16 November 2026

TLP: WHITE

EMERGING THREATS

Weaponization of the ARTEX Penetration Testing Tool

ARTEX is an open-source, AI-driven offensive framework originally observed in July 2026 that has been increasingly weaponized by financially motivated and espionage-oriented threat actors. Since August 2026, ARTEX has been observed targeting organizations across the United States, Europe, and Asia, including South Korea, with affected industries spanning financial services, government, technology, defense, healthcare, manufacturing, telecommunications, and energy. Unlike traditional intrusion frameworks, ARTEX utilizes multiple AI agents to automate reconnaissance, exploitation, privilege escalation, and post-compromise activity with limited human interaction. Furthermore, researchers have linked ARTEX-enabled operations to significant data theft, including the exposure of approximately 67,000 individuals' personal information at South Korean financial institutions and a supply chain compromise affecting more than 2,250 ConnectWise Cloud Backup tenants.

THREAT SUMMARY

ARTEX is an open-source, AI-driven offensive framework originally observed in July 2026 that has been increasingly weaponized by financially motivated and espionage-oriented threat actors. Since August 2026, ARTEX has been observed targeting organizations across the United States, Europe, and Asia, including South Korea, with affected industries spanning financial services, government, technology, defense, healthcare, manufacturing, telecommunications, and energy. Unlike traditional intrusion frameworks, ARTEX utilizes multiple AI agents to automate reconnaissance, exploitation, privilege escalation, and post-compromise activity with limited human interaction. Furthermore, researchers have linked ARTEX-enabled operations to significant data theft, including the exposure of approximately 67,000 individuals' personal information at South Korean financial institutions and a supply chain compromise affecting more than 2,250 ConnectWise Cloud Backup tenants.

Over the past several months, ARTEX has evolved from a publicly available penetration testing framework into an offensive platform capable of conducting complex intrusions at machine speed. Although its original GitHub repository was removed in October 2026, the framework continues to circulate through modified variants, community forks, and a commercial offering known as ARTEX PRO. It is worthy to note that ARTEX can rapidly identify attack paths, adapt to failed exploitation attempts, and progress from compromised credentials to privileged access. These capabilities allow malicious actors to compromise cloud infrastructure, abuse trusted relationships, steal credentials, deploy web shells, and exfiltrate sensitive information, significantly increasing the speed and scale of enterprise intrusions.

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

THREAT SYNOPSIS

At the outset, ARTEX has been observed leveraging compromised credentials, vulnerable internet-facing applications, and exposed administrative interfaces to establish initial access. The Go-based framework incorporates a Next.js web console and six specialized AI agents that utilize large language models to automate exploitation and post-compromise operations. Researchers observed ARTEX exploiting SQL injection, server-side request forgery (SSRF), authentication weaknesses, and exposed APIs to compromise applications and cloud infrastructure. During reconnaissance, the framework enumerates Azure service principals, AWS IAM permissions, storage account keys, and Active Directory resources to identify additional attack paths. In one instance, ARTEX manipulated MySQL logging configurations through an exposed SQL API to write malicious .jsp web shells, automatically modifying its payloads following execution failures. Additionally, the framework has abused Azure Kudu administrative APIs to execute commands and stage PowerShell, Python, and C# scripts.

Following initial compromise, ARTEX automates privilege escalation, lateral movement, persistence, and data collection across compromised environments. Researchers observed PowerShell-based Active Directory reconnaissance, Kerberoasting, DCSync operations targeting the krbtgt account, and lateral movement attempts through WinRM, Pass-the-Hash, and Pass-the-Ticket techniques. Then for persistence and remote access, ARTEX has deployed PHP and JSP web shells, created unauthorized administrator accounts and SSH keys, and utilized tools such as WISP, vshell, and AdaptixC2. The framework also leverages curl, rotating webhook.site endpoints, and tunneling utilities such as Chisel and SoftEther to retrieve payloads, transmit command output, and facilitate communications. Subsequent activity includes accessing SQL databases, collecting credentials, and enumerating cloud storage and snapshots for potential exfiltration. Its ability to execute automated attack sequences within seconds significantly reduces the time available for defenders to identify and respond to malicious activity.

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

ARTEX HUNT COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('546ceb3c-e8ae-4372-8062-e9bac8d47021'),touched:!t)

https://verity.intel471.com/hunt/research/search?state=(community:!f,compatible:!f,filters:(),lastUpdated:!n,library:!(cyborg_collections),page:0,size:10,sort:relevance,term:!(%27546ceb3c-e8ae-4372-8062-e9bac8d47021%27),touched:!t)

RELATED HUNT PACKAGES

Production Snapshot Cloning to Unauthorized Instances

https://hunter.cyborgsecurity.io/research/hunt-package/0c9e0bfa-37a9-47ac-8ce0-82bc1902017d

https://verity.intel471.com/hunt/research/hunt-package/0c9e0bfa-37a9-47ac-8ce0-82bc1902017d

HTTP GET Request to jsp File Containing Command Strings in URI - Potential WebShell/Exploitation

https://hunter.cyborgsecurity.io/research/hunt-package/de91ffa1-c4b9-4dab-a881-235ff3de0c3f

https://verity.intel471.com/hunt/research/hunt-package/de91ffa1-c4b9-4dab-a881-235ff3de0c3f

ActiveDirectory PowerShell Module Cmdlet Usage - Potential Active Directory Discovery Commands

https://hunter.cyborgsecurity.io/research/hunt-package/ED9E131D-3495-44F4-A594-4C06CDE87779

https://verity.intel471.com/hunt/research/hunt-package/ED9E131D-3495-44F4-A594-4C06CDE87779

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

Suspicious Curl Usage for Remote File Retrieval - Payload Delivery Technique

https://hunter.cyborgsecurity.io/research/hunt-package/a5d83f68-d233-4f33-b97e-1df2f5e0d192

https://verity.intel471.com/hunt/research/hunt-package/a5d83f68-d233-4f33-b97e-1df2f5e0d192

Suspicious SOCKS Proxy Process Creation

https://hunter.cyborgsecurity.io/research/hunt-package/e1650196-ebc1-4dee-a65e-2fcaacf5255e

https://verity.intel471.com/hunt/research/hunt-package/e1650196-ebc1-4dee-a65e-2fcaacf5255e

AWS General Discovery Activity

https://hunter.cyborgsecurity.io/research/hunt-package/e58d5a8d-1b7a-42f7-97b4-e750ea97027c

https://verity.intel471.com/hunt/research/hunt-package/e58d5a8d-1b7a-42f7-97b4-e750ea97027c

Cloud Metadata Service Discovery - Command Line Telemetry

https://hunter.cyborgsecurity.io/research/hunt-package/a33dabe7-6e16-4e3e-be72-d9ba121ec60a

https://verity.intel471.com/hunt/research/hunt-package/a33dabe7-6e16-4e3e-be72-d9ba121ec60a

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

MITRE CONTEXT

- MITRE Technique IDs:
  - T1190
  - T1578.001
  - T1016
  - T1201
  - T1087.002
  - T1578.002
  - T1090.003
  - T1202
  - T1526
  - T1105
  - T1087.004
  - T1552.005
  - T1572
  - T1580
  - T1482
  - T1059.001
  - T1082

- MITRE Technique Names:
  - Multi-hop Proxy
  - Cloud Infrastructure Discovery
  - System Information Discovery
  - Indirect Command Execution
  - Cloud Account
  - System Network Configuration Discovery
  - Ingress Tool Transfer
  - Protocol Tunneling
  - Domain Trust Discovery
  - Cloud Instance Metadata API
  - Exploit Public-Facing Application
  - Create Snapshot
  - Create Cloud Instance

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

    - Password Policy Discovery
    - Domain Account
    - PowerShell
    - Cloud Service Discovery

- MITRE Tactic Names:
    - Execution
    - Command and Control
    - Initial Access
    - Credential Access
    - Discovery
    - Defense Evasion

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

REFERENCES

1. https://blog.malwaremustdie.org/2026/11/mmd-072-2026-artex-detection-signature.html?m=1
2. https://www.bleepingcomputer.com/news/security/fbi-warns-artex-ai-hacking-tool-is-powering-global-cyberattacks/
3. https://www.ic3.gov/CSA/2026/261113.pdf
4. https://cloud.google.com/blog/topics/threat-intelligence/artex-and-friends-enter-agentic-offensive-frameworks
5. https://blog.talosintelligence.com/artex-and-beyond/

STAY AHEAD OF THE THREAT

Looking to hunt these threats yourself? Join the HUNTER Community for free and get access to behavioral threat hunting content for your SIEM, EDR, NDR, and XDR platforms.

Get Your Free HUNTER Community Account

Copyright © 2026 Intel 471, Inc. All Rights Reserved.