Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets

The BlackBerry Research & Intelligence Team ⋮⋮ 12/6/2022

Mustang Panda continue targeting countries across Europe and Asia Pacific, utilizing current geopolitical events to their advantage. Their attack chain remains consistent, with the continued use of archive files, shortcut files, malicious loaders, and the use of PlugX malware. Based on the lure covered in this blog, the goal of this particular operation appears to be collecting sensitive information from European countries and states from Asia, which might be supporting Western countries.

Summary

As part of ongoing hunting and continuous monitoring efforts regarding the advanced persistent threat (APT) group Mustang Panda, the BlackBerry Threat Research and Intelligence team recently came across an interesting RAR file titled "*Political Guidance for the new EU approach towards Russia.rar*".

This file captured our interest due to the ongoing geopolitical situation in Eastern Europe. An examination of its contents revealed a decoy document matching the naming convention of the RAR, along with additional components that are often seen as part of a typical PlugX infection chain.

By delving into the associated network infrastructure and pivoting off related network artifacts, additional files and infrastructure were uncovered. These conformed to similar Tactics, Techniques, and Procedures (TTPs) and appeared to be part of a larger campaign from this same threat actor targeting multiple entities, both Government and Private, in several industries and throughout many countries across the world. In this report, we document what we found.

You can read our previous post on Mustang Panda here.

Weaponization and Technical Overview

Weapons	DLL Loaders + encrypted .dat payloads
Attack Vector	Current event-themed phishing lures
Network Infrastructure	Web based command-and-control (C2)
Targets	Mining, Education, Telecoms, Financial, CDN Companies, Internet Service Providers, Internet Security Firms, Web Hosting Companies

Technical Analysis

Context

Mustang Panda, also known as HoneyMyte, Bronze President or Red Delta, is one of the more active APT groups in operation on the threat landscape today, with a wide variety of campaigns documented as far back as 2012. It is publicly attributed to China-based cyberespionage threat actors.

It is continually honing its capabilities, but its core approach remains consistent, with the use of themed lures related to current events. These contain decoy documents and legitimate applications that are susceptible to DLL search order hijacking.

This is exploited to coerce targets into executing a malicious loader to deliver a PlugX payload. The RAR archive – "*Political Guidance for the new EU approach towards Russia.rar*" – aligned with numerous TTPs related to Mustang Panda that have previously been documented by both BlackBerry and other vendors.

Mustang Panda Attack Vector

A RAR file is an archive that contains one or more files compressed with RAR compression. As seen in recent campaigns, the use of archives is a common infection vector for Mustang Panda. The political theme of the RAR file is a tactic employed by the threat actor to coerce targets into opening the file. Once the archive is open, the victim will see a directory called "_" and a shortcut file named with the same politically themed lure.

The .LNK file uses a double file extension in an attempt to disguise the shortcut file as a document in the hope the target would open it, in the process executing the shortcut file. This utilization of double extensions has been used by Mustang Panda in the past as a way to convince users to execute the shortcut file.

The shortcut file contains a command that kicks off the initial execution of the attack chain:

"C:\Windows\System32\cmd.exe /c "____________________\test11.bpu||(forfiles /^P %USERPROFILE%\ /S /^M "Political Guidance for the new EU approach towards Russia.rar" /C "cmd /c (c:\progra~1\7-Zip\7z x -y -aoa @path||c:\progra~2\7-Zip\7z x -y -aoa @path"

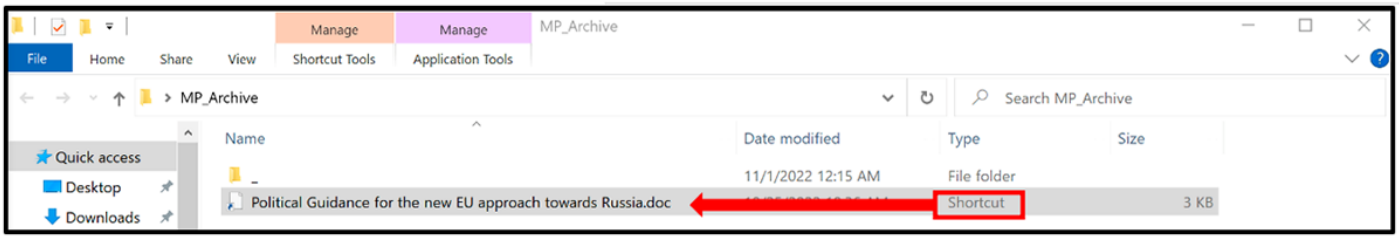

Figure 1: Phishing lure contents

The LNK file looks to execute “test11.bpu”, which is a legitimate portable executable (PE) file called “ClassicExplorerSettings.exe” belonging to Classic Shell, which is a freeware utility used to customize the look of the Windows® system.

