Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

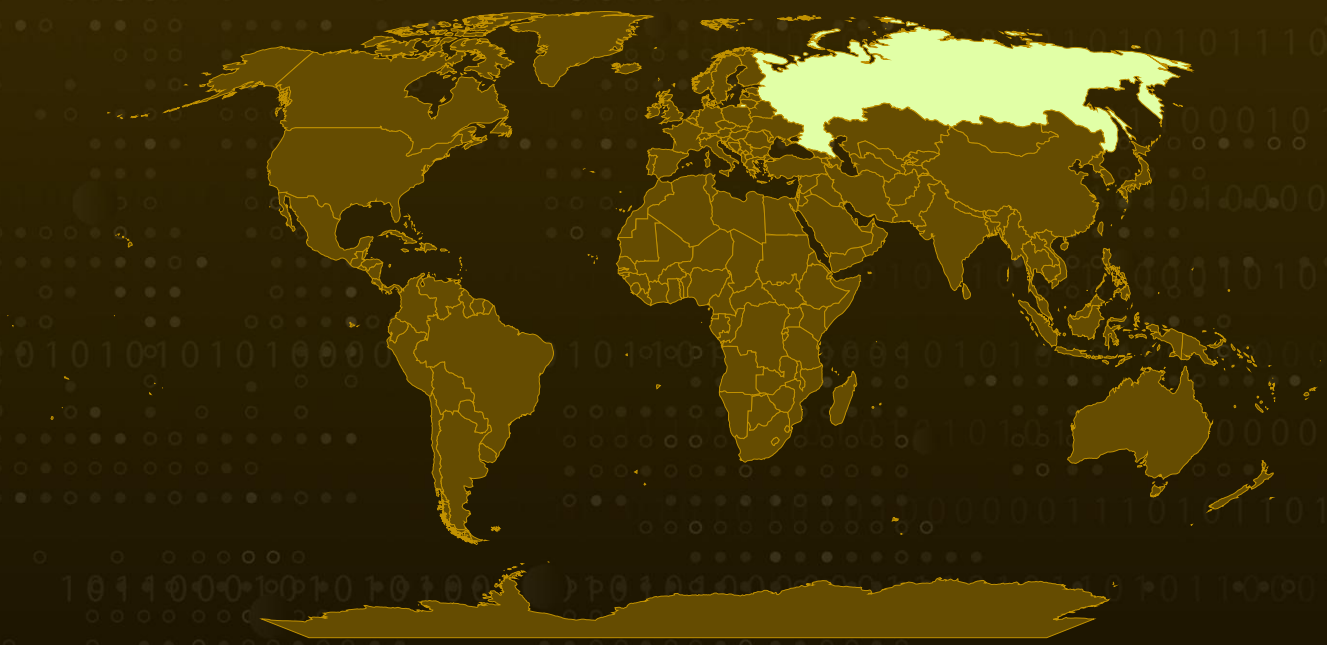
Pure RAT's Stealthy Campaign Sweeps Russian Enterprises

Date of Publication	Admiralty Code	TA Number
May 23, 2025	A1	TA2025161

Summary

Attack Started: March 2023
Malware: PureRAT, PureLogs, PureCrypter
Targeted Industry: Banking, Finance
Targeted Country: Russia
Attack: A stealthy malware campaign is hitting Russian companies hard, spreading through phishing emails disguised as routine financial documents. Once opened, the malware PureRAT gains full control of the system, stealing data, logging keystrokes, and even hijacking crypto transactions. Paired with tools like PureCrypter and PureLogs, it operates quietly in the background, making it a serious threat to business security in 2025.

Attack Regions



Attack Details

#1 Since March 2023, Russian organizations have been increasingly targeted by a sophisticated cyber campaign leveraging the Pure malware family which is sold through a Malware-as-a-Service (MaaS) model. The scale of these attacks has grown significantly, with 2025 seeing a fourfold increase in incidents compared to the same timeframe in 2024. These attacks typically begin with phishing emails containing RAR archives disguised as business-related documents. The attackers use convincing filenames with double extensions like .pdf.rar to trick recipients into opening the attachments.

#2 Upon execution, the embedded Trojan extracts and decrypts an additional payload, which injects itself into a legitimate process. The injected module is PureRAT, a remote access trojan capable of establishing encrypted connections and sending protobuf-formatted data to its command-and-control (C2) servers. These messages contain detailed system metadata, including OS version, antivirus status, device identifiers, and IP address. PureRAT is designed for stealth and persistence, executing commands to self-delete, restart or shut down the host, and capture activity within specific applications based on keyword detection.

#3 One of PureRAT's more invasive capabilities includes scanning active windows for financial or personal terms such as "password," "bank," and "WhatsApp." When such terms are found, the malware captures a screenshot and sends it to the operators. It also includes a plugin that monitors the clipboard for cryptocurrency wallet addresses and replaces them with attacker-controlled values an unusual but lucrative tactic for corporate-targeted malware. In addition, it provides full system control through modules for keylogging, remote desktop access, and file execution.

