Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

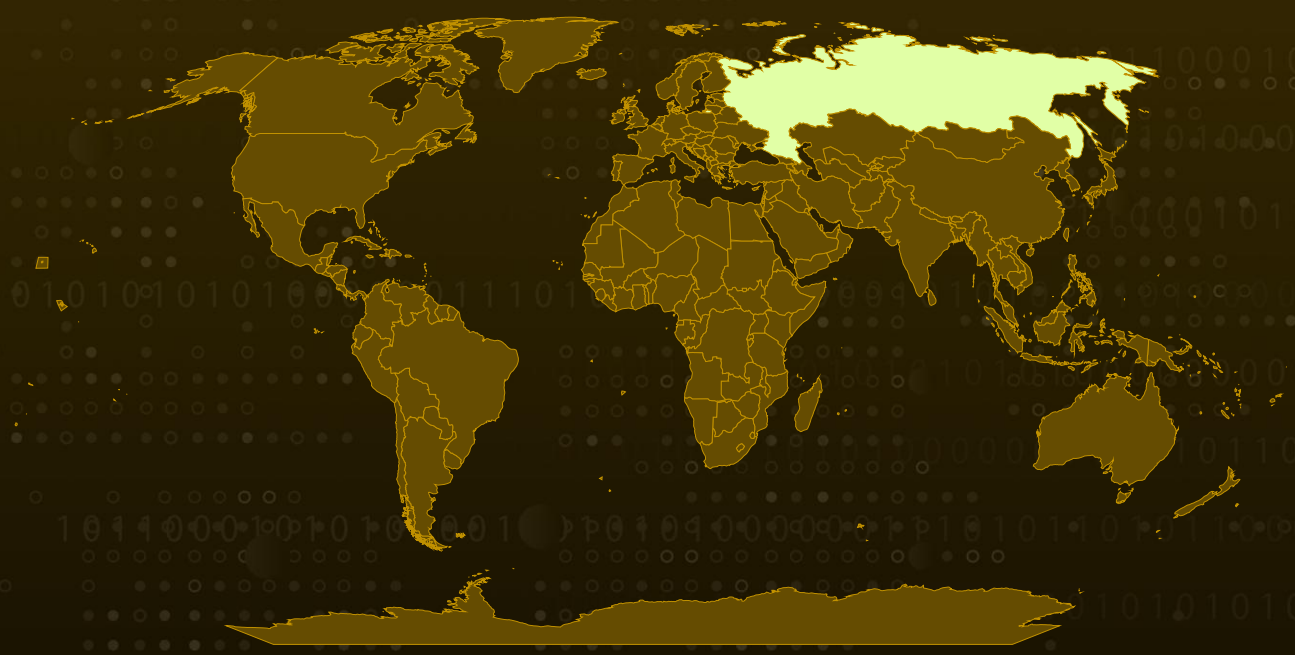
Batavia Multi-Stage Spyware Campaign Targeting Russian Industrial Sector

Date of Publication	Admiralty Code	TA Number
July 11, 2025	A1	TA2025213

Summary

First Seen: July 2024
Targeted Region: Russia
Malware: Batavia Spyware
Affected Platform: Windows
Targeted Industry: Industrial Enterprises
Attack: Batavia is a newly identified Windows spyware strain that emerged in July 2024 and has been actively targeting Russian industrial enterprises through a sophisticated, multi-stage phishing campaign. The operation is ongoing as of July 2025 and has affected over 100 users at several dozen organizations.

Attack Regions



Attack Details

#1

Batavia is a newly discovered Windows spyware that has been actively targeting Russian industrial enterprises since at least July 2024. The campaign uses highly targeted phishing emails, often disguised as contract or business-related communications, to lure victims into downloading malicious Visual Basic Encoded (.VBE) scripts. These emails typically appear to come from legitimate sources and contain links that, when clicked, initiate a multi-stage infection process designed to steal sensitive corporate data.

#2

The infection chain begins when a victim clicks the link in the phishing email, which downloads an archive containing a malicious .VBE script. Once executed, this script profiles the infected system and sends information to the attackers' command-and-control (C2) server. It then downloads the next-stage payload, a Delphi-based executable called WebView.exe, which displays a fake contract document as a decoy while secretly collecting system logs, office documents, and screenshots. The collected data is exfiltrated to a separate C2 server, and the malware further downloads an additional component, javav.exe, to expand its data theft capabilities.

#3

Javav.exe, written in C++, broadens the scope of the attack by targeting a wider variety of files, including images, emails, presentations, archives, and text documents. It uses file hashing to avoid redundant uploads and establishes persistence by creating a shortcut in the Windows startup folder, ensuring it runs on every reboot. There are indications of a possible fourth-stage payload, windowsmsg.exe, which may further extend the malware's capabilities, but details about this component remain unknown.

#4

As of early July 2025, more than 100 infected users have been confirmed, all located within Russian organizations. Given the targeted nature of the campaign and its modular design, the Batavia spyware could be adapted to target other regions or sectors with minimal modification.

