Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

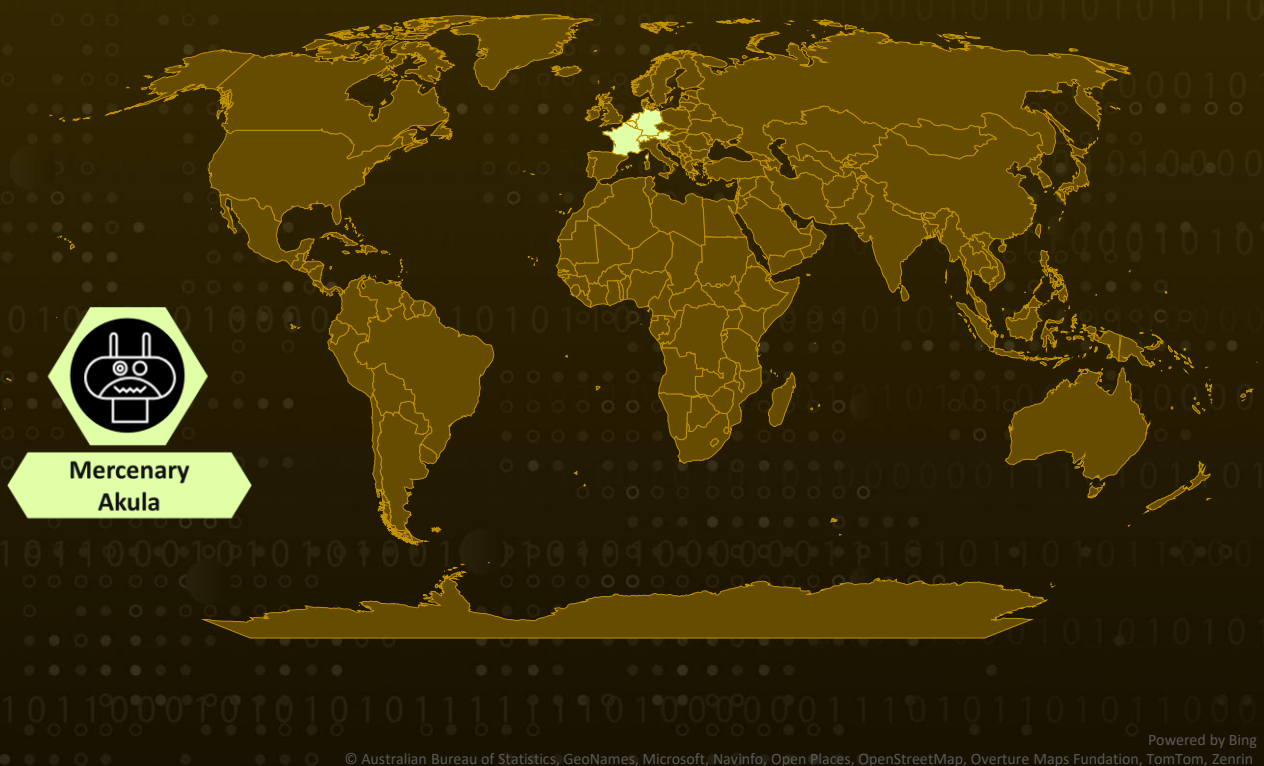
Mercenary Akula’s Court-Themed Campaign Hits European Finance

Date of Publication	Admiralty Code	TA Number
February 25, 2026	A1	TA2026055

Summary

First Seen: February 9, 2026
Targeted Regions: Western Europe
Targeted Platforms: Windows
Targeted Industries: Financial Services
Threat Actor: Mercenary Akula (aka UAC-0050, DaVinci Group, Fire Cells Group)
Attack: A Russia-aligned cyber threat group, Mercenary Akula (UAC-0050), conducted a targeted spear-phishing attack against a European financial institution involved in regional development and reconstruction initiatives supporting Ukraine. The attack spoofed a Ukrainian judicial domain to deliver an email containing a link to a remote access payload hosted on PixelDrain. The campaign employed a multi-layered archive chain culminating in the deployment of Remote Manipulator System (RMS), a legitimate Russian remote administration tool, to establish persistent and stealthy access to the victim's environment for likely intelligence gathering or financial theft.

Attack Regions



Attack Details

#1 On February 9, 2026, a highly targeted social engineering campaign was uncovered against a European financial institution involved in regional development and reconstruction initiatives. The operation has been attributed to Mercenary Akula, also tracked as UAC-0050, DaVinci Group, and Fire Cells Group. The attackers initiated the intrusion through a carefully crafted spear-phishing email referencing an alleged request from the Chernihiv Administrative Court. The message was sent from a spoofed Ukrainian judicial domain. Specifically, it targeted a senior legal and policy advisor responsible for procurement, an individual with privileged visibility into internal financial processes and institutional decision-making. A related sample revealed another spoofed sender address impersonating a security company based in Suceava, Romania. The phishing email directed the recipient to download an archive hosted on PixelDrain, a public file-sharing platform that this threat actor frequently abuses to circumvent reputation-based detection mechanisms.

