

English

Threat Research Center   Threat Research   **Cloud Cybersecurity Research**

CLOUD CYBERSECURITY RESEARCH

# The Evolution of Linux Binaries in Targeted Cloud Operations

8 min read

RELATED PRODUCTS



Cortex



Cortex Cloud



Unit 42 Incident Response

 **By:** Nathaniel Quist , Bill Batchelor

 **Published:** June 10, 2025

 **Categories:** Cloud Cybersecurity Research , Malware , Threat Research

 **Tags:** Endpoint , Linux Malware , Machine Learning , PowerShell , Remote Access Trojan , VBScript , Winnti

Share 

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie  
Settings**



THREAT RESEARCH CENTER

# Defend with intelligence.

The latest reports, trends and expert insights delivered directly to you.

**SUBSCRIBE NOW**

## Table of Contents

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

Linux OS instances within the standard cloud environment.

Our researchers pinpointed examples of evolving strains of ELF-based malware that include NoodleRAT, Winnti, SSHdInjector, Pygmy Goat and AcidPour. These ELF binaries use techniques such as dynamic linker hijacking, where they abuse the `LD_PRELOAD` environment variable to:

- Inject malicious code into legitimate system processes
- Hook into critical Linux services such as the SSH daemon (`sshd`)
- Exploit vulnerabilities or misconfigurations found in containerized infrastructure

This allows threat actors to achieve persistence, maintain stealthy command and control (C2) channels, covertly exfiltrate data and impact operations by wiping critical data.

## NoodleRAT

This malware enables threat actors to perform C2 operations on a targeted endpoint, including:

- Access via reverse shell
- SOCKS proxy tunneling
- Encryption of communications
- Scheduled code execution
- Uploading and downloading of files
- Process name spoofing

NoodleRAT has both Windows and Linux variants. The **Linux variant** is an ELF-based backdoor. Although Linux NoodleRAT code bears similarities to other Linux backdoor malware, including Rekoobe and Tiny SHell, NoodleRAT is considered its own malware family.

NoodleRAT has been observed in both cybercriminal and cyberespionage intrusions, including from Chinese-speaking threat actors such as **Rocke** and suspected nation-state actors associated with the **Cloud Snooper** campaign. The actors behind the Linux variant of NoodleRAT have targeted entities in multiple countries across the Asia-Pacific region including Thailand, India, Japan, Malaysia and Taiwan.

## Winnti

Winnti has both Windows and Linux versions. This malware achieves persistence through abuse of the `LD_PRELOAD` environment variable, enabling it to load into memory without altering any legitimate system binaries.

The backdoor has the following functionality:

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

The **Linux variant of Winnti** malware is a backdoor reportedly used by several China-nexus threat actors, including those that we track as Starchy Taurus (aka **Winnti** Group and BARIUM) and Nuclear Taurus (aka Tumbleweed Typhoon, THORIUM, **Bronze Vapor**). The backdoor consists of two files: a primary ELF executable (`libxselinuX`) and an additional dynamic library (`libxselinuX.so`).

## SSHdInjector

This **Linux SSH backdoor** injects malicious code into the SSH daemon (`sshd`) at runtime. The injected code grants the threat actor persistent access and facilitates malicious activities such as:

- Credential theft
- Remote command execution
- Malware ingress
- File and directory access
- Opening a remote shell
- Data exfiltration

SSHdInjector has been observed being used by several China-nexus threat actors, including one that we track as **Digging Taurus** (aka Daggerfly, Evasive Panda). **Targets** are cyberespionage-related and have included individuals, government institutions, and telecommunications organizations.

## Pygmy Goat

Pygmy Goat is a Linux backdoor that was **discovered on Sophos XG firewall devices [PDF]** but is designed to target additional Linux-based systems. The malware gains initial access and persistence through rootkit functionality by leveraging the `libsophos.so` library file, which is vulnerable to authentication bypass (**CVE-2022-1040**).

The executable then injects itself into the SSH daemon (`sshd`) using the `LD_PRELOAD` environment variable on the targeted device and intercepts SSH communications. The threat actor can initiate communications with the malware by sending specially crafted ICMP packets — a technique known as “**port knocking**” — or by sending a series of **magic bytes** embedded in SSH traffic.

Its capabilities include:

- Establishing remote shells
- Capturing network packets
- Creating cron jobs
- Tunneling via a reverse SOCKS5 proxy

AcidRain and the newer **AcidPour** variant are strains of destructive Linux wiper malware linked to the Russian threat actor **Razing Ursa** (aka Sandworm, Voodoo Bear). AcidRain is an ELF binary that targets modems and routers that are based on the **MIPS architecture**.

AcidPour is a similar ELF binary but is compiled for x86. It can affect a broader range of targets, such as Linux x86-based storage arrays, network devices and industrial control systems.

Both wipers use Input/Output Controls (IOCTLs) to effect destruction of data and then they self-delete for defense evasion. AcidPour or a new variant of this binary would be effective at wiping unprotected x86-based cloud systems if a threat actor gained shell access, for example via a successful web shell deployment or container escape.

We observed new hash values of these malware families in the months preceding this report. As organizations continue to migrate to the cloud, threat actors will continue to develop these malware families and pivot into cloud runtime environments. This highlights the need for enhanced detection and prevention security capabilities in cloud workloads and containers.

## Conclusion

Cloud-based alerts increased on average 388% during 2024. We predict that threat actors targeting cloud environments will start using more complex tools in their attacks. This includes reworking, improving and tailoring existing tools that historically only targeted Linux OS systems.

Given the estimates previously cited that as many as 90% of cloud environments operate on Linux compute instances, the logical next step is for threat actors to use these malware families against cloud environments.

It is more critical than ever to implement endpoint security agents on cloud computing instances to ensure that all malicious runtime processing, network traffic and suspicious behavioral operations are detected. Modern cloud endpoint agents can detect these malware families. The introduction of machine learning in endpoint detection is a significant advancement in cloud security.

### Palo Alto Networks Protection and Mitigation

We recommend a machine-learning detection approach to flag binaries. An evolving approach should consider factors like:

- Kernel-mode system calls
- Import functions
- Evasion techniques
- Network traffic
- Unknown binary patterns

Figure 1 shows a previously unknown ELF binary that triggered the Cortex Machine Learning alert.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)


 Screenshot of Cortex XDR showing an execution flow. At the top are numerous icons representing a chain of events. At bottom is a table explaining the different processes. These include the Resource, Category, Action, Alert Name and more.

Figure 1. Cortex Cloud ELF Machine Learning execution alert.

## ELF Machine Learning Detections

**Palo Alto Networks Cortex Cloud** has developed a new machine learning module specifically to detect Linux ELF files. Cortex researchers conducted tests using over 100 unique ELF binaries across all five of the malware families discussed in this article. Each malware family was successfully detected, and 92% of all samples were accurately flagged as malicious.

The remaining 8% were found to contain Linux shared (.so) libraries that were out of scope for the model used.

The files that were detected fell within the following testing criteria:

Malicious

Suspicious

Benign

Samples that received a score of 0.85 or above are categorized as malicious, results between 0.84 and 0.65 are considered suspicious and any result below 0.64 is considered benign.

Figure 2 shows that 61% of the samples tested had results above 0.85 and were considered malicious.


 Pie chart of the machine learning testing scores showing the distribution as: 61.5% malicious, 30.8% suspicious, and 7.7% benign.

Figure 2. ELF machine learning testing scores by percentage of benign, suspicious or malicious.

92.3% of all samples submitted surpassed the suspicious threshold of 0.65. This demonstrates that all but 7.7% of the samples provided are considered suspicious and would trigger an alert if they were executed within the environment.

## PowerShell and VBS Machine Learning Detections

We also used the Cortex PowerShell and VBS Machine Learning module to investigate the detection of cloud-specific operations. We submitted over 100 PowerShell and Visual Basic scripts (VBS) to the ML model. These scripts were hand picked as malicious scripts that performed the following activities:

- Cloud resource discovery and creation
- Storage container object deletion and exfiltration
- Identity access and management (IAM) operations

Figure 3 shows that 67% of these scripts were successfully identified as malicious or suspicious. Notably, nearly 96% of the malicious samples received a score of 0.95 or higher.


 Pie chart of the PowerShell and VBS machine learning testing scores as: 56.8% Malicious (>95%), 33.0% Benign, 8.0% Suspicious, and 2.3% Malicious.

Figure 3. PowerShell and VBS Machine Learning testing scores by percentage of benign, suspicious or malicious.

## Cortex Cloud

Defenders can gain valuable insights by threat hunting for common ELF malware executions within cloud endpoints. This can be done through cloud detection and response (CDR), which is a cloud security solution that combines:

- Endpoint detection and response (EDR) capabilities
- Detection and prevention of executable processes running on cloud endpoints
- Auditing and logging capabilities inherent within the cloud service platform

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Cortex ELF Machine Learning detection module
- Cortex PowerShell and VBS Machine Learning detection module

If you think you may have been compromised or have an urgent matter, get in touch with the **Unit 42 Incident Response team** or call:

North America: Toll Free: +1 (866) 486-4842 (866-4-UNIT42)

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)



Australia: +61.2.4062.7950

India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

## Additional Resources

Several sources were used to support and guide this research:

[Cloud Threats on the Rise](#) – Unit 42, Palo Alto Networks

[2024 State of the Cloud Report](#) – Unit 42, Palo Alto Networks

[AcidPour Wiper Malware: Threat Analysis and Detections](#) – Splunk, CISCO

[AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine](#) – SentinelLABS, SentinelOne

[Malware Analysis Report: Pygmy Goat \[PDF\]](#) – Nation Cyber Security Centre

[Analyzing ELF/Sshdinjector.A!tr with a Human and Artificial Analyst](#) – Fortinet

[Noodle RAT: Reviewing the Backdoor Used by Chinese-Speaking Groups](#) – Trend Micro

[RevivalStone: Winnti Group](#) – LAC's Cyber Emergency Center

[Back to top](#)

### TAGS

Endpoint

Linux Malware

Machine Learning

PowerShell

Remote Access Trojan

VBScript

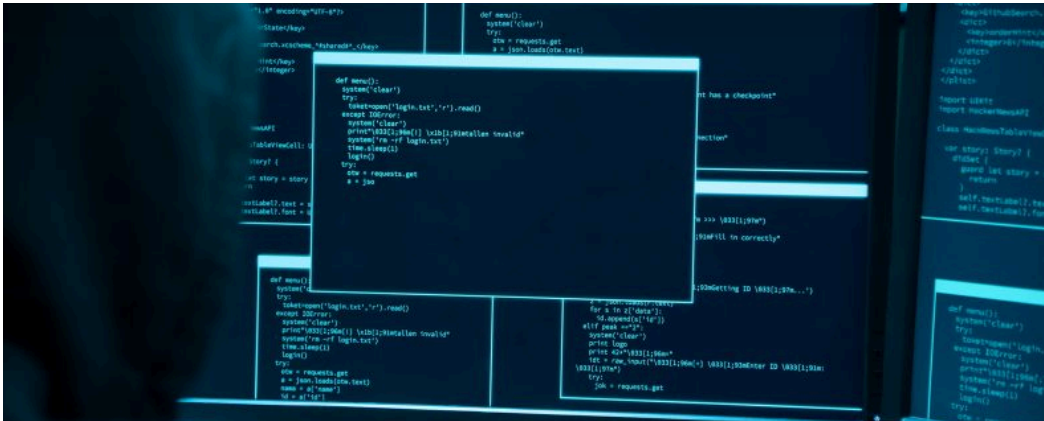
Winnti

Threat Research Center

Next: Roles Here? Roles There? Roles Anywhere:  
Exploring the Security of AWS IAM Roles Anywhere

## Related Resources

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)



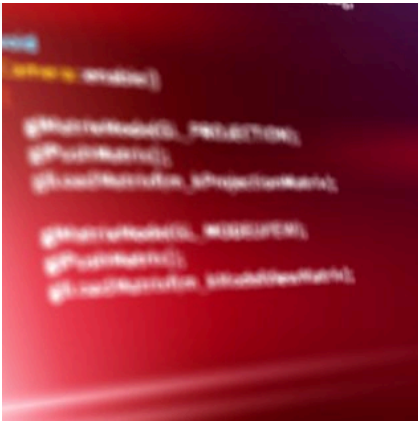
THREAT RESEARCH

June 20, 2025

Resurgence of the Prometei Botnet

Botnet   Cryptominers   Linux

[Read now](#)



THREAT RESEARCH

June 17, 2025

Exploring a New KimJongF Implementation

PowerShell   Infostealer

[Read now](#)

Newsletter



UNIT 42  
Get updates from Unit 42  
Small  
Log

Peace of mind comes from staying ahead of threats. Subscribe today.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

Subscribe



## Products and Services

## Company

## Popular Links



Privacy

Trust Center

Terms of Use

Documents

Copyright © 2025 Palo Alto Networks. All Rights Reserved



EN

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)