Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

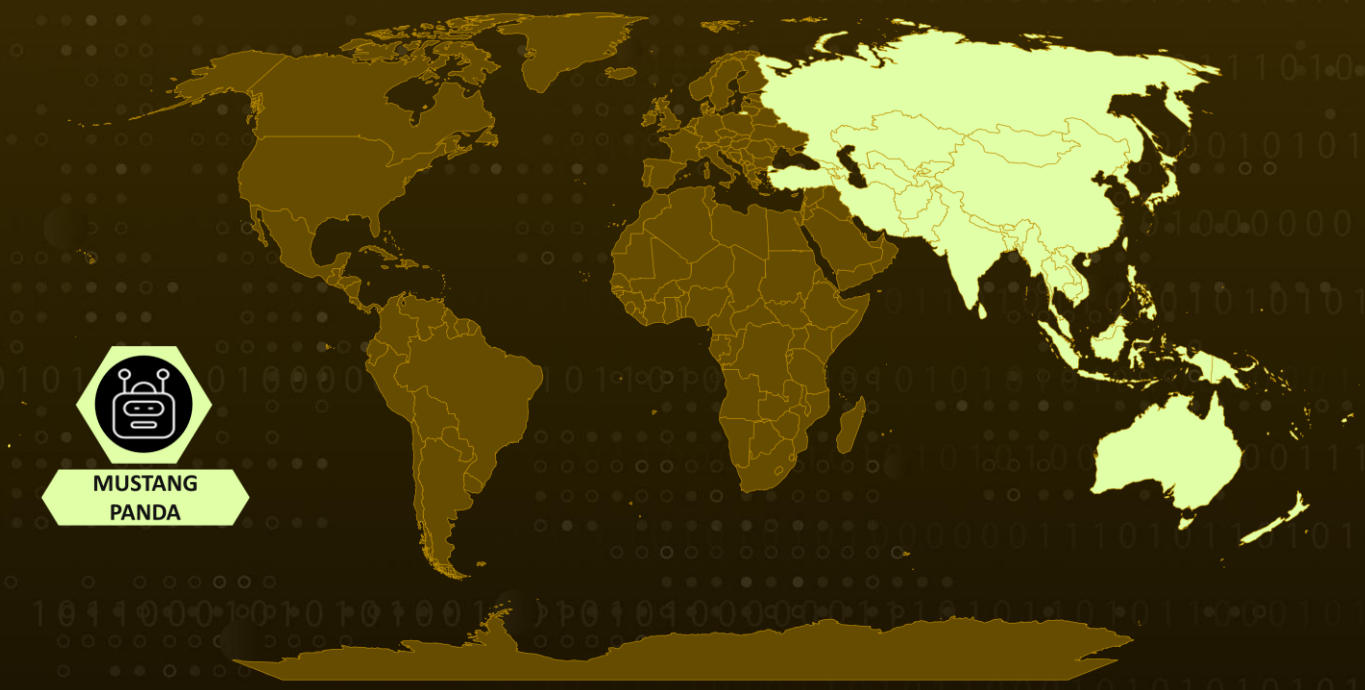
Mustang Panda Reloaded with an Expanding Malware Arsenal

Date of Publication	Admiralty Code	TA Number
September 12, 2024	A1	TA2024351

Summary

Threat Actor: Mustang Panda (alias Earth Preta, Stately Taurus, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG)
Malware: DOWNBAIT, PULLBAIT, CBROVER, PLUGX, PUBLOAD (aka ClaimLoader)
Targeted Region: Asia-Pacific (APAC)
Targeted Industries: Government, Military, Foreign Affair, Education
Attack: Mustang Panda, also known as Earth Preta and Stately Taurus, is an advanced cyber threat actor that has recently enhanced its operations with new malware variants and refined attack strategies. The group has been deploying sophisticated worm-based attacks and conducting spear-phishing campaigns aimed at compromising high-value targets.

