UAC-0215 Phishing Campaign Targets Ukraine's Critical Sectors

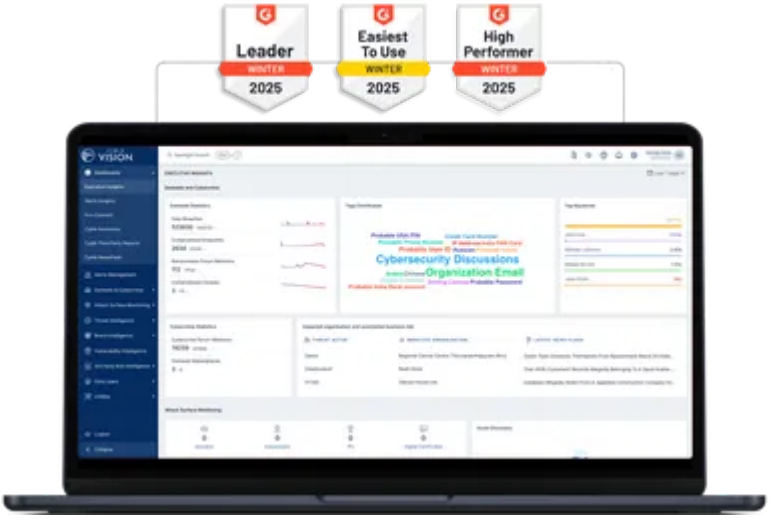
Published: 2024-10-29 · Archived: 2026-04-05 16:22:42 UTC

Threat actor UAC-0215 launches a phishing campaign threatening Ukraine's public, industrial, and military sectors.

Overview

CERT-UA, the Cyber Emergency Response Team for Ukraine, uncovered a phishing campaign orchestrated by the threat actor UAC-0215. This campaign specifically targeted public institutions, major industries, and military units across Ukraine.

The phishing emails were cleverly disguised to promote integration with popular platforms like Amazon and Microsoft, as well as advocating for Zero Trust Architecture (ZTA). However, the emails contained malicious .rdp configuration files that, when opened, established a connection to an attacker-controlled server.



This connection provided unauthorized access to a variety of local resources, including disk drives, network assets, printers, audio devices, and even the clipboard. The sophistication of this campaign raises security concerns for critical infrastructure in Ukraine.

Campaign Overview

The campaign was first detected on October 22, 2024, with intelligence suggesting that the preparatory groundwork was laid as early as August 2024. The phishing operation’s extensive reach highlights not only a localized threat but also a broader international concern, as multiple cybersecurity organizations worldwide have corroborated it. The implications of this attack extend beyond individual organizations, threatening national security.

The primary targets of the phishing campaign include public authorities, major industries, and military organizations within Ukraine. This operation is assessed to have a high-risk score, indicating a threat to these sectors. The campaign is attributed to the advanced persistent threat (APT) group known as UAC-0215, utilizing rogue Remote Desktop Protocol (RDP) techniques.

Technical Details

The phishing campaign attributed to UAC-0215 utilizes rogue Remote Desktop Protocol (RDP) files to infiltrate key Ukrainian institutions. The malicious emails are designed to appear legitimate, enticing recipients to open attachments that ultimately compromise their systems. When a victim unwittingly opens the .rdp configuration file, it connects their computer to the attacker's server, granting extensive access to critical local resources, including:

1. Disk Drives
2. Network Resources
3. Printers
4. COM Ports
5. Audio Devices
6. Clipboard
7. This access allows the attackers to execute unauthorized scripts and programs, further compromising the system.

Conclusion

The intelligence gathered suggests that the UAC-0215 campaign extends beyond Ukrainian targets, indicating a potential for broader cyberattacks across multiple regions, especially amid heightened tensions in the area, including recent cyberattacks on Ukraine that have garnered international concern.

This campaign highlights the growing sophistication of phishing tactics employed against Ukraine, as the attackers exploited RDP configurations to gain significant control over critical systems within public and industrial sectors, jeopardizing sensitive information and operational integrity.

Recommendations and Mitigations

To mitigate the risks posed by UAC-0215 and similar threats, organizations are advised to implement the following strategies:

- Establish better filtering rules at the mail gateway to block emails containing .rdp file attachments. This measure is critical in reducing exposure to malicious configurations.
- Limit users' ability to execute .rdp files unless specifically authorized. This precaution will minimize the risk of accidental executions that could lead to breaches.
- Configure firewall settings to prevent the Microsoft Remote Desktop client (mstsc.exe) from establishing RDP connections to external, internet-facing resources. This step will thwart unintended remote access and reduce the potential for exploitation.
- Utilize Group Policy to disable resource redirection in RDP sessions. By setting restrictions under "Device and Resource Redirection" in Remote Desktop Services, organizations can prevent attackers from accessing local resources during RDP sessions.
