IMPORTANT CYBERSECURITY NEWS: Lazarus Breaches IIS Servers With Web Shells & Evolving C2 Tactics

Vairav Cyber Security News Report

Date: March 14th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

The North Korean threat actor known as the Lazarus Group has been identified exploiting Windows web servers running Internet Information Services (IIS) to establish command-and-control (C2) infrastructures. By deploying ASP-based web shells and evolving their C2 tactics, they leverage compromised servers as proxies for further attacks. This advancement underscores the group's persistent efforts to maintain covert operations and poses significant risks to organizations utilizing IIS servers.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Lazarus Group has been breaching Windows IIS servers to deploy web shells, specifically the "RedHat Hacker" variant, facilitating unauthorized remote access and control. They further install malware such as "LazarLoader" to download and execute additional payloads in-memory, enhancing their attack capabilities.

Identification: Researchers at the AhnLab Security Intelligence Center (ASEC) uncovered this multi-stage attack chain, noting the deployment of web shells and the use of privilege escalation tools.

Affected Entities/Industries: Organizations operating Windows IIS servers are primarily targeted, with potential implications across various industries relying on this technology.

Potential Impact: Risks include unauthorized data access, operational disruptions, financial losses, and reputational damage due to the covert nature of the attacks and the potential for further exploitation.

Exploitation Methods: The group employs ASP-based web shells for initial access, utilizes "LazarLoader" malware for downloading additional payloads, and leverages privilege escalation tools to maintain persistence and control within compromised systems.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Scan IIS servers for unauthorized web shells and remove any found.
- Update and patch IIS servers to the latest security standards.
- Monitor network traffic for unusual activities indicating potential C2 communications.

Security Best Practices

- Implement multi-factor authentication (MFA) for administrative access.
- Regularly review and update firewall and security configurations.
- Conduct routine security assessments and penetration testing.

For Advanced Security Teams

- Deploy intrusion detection and prevention systems (IDPS) to identify and block malicious activities.
- Analyze logs for indicators of compromise (IOCs) related to Lazarus Group tactics.
- Engage in threat hunting activities focusing on APT behaviors.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://securityonline.info/lazarus-breaches-iis-web-shells-evolving-c2-tactics-unveiled/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com