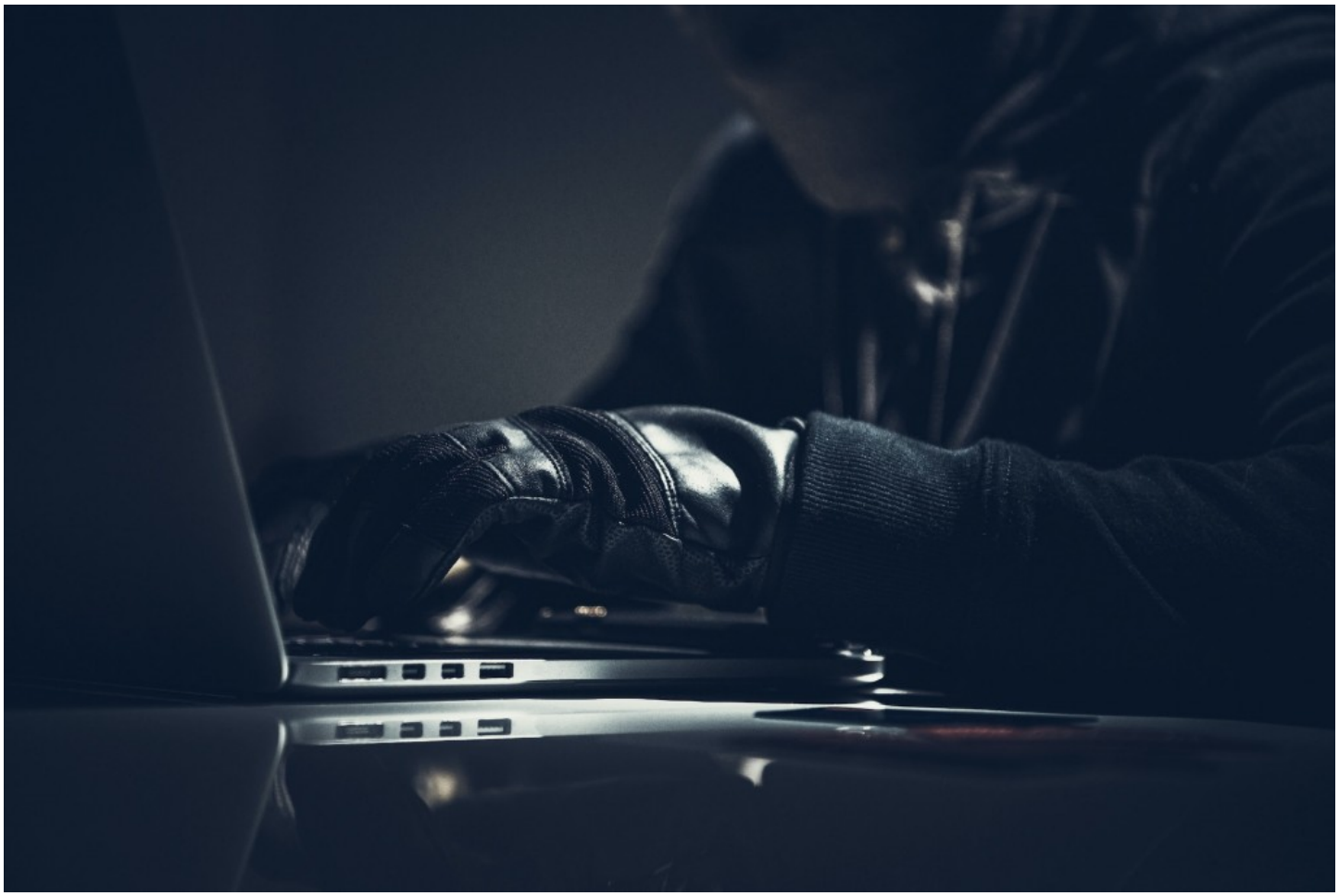
Geeky News Highlights Midnight Blizzard's Latest Attacks Targeting Microsoft Teams Users

The APT Group meticulously orchestrated social engineering attacks employing sophisticated credential theft phishing tactics to bypass the Multi-Factor Authentication (MFA) protection of numerous organisations



Surrey, United Kingdom Aug 24, 2023 (Issuewire.com**)** - Geeky News, a technology and lifestyle journal, has unveiled a disconcerting cybersecurity revelation that underscores the escalating sophistication of digital threats. In an article titled "Microsoft Teams Targeted by Midnight Blizzard APT Group," the journal sheds light on the alarming tactics employed by an Advanced Persistent Threat (APT) group known as Midnight Blizzard. The group has leveraged Microsoft Teams as a vector for targeted phishing attacks.

Microsoft Threat Intelligence has brought to light this unsettling development, revealing that the APT group orchestrated meticulously planned social engineering attacks. By employing intricate credential theft and phishing tactics, the attackers managed to circumvent Multi-Factor Authentication (MFA) protections, thus penetrating the defences of numerous organisations. The report attributes these attacks to the Russian Midnight Blizzard threat actor, a group previously recognised as Nobelium.

The APT group's tactics were quite sophisticated. They exploited Microsoft 365 tenants owned by small businesses that had been compromised in advance. This modus operandi involved renaming the

compromised tenant and introducing a new onmicrosoft.com subdomain, all while creating a new user linked to the domain. These fake tenants and subdomains frequently included security or product-related terms, such as "teamsprotection," "azuresecuritycenter," or "teamsprotection," lending an air of authenticity to their operations.

The attackers initiated their campaign by ingeniously sending Microsoft Teams message requests to targeted company staff members. Once accepted, the recipients would then receive subsequent Teams messages with instructions to input a code into Microsoft Authenticator on their mobile devices. This seemingly innocuous action inadvertently granted the attackers access tokens, providing unauthorised entry into the target user's Microsoft 365 account.

Upon successful breach, the attackers proceeded with post-compromise activities, often involving the pilfering of sensitive data from compromised Microsoft 365 accounts. In some instances, the hackers even ventured to introduce unauthorised devices into organisations, disguising them as managed entities through Microsoft Entra ID, potentially sidestepping access restrictions.

Microsoft reacted swiftly by initiating an investigation into the methods employed by the attackers to compromise legitimate Azure tenants. The software giant has taken proactive steps to dismantle the malicious subdomains used by the threat actors and mitigate the ongoing impact of the campaign. However, the scale of the damage is deeply concerning. Microsoft's comprehensive investigation has revealed that around 40 global organisations have fallen victim to this orchestrated campaign.

The victims of this cyber onslaught span a wide range of sectors, including government agencies, non-government organisations (NGOs), technology firms, IT services, media businesses, and discrete manufacturing companies. Notably, these organisations are primarily based in the US and Europe, highlighting the global reach of this insidious cyberattack.

The campaign's sophistication has left cybersecurity experts astounded, further underscoring the urgency of strengthening defences. The attackers' utilisation of legitimate Microsoft domains as part of their strategy makes it exceedingly difficult for users to identify the deceptive nature of their prompts.

In response to this incident, Microsoft urges organisations prioritising training employees to recognise the dangers posed by social engineering and credential phishing attacks. For enhanced security awareness and an elevated cybersecurity posture, organisations can consider specialised cybersecurity training programs, such as those offered by CultureAI.

Whilst employee training is a pivotal element, Microsoft also advises organisations to enhance their cybersecurity posture. This can be done by deploying phishing-resistant authentication methods and reinforcing the strength of conditional access authentication for mission-critical applications, thereby embracing a multi-faceted approach to security.

To read the full article, please visit: https://www.geekynews.co.uk/microsoft-teams-targeted-by-midnight-blizzard/

Media Contact

Geeky News

press@geekynews.co.uk

+44 20 3800 1212

Parallel House, 32 London RoadGuildford,Surrey

Source : Geeky News

See on IssueWire