Cyber Threat Advisory

IT ORIGIN



Table Of Contents

- Executive Summary
- ClickFix Malware Loaders: Lorem Ipsum and Axolotl Enable Covert C2 Tunneling
- FortiManager Exploitation and PEERSTITCH Malware Targeting FortiGate Firewalls
- Windows BitLocker Vulnerabilities Could Allow Privilege Escalation and Security Bypass
- Indicator of Compromise
- Annexure

Executive Summary

Tactic Name	Discovery, Execution, Collection, Command and Control, Execution, Defense Evasion, Privilege Escalation, Lateral Movement, Credential Access.
Technique Name	System Information Discovery, File and Directory Discovery, Data from local system, Execution, Native API, Ingress Tool Transfer, Software Deployment Tools.
Attack Type	Vulnerability / APT
Target Application / Server	Generic
Threat Intel IOC	Multiple
Recommendation	Read detailed advisory
Impact	**High**

ClickFix Malware Loaders: Lorem Ipsum and Axolotl Enable Covert C2 Tunneling

Summary: ForescoutVedere Labs published an analysis on October 14, 2026, comparing two Windows malware loaders: Lorem Ipsum Loader and Axolotl Loader. In a late-September incident, attackers used ClickFixsocial engineering to deploy Lorem Ipsum Loader and install a Python-based tunneling client. The intrusion was contained beforeransomware was deployed, but investigators assessed that ransomware delivery was likely the attacker's objective. The loaders use multiple delivery methods, including malicious ZIP archives, trojanizedMicrosoft-signed executables, DLL side-loading, fake Microsoft Teams MSI installers, Node.js and standalone PowerShell scripts.Their payloads use obfuscation, encrypted or encoded shellcode, persistence mechanisms and Windows API manipulation to evade detection. The final Python tunneling client communicates through TLS and WebSocket, allowing attackers to relay arbitrary TCP traffic through a compromised endpoint. Forescoutfound overlapping C2 infrastructure and behavioral similarities between the loaders, but could not conclusively establish that Lorem Ipsum is a later version of Axolotl.

Severity: High

Impact:

- Ransomware Risk: Loader deploymentand Python tunneling can provide a pathwayforsubsequentransomwareoperations.
- Initial Access: ClickFixand TerminalFixtechniques trick users into executing attacker-provided commands.
- DLL Side-Loading: Malicious DLLs are loaded by legitimate-looking, signed executables.
- EDR Evasion: Lorem Ipsum can unhook ntdlland manipulate memory protections.
- Covert Communications: TLS and WebSocket traffic can conceal tunneled connections within normal-looking HTTPS communications.
- Lateral Movement Potential: The Python tunnel can relay arbitrary TCP traffic to attacker-selected destinations.
- Payload Delivery: Additional scripts and shellcode can be retrieved and executed after initial compromise.

Recommendation & Mitigation Steps:

- Educate users about ClickFixand TerminalFixattacks that ask them to paste commands into Windows Run, PowerShell or Windows Terminal.
- Monitor Sysmon Event ID 1 and Windows Security Event ID 4688 for suspicious powershell.exe and cmd.exe execution chains involving 1.bat and unexpected executables.
- Detect signed executables loading DLLs from user-writable or unusual directories, especially vdsldr.exe with vdsutil.dll and CertEnrollCtrl.exe with CertEnroll.dll.
- Correlate new Registry Run entries with scheduled-task creation, particularly similarly named entries containing nine random characters.
- Investigate non-browser processes accessing letsdiskuss[.]com or digitalpoint[.]com for dead-drop resolver profiles.
- Monitor suspicious HTTP requests to /api/init/ with Content-Type: image/jpeg, the reported Firefox 143 user-agent and repeated five-second polling.
- Restrict unauthorized PowerShell and script execution through application control and endpoint security policies.
- If an endpoint is compromised, isolate it, preserve forensic evidence, investigate persistence and lateral movement, and assess whether additional ransomware payloads were • delivered.

