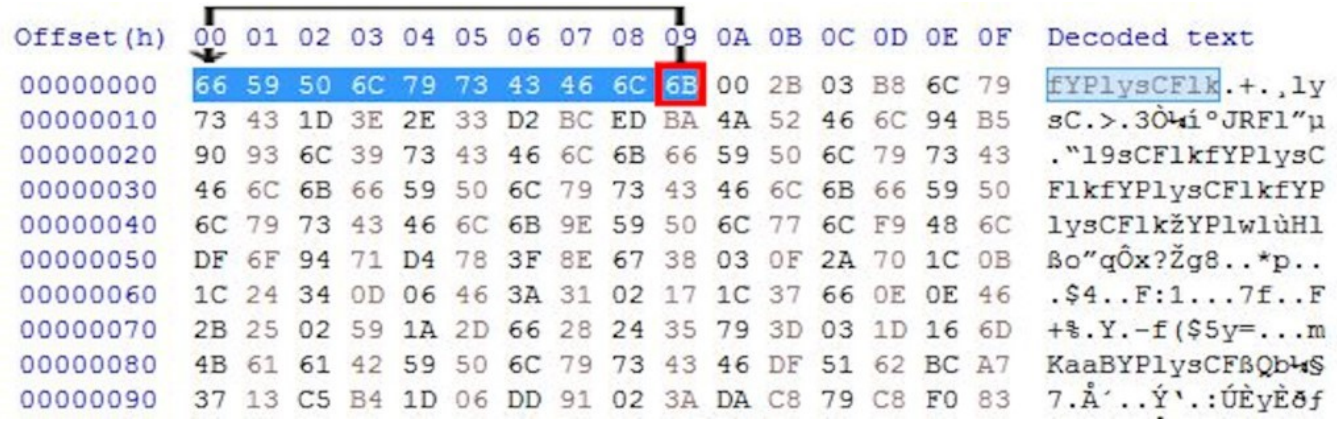
Consistent TA416 Tools

The PlugX malware payload, unlike the Golang loader variant, seems to remain consistent when compared with previous versions.

> Historical analysis conducted by Avira and Recorded Future has documented that the encrypted PlugX payloads, which have been disguised as data and gif files, are in fact encrypted PE DLL files. These encrypted files contain a hardcoded XOR decryption key that begins at offset x00 and continues until a null byte is read.[4] In this case the Golang Binary PlugX loader reads the encryption key in the same manner from x00 to null byte, with the hardcoded key ending at offset x09. This represents continued usage of an anti-analysis method which makes the execution of PlugX payloads more complex and complicates the detection of command and control infrastructure which the malware communicates with.

Hardcoded Decryption Key / Byte Sequence
66 59 50 6C 79 73 43 46 6C 6B

Figure 3: PlugX malware XOR decryption key.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	66	59	50	6C	79	73	43	46	6C	6B	00	2B	03	B8	6C	79	fYPlysCFlk.+.¸ly
00000010	73	43	1D	3E	2E	33	D2	BC	ED	BA	4A	52	46	6C	94	B5	sC.>.3Ò¼í°JRFl"µ
00000020	90	93	6C	39	73	43	46	6C	6B	66	59	50	6C	79	73	43	."l9sCFlkfYPlysC
00000030	46	6C	6B	66	59	50	6C	79	73	43	46	6C	6B	66	59	50	FlkfYPlysCFlkfYP
00000040	6C	79	73	43	46	6C	6B	9E	59	50	6C	77	6C	F9	48	6C	lysCFlkžYPlwlùHl
00000050	DF	6F	94	71	D4	78	3F	8E	67	38	03	0F	2A	70	1C	0B	ßo"qÔx?Žg8..*p..
00000060	1C	24	34	0D	06	46	3A	31	02	17	1C	37	66	0E	0E	46	.$4..F:1...7f..F
00000070	2B	25	02	59	1A	2D	66	28	24	35	79	3D	03	1D	16	6D	+%.Y.-f($5y=...m
00000080	4B	61	61	42	59	50	6C	79	73	43	46	DF	51	62	BC	A7	KaaBYPlysCFßQb¼§
00000090	37	13	C5	B4	1D	06	DD	91	02	3A	DA	C8	79	C8	F0	83	7.Å´..Ý'.:ÚÈyÈðƒ

Figure 4: PlugX malware byte sequence and hardcoded XOR decryption key.

