MDR CYBER
Part of the Mishcon de Reya Group

January 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

January 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Mandiant's Twitter account compromised for scam, despite having multi-factor authentication.	Attack highlights the potential for cybercriminals to exploit social media platforms for financial gain or reputational damage.	Necessity for strong, unique passwords, restricted access on corporate social media accounts coupled with employee education around overcoming MFA, and a comprehensive response plan.
Ivanti patched am EPM vulnerability which allows hijackers to bypass authentication and control servers remotely.	The critical vulnerability allows remote execution only once the hacker is inside the network, getting unauthenticated access to core servers and enrolled devices using SQL injection.	Implement the released patch update to ensure protection and restrict network access if immediate patching is not possible, monitoring and logging activity are advised as effective countermeasures.

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.

Mandiant attack underlines importance of social media security procedures

What?

On January 4th, 2024, the verified Twitter account of Mandiant, a prominent cybersecurity firm, was hijacked.[1] Attackers then leveraged the compromised account, which has over 100k followers, to disseminate a fraudulent cryptocurrency giveaway and engage in hostile communications directed towards Mandiant. Another security company suffered a similar attack at around the same time.[2] A recent report also indicated a surge in the sale of Twitter "Gold" accounts on the dark web, suggestive of a continuing trend of cybercriminals exploiting social media platforms for financial gain or reputational damage.[3]

The nature of the attack remained unclear at the time of writing, but the announcement following the attack indicated the account was protected through multi-factor ("2FA") authentication meaning the attackers had overcome this added layer of protection.

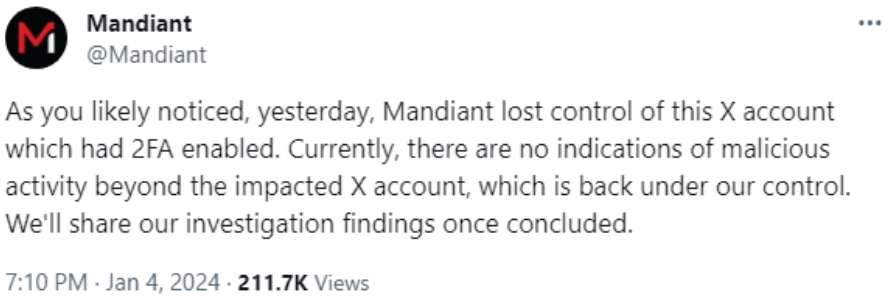


Figure 1 - Mandiant announcement

So what?

The Mandiant attack and the rise of compromised account sales on the dark web raise several concerns, not least that high-profile and well-protected entities can be successfully targeted. Mandiant announced that the account had been protected with two-factor authentication, saying it would share details once an investigation had been completed.

This raises unanswered questions about how the additional authentication process was overcome, with some commentators hypothesising social engineering, malware on a user's machine or a supply-chain attack.

Regardless of the tactics, techniques and procedures (TTPs) the attackers used, the incident underlines the necessity for assurance around social media accounts, particularly those used by

[1] Mandiant's X (Twitter) Account Hacked to Promote Crypto Scam, https://www.darkreading.com/cyberattacks-data-breaches/mandiant-s-x-twitter-account-hacked-to-promote-crypto-scam
[2] CertiK Twitter account hijacked by cryptocurrency scammer posing as Forbes journalist, https://grahamcluley.com/certik-twitter-account-hijacked-by-cryptocurrency-scammer-posing-as-forbes-journalist/
[3] Gold Rush on the Dark Web: Threat Actors Target X (Twitter) Gold Accounts, https://www.cloudsek.com/whitepapers-reports/gold-rush-on-the-dark-web-threat-actors-target-x-twitter-gold-accounts

high-profile and corporate entities, and especially those with a large following, which are more attractive to attackers, given their potential reach.

Key recommendations include:

- Enforce strong, unique passwords and encourage regular resets. Do not allow users to share passwords across online accounts.
- Good password hygiene can be managed with the use of password managers, including enterprise versions that simplify this process.
- Enable multi-factor authentication (MFA). Despite this being overcome in this attack, it is a good line of defence.[4]
- Restrict access to only a small group of users that need to have it.
- Employee education, particularly around phishing and the ways in which attackers can overcome MFA through social engineering.[5]
- Larger organisations may also wish to monitor social media for early signs of a problem as well as other negative sentiment.
- Have a response plan that considers the possibility of account takeover and what steps to take.

[4] Multi-factor authentication for online services, https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

[5] What Is a Multi-Factor Authentication (MFA) Bypass? https://abnormalsecurity.com/glossary/mfa-bypass

Ivanti patches EPM vulnerability which allows hijackers to bypass authentication and control servers remotely

What?

On 4th January 2024, Ivanti, the enterprise software company in the US fixed a critical vulnerability in their Endpoint Management software (EPM) allowing threat actors to gain unauthenticated access to core server or enrolled devices.[6] At the time of writing, no real-world exploitation had been observed, although enterprises using the software are advised to remediate.

The EPM platform is used to help manage client devices running different platforms ranging from Chrome OS and MacOS to Windows and IoT operating systems. The security flaw is being tracked as CVE-2023-39336 and has been given a high score of 9.6 out of 10 on the common vulnerability scoring system (CVSS). Exploitation could lead to remote execution on vulnerable servers.[7]

The exploit the vulnerability, attackers must have access to the internal network, somewhat mitigating the immediate risk. However, following this, SQL injection may be performed by the attacker – a technique which uses commands inserted into SQL data entry fields to force it to reveal or alter its database without the need to authenticate. If an attacker gains control of the machines running the EPM agent , the attacker could perform remote executions on the core server, and follow on actions.[8]

So what?

Ivanti did not find any indications that customers had been impacted by the vulnerability, the issue was addressed in an Ivanti EPM 2022 service update 5. The fix is available on the EPM platform for all supported versions.

This issue follows a series of other recent vulnerabilities in Ivanti software – in summer 2023, several vulnerabilities were exploited in real world attacks, demonstrating the attraction of the software to attackers, which is widely used by corporations.

We recommend the following actions for those using the affected software:

- Apply the Patch: Ivanti has released a security patch addressing this vulnerability. Please ensure that your Ivanti Patch for Endpoint Manager (EPM) is updated with the latest version containing the necessary security fixes.

- Restrict network access: If immediate patching is not possible, temporarily restrict network access to the Ivanti Endpoint Manager server to mitigate the risk of exploitation. This will limit the potential attackers to those already within your internal network.

[6] Ivanti warns critical EPM bug lets hackers hijack enrolled devices, https://www.bleepingcomputer.com/news/security/ivanti-warns-critical-epm-bug-lets-hackers-hijack-enrolled-devices/
[7] Ivanti fixed a critical EPM flaw that can result in remote code execution, https://securityaffairs.com/156951/security/ivanti-critical-epm-flaw.html
[8] Ivanti Patches Critical Vulnerability in Endpoint Manager, https://www.securityweek.com/ivanti-patches-critical-vulnerability-in-endpoint-manager/

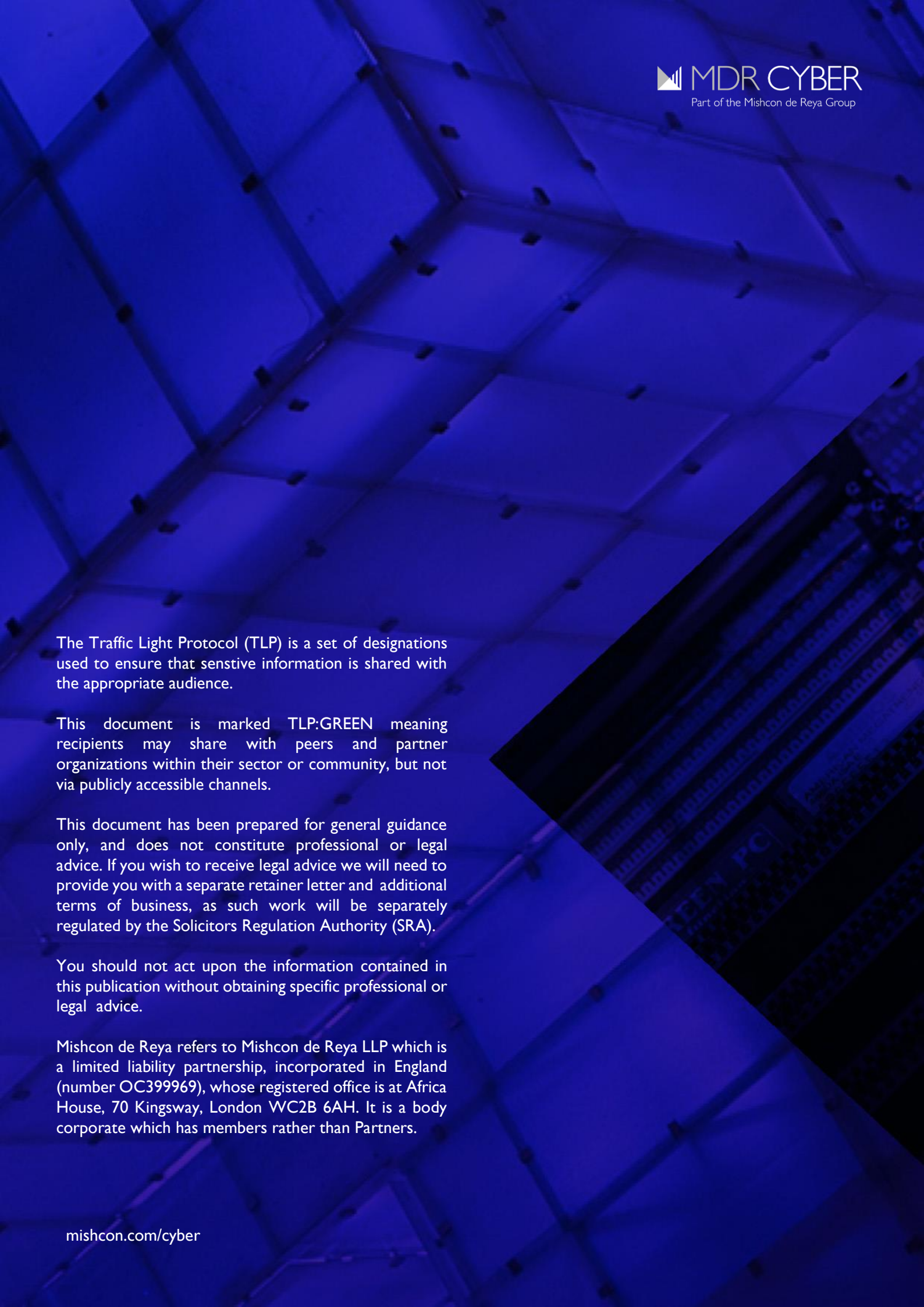
- Review and Enhance Authentication Policies: Evaluate and reinforce authentication protocols within your network to add an extra layer of defence against unauthorized access attempts.

- Network Monitoring and Intrusion Detection: Implement robust network monitoring and intrusion detection systems to promptly identify and respond to any unusual or unauthorized activities on your servers.

- User Education and Awareness: Educate your team members about potential phishing attempts and the importance of practicing safe online behaviour to reduce the risk of social engineering attacks.

- Backup and Recovery Planning: Regularly backup critical data and establish a comprehensive recovery plan to minimize potential data loss and downtime in the event of a security incident.

- Input validation: Implement strict input validation on all user input entering Ivanti Endpoint Manager. This helps prevent malicious SQL code from being injected into the system. Use an "allow list" approach to restrict acceptable characters and data formats and sanitize user input to remove potentially dangerous characters.



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.