Reference: https://www.forescout.com/blog/from-clickfix-to-c2-comparative-analysis-of-two-malware-loaders/

FortiManager Exploitation and PEERSTITCH Malware Targeting FortiGate Firewalls

Summary: Palo Alto Networks Unit 42 investigated a multi-stage cyber intrusion targeting a telecommunications managed service provider inSeptember 2024. The attackers exploited CVE-2024-47575, a critical FortiManagervulnerability, to gain unauthorized access to a centralized management appliance and steal an archive containing firewall configurations, credentials, cryptographic material, and network topology information associated with more than 500 managed FortiGate firewalls.The attackers subsequently recovered credentials, established unauthorized SSL VPN sessions, conducted network reconnaissance, and deployed packet-capture configurations to intercept sensitive traffic. They also exploited CVE- 2025-61624, a FortiOSprivilege-escalation vulnerability, to deploy PEERSTITCH, a stealthy ARM64 malware implant. PEERSTITCH operates in memory, injects code into legitimate FortiOSprocesses, and avoids creating persistent malware files or opening listening ports, making conventional detection more difficult. Unit 42 confirmed exposure of configuration and credential material but did not establish that every downstream client network was compromised.

Severity: High

Impact:

- Unauthorizedaccess: Exploitationof FortiManagerenabledattackers to executecommands without authentication.
- Credential exposure: Administrative and VPN credentials stored in stolen configurations were recovered.
- Network reconnaissance: Attackers obtained firewall configurations, routing information, network topology, and device inventories.
- Traffic interception: Unauthorized packet-capture rules targeted HTTP, TFTP, RADIUS, LDAP, and other services.
- Stealthy persistence: PEERSTITCH modified the memory of legitimate FortiOSprocesses to maintain covert access.
- Privilege escalation: Exploitation of CVE-2025-61624 enabled execution with root privileges on affected firewalls.
- Downstream exposure: Compromise of a centralized management appliance exposed sensitive trust material associated with hundreds of managed firewalls.
- Defense evasion: Attackers terminated logging services, cleared crash logs, and removed malicious configuration artifacts.

Recommendation & Mitigation Steps:

- Patch FortiManagerand FortiOSusing Fortinet's recommended fixed versions.
- Restrict management access and FGFM connectivity to trusted systems.
- Rotate potentially compromised credentials, certificates, and private keys.
- Review VPN sessions, administrator accounts, auto-script configurations, and packet-capture settings.
- Investigate suspicious process activity, logging interruptions, and outbound connections to known indicators.
- Assess all downstream firewalls managed by a potentially compromised appliance.

Reference: https://unit42.paloaltonetworks.com/fortimanager-cve-2024-47575-peerstitch-malware/

Windows BitLocker Vulnerabilities Could Allow Privilege Escalation and Security Bypass

Summary: Cybersecurity forum reported three Windows BitLocker vulnerabilities disclosed on last week. The issues include two privilege-escalation vulnerabilities and one security-feature bypass. Depending on the vulnerability, exploitation requires existing local privileges or physical access to the device. The report does not confirm active exploitation or specify affected Windows versions and remediation packages. Organizations should validate the vulnerabilities against Microsoft's official Security Update Guide before determining exposure..

Severity: Medium to High

Impact:

- Potential unauthorized privilege escalationon affected Windowssystems.
- Possible compromise of system confidentiality, integrity, and availability.
- Potential bypass of security protections under specific access conditions.
- CVE: CVE-2026-85920: Local privilege escalation involving a time-of-check-to-time-of-use (TOCTOU) race condition.
- CVE-2026-88070: Local privilege escalation associated with an out-of-bounds read.
- CVE-2026-83500: Security-feature bypass; the reported relationship to BitLocker remains unclear.

Recommendation & Mitigation Steps:

- Review Microsoft's official advisories for all three CVEs.
- Identify affected Windows systems after confirming the applicable versions.
- Apply Microsoft security updates once the relevant fixes are verified.
- Restrict local administrative privileges and physical access to endpoints.
- Monitor for suspicious local privilege escalation and unexpected changes to security settings.

