Lazarus Hackers Exploiting IIS Servers: How to Protect Your Organization

March 14, 2025

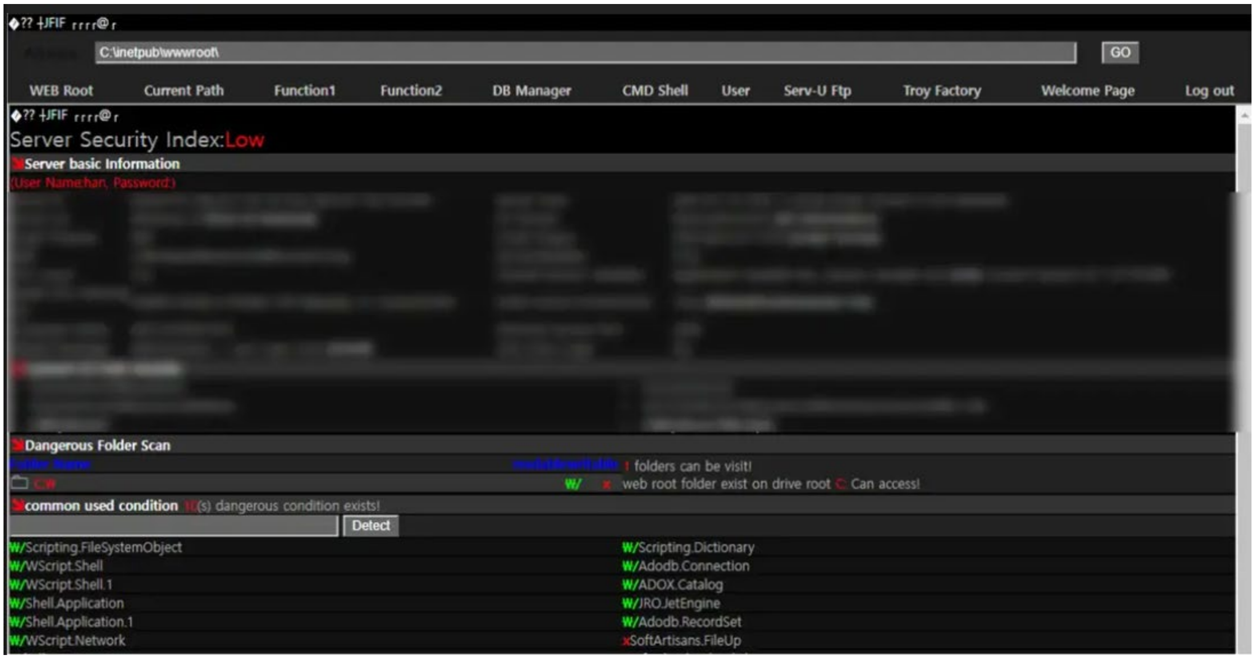
Overview

The Lazarus Group, a notorious state-sponsored hacking collective, is once again making headlines with their latest campaign targeting South Korean web servers. By breaching Microsoft IIS servers, these cybercriminals deploy ASP-based web shells to establish initial command and control (C2) infrastructure, making it easier to orchestrate sophisticated attacks. These incidents, first identified in January 2025, signal a dangerous evolution of techniques previously observed in mid-2024.

For businesses and cybersecurity professionals, this attack wave is a stark reminder of the growing need for robust defense strategies. At Blackswan Cybersecurity, we specialize in proactive threat intelligence and advanced security solutions designed to detect, mitigate, and prevent threats like these before they compromise critical assets.

Understanding the Lazarus Attack Chain

Lazarus has a consistent history of leveraging compromised legitimate web servers to establish their attack framework. In the latest wave of attacks, researchers at AhnLab Security Intelligence Center (ASEC) found that the hackers installed multiple ASP-based web shells on vulnerable IIS servers. These include a modified version of the "RedHat Hacker" web shell, along with additional malicious scripts like "file_uploader_ok.asp" and "find_pwd.asp." These tools grant attackers extensive capabilities, such as file manipulation, process control, and even SQL query execution.



```
�?? +JFIF rrrr@r
C:\inetpub\wwwroot\
�?? +JFIF rrrr@r
Server Security Index:Low
Server basic Information
(User Name:han, Password:)
Dangerous Folder Scan
1 folders can be visit!
C:\                W/  x  web root folder exist on drive root C: Can access!
common used condition 10(s) dangerous condition exists!
W/Scripting.FileSystemObject        W/Scripting.Dictionary
W/WScript.Shell                     W/Adodb.Connection
W/WScript.Shell.1                   W/ADOX.Catalog
W/Shell.Application                 W/JRO.JetEngine
W/Shell.Application.1               W/Adodb.RecordSet
W/WScript.Network                   xSoftArtisans.FileUp
```

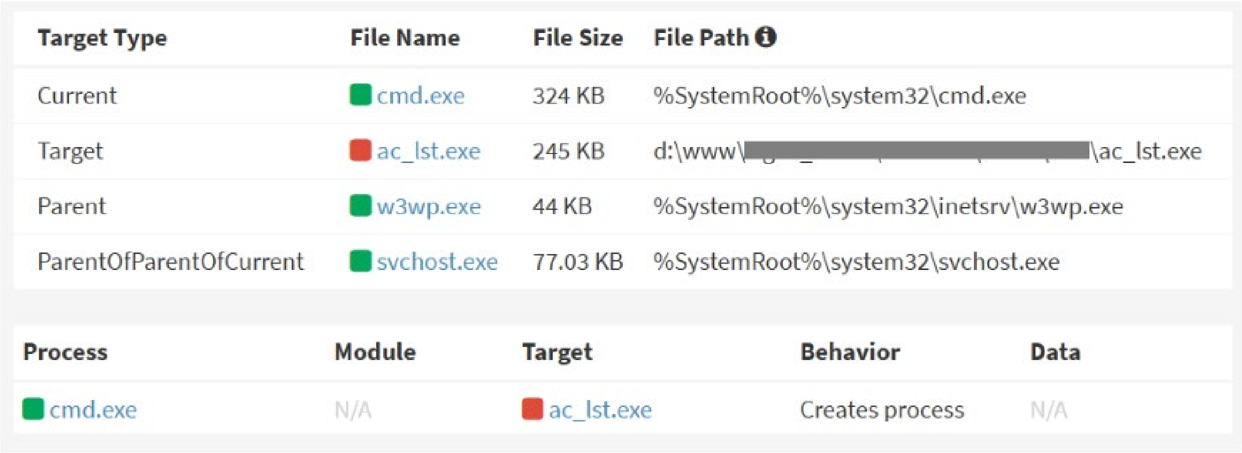
FIGURE 1. REDHAT HACKER WEB SHELL

These web shells employ advanced obfuscation techniques, making them difficult to detect and analyze. A key feature of their malicious scripts includes encryption mechanisms that verify initialization packets and obscure critical command execution paths. This increasing level of sophistication highlights the persistent and adaptive nature of the Lazarus Group's operations.

How Lazarus Deploys Its Malware

Beyond web shells, the attackers also deploy LazarLoader malware, which is specifically designed to download and execute additional payloads in memory using advanced encryption techniques. Their infection chain follows a structured process:

1. **Web Shell Installation** – Malicious ASP-based scripts are uploaded to vulnerable IIS servers.
2. **Malware Deployment** – LazarLoader is executed via the IIS web server process (w3wp.exe), allowing attackers to maintain stealth and persistence.
3. **Privilege Escalation** – A sophisticated malware component named “sup.etl” enables User Account Control (UAC) bypass to escalate privileges and execute malicious commands.



Target Type	File Name	File Size	File Path
Current	🟩 cmd.exe	324 KB	%SystemRoot%\system32\cmd.exe
Target	🟥 ac_lst.exe	245 KB	d:\www\[redacted]\ac_lst.exe
Parent	🟩 w3wp.exe	44 KB	%SystemRoot%\system32\inetsrv\w3wp.exe
ParentOfParentOfCurrent	🟩 svchost.exe	77.03 KB	%SystemRoot%\system32\svchost.exe

Process	Module	Target	Behavior	Data
🟩 cmd.exe	N/A	🟥 ac_lst.exe	Creates process	N/A

FIGURE 2. INSTALLATION LOG OF LAZARLOADER

Protecting Your Organization from IIS Server Exploits

With Lazarus continuously refining its tactics, organizations must take a proactive approach to security. Here’s how Blackswan Cybersecurity can help:

1. Proactive Threat Hunting & Incident Response

Powered by our North Texas-based Cyber Fusion Center, Blackswan’s advanced threat detection and incident response teams continuously monitor the evolving threat landscape, ensuring early identification of malicious activity. We deploy cutting-edge behavioral analytics to spot anomalous behavior that could indicate an ongoing compromise.

2. Secure Web Server Configurations

Properly securing IIS servers is crucial in preventing unauthorized access. Blackswan Cybersecurity helps businesses implement:

- Regular vulnerability assessments and penetration testing
- Strict access controls and multi-factor authentication (MFA)
- Secure coding practices to prevent file upload vulnerabilities

3. Advanced Endpoint & Network Protection

With Lazarus leveraging sophisticated obfuscation techniques, traditional security solutions may fall short. Blackswan provides:

- AI-powered malware detection and response
- Next-gen endpoint protection with real-time threat analysis
- Deception technology to detect and mitigate hidden threats

4. Employee Training & Awareness

Human error remains a significant factor in cyber breaches. Our security awareness training programs equip employees with the knowledge to recognize social engineering attacks and prevent accidental security lapses.

5. Continuous Monitoring & Threat Intelligence

Blackswan Cybersecurity integrates 24/7 security monitoring with advanced threat intelligence feeds to detect Lazarus group indicators of compromise (IOCs). Our threat intelligence teams provide real-time alerts on emerging threats, ensuring your organization stays ahead of cyber adversaries.

Indicators of Compromise

- 0620fa617bc9ef32b93adcf40fe291a4
- 0734a2c3e827ccf558daf48290d06d8c
- 41ffc15c24259156db000af297c71703
- 89921e5f39407a5e63df013468181991
- adabf920682fac1e6a81e655b1182590

File Detection

- Trojan/ASP.Proxy.SC198862 (2025.01.16.02)
- WebShell/ASP.Generic (2025.01.20.02)
- WebShell/ASP.Generic (2025.01.20.02)
- WebShell/ASP.Generic (2025.01.17.01)
- Trojan/Win.LazarLoader.C5730315 (2025.02.14.03)
- Trojan/Win.LazarLoader.R692195 (2025.02.14.03)
- Trojan/Win.UACMe.R455616 (2021.12.28.00)

Conclusion

The Lazarus Group's latest attacks serve as a reminder that no organization is immune to advanced cyber threats. By leveraging proactive security measures, organizations can defend against persistent threat actors targeting critical infrastructure.

Blackswan Cybersecurity is committed to safeguarding businesses from state-sponsored attacks with tailored cybersecurity solutions that offer real-time threat mitigation and comprehensive defense strategies.

Is your organization secure? Contact Blackswan Cybersecurity discuss, or take our free vulnerability assessment to better understand your current security posture and stay one step ahead of cybercriminals.

References

1. https://securityonline.info/lazarus-breaches-iis-web-shells-evolving-c2-tactics-unveiled/
2. https://cybersecuritynews.com/lazarus-hackers-exploiting-iis-servers/
3. https://asec.ahnlab.com/en/86687/