Rewterz Threat Alert – China-Linked Earth Krahang APT Breached 70 Organizations in 23 Nations – Active IOCs - Rewterz

Published: 2024-03-19 · Archived: 2026-04-05 17:50:38 UTC

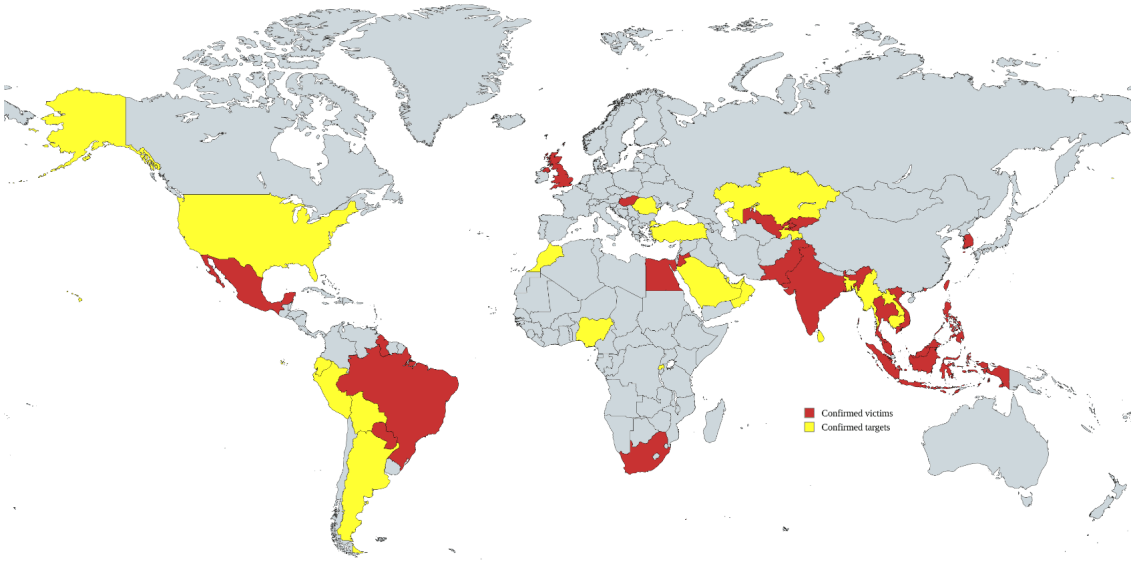
Severity

High

Analysis Summary

An advanced cyber campaign targeting at least 116 organizations in 45 countries has compromised 70, and it is believed to be the work of the Chinese advanced persistent threat (APT) group known as “Earth Krahang.” The campaign has been ongoing since at least 2022 and it mainly targets government organizations.

In particular, 48 federal agencies—ten of which are ministries of foreign affairs—have been infiltrated by the threat actors, who have also targeted 49 other government institutions. The attackers utilize spear-phishing emails and weak internet-facing servers to install custom backdoors and conduct cyber espionage. Earth Krahang creates VPN servers on infected systems, employs brute force to break passwords for important email accounts, and exploits its presence on exploited government infrastructure to attack other governments.



> Cybersecurity analysts said, “One of the infection vectors used involves the scanning of public-facing servers. Earth Krahang heavily employs open-source scanning tools that perform recursive searches of folders such as .git or .idea.”

The threat actors use open-source tools to search public-facing servers for specific vulnerabilities like CVE-2022-21587 (Control Web Panel) and CVE-2023-32315 (Openfire). They use web shells to get unauthorized access and persist on victim networks by taking advantage of these security flaws. Alternately, they employ spear-phishing

for initial access, luring the recipients into opening the attachments or clicking on the links with communications centered on geopolitical themes.

After gaining access to the network, Earth Krahang hosts malicious payloads, engages in proxy attacks, and sends spear-phishing emails to its associates or other governments using compromised government email accounts. Notably, Earth Krahang fetches hundreds of email addresses from their targets in the reconnaissance phase. In one instance, the actor sent a malicious attachment to 796 email addresses associated with the same government agency via a compromised mailbox.