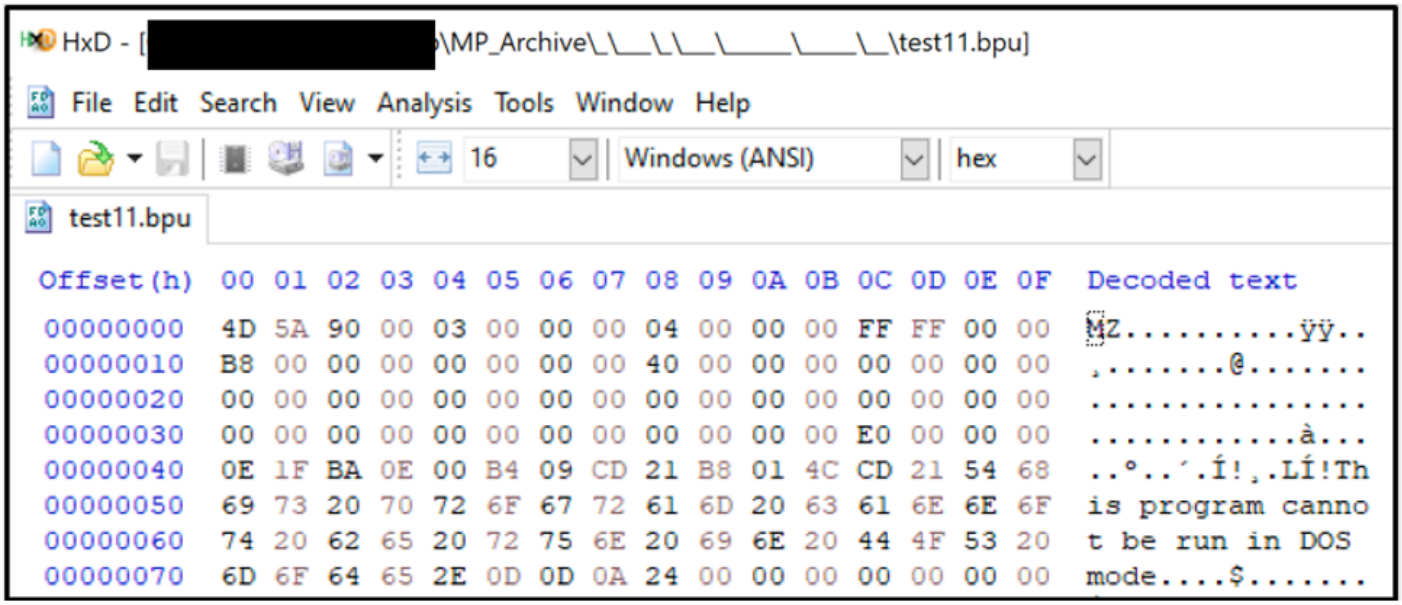

Figure 2: MZ file header

Hashes (md5, sha-256)	7177ab83a40a4111eb0170a76e92142b f70d3601fb456a18ed7e7ed599d10783447016da78234f5dca61b8bd3a084a15
File Name	Political Guidance for the new EU approach towards Russia.rar
File Size	567144 bytes
Created	2022-11-01 02:32
Last Modified	1979-11-29 13:00

Weaponization

The Mustang Panda attack chain is reliant on the DLL sideloading technique previously used in their campaign targeting Myanmar, where the threat actor plants both a legitimate executable and a payload alongside each other, a technique which is designed to take advantage of the search order of a program as soon as the legitimate application has been invoked. Once the shortcut file is executed, the legitimate application will be launched and the malicious DLL loader will also get invoked.

