PRIMUS PARTNERS®

Quote by Devroop Dhar, Co-founder & CEO, Primus Partners

Published in CSO
October 15, 2025

Flax Typhoon exploited ArcGIS to gain long-term access

Flax Typhoon turned the trusted ESRI mapping tool into a web shell, gaining persistent access

Read on: https://www.csoonline.com/article/4072876/flax-typhoon-exploited-arcgis-to-gain-long-term-access.html

Article Content: An advanced persistent threat (APT) group, Flax Typhoon, was able to gain persistent access to the mapping tool ArcGIS for over a year, putting several enterprises at risk.

ArcGIS is a geospatial platform developed by ESRI, often relied upon by organizations to understand and analyze data in a geographic context.

China-based Flax Typhoon, also known as Ethereal Panda, modified the geo-mapping application's Java server object extension (SOE) into a functioning web shell, according to new research from ReliaQuest.

Flax Typhoon had gated access with a hardcoded key for exclusive control and embedded it in system backups. This helped the actor in achieving deep, long-term persistence that could survive a full system recovery. It prioritized persistence, lateral movement, and credential harvesting, typically gaining initial access by exploiting public-facing servers, deploying web shells, and establishing VPN connections, noted the company.

“The tactics are getting more sophisticated in compromising and manipulating trusted components or tools such as PowerShell or custom SoEs or public-facing portal connects instead of building and injecting a malware,” said Neil Shah, vice president at Counterpoint Research. “This could thus go undetected as there is some form of already established baseline or higher level of trust regarding security and is whitelisted by enterprises with onus on the application or tool developer.”

Turning ArcGIS into a web shell

The activity began with modifying an ArcGIS server SOE to behave as a web shell, ReliaQuest explained. The attackers found a public-facing ArcGIS server that was connected to a private, internal ArcGIS server for backend computations (a common default configuration). It then executes base64-encoded (disguised) commands to the portal server, consistent with this proxying model.

For initial execution, actors sent a malicious GET web request with a base64-encoded payload in the layer parameter. Decoded, it resolved to “cmd.exe /c mkdir C:\Windows\System32\Bridge,” instructing the server to create a hidden system directory named Bridge. This serves as a private workspace for the attackers. A hardcoded key was appended to the request, which was required to trigger the web shell and execute commands.

This was followed by repeatedly abusing this same web shell to run additional encoded PowerShell commands, routed through the same “JavaSimpleRESTSOE” extension and “getLayerCountByType” operation. This consistent method allowed them to advance their objectives while blending in with normal server traffic.

Learning the web shell worked, the threat actor used discovery commands like “whoami” to discover the compromised service account with local administrator rights and created new directories to serve as a staging area for the tools they would use later.

Activity was ramped up by scanning the internal network over various protocols, including Secure Shell (SSH), HTTPS, Server Message Block (SMB), and Remote Procedure Call (RPC), and conducting several SMB scans across different internal subnets. Next, to establish long-term access, the renamed SoftEther VPN executable “bridge.exe” was uploaded into the default Windows System32 directory, which reduced the chances of detection. The malicious SOE also provided ongoing access, and given that it was on the ArcGIS server for an extended period, it was stored in the victim’s backups as well.

Who is at risk?

In the first documented case confirmed by ArcGIS, where the malicious SOE was used, ReliaQuest identified that the password for the ArcGIS portal administrator account was a leet password of unknown origin, suggesting that the attacker had access to the administrative account and was able to reset the password.

“Any organization that uses ArcGIS in a networked environment, if it is exposed externally or to other enterprise data systems, is at risk,” said Devroop Dhar, co-founder and MD at Primus Partners. “The main risk is that attackers can use a compromised extension to maintain access and take out sensitive data. As ArcGIS is widely used in mapping, logistics, and public-sector planning, the data it has can be sensitive, like network maps, population records, and infrastructure layouts.”

As a result, for most enterprises, the concern is not just immediate disruption but also silent observation. If an attacker sits inside a system that tracks infrastructure or logistics, that is a serious intelligence advantage.

“To verify if compromised, organizations should start by taking a complete inventory of all ArcGIS Server versions in their environment and enumerating every Server Object Extension (SOE) and Server Object Interceptor (SOI) in use,” said Amit Jaju, senior managing director – India at Ankura Consulting. “Then they should compare these against known source and vendor hash values to detect unauthorized changes. Conduct a detailed hunt for any anomalous SOE JAR files or class structures, hardcoded tokens or encryption keys, suspicious admin activity logs, and web shell indicators identified by security researchers.”

Jaju added that CISOs should not overlook backups or AMIs, and verify that they aren’t seeded with malicious SOEs and confirm the integrity of your golden images.

For remediation, immediately isolate affected ArcGIS servers, rotate all related service accounts and secrets, and apply strict least-privilege controls to ArcGIS service identities. “Rebuild compromised systems only from known-good media, redeploying extensions that are both signed and independently reviewed. Where possible, enforce code-signing validation for all SOEs to prevent tampering. Finally, strengthen your monitoring posture, add detections specifically for SOE abuse and abnormal ArcGIS administrative endpoint activity, and diversify your threat intelligence sources by subscribing to multiple feeds rather than relying solely on KEV,” added Jaju.

Trusted software is the new attack surface

Security analysts say that the Flax Typhoon case highlights a worrying evolution in the weaponization of trusted components rather than the deployment of conventional malware.

In 2023, the same group targeted dozens of organizations in Taiwan with the likely intention of performing espionage, reported Microsoft. In 2020, SolarWinds was targeted by hackers. They deployed malicious code into SolarWinds Orion IT monitoring and management software that was used by thousands of enterprises and government agencies worldwide.

In March 2023, 3CX suffered a serious software supply-chain compromise that resulted in both its Windows and macOS applications being poisoned with malicious code.

According to experts, threat actors have realized that compromising a trusted vendor module gives them free access. As a result, vendor software should not be treated as safe by default. “Trusted platforms also need continuous verification. Regular code-integrity checks, tighter monitoring of vendor updates, and periodic pen testing of integrated systems are essential,” added Dhar.

CISOs should also push vendors to provide transparency and clarity, like SBOMs (Software Bills of Materials), details of their own security testing and disclosure protocols, Dhar said. “It is also important to separate privileges; just because a module comes from a trusted vendor does not mean it needs access to everything in the network.”

Using AI efficiently to real-time monitor any anomaly in behavioral analytics, comparing with a longish history rather than a slice in time is critical added Shah.