Attack Regions



Attack Details

#1 Mustang Panda, also known as **Earth Preta** and Stately Taurus, has escalated its cyber operations with new malware variants and refined attack strategies. These enhancements include worm-based attacks and time-sensitive spear-phishing campaigns.

#2 Their spear-phishing emails use multi-stage downloaders such as DOWNBAIT, which retrieves a decoy document from an attacker-controlled server. At the same time, the server delivers and executes PULLBAIT, a lightweight shellcode, directly in memory. This shellcode initiates the download and execution of the CBROVER backdoor, paving the way for the deployment of PLUGX malware.

#3 One of Mustang Panda's more innovative techniques leverages Visual Studio Code's embedded reverse shell feature. This allows the group to run arbitrary code and introduce additional payloads, creating a foothold within compromised networks.

#4 The group also uses a modified version of the HIUPAN worm to spread PUBLOAD via removable drives. PUBLOAD acts as the main control tool, performing tasks such as file collection with RAR and data exfiltration using curl.

#5 Infected environments often see additional tools introduced by PUBLOAD, including FDMTP, a malware downloader that functions as a secondary control mechanism. FDMTP mirrors PUBLOAD's operations, while PTSOCKET is deployed for multi-threaded data exfiltration. Earth Preta's ongoing adjustments to its malware **arsenal** and tactics reflect a continual evolution in its methods, underscoring its adaptability as a threat actor.

Recommendations

Advanced Threat Protection: Use advanced threat protection for email to detect and block spear-phishing attempts. Regularly train employees to recognize and report phishing attempts, focusing on identifying malicious attachments and links.

Harden Development Environments: Apply security best practices to development environments, such as disabling unnecessary features in Visual Studio Code and other development tools to prevent misuse of embedded features like reverse shells.

Deploy Data Loss Prevention (DLP) Solutions: Use DLP solutions to inspect and control sensitive data being transmitted across the network, preventing unauthorized data exfiltration by malware like PUBLOAD and FDMTP. Implement and enforce data protection policies that prevent the movement of sensitive data outside of authorized channels.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1091 Replication Through Removable Media	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1053.005** Scheduled Task	**T1574.002** DLL Side-Loading	**T1574** Hijack Execution Flow
T1480.001 Environmental Keying	**T1553.002** Code Signing	**T1055** Process Injection	**T1518** Software Discovery
T1518.001 Security Software Discovery	**T1049** System Network Connections Discovery	**T1016** System Network Configuration Discovery	**T1005** Data from Local System
T1560.001 Archive via Utility	**T1567.002** Exfiltration to Cloud Storage	**T1048** Exfiltration Over Alternative Protocol	**T1071.001** Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ee986beeb058ec27d0dad9a0a671bbabaa56057102faf30f63397bdbe7fca81f, 3514d2e74b476e1569bbf3311934809c6f8e97df5c9669a5fe475e508886df9f, 24a850f15a023f59389bf8fd1c33796cf3a5d8d08f77dda049d1c978a1825dde, 2e44ebe8d864ae19446d0853c51e471489c0893fc5ae2e042c01c7f232d2a2c2, a062fafaff556b17a5ccb035c8c7b9d2015722d86a186b6b186a9c63eeb4308a, d1492101eb450f0e9badaea254e5551b49297fa4a98c53c939bb96bafd2151fe, 586632c8bb5890c760efc21662105e649177deaf2b2c2eef3ede1da088f23a6c, 68bec53e4772eee6c13278a471d669b916cdc797c81d128ee103ee90841fa19e, 71f114842c30e94c95e57ad394969d5766ca28d056dc724c9820717cf03eb0fe, 959fd255338558d02c567680625d88f5c48e43827bbb1c408f2d43b01807809a, 466684ad5755c9ee6080ff2a01646824c63a90d3e5be923581b89c707267e79f, f67ce881d31e7475d3bd70cad8bdc8fe0e8fd5f66b87ede0e49109395f7033aa, e2f4b2d71e02b49a2721a88eea7bf7308143ee55d7d8119e5e291eafd4859af5, ea18df47214ac1f96a75b1dffbe510b2855197490bc65f47886b25fc7e8aca15, 533f47bc4997eed0491f58f24d45c7850cb460da252de90635938e095b5fc213, c2bed145cf09022ee6a378dc5e9b3ae49b7c95a6551fa7310a1d997f93f6e2d1, 99071b9df19024480e1b6d7049e6713486418759b7f0191643776bd0ac08172b, 756b9d6f50bd56adca1fa3d48ff07edf8ee3cc568fb32cbdd892403670343b43, d69a4a7aa3144ee7ec35e7c3a3a4220f5a43bc29cc4cfa0f27fef60b4d93de8d, 107ba73ae05ec6ba6d814665923191f14757015557eeeff16206cc957da29be3, 14a9a74298408c65cb387574ffa8827abd257aa2b76f87efbaa1ee46e8763c57,

