Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

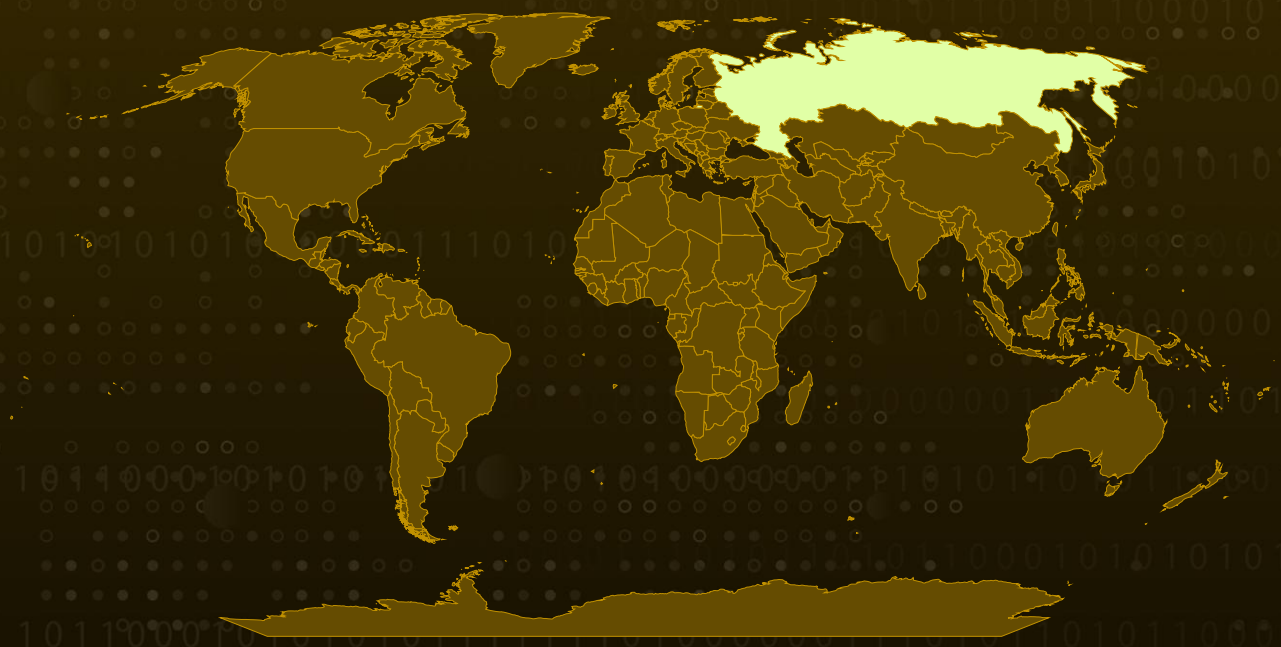
Phantom Stealer Hidden in Fake Bank Confirmations

Date of Publication	Admiralty Code	TA Number
December 15, 2025	A1	TA2025379

Summary

Attack Discovered: 2025
Targeted Country: Russia
Targeted Industries: Finance, Accounting, Treasury, Procurement, Legal, HR/Payroll, Executive Assistants, SMEs
Affected Platform: Windows
Malware: Phantom
Campaign: Operation MoneyMount-ISO
Attack: Operation MoneyMount-ISO is an active phishing campaign originating from Russia that deploys the Phantom information-stealing malware through a multi-stage attack chain. The campaign utilizes fake payment confirmation lures delivered via email, containing malicious ZIP archives with embedded ISO files. When victims open the ISO file, it auto-mounts as a virtual CD drive and presents an executable disguised as a legitimate bank transfer confirmation document. Execution triggers a sophisticated payload chain that ultimately deploys Phantom Stealer, a comprehensive credential theft and data exfiltration tool targeting financial assets, cryptocurrency wallets, browser credentials, and sensitive communications.

Attack Regions



Attack Details

#1 An active phishing campaign linked to Russian threat activity is leveraging fake payment confirmation emails to quietly deliver Phantom Stealer malware. The attack relies on a familiar social engineering tactic: presenting the message as routine financial correspondence to lower suspicion. By abusing multi-stage attachments and trusted-looking language, the campaign targets users who are likely to open documents quickly, particularly those in finance or accounting roles.

#2 The phishing email itself is written in Russian and carries the subject “Подтверждение банковского перевода” (Confirmation of Bank Transfer). It is sent under the name of “Anton Vladimirovich Demyanenko” from a domain unrelated to the organization it claims to represent, posing as a legitimate currency broker. The message urges the recipient to review an attached document related to a supposed bank transfer, using a formal and professional tone to appear credible. Notably, the generic salutation (“Sir”) suggests the campaign is mass-distributed rather than carefully personalized.

#3 Attached to the email is a ZIP archive that contains an ISO file, a format increasingly abused to bypass security controls. When the ISO is opened, it automatically mounts as a virtual drive and presents an executable masquerading as a payment confirmation document. Launching this file triggers the infection chain, ultimately deploying Phantom Stealer on the victim’s system. The mismatch between the sender’s domain and the impersonated company, combined with the unusual attachment format, points to a deliberate and well-crafted deception attempt.

#4 Technical analysis shows that the initial executable loads an encrypted payload embedded within a DLL, which is decrypted in memory before injecting Phantom Stealer. The malware includes extensive anti-analysis capabilities designed to evade detection and frustrate analysts. It actively checks for virtual machines, sandboxes, suspicious usernames, analysis tools, blacklisted IP ranges, and even system identifiers such as the MachineGuid. If these checks are triggered, the malware terminates itself to avoid further scrutiny.

