

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Zero-Day Exploit in 7-Zip Fuels SmokeLoader Attacks on Ukraine

Date of Publication

February 5, 2025

Admiralty Code

A1

TA Number

TA2025030

Summary

First Seen: September 2024

Affected Products: 7-Zip

Affected Platform: Windows




Targeted Country: Ukraine

Targeted Industries: Government and Civilian organizations

Malware: SmokeLoader

Impact: A critical zero-day flaw in the 7-Zip archiver, tracked as CVE-2025-0411, has been actively exploited since September 2024. This vulnerability allows attackers to bypass Windows' Mark of the Web (MotW) security feature, enabling the seamless execution of malicious files. Russian cybercrime groups actively leveraged this flaw in spear-phishing campaigns, using sophisticated homoglyph attacks to spoof document extensions. This tactic deceived users ultimately facilitating the delivery of SmokeLoader malware in targeted attacks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0411	7-Zip Mark-of-the-Web Bypass Vulnerability	7-Zip			

Vulnerability Details

#1

A zero-day vulnerability in 7-Zip, identified as CVE-2025-0411, which allows attackers to bypass Windows' Mark of the Web (MotW) security feature, making it easier to execute malicious files without raising red flags. Russian cybercriminal groups exploited this flaw to deliver **SmokeLoader** malware, targeting Ukrainian organizations likely for cyberespionage purposes. They leveraged spear-phishing campaigns with homoglyph attacks to disguise malicious files, tricking windows users into running them.

#2

CVE-2025-0411 allows attackers to bypass Microsoft Windows' Mark-of-the-Web (MoTW) security feature by embedding malicious scripts or executables within double-archived files created using 7-Zip. This flaw, present in versions prior to 24.09, stems from 7-Zip's failure to apply MoTW protections to nested archives, enabling files to execute without triggering security warnings.

#3

The vulnerability was actively exploited in phishing campaigns targeting Ukrainian government entities and businesses. Emails sent from compromised Ukrainian accounts tricked recipients into opening seemingly legitimate attachments. One notable target was the helpdesk of Zaporizhzhia Automobile Building Plant (PrJSC ZAZ), a major vehicle manufacturer.

#4

Attackers employed homoglyph techniques, swapping characters with visually similar ones to deceive users. In one instance, the invoice.zip archive hid an executable as a PDF, with attackers using compromised emails to increase credibility and infection rates.

#5

Due to the active exploitation of CVE-2025-0411 since September 2024, upgrading to 7-Zip version 24.09 is critical. This case highlights the growing sophistication of cyberattacks amid the Russo-Ukrainian conflict, marking the first known instance of a homoglyph attack integrated into a zero-day exploit chain a concerning evolution in threat tactics.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-0411	7-Zip Version Prior to 24.09	cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*	CWE-693

Recommendations



Stay Updated: Update 7-Zip to version 24.09 or later. Regularly apply Windows and critical software updates to close security gaps and reduce the risk of exploitation.



Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.



Enhanced Email Security: Enhance email security by implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.



Restrict Automatic File Execution: Turn off the automatic execution of files from untrusted sources and set up systems to prompt users for confirmation before opening them.



Strengthen Defenses: Implement domain filtering and URL monitoring to block homoglyph-based phishing attacks. Regularly update blacklists to include new malicious domains.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0005</u> Defense Evasion
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1566</u> Phishing	<u>T1566.001</u> Spearphishing Attachment
<u>T1204</u> User Execution	<u>T1204.002</u> Malicious File	<u>T1036</u> Masquerading	<u>T1059</u> Command and Scripting Interpreter
<u>T1583</u> Acquire Infrastructure	<u>T1583.001</u> Domains	<u>T1553</u> Subvert Trust Controls	<u>T1553.005</u> Mark-of-the-Web Bypass
<u>T1586</u> Compromise Accounts	<u>T1586.002</u> Email Accounts	<u>T1584</u> Compromise Infrastructure	