“ClassicExplorer32.dll” is planted in the same directory as “test11.bpu” to abuse the search order once the executable is invoked. The purpose of the DLL is to load the “ClassicExplorerLog.dat” file and execute the shellcode within it. Interestingly, the loader used seems to have a subtle change in how the shellcode is decrypted and executed.

Mustang Panda DLL loaders reported by Secureworks back in September were utilizing the *EnumThreadWindows* API to pass execution to the start of the malicious payload file. In these more recent samples, the DLL loader uses the *EnumSystemCodePagesW* API to execute the shellcode similarly. A pointer to the already decrypted shellcode is passed to *EnumSystemCodePagesW* API as an application-defined callback function, as seen in Figure 3 below. The use of the *EnumSystemCodePagesW* API was mentioned in a Twitter thread by kienbigmummy and also seen in a Black Hat Asia presentation. The purpose of the shellcode is to decrypt and execute the final malicious payload – PlugX – in memory.

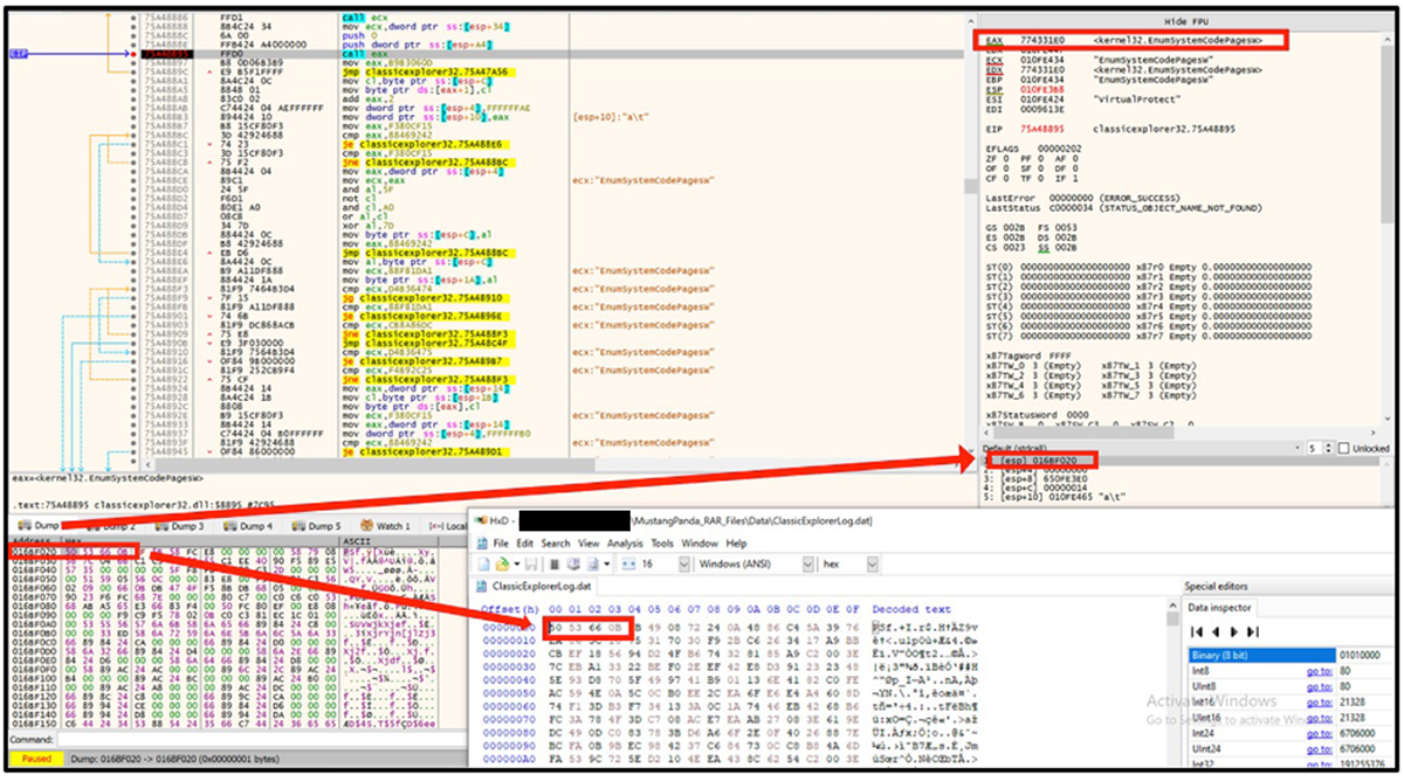

Figure 3: DLL Loader utilizing EnumSystemCodePagesW to load and execute shellcode

