Hive Pro

THREAT ADVISORY

Mustang Panda targets European diplomats using enhanced PlugX backdoor	**TA2022056**
Threat Level **RED**	**Publish Date –** Mar 11, 2022

Mustang Panda, a Chinese cyberespionage group, has been targeting European diplomats with a revised version of the PlugX backdoor in an ongoing campaign linked to the ongoing conflict in Ukraine. The group, also known as RedDelta and TA416, has previously been observed targeting entities associated with the Vatican-Chinese Communist Party diplomatic ties, as well as other critical sectors in Asia, Europe, and the United States.

The group has been observed distributing phishing emails including links to dangerous Zip files housed on Dropbox. If the files are opened, they finally lead to the execution of PlugX on the victim's device. Web bugs are used to profile users before distributing a variety of PlugX malware payloads through malicious URLs. Previously, DLL search order hijacking was used to deploy PlugX, but in newer operations, the threat actor shifted to employing potplayermini.exe to start the hijacking process. In addition, the attackers improved the encoding process of their virus and enhanced its configuration possibilities.

The TTPs commonly used by Mustang Panda are:
TA0042 - Resource Development
TA0001 - Initial Access
TA0002 - Execution
TA0003 - Persistence
TA0004 - Privilege Escalation
TA0005 - Defense Evasion
TA0006 - Credential Access
TA0007 - Discovery
TA0008 - Lateral Movement
TA0009 - Collection
TA0011 - Command and Control
TA0010 - Exfiltration
T1583.001: Acquire Infrastructure: Domains
T1071.001: Application Layer Protocol: Web Protocols
T1560.001: Archive Collected Data: Archive via Utility
T1560.003: Archive Collected Data: Archive via Custom Method
T1119: Automated Collection
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1059.001: Command and Scripting Interpreter: PowerShell
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1059.005: Command and Scripting Interpreter: Visual Basic
T1074.001: Data Staged: Local Data Staging
T1573.001: Encrypted Channel: Symmetric Cryptography
T1546.003: Event Triggered Execution: Windows Management Instrumentation Event Subscription
T1052.001: Exfiltration Over Physical Medium: Exfiltration over USB
T1203: Exploitation for Client Execution
T1083: File and Directory Discovery

T1564.001: Hide Artifacts: Hidden Files and Directories
T1574.002: Hijack Execution Flow: DLL Side-Loading
T1070.004: Indicator Removal on Host: File Deletion
T1105: Ingress Tool Transfer
T1036.005: Masquerading: Match Legitimate Name or Location
T1036.007: Masquerading: Double File Extension
T1027: Obfuscated Files or Information
T1027.001: Binary Padding
T1003.003: OS Credential Dumping: NTDS
T1566.001: Phishing: Spearphishing Attachment
T1566.002: Phishing: Spearphishing Link
T1057: Process Discovery
T1219: Remote Access Software
T1091: Replication Through Removable Media
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.004: Signed Binary Proxy Execution: InstallUtil
T1218.005: Signed Binary Proxy Execution: Mshta
T1518: Software Discovery
T1082: System Information Discovery
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery
T1204.001: User Execution: Malicious Link
T1204.002: User Execution: Malicious File
T1047: Windows Management Instrumentation

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Mustang Panda (TA416, RedDelta, BRONZE PRESIDENT)	China	Australia, China, Czech, Ethiopia, Germany, Hong Kong, India, Indonesia, Italy, Myanmar, Slovakia, Spain, Ukraine, USA, UK Vietnam, Singapore, South Korea, Taiwan	Aviation, Government, Law enforcement, Telecommunications, Embassies	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
SHA-256	6fd9d745faa77a58ac84a5a1ef360c7fc1e23b32d49ca9c3554a1edc4d761885, 5851043b2c040fb3dce45c23fb9f3e8aefff48e0438dec7141999062d46c592d, effd63168fc7957baf609f7492cd82579459963f80fc6fc4d261fbc68877f5a1, b2ff5535caa1d70c9d0d59cd68619b142858ae018064c891b4671154aa93abf3, 54b491541376bda85ffb02b9bb40b9b5adba644f08b630fc1b47392625e1e60a, a4ff2c5913cce536759777acee3cfcc8824b927304c8a93ac64d37d1b01a576f, a07cece1fa9b3c813c0b6880b24a6494a9db83e138102da3bce30ebff51909c0, 0c2f5b6fe538d088fed11ab10925210cb2eb782f471e6f09c484677e82fc5f26, ec32ff0c049bd8812a35aeaaaae1f66eaf0ce8aefce535d142862ae89435c2e2, 76da9d0046fe76fc28b80c4c1062b17852264348fd873b7dd781f39491f911e0, 19870dd4d8c6453d5bb6f3b2beccbbbe28c6f280b6a7ebf5e0785ec386170000, e1dbe58393268d7ddabd4bed0cdedf0fbba85d4c3ef1300580ed4c74e147aa61,