Reference: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85920

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88070

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83500

Indicators of Compromise

IOC'S	Malicious Score
scriptedgeapp.com	4/92
213.109.203.107	3/92
transferrootway.com	1/92
45.66.249.57	3/92
updaterdeskarc.com	3/92
185.28.119.81	3/92
signinbyte.com	8/92
bloganimals.com	15/92
letsdiskuss.com	3/92
1a9541e8bf01f6f904d1759feeffea644f8669fc8d6a768cd55e0964e282e7c3	28/70

Indicators of Compromise

IOC's	Malicious score
213.109.203.107	3/92
45.66.249.57	3/92
185.28.119.81	3/92
23.240.77.233	7/92
47.18.167.159	7/92
45.32.41.202	12/92
198.199.122.22	6/92
185.28.119.14	3/92
45.66.249.132	2/92
185.28.119.138	2/92
91.236.230.173	1/92
92.118.126.226	1/92
scriptedgeapp.com	3/92
transferrootway.com	1/92
updaterdeskarc.com	3/92
signinbyte.com	8/92
bloganimals.com	15/92
letsdiskuss.com	3/92
queuepodnet.com	11/92
vaycia.shop	1/92
animals-offline.com	11/92
loginrestforest.com	18/92
animalsviewstory.com	13/92
blogpostmessage.com	13/92

Indicators of Compromise

IOC's	Malicious score
creativecurrentmedia.com	15/92
dailydoodleart.com	13/92
oiedra.com	13/92
uoidsod.com	13/92
wandertalesblog.com	12/92
biblegodlike.com	14/92
reeeeealy.com	18/92
semigoddess.com	18/92
bestpopularimages.com	13/92
editdocumentfree.com	15/92
opendocumentonline.com	11/92
photocategories.com	15/92
seephotoalbum.com	11/92
topimagechecker.com	16/92
topphotoalbum.com	15/92
cloudbreachdetection.com	15/92
beastcloudsecurity.com	15/92
peekyourphoto.com	14/92
newpopularimages.com	15/92
yourbestsupervisiournow.com	3/92
metricsdataway.com	17/92
cooldogshistory.com	14/92
syalae.com	2/92
1a9541e8bf01f6f904d1759feeffea644f8669fc8d6a768cd55e0964e282e7c3	28/75
e45888af7b94c773db1b956f6f1f8b3350c822505472522696c4f7942ce36cdd	38/75

Indicators of Compromise

IOC's	Malicious score
9d054b244561b577365277b8338b0e702f35d892be8383cd2d65d79aee6dbc6b	32/75
f2d0445f6b6d9fe1143646c2c46b613405d418f11af98e464401205b36490ad4	37/75
53fecaa44dee57e25855f974b6e9662efccaf32bda965a83a1cd0b78e05fa2b3	36/75
dc87b21776e184903d8f90a836422e3146b1f86ffa3997dd3630946d88ef91f5	0/75
8a326b3512b7fb473f65630f6225a77717cef4ad574d0afe6654af279adf062f	15/75
0d1953c17fa0d705ea86d79b3df0ef8e0c5a49053acdce09fdbd07f74a23a7c6	48/75
29491ba6d7d8ca6850c68a067f01cdb917904b7a61b4299255c90a6cd6b78b48	48/75
3a7d7e18c2a4beef280c564a90516af931ecb9be0dbacbe905b5df2c2f73682c	46/75
54e71dabe16426e3f96500236a5de4ea5ed8ba74af5eb2b5ccb4c885dad9d60c	45/75
5ce2c6a2eb3ebd2f66d72cdbeec4c98ce507b0bc317c5beedd61053b4f871e75	45/75
7d1fa95404b611ed1301e9a676f0fd6b90f24cd7c766b605bc9c0d08516b1f73	49/75
8b6e79b74859b22dbe9ef9d9ae2c27236640f062560fb4a9d743245d2389091a	46/75
a557a320aa0c8fed986cd969596481b23d2c77abf7469e67b70f1231f0103682	46/75
cf184310de31b720d0294d673b308eb7b82fdab4d7999953cdf12acef9631c03	47/75
3d3d9d404a54a43f0d500546f54e64fb944705fff41f93d5e82ad7024eba8ba9	46/75
5d00d7882328e6d10c7e9dc4ab241ea507286efe4e3d87c2be8436d0af703581	45/75
68848814c4efb2269b898a53cf0ffa265cd7fb58ca4cc71c90206e5e4444d6c7	47/75
95fc2dd8decd8c37ac3e985b63a58fd477bc98888d0754e7f041f7f1f8d0f043	46/75
acfecbebe0e30deafec6ef578c4adea2ba7c2279d92df808018142819bd8808f	45/75
ee046a0baa3bbb928192e8fcf13533e806acba1fef6d93f4be24edb27e4bd811	44/75
f66c6ec3837107d3163fc260921d598375cc5a9beae06e961bf4b073fb2b7664	50/75
267d4018543138409387506aabafe2318980ae3cf5e06ebe2675bf36cb24116c	38/75
3c8d7b6c7a37fb489c3d62b4427c3c09b5b8f3797a02d0465d4828c9812a62eb	36/75
8f6e2d874ac99b12bd0451b554a522894923b6858ee9ca11fdf011aa1ca67f59	46/75
186d4c16a3758b20967d712582fbe74e7dc0d566ff99753adcb11dc857006a96	43/75

