Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

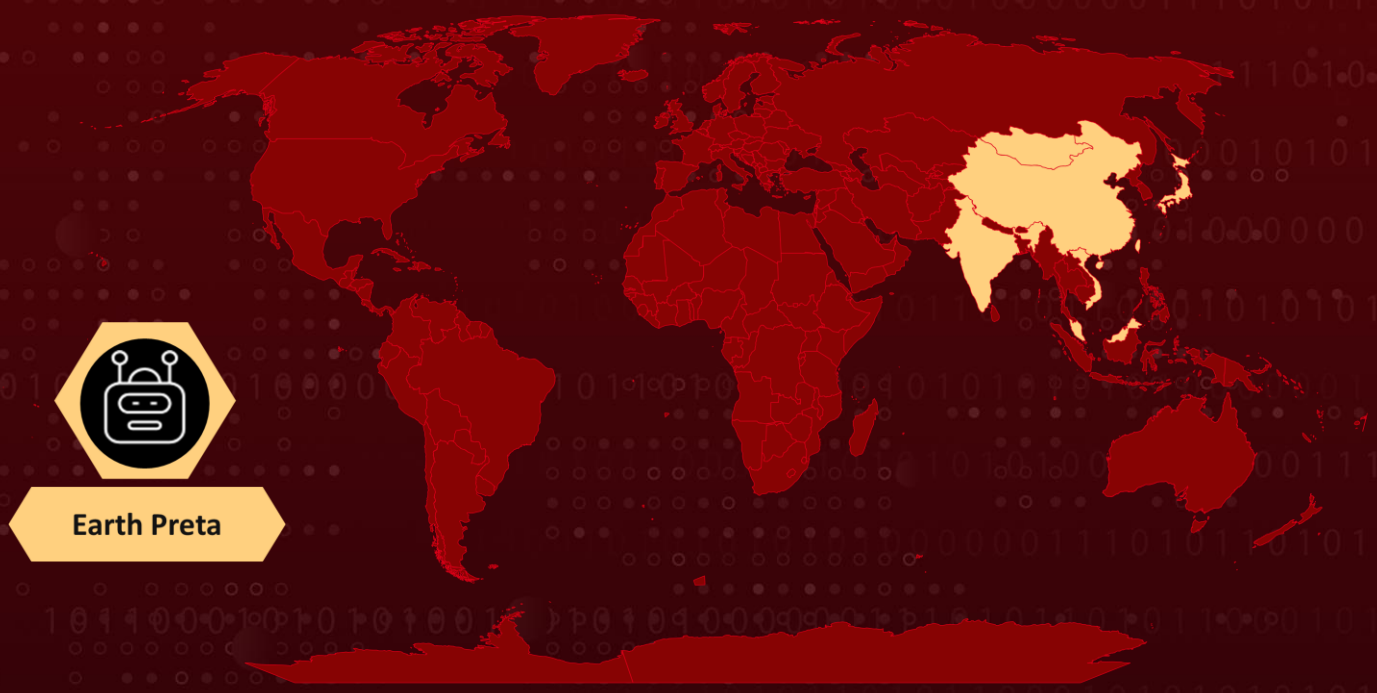
Earth Preta's DOPLUGS Leaves its Mark in Asia

Date of Publication	Admiralty Code	TA Number
February 22, 2024	A1	TA2024071

Summary

First Seen: September 2022
Threat Actor: Earth Preta (aka Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, Stately Taurus)
Malware: DOPLUGS
Attack Region: Taiwan, Vietnam, Malaysia, Mongolia, China, Singapore, Hong Kong, Japan, India
Attack: The Chinese threat actor, Earth Preta, strategically targeted numerous Asian countries by employing a customized version of the PlugX backdoor known as DOPLUGS. This sophisticated threat was allegedly revealed during the SMUGX campaign in July 2023.

Attack Regions



Attack Details

#1 The Chinese threat entity identified as **Earth Preta** (aka Mustang Panda and Bronze President) has systematically targeted various Asian nations utilizing a modified version of the PlugX backdoor known as DOPLUGS. This tailored PlugX malware was allegedly exposed during a campaign named **SMUGX** in July 2023.

#2 The deployment of DOPLUGS occurred through sophisticated social engineering techniques, utilizing enticing baits like the Taiwanese presidential election that occurred in January 2024. For instance, one lure was crafted in traditional Chinese, focusing on the urban renewal project in Taiwan, while another was composed in Mongolian, warning about floods in Mongolia.