Recommendations

Restrict Script-Based Execution: Block execution of script-based file formats such as .vbe, .vbs, .js, and .hta through endpoint protection policies and Group Policy Objects (GPO). These files are frequently used for initial payload delivery in phishing campaigns and are not required in most business environments. Implement application whitelisting (e.g., AppLocker, WDAC) to prevent unauthorized binaries such as WebView.exe and javav.exe from executing.

Harden Endpoints and Monitor for Persistence: Deploy EDR or XDR solutions capable of detecting registry-based persistence, UAC bypass attempts, and the use of dual-purpose tools like wscript.exe and cmd.exe. Monitor for suspicious creation of scheduled tasks and unauthorized autorun entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Alert on parent-child process anomalies involving scripting engines and unknown executables.

Strengthen Email Security and User Awareness: Ensure that email gateways are configured to detect and quarantine spear-phishing messages with encoded script attachments. Implement attachment filtering to block high-risk file types, and use URL sandboxing for links embedded in contract-themed lures. Conduct regular phishing simulation exercises to increase user awareness of socially engineered messages designed to impersonate business communications.

Network Segmentation and Traffic Control: Segment high-value systems from general user networks to limit lateral movement. Apply strict firewall policies to block outbound traffic to known Batavia command-and-control domains such as ru-exchange[.]com. Inspect DNS logs and network telemetry for anomalous connections or encrypted data flows originating from suspicious processes or hosts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0010 Exfiltration
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0005 Defense Evasion
T1566.001 Spearphishing Attachment	T1566 Phishing	T1059 Command and Scripting Interpreter	T1071 Application Layer Protocol
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information	T1059.005 Visual Basic
T1204 User Execution	T1204.001 Malicious Link	T1082 System Information Discovery	T1083 File and Directory Discovery
T1005 Data from Local System	T1113 Screen Capture	T1104 Multi-Stage Channels	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	FC5B89A0A042291020FC62020E000C4D29B42CF425BA161057B3495D561F5390, 628D2B7D9E70DC8C6042671433009BD46FFD96BF55950B5D7B462F4275CE4F88, 294EF6C3EBBE88EA82E5F35E5A1A5F99C067577905EA7A955F969E9D669E001D
MD5	2963FB4980127ADB7E045A0F743EAD05, 5CFA142D1B912F31C9F761DDEFB3C288, 03B728A6F6AAB25A65F189857580E0BD

TYPE	VALUE
Domains	oblast-ru[.]com, ru-exchange[.]com

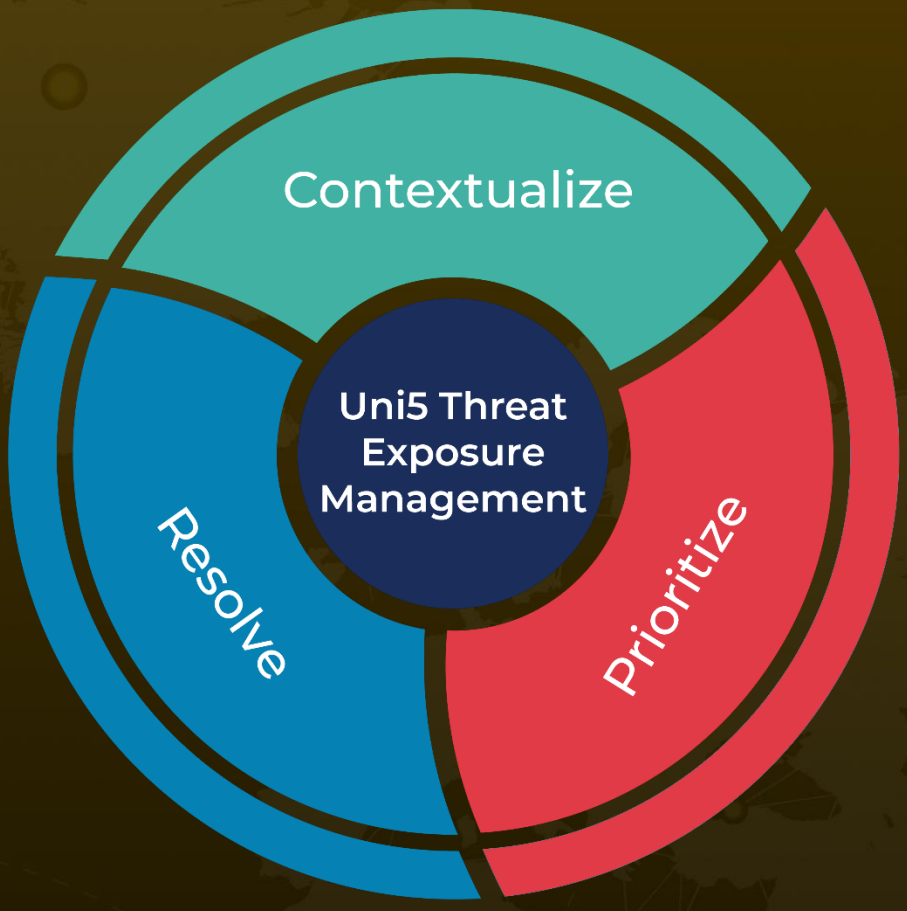
References

https://securelist.com/batavia-spyware-steals-data-from-russian-organizations/116866/

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

July 11, 2025 • 2:30 PM

More at www.hivepro.com