Following decryption, the resulting file reflects a valid PE header for the PlugX malware payload. Shellcode appears between the MZ header and the DOS message. The function of this shellcode is to write the PE DLL into RWX memory and begin execution at the beginning of the file. This establishes an entry point for the payload and prevents an entry point not found error when executing the malware. This is a common technique observed by many malware families and is not exclusive to TA416 PlugX variants. This shellcode is unlikely to appear in legitimate software DLLs.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	E8	00	00	00	00	5B	52	45	55	8B	EC	81	C3	99	MZè....[REU‹ì.Ã™
00000010	11	00	00	FF	D3	C9	C3	00	40	00	00	00	00	00	00	00	...ÿÓÉÃ.@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F8	00	00	00	.....ø...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..´.Í!¸.LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....
00000080	FD	86	62	24	B9	E7	0C	77	B9	E7	0C	77	B9	E7	0C	77	ý†b$¹ç.w¹ç.w¹ç.w
00000090	FF	B6	ED	77	A1	E7	0C	77	FF	B6	D3	77	A8	E7	0C	77	ÿ¶íw¡ç.wÿ¶Ów¨ç.w
000000A0	FF	B6	EC	77	D3	E7	0C	77	B0	9F	8F	77	BA	E7	0C	77	ÿ¶ìwÓç.w°Ÿ.wºç.w
000000B0	B0	9F	9F	77	BC	E7	0C	77	B9	E7	0D	77	EF	E7	0C	77	°ŸŸw¼ç.w¹ç.wïç.w
000000C0	B4	B5	ED	77	A2	E7	0C	77	B4	B5	D0	77	B8	E7	0C	77	´µíw¢ç.w´µÐw¸ç.w
000000D0	B4	B5	D7	77	B8	E7	0C	77	B9	E7	9B	77	B8	E7	0C	77	´µ×w¸ç.w¹ç›w¸ç.w
000000E0	B4	B5	D2	77	B8	E7	0C	77	52	69	63	68	B9	E7	0C	77	´µÒw¸ç.wRich¹ç.w
000000F0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	05	00	........PE..L...
00000100	A9	E4	49	5E	00	00	00	00	00	00	00	00	E0	00	02	21	©äI^........à..!
00000110	0B	01	0C	00	00	02	02	00	00	48	01	00	00	00	00	00	.........H.....

Figure 5: PlugX malware byte sequence and XOR decryption key.

Command and Control Infrastructure

The command and control communication observed by these PlugX malware samples are consistent with previously documented versions. The C2 traffic was successfully detected by an existing Proofpoint Emerging Threats Suricata signature for PlugX malware which is publicly available as part of the ET OPEN public ruleset.[5] The following IP and example command and control communication URLs were identified:

- 45.248.87[.]162
- hxxp://45.248.87[.]162/756d1598
- hxxp://45.248.87[.]162/9f86852b

Further research regarding the command and control IP indicated that it was hosted by the Chinese Internet Service Provider Anchnet Asia Limited. It appeared to be active and in use as a command and control server from at least August 24, 2020 through September 28, 2020. It is notable that this time period predates the period of dormancy discussed above that likely resulted from Recorded Future's publication on TA416 activity. Additionally, it indicates that this server ceased being used during this dormancy period possibly indicating an infrastructure overhaul by actors during this time.

