Microsoft Warns of Widespread Credential Stealing Attacks by Russian Hackers

Jun 26, 2023 Ravie Lakshmanan Cyber Threat / Password Security

Microsoft has disclosed that it's detected a spike in credential-stealing attacks conducted by the Russian state-affiliated hacker group known as Midnight Blizzard.

The intrusions, which make use of residential proxy services to obfuscate the source IP address of the attacks, target governments, IT service providers, NGOs, defense, and critical manufacturing sectors, the tech giant's threat intelligence team said.

Midnight Blizzard, formerly known as Nobelium, is also tracked under the monikers APT29, Cozy Bear, Iron Hemlock, and The Dukes.
The group, which drew worldwide attention for the SolarWinds supply chain compromise in December 2020, has continued to rely on unseen tooling in its targeted attacks aimed at foreign ministries and diplomatic entities.

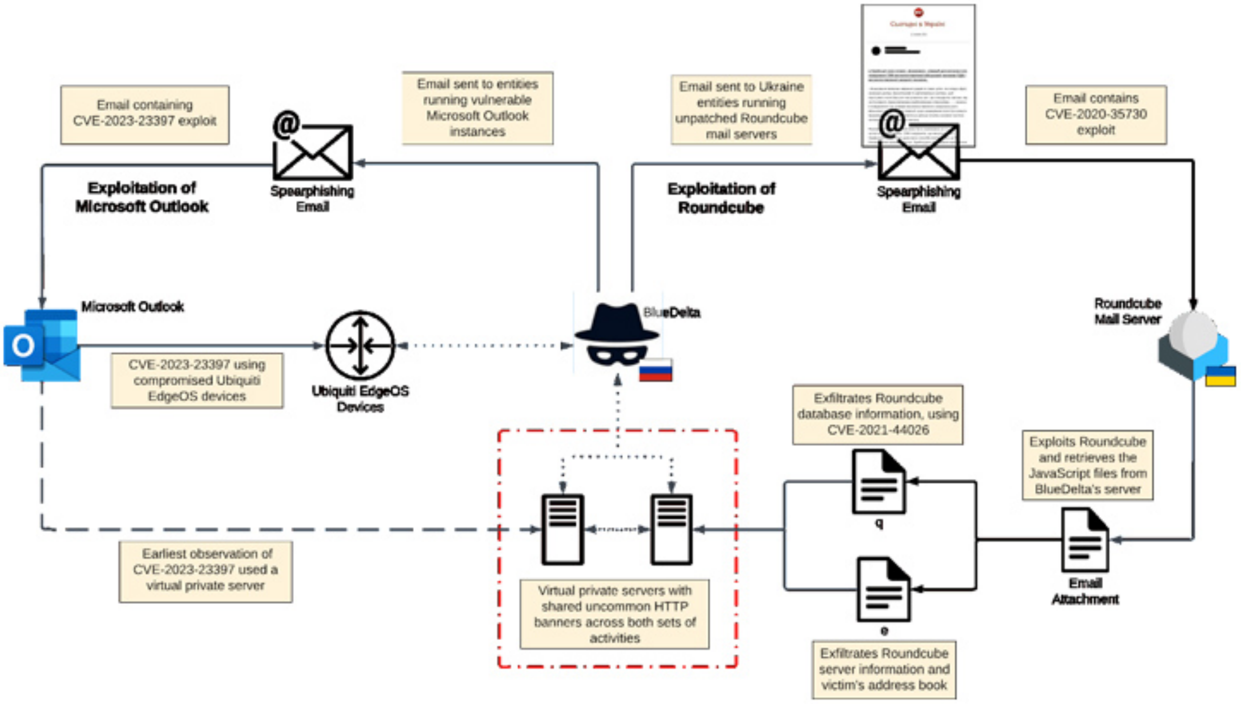
It's a sign of how determined they are to keep their operations up and running despite being exposed, which makes them a particularly formidable actor in the espionage area.

"These credential attacks use a variety of password spray, brute-force, and token theft techniques," Microsoft said in a series of tweets, adding the actor "also conducted session replay attacks to gain initial access to cloud resources leveraging stolen sessions likely acquired via illicit sale."
The tech giant further called out APT29 for its use of residential proxy services to route malicious traffic in an attempt to obfuscate connections made using compromised credentials.

"The threat actor likely used these IP addresses for very short periods, which could make scoping and remediation challenging," the Windows maker said.

The development comes as Recorded Future detailed a new spear-phishing campaign orchestrated by APT28 (aka BlueDelta, Forest Blizzard, FROZENLAKE, Iron Twilight, and Fancy Bear) targeting government and military entities in Ukraine since November 2021.

The attacks leveraged emails bearing attachments exploiting multiple vulnerabilities in the open-source Roundcube webmail software (CVE-2020-12641, CVE-2020-35730, and CVE-2021-44026) to conduct reconnaissance and data gathering.


Email containing CVE-2023-23397 exploit
Exploitation of Microsoft Outlook
Spearphishing Email
Email sent to entities running vulnerable Microsoft Outlook instances
Email sent to Ukraine entities running unpatched Roundcube mail servers
Exploitation of Roundcube
Spearphishing Email
Email contains CVE-2020-35730 exploit
Microsoft Outlook
CVE-2023-23397 using compromised Ubiquiti EdgeOS devices
Ubiquiti EdgeOS Devices
BlueDelta
Roundcube Mail Server
Exfiltrates Roundcube database information, using CVE-2021-44026
Exploits Roundcube and retrieves the JavaScript files from BlueDelta's server
q
Email Attachment
e
Earliest observation of CVE-2023-23397 used a virtual private server
Virtual private servers with shared uncommon HTTP banners across both sets of activities
Exfiltrates Roundcube server information and victim's address book

A successful breach enabled the Russian military intelligence hackers to deploy rogue JavaScript malware that redirected the incoming emails of targeted individuals to an email address under the attackers' control as well as steal their contact lists.

"The campaign displayed a high level of preparedness, quickly weaponizing news content into lures to exploit recipients," the cybersecurity company said. "The spear-phishing emails contained news themes related to Ukraine, with subject lines and content mirroring legitimate media sources."

More importantly, the activity is said to dovetail with another set of attacks weaponizing a then-zero-day flaw in Microsoft Outlook (CVE-2023-23397) that Microsoft disclosed as employed by Russia-based threat actors in "limited targeted attacks" against European organizations.

The privilege escalation vulnerability was addressed as part of Patch Tuesday updates rolled out in March 2023.

The findings demonstrate Russian threat actors' persistent efforts in harvesting valuable intelligence on various entities in Ukraine and across Europe, especially following the full-scale invasion of the country in February 2022.

The cyberwarfare operations aimed at Ukrainian targets have been notably marked by the widespread deployment of wiper malware designed to delete and destroy data, turning it into one of the earliest instances of large-scale hybrid conflict.

"BlueDelta will almost certainly continue to prioritize targeting Ukrainian government and private sector organizations to support wider Russian military efforts," Recorded Future concluded.