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	554d9ddd6fd1ccb15d7686c8badb8653323c71884c7f20efb19b56324ff34fc1, 2e33c2010f95cbda8bf0817f1b5c69b51c860c536064182b67261f695f54e1d5, 84ab6c3e1f2dc98cf4d5b8b739237570416bb82e2edaf078e9868663553c5412, 54678013c8741db3340960e54ba93001c27619ead5cf5cc2eafd4c0fcf797ae6, 62eb856a5f646c2883a3982f15c3eb877641f9e69783383ce8a73c688eccd543, cd123c288f623878218be31125000441bb8c5447375af67bc3c1d27d16eb5f8c, 8ee225bdd38cf6fd014a16beb9e33a0650147a9b7ea2104afe2f47c01bd1db0b, a059d671d950abee93ef78a170d58a3839c2a465914ab3bd5411e39c89ae55a2, b3df042c5286fa91a4555e105038364bc66bfe7fdfe3769eb26b96e0ffe6096b, 915b73a57aaf759fbd5352d79656e1b697545e6c9d953ab05aacf61ed4f6e397, d6d722ae73dfff1ad7c468feca882b159a2a6e267df8b219482b514cdab74c21, fdfbdd42944c9e3b9697a8d8375e4e5cfd45c86941aa3f8f6dd0d08607b73144, 5c7d582ba61ac95fb0d330ecc05feeb4853ac1de1f5a6fd12df6491ddb7ea34, 888f68917f9250a0936fd66ea46b6c510d0f6a0ca351ee62774dd14268fe5420
URLs	file[://]185[.]156[.]72[.]78/MyFolder/invoce[.]zip, hxxp[://]alfacentarusmulticopter[.]ru/index[.]php, hxxp[://]johnfabiconinteraption[.]ru/index[.]php, hxxp[://]storeagroculturnaya[.]ru/index[.]php, hxxp[://]alfacentarusmulticopter[.]ru/index[.]php, hxxp[://]storeagroculturnaya[.]ru/index[.]php, hxxp[://]johnfabiconinteraption[.]ru/index[.]php, hxxp[://]alfacentarusmulticopter[.]ru/index[.]php, hxxp[://]unicalads[.]ru/index[.]php hxxp[://]lazaretmed[.]pw/index[.]php, hxxp[://]technoads[.]pw/index[.]php hxxp[://]oncomnigos[.]online/index[.]php, hxxp[://]185[.]156[.]72[.]78/MyFolder/pay[.]zip, hxxp[://]southlander[.]ru/dklfhgjd fhgjd78khdgfhgh/akt[.]bat,

TYPE	VALUE
URLs	hxxp[:]//[goodmastersportunicum[.]ru/load/svc[.]exe hxxp[:]//[ukr-netfilediscdownloadapplication[.]ru/file/download/6852365456384563846538458,5863874653786587365934/AKT_PAX_26_09_2024p[.]rarhxxps[:]//[ukr-netfilediscdownloadapplication[.]ru/file/download/6852365456384563846538458,5863874653786587365934/AKT_PAX_26_09_2024p[.]rar
Domains	alfacentarusmulticopter[.]ru, johnfabiconinteraption[.]ru, storeagroculturnaya[.]ru, alfacentarusmulticopter[.]ru, storeagroculturnaya[.]ru, johnfabiconinteraption[.]ru, alfacentarusmulticopter[.]ru, unicalads[.]ru, lazaretmed[.]pw, technoads[.]pw, oncomnigos[.]online, southlander[.]ru, goodmastersportunicum[.]ru, ukr-netfilediscdownloadapplication[.]ru
IPv4	185[.]156[.]72[.]78

Patch Details

Update 7-Zip to version 24.09 or later.

Link: <https://www.7-zip.org/>

References

https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html

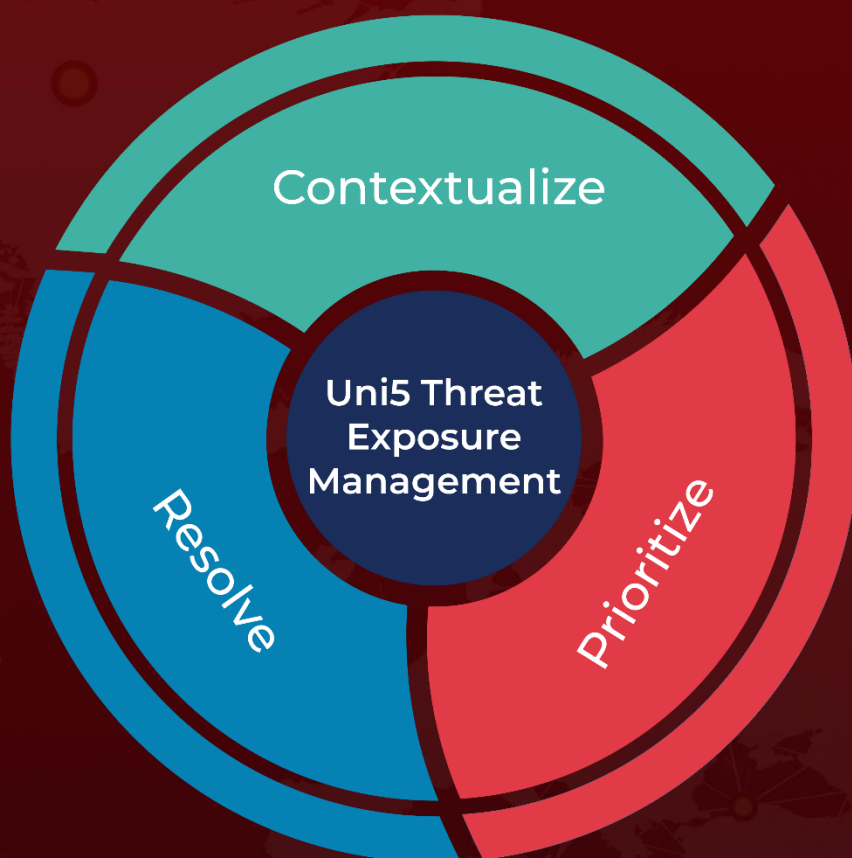
<https://www.zerodayinitiative.com/advisories/ZDI-25-045/>

<https://hivepro.com/threat-advisory/smokeloader-strikes-taiwan-unveiling-a-modular-malwares-sophisticated-attack-chain/>

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 5, 2025 • 5:45 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com