

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

Telegram-Powered Credential Theft Campaign Sweeps Europe

Date of Publication

November 13, 2025

Admiralty Code

A1

TA Number

TA2025344

Summary

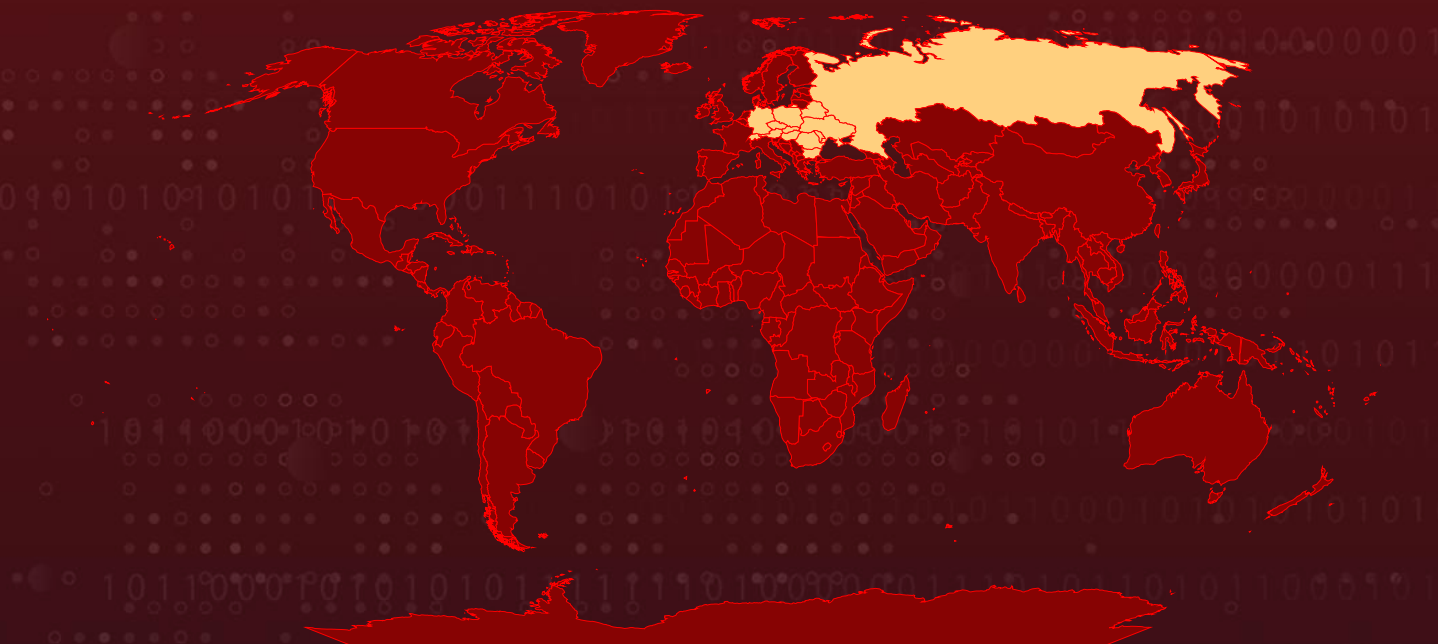
Attack Discovered: 2025

Targeted Region: Central and Eastern Europe

Targeted Industries: Agriculture & Livestock, Automotive, Construction, Consumer Goods, Education, Energy & Utilities, Government & LEA, Hospitality, IT & ITES, Manufacturing, Media & Entertainment, Professional Services, Retail, Telecommunications, Technology

Attack: A sophisticated phishing campaign is making waves across Europe, using cleverly crafted HTML attachments to steal user credentials while bypassing traditional security checks. Instead of relying on malicious links or remote servers, attackers embed JavaScript within the HTML files to mimic trusted brands like Adobe, Microsoft, and FedEx, tricking users into entering their credentials on fake login pages. The stolen data is then funneled directly to Telegram bots controlled by the attackers, creating a fast, low-cost, and hard-to-trace operation. With regional customization, realistic business lures, and anti-analysis techniques, this campaign highlights how phishing has evolved into a stealthy, scalable threat that blends automation, deception, and social engineering to breach even well-protected organizations.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Powered by Bing



Attack Details

#1

A widespread and sophisticated phishing campaign has emerged, targeting multiple global brands to steal user credentials through cleverly disguised HTML attachments. Unlike traditional phishing attempts that rely on malicious URLs or remote servers, this campaign delivers self-contained HTML files via email that execute JavaScript to capture login credentials and send them directly to Telegram bots controlled by the attackers. By avoiding external hosting and employing deceptive login pages, the attackers effectively bypass many conventional email and web security filters, making detection significantly harder.

#2

The campaign's emails typically contain attachments with RFC-compliant filenames or are compressed into ZIP files to appear legitimate. Once opened, the file displays a counterfeit Adobe login page that prompts users to "sign in to view" the document. Behind the scenes, JavaScript scripts send the entered credentials to the Telegram Bot API using hardcoded bot tokens and chat IDs. The entire process is localized within the HTML file, showing no external network activity until the credentials are transmitted, a design that underscores the attackers' technical refinement and adaptability.

#3

Upon submission, victims unknowingly send their credentials through a JavaScript-based POST request to Telegram, after which they are met with a fake "login error" message to conceal the compromise. The malicious samples revealed two notable variants showcasing varying levels of sophistication. Sample 1 uses CryptoJS AES encryption to obfuscate its code and captures not only credentials but also IP addresses and browser details using APIs. Victims are often prompted to re-enter their credentials after being told their password was incorrect, ensuring data accuracy. Meanwhile, Sample 2 adopts a sleeker approach with the native Fetch API, integrating anti-analysis techniques that block shortcuts like F12 or Ctrl+Shift+I, preventing users from inspecting the malicious code.

#4

A network of decentralized Telegram bots managed by multiple threat actors. Each bot used unique tokens and exhibited distinct behavioral patterns. It was also observed token reuse across campaigns, suggesting collaboration or shared toolkits among operators. Many HTML templates shared consistent visual elements, such as Adobe-styled modals and blurred invoice backdrops, indicating the likely use of an automated phishing generator or toolkit.

#5

This campaign primarily targets organizations across Central and Eastern Europe, including the Czech Republic, Slovakia, Hungary, and Germany, where emails mimic authentic business correspondence. The threat actors adapt their strategy regionally, impersonating well-known brands such as Adobe, Microsoft, WeTransfer, DocuSign, FedEx, DHL, and Telekom Deutschland. Their ability to blend localized language and branding with globally recognized corporate identities demonstrates a scalable and adaptable phishing infrastructure designed for maximum reach and credibility. Overall, this campaign represents a highly scalable, cost-effective credential theft operation that successfully evades traditional detection systems.

Recommendations



Be Cautious with HTML Attachments: Avoid opening unexpected HTML or ZIP attachments, especially those claiming to contain invoices or quotations. Treat all unsolicited attachments as suspicious until verified through a trusted channel.



Verify Before You Click or Sign In: If an email asks you to “sign in to view” a document, confirm the request directly with the sender using a known email address or phone number. Genuine companies rarely ask you to log in through attached files.



Restrict Telegram API Access: Many attackers are using Telegram bots for data exfiltration. Network administrators should consider blocking Telegram’s API at the firewall or proxy level where feasible, especially in enterprise environments.



Enable Multi-factor Authentication (MFA): Even if credentials are stolen, MFA provides an extra layer of defense, preventing unauthorized access to accounts. Ensure MFA is enforced across all critical business systems.



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.



Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access
<u>TA0010</u> Exfiltration	<u>T1566</u> Phishing	<u>T1566.001</u> Spearphishing Attachment	<u>T1204</u> User Execution
<u>T1204.002</u> Malicious File	<u>T1056</u> Input Capture	<u>T1056.003</u> Web Portal Capture	<u>T1567</u> Exfiltration Over Web Service

<u>T1567.002</u> Exfiltration to Cloud Storage	<u>T1027</u> Obfuscated Files or Information	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript
<u>T1036</u> Masquerading	<u>T1656</u> Impersonation		

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	fb6b07ed5cbd049bb6126ada3ced943a66c5ca6b022aa10017512fa25521a21e, 386e4755fd2fe87454936ddea4a01425f36d8ab434bf0f892054ac13bebdb2bd, f3213b98a33b4f156f6f8860fdfa54b02479d662d80be8f59012aa1b0a77210d, 30108ee705dba4a4c73e6b502d7899f66de65f51090d9119c0c6db6e6c316ee7, 180bd9d3485762203a3450ddf25ba709fc2fa78eaf98c4e327ea6d55319dcdec, ee1f979fc9ba43d9703af9339c61f6d68ffd662e30aa2eef8870ef652e49d062, d2397acb1248e82e0ef52bbe9649aa379b111458691fae50b0e80ea88b7c5c8e, 0a3077a21194e1e4266956d984fee66f8bb25061995d72b65a0bb9b851dd8b8b, b205d3d54a53264fd638597dcaa57bc9550aecc47a244328c1f2e0d70e2489c6, 594659e760e97b5ab4c7c790dce0c4bfb821bbe86cbb5acafd8151a17c458411, e4375e379ce6d8bdc5d3d9064409d999b4e21a61dec6d5a7e697b4c3c574041c, eb0d707327bc55e2f1f2933b5f759dc9d6174f6e315fadd17804deb5a0bea80d, 753baed1c2d1fa4448b4c276cac50acafb82082ee7bca40df1b9f5f5b30b7736, 1ecef19e4aed7f8e25719a7d10e40c18bf520eb127661ffe296abed1ef227a1c, 2628c5da2061cba2963e45857d3d8db48902c261cc4fa61866e4e84518e408f4,

TYPE	VALUE
SHA256	e8e99fb2e0c774f2709f9e1d0d4481738e563dc27cefce49a9aa3995e a33574c, f1595bd2da01dc1e72430917ae18629640608afb1508ee21355007d4 83b2f64c, ef498210b91af5ed513180fe5b4631612f6d05b2637ce90bd2488199 832a269a, 9c386f40e2f6111d5d96bfedad9d1eebe228887b8fecb12c1c89705f0 b4ccd36, ccc6a7a853b1940c658edb343ec4730cf38440c0885158d832e47eb d691e2f6, 66202aef6178ab2a209edb11acd626383b0bf1f53ad5b9c29ab52dda d685bf1d, e494e168d95fa4be0564f080f39793aef9c64aeaebd6d9c12138baf9e bea7407, 74f816695e6de16ce00d1d72af8dadae08658d70c99aa21aa704866b abeae71a, eb4a8b5309302ac883ca41182d10691787121eb78fee1b58e6c8bddd 44a051f6, 05ecefcc10e55f0cadd74f9e18a91b555946e747344560695f583a462f 9efb90, 00aa7478cdfcfec9c7efa81a5f50c3cbe50062c33bedbbbebaebb659962 5d3d06, 7606d6957f50e336b0c9515dcbb29369e05d11aecd6fdc8dc678c35a 20f039ab, 11c27da12f43d7be371e9a2d3220d13e17b293e1eeb7f357f944e347 2818477a, d06c6942379aa4b7b831785207c6693664270cf0f9c3a2bcb309af9a3 43de337, 4317b4436dbd8b4a053054ad189ef875f77c2ec864c083c57c78f34a7 f3db322, b8623f658fba39c0004bfeb0e75c24f46f06acd6e0e0054076cb8c62b 7736d5f, ae8b089b48edcb76cdc2b85e45fc8f9df7a7e6883f7b44fd020bf5529b 2e1c78, 90a27888cfefad9086ae4cd90bd92175a8fe80b9ab9cabf00384208d7 7ddb79f, 24a32845ef75ec3c9439d08ec7111ec933e79b803966f5a7c704649e 281a9fd0, 32d989ae75589f8c0f1347a81bb97b9ff5e1cd10ca225d40792be74b0 ab9a1d1, e6bbc26691c82b62be7274cc3c0b14c0241cd022edee18c6fc14f64a5 558a1bb

Note: The remaining Indicators of Compromise (IOCs) can be accessed on the platform.

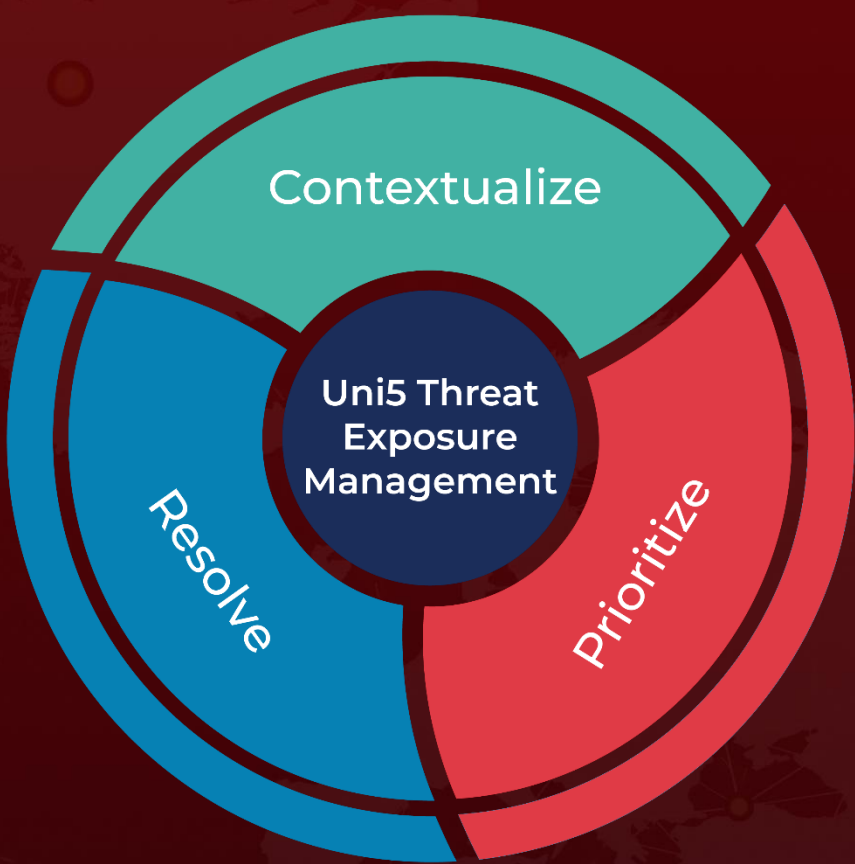
References

<https://cyble.com/blog/multi-brand-phishing-campaign-harvests-credentials/>

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
November 13, 2025 • 7:00 AM

