Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

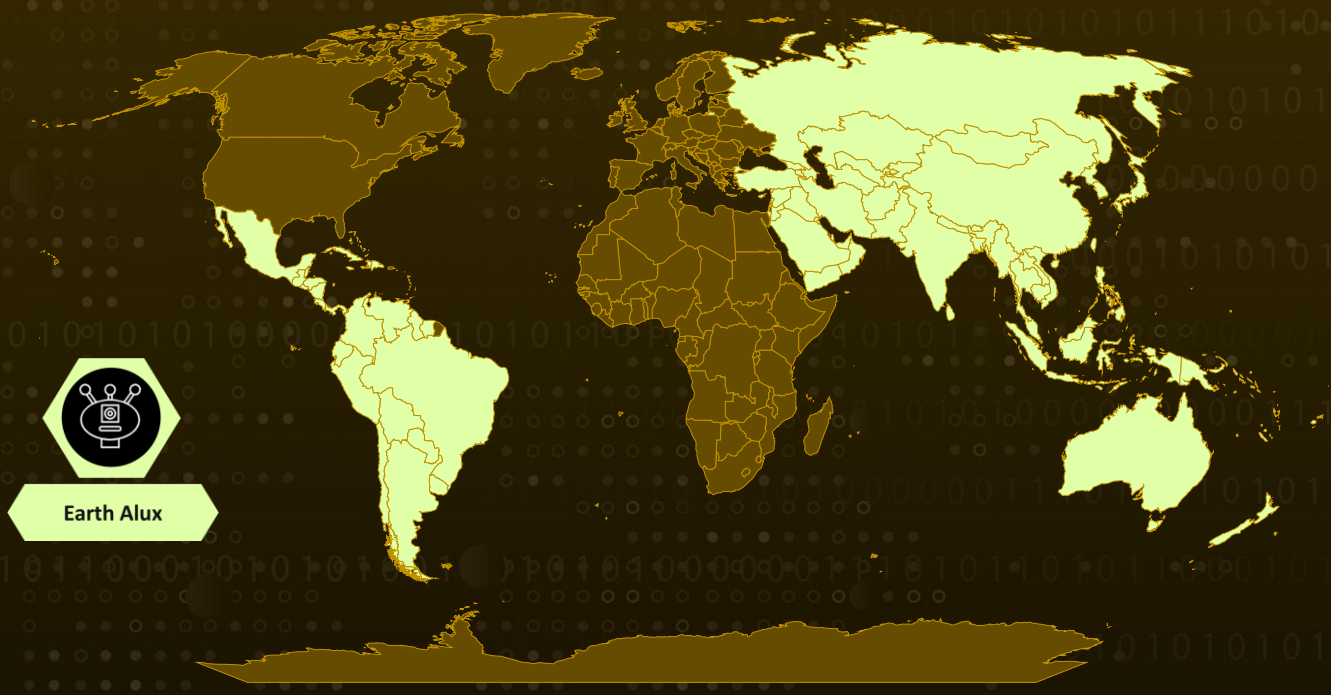
# Earth Alux the Cyber Threat Hiding in Plain Sight


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| April 3, 2025 | A1 | TA2025100 |

# Summary

**Attack Commenced:** April 2023
**Threat Actor:** Earth Alux
**Malware:** GODZILLA, VARGEIT, RAILLOAD, MASQLOADER
**Affected Platform:** Windows
**Targeted Regions:** Asia-Pacific (APAC) and Latin American
**Targeted Industries:** Government, Technology, Logistics, Manufacturing, Telecommunications, IT Services, Retail
**Attack:** Earth Alux, a stealthy China-linked APT group, is making waves in the cyberespionage world with its advanced tactics and near-invisible intrusions. Targeting high-value sectors across APAC and Latin America, it exploits vulnerabilities, plants sophisticated backdoors like VARGEIT and seamlessly hijacks legitimate processes to steal sensitive data all while staying under the radar.

## Attack Regions



# Attack Details

**#1** Earth Alux, a China-linked APT group, orchestrates sophisticated cyberespionage campaigns across the APAC and Latin American regions, employing advanced techniques to remain undetected while exfiltrating sensitive data. Their initial foothold is established by exploiting vulnerabilities in exposed servers, followed by the deployment of web shells like GODZILLA to facilitate backdoor installation.

**#2** At the core of their toolkit is VARGEIT, their primary backdoor, which enables fileless execution of auxiliary tools for lateral movement and network reconnaissance. Alongside VARGEIT, Earth Alux employs COBEACON (aka Cobalt Strike Beacon) as an initial backdoor, while VARGEIT itself operates at multiple stages of the attack.

**#3** A defining characteristic of VARGEIT is its ability to inject additional tools from its command-and-control (C&C) server into newly spawned Microsoft Paint processes, streamlining reconnaissance, data collection, and exfiltration.

**#4** Its deployment follows a structured process initially loaded via a debugger script before transitioning to DLL sideloading, incorporating execution guardrails and timestomping via RAILLOAD a loader and RAILSETTER an installation and timestomping tool. The malware can also be executed through MASQLOADER or via RSBINJECT, a Rust-based shellcode loader.

**#5** To ensure stealth and longevity, Earth Alux leverages VirTest, a tool commonly used in Chinese-speaking cybercriminal circles, to refine its evasion tactics. Their targets span critical sectors, including government, technology, logistics, manufacturing, telecommunications, IT services, and retail, highlighting their focus on infiltrating high-value environments and acquiring strategically significant intelligence.

# Recommendations

**Deploy Endpoint Detection and Response (EDR) Solutions:** Implement EDR tools to detect suspicious activities, such as unauthorized registry changes, process injections, and the creation of persistent tasks. Ensure rapid response and containment capabilities to neutralize threats as they occur.

**Strengthen Perimeter Security:** Regularly patch and update all exposed services to eliminate vulnerabilities. Conduct routine vulnerability assessments and penetration testing to identify weak points before attackers do.

**Zero Trust Security Architecture:** Enforce continuous identity verification for all users, devices, and applications accessing critical systems. Segment networks to minimize attack spread and restrict access between different operational zones.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence |
| **TA0005** Defense Evasion | **TA0007** Discovery | **TA0008** Lateral Movement | **TA0009** Collection |
| **TA0011** Command and Control | **TA0010** Exfiltration | **T1190** Exploit Public-Facing Application | **T1083** File and Directory Discovery |
| **T1055** Process Injection | **T1480** Execution Guardrails | **T1588** Obtain Capabilities | **T1588.002** Tool |
| **T1588.006** Vulnerabilities | **T1211** Exploitation for Defense Evasion | **T1564** Hide Artifacts | **T1070** Indicator Removal |
| **T1070.004** File Deletion | **T1070.009** Clear Persistence | **T1057** Process Discovery | **T1570** Lateral Tool Transfer |
| **T1543** Create or Modify System Process | **T1574** Hijack Execution Flow | **T1574.002** DLL Side-Loading | **T1005** Data from Local System |
| **T1001** Data Obfuscation | **T1041** Exfiltration Over C2 Channel | **T1588.005** Exploits | **T1070.006** Timestomp |