#5 Once active, Phantom Stealer focuses on large-scale data theft. It targets browser-stored credentials, cookies, credit card data, cryptocurrency wallet extensions, desktop wallet applications, Discord authentication tokens, clipboard contents, and keystrokes. Stolen data is organized, archived, and exfiltrated through multiple channels, including Telegram bots, Discord webhooks, and FTP servers. This campaign, tracked as Operation MoneyMount-ISO, highlights how financially motivated actors are combining ISO-based delivery, staged payloads, and robust evasion techniques to steal sensitive data efficiently, reinforcing the need for stricter email attachment controls, behavioral monitoring, and heightened scrutiny of finance-related emails.

Recommendations

- **Treat Payment-related Emails With Extra Caution:** Emails that claim to confirm bank transfers, invoices, or urgent payments should always be verified through a trusted, separate channel. If a message pressures you to open an attachment to "confirm" a transaction, pause and validate it with the sender before taking any action.
- **Block Risky Attachment Types at the Email Gateway:** ISO, IMG, and ZIP-based container files are increasingly abused to deliver malware. Where possible, restrict or quarantine these attachment types, especially in emails sent to finance, accounting, and procurement teams.
- **Improve Monitoring and Incident Readiness:** Log and monitor outbound connections to services commonly abused for exfiltration, such as Telegram, Discord webhooks, and FTP. Establish clear incident response procedures so suspected phishing infections can be isolated and investigated quickly.
- **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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File
T1106 Native API	T1027 Obfuscated Files or Information	T1027.003 Steganography	T1497 Virtualization/Sandbox Evasion

T1036 Masquerading	**T1070** Indicator Removal	**T1070.004** File Deletion	**T1055** Process Injection
T1055.001 Dynamic-link Library Injection	**T1620** Reflective Code Loading	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1082 System Information Discovery	**T1057** Process Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1056 Input Capture	**T1056.001** Keylogging	**T1115** Clipboard Data	**T1528** Steal Application Access Token
T1567 Exfiltration Over Web Service	**T1560** Archive Collected Data	**T1560.001** Archive via Utility	**T1539** Steal Web Session Cookie
T1573 Encrypted Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	27bc3c4eed4e70ff5a438815b1694f83150c36d351ae1095c2811c962591e1bf, 4b16604768565571f692d3fa84bda41ad8e244f95fbe6ab37b62291c5f9b3599, 60994115258335b1e380002c7efcbb47682f644cb6a41585a1737b136e7544f9, 78826700c53185405a0a3897848ca8474920804a01172f987a18bd3ef9a4fc77

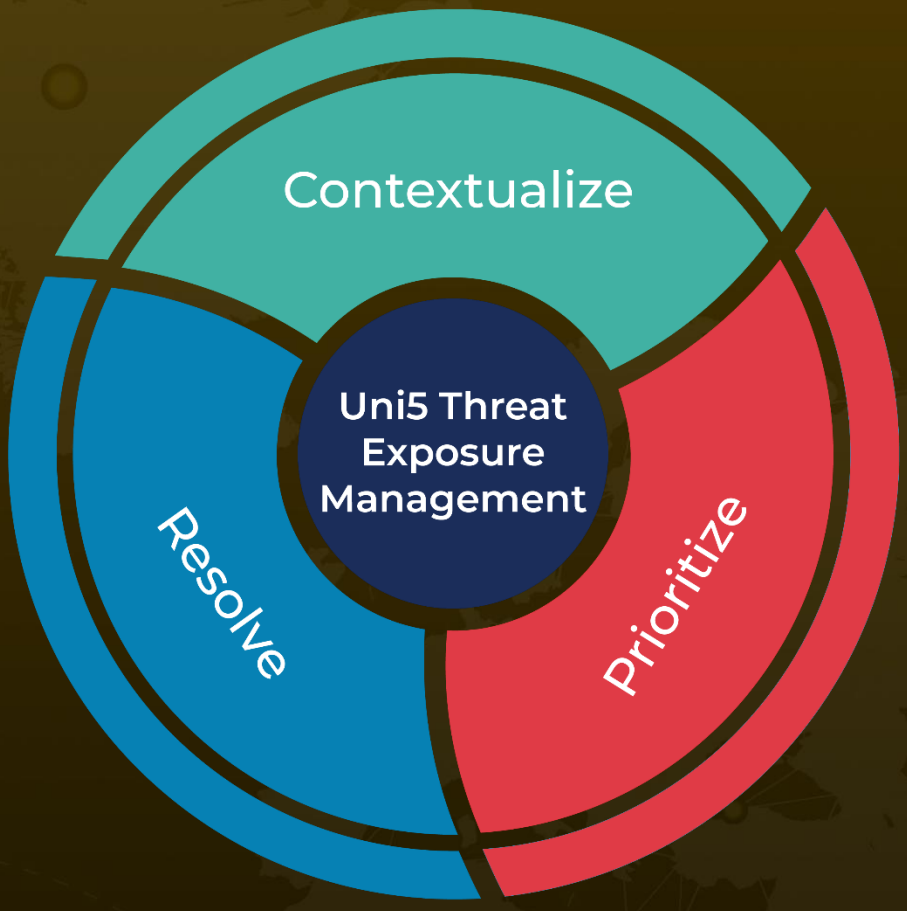
References

https://www.seqrite.com/blog/operation-moneymount-iso-deploying-phantom-stealer-via-iso-mounted-executables/

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

December 15, 2025 • 7:00 AM

More at www.hivepro.com