Indicators of Compromise

IOC's	Malicious score
1cb54b0217afe3bb8d4b2577f5be4f16cbd00b3e2c79ec18ebb1d9daad0e3588	40/75
24fc515ddfc5c60cfdc2f369831cf462ca7b14318a925aaee261272ff9a394d2	42/75
2c439ef59a7ed4510ac93924f12e690b291b887624356aa8269ac5b3e307ef16	43/75
4bcf66570431b60c9822d444071f909ab9c235c675ece1649e8c64dc061622cb	45/75
786ebc7d74a5229495a44eaf6bd422a53cfaefdd555596d037eaffa76f434b69	46/75
9bda1a463f363f67db1905824b28bf16f3e927752a15b7d5ac3d307125509718	44/75
9c45329f4334ef71d927ec66ea277cc276087628054881303f78ef0b2cac93b8	44/75
a9ac7de9161d9ca3a791179beee7a51c1b94d4c381e131308e6586b6009dd867	44/75
b3c5b9b37bcc9093439e9846c9f175bad09121c9809fee2bd96835419eceec7e	41/75
004fb2c36532c00d3c3eb041c12fba99d26eb900880a361cb664f76e4d022a26	37/75
0fb48494ed9b87a63f24a4b09923d2aeb0fa63585d85e823c1cbb5250cbd8a0f	39/75
12049c977e193972b665995720243571cf775f6f0428460192536d92c8528dbb	40/75
7dc54e91f58ec057f2596598b81ededf5c6c0976725bf2c1a2fc032f4d87f2f2	38/75
8643a4a4612b85f78cf246039bec6252caa56b4ed018978d9b42789e9058d1e6	37/75
a09eee349d00f3cdc17562eb2b2373efba1fa5c498da94ee38c102918cb095a7	41/75
abe4a4dbb2de862a3fba8b4efd58cacd020eac3a70bb6a8f92eec74c23dedc91	36/75
b43820a5dd317a18cc21d529e2dc242a705c45a204b1b01a7106d4407e5a7e24	40/75
d08e8ba4011438dacca0db41877febd6b6995936ddebe88d2cd124ec03182af6	40/75
f8a1c837254b8be9204f073f91af539463bf4e1ffabfe626c7aca2a0552ae683	39/75
b7ae166fd49a7ecfe6322a80b8aa56d6aa0825d8f5d106dab2e4fb7d14ce15a8	4/75
8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92	0/75

Indicators of Compromise

IOC'S	Malicious Score
53fecaa44dee57e25855f974b6e9662efccaf32bda965a83a1cd0b78e05fa2b3	36/67
9d054b244561b577365277b8338b0e702f35d892be8383cd2d65d79aee6dbc6b	32/67
23.240.77.233	6/92
47.18.167.159	7/92
45.32.41.202	12/92
198.199.122.22	6/92

Thank You