| | | | |
|---|---|---|---|
| **T1053** Scheduled Task/Job | **T1027** Obfuscated Files or Information | **T1505.003** Web Shell | **T1082** System Information Discovery |
| **T1036** Masquerading | **T1135** Network Share Discovery | **T1105** Ingress Tool Transfer | **T1518.001** Security Software Discovery |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 00a41c8272d405ba85ae9d0e435e3030033e8a032f3d762367d0a57d41524f3a, 0d3ec88b0bfa5530e45dec75dfbea7ae683bdea91105b5f90a787beaabd1ef27, 0f6fe5d0ee754d581d4a8d989e83272b121d0125bd3c77e57a6b14db23f425ab, 13e0aef0ab6d218e68c5c5b6008872eb73104f161c902511aec3df5bce89136e, 16509adf92b1ac3097452affd8dda640936c8a40272592b978db3698487df5fa, 19bcca292814942f2fe8d142a679cc6a97fa6cbf77a0c98873146e918013bb5c, 1c8c14251710fbdef994d9ccf1d3507cf0ef5cd6c7d3495af2adfe7f97cc0dc2, 1c93ba375016bcb41b915b78eb4ab023ecf456e240823a1d6d2b5297b3523956, 245fdb5e35b6f51b26d4cf3999a40dde13987240f9bf565fe03a1f6adb9da9b2, 281fc3aff361f202a41f4aff84a5f61e5728fd8ea0c1219a8bca540a959a4ee2, 28517bff286ade02b81da52f9fcddcb9764023ae7035bc593d081fdd2a8c85d9, 2971a53769745c107a89eeb5f48e3b3e9680d371bf06b028c7769c961e6f9e55, 3129bfad321be526f231c64aac10d7d8f416dc14cab11c1bbc57252c75823959, 3b7c29489c1feaafc587eac0ffcca79964259c9687d86a5cce5ea70261f7439b, 3f0157cfb493df1cd051cc87364c7bdbe3719927335b76b7c567b369ab47b3be, 41410a8aa4a4fcd811ef67ba023e263f4cd6667039b01547d23a3eb758d97b96, 43e5c3d6182ab6d9d71b5892c5087b4ef4b3093126bcdf4ebcef0b15e04e0c03, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 442446fbc012847a12448398b619837614498bb611968e64166f0e9040c311db,<br>455510fe663775e09a2d0bbfdc4c8ec2e26665e10f9599b05dc59ea460f06ac8,<br>47ea0392ec123e3949b9ae2638b9078cd5efd4da942e38f149ccfb74d8e70123,<br>4be6f5e76ea02ae348b26fc32a0dabe009d05b701e53270cf40ca50fa76197b0,<br>529e691a9d60b8ae0c64de82402e76c112df3bc27be5f2e94ee58252a67804a1,<br>52c8eacbcc8906036894a3a11cb4181d454c3a4f685500a799263cdcf6c6d88e,<br>5502735d81accb96c58300d1e21765b8b53a4749aad68e513b2558ed79f83cc4,<br>5518b542afd9d456ee8dea4dec3e0e8a98a42982b33f8f629d3d8edeca0dbf4d,<br>55b4e3814a349c9de4c99237f62d42787a6fef64b809db9cf52cfe0602cac01e,<br>5872da9dfd5ed3c0b9e0a05466a56c6ac6966012b5b3e14ac43a1225ba5e6bb2,<br>5aaca0994795ba7da0f10cd393ac32cc1e78c9afd4e9d09bbbe430f168c0eebe,<br>5c829480c4563f736c8f6a4a2987fc4cd3fc330804db82cd98217d0110531b6e,<br>5d358bcd0acb999fdec332f0a2d1fe51952542f0836b9618ab18f253597d244c,<br>5dcd5cb720a40692b7e49540a42f1d12e831aaab369d9fe31a66b0433b825264,<br>62d71b61af750ad3b763d98504a174a1949a359a4cb4f6ce2795b7b3240919eb,<br>67dddc4ce777df1baa19acb1c3535eb01a54f24516a85312bafe4cba11d74483,<br>681e9aab60b1c64dacbc7c8574d294333b9cd4494ec683b0c780866c3e1e7d40,<br>762525805afe6a0891275ebc2ae1f067e9aad8f310afc0b1ad800cc980ed8b55,<br>7654e7f7076f07e76ae478c1df65f1711918ad4f36c45f520cc46cdcb1128cc2,<br>7ad44f7e1f78ee83f20da498584ec7138c2514580ddfe62698be7587ae2678e1,<br>83968575244ab2e44a5b94423bb1cacd10bb293ddcbbddbc2fc117f9335b6e78,<br>846be29c140850fd9524339acd67eac4b84bc59ed056544356d199226452ea88,<br>85f9bac9eefb5fbc1e51508ce12cda10a69d8bde82952891081b19d6833297ab, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 