KPMG

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Researchers Disclosed Chinese APT Earth Preta’s Stealthy Strategies

**Tracker ID:** TN2352 **Date:** March 29, 2023 **Category:** Campaign **Industry:** All **Region**: All

### Background

A recent campaign launched by “Earth Preta” suggests the involvement of a nation-state threat group linked with China that has grown adept and skilled at evading security systems. The threat actor is active since 2012 and is tracked by the cybersecurity community under the moniker Bronze President, HoneyMyte, Mustang Panda, RedDelta, and Red Lich. Attack chains mounted by the group commence with a spear-phishing email to deploy a wide range of tools for backdoor access, command-and-control (C2), and data exfiltration. Similar infection network groups that distribute Cobalt Strike have previously been seen operating with Google Drive links.

Earth Preta conceals malicious payloads in fake files that are disseminated as legitimate ones to avoid investigation. This entry point method, which was first identified towards the end of last year, has since undergone a minor modification in which the download link for the archive is embedded within a separate bogus document and the file is password-protected to circumvent email gateway defenses. The document's password can then be used to retrieve the data from the inside.

The email messages usually contain malicious lures for archive files that are distributed through Dropbox or Google Drive links containing LNK shortcut files, fake file extensions, and DLL side-loading as initial vectors to gain a foothold and drop backdoors like TONEINS, TONESHELL, PUBLOAD, and MQsTTang. Additionally, the threat actor has also been seen using malware like "USB Driver.exe" (HIUPAN or MISTCLOAK) and "rzlog4cpp.dll" (ACNSHELL or BLUEHAZE) to set up shop on portable devices and building a reverse shell to move laterally across the network. A backdoor called "CLEXEC" can execute instructions and delete event records, whereas implants called "COOLCLIENT" and "TROCLIENT" can access and write files as well as monitor keystrokes.

Threat actor also developed highly customized tools used for exfiltration, such as NUPAKAGE and ZPAKAGE, which collect sensitive Microsoft Office files. Chinese cyber espionage actors are diversifying their technological arsenal and accelerating their operations to avoid detection. Earth Preta is competent, continually enhancing its TTPs, development abilities and compiling a variety of tools and malwares to infiltrate networks. We advise businesses to organize phishing awareness training for their partners and employees to emphasize the value of employing care when reading emails, particularly those coming from unknown senders or with obscure topics.

### MITRE ATT&CK Tactics

Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Command and Control and Exfiltration.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Researchers Disclosed Chinese APT Earth Preta’s Stealthy Strategies

**Tracker ID:** TN2352 **Date:** March 29, 2023 **Category:** Campaign **Industry:** All **Region**: All

### 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.
- Implement email restrictions on downloading Google or Dropbox files, files with fake file extensions, LNK files, shortcut files, or other similar/suspicious files from unknown sources.
- We advise businesses to organize phishing awareness training for their partners and employees to emphasize the value of employing care when reading emails, particularly those coming from unknown senders or with obscure topics.
- Check the URL the one is visiting to ensure the site is legitimate before clicking on it or downloading software. The intended URL may be like a legitimate domain name, but it may have errors like a misplaced letter.
- Verify the sender's email and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link’s target.
- Check the sender’s identity. Unfamiliar email addresses, mismatched email and sender names, and spoofed company emails are some of the signs that the sender has malicious intent.
- Block users from connecting to dangerous domains, IP addresses, and URLs, regardless of whether they are on or off the business network.
- In order to prevent malware or TAs from stealing data, keep an eye on the beacon at the network level.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

### References

- Vickie Su, Nick Dai, Sunny Lu, Pack it Secretly: Earth Preta’s Updated Stealthy Strategies, Trend Micro, March 23, 2023, External Link (trendmicro.com).
- Ravie Lakshmanan, Researchers Uncover Chinese Nation State Hackers' Deceptive Attack Strategies, Hackers News, March 24, 2023, External Link (thehackernews.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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Researchers Disclosed Chinese APT Earth Preta’s Stealthy Strategies

**Tracker ID:** TN2352 **Date:** March 29, 2023 **Category:** Campaign **Industry:** All **Region**: All

*

| SHA256 Hash | IP | Domain |
|---|---|---|
| 3fd8cd848e89e792d3915bfc0b485de80d7615a1422047c589ac0b34f4c9e7b0 | 23.106.122.81 | closed.theworkpc.com |
| 10d37878e595e76513156a538c34d23b1533b84f984609b405b84e74a26a7381 | 38.54.33.228 | appcloud.appmdb.com |
| 0a43705f5c10aad9317c49c81d9f12db4aee5e2557a39020973d25019955d345 | 212.114.52.210 | |
| 7cc2a21bcb3d58c2c82cee3e6b97c34aff1892d52658ecb5d10659c266c53b16 | 158.255.2.63 | |
| 8b98e8669d1ba49b66c07199638ae6012adf7d5d93c1ca3bf31d6329506da58a | 188.127.237.27 | |
| 87f6adcd16f8a65096f4c192d52107fff98f411b1e166ded69cf3800d8a2933d | | |
| a8b31d491f4e7f41e7a7c3aeb35030ba3363dfb34ae74c84b02c25df125db23d | | |
| 1f7d961d9c15aa8f4b9b5a2e17de277aaded55f11aefed34b3ebd0af545f5448 | | |
| e4189bd43996250dfb525f64844525343a80bf9dc2039d46cb8ccc430a24a0ce | | |
| 2a61fc95c432328d2600615a5bbbe8f0ee75fad2035417879a742cc58306e071 | | |
| e79aef1efd60d55274d42d2da0a8158f131dcd56234cfc1b77d1600ceed7977e | | |
| 3d18ef92a3d5f97d9be130fdda90d49dbcd661f3d2b992c3c539789df5ff379c | | |
| 7e2e4943099652a5367ff2c3ee7fc664791cf17a405505514f3660c8dedd6fb0 | | |
| 946b09e543ea9f1fe37dd9958a03ee061f00d711a04b5810e31e8bf9849e7f90 | | |
| ef6a278bb6e09a67622de7b1c3403c4a5cb80ab2c0038654431b84feadb8fd79 | | |
| 5d5d5dbd752da8a96414d067b352501a67067abbb6b18b623c55a3ae68f969a6 | | |
| ae9824355384c7ea34035ebc7e8832b6fb17e227a79efa72e4501cb9ddd2dd0a | | |
| e8357cacdccdb4670f6ae427a781f36a9c4b268907f83c1ce3502a0fd9ce2606 | | |
| cfe1447e7515ad831fcfedb9a5c1a721885b0542b775e4028a277a27e724ec73 | | |
| 4bdc913cef96b0abd0c1a8231a7961ac901fc9c28f87bba3b8c59e6928c0cda4 | | |
| 12216b083ce2461c338bf571411ab53cd28fc0e3361add69a0b1c6d22b57e9c1 | | |
| 28a992ea7b9df22a7b7bcc04ecb3f3b89e5ea022f03b765bf1f12edd61df779f | | |
| 634977a24e8fb2e3e82a0cddfe8d007375d387415eb131cce74ca03e0e93565f | | |
| c835577f1ddf66a957dd0f92599f45cb67e7f3ea4e073a98df962fc3d9a3fbe0 | | |
| 2937580b16e70f82e27cfbc3524c2661340b8814794cc15cb0d534f5312db0e0 | | |
| c2f5a12ebaeb39d4861e4c3b35253e68e6d5dc78f8598d74bc85db21aeb504e8 | | |
| 711c0e83f4e626a7b54e3948b281a71915a056c5341c8f509ecba535bc199bee | | |
| 869e2a35107f7469cc0a8eef44d2eaf311ce8c6fff7acd3e429b11167c6bcd57 | | |
| 9635bc2009415b05cfb3fa1c5f40042916891d7e289502572f5d20043dc0e2a8 | | |
| 12a04989fdbcf7fa2f70a708521968e609b0d247acf842fe8c0e5f5bac3a09db | | |
| 6f924de3f160984740fbac66cf9546125330fc00f4f5d2dbf05601d9d930b7d9 | | |
| 6b703611c93f20513fee6080ff9fdd23f3c73db5b21a63324ef9e36e4d728b22 | | |
| 055fa35e8153242417d39c75e10e0de0758c05a9f31409926744c3f5ceeb4100 | | |
| c07bc0b020f1250c69ee6ab804dd08095d42fe1fb80f591d2bb198a4409f2300 | | |
| a61ed84f72ac995156a18450864444edc20ae7859fb4fa667b14a61416841659 | | |
| c3bbf0600f3833f3eaddb2e8c65d68e2a858644cf22b67851fff3e379cfbf08c | | |
| fb5edfcba99e2df2b7f6f40e8615f5cb247803180464e584161c7c91405aae4a | | |
| c47590218e7a933350e09d3fe7e01cdf5e3cff1130557380ad96c2106ac15ab1 | | |
| 9182bb02d99a62357918ad459ccdbb8edb21d1e61a225d350db94e22525f273f | | |
| 4c79bb9fbac4b189898095f81d4ee1ba7877cfbd16c6a10f933ca564ced737d2 | | |
| 950bcbf83029f47e85f615494b4922cd0cdc04ca2c3d9699a0fb5d1fd2076dc5 | | |
| 26f7ed0b66fd464caab9d648127ad17e8cd46d50fee94704627308a377dd821b | | |
| 19001883ec8d29ae6c8e54d4219631d1b0098e1fd246234a171a67509e87b621 | | |
| 2139e3df912887b34b4d59fca098a8d511ea10530d7168b280acca844513ffad | | |
| 77e9dd17c26f4755bf0844991ea92363a9031fbf094f904c2c3953e97575fe99 | | |
| 4936b873cfe066ec5efce01ef8fb1605f8bc29a98408a13bc8fe4462b2f09c5a | | |
| 5231a0e725a70ee9b56cb461a3884755f2dbde58264040151b5224c2795f85f7 | | |
| 1f9c3a12631b13f4fd128f93a8d14e63fb8e9e8529e55da1bfc0f2274b819671 | | |

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia