

UAT-10147 AI-Assisted exploitation of internet-facing web servers

Original report published on: August 20, 2026^[1]

Executive Summary

Cisco Talos reported that UAT-10147, a financially motivated threat actor, targets vulnerable Windows and Linux web servers globally including organisations in the media, government, education, technology and gaming sectors.

Active since early 2026, UAT-10147 exploits known vulnerabilities in internet-facing systems to gain remote code execution (RCE) before deploying web shells, backdoors and malware for persistence, reconnaissance, search engine optimisation (SEO) fraud and data theft.

Notably, the threat actor integrates AI-driven tools into its offensive operations, including DeepAudit^[2] for source code vulnerability scanning and PentestGPT^[3] for scanning web servers and executing relevant proof-of-concept exploits. The actor also uses AI-assisted workflows with the ysoserial^[4] framework to generate malicious payloads, validate exploits, troubleshoot issues and support post-compromise activities.

Background

UAT-10147 scans internet-facing web servers for known vulnerabilities, including CVE-2022-27925 (Zimbra Collaboration Suite), CVE-2021-23758 (AjaxPro), CVE-2021-29441 and CVE-2021-29442 (Alibaba Nacos), and CVE-2019-18935 (Progress Telerik UI). The threat actor also exploits multiple Linux local privilege escalation vulnerabilities to obtain root access.

On Windows systems, UAT-10147 uses open-source tools such as EfsPotato (renamed as prcc1.rar) to escalate privileges, modifies Windows Defender exclusions and deploys malware including BadIIS, QuasarRAT, Gh0stCringe and SPECTRE. The threat actor also creates scheduled tasks and privileged local accounts to maintain persistent access. On Linux systems, UAT-10147 exploits known privilege escalation vulnerabilities before deploying NoodleRAT, SPECTRE and Meterpreter.

UAT-10147 was also observed using AI-enabled tools, including DeepAudit and PentestGPT to support vulnerability scanning and exploitation. AI-generated scripts were used to validate ASP.NET ViewState RCE, identify writable directories, deploy the SPECTRE implant and web shells, conduct reconnaissance and exfiltrate information through HTTP callbacks.

Cisco Talos identified a target list containing approximately 170,000 URLs, indicating the threat actor's intent to conduct exploitation at scale. Talos also identified compromised servers located in Brazil, Bolivia, China, Canada and Vietnam.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the UAT-10147 activity identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities ([Annex A](#)).
- Refer to the MITRE ATT&CK techniques in this advisory ([Annex B](#)):

- Create, test and validate detection rules against the threat behaviours.
- Validate and deny/disable processes, ports and protocols that have no business need.
- Identify and apply relevant vendor security updates, prioritising Internet-facing systems.
- Implement continuous threat exposure management to identify exposed services, security risks, misconfigurations and vulnerabilities across web servers and other internet-facing systems, and remediate identified issues.
- Monitor for suspicious use of PowerShell, certutil, curl and appcmd.exe, particularly for payload downloads, encoded commands, reconnaissance and outbound callbacks.
- Consider using approved AI-assisted security tools to identify vulnerabilities and support remediation, subject to appropriate security testing and risk assessment.
- Monitor for suspicious or newly created scheduled tasks and privileged local accounts, including accounts added to the Administrators or Remote Desktop Users groups.
- Review Windows Defender exclusions and investigate unauthorised exclusions, particularly those involving IIS directories.
- Monitor IIS web directories for unauthorised ASHX web shells, DLLs and other executable content.
- Ensure ASP.NET MachineKey values are securely generated and protected, and rotate them where compromise or exposure is suspected.
- Enforce least privilege for IIS application pools and monitor for abuse of privileges such as SeImpersonatePrivilege.
- Deploy EDR/XDR coverage across Internet-facing systems and monitor for privilege escalation tools, web shells and malware associated with the campaign.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

URL	Description
https[:]//adminapi[.]tippusoni[.]in/4/pr[.]exe	Malicious URLs associated with the campaign
https[:]//adminapi[.]tippusoni[.]in/4/prcc2[.]txt	
https[:]//adminapi[.]tippusoni[.]in/4/prcc2[.]rar	
https[:]//adminapi[.]tippusoni[.]in/4/dll[.]zip	
https[:]//adminapi[.]tippusoni[.]in/4/user[.]txt	
https[:]//adminapi[.]tippusoni[.]in/4/back[.]txt	
https[:]//adminapi[.]tippusoni[.]in/4/bai[.]txt	
https[:]//adminapi[.]tippusoni[.]in/4/svchosts[.]exe	
https[:]//adminapi[.]tippusoni[.]in/5/pr[.]exe	
https[:]//adminapi[.]tippusoni[.]in/5/bai[.]txt	
https[:]//adminapi[.]tippusoni[.]in/5/svchosts[.]exe	
https[:]//kl21177[.]com/1/prcc1[.]rar	
https[:]//kl21177[.]com/1/dll[.]zip	
https[:]//kl21177[.]com/1/user[.]bat	
http[:]//139[.]180[.]197[.]150:54321/4/pr[.]exe	
http[:]//139[.]180[.]197[.]150:54321/4/bai[.]txt	
http[:]//139[.]180[.]197[.]150:54321/4/svchosts[.]exe	

SHA256 Hash	Description
175e83adc721cd7d634ebd2c63fb8d2404c009067bc7719ef02c5d1f9d81e9a1	Malicious file associated with UAT-10147 activity.
1f0496ad392b5b9edf9e59a56af4d8e17638ddbb12e086f104d9a0f316ad59a1	
37cab04da36e710dd4aee8609ab7553c039a54dd085460854e9ddb49b0e7032	
50232092004b9ad335e1e72e3a6dcfde93c4470007ddfcc637e6e5f899f68be0	
73b272612cec9e03a7e2f7516ece600fb1b45b719fa9d93b382ed25ec314e5c0	
9fa27b231502d6d33441ab54227da50cbd325847ce2272f9c0e79b4ea873e432	

cfce59111338701b2990be9aad80166ac0618cb57483d6a065f1e2526a34494	
fbe9c6052d7261bd252322e155d86bd370340f1fbb2b0a1e9c7b444f6275614a	
00892f276299a13721642e8a9bcbcb949a658547c6c8271866a1997b79f1e5c5	
23a83c6bbdd7d6c09a5187338065d15f2a90a252772813cba83b9818aa56cef7	
8280502c2c6902e61fc4c02a9a81b4720688449a5bca3d89dbd1e2edd507c69a	
d190b349d791267a9583ba9f4a1ab0e4199d1a3abfd4dae514ed5def0754ba94	

IP Address	Description
139[.]180[.]197[.]150	threat actor open-directory download/staging server; web shell fallback host (port 54321)
18[.]140[.]163[.]186	Associated with UAT-10147 activity.

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
	T1136.001	Create Account: Local Account
	T1505.003	Server Software Component: Web Shell
Privilege Escalation	T1068	Exploitation for Privilege Escalation
	T1134	Access Token Manipulation
Defence Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
	T1070.004	Indicator Removal: File Deletion
Discovery	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1016	System Network Configuration Discovery
Command and Control	T1105	Ingress Tool Transfer
	T1219	Remote Access Software
Exfiltration	T1041	Exfiltration Over C2 Channel
	T1567	Exfiltration Over Web Service

References

1. [UAT-10147: Chinese-speaking adversary integrates agentic AI into post-compromise operations](#)
2. [DeepAudit: Open-source, multi-agent AI tool for source-code vulnerability analysis and validation](#)
3. [PentestGPT: LLM-powered penetration testing framework that automates scanning, vulnerability analysis and exploitation](#)
4. [ysoserial: Open-source tool for generating Java deserialization payloads, used with AI-generated exploitation workflow](#)