86e2d56761fb4dc16c7b0cd8da241c9899af851f5df751ffc67a2d68062e71f4,<br>86f5f088cf997766e52860b57506ba0923454a63bee39e4e3de2fb98c4fee240,<br>8b0023248bc037631b26694f34d7bc8163e2d5f5919fe61f3dbc1354f87d6792,<br>8c89362d4bed8bd2f0fbffc450bca4e7666fc7a3e88ec56a5dd149593fd697ec,<br>91034c01e800b116095eecdb073a5262852fc2c788f9fcd09259d6c09ce88ac6,<br>9366ece5ff9082145184adb2e91053d5e0d68d4d9f9a9f054aad68b8e7368443,<br>9b5e6c2f287ea7931bb27f63111ef0035265bc27751f01bd6c7f3dd3395bbaf5,<br>9d9f40c6c2dc14118452f7f1b56346e60a8681fb83300e4292576e635b37f9c8,<br>9f94bb59bfc32958a15cd8e225f270802bd9e14929e5d0f4f488842710a361ea,<br>a042157e7460f6c28c984a1c1f3803521a556c67e26411854e497685ef436325,<br>a14e226a50c12e637e8b280ad688e5637db752c72d0f8b2bac5f2d3d487e1c21,<br>a79679d8f9551810504ff316465fb289d1ac64dc52bcaabd70267217d33d603c,<br>a845cb84ea11f0fa7a982407705e892f58d7cb407eadc5329416464cccdd6a23,<br>a9804fa05845707f094fe91668a5c3792f2441d371816b46fbe636953fc5787d,<br>ab6145f1ea6c8a682bea289cef06c0f27fa076b8f88a89a2631167541fc835e9,<br>ac70d98af57d9e3da9ee485a4ab1badbb28e89d15c4ef2df521423881a147e43,<br>afd83d598843f93f7cad02bbe8467da2f257b5344600090034bb795844f05bdc,<br>b0a42d1c5a07bbe317a034e204c0eb64ae5d99e3dfbfbd9b3b098caea4b19f96,<br>b32dd5d549bcf4b674b4e7cf5481064b38ea614c666b158afedc7084b715c1fa,<br>b8accaa144c035c670fb3c2bf580d2fb64ab562c89835f7e30b044a8711cb5e5,<br>b8e1a46146c09ef54b802a6989b485ef5982a86228a24ec0839ec5af7b42e648,<br>b92452a6c2cd13193a6df88278c31c85008acf448655c18389c84b353026d15e,<br>b9fefe3946d0c9e000262a10b184090da45925f24b7dfc9d25abe63bc55ca7ed, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | ba0105c8fa99b8f3a82c32d20e94031f22e277286b738db529e763955df248dc, bd0dbf799e98137238ae38f134c7af82d7ff673c0a418044add0220211d98a27, be01089ad2c2e7af32677ec0a7a9a541dee1cb149639d60fb7b7e9b641d2ccdb, c0d1deb30fd3507455dae99aabf1cc23638b2bcf1908099e08081ee2691a24b0, c56c88ce8e45a9caa043f1f4831442f09bae6f1a083910f772afc1e27be3b606, c6a28c9cac9c4b5ef57998bdc7a7f430fff7c9ac819fef278f8350751b6edaab, cd385806117ebe1504af4669671b4c0a252faec873e1402aaebeb413fdd58556, d31eb16688d1b36652e87d43ad5755d139eedd74b500ddcee97a5545d8d1fe7b, d34947e11879598b85d9baa703cb96a83d7c3ccb53868ab86ff9a2f37dc91459, d692c85da91bb5e5724f520ca392b68eee144a3719a7441c779c8ce73d3b25dc, d83a837910305567acfd49d2d416fc4b113f080e31730c9b0abefa4b01192a40, ded42e37f05950374496824ce3f4d540a45e97be35ed6d7ddcfcf12a7b2cd46f, dfbb857e6383789545c719c99d878a678a0aeae2a6a1c8f44e87b7aa478fc354, e03062caa13400df3d60efb1aa2b0f19dcf65fefc38d4bc9931c0918b5dc4865, e299b865cdb0fdd9605e3c5e9d00fb473c77af4ed213775d594cc0fe91b8dd3a, e3465c996e149b218d95a4b109e6e3ff268e8d63aafa73d4855750b33c66a33c, e6141757775ce9747b12f21cc7f8411e5ab4916649f38738f4e93b2ca7cc274a, ee8385313e03890c6862f70c94f2c5a3e9cd09764fcac4488fabc5ce9613228a, f0cd90b42969706d1a78e75608aded6d5ac8610f36cab8f8be7160c5cbf485a5, f92493bf2b46873feee38ea2dac69ff830637983d569b64ee87e75f7fe08de88, fd1720b11ddd7ae226889deca9a6532df676a4991f0209c0a3d6d7be52276dcf, fd3637392404c3ed169a4999f6a05274715109f9fa028be9ad9ce7853d983d54 |

