Hive Pro

Hiveforce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Earth Hundun's Deuterbear Sets Sights on High-Value Sectors

Summary

**Malware:** Waterbear backdoor (aka Deuterbear)
Threat Actor: Earth Hundun (aka BlackTech)
Attack Region: Asia-Pacific region
Targeted Industries: Technology, Research, and Government
Attack: The Earth Hundun group has recently initiated a sequence of cyber intrusions directed at the Asia-Pacific region. These attacks foreshadow the introduction of an enhanced iteration of their modular backdoor, Waterbear, alongside its more sophisticated successor, Deuterbear.

⚔ Attack Regions
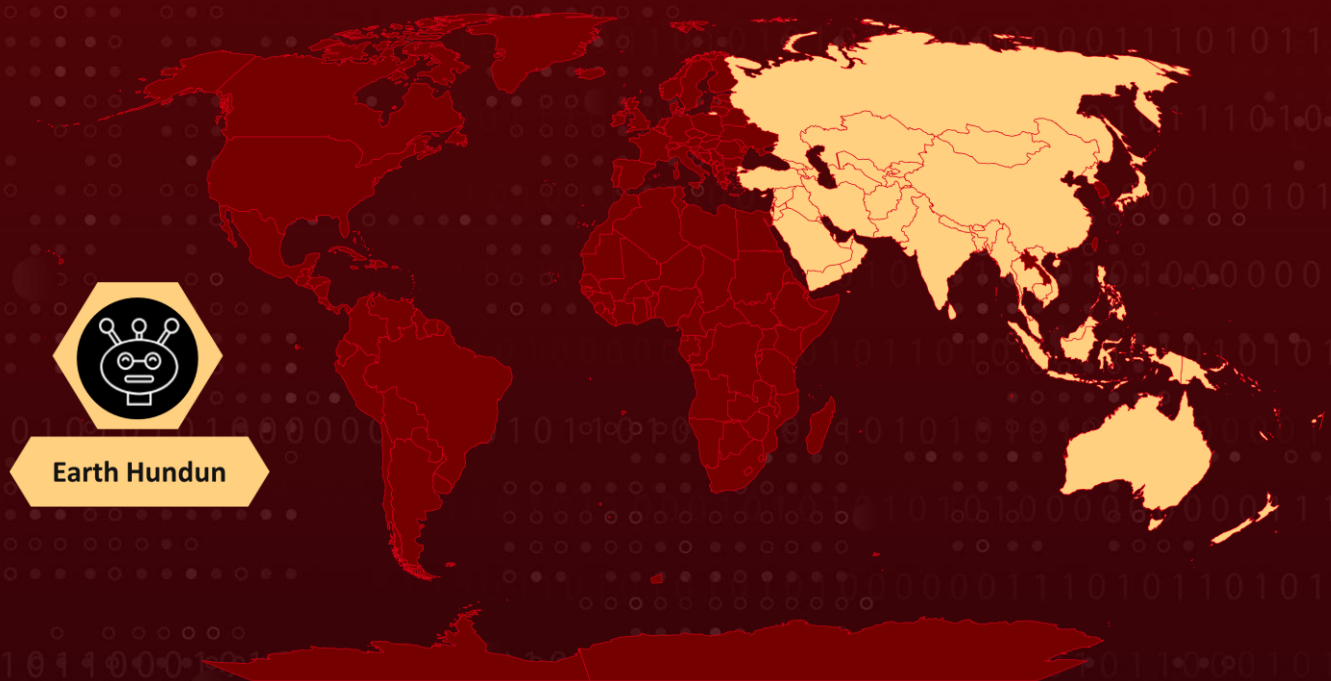
Earth Hundun

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The Earth Hundun faction also recognized as BlackTech, has orchestrated a recent surge in cyber intrusions primarily targeting the Asia-Pacific region. These breaches serve as a precursor to the deployment of an upgraded iteration of their modular backdoor, known as Waterbear, alongside its advanced successor, named Deuterbear.