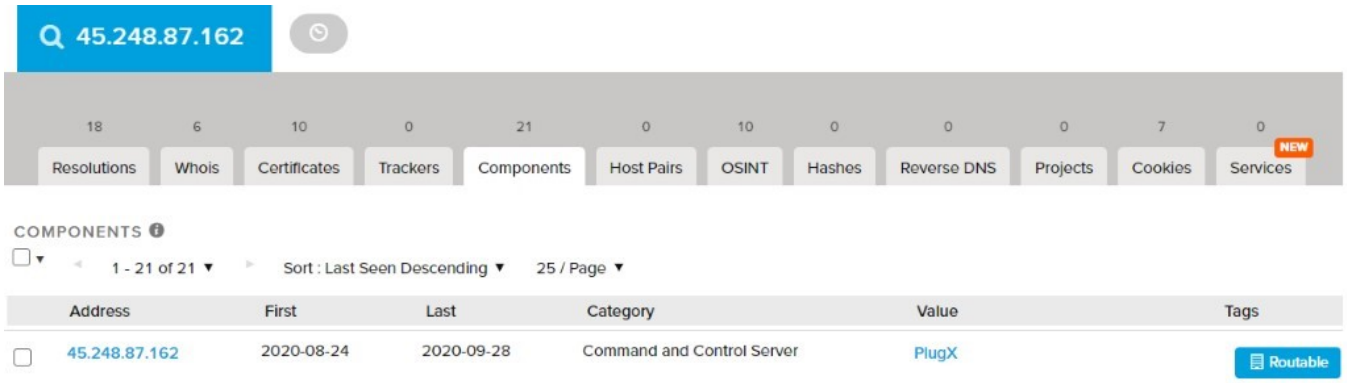


Figure 6: RiskIQ data indicating TA416 command and control server's period of activity.

Conclusion

Continued activity by TA416 demonstrates a persistent adversary making incremental changes to documented toolsets so that they can remain effective in carrying out espionage campaigns against global targets. The introduction of a Golang PlugX loader alongside continued encryption efforts for PlugX payloads suggest that the group may be conscious of increased detection for their tools and it demonstrates adaptation in response to publications regarding their campaigns. These tool adjustments combined with recurrent command and control infrastructure revision suggests that TA416 will persist in their targeting of diplomatic and religious organizations. While the specifics of the tools and procedures have evolved it appears their motivation and targeted sectors likely remain consistent. TA416 continues to embody the persistent aspect of "APT" actors and Proofpoint analysts expect to continue to detect this activity in the coming months.

IOCs

IOC	IOC Type	Description
930b7a798e3279b7460e30ce2f3a2deccbc252f3ca213cb022f5b7e6a25a0867	SHA256	AdobeImdyU.exe Archive Containing PlugX
6a5b0cfdaf402e94f892f66a0f53e347d427be4105ab22c1a9f259238c272b60	SHA256	Adobel.exe Extracting RAR Archive Containing PlugX
0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681	SHA256	Adobelm.exe PE that loads Golang PlugX Loader
235752f22f1a21e18e0833fc26e1cdb4834a56ee53ec7acb8a402129329c0cdd	SHA256	hex.dll Golang binary PlugX Loader
e3e3c28f7a96906e6c30f56e8e6b013e42b5113967d6fb054c32885501dfd1b7	SHA256	AdobeHelp.exe PE File
afa06df5a2c33dc0bdf80bbe09dade421b3e8b5990a56246e0d7053d5668d917	SHA256	adobeupdate.dat Encrypted PlugX Payload
45.248.87[.]162	C2 IP	Command and control IP
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Microsoft\ Windows\CurrentVersion\Run\AdobeImdyU	RegKey	Registry Key that establishes PlugX malware persist

Emerging Threats Signatures

2018228 - et trojan possible plugx common header struct

References:

[1] Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations

[2] Back Despite Disruption: RedDelta Resumes Operations

[3] Holy See and China renew Provisional Agreement for 2 years

[4] New wave of PlugX targets Hong Kong

[5] Emerging Threats Ruleset

Subscribe to the Proofpoint Blog