Hashes (md5, sha-256)	ae105528a6c5758ccf18705a8c208a97 b44cc792ae7f58e9a12a121c14a067ee1dd380df093339b4bf2b02df5937b2af
ITW File Name	ClassicExplorerSettings.exe
Compilation Stamp	2017-08-13 15:49:42 UTC
File Type/Signature	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	98616 bytes
Hashes (md5, sha-256)	6d6a0ca7c7343eedfffeb697229a4929 8e27900949a087349488d82e7434937bd253d31749041bb0233000a7339fc3e1
ITW File Name	ClassicExplorer32.dll
Compilation Stamp	2022-10-25 09:32:51 UTC
File Type/Signature	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File Size	115000 bytes
Hashes (md5, sha-256)	a95f48acd5da4beddd4115e12653c23c 9c1ea202237726984b754d17528cfab0212ff9587bbffaf01c8535277b01c24a
ITW File Name	ClassicExplorerLog.bin, ClassicExplorerLog.dat
File	DATA File

Type/Signature	
File Size	614718 bytes

Once the PlugX payload has been decrypted and execution is passed to the payload, we can see the config also get decrypted into memory. Here we can see the IP address 5[.]34[.]178[.]156, the campaign ID of “test222”, as well as the name of the decoy document that gets displayed to the victim.