TYPE	VALUE
SHA256	8ebb12d253a4b4c28435b25478abb590e94bdb55b83c55cda6d44c58a03bf9be, 56cb16589ab852de4900496ef74212c17902867e90253b4d9d7f335ef7d45a7b, c662f5c851314d952cf3594232a7db5b96cb528716cd71bf38393b647cfd4c82, f452b787e47493e89078e884bf92c61626e6ff4b9bc8eee8ae3728ddc65b7e46, fd68b49acf9234a8592497ef1d675acd57c6a67c6975313772d12c837f3264d1, 565fa2992212c89bdec334c0fd318b3fd2c91707431fd8186016f11645925892, df0e16a29c9dffe2ff7b3d4c957af7459fd7e6fa8026d067202912b997773749, 3278c06b5510edabb3318aa1892eb7e426e97946b86eea925965a46ba1725ebd, 3b9ef9701ea2b2c1a89489ed0ed43ffabec9e22b587470899c0d5aca1a1e4302, 9dd62afdb4938962af9ff1623a0aa5aaa9239bcb1c7d6216f5363d14410a3369, d8747574251c8b4ab8da4050ba9e1f6e8dbbaa38f496317b23da366e25d3028a, 7c520353045a15571061c3f6ae334e5f854d441bab417ebf497f21f5a8bc6925, b63bc07202491a4dcd34cc419351edb2f2c395b2671d7acf7bfc88abada344ec, 44d2d35ca87bf4292e4586bd08f3fe51d3fff693fed2f9795ff49733338ae8a7, afed5635fa6d63b158fc408d5048bf2dafd6da210a98f308c02c94514ae28fc8, b37b244595cac817a8f8dba24fbea208205e1d1321651237fe24fdcfac4f8ffc, de08f83a5d2421c86573dfb968293c776a830d900af2bc735d2ecd7e77961aaf, d32d7e86ed97509289fff89a78895904cf07a82824c053bfaf1bc5de3f3ba791, 506fc87c8c96fef1d2df24b0ba44c8116a9001ca5a7d7e9c01dc3940a664acb0, aa2c0de121ae738ce44727456d97434faff21fc69219e964e1e2d2f1ca16b1c5, 8fdac78183ff18de0c07b10e8d787326691d7fb1f63b3383471312b74918c39f, 39ceb73bcfd1f674a9b72a03476a9de997867353172c2bf6dde981c5b3ad512a, 0f11b6dd8ff972a2f8cb7798b1a0a8cd10afadcea201541c93ef0ab9b141c184,