#2 Within the arsenal wielded by the Earth Hundun group, the Waterbear backdoor stands out as a formidable entity, boasting a sophisticated array of countermeasures against debugging, sandboxing, and conventional antivirus systems.

#3 Furthermore, the continual refinements by its developers have fortified its evasion capabilities, incorporating enhancements to its loading mechanisms, download processes, and communication protocols. In the year 2022, Earth Hundun transitioned to employing the latest iteration of Waterbear, dubbed Deuterbear, which brings forth several significant alterations.

#4 Notable among these enhancements are anti-memory scanning functionalities and decryption routines. The Deuterbear downloader utilizes HTTPS encryption to safeguard network traffic and incorporates various updates in malware execution, including adjustments to function decryption, debugger, and sandbox detection mechanisms, as well as alterations to traffic protocols.

Recommendations

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Heighten Employee Awareness: Educate employees on cybersecurity best practices, emphasizing the importance of vigilance against phishing attempts. Encourage reporting of any suspicious emails or activities.

⚛ Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1129** Shared Modules
T1106 Native API	**T1574.002** DLL Side-Loading	**T1547.012** Print Processors	**T1027.001** Binary Padding
T1036.005 Match Legitimate Name or Location	**T1140** Deobfuscate/Decode Files or Information	**T1480** Execution Guardrails	**T1497.003** Time Based Evasion
T1622 Debugger Evasion	**T1083** File and Directory Discovery	**T1016.001** Internet Connection Discovery	**T1049** System Network Connections Discovery
T1057 Process Discovery	**T1082** System Information Discovery	**T1012** Query Registry	**T1005** Data from Local System
T1041 Exfiltration Over C2 Channel	**T1071.001** Web Protocols	**T1573** Encrypted Channel	**T1132.002** Non-Standard Encoding

⚔ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e669aaf63552430c6b7c6bd158bcd1e7a11091c164eb034319e1188d43b5490c, 0da9661ed1e73a58bd1005187ad9251bcdea317ca59565753d86ccf1e56927b8,

TYPE	VALUE
SHA256	ca0423851ee2aa3013fe74666a965c2312e42d040dbfff86595eb530be3e963f, 6dcc3af7c67403eaae3d5af2f057f0bb553d56ec746ff4cb7c03311e34343ebd, ab8d60e121d6f121c250208987beb6b53d4000bc861e60b093cf5c389e8e7162, a569df3c46f3816d006a40046dae0eb1bc3f9f1d4d3799703070390e195f6dd4, e483cae34eb1e246c3dd4552b2e71614d4df53dc0bac06076442ffc7ac2e06b2, c97e8075466cf91623b1caa1747a6c5ee38c2d0341e0a3a2fa8fcf5a2e6ad3a6, 6b9a14d4d9230e038ffd9e1f5fd0d3065ff0a78b52ab338644462864740c2241, d665aea7899ad317baf1b6e662f40a10d42045865f9eea1ab18993b50dd8942d, dc60d8b1eff66bfb91573c8f825695e27b0813a9891bd0541d9ff6a3ae7e8cf2, 4540132def6dfa6d181cabf1e1689bede5ecfef6450b033fecb0aeb1fe1b3fe9, 8f26069b6b49391f245b8551aa42ca4814c52e7f52d0343916f5262557bf5c52, 74efa0ce94f4285404108d3d19bf2ff64c7c3a1c85e9b59cf511b56f9d71dc05, d6ac4f364b25365eb4a5636beffc836243743ecf7ef4ec391252119aed924cab
Domains	freeprous.bakhell[.]com, cloudflaread.quadrantbd[.]com, showgyella.quadrantbd[.]com, rscvmogt.taishanlaw[.]com, smartclouds.gelatosg[.]com, suitsvm003.rchitecture[.]org, cloudsrm.gelatosg[.]com

⚙ References

https://www.trendmicro.com/en_us/research/24/d/earth-hundun-waterbear-deuterbear.html

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.

More at www.hivepro.com