MDR CYBER
Part of the Mishcon de Reya Group

June 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

June 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Data theft and extortion campaign targeting Snowflake customer database instances via stolen credentials.	The threat actor "UNC5537" used infostealer malware to acquire old and unsecured credentials, leading to successful breaches due to the absence of multi-factor authentication and network allow lists.	165 potentially impacted organisations, emphasises the need for credential monitoring, MFA enforcement, and secure authentication practices.
Phishing email, leading to remote access via SuperOps RMM software, disguised as Minesweeper game.	The threat actor, known as "UAC-0188," used a phishing scheme to distribute a malicious executable, which when run, deployed a legitimate remote management tool for unauthorised access.	Attack part of a larger campaign against EU and US financial services. Organisations are urged to monitor for SuperOps RMM-related network activity and review CERT-UA's IOCs for threat detection and prevention.
Zero-day attacks exploit Check Point VPN since April	Attackers exploit an information disclosure vulnerability to gain access to password-only authentication account and move laterally in network.	Check Point has released a hot fix, to address the issue and advised to implement MFA and monitor network traffic for malicious activity.

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.

Attackers target Snowflake customer databases with stolen credentials

What happened?

On 10 June 2024, Mandiant reported on a campaign against Snowflake, a cloud-based data warehousing service used by many organisations to store and analyse data[1]. Attackers targeted customer database instances using stolen credentials.

The attackers aimed to steal data and extort victims. Breaches observed by Mandiant were not due to a compromise of Snowflake's systems but rather stemmed from customer credentials that had been compromised, often through infostealer malware.

The campaign was first discovered in April 2024 when database records for sale were traced back to a compromised Snowflake instance. The victim organisation's credentials had likely been stolen via malware, and the account did not have multi-factor authentication (MFA). Mandiant and Snowflake have since notified approximately 165 potentially affected organisations and provided them with support and guidance.

The threat actor, UNC5537, likely obtained credentials through infostealer malware, which had infected systems not owned by Snowflake. These credentials were sometimes years old and had not been changed or secured with MFA. The campaign was successful due to the lack of MFA, valid stolen credentials, and the absence of network allow lists to restrict access to trusted locations.

Investigations revealed that contractors using personal devices for work and personal activities were often the initial point of compromise. The attackers used a variety of tools to perform reconnaissance and data exfiltration from the Snowflake instances.

So what?

The campaign highlights the risks associated of stolen credentials, which continue to be one of the most popular sources of intrusions[2]. The campaign also underscores the dangers of password reuse and the failure to implement basic security measures like MFA and credential rotation.

The campaign's success was also partly due to the popular infostealer marketplace, where stolen credentials are readily available. This has broader implications for the security of SaaS platforms, as threat actors may continue to target them using similar tactics.

Mandiant's findings emphasise the need for organisations to monitor credentials, enforce MFA universally, restrict network access to trusted locations, and be vigilant for abnormal access attempts. The incident serves as a reminder of the importance of cybersecurity hygiene and the need for consistent security awareness to protect against data theft and extortion.

[1] UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[2] Verizon DBIR: Threat Actors Continue to Leverage Compromised Credentials to Steal Corporate Data, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/may/Verizon-DBIR-Compromised/

Organisations using Snowflake should follow the hardening guidance provided by Snowflake[3] and to stay informed about the latest threat intelligence to prevent similar compromises. Mandiant's Snowflake threat hunting guide and Snowflake's published detection and hardening guidance[4] are resources that organisations can use to secure their data environments against such threats.

[3] Snowflake Security Overview and Best Practices, https://community.snowflake.com/s/article/Snowflake-Security-Overview-and-Best-Practices

[4] Detecting and Preventing Unauthorized User Access, https://community.snowflake.com/s/question/0D5VI00000EmyI00AB/detecting-and-preventing-unauthorized-user-access

Minesweeper phishing leads to remote access targeting financial services

What?

On 23 May 2024, the Ukrainian Computer Emergency Response Team (CERT-UA) published details about a cyber-attack targeting Ukrainian organisations.

The attackers gained unauthorised remote access to computers by exploiting a legitimate remote management software called SuperOps RMM.

The attacker, designated as "UAC-0188" started with a phishing email from the email address "support@patient-docs-mail.com," impersonating a medical centre with the subject "Personal Web Archive of Medical Documents."

The recipient was then prompted to click on a Dropbox link, which when clicked, downloaded an executable .SCR file disguised as the classic game of Minesweeper. This file, created with the software PyInstaller, included a large base64-encoded string. Additional Python code was fetched from anotepad.com, which then decoded and executed further instructions.

The code from Minesweeper included a function called "create_license_ver." This function was used to decode and activate concealed malicious code. Subsequently, a base64-encoded string was decoded to create a ZIP archive, which held an MSI installation file for the SuperOps RMM software. This installer was then extracted and run using a static password.

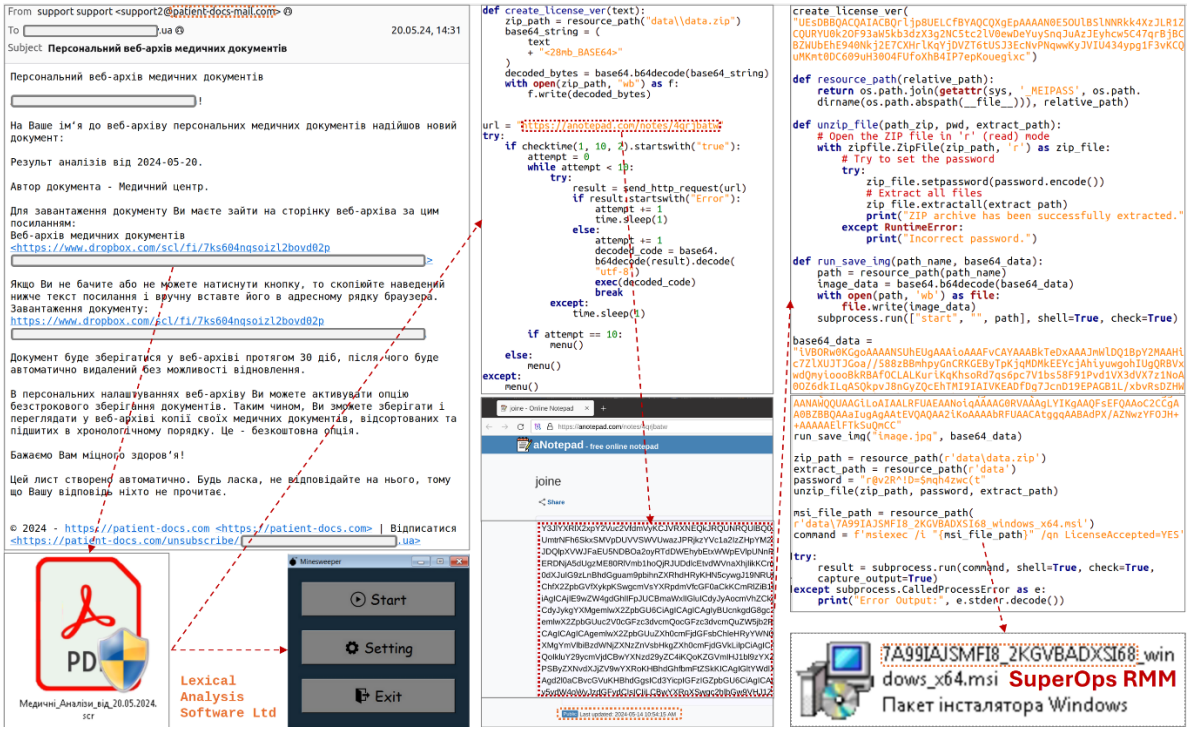


Figure 1 - Screenshots provided by CERT-UA

So what?

CERT-UA's investigation revealed that this attack was likely part of a broader campaign against financial and insurance institutions across Europe and the USA since at least February-March 2024. This suggests a widespread campaign with potentially numerous victims.

The use of legitimate software for malicious purposes makes detection more challenging. Organisations are advised to check for network activity related to SuperOps RMM, especially if they are not users, to prevent unauthorised access.

The detailed indicators of compromise (IOCs) provided by CERT-UA[5], including file hashes, network addresses, and host information, are helpful for organisations to detect and respond to this threat.

[5] https://cert.gov.ua/article/6279419

Zero-day attacks exploit Check Point VPN since April

What?

A zero-day vulnerability in Check Point's VPN software has been exploited by attackers since late April 2024. The vulnerability allows unauthorised access to networks using the VPN, bypassing authentication mechanisms and potentially leading to data interception and lateral movement within the network.[6]

The attackers exploited old VPN service accounts using password-only authentication. The vulnerability tracked as CVE-2024-24919 has been exploited to extract Active Directory data and password hashes of accounts with password-only authentication in place.[7]

The vulnerability has a CVSS score of 8.6 out of 10, marking it as particularly high as it is easy to exploit it remotely with no user interaction or privileges.[8]

So what?

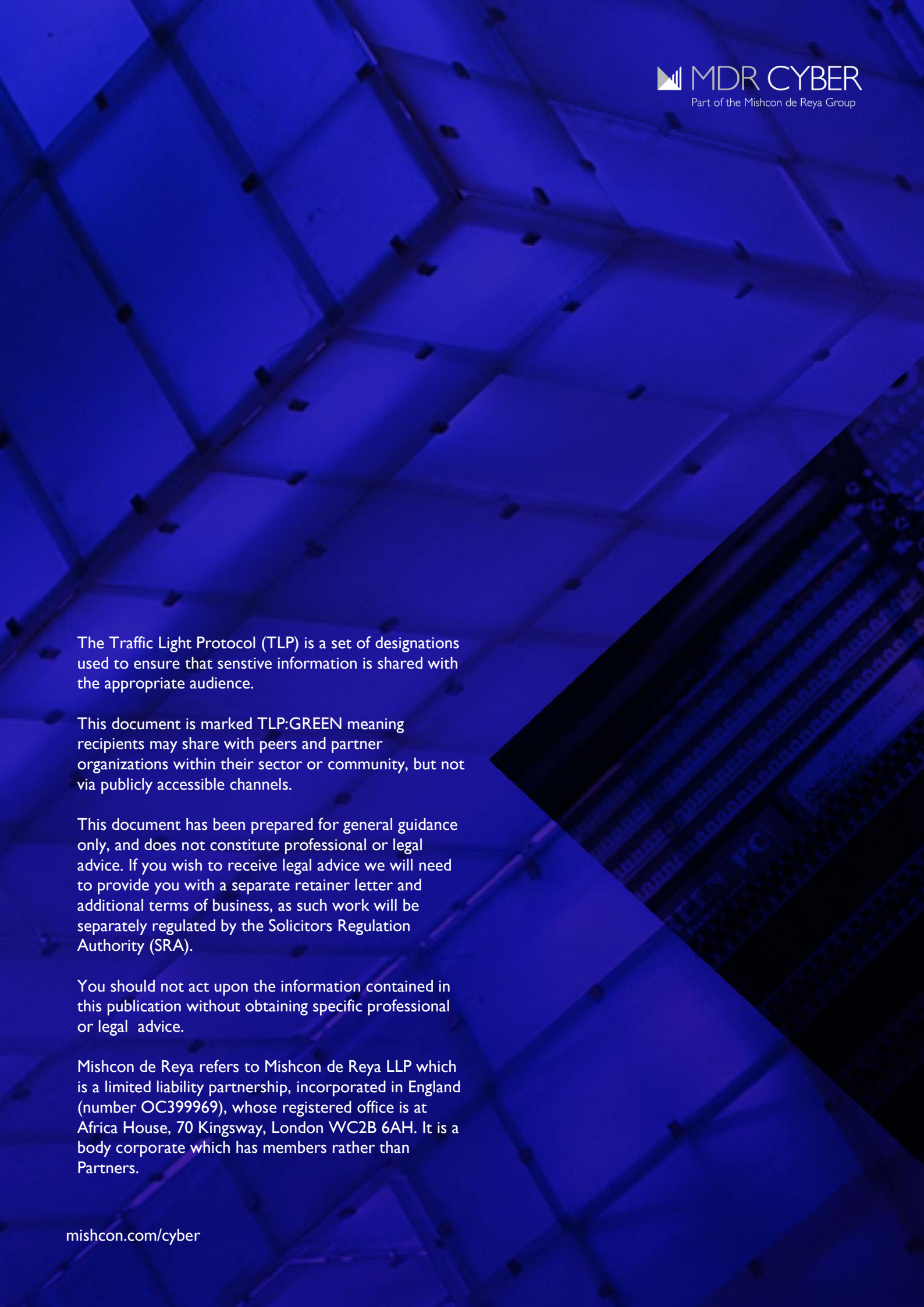
At the time of review, the exploit was still being investigated. Any significant impact had not been disclosed. Check Point was quick to react and released a hot fix - a package containing all the necessary information to address the software issue, to remove password-only logins.[9]

Users should review authentication logs for suspicious connections, prevent local accounts from connecting to the VPN with password authentication. This will force local accounts to implement multi-factor authentication (MFA).

Along with these recommendations, general security "hygiene" measures should also be considered to implement a layered security approach:

- Regular updates: Ensure that your operating system, applications, and security software are up to date. Regularly apply security patches.
- Strong authentication: Use strong, unique passwords for all accounts. Consider using a password manager.
- Multi-factor authentication (MFA): Enable MFA wherever possible to add an extra layer of security.
- Firewall and Intrusion Detection Systems (IDS): Implement a firewall and IDS to monitor and block suspicious network traffic.
- Network Segmentation: Segment your network to limit the impact of potential breaches.
- Security Awareness Training: Educate users about phishing, social engineering, and safe online practices.

[6] Check Point VPN zero-day exploited in attacks since April 30, https://www.bleepingcomputer.com/news/security/check-point-vpn-zero-day-exploited-in-attacks-since-april-30/
[7] Check Point VPN Attacks Involve Zero-Day Exploited Since April, https://www.securityweek.com/check-point-vpn-attacks-involve-zero-day-exploited-since-april/
[8] Thousands of internet-facing devices vulnerable to Check Point VPN zero-day, https://therecord.media/thousands-of-devices-vulnerable-checkpoint
[9] Preventative Hotfix for CVE-2024-24919 - Quantum Gateway Information Disclosure, https://support.checkpoint.com/results/sk/sk182336



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.