Microsoft warns of credential theft attack

Microsoft has just detected a spike in credential theft attacks carried out by the Midnight Blizzard (Russian) hacker group.

According to researchers, the hacker group used residential proxy services to obfuscate the source IP addresses of attacks targeting governments, IT service providers, NGOs, defense and important manufacturing sectors.

Midnight Blizzard was previously known as Nobelium, APT29, Cozy Bear, Iron Hemlock. This group attracted worldwide attention after attacking the SolarWinds supply chain in December 2020, as well as carrying out attacks. Intentional attacks targeting foreign ministries and diplomatic organizations.

"These credential attacks use a variety of password theft, brute-force, and token theft techniques," Microsoft said in a series of tweets.

'The threat actor may have used these IP addresses for very short periods of time, which makes scoping and remediation difficult,' Microsoft said.

Recently, cybersecurity company Recorded Future also revealed a new online phishing campaign orchestrated by APT28 (also known as BlueDelta, Forest Blizzard, FROZENLAKE, Iron Twilight and Fancy Bear) targeting major organizations. government and military in Ukraine since November 2021.

The attacks leveraged emails with 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 collection.

The cyber security firm said: 'The campaign demonstrated a high level of preparation, quickly weaponizing news content into bait to exploit recipients.'

More importantly, this activity is said to be consistent with a series of attacks exploiting a zero-day vulnerability in Microsoft Outlook (CVE-2023-23397) against European organizations.

The privilege escalation vulnerability is currently fixed in the Patch Tuesday patch released in March 2023.