KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Mustang Panda Victimizes Businesses in Asia, Africa, Europe and Middle East

Tracker ID: TN2355 **Date:** April 10, 2023 **Category:** Campaign **Industry:** All **Region**: Asia, Africa, Europe, Middle East

Background

Since 2022, more than 200 victims have been the focus of cyberespionage operations by 'Mustang Panda' also known as Earth Preta. Several Mustang Panda subgroups used various TTPs to carry out multiple strikes in Asia (51%), Africa (16.8%), Europe (13.3%), and the Middle East (5.6%) regions. Academic institutions, financial services, mining and material refineries, specialist fabrication companies, and energy production and distribution were the main targets of these attacks. By the end of 2022, it moved its focus toward organizations involved in immigration, border security, and the maritime sector.

Mustang Panda is a centralized development unit for the China-based threat group that distributes malware implants and tools to other operating groups. These operational organizations control their own initial access and privilege escalation, exhibiting a high degree of specialization in their assault methodologies. Some operating units focused on government and diplomatic organizations, while some stole intellectual property and confidential corporate information. Several occasions exist where victims were compromised by two groups, suggesting a potential overlap in goals, toolkits, and materials amassed by both groups.

Mustang Panda (also known as Bronze President, HoneyMyte, RedDelta, Red Lich, Earth Preta, PKPLUG, and TA416) is a threat actor based in China. The cyber-attacks have targeted foreign governments, non-governmental organizations, and other organizations deemed opponents of the Chinese communist regime. Previously, attacks have targeted Taiwan, Hong Kong, Myanmar, Mongolia, Vietnam, the Catholic Vatican, and religious minority groups in China. Mustang Panda was discovered in 2017 by threat researchers, however, it has been active since 2012. Mustang Panda coerces engagements through well-crafted spear phishing attacks that imitate government services organizations in the targets' home languages and leverage current international issues such as COVID-19 and the Russian-Ukraine war.

The targeted overlaps have mostly been found between groups 724, 1358, and 5171. Group 724's attack strategy makes use of physical entry points into a target's system, like a USB drive. It then utilizes Adobe CEF Helper and DLL sideloading to get a persistent foothold in the user's home directory. The WSC DLL from Avast is abused by Group 1358's attack strategy to sideload and run malicious malware. The group continues to use PlugX as their malware of choice and employs USB sticks for data exfiltration. Group 5171's attack strategy distinguishes itself by utilizing the moving laptop attack (a laptop with malicious code in transit). It focuses on certain industries and adopts a more opportunistic strategy.

The effects of Earth Preta's cyberespionage operations on global security and intellectual property are influential. There is significant evidence of traditional intelligence gathering techniques and cyber operations operating together points to a well-planned and sophisticated cyberespionage operation. A highly specialized and well-organized cyberespionage operation can be noted by the fact that the researchers were able to identify several distinct operational groups, each with its own TTPs and goals.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Mustang Panda Victimizes Businesses in Asia, Africa, Europe and Middle East

Tracker ID: TN2355 **Date:** April 10, 2023 **Category:** Campaign **Industry:** All **Region**: Asia, Africa, Europe, Middle East

MITRE ATT&CK Tactics

Initial Access, Execution, Persistence and Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Administrators and organizations are encouraged to keep the systems and devices up-to-date and patched against the identified vulnerabilities and exploits as soon as possible.
- Establish a data recovery strategy and routinely backup your files to a secure offsite place. The ability to rescue your data after a ransomware assault is guaranteed by routine data backups.
- Follow a prioritized patching regime and implement multi-factor authentication on critical systems and accounts.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Ensure endpoints have modern next-gen protection capabilities to guard against downloading malicious files from untrusted sources.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Trend Micro, Earth Preta's Cyberespionage Campaign Hits Over 200, March 27, 2023, External Link (www.trendmicro.com).
- Cyware Alerts - Hacker News, Mustang Panda Cyberespionage Strikes Over 200 Targets, April 03, 2023, External Link (cyware.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Mustang Panda Victimizes Businesses in Asia, Africa, Europe and Middle East

