Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

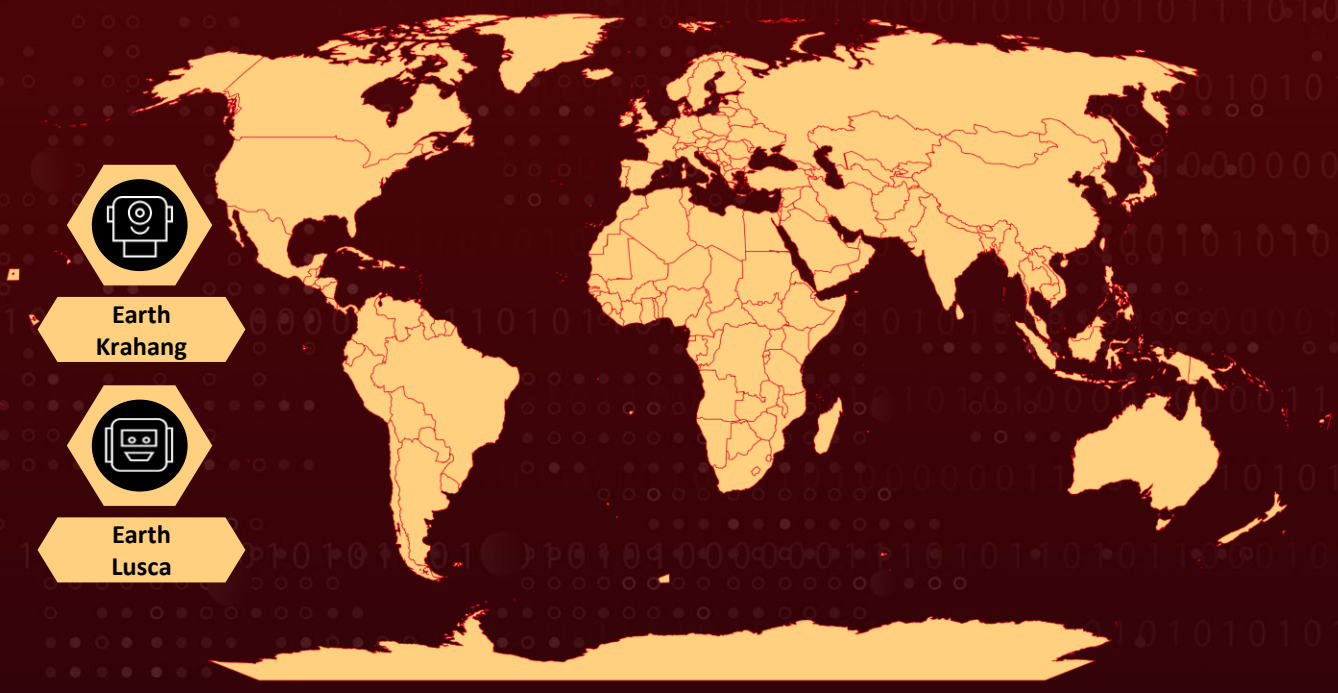
Earth Krahang APT Campaign Targeting Governments Globally

Date of Publication	Admiralty Code	TA Number
March 19, 2024	A1	TA2024106

Summary

Attack Began: February 2022
Targeted Countries: Worldwide
Threat Actor: Earth Krahang and Earth Lusca
Malware: RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad
Targeted Industries: Government, Education, Telecommunications, Finance, Insurance, Foundations, NGOs, Think tanks, Healthcare, IT, Manufacturing, Media, Military, Real estate, Retail, Sports, and Tourism
Affected Platform: Windows and Linux
Attack: Earth Krahang, an APT campaign since 2022, targets global government entities, employing spear phishing and server exploitation tactics. Operating independently but with potential links to Chinese threat actors, it utilizes malware like Cobalt Strike and XDealer for espionage, urging organizations to bolster security measures and patch vulnerabilities.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Ignite Realtime Openfire	✗	✓	✓
CVE-2022-21587	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	✗	✓	✓

Attack Details

#1

A new APT campaign named Earth Krahang has been monitored since early 2022, targeting government entities globally, especially in Southeast Asia but also in Europe, America, and Africa. Earth Krahang operates independently from another China-linked threat actor, Earth Lusca, although they share some infrastructure and tactics.

