Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

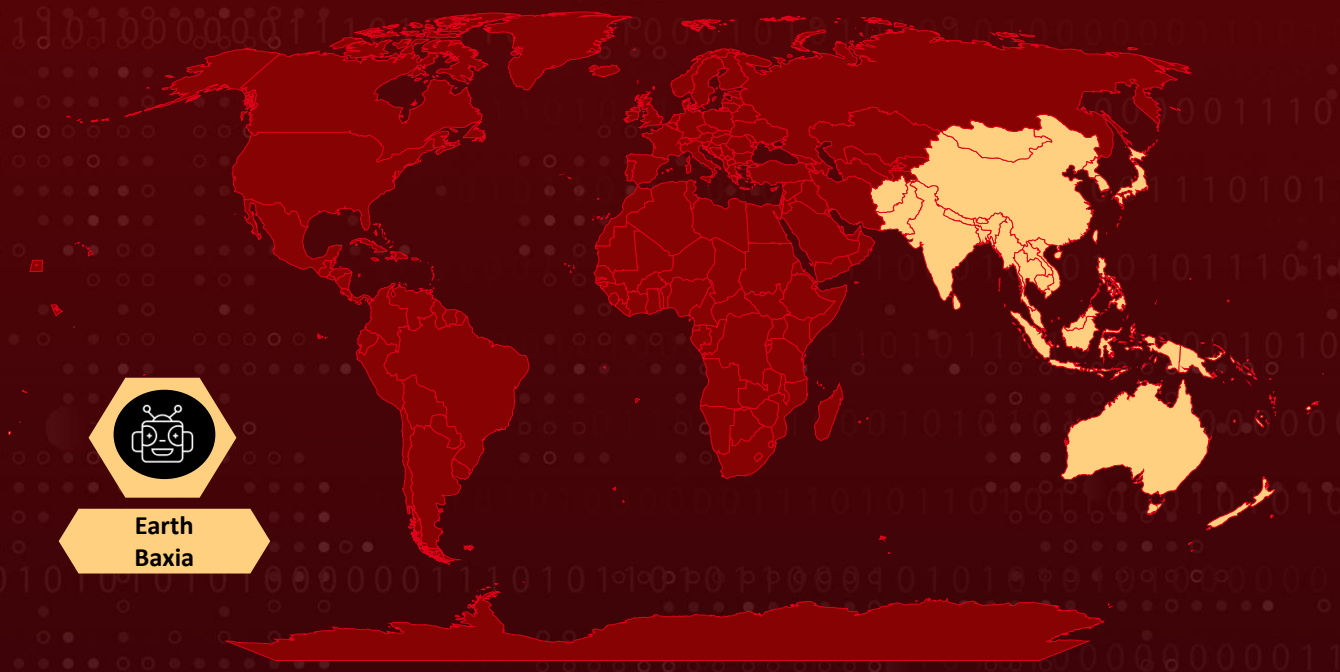
Earth Baxia: A New Threat to APAC Governments

Date of Publication	Admiralty Code	TA Number
September 23, 2024	A1	TA2024367

Summary

First Appearance: June 21, 2024
Threat actors: Earth Baxia
Malware: EAGLEDOOR
Targeted Region: Asia–Pacific
Targeted Industries: Government, Telecommunication, and Energy
Attack: Earth Baxia is a cyber espionage group targeting government organizations in the Asia-Pacific region, particularly Taiwan, through spear-phishing and exploiting the GeoServer vulnerability (CVE-2024-36401). Their attacks involve deploying customized Cobalt Strike payloads and a new backdoor called EAGLEDOOR, which supports multiple communication protocols for data exfiltration. Organizations must enhance their cybersecurity measures to defend against these sophisticated threats.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-36401	OSGeo GeoServer GeoTools Eval Injection Vulnerability	Ivanti Endpoint Manager	✗	✓	✓

Attack Details

#1

Earth Baxia, a sophisticated cyber espionage group likely based in China, has been actively targeting government organizations and critical sectors in the Asia-Pacific (APAC) region, particularly focusing on Taiwan. Their attack strategy primarily involves spear-phishing campaigns and the exploitation of a critical vulnerability in GeoServer, identified as CVE-2024-36401.

#2

The attack typically begins with spear-phishing emails crafted to deceive recipients into downloading malicious attachments or clicking on harmful links. One notable case involved a Taiwanese government organization that reported receiving over 70 phishing emails within a two-week period. These emails often contained decoy documents designed to appear legitimate, which, when opened, would execute a malicious .NET application. This application facilitates further payload injections into the victim's system using advanced techniques such as AppDomainManager injection.

#3

In conjunction with spear-phishing, Earth Baxia exploits the GeoServer vulnerability (CVE-2024-36401), which allows for remote code execution (RCE). By leveraging this exploit, attackers can execute arbitrary commands on compromised systems. For instance, they use commands like curl and scp to download malicious components directly into the victim's environment.

#4

Once initial access is achieved through either spear-phishing or the GeoServer exploit, Earth Baxia deploys customized versions of Cobalt Strike a well-known penetration testing tool modified to evade detection. This modified Cobalt Strike includes altered internal signatures and configuration structures, making it difficult for traditional security measures to identify malicious activity. The deployment often occurs through DLL side-loading techniques, allowing the attackers to maintain stealth during their operations.

#5

Additionally, Earth Baxia has introduced a new backdoor known as EAGLEDOOR. This backdoor supports multiple communication protocols, including DNS, HTTP, TCP, and Telegram. EAGLEDOOR enables the group to gather sensitive information from compromised machines and exfiltrate data efficiently while maintaining long-term access to the systems. Sensitive data collected from compromised systems is typically exfiltrated using commands like curl, sending the information back to the attackers' remote servers.

#6

The Earth Baxia campaign exemplifies a sophisticated approach to cyber espionage that combines spear-phishing tactics with exploitation of critical vulnerabilities. Their focus on government and energy sectors across multiple APAC countries highlights the need for organizations to strengthen their cybersecurity measures against such targeted attacks.

Recommendations

Regular Patching and Vulnerability Management: Regularly update GeoServer and other software. Attackers like Earth Baxia exploit outdated software to gain unauthorized access. Regularly applying patches will close known vulnerabilities and reduce the attack surface.

Enhance Email Security: Strengthening email filters is crucial to detecting spear-phishing attempts. Anti-phishing tools should be integrated to identify suspicious emails, and staff should be trained to recognize common phishing tactics, such as unfamiliar attachments or links disguised as legitimate sources.

Network Segmentation: By dividing critical systems from other parts of the network, companies can limit the spread of malware or unauthorized access. If one segment is compromised, attackers will be prevented from gaining access to more sensitive areas, thus minimizing potential damage and data loss.

Implement Multi-factor Authentication (MFA): MFA provides additional layers of security beyond just passwords. With Earth Baxia using phishing as an entry method, MFA ensures that even if login credentials are compromised, attackers cannot easily breach accounts without a second form of verification.

Regular Security Audits: Conducting frequent and thorough security audits helps identify weaknesses and potential entry points before attackers do. This proactive measure ensures that any security gaps are addressed swiftly and helps maintain compliance with industry security standards.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
TA0011 Command and Control	TA0010 Exfiltration	T1071.001 Web Protocols	T1071.004 DNS
T1566.001 Spearphishing Attachment	T1566 Phishing	T1574.014 AppDomainManager	T1105 Ingress Tool Transfer
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1027.010 Command Obfuscation	T1027 Obfuscated Files or Information

T1082 System Information Discovery	T1620 Reflective Code Loading	T1190 Exploit Public-Facing Application	T1027.013 Encrypted/Encoded File
T1001 Data Obfuscation	T1071 Application Layer Protocol		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	916f3f4b895c8948b504cbf1beccb601ff7cc6e982d2ed375447bce6ecb41534, 4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54, 6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbed3094612a6696a40c664ce, 1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448, 4ad078a52abeced860ceb28ae99dda47424d362a90e1101d45c43e8e35dfd325, 04b336c3bcfe027436f36dfc73a173c37c66288c7160651b11561b39ce2cd25e, c78a02fa928ed8f83bda56d4b269152074f512c2cb73d59b2029bfc50ac2b8bc, 1c13e6b1f57de9aa10441f63f076b7b6bd6e73d180e70e6148b3e551260e31ee, 9b50e888aaec0e4d105a6f06db168a8a2dcf9ab1f9deeff4b7862463299ab1ca, d23dd576f7a44df0d44fca6652897e4de751fdb0becc6b14b754ac9aafc9081c, d3c1ada67f9fe46dfb11f72c1754667d2ccd0026d48d37b61192e3d0ef369b84, e9854ab68dad0a744925118bfae4ec6ce9c4b7727e2ad6763aa50b923991de95, b3b8efcaf6b9491c00049292cdff8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4befa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7, 1c26d79a841fdca70e50af712f4072fea2de7faf5875390a2ad6d29a43480458

TYPE	VALUE
Domains	recordar-simmco.s3.sa-east-1.amazonaws[.]com, wordpresss-data.s3.me-south-1.amazonaws[.]com, ecgglass-arq.s3.sa-east-1.amazonaws[.]com, souzacambos.s3.sa-east-1.amazonaws[.]com, cooltours.s3.sa-east-1.amazonaws[.]com, xiiltrionsoledadprod.s3.sa-east-1.amazonaws[.]com, app-dimensiona.s3.sa-east-1.amazonaws[.]com, bjj-files-production.s3.sa-east-1.amazonaws[.]com, footracker-statics.s3.sa-east-1.amazonaws[.]com, proradead.s3.sa-east-1.amazonaws[.]com, s3-contemp.s3.sa-east-1.amazonaws[.]com, homologacao-sisp.s3.sa-east-1.amazonaws[.]com, doare-assets.s3.sa-east-1.amazonaws[.]com, kcalmoments.s3.me-south-1.amazonaws[.]com, speedshare.oss-cn-hongkong.aliyuncs[.]com, 360photo.oss-cn-hongkong.aliyuncs[.]com, bobs8.oss-cn-hongkong.aliyuncs[.]com, status.s3cloud-azure[.]com, api.s2cloud-amazon[.]com, visualstudio-microsoft[.]com, us2.s3bucket-azure[.]online, static.trendmicrotech[.]com, rocean.oca[.]pics, static.krislab[.]site, ms1.hinet[.]lat, msa.hinet[.]ink
IPv4	167[.]172[.]89[.]142, 167[.]172[.]84[.]142, 152[.]42[.]243[.]170, 188[.]166[.]252[.]85

Patch Details

Upgrade to the latest versions of GeoServer 2.23.6, 2.24.4, and 2.25.2, and GeoTools 29.6, 30.4, and 31.2.

Patch Links:
https://sourceforge.net/projects/geotools/files/

https://geoserver.org/download/

References

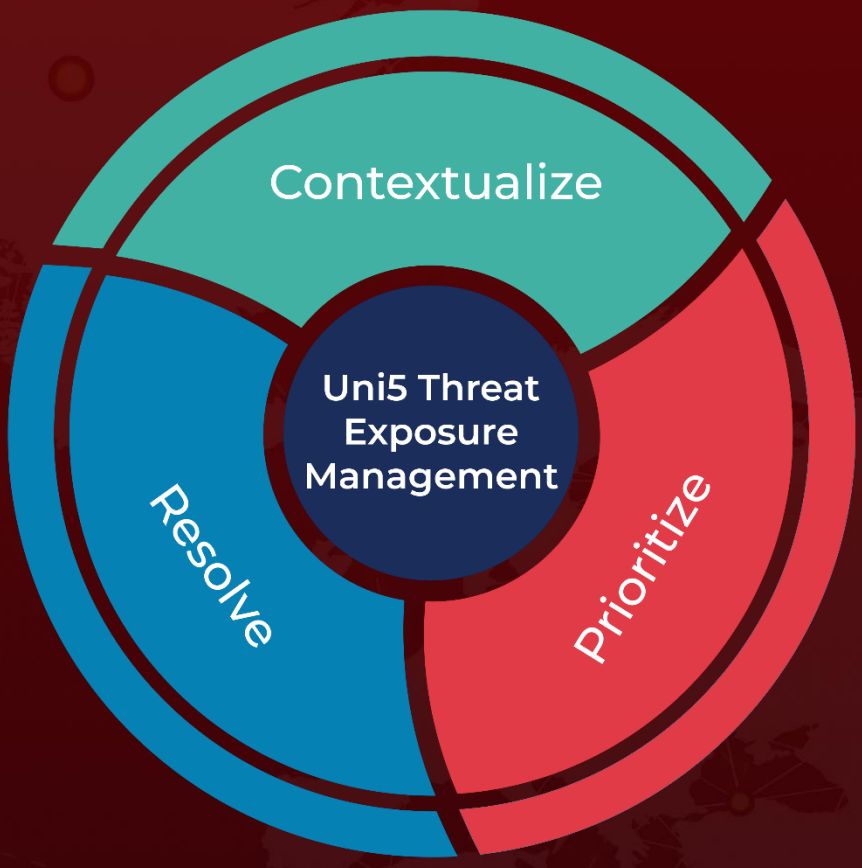
https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html

https://hivepro.com/threat-advisory/critical-geotools-rce-flaw-exploited-in-geoserver-attacks/

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

September 23, 2024 . 10:30 PM

More at www.hivepro.com