Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

European Ministries Fall Victim to Chinese Hacker's SmugX Campaign

Date of Publication	Admiralty Code	TA Number
July 05, 2023	A1	TA2023287

Summary

First Seen: December 2022
Malware: a new variant of the PlugX
Targeted Industry: Foreign Affairs ministries and embassies
Attack Region: Europe
Attack: A Chinese nation-state group has been persistently conducting a campaign targeting Foreign Affairs ministries and embassies in Europe. They employ HTML smuggling techniques to distribute a new variant of the PlugX remote access trojan.

Attack Regions

Attack Details

#1 Since at least December 2022, a Chinese nation-state group has been engaging in a persistent campaign that involves using HTML smuggling techniques to deliver a new variant of the PlugX remote access trojan employed in the SmugX campagin. The group primarily targets Foreign Affairs ministries and embassies in Europe.

#2 This activity aligns with a broader pattern observed among Chinese adversaries, such as the RedDelta and Mustang Panda Chinese APT actors, who are also involved in similar campaigns. It is important to note that there is currently insufficient evidence to establish a direct connection between this ongoing campaign and Camaro Dragon.

#3 The latest attack sequence is noteworthy because it involves the use of HTML Smuggling, It is a covert technique that exploits legitimate HTML5 and JavaScript features to assemble and activate the malware. The campaign employs two main infection chains, both of which start with HTML smuggling resulting in the download of either a JavaScript file that downloads and executes an MSI file or a ZIP file that invokes Powershell to execute a malicious LNK file. On successful execution, it drops & infects the system with PlugX RAT.

#4 This technique is employed in the decoy documents attached to spear-phishing emails. The content of the lures used in the SmugX campaign reveals the target profile of the threat actor and indicates that the primary objective of the campaign is likely espionage.

Recommendations

- Strengthen email security protocols to detect and block spear-phishing attempts utilizing HTML Smuggling techniques. Implement advanced threat intelligence solutions to identify and filter out malicious attachments and decoy documents.
- Deploy robust intrusion detection and prevention systems capable of identifying and mitigating advanced malware, such as the PlugX trojan. Additionally, establish an incident response plan to enable swift actions in the event of a successful attack, encompassing containment, analysis, and recovery procedures.
- Conduct regular cybersecurity awareness training sessions to educate employees about the risks associated with spear-phishing and social engineering tactics. Emphasize the importance of carefully scrutinizing email attachments, especially those received from unfamiliar or suspicious sources.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1203 Exploitation for Client Execution	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading
T1036 Masquerading	T1140 Deobfuscate/Decode Files or Information	T1497 Virtualization/Sandbox Evasion	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1010 Application Window Discovery	T1046 Network Service Discovery	T1057 Process Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1573 Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd, 736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af, 0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1, 989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05, 10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee, 324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b

TYPE	VALUE
SHA256	c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1, 9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a, 5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db, baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3, 720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05, 460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76, 277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347, 3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee, 27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c, ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2, fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429, 3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb, 04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61, bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6, ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a, b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405, 2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e, 0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0, 0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1, a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7, bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880, 4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838, 0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0

TYPE	VALUE
SHA256	62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c, f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42, bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5, 8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8, ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4, bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1, ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659, 8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32, 8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3, ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d, 1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885, 08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12
IPv4	45[.]90[.]58[.]69, 62[.]233[.]57[.]136, 217[.]12[.]207[.]164, 152[.]152[.]12[.]12
Domains	jcswcd[.]com, newsmailnet[.]com
Paths	C:\Users\<username>\VirtualFile, C:\Users\Public\VirtualFile, C:\Users\<username>\SamsungDriver, C:\Users\Public\SamsungDriver, C:\Users\Public\SecurityScan

References

https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/#single-post

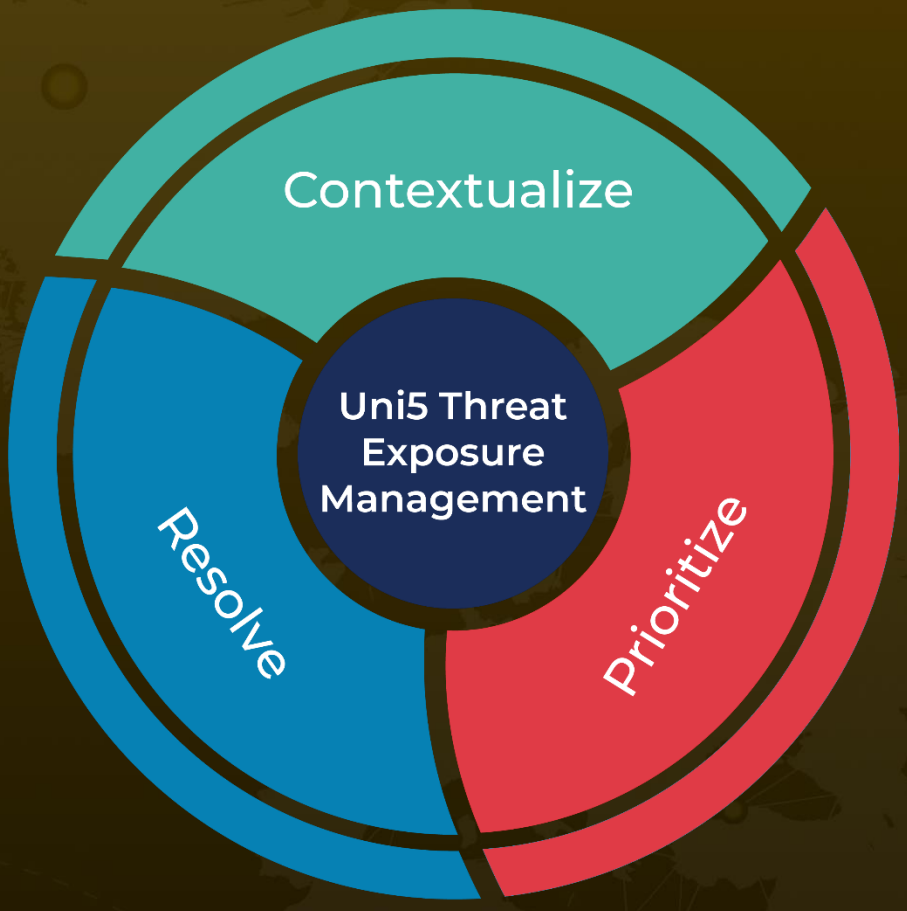
https://www.hivepro.com/mustang-panda-apt-targets-europe-with-customized-plugx-malware/

https://www.hivepro.com/camaro-dragon-targets-european-foreign-affairs-with-malicious-firmware-implant/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 05, 2023 • 10:15 PM

More at www.hivepro.com