Mustang Panda Abuses Legitimate Apps to Target Myanmar Based Victims

The BlackBerry Research & Intelligence Team ⋮⋮ 10/6/2022

Executive Summary

The BlackBerry Research & Intelligence Team recently uncovered a campaign by an advanced persistent threat (APT) group called Mustang Panda that is leveraging the PlugX malware family to target the Southeast Asian state of Myanmar.

Our team analyzed the samples in question and found their embedded configurations revealed a set of command-and-control (C2) domains that masquerade as Myanmar news outlets. This is not the first time a campaign targeting this state has impersonated Myanmar news outlets or used PlugX malware.

These tactics, techniques, and procedures (TTPs), along with other corroborating evidence – such as a previous indication that the group was active in this location – lead us to assert with reasonable confidence that the China-based threat group known as Mustang Panda is responsible for this campaign

Mustang Panda: an Origin Story

Mustang Panda (aka HoneyMyte, Bronze President or Red Delta) is a prolific APT group that has been publicly attributed as being based in China. This group conducted malware campaigns as far back as 2012, which primarily related to cyber-espionage.

Their targets have included Government and Non-Government Organizations (NGO) in many locations around the world, from various states in Southeast Asia to the European Union to the U.S. and beyond.

Figure 1 – Partial map of countries previously targeted by Mustang Panda

Mustang Panda Attack Vector

Mustang Panda typically sends phishing emails with malicious document attachments as an initial infection vector. These documents are usually designed to mimic those of the targeted country or organization, or even current world affairs applicable to that region.

Once threat actors gain a foothold within a target organization, they typically deploy one of a variety of payloads such as Cobalt Strike, Poison Ivy, or PlugX, the latter of which is used most extensively.

Initial Thread

In late May of this year, BlackBerry detected some unusual network traffic to a domain – www[.]myanmarnewsonline[.]org. At first glance, this URL appeared to be a Myanmar news website.

The files found to be communicating with this site were encompassed in several .RAR files. These files had a relatively low detection ratio on VirusTotal (VT), and as shown in Figure 2, they followed a naming convention designed to make them appear to be legitimate utilities relating to Hewlett-Packard (HP) printers.

Figure 2 – Communicating RAR files

The RAR archives contained a legitimate signed utility from HP, along with a DLL loader and a DAT file that is an encrypted PlugX payload.

One of the legitimate utilities ("HPCustParticUI.exe" – SHA256 8857232077b4b0f0e4a2c3bb5717fd65079209784f41694f8e1b469e34754cf6) was previously used in a similar fashion as part of a PlugX execution chain, which was documented by another vendor in September 2021.

In early June of this year, a tweet from the user **@kienbigmummy** (shown in Figure 3) mentioned an additional .RAR file titled "service Log.rar" that was linked with a sub-domain of the previously mentioned website – images[.]myanmarnewsonline[.]org – that was associated with PlugX and the Mustang Panda APT group.

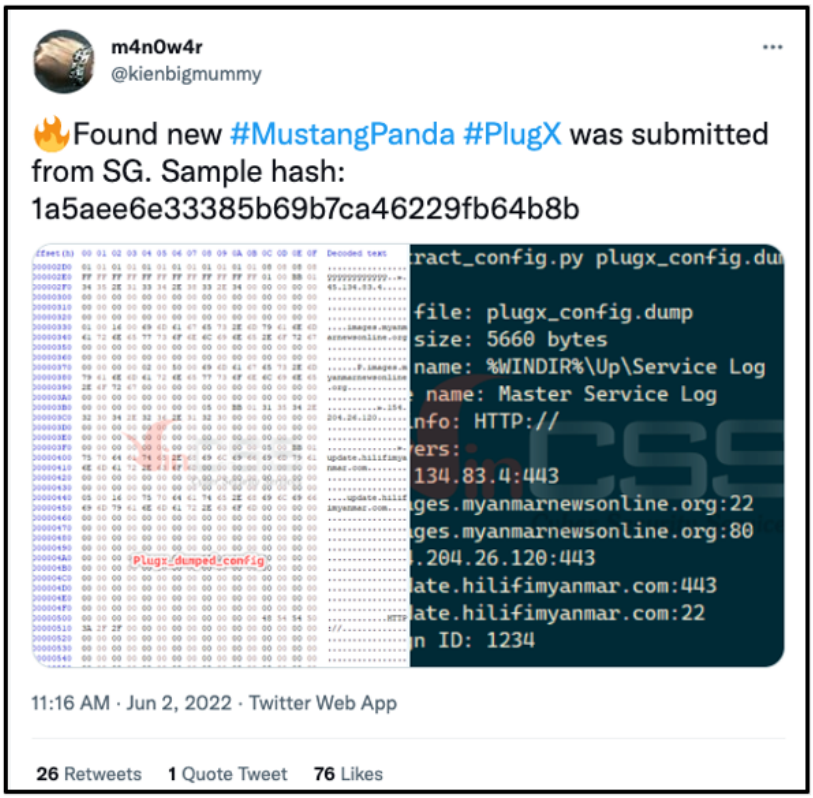

Figure 3 – June 2nd PlugX tweet by @kienbigmummy

We examined the network infrastructure (shown in Figure 4) linked to each of these three RAR files, which provided evidence of additional samples that conform to the same or similar TTPs going back as far as late 2020, along with other sample types such as Cobalt Strike beacon.

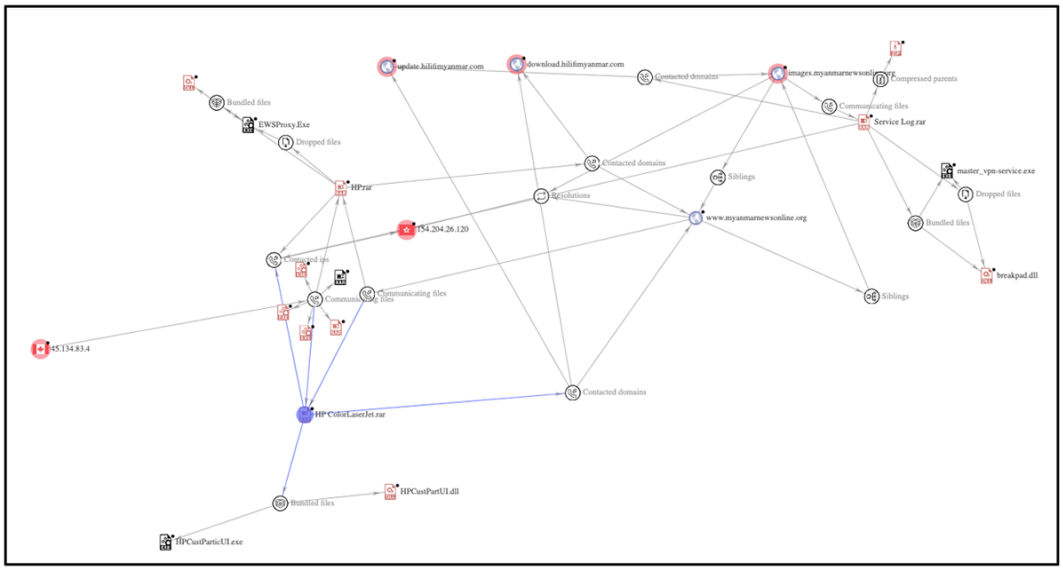

Figure 4 – VirusTotal graph of network infrastructure

What is PlugX?

PlugX is a remote access tool (RAT) used by several threat groups. It is the malware of choice for the Chinese APT group Mustang Panda. This group delivers the PlugX implant in the form of an encrypted data blob, which is typically paired with a DLL loader as well as a benign application.

This actor has commonly employed the stealthy technique of side-loading the malicious DLLs into legitimate applications during execution. This action then deploys the PlugX implant into memory.