#2 The downloaded archive, titled in Ukrainian to resemble an official electronic court request dated February 9, 2026, was designed with a multi-layered obfuscation chain to evade security controls. The initial ZIP archive contained a RAR file, which in turn held a password-protected 7-Zip archive. The final payload was an executable disguised as a PDF document using the common double-extension technique (*.pdf.exe). Once executed, the file launched an MSI installer deploying Remote Manipulator System (RMS), a legitimate remote administration tool developed by the Russian company TektonIT. Technical inspection of the MSI package revealed embedded Windows Installer properties referencing the RMS vendor domain, confirming the abuse of legitimate software. By leveraging living-off-the-land remote administration tools, the attackers gained persistent and stealthy remote access while reducing the likelihood of detection by traditional antivirus solutions.

#3 Indicator analysis from the same campaign timeframe shows that the judicial-themed lure was only one facet of a broader, coordinated phishing effort. The threat actor also distributed emails impersonating notifications related to M.E.Doc, a Ukrainian accounting software platform previously weaponized in regional cyber operations. This thematic pivot underscores the group's familiarity with operational technologies commonly used by financial departments. By targeting accountants and financial officers, the attackers align their tactics with Mercenary Akula's established objective of rapid financial theft.

#4 This incident marks a significant shift in Mercenary Akula's operational scope. Historically, the group has focused primarily on Ukrainian organizations, particularly those in financial and accounting roles. However, the targeting of a European institution supporting Ukrainian reconstruction efforts suggests strategic expansion beyond domestic Ukrainian entities. CERT-UA assesses UAC-0050 as a mercenary-aligned threat cluster with links to Russian law enforcement interests, conducting data collection, financial theft, and influence operations under the Fire Cells brand. The group consistently abuses commercially available remote administration tools such alongside remote access trojans. While their tooling remains relatively consistent, their social engineering narratives continue to evolve, demonstrating adaptability in tailoring lures to new geographic and institutional targets.

Recommendations

Block Known Sender Domains Used in Lures: Add the spoofed sender domains chernigiv-rada[.]gov[.]ua and rpgsuceava[.]ro to email gateway blocklists. Implement SPF, DKIM, and DMARC validation to detect and quarantine spoofed emails impersonating government and institutional domains.

Restrict PixelDrain and Public File-Sharing Services: Block or monitor access to PixelDrain and related file-sharing platforms (qaz[.]im, qaz[.]is, qaz[.]su, Bitbucket) at the web proxy or firewall level, particularly for users in finance, legal, and procurement roles who are primary targets of this campaign.

Enforce Application Whitelisting for Remote Access Tools: Deploy application control policies to prevent unauthorized installation or execution of remote administration software including RMS (Remote Manipulator System), LiteManager, and Remote Utilities. Alert on any MSI installer activity referencing rmansys[.]ru or TektonIT-associated binaries.

Harden Email Security Against Multi-Layered Archive Delivery: Configure email gateways and endpoint protection to scan nested archives (ZIP containing RAR containing 7-Zip) and flag or quarantine password-protected archives. Implement policies to block executable files with double extensions (e.g., .pdf.exe) at the email gateway and endpoint level.

Monitor for RMS and Related Remote Access Tool Indicators: Deploy detection rules for RMS-specific network signatures, process creation events associated with RMS binaries, and MSI installer activity. Monitor for outbound connections to known RMS command-and-control infrastructure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1589: Gather Victim Identity Information	T1589.003: Employee Names
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Execution	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1036: Masquerading	T1036.007: Double File Extension
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1562: Impair Defenses	T1562.004 : Disable or Modify System Firewall
	T1672: Email Spoofing	
Command and Control	T1219: Remote Access Software	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f5ab8640a0ae68f25dcd0a7461266a46322f01a790fec8dafe7ec32a535e5d8e, 98ba3d70d71d6264ec9cb442338c05fa368f6d0aa5e2c67a6e06356adcd6a028, 42de03e314c4c9fd69cb042833e8d25950b0a842c28e9b2e18f363c843a9d283, 8c675f69537341aac4857f6d6278109177829a47ee65cf90e073ecc274ba1527, d9e1a79bd2aef55b73b9d4cbc7983a77f918ea6fc344ab9c59e35bc8afaaff6f, b275f1c64aa21d0d455920f0e663ff222729b068e58e105e0952cebe6a99bf0f, 4f20691c7890e20af642763d030c608a96a84182e44c902aaa89d4f1394dac0a, 17248c87d1b895d23d1391caa2ea258bbcce8c6609490912b5efc226a4c1ac49, cd652cb4dcbc0c077bc4772fde6e7654be399517879201b820147abb58d2b9bd, a939d79a9908744169247b4ca65ab256290f52a3bded15f541eebb668dea48be, 9b61bb9374de332fd80909f30d102043befcd569d264715b0a4d5d5a8d0762d3, b7dd90ee36e52033ae2386edb9e2d8b1ce4559b1defaf87ee57c88b41bba7f66, 3d99abebdc72cd840ff42b3a5b4cf6e8e3a50616881097d0ceb058f87d2b3909, 9900e3bc74c9dc9886d8e5c4395700d0b1b1533f51ac763fa157a7307c333ab6, 761d4add56e0766e7e6314950d5cf4ebf759d43c75e74375c2a65f29040dd6fd, 0c2e71612aa0d9c56393d8eb18d6446ad709cb40e856fcde21754d6845407055, 28926919956c3e3f281f504c45dfe3419d4f37683806f76393f2a7c6d6e1abfa, f902b8a547c705d736ced5e6c6db5e9a34da09940d08be37303b34797afebdca, 690ee1907bfb425a791e255eabe7351903e8a9e92089a099997afa2a8070383b
Domains	pixeldrain[.]com, rmansys[.]ru

TYPE	VALUE
URL	hxxps[:]//rmansys[.]ru/IS_PREVENT_DOWNGRADE_EXITZ_DOWNGRADE_DETECTED;Z_UPGRADE_DETECTED;COMPANYNAME;INSTALLDIR;ISFOUNDNEWERPRODUCTVERSION;ISX_SERIALNUM;SUPPORTDIR;USERNAME;integrate_firewall;IS_SQLSERVER_LIST;LAUNCHPROGRAM1;LAUNCHPROGRAM;INTEGRATE_FIREWALL1;PRINTER_INSTALL;REMOVE_SETTINGS;INTEGRATE_FIREWALL;SHOW_SETTINGS;MONITOR_DRIVERSecureCustomPropertiesALLUSERSCEBB978F0EDBD74FE9ACC7FF3E6B978FBEBB908FDEAB97CFCEBBB00FF97CE7DFC9FCB73F49ACDWUSLINKLaunchPROGRAMFILETOLAUNCHATEND{&Tahoma8}

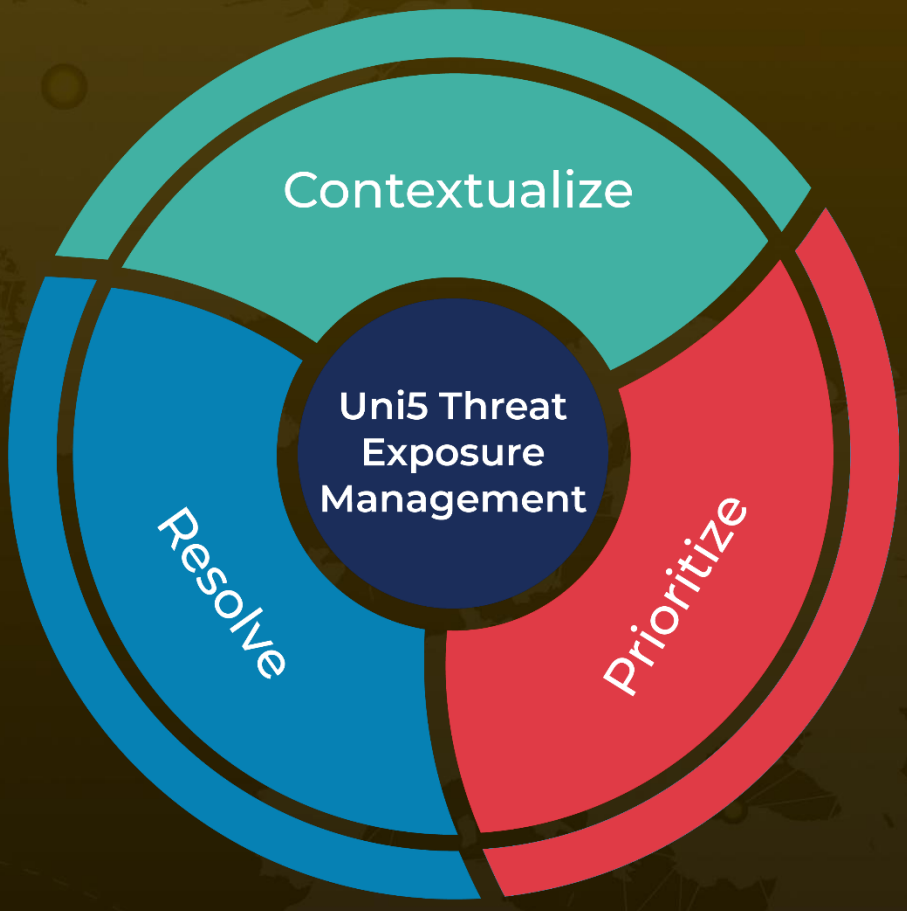
References

https://www.bluevoyant.com/blog/mercenary-akula-hits-financial-institution

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 25, 2026 • 7:30 AM

More at www.hivepro.com