Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

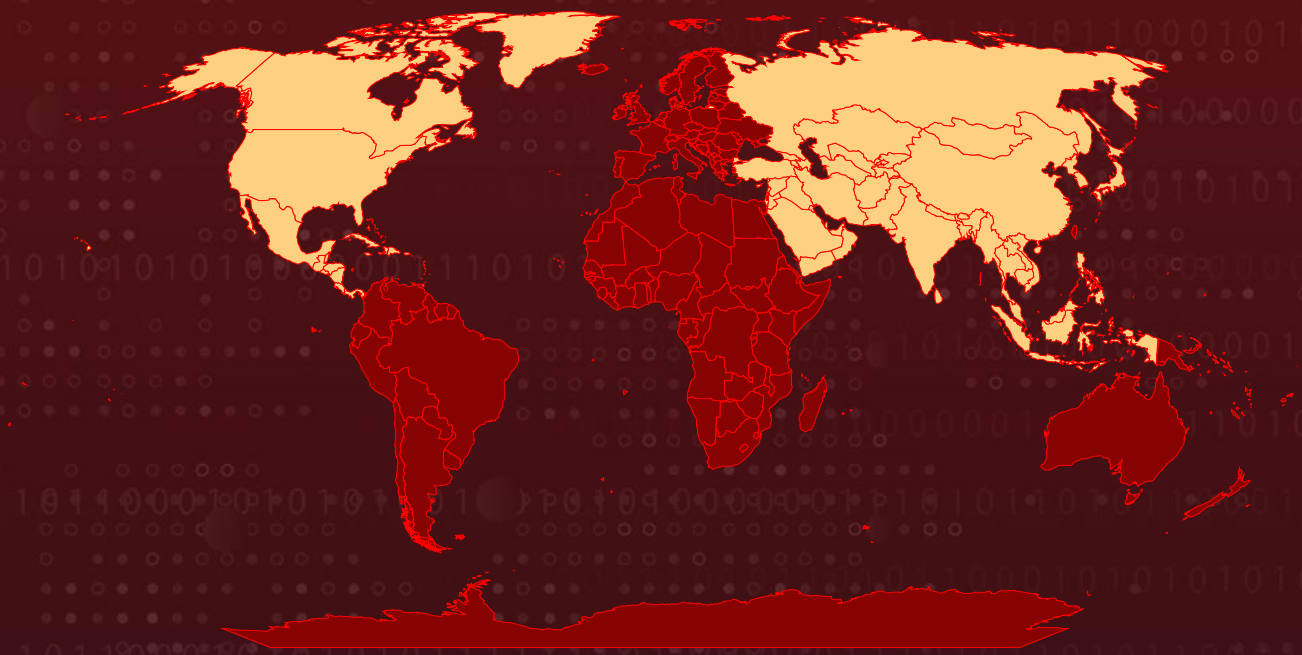
Auto-Color: The Stealthy Linux Malware Lurking in the Shadows

Date of Publication	Last Update Date	Admiralty Code	TA Number
February 27, 2025	July 30, 2025	A1	TA2025060

Summary

Attack Discovered: November 5, 2024
Targeted Countries: North America and Asia
Affected Industries: Universities, Government Offices, Chemical Industry
Affected Platform: Linux
Malware: Auto-color
Attack: Between early November to December 2024, researchers uncovered a new Linux malware strain named Auto-color, derived from the filename it adopts after installation. This stealthy backdoor is being deployed against educational institutions and public sector organizations in the U.S. and Asia, enabling attackers to maintain persistent access while evading detection and removal. Once embedded, Auto-color grants threat actors' full remote control over compromised systems, making it exceptionally difficult to eliminate without specialized security tools. Its ability to blend into the system and resist deletion highlights the growing sophistication of Linux-targeted threats. More recently, attackers were seen delivering Auto-Color by exploiting a critical SAP NetWeaver flaw (CVE-2025-31324), using it as a quiet entry point into targeted networks.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓

Attack Details

#1 A new Linux malware strain called Auto-color was uncovered, built to infiltrate systems while staying under the radar. This malware disguises itself with harmless-looking filenames, hides its communication with C2 servers, and uses custom encryption to avoid detection. Once installed, it grants attackers full remote access, making it incredibly difficult to remove without specialized tools. Each instance of the malware adopts a different filename to evade traditional security measures. Its execution depends on victims unknowingly running the malicious file, but the exact infection process remains unclear.

#2 When executed, Auto-color checks whether its filename matches "Auto-color." If not, it begins its installation process, embedding a hidden library implant within the executable. If the user lacks root privileges, the malware halts its installation to avoid detection. However, when executed with elevated privileges, it installs a malicious library named which mimics a legitimate system library to stay unnoticed. To establish persistence, the malware modifies a Linux configuration file that forces the system to load specific libraries before others. By doing so, it overrides core system functions and manipulates processes without raising alarms.

#3 Auto-color's malicious library is designed to intercept and manipulate system calls, especially those related to network activity and file access. It hooks into standard Linux functions to hide its operations, ensuring that security tools and administrators cannot easily detect its presence. When an attempt is made to inspect /proc/net/tcp, which logs active network connections, the malware returns fake data to conceal its communication with attackers. Additionally, it protects itself from removal by preventing any modifications to /etc/ld.preload, making cleanup efforts much more challenging.

#4 To communicate with its operators, Auto-color decrypts an embedded list of remote C2 servers. It uses a custom encryption algorithm, dynamically generating keys to extract target addresses. Once a connection is established, the malware performs a handshake by sending a random 16-byte challenge and expecting the server to respond with the same value for verification. After authentication, Auto-color enters an ongoing command loop, waiting for further instructions from the remote server.

#5 Auto-color is a highly evasive and persistent threat capable of maintaining long-term access to infected systems. By hooking into system libraries, disguising network activity, and preventing removal, it ensures attackers retain control over compromised machines. Its ability to establish reverse shell backdoors makes it a serious cyber espionage tool, allowing attackers to steal data, execute remote commands, and sustain access to high-value targets for extended periods.

#6 In a recent attack, the Auto-Color backdoor was deployed by exploiting the critical SAP NetWeaver vulnerability CVE-2025-31324. The attackers specifically targeted the Visual Composer Metadata Uploader component of a U.S.-based chemicals company. This flaw enabled unauthenticated attackers to upload ZIP files containing malicious scripts, which, when executed, downloaded the Auto-Color backdoor disguised as an ELF binary log file. The malware achieved persistence through the ld.so.preload mechanism and adapted its behavior based on privilege level suppressing malicious activity if the command-and-control (C2) server was unreachable to evade detection.

Recommendations

Update Immediately: Update SAP NetWeaver right away to fix the CVE-2025-31324 issue. Don’t wait for your usual patch schedule this update is critical and should be handled as an emergency.

Monitor File Uploads and Execution Activity: Implement logging and alerting for unusual file uploads or ZIP extractions in SAP directories. Watch for execution of scripts or binaries in non-standard locations.

Block Untrusted Programs from Running: Configure Linux systems to prevent the execution of unknown or unverified files, particularly those from untrusted sources. Implement application whitelisting to ensure that only approved software can run, reducing the risk of malware infections.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Safeguard Critical System Files: Continuously monitor /etc/ld.preload and other essential system configurations for unauthorized modifications. Deploy file integrity monitoring (FIM) tools to detect and alert on any unexpected changes, ensuring system security and integrity.

Implement Least Privilege Access: Restrict user accounts to the bare minimum permissions necessary for their tasks. Prevent non-administrative users from installing software or altering critical system files, reducing the risk of malware persistence and unauthorized changes.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**TA0040** Impact	**T1082** System Information Discovery
T1057 Process Discovery	**T1090** Proxy	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1036.005 Match Legitimate Resource Name or Location	**T1083** File and Directory Discovery	**T1070** Indicator Removal	**T1070.004** File Deletion
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1056** Input Capture	**T1056.004** Credential API Hooking
T1049 System Network Connections Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1059** Command and Scripting Interpreter	**T1059.004** Unix Shell
T1562 Impair Defenses	**T1562.012** Disable or Modify Linux Audit System	**T1543** Create or Modify System Process	**T1021** Remote Services
T1485 Data Destruction	**T1588** Obtain Capabilities	**T1588.001** Malware	**T1588.006** Vulnerabilities

T1189 Drive-by Compromise	**T1001** Data Obfuscation	**T1571** Non-Standard Port	**T1048** Exfiltration Over Alternative Protocol
T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol	**T1222** File and Directory Permissions Modification	**T1546** Event Triggered Execution	**T1546.006** LC_LOAD_DYLIB Addition

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43, 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4, 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a633, a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d53d0a, bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f02d6b, e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc3048f7, 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042bb255, bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b051510d1ca
IPv4:Port	146[.]70[.]41[.]178[:]443, 216[.]245[.]184[.]214[:]443, 146[.]70[.]87[.]67[:]443, 65[.]38[.]121[.]64[:]443, 206[.]189[.]149[.]191[:]443
Filenames	exploit.properties, helper.jsp, 0KIF8.jsp, cmd.jsp, test.txt, uid.jsp, vregrewfsf.jsp
IPv4	146[.]70[.]19[.]122, 149[.]78[.]184[.]215, 196[.]251[.]85[.]31,

TYPE	VALUE
IPv4	120[.]231[.]21[.]8, 148[.]135[.]80[.]109, 31[.]222[.]254[.]27, 45[.]32[.]126[.]94, 110[.]42[.]42[.]64, 119[.]187[.]23[.]132, 18[.]166[.]61[.]47, 183[.]2[.]62[.]199, 188[.]166[.]87[.]88, 91[.]193[.]19[.]109, 123[.]146[.]1[.]140, 139[.]59[.]143[.]102, 155[.]94[.]199[.]59, 165[.]227[.]173[.]41, 193[.]149[.]129[.]31, 202[.]189[.]7[.]77, 209[.]38[.]208[.]202, 31[.]222[.]254[.]45, 58[.]19[.]11[.]97, 64[.]227[.]32[.]66

Patch Link

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

References

https://unit42.paloaltonetworks.com/new-linux-backdoor-auto-color/

https://www.darktrace.com/blog/auto-color-backdoor-how-darktrace-thwarted-a-stealthy-linux-intrusion

https://hivepro.com/threat-advisory/critical-cve-2025-31324-flaw-in-sap-netweaver-under-active-attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

February 27, 2025 • 4:20 AM

More at www.hivepro.com