#3 Earth Preta's scope extended to include other Asian countries such as China, Singapore, Hong Kong, Japan, India, Malaysia, and Mongolia. The spear-phishing emails dispatched to the victims contain a Google Drive link embedded with a password-protected archive file. Upon activation, this file downloads the DOPLUGS malware, which functions as a downloader equipped with four backdoor commands. Notably, one of these commands is specifically designed to download the general type of PlugX malware.

#4 DOPLUGS is intricately interwoven with the KillSomeOne module, a plugin responsible for various malicious activities, including malware distribution, information gathering, and document theft through USB drives. This variant exhibits an additional launcher component that executes a legitimate executable for DLL-sideloading, complemented by functionalities supporting command execution and the downloading of subsequent-stage malware from a server controlled by the threat actor.

#5 This sophisticated architecture indicates that Earth Preta has been refining its arsenal over an extended period, consistently incorporating new functionalities and features into its malicious tools.

Recommendations

Email Security: Implement robust email filtering solutions to detect and block phishing attempts, especially those involving deceptive webinar portals. Encourage the use of multi-factor authentication (MFA) to add an extra layer of security for email accounts.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

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	T1583.004 Server
T1587.001 Malware	T1585.002 Email Accounts	T1588.002 Tool	T1608.001 Upload Malware
T1608.005 Link Target	T1566.002 Spearphishing Link	T1090 Proxy	T1204.002 Malicious File
T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading	T1053.005 Scheduled Task	T1140 Deobfuscate/Decode Files or Information
T1036.005 Match Legitimate Name or Location	T1070.009 Clear Persistence	T1564.001 Hidden Files and Directories	T1056.001 Keylogging
T1083 File and Directory Discovery	T1016.001 Internet Connection Discovery	T1049 System Network Connections Discovery	T1082 System Information Discovery
T1012 Query Registry	T1091 Replication Through Removable Media	T1005 Data from Local System	T1025 Data from Removable Media
T1071.001 Web Protocols	T1573 Encrypted Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[://]estmongolia[.]com/Үер усны сэрэмжлүүлэг , hxxps[://]getfiledown[.]com/utdkt, hxxps[://]getfiledown[.]com/vgbskgyu, hxxps[://]getfilefox[.]com/enmjgwvt
C2	ivibers[.]com:443, meetviberapi[.]com:443, iamc2c2[.]com:443, thisistestc2[.]com:443, electrictulsa[.]com:443, mongolianshipregistrar[.]com:443, web.bonuscave[.]com:8080, www.markplay[.]net:8080, images.markplay[.]net:443, news.comsnews[.]com:443, news.comsnews[.]com:5938, images.kiidcloud[.]com:443
IPv4:PORT	103[.]107[.]104[.]37:443, 149[.]104[.]12[.]64:443, 185[.]82[.]216[.]184:443, 195[.]211[.]96[.]99:443, 195[.]123[.]246[.]26:22, 149[.]104[.]12[.]64:443, 45[.]83[.]236[.]105:443, 45[.]131[.]179[.]179:22, 45[.]131[.]179[.]179:443, 45[.]131[.]179[.]179:5938, 103[.]192[.]226[.]46:443, 154[.]204[.]27[.]181:80, 154[.]204[.]27[.]181:110, 103[.]56[.]53[.]120:80, 103[.]56[.]53[.]120:8080, 176[.]113[.]69[.]91:443, 45[.]251[.]240[.]55:443, 45[.]251[.]240[.]55:8080, 149[.]104[.]11[.]29:443
SHA256	c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1, 25967270d67253c72532a7e0416eb27ff249bc17dc1d7cded0148f8f4b932789, 32609faef0b04f0c37c4cf081c147872a45c59d7c4fbca35deb40d144b0226ad,

TYPE	VALUE
SHA256	364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321, 471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132, 42663f9d1ad0fe190912800b92c64d38b6f74fac23281b87180a4fef5bc2efd6, 7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b, c9da5b0a8dee27fbf5d7bbb4c9b9b38d8c0c547479d315efd62599a3c5d9cb13, 6e625bbcecc45b6b556141eef37ffd31aa4861ce4debca6500be72364172ffc7, dca39474220575004159ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c, 26b1d37ea3da6a6213b65b000dbb39575d858fa274aea895cc3bf62e706fce5d, 651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859, f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5, 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6, b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb, 88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b, 12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd, 71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787, 908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8, 5700535f19a382c8b84db6bff3a077e15269df0ec10ea6257e2fa203720356b4, a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f, 0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4, 095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1, 8e4a4d202d57c79dc0f40ae032f9d7b0ea7ce5024128a2aa227decc228e16113, 95205b92d597489b33854e70d86f16d46201803a1a9cb5379c0d6b7c0784dbc7, 70fac63465187ae5c2f057efc291bc34987dff46bec565a7e8f07f9899527224,