We noted threat actors had used three separate legitimate applications within our RAR files; A free VPN service, and two legitimate HP applications related to HP's Digital Imaging. Each legitimate application was bundled with a DLL and a data file. In two out of the three RAR files, the DAT file masqueraded as a different file format, such as JSON or CHM.

Upon execution of the legitimate application, the threat loads a malicious DLL loader in a specific set order, which the threat actor has strategically placed in the same folder to replace a legitimate one. This proceeds to side-load the DLL by abusing the DLL search order, which is a technique also known as DLL Search Order Hijacking. The malicious DLL is then loaded into the legitimate application, where it decrypts, loads and deploys the malicious PlugX implant. This execution chain is shown in Figure 5.

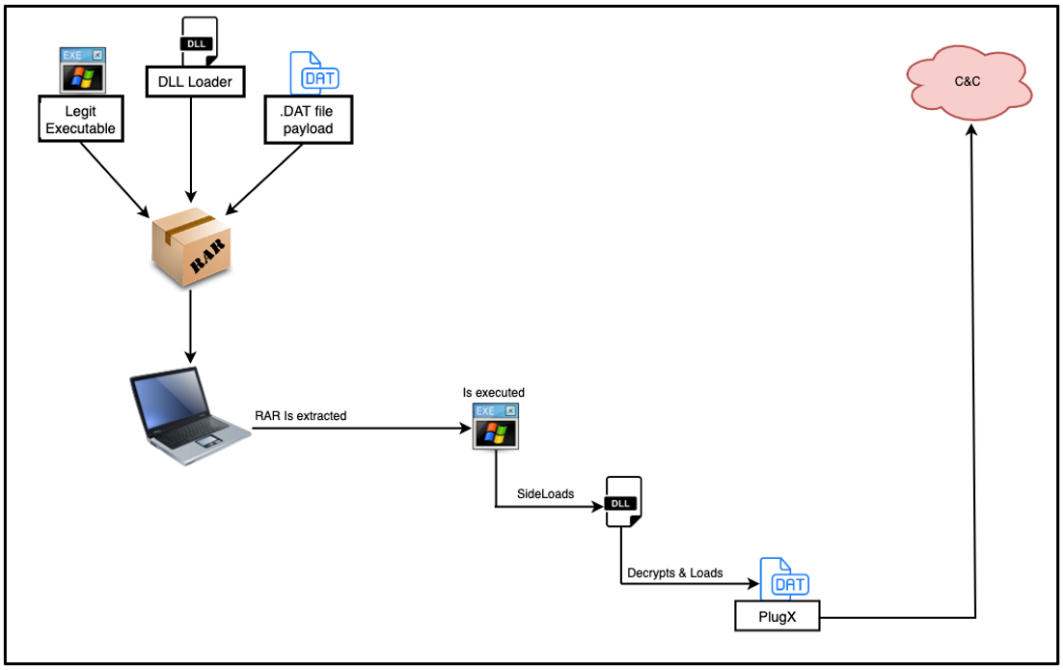

Figure 5 – PlugX side-loading execution chain

Technical Analysis

The DLL loader is heavily obfuscated and employs dynamic API resolution upon runtime. It retrieves a handle to the encrypted PlugX implant, then reads the data into a newly allocated region within memory. Execution is then passed to the implant, where the shellcode is executed, and it XOR decrypts the embedded payload, as shown in Figure 6. Once decryption is complete, **RtlDecompressBuffer** is called to decompress the decrypted payload to its final form as shown in Figure 7.