#2

The campaign involves exploiting vulnerabilities in public-facing servers, conducting spear phishing attacks, and using compromised government infrastructure to host malicious payloads and send spear phishing emails. Earth Krahang employs various post-exploitation techniques including installing VPN servers, maintaining backdoor persistence, accessing credentials, lateral movement, and email exfiltration.

#3

Malware families used by Earth Krahang include Cobalt Strike, RESHELL, and XDealer, with the latter being more comprehensive. The campaign primarily targets government organizations but also includes other sectors such as education, telecommunications, and finance.

#4

The campaign has targeted approximately 70 victims across 45 countries, primarily government organizations. There are suspected links between Earth Krahang and Earth Lusca, potentially managed by the same threat actor or organization. However, Earth Krahang operates independently, focusing on similar victim profiles.

Recommendations

Patch Management: Implement a robust patch management process to ensure that software and systems are regularly updated with the latest security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors like Earth Krahang.

Access Control and Authentication: Deploy strong access controls and authentication mechanisms to prevent unauthorized access to sensitive systems and data. Enforce the principle of least privilege to limit user access rights and privileges to only those necessary for their role.

Email Security Measures: Deploy email security solutions to detect and block phishing emails, malware attachments, and suspicious URLs. Implement email authentication protocols such as SPF, DKIM, and DMARC to prevent email spoofing and impersonation attacks.

Network Monitoring and Intrusion Detection: Deploy network monitoring and intrusion detection systems to detect anomalous behavior and potential indicators of compromise. Monitor network traffic for signs of reconnaissance, lateral movement, and data exfiltration associated with APT campaigns like Earth Krahang.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1583.001 Domains	T1583.003 Virtual Private Server	T1586.002 Email Accounts
T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1586 Compromise Accounts	T1583 Acquire Infrastructure

T1588.001 Malware	T1588.003 Code Signing Certificates	T1608.001 Upload Malware	T1608.002 Upload Tool
T1588 Obtain Capabilities	T1608.005 Link Target	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link
T1595.001 Scanning IP Blocks	T1595.002 Vulnerability Scanning	T1595.003 Wordlist Scanning	T1592 Gather Victim Host Information
T1566 Phishing	T1059.006 Python	T1203 Exploitation for Client Execution	T1569.002 Service Execution
T1569 System Services	T1204.002 Malicious File	T1047 Windows Management Instrumentation	T1543.003 Windows Service
T1133 External Remote Services	T1053.005 Scheduled Task	T1505.003 Web Shell	T1068 Exploitation for Privilege Escalation
T1078.003 Local Accounts	T1140 Deobfuscate/Decode Files or Information	T1574.002 DLL Side-Loading	T1656 Impersonation
T1036.005 Match Legitimate Name or Location	T1036.007 Double File Extension	T1112 Modify Registry	T1110.003 Password Spraying
T1003.001 LSASS Memory	T1003.002 Security Account Manager	T1539 Steal Web Session Cookie	T1087.001 Local Account
T1087.002 Domain Account	T1069.002 Domain Groups	T1057 Process Discovery	T1033 System Owner/User Discovery
T1007 System Service Discovery	T1210 Exploitation of Remote Services	T1534 Internal Spearphishing	T1021.006 Windows Remote Management
T1021 Remote Services	T1119 Automated Collection	T1114 Email Collection	T1071.001 Web Protocols

T1573 Encrypted Channel	T1105 Ingress Tool Transfer	T1572 Protocol Tunneling	T1020 Automated Exfiltration
T1199 Trusted Relationship	T1078 Valid Accounts	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1590 Gather Victim Network Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f, 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1, 1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3, 244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a, 35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa, 3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815, 50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab, 57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829, 5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe, 6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb047322f2, 898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce, c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c, d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578, d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3, e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213,

TYPE	VALUE
SHA256	e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36, ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272, 2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa, 8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d, 2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee, 521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a, 9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1, 9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82, bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4, d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b, fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39, 01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c, 05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243, 241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8, 5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472, b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab, c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab, f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac, acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2, ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d, ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e, ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136, 4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9, 63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d,

TYPE	VALUE
SHA256	6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64, f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934, 992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e, bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288, 15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45, 6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2, 98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541, a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91, bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff, ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e, 1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c, 36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1, 46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2, 4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66, 67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355, 6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716, 804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3, 82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846, b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a, da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577, f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb, 07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb, 1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124, 2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780,

TYPE	VALUE
SHA256	2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497, 2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f814028469806cb6bd7, 363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544, 3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030, 45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e, 4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944, 5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5, 5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6, 6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534, 7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c, 767694e220e5119425ed808bc0801a007022614812868e60962660863de42fa5, 799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a, 7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372, 7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c, a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e, a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff, b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8, d2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71, d462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc, dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740, ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4, fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab, 42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956, 44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448,

TYPE	VALUE
SHA256	d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519, 0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9, 4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014, 484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0, b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682, d096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f, 7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa, b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865, bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a, f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1, f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e, c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e, a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea, 0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade, b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f, c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de
IPv4	23[.]106[.]122[.]5, 207[.]148[.]69[.]1, 45[.]76[.]157[.]92, 50[.]7[.]61[.]26, 50[.]7[.]61[.]27, 50[.]7[.]61[.]28, 207[.]148[.]75[.]122, 45[.]32[.]33[.]17, 23[.]106[.]122[.]46, 23[.]106[.]124[.]152, 115[.]126[.]98[.]204, 118[.]99[.]6[.]202, 199[.]231[.]211[.]19, 149[.]28[.]26[.]2

TYPE	VALUE
Domains	www[.]security-microsoft[.]net, update[.]centos-yum[.]com, update[.]microsoft-setting[.]com, update[.]windows[.]server-microsoft[.]com, cdn-dev[.]helpkaspersky[.]top, data-dev[.]helpkaspersky[.]top, happy[.]gitweb[.]cloudns[.]nz, support[.]helpkaspersky[.]top, gtldgtld[.]store, softupdate[.]xyz, tfirstdaily[.]store

Patch Links

https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm

https://www.oracle.com/security-alerts/cpuoct2022.html

References

https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html

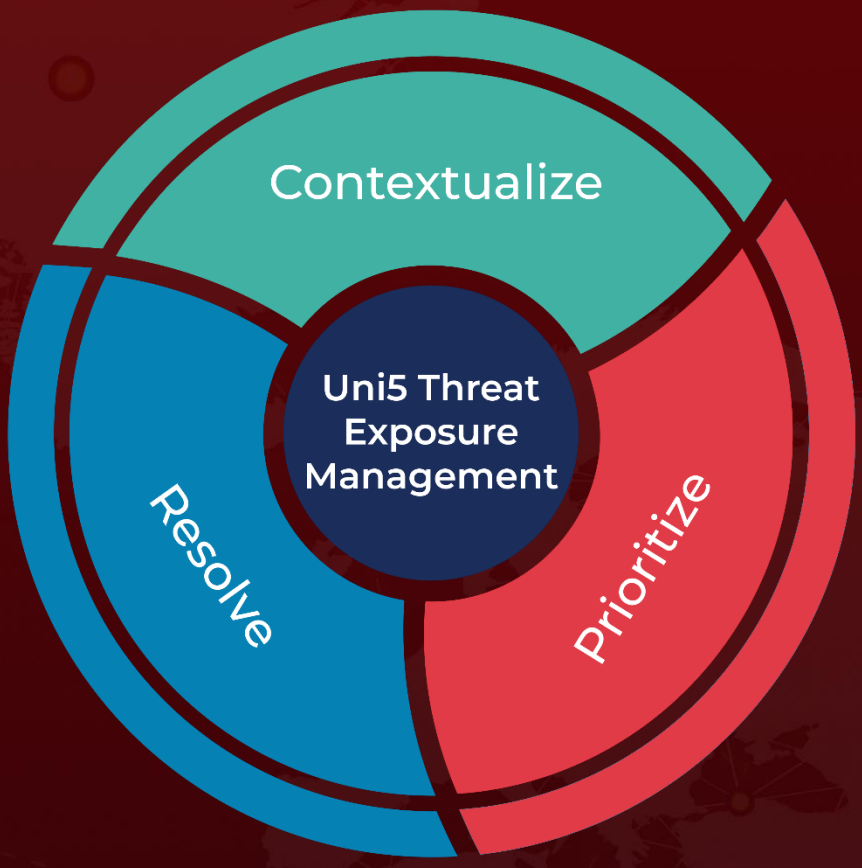
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/c/earth-krahang-exploits-intergovernmental-trust-to-launch-cross-government-attacks/earth_krahang_iocs.txt

https://www.hivepro.com/threat-advisory/earth-luscas-sneaky-moves-unleashes-new-linux-backdoor/

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

March 19, 2024 • 5:30 AM

More at www.hivepro.com