Confidential

MDR CYBER
Part of the Mishcon de Reya Group

February 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

February 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Russian Hacker Group infiltrate senior employees email accounts	The nation backed state actor group, Nobellium accessed senior employee email accounts through password spray attack gained compromised access legacy systems	The attack highlights the need to upgrade legacy systems, strengthening security practices, applying MFA and developing incident response plan to ensure continuous monitoring.
Vulnerability in Ivanti Connect Secure and Policy Secure products allows bypass of authentication, and access to data.	Attacker exploitation reported following public "proof of concept" exploit release. Vulnerable products are at elevated risk.	Ivanti has issued patches, but ongoing monitoring of security resources is essential for users, given this is one of a series of serious flaws discovered in Ivanti products in the past three months.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

The document has three main purposes to assist cybersecurity leaders:

1. To be 'threat-led' and help prioritise defences against particular types of attackers
2. To justify business decisions on cybersecurity changes, technology or services
3. To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Russian Group infiltrates senior employees' email accounts via legacy system

What?

On January 12, 2024, Microsoft's security team detected and responded to a sophisticated cyberattack by the suspected Russian state actor known as Midnight Blizzard, or Nobelium[1].

The attackers employed "password spraying", a technique which involves trying common passwords to log into different accounts to compromise a legacy non-production test tenant account, which they then used to access a small subset of Microsoft's corporate email accounts. These accounts included those of senior leadership and employees in sensitive roles such as cybersecurity and legal departments. [2]

The attackers successfully exfiltrated some emails and attached documents. Initial targets included information related to the group Midnight Blizzard itself. Microsoft has confirmed that the attack did not exploit any vulnerabilities in their products or services and that there was no access to customer data, production systems, source code, or AI systems[3].

So what?

The incident demonstrates the tenacity, motivation and consequently the risk posed by groups that are likely backed by a nation state towards companies including those with sophisticated security measures in place. It also underlines the importance of rapid detection and response capabilities and ensuring legacy systems are secured.

Furthermore, it underscores the value of sharing threat intelligence within the security community to enhance collective defence. Organisations are advised to review their incident response plans, strengthen their password policies, implement multi-factor authentication, continuously monitor for suspicious activity, and educate employees on cybersecurity awareness.

Key recommendations include:

- Implement robust password policies and consider multi-factor authentication to prevent password spray attacks.
- Review and upgrade security measures for legacy systems, even if it requires significant changes to business processes.
- Develop and regularly update an incident response plan to quickly react to similar cyber threats.
- Engage in information sharing with industry peers and authorities to stay informed about the latest threat actors and their tactics.
- Maintain continuous monitoring of systems and networks for unusual activity to detect and respond to threats promptly.

[1] Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard, https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[2] Microsoft says Russian group infiltrated some employees' email accounts, https://www.ft.com/content/d4639b30-80b0-4dc1-a1d5-50f854d60064?desktop=true&segmentId=d8d3e364-5197-20eb-17cf-2437841d178a#myft:notification:instant-email:content

[3] Microsoft corporate emails hacked by Russian-backed group, company says, https://abcnews.go.com/Business/microsoft-corporate-emails-hacked-russian-backed-group-company/story?id=106527859

- Conduct regular security awareness training for employees to recognise and report potential cyber threats.

Further Ivanti vulnerability under mass exploitation

What?

A Secure Server-side Request Forgery (SSRF) vulnerability discovered in Ivanti's Connect Secure and Ivanti Policy Secure products is under mass exploitation by attackers.

The vulnerability resided in a Security Assertion Markup Language (SAML) component, allowing attackers to forge requests and bypass authentication controls. This enabled them to potentially access sensitive internal data. SAML is an XML-based open-standard for transferring identity data between two parties.

Ivanti first warned about the vulnerability (CVE-2024-21893) on 31 January 2024, at the time revealing only a small number of customers being impacted. As of early February, security researchers Shadowserver, were reporting multiple examples of exploitation[4]. This followed release of a public "proof of concept" (POC) exploit.

So what?

Ivanti released security patches and mitigation instructions in January and February and has continued to provide fixes to the various other vulnerabilities that have been exposed.[5] Businesses affected by these vulnerabilities should immediately follow these steps to avoid exploitation.

As the situation is developing, it is likely that as more research is conducted, further security issues are discovered, which require other mitigation. For that reason, businesses using Ivanti products are strongly encouraged to monitor the Ivanti resources and cybersecurity guidance, to ensure they remain protected.

Ivanti products have suffered a high number of vulnerabilities in recent months leading to the US Cybersecurity and Infrastructure Security Agency issuing an executive directive to federal agencies to mitigate the problems and to disconnect all Ivanti Connect Secure and Policy Secure VPN appliances vulnerable to multiple actively exploited bugs, highlighting the perceived severity of the problems.[6] The directive was to remain in effect until CISA determined that agencies had sufficiently mitigated. European Union agencies have also released statements reinforcing the widespread and global nature of the issues.[7]

This event highlights the importance of a layered security approach. By combining proactive patching, strong authentication, network segmentation, threat intelligence, and incident response readiness, security professionals can significantly reduce the risk of successful cyberattacks against vulnerabilities like CVE-2024-21893.

[4] https://twitter.com/Shadowserver/status/1754145361029960189

[5] https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

[6] https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

[7] https://www.europol.europa.eu/media-press/newsroom/news/joint-statement-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

MDR CYBER
Part of the Mishcon de Reya Group

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.

This document has been prepared for general guidance only, and does not constitute professional or legal advice. If you wish to receive legal advice we will need to provide you with a separate retainer letter and additional terms of business, as such work will be separately regulated by the Solicitors Regulation Authority (SRA).

You should not act upon the information contained in this publication without obtaining specific professional or legal advice.

Mishcon de Reya refers to Mishcon de Reya LLP which is a limited liability partnership, incorporated in England (number OC399969), whose registered office is at Africa House, 70 Kingsway, London WC2B 6AH. It is a body corporate which has members rather than Partners.

mishcon.com/cyber