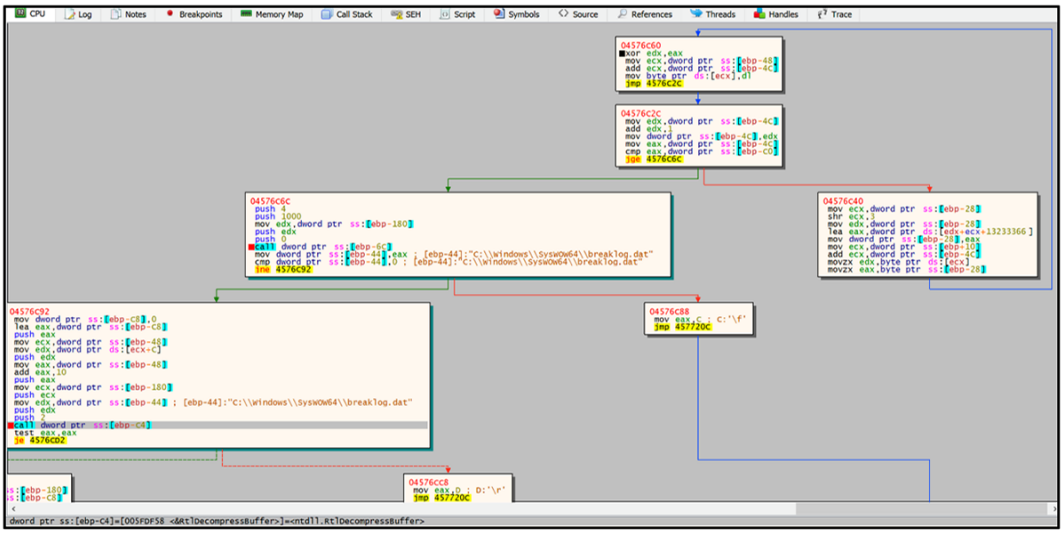

Figure 6 – Decryption routine

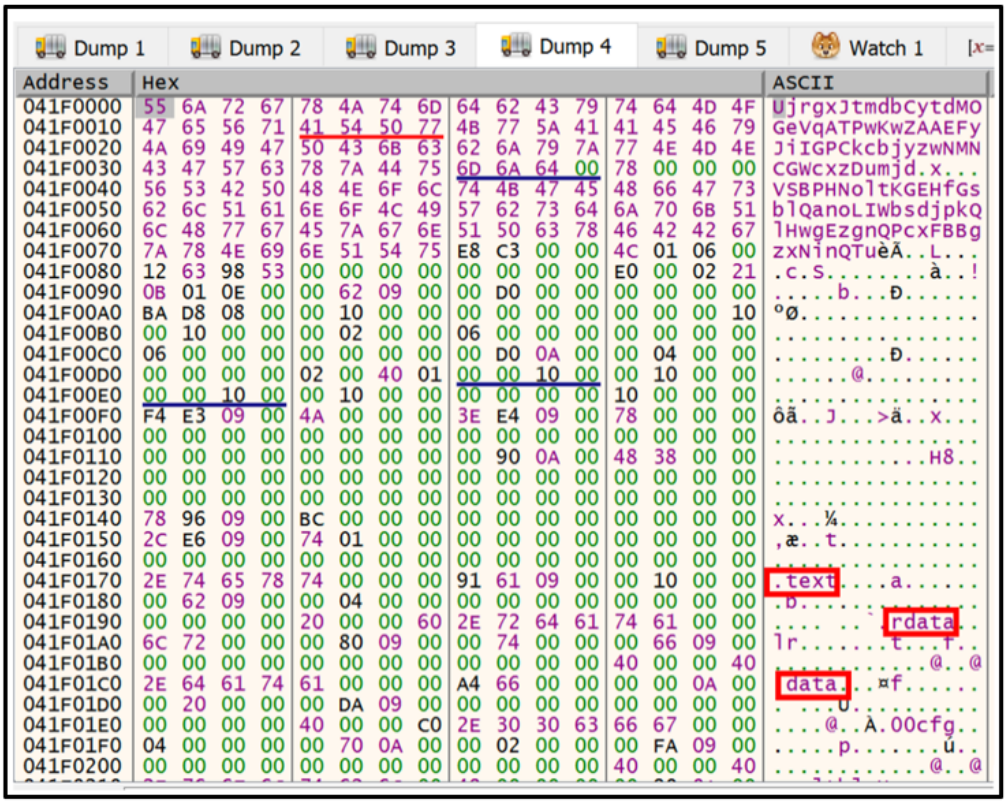

Figure 7 – Decrypted payload header

Conclusion

Mustang Panda, which is publicly known as a Chinese-affiliated APT group, has an established history of using the PlugX malware and targeting nations throughout South-East Asia. This threat actor has been previously linked to campaigns targeting Myanmar government entities using custom lures and compromising the website of the office of Myanmar's president.

The TTPs associated with the campaign covered in this report align with those of Mustang Panda. We observed a typical attack chain employed by the group, where attackers used a benign executable to side-load a malicious DLL loader, which then decrypts and loads the PlugX implant. We have also confirmed the C2 infrastructure associated with this campaign has been used to target entities in Myanmar, including a government VPN portal, from early March onwards.

Indicators of Compromise (IoCs)

File

SHA256	Name	Description
843709a59f12ff7aa06a5837be7a1a93fdf6f02f99936af6658c166e8abcaa2d	Service Log.rar	RAR file encompassing a legit signed utility + a DLL loader + a DAT PlugX payload
0f3ec2a01ae57c7dd2bb8f130f0f2d1c20fcb397e5b8bbff491517b6d179919e	HP.rar	RAR file encompassing a legit signed utility + a DLL loader + a DAT PlugX payload
558cbbcb969fe2fa3f1c74c376e307efcdbe3bad7497095619927edd5762363a	HP ColorLaserJet.rar	RAR file encompassing a legit signed utility + a DLL loader + a DAT PlugX payload

Network

Indicator	Type	Description
Update[.]hilifimyanmar[.]com	Domain	C&C