| TYPE | VALUE |
| --- | --- |
| IPv4 | 8[.]218[.]222[.]216 |
| Domains | www[.]upload-microsoft[.]com,<br>store[.]azure-clouds[.]com,<br>google[.]otp[.]us[.]kg |

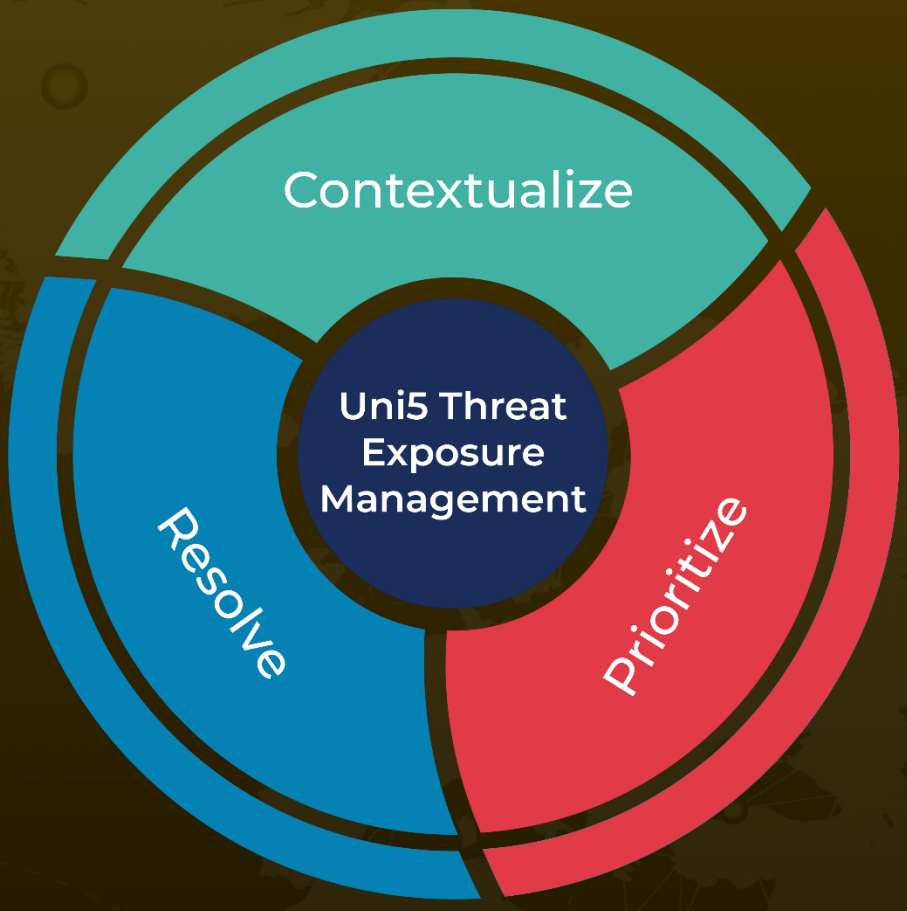
## References

https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolkit-of-earth-alux.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.




REPORT GENERATED ON

**April 3, 2025 • 5:00 AM**



More at www.hivepro.com