#4 The infection chain often begins with the execution of StilKrip.exe, a component of PureCrypter, another malicious toolkit. PureCrypter's role is to download additional payloads masked as innocuous media files decrypt them and execute them in-memory to avoid disk-based detection. The malware also ensures persistence by copying itself to %AppData% as Action.exe and creating a startup script that runs on every reboot. The final stage involves the delivery of PureLogs, a powerful stealer capable of extracting sensitive information from browsers, email clients, messaging apps, VPNs, and cryptocurrency wallets.

#5 Although PureLogs is classified as a data stealer, it also doubles as a downloader, enabling attackers to execute additional payloads post-infection. This dual capability makes it even more dangerous in enterprise environments where attackers can maintain long-term access and perform follow-up attacks.

Recommendations

Be Cautious with Email Attachments: Most of these attacks start with a simple email. If you or your team receive attachments in .RAR format or files with odd double extensions like .pdf.rar, don't open them without verifying. Train your employees to spot phishing attempts, especially if the email looks like it's about payments or invoices but comes from someone unexpected.

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.

Keep Devices and Security Tools Updated: Always install the latest security updates not just for your antivirus, but also for your operating systems and everyday tools. Updates often include fixes that block malware from slipping through cracks in outdated software.

Limit What Can Run on Your Systems: Not every computer needs to run every kind of software. Create a list of approved programs and block everything else. This way, even if malware sneaks in, it won't be able to run. Also, disable rarely used tools like scripting features (e.g., VBS, PowerShell) if you don't need them.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0040 Impact	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder

T1518 Software Discovery	T1518.001 Security Software Discovery	T1082 System Information Discovery	T1036 Masquerading
T1056 Input Capture	T1056.001 Keylogging	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1497 Virtualization/Sandbox Evasion	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information	T1574 Hijack Execution Flow
T1574.001 DLL	T1071 Application Layer Protocol	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1115 Clipboard Data	T1113 Screen Capture	T1529 System Shutdown/Reboot	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	9B1A9392C38CAE5DA80FE8AE45D89A67, DD2C1E82C5656FCB67AB8CA95B81A323
SHA256	BD6F35F5D87C04A30775AA53432C009383CA08284208E737BA435D96BDB8ABFE, 3ACD18C8790F7556671ADED0785BEBFEF8EEFC57137B58C2118ADD5834C82C33
IPv4:Port	195[.]26[.]227[.]209[:]56001, 195[.]26[.]227[.]209[:]23075
URL	hxxps[:]//apstori[.]ru/panel/uploads/Bghwwhmlr[.]wav

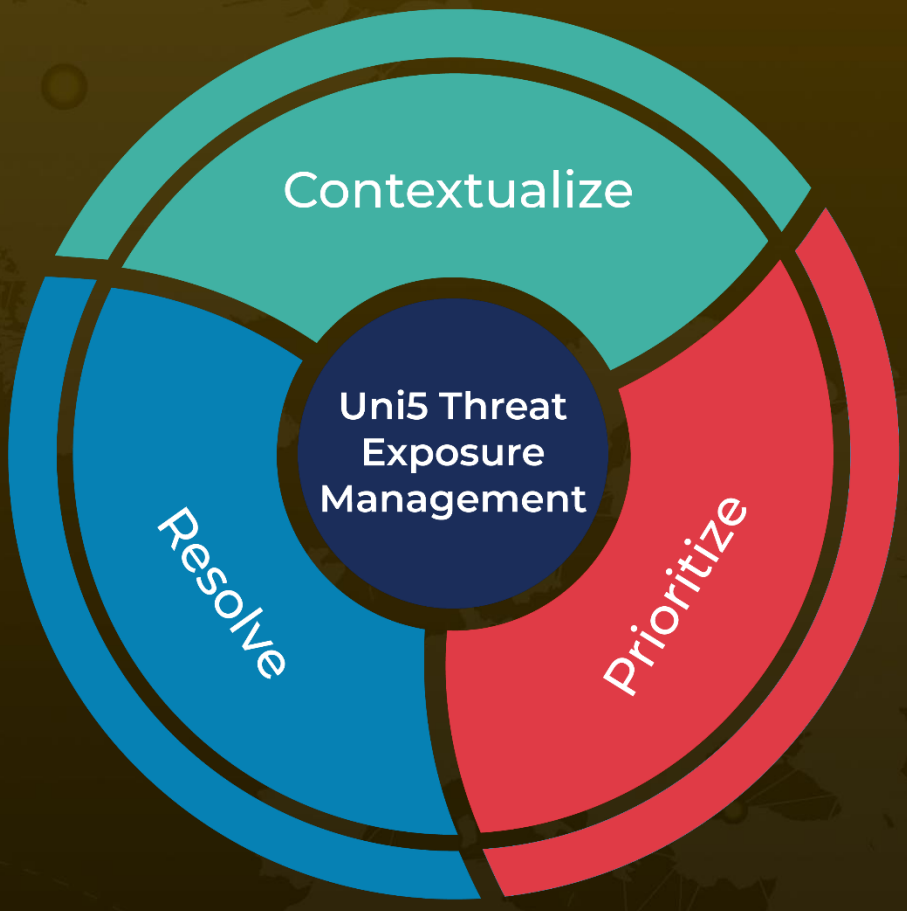
References

https://securelist.ru/purerat-attacks-russian-organizations/112619/

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

May 23, 2025 • 4:50 AM

More at www.hivepro.com