TYPE	VALUE
SHA256	456e4dae82a12bcda0506a750eac93bf79cc056b8aad09ec74878c90fd67bd8f, bdadcd2842ed7ba8a21df7910a0acc15f8b0ca9d0b91bebb49f09a906ae217e6, ac34e1fb4288f8ad996b821c89b8cd82a61ed02f629b60fff9eb050aaf49fc31, 440e7bce4760b367b46754a70f480941a38cd6cd4c00c56bbaeb80b9c149afb1, 5bfc45f7fce27d05e753a61dde5fab623efff3e4df56fb6a0cf178a0b11909ce, fb0c4db0011ee19742d7d8bd0558d8ee8be2ef23c4c61a3e80a34fba6c96f3ff, 965dd0b255f05ff012d2f152e973e09ceb9e95b6239dc820c8ac4d4492255472, acedfe9c662c2666787cbbf8d3a0225863bab2c239777594b003381244ed81ba, cca63c929f2f59894ea2204408f67fc1bff774bb7164fde7f42d0111df9461bd, 3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05
IPv4	103[.]15[.]29[.]17, 154[.]90[.]32[.]88, 47[.]76[.]87[.]55, 154[.]90[.]32[.]88, 47[.]253[.]106[.]177, 16[.]162[.]188[.]93, 18[.]163[.]112[.]181, 216[.]83[.]40[.]84, 185[.]132[.]125[.]72
Domains	www[.]ynsins[.]com, www[.]aihkstore[.]com, www[.]bcller[.]com

References

https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html

https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/

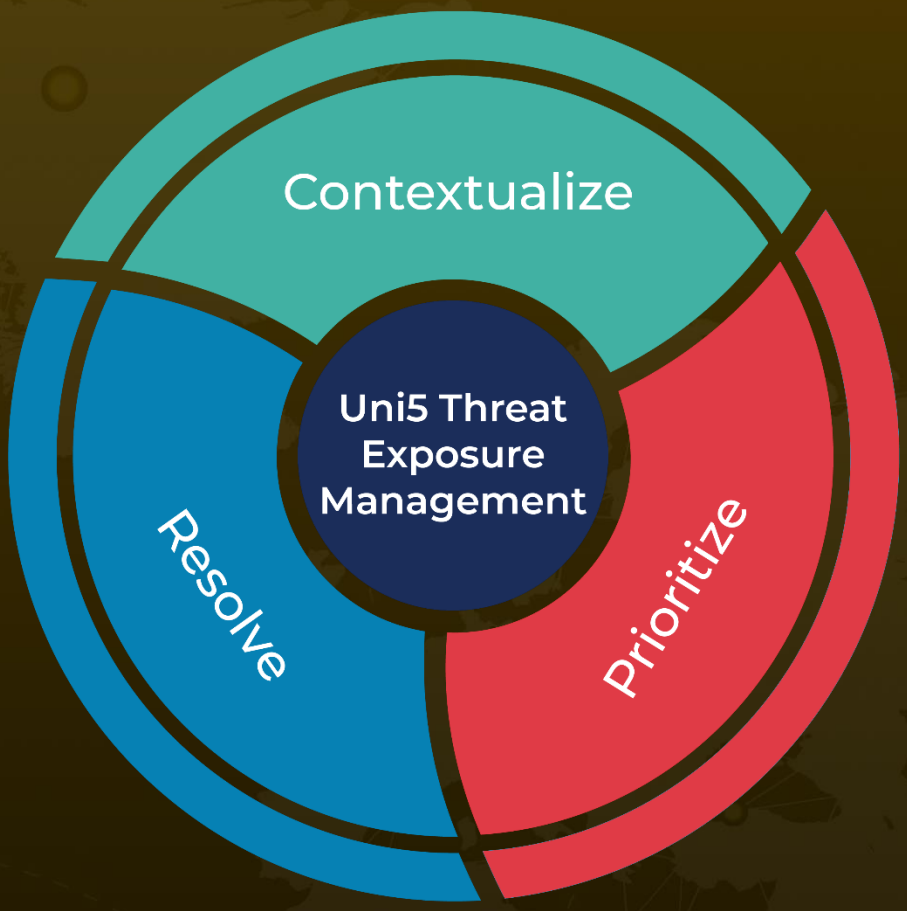
https://hivepro.com/threat-advisory/earth-pretas-doplugs-leaves-its-mark-in-asia/

https://hivepro.com/threat-advisory/chinese-apt-earth-preta-runs-spearphishing-campaigns/

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

September 12, 2024 • 1:00 AM

More at www.hivepro.com