To propagate the infection and achieve redundancy in the event of detection and cleanup, these emails contain malicious attachments that open backdoors on the machines of the victims. According to the researchers, the attackers employ hacked Outlook accounts to try and guess Exchange credentials, and they have also discovered Python scripts designed to extract emails from Zimbra servers.

The APT group also uses SoftEtherVPN to create VPN servers on infected public-facing servers to gain access to their victims' private networks and increase their capacity to move laterally within such networks. After being established on the network, Earth Krahang uses tools and malware that can execute commands and gather data, like Cobalt Strike, RESHELL, and XDealer. The more advanced and intricate of the two backdoors, XDealer, can intercept clipboard data, record keystrokes, grab screenshots, and work with both Windows and Linux.

Based on command and control (C2) overlaps, the security researchers claim to have first discovered connections between Earth Krahang and another China-linked actor Earth Lusca, although it has now concluded that this is a distinct cluster. These threat groups probably function as a specialized task force for cyber espionage against government institutions, working under the Chinese corporation I-Soon.

Furthermore, XDealer and RESHELL were formerly connected to the 'Luoyu' threat actors and the 'Gallium' organization respectively. The analysis, however, indicates that these instruments are probably distributed among the threat actors, each of whom uses a different encryption key.

Impact

- Cyber Espionage
- Unauthorized Access
- Sensitive Data Theft

Indicators of Compromise

MD5

- ac805ddb262214cc50b1e7ae45551e3e
- d524867c321910ab6ea584019e74c99b
- aac4141dba6328f3529b38a28f8dbb92
- 87fb1af534b0913bb23fe923afd34064
- 8d403b49e57dbec1de505bb244b6dbe6
- c667cae395fd34323e7acecbed584db8
- 5b7ce4a1328f3e9fff4f678999a9dbe8
- bd824d170b9422375b3c9931f746f1f2
- 6c52c837ba6ebe6615d18bfb15f26dce
- 8138f1af1dc51cde924aa2360f12d650
- 6c23ce5827c541f6a713ea991fc35a17

SHA-256

- 10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f
- 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1
- 1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3
- 2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa
- 8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d
- 2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee
- 521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a
- 01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c
- acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2
- 15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
- 1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c

SHA-1

- 9da6d0356582c17d9abeceb81bc4474eaba01e5c
- bfe73dfed7863ff9dbf26390bec2b004f7f1bb4f
- e5bde7ae2fde36edcab5885cb5fbc52a905e06ea
- 8d4770c418ae0e99fb4d5e3c70d3cbe15e45602c
- c905ebe27704ef84d78d193dd36b59cf1c682ec7
- 44cf84693216f7a4b44c89bdbffa10e72fbfffdd
- 8a2382101c784c683d3e649861b991e2f307ed44
- 5eb6c7b72120fbdacc41c4abcf676af7b58daf69
- ced4d0919179210c0fdbd5db440de17c65a7a4e1
- 74b1da190d670fa4c207afb0fbca4d7df701538a
- c747544c6a42afd337351c096a0baa97e1343c85

Domain Name

- gtldgtld.store
- tfirstdaily.store

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls
- Never trust or open links and attachments received from unknown sources/senders.
- Identify and isolate compromised systems or hosts that are confirmed to be affected by the malware. Disconnect them from the network to prevent further communication with command-and-control servers.
- Regularly update and patch software and systems to mitigate vulnerabilities.
- Conduct regular security audits and penetration testing to identify and address weaknesses.
- Review and reset user account passwords, especially those with elevated privileges, to prevent unauthorized access. Disable or remove any compromised accounts.
- Ensure secure storage of backups and sensitive information with access restricted to authorized personnel only.
- Implement strict access controls and the principle of least privilege (PoLP) to restrict user and system access rights. This reduces the attack surface.
- Continuously monitor command-and-control (C2) traffic patterns and communications to identify anomalies and block malicious C2 activity.
- Train employees and staff on cybersecurity best practices and how to recognize phishing attempts and social engineering tactics.
- Develop a robust incident response plan that outlines steps to take in the event of a breach. This should include procedures for containment, investigation, and notification of affected parties.
