Mercenary Akula Hits Ukraine-Supporting Financial Institution

By Patrick McHale and Joshua Green

Archived: 2026-04-05 14:58:26 UTC

February 24, 2026 | 6 min read

What Happened?

BlueVoyant's Security Operations Center (BVSOC) recently identified and responded to a targeted social engineering attack on a European financial institution involved in regional development and reconstruction initiatives. The attack exhibits hallmarks of activity attributed to the Russia-aligned Mercenary Akula (tracked by CERT UA as UAC-0050), a financially motivated mercenary entity also linked to cyber espionage and psychological operations. The attack spoofed a Ukrainian judicial domain to deliver an email containing a link to a remote access payload. The target was a senior legal and policy advisor involved in procurement, a role with privileged insight into institutional operations and financial mechanisms. This targeting highlights the adversary's likely intent to conduct intelligence gathering or financial theft. Notably, this activity suggests the adversary may be expanding beyond the primarily Ukraine-based targeting cited in previous OSINT reporting.

On February 9, 2026, BVSOC observed a spearphishing email sent to the targeted user. The email, with the subject "*Request from the Chernihiv Administrative Court for Case #81435126*," originated from *4ml@chernigiv-rada[.]gov[.]ua*. The email directed the recipient to download an archive file hosted on the public file-sharing service Pixeldrain, a tactic frequently used in Mercenary Akula campaigns to bypass reputation-based security controls. In a separate sample recovered from research (pictured below), the email appeared to come from *florin[.]musteata[@]rpgsuceava[.]ro*, another spoofed sender domain appearing to originate from an employee with Real Protection Guard (RPG) Suceava, a security and protection company based in Suceava, Romania.


Figure 1

The archive, named *Електронний судовий запит №837744-8-2026 від 09.02.2026 — 865.zip*, employed a layered obfuscation chain. The ZIP archive contained a nested RAR which contained a password-protected 7-Zip file, with the password conveniently provided in an accompanying *Код.txt* (translated: Code.txt) file. Opening the .txt file reveals the text, "*З метою інформаціоного захисту вставлено код доступ:: 5847395844*", which translates loosely as "Information protected with the established access code: 5847395844". This multi-stage extraction process is a known evasion technique designed to defeat automated scanning and condition the user into normalizing suspicious activity.


Figure 2

The final payload was an executable file, *Електронний судовий запит №837744-8-2026 від 09.02.2026.pdf.exe*, masquerading as a PDF document through a double-extension trick. Upon execution, it deployed an MSI installer for the Remote Manipulator System (RMS), a legitimate remote administration tool developed by the Russian company TektonIT. This aligns with consistent reporting on Mercenary Akula, which frequently abuses commercially available remote access software like RMS, LiteManager, and Remote Utilities as well as remote access tools/trojans Remcos, QuasarRAT and others. The use of such "living-off-the-land" tools provides attackers with persistent, stealthy access while often evading traditional antivirus detection.

Technical analysis of the executables and MSI packages identified an embedded string resembling Windows Installer properties for Remote Manipulator System (RMS), presented as a pseudo-URL referencing the vendor domain *rmansys[.]ru*. This is not a live web link but rather a list of parameters likely used to preconfigure an MSI-driven installation. The strings include options such as INSTALLDIR, INTEGRATE_FIREWALL, LAUNCHPROGRAM, SHOW_SETTINGS, MONITOR_DRIVER, and ISX_SERIALNUM, indicating an intent to install a legitimate remote administration tool with predefined settings and minimal user interaction.

> *hxxps[:]//rmansys[.]ru/IS_PREVENT_DOWNGRADE_EXITZ_DOWNGRADE_DETECTED;Z_UPGRADE_DETECTED;COMPANYNAME;INSTALLI*

While the TFC did not observe direct outbound connections to RMS infrastructure, the presence of serial identifiers and long hexadecimal tokens suggests the installer is prepared for remote connectivity. This configuration baked into the installer enables rapid deployment of a remote access capability and can facilitate persistence and firewall adjustments consistent with "silent" or unattended installation behavior.

Analysis of related indicators from the same period reveals that this specific 'court request' lure is part of a campaign employing multiple, tailored social engineering themes; a campaign likely ongoing for years. In this latest iteration, the threat actor simultaneously utilizes lures impersonating Ukrainian judicial bodies and, more critically, notifications related to 'M.E.Doc,' a Ukrainian accounting software package historically exploited as a major attack vector in the region. The use of M.E.Doc-themed lures indicates the adversary has specific knowledge of the operational software used by target organizations and is directly targeting financial and accounting personnel. This approach aligns with Mercenary Akula's

primary objective of financial theft. CERT-UA has previouslywarned that accountants compromised via such lures can be used to initiate fraudulent bank transfers within hours of infection. This multi-pronged social engineering strategy demonstrates a sophisticated and adaptable threat focused on gaining remote access to systems from which sensitive financial or legal information can be extracted or direct financial fraud can be executed.

This campaign is not an isolated event but a manifestation of Mercenary Akula's mature, persistent, and highly adaptable operational model. Historical CERT-UA assessments describe the group as a mercenary entity associated with Russian law enforcement and operating with the speed and precision of access brokers. Complementary open-source analysis by BushidoToken further profiles Mercenary Akula under the 'DaVinci Group/Agency DaVinci' branding, noting ties to Russian law enforcement and an initial access broker-style role. In parallel, CERT-UA attributes the actor's psychological/information operations to the 'Fire Cells Group' persona, which has conducted bomb-threat campaigns against Ukrainian embassies and media—an assessment corroborated by Recorded Future's reporting.


Figure 3

This attack reflects Mercenary Akula's well established and repetitive attack profile, while also offering a notable development. The group's operations consistently converge on several defining characteristics, as documented across numerous campaigns from 2023 through 2026. First, their targeting has been primarily focused on Ukraine-based entities, especially accountants and financial officers. However, this incident suggests potential probing of Ukraine-supporting institutions in Western Europe. Their psychological operations had already exhibited global reach through bomb-threat campaigns targeting Ukraine embassies and associated media. Second, their social engineering leverages a rotating portfolio of highly credible, localized lures, impersonating Ukrainian courts, the National Bank of Ukraine (NBU), the State Tax Service, and business software like M.E.Doc to exploit institutional trust. Third, their technical execution relies on abusing legitimate infrastructure and tools: they distribute multi-layered archives via public file-sharing services (Pixeldrain, qaz[.]im, qaz[.]is, qaz[.]su, Bitbucket, etc.) and deploy signed, commercial remote administration software as backdoors. Finally, their objectives are dual-purpose and rapid, blending financial theft—with funds sometimes stolen within an hour of infection—with cyber espionage.

Conclusion

The attempted breach underscores Mercenary Akula (a.k.a. UAC-0050, DaVinci Group, Fire Cells Group), status as a persistent and capable threat to organizations operating in Ukraine. It also signals a potential expansion into Ukraine-supporting institutions outside the country. By mirroring the group's long-established tactics—localized social engineering, multi-stage payload delivery, and the deployment of signed remote administration tools—this incident is a stark reminder of their operational consistency and focus on high-value financial and intelligence targets.

For potential targets, especially financial and development institutions, this analysis reinforces the necessity of a defense-in-depth strategy. This should include heightened user awareness of region-specific lures, improved email filtering for complex archives, strict application control policies to block unauthorized remote access software, and enhanced financial transaction authentication that cannot be bypassed through endpoint compromise. Vigilance against this predictable yet effective threat profile is a key component of regional cybersecurity posture.

MITRE ATT&CK Techniques

T1566.002 (Spearphishing Link)

T1560.001 (Archive via Utility)

T1036.007 (Double File Extension)

T1219 (Remote Access Tools)

T1218.011 (Rundll32)

T1071.001 (Web Protocols)

T1204.002 (Malicious File)

T1547.001 (Registry Run Keys/Startup Folder)

T1562.004 (Disable or Modify System Firewall)

T1027.013 (Encrypted/Encoded File)

T1102 (Web Service)

T1672 (Email Spoofing)

Indicators

f5ab8640a0ae68f25dcd0a7461266a46322f01a790fec8dafe7ec32a535e5d8e

98ba3d70d71d6264ec9cb442338c05fa368f6d0aa5e2c67a6e06356adcd6a028

42de03e314c4c9fd69cb042833e8d25950b0a842c28e9b2e18f363c843a9d283

8c675f69537341aac4857f6d6278109177829a47ee65cf90e073ecc274ba1527

d9e1a79bd2aef55b73b9d4cbc7983a77f918ea6fc344ab9c59e35bc8afaaff6f

b275f1c64aa21d0d455920f0e663ff222729b068e58e105e0952cebe6a99bf0f

4f20691c7890e20af642763d030c608a96a84182e44c902aaa89d4f1394dac0a

17248c87d1b895d23d1391caa2ea258bbcce8c6609490912b5efc226a4c1ac49

cd652cb4dcbc0c077bc4772fde6e7654be399517879201b820147abb58d2b9bd

a939d79a9908744169247b4ca65ab256290f52a3bded15f541eebb668dea48be

9b61bb9374de332fd80909f30d102043befcd569d264715b0a4d5d5a8d0762d3

b7dd90ee36e52033ae2386edb9e2d8b1ce4559b1defaf87ee57c88b41bba7f66

3d99abebdc72cd840ff42b3a5b4cf6e8e3a50616881097d0ceb058f87d2b3909

9900e3bc74c9dc9886d8e5c4395700d0b1b1533f51ac763fa157a7307c333ab6

761d4add56e0766e7e6314950d5cf4ebf759d43c75e74375c2a65f29040dd6fd

0c2e71612aa0d9c56393d8eb18d6446ad709cb40e856fcde21754d6845407055

28926919956c3e3f281f504c45dfe3419d4f37683806f76393f2a7c6d6e1abfa

f902b8a547c705d736ced5e6c6db5e9a34da09940d08be37303b34797afebdca

690ee1907bfb425a791e255eabe7351903e8a9e92089a099997afa2a8070383b

pixeldrain[.]com

rmansys[.]ru

hxxps[:]//rmansys[.]ru/IS_PREVENT_DOWNGRADE_EXITZ_DOWNGRADE_DETECTED;Z_UPGRADE_DETECTED;COMPANYNAME;INSTAI