TYPE	VALUE
SHA256	8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be, b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177, 583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83, e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280, 60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797, eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13, 16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe, 5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914, 3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b, a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916, 17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82, d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc, d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4, c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692, 39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a, 42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5, 9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58, 4c1b5283f05322edfb0ef8b9d5cf75b62b558fcaefed921f1143765a3bd6248e, e6bc87e3e3d98a0a8db4fcd7cd5a9b89d4a7b125de450dfb8f387d2a9e09face, 13c31dbbae53517a17f7e6c99031480babe2bd8a07151dbb7f344ab620f3ac11, ca1ada6770b85771f98e5c02310449ab73231034cfa78b8861850368208c7698, abd6521990e88bd18bbcba063744efe0ccac23063bb340720cc3f610d9b1c770,

TYPE	VALUE
SHA256	77a49637bf4047959419c41867437957619d03059b5d3f8d9af26e6ae2347db6, f4f36c78cbf9901f224de427f42b390c83190c7c1cc4bce8b66f596e62df02d0, 48e37bb7e1ac185d314f262894014e1337a3c14455cd987dd83ac220bae87b3a, 33ff6318a3e745420c884f35709f2799f2fe461a6a5bb5b1e3166b9ab2ff142f, 04679defa1a4009bddab2a5d81be747b51a7f0f7aa5e7ebb937b40379a6a4690, a102626700691e57ece83a4ce24d995e57449508238eb5688954b78448be9172, 1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c, a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129, cd60e1c7d418a9c6ad4705d315f8ace2cdc3fd0528e71064dd80bbbd51bc2b76, 74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1

References

https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html

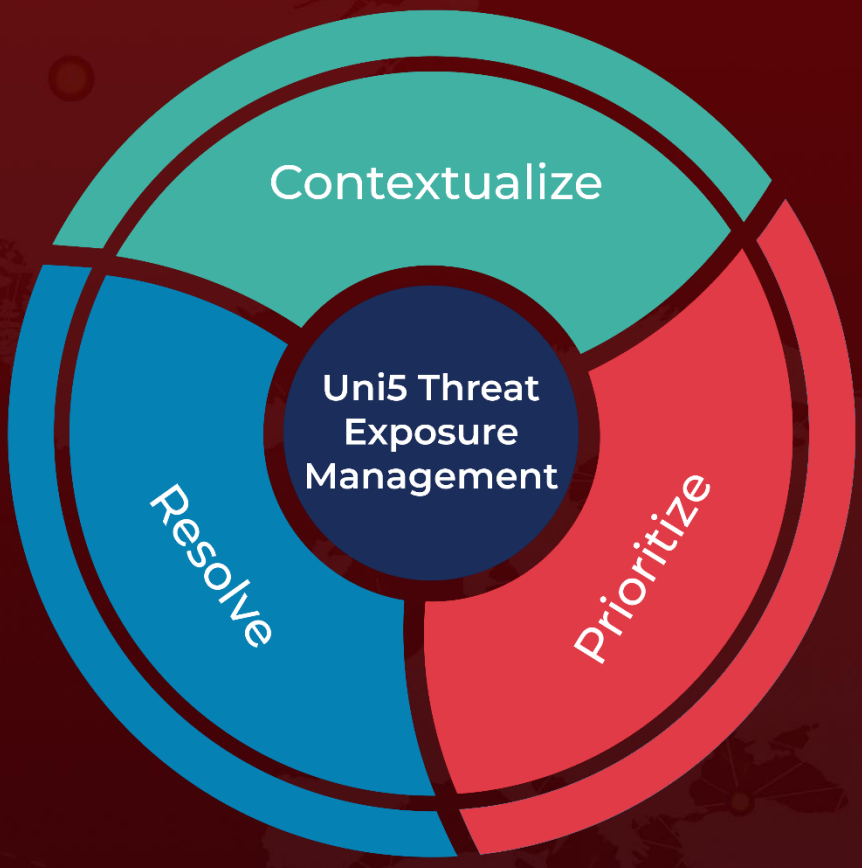
https://www.hivepro.com/threat-advisory/european-ministries-fall-victim-to-chinese-hackers-smugx-campaign/

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

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

February 22, 2024 • 4:40 AM

More at www.hivepro.com