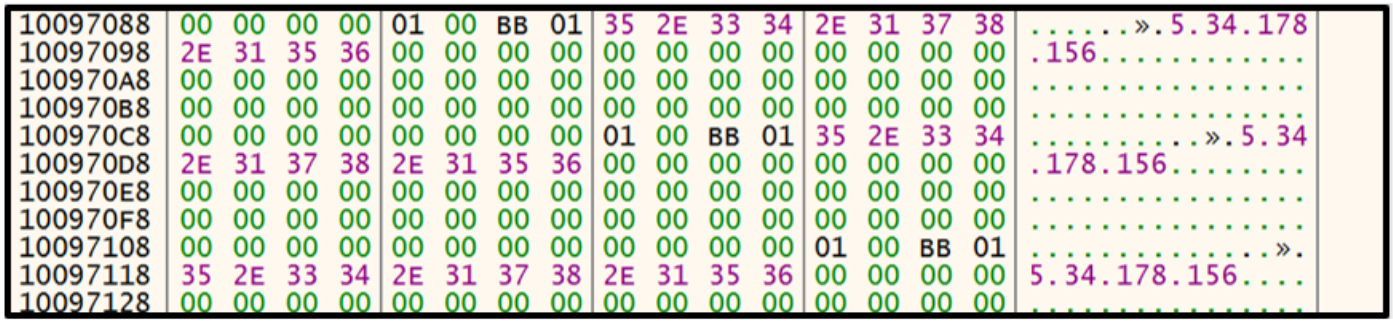

Figure 4: PlugX config C2

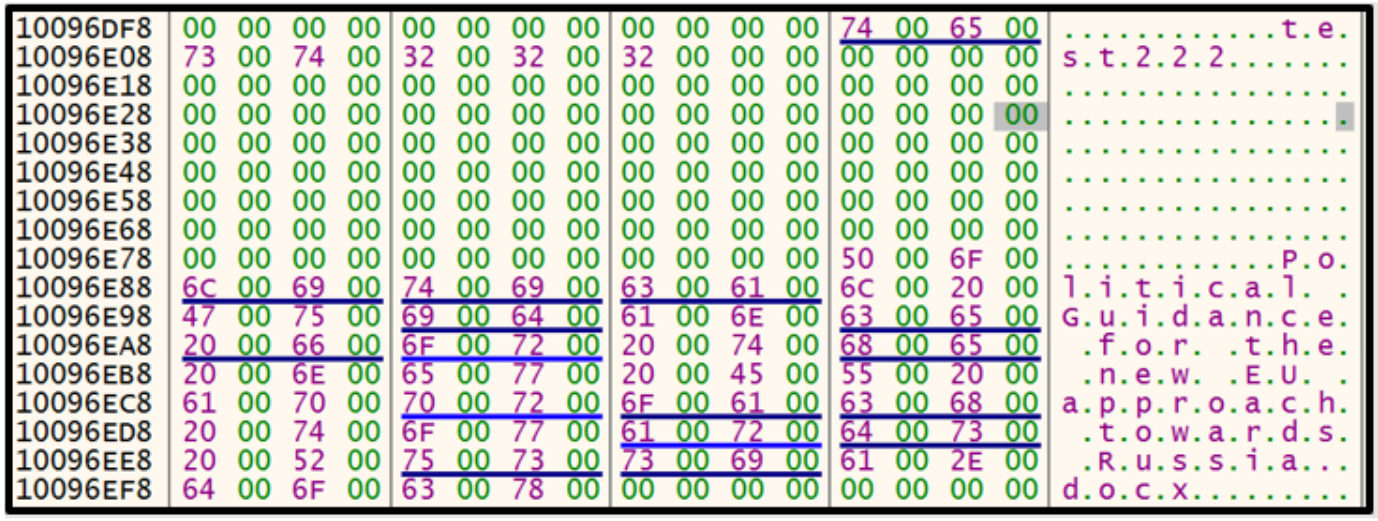

Figure 5: PlugX campaign ID + decoy document name

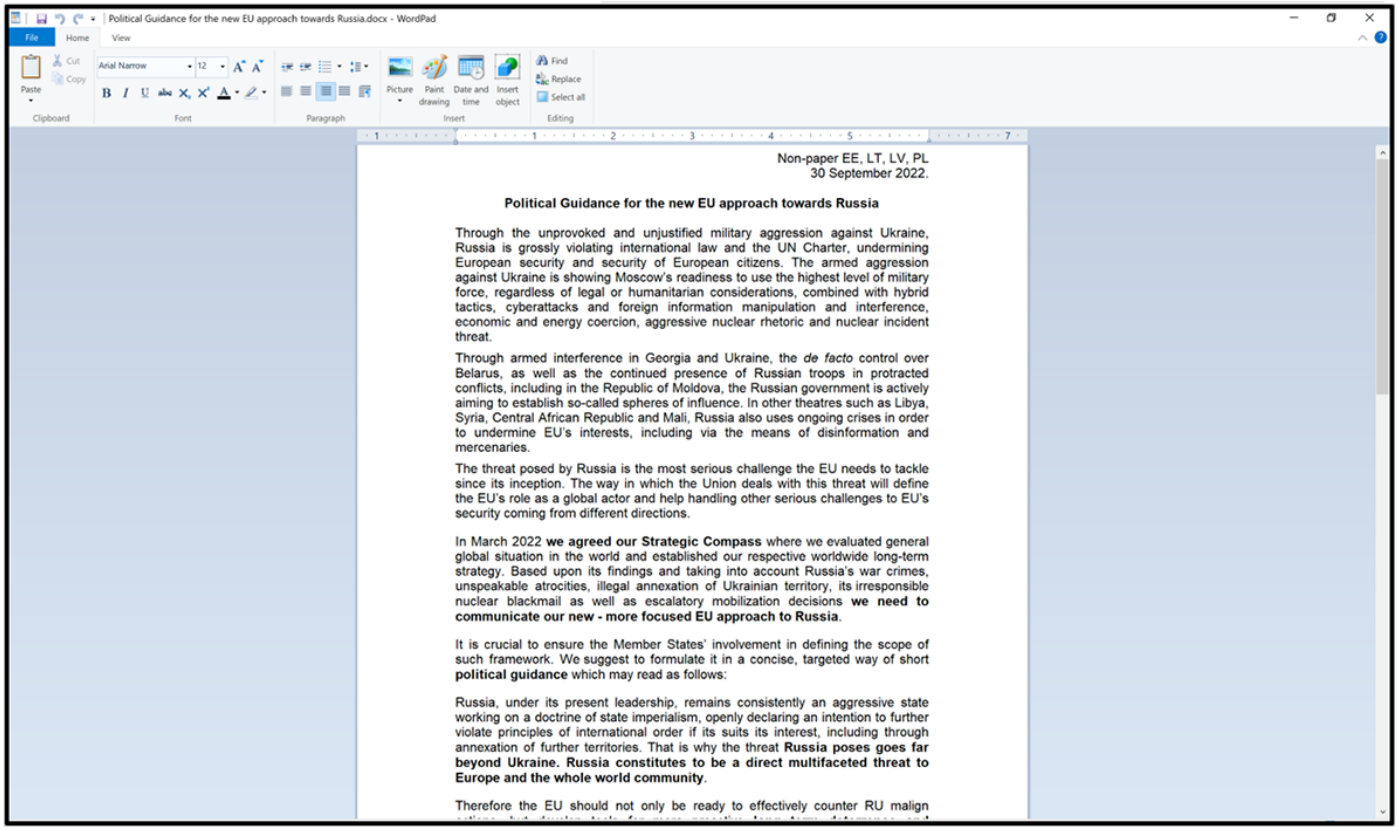

Figure 6: Decoy document

Network Infrastructure

The C2 IP address – 5[.]34[.]178[.]156 – was seen to be hosting a service on port 443 with a unique SSL certificate. The SSL certificate was first seen being associated with this IP from the period 2022-10-07 to 2022-10-30.

Domain Name	Samples' Hashes	First/Last Seen/ASN
5[.]34[.]178[.]156	a95f48acd5da4beddd4115e12653c23c 9c1ea202237726984b754d17528cfab0212ff9587bbffaf01c8535277b01c24a	2022-07-19 2022-10-31 ASN:204957

CN=45.134.83.29,OU=TLS Demo Cert,O=File Transfer Service, 2.5.4.46= #13186d67332f6d4c506d4b335966582f4d614a43732f6d673d3d Issuer - CN=CTA Root CA, O=TEST TEST TEST, 2.5.4.46=#13185843794c4248705065757479714b4344383866614e773d3d

Additional Linked Infrastructure

Pivoting on the certificate showed 15 other IP addresses utilizing the same SSL certificate. Five of these were being used as C2 servers for the same attack chain delivering lures/decoys in the form of RAR files, in the hopes of the victims executing PlugX malware in memory.

The lures all varied but all aligned with the previous campaigns associated with Mustang Panda.