Download[.]hilifimyanmar[.]com	Domain	C&C
Images[.]myanmarnewsonline[.]org	Domain	C&C
www[.]myanmarnewsonline[.]org	Domain	C&C
154[.]204[.]26[.]120	IP	C&C
45[.]134[.]83[.]4	IP	C&C

Defense

Yara Rule for Mustang Panda

```
rule targeted_MustangPanda_dll {
   meta:
      description = "Rule to detect malicious DLL originally used to target Myanmar"
      author = "The BlackBerry Research & Intelligence team"
      version = "1.0"
      last_modified = "2022-08-02"
      hash = "74fe609eb8f344405b41708a3bb3c39b9c1e12ff93232d4b7efe648d66ea7380"
      hash = "a0d7e541d5c579d2e0493794879fee58d8603b4f3fb146df227efa34c23d830e"
      hash = "efade7cf8f2caeb5a5d1cf647796975b0b153feac67217fccbdd203e473a4928"
      license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and oper
or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research
Team"
   strings:
      $code1 = {88E280F20088DD20D588C680F6FF80E60020D008E908C630F188D834FF88CA30C220CA88D834FF88F920C
D988C834FF88D530C520D588D034FF88CE20C680F1FF20CA08D688E834FF88F180F1FF80F4}
      $code2 =
{EA08D188DA80F2FF88CD30D520CD34FF88F980F1FF88E280F20008C880CA0034FF20D088E920C130C508E988D834FF88
F88DD20C508EA88D820}
   condition:
   uint16(0) == 0x5A4D and
   filesize < 10MB and
   any of them
}
```

MITRE ATT&CK

T1583.001 Acquire Infrastructure: Domains

T1027 Obfuscated Files or Information

T1036.005 Masquerading: Match Legitimate Name or Location

T1574.002 Hijack Execution Flow: DLL Side-Loading

D3FEND

D3-FA (File Analysis)

D3-LFP (Local File Permissions)

D3-DA (Dynamic Analysis)

D3-EFA (Emulated File Analysis)

D3-EAL (Executable Allowlisting)

D3-SCA (System Call Analysis)