Type	Value
SHA-256	436d5bf9eba974a6e97f6f5159456c642e53213d7e4f8c75db5275b66fedd886, a01f353c92afcd45b5731815c79f1e1d01366cefa75b41550a28d999857c5b88, 472822c6bdc710175987eb7d9171f780c974a83ea2b26f117b748babb9b796b8, fac8de00f031299f6c698b34534d6523428b544aad6a40fdc4b000a04ee82e7c, 82df9817d0a8dca7491b0688397299943d9279e848cdc4a5446d3159d8d71e6f, b9e330373b382beaf4f0bcce83d65f13399d42dc3e9fcdc7b4ef26fa89360762, 03a836034360841fd6b99927c5b639d074e9fce4f16bd4f77ab57a9e5c12d976
IPs	103.107.104[.]19, 69.90.184[.]125, 45.154.14[.]235
URLs	hxxps://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip, hxxps://www.dropbox[.]com/s/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip?dl=1, hxxps://www.dropbox[.]com/s/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip/?dl=1, hxxps://www.dropbox[.]com/s/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip/?dl=1, hxxps://uepspr[.]com/2023/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip, hxxps://uepspr[.]com/2023/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip, hxxps://www.dropbox[.]com/s/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip/?dl=1, hxxps://www.dropbox[.]com/s/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip/?dl=1, hxxps://uepspr[.]com/2023/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip, hxxps://uepspr[.]com/2023/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip, https://upespr[.]com/Council conclusions on the European security situation.zip hxxps://45.154.14[.]235/mfa/Council%20conclusions%20on%20the%20European%20security%20situation.pdf, hxxp://www.zyber-i[.]com/europa/2022.zip, hxxps://69.90.184[.]125/lt/2023.rar, hxxps://45.154.14[.]235/2023/PotPlayer.exe, hxxps://45.154.14[.]235/2023/PotPlayer.dll, hxxps://45.154.14[.]235/2023/PotPlayerDB.dat, hxxp://103.107.104[.]19/2022/eu.docx, hxxp://103.107.104[.]19/FontEDL.exe, hxxp://103.107.104[.]19/DocConvDll.dll, hxxp://103.107.104[.]19/FontLog.dat, hxxps://69.90.184[.]125/lt/2022.pdf, hxxps://69.90.184[.]125/lt/FontEDL.exe, hxxps://69.90.184[.]125/lt/DocConvDll.dll, hxxps://69.90.184[.]125/lt/FontLog.dat, hxxps://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf, hxxps://45.154.14[.]235/PotPlayer.exe, hxxps://45.154.14[.]235/PotPlayer.dll,

Type	Value
URLs	hxxps://45.154.14[.]235/PotPlayerDB.dat, hxxp://upespr[.]com/PotPlayerDB.dat, hxxp://upespr[.]com/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf, hxxp://upespr[.]com/PotPlayer.dll, hxxp://upespr[.]com/PotPlayer.exe, hxxps://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf, hxxps://45.154.14[.]235/PotPlayer.exe, hxxps://45.154.14[.]235/PotPlayer.dll, hxxps://45.154.14[.]235/PotPlayerDB.dat
Domain	upespr[.]com, www.zyber-i[.]com

References

https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://www.securityweek.com/chinas-hacking-european-diplomats-aligns-russia-ukraine-conflict