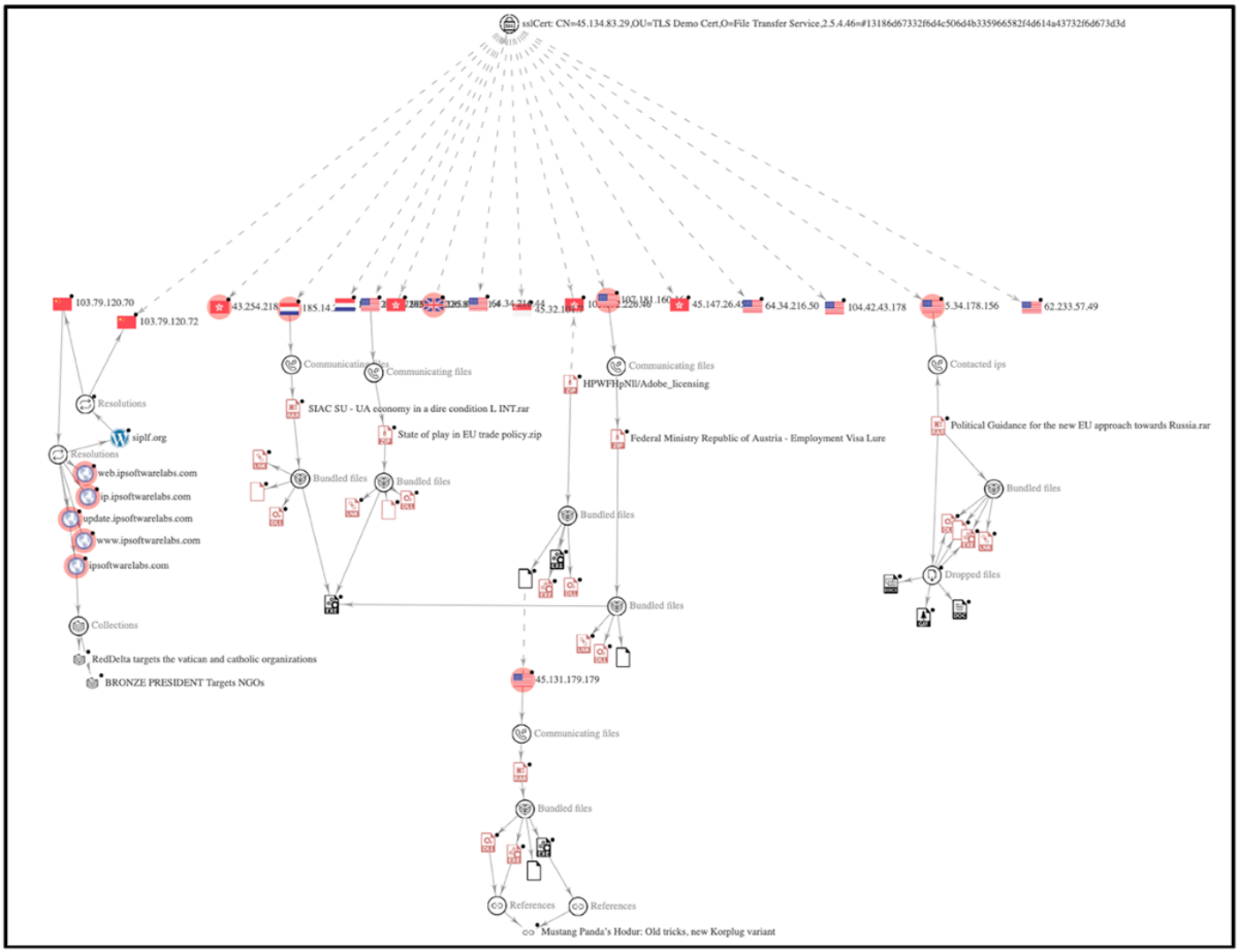

Figure 7: SSL certificate showing C2 pivoting

Targets

Mustang Panda's previous 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. Considering the decoy lures found, as well as the correlating network telemetry, we found the threat actor to be targeting areas in Europe as well as Asia-Pacific, specifically Vietnam. This is not an exhaustive list as we have been unable to identify the industries of all the victims thus far.

Figure 8: Partial list of victims

Conclusions

Mustang Panda continues to utilize well-thought-out lures related to current events to deliver the PlugX malware that the group is synonymous with. While Mustang Panda has stayed within their typical TTPs with PlugX, including custom lures, double extensions, and infrastructure re-use, they do make subtle changes along the way in the hope of evading detection. The historical data associated with the pivoted SSL certificate shows it being first seen on 2022-02-27. It is still being actively used at the time of writing.

Mustang Panda has a history of targeting many different entities across the globe, but their target aligns with the interests of the Chinese government. From the associated lures, NetFlow data, and other characteristics, the EU and APAC have been their biggest targets as of late.

Referential Indicators of Compromise (IoCs)

Main File

File Name	Political Guidance for the new EU approach towards Russia.rar
SHA256	F70d3601fb456a18ed7e7ed599d10783447016da78234f5dca61b8bd3a084a15
File Type	RAR
Network Indicator (C2)	5[.]34.178.156

Network Indicators

C2
104[.]42.43.178
64[.]34.216.50
45[.]147.26.45
45[.]32.101.7

64[.]34.216.44
185[.]80.201.4
103[.]192.226.87
194[.]124.227.90
43[.]254.218.128
62[.]233.57.49

Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique name
Execution	T1203	Exploitation for Client Execution
Execution	T1106	Native API
Execution	T1129	Shared Module
Execution	T1559.001	Component Object Model
Execution	T1204.002	Malicious File
Execution	T1059.003	Windows Command Shell
Persistence/Privilege Escalation	T1547.001	Registry Run Keys / Startup Folder
Defense Evasion	T1574.002	DLL Side-Loading
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1036	Masquerading
Defense Evasion	T1036.007	Double File Extension
Defense Evasion	T1218	System Binary Proxy Execution
Defense Evasion	T1564.001	Hidden Files and Directories
Defense Evasion	T1140	Deobfuscate Decode Files or Information
Discovery	T1057	Process Discovery
Discovery	T1082	System Information Discovery
Discovery	T1518	Software Discovery
Discovery	T1033	System Owner/User Discovery
Collection	T1560.001	Archive via Utility
Persistence	T1547.009	Shortcut
Command and Control	T1071.001	Web Protocols