Tracker ID: TN2355 **Date:** April 10, 2023 **Category:** Campaign **Industry:** All **Region**: Asia, Africa, Europe, Middle East

*

Hash SHA256
28875b1d6206e41ddcdbae56c6001915735c08f11f6a77db5a7107a4236afb34
c143fb5cff5f564529efc746158b0c34a833a0301df44b5bc3d0d00567033353
c7d98e50c56199a25abaff481d884c6906561a4357de00a0e149da2a3dbfad56
282a2f61fdf5d55134f4beb7591d8e434c03ef19cfdc87f0d268dc560c8e3c0b
0f7c5ac8f130fbeb828b82f8ff07294924adcf083cf32fa246f248353abdd92e
2b6e6fb1e58f4a89172dae2e47497ae36a32d9699ed60c512b7190ceb4c5e50b
4432887f94cefc8ef5209af5a7cd333a225aa4b34952fbf69c37306404c6fec0
531c628819c99207dd031923f21fdf2424b6fc68c4326c38cc9d4e1cb765f6c8
a449b769f4f4fabf5dfcdd5b7570592aaaaab1ee7a1f93396b866899ccdc14b3
aaecdea90ccaff4a3a5239c1a9c83ec533abe84d33bd84d584276aa6eac6ecd9
aeba4f0f7e577fca60908db0ad091a4600635353 39b885e70ea0ada854a15f8d
e0fb4cb5cd28aefd2692cfa1659558a0974de27ddcabb51b96fe26cb760992cb
f0f2ff31b869fdb9f2ef67bfb0cc7840f098a37b6b21e6eb4983134448e3d208
02d48e9dcf7d4a95b0720039586b711ca3c3921f76a5002a7a4b8e8559be5c5d
352fb4985fdd150d251ff9e20ca14023eab4f2888e481cbd8370c4ed40cfbb9a
52572005329b386f4bc638f5950af811ac8f824001c560df9ac4e090cff96d8c
53cffbfed8c751333f70037e125f520c0d7ecc3456148948cba9e27a709eec8a
6491c646397025bf02709f1bd3025f1622abdc89b550ac38ce6fac938353b954
6bb959c33fdfc0086ac48586a73273a0a1331f1c4f0053ef021eebe7f377a292
7119ced7efb3df578168e8c5234d459cafcf679f5ec0201dd2bc9e573e9ed4b1
8eb94ed9fb0c3f69990025d195375ef8a44abe64ee3c8489084b4be736608d72
aa37b5d0e254e300b6d09f28ed51f1c2ab094a765b09f16c8a1f5e9fa55b8aa1
af7af50a9bd1dc33ff7157866f7792161487bbe7d5dd31fb4d78ec219f114ebb
cb67d91878525f8a5094a2badd035fc6422f721a79a10003b34930c95086229b
d91854daa4fdab1359e8c7f58e15c69f239281aecfcfd1ceb41d85f60173e3f1
e5c148dbddd79a3592b69317dcda88c45332c1e84d88850f0514a78653985542
edaa8b62467246d9a43e0f383ed05bc3272d2f8b943a79d9d526f8225c58d1e6
0c09080aefba65e1d3f9b6f2552a9d868314a1eeceaac202b3156c03c704700a
0f38cea4c1f48468887b7dd81476ae68d7de6aec3b274db6b74e560302e2544e
1daceaeee5a776a5cdfc782e331c3962b4a833b1598911983b2359c2c52a4e31
22682e109d080ce25b369ca5d263c39479a192c6f9d928f9d5689b1afd0408cb
22f2d015e39f84d0b92c5e919cee874f83826c9541608af634aa896682558402
2b462375106f1ca2f50fe88f27821fe60a27ab5910953d359cd4e136c70999f7
335d94fb89b76bbdaf50eb01395af2933963a1c7bc0b80d558d0b9b4a4d0ab7e
5928048ed1d76df1ae4f3ede0e3da0b0006734f712a78036e6f4b6a78c05f0c6
5bf291fd726770a7c3e60192be74b960fe34c4733c4e0e770202e8e8f85cbd02
7456ddf511e1717af17fd8224bba94153391e3bcda6540127cf7f79b75906d2a
7f303dfd90cd295c46fae15f2d8f11a808bbe8bf2163d3e74e1c233872d96ac1
81e93cd01e30ddcd3896000eb89aa79749e2a3a998ea2f972d1a14c050ddb2d7
9c13ffe918fc50b12e0b8028d9cc7649ae6b873ddb72f4739de3323835189e71
ab3f23efa4e511e56af91b5317df6abf3427f5f39399726 89db88c09d850490f
ac51ac3165ecba237b23229ef02088168c7ee4f4f3d36cd0dbe64627cd9175b0
e358c40086002e93b213ffc41721b5ad86d95b035852c8bc284500edc9eb7ef4
ebc326bc8a3b8f63ec4c2ea4cda1559ddcb2066ad10a5789e2311c7c9ef3c884
efa333ac1ecd0726cf4201f4a620e7f1a86bbf762495221e800298eb4e1dc01b
8ec37dac2beaa494dcefec62f0bf4ae30a6ce44b27a588169d8f0476bbc94115
0490ceace858ff7949b90ab4acf4867878815d2557089c179c9971b2dd0918b9
d28894c660c6548fb02b8ee6a09472fc5ec404babca60d142033d99dd565c7d0
8871bd39918868d4f4390e430e82730819182a8ae9fb3ef7096c2ce5dbafbe26
14f9278f3515fae71ccb8073cfaf73bdcc00eab3888d8cee6fb43a4f51c9e699
2e5412c25b53b9f86dd03ef44db66ed02bf7f984ac012f439efdc1835a05e6b3
5b807629ab299abec70f88f861487c55a6795d6e27e5d85c64080f072132558c
617ff22ba57099087ab4a823c6b682f506229f56b675db8a8dc5ae626c5d2948
6e506c8b469ad0248f99127dbaaf44e1f840ec146bb4e39029b00805344cd2b0
6fc8c2e28dfa39b20154ecb3339eb784a025ea1a7c79e15e0930f679280bb63e
842efbc6a635968a2735c132135bc43ddfdf203e22fee870b1030688d2dd9e79
8be6c10e9e150d01601f77485444e409667ba905100982f57743e01d20a26121
a75598a76d2df2afc747757d3ec278285c5262fadf654be2243f8e08762dbcea
a8767be010e1cd90d77034f3c4f69821f764ae976d32dc34d29d19659afa5950
af6cb7f9aaa2e1cff577888164f689c4bdb62490bd78915595d7fdd6462d09c4
b9f3cf9d63d2e3ce1821f2e3eb5acd6e374ea801f9c212eebfa734bd649bec7a
d0fdc08dab55f2cba6faccad2a6a889859ac6349d35f19a695bcc8aa18103cbc
d1f848a8477f171430b339acc4d0113660907705d85fa8ea4fbd9bf4ae20a116
e238f4e14d267630edc675a6aabf724e879c0ee2af93fed594f1f6f3170fa4ec
f331eb3d7f6789e48f2e3bfb1a8759556 1722f45aaec150df537488587024096
f5afaf33dfd6cc00024334e9a7104c61c21b79b6417f76baade6117bf973c1de
bda6f53d37e51385ed739ab51055420254defafff0db669aa55229e0eda9fc66
0c36cc54632519eac51c58e084be9f954888410e2602056dde2e979ed5a75fae
1be83d9511d7a26ca6351040d9681d39f634e699c9796b15fd899c6b4a397828
7cd6e1326aa0f6f07faa8d18810c1334368d67c1098c8699fef05190aa722229