MDR CYBER
Part of the Mishcon de Reya Group

March 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

March 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Severe flaws in ConnectWise ScreenConnect remote desktop software need attention from users.	Two critical vulnerabilities in the software that are trivial to exploit and under active use allow for attackers to gain complete control and remotely execute code.	On-premises users should immediately update, cloud users are automatically protected. Older software users should update to newer versions. Users should proactively investigate for signs of compromise.
LockBit group disrupted but threat from ransomware remains.	After international law enforcement successfully disrupted LockBit's operation, the ransomware gang announced that they are planning a return.	Despite the successful disruption, the threat from LockBit and other ransomware groups remain. Organisations should remain vigilant and follow best practice guidance to reduce risks.

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.

Severe flaws in ConnectWise ScreenConnect needs attention from users

What?

Two significant vulnerabilities in ConnectWise ScreenConnect were identified in the widely used remote desktop software and need attention from users on 19 February 2024. The flaws allow for anonymous attackers to exploit an authentication bypass flaw and create admin accounts on publicly exposed instances. This means that they will have administrative access to systems, allowing them to have control, remotely execute code and delete other users, for example.

The vulnerability was trivial to exploit[1] and a "proof-of-concept" was publicly disclosed, meaning that it was known and accessible to threat actors with the motivation to use it.[2] It has been under active exploitation since shortly after its disclosure.[3]

Vulnerable users include those running a self-hosted instance running version 23.9.7 and prior. The vulnerabilities were assigned the identifiers CVE-2024-1709 & CVE-2024-1708.

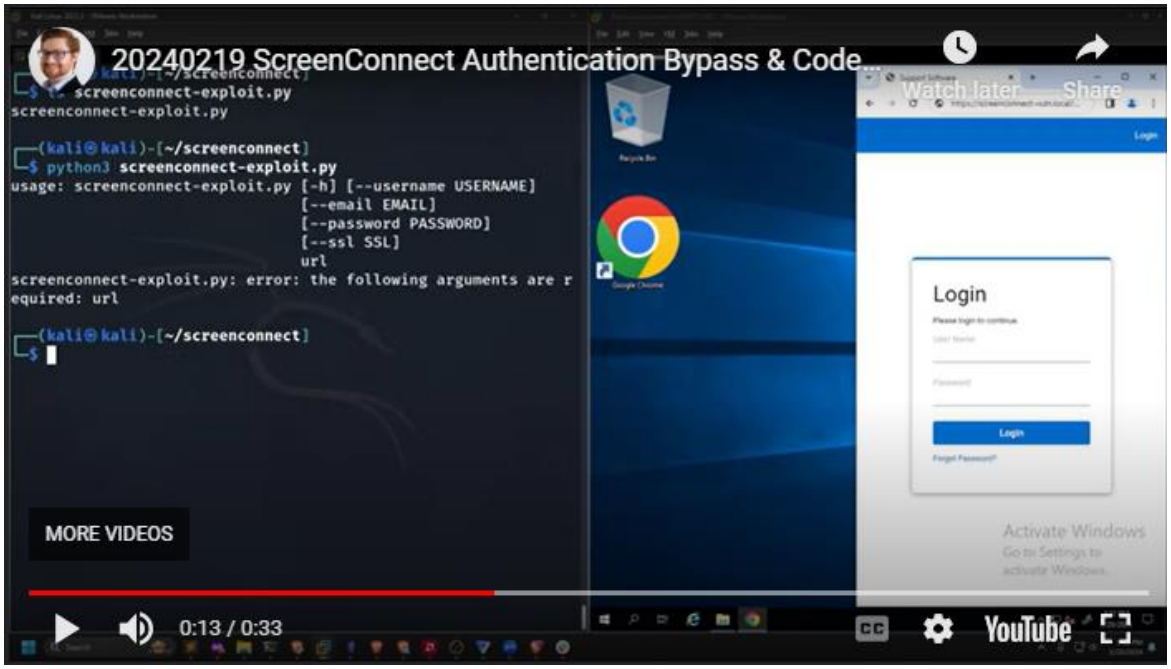


Figure 1 - Huntress demonstration of Proof of Concept in action

[1] A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708), https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass

[2] GitHub proof of concept, https://github.com/watchtowrlabs/connectwise-screenconnect_auth-bypass-add-user-poc

[3] ConnectWise Confirms ScreenConnect Flaw Under Active Exploitation, https://www.securityweek.com/connectwise-confirms-screenconnect-flaw-under-active-exploitation/

So what?

ConnectWise have released mitigation details.[4] On-premises versions of the vulnerable software must be updated. Cloud instances are automatically patched. ConnectWise have encouraged on-premises users of older versions to update to the latest release as it includes security updates, bug fixes and other updates.[5]

Users of the on-premises software are strongly advised to also review systems and endpoint detection and response (EDRs) for evidence of suspicious activity such as commands run from webshells, or other indicators of compromise (IOCs)[6]. Hardening advice is also available to enable appropriate logging and investigation.[7]

If evidence of suspicious activity is discovered, contact MDR Cyber for specialised assistance.

[4] ConnectWise ScreenConnect 23.9.8 security fix, https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

[5] Upgrade an on-premises installation, https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/On-premises/Get_started_with_ConnectWise_ScreenConnect_On-Premise/Upgrade_an_on-premises_installation?_gl=1*wafamz*_ga*MTM5OTcxNTAyOS4xNzA5MzAyNzc2*_ga_QSGE0F7K8V*MTcxMDMyNDgwOS4yLjEuMTcxