Rewterz Threat Update - Pro-Ukraine Hacktivists Breach Russian ISP as Revenge for KyivStar Attack - Rewterz

Published: 2024-01-11 · Archived: 2026-04-05 12:37:55 UTC

Severity

High

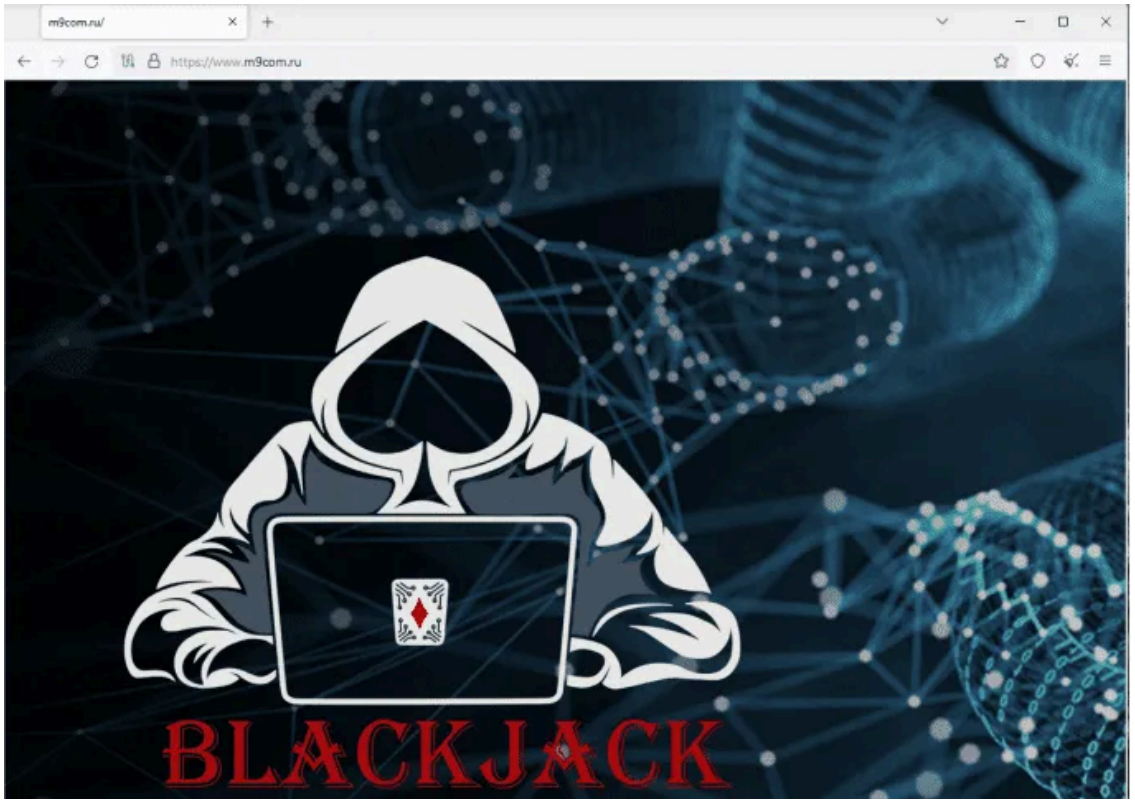
Analysis Summary

In the heat of the ongoing Russia-Ukraine cyberwarfare, a hacktivist group supporting Ukraine named ‘Blackjack’ has recently claimed a cyberattack against Russian internet service provider M9com as a response to the attack against Kyivstar, which is Ukraine’s largest telecom company.

Kyivstar’s services were disrupted to a severe degree in December 2023, later to be revealed that it was caused due to a cyberattack from Russian threat actors. An investigation by Ukraine’s security organizations showed that the Russian attackers initially intruded on Kyivstar in May 2023 and had been preparing for the attack since then. The attack resulted in the wiping of thousands of virtual computers and servers.

A few days ago, the Blackjack threat actor group announced on Telegram that they had breached into M9com, one of the largest internet service providers (ISP) in Moscow. The hacktivists claimed that they stole sensitive data from the company along with disrupting M9com’s internet services. They also shared a Tor URL for three ZIP archives containing images to prove their access to M9com’s systems, 50GB of call data, and account credentials of several customers and employees.

Various screenshots also show FTP command execution used to delete server files, remove configuration files, wipe backup data, a screenshot of the vSphere client, the RIPE billing portal and database, and the dashboard for the Resource Public Key Infrastructure (RPKI). Some leaked files have full names, usernames, email addresses, and passwords in cleartext form, along with other sensitive data. Blackjack also defaced the official website of M9com.



M9com has not given any public statement on the authenticity and validity of the leaked data. On the other hand, Blackjack has posted a public message promising that this is just one of the many attacks they are planning to launch as revenge for the Kyivstar breach.

Many pro-Russian hacktivists are aiming to take down services in distributed denial-of-service attacks, but the activity Blackjack group has carried out shows a much greater impact because recovery from wiped servers proves to be very difficult when the backups are also destroyed. According to a source from Ukraine's law enforcement agencies, the Blackjack group may be related to the Security Service of Ukraine (SBU). They managed to delete 20 TB of data during the cyberattack.

Impact

- Data Loss
- Sensitive Information Theft
- Web Defacement

Remediation

- Implement multi-factor authentication (MFA) on all accounts to add an extra layer of security to login processes.
- Consider the use of phishing-resistant authenticators to further enhance security. These types of authenticators are designed to resist phishing attempts and provide additional protection against social engineering attacks.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.

- Organizations need to stay vigilant and follow best practices for cybersecurity to protect their systems and data from potential threats. This includes regularly updating software and implementing strong access controls and monitoring tools.
- Develop a comprehensive incident response plan to respond effectively in case of a security breach or data leakage.
- Maintain regular backups of critical data and systems to ensure data recovery in case of a security incident.
- Adhere to security best practices, including the principle of least privilege, and ensure that users and applications have only the necessary permissions.
- Establish a robust patch management process to ensure that security patches are evaluated, tested, and applied promptly.
- Conduct security audits and assessments to evaluate the overall security posture of your systems and networks.
- Implement network segmentation to contain and isolate potential threats to limit their impact on critical systems.
- Never trust or open links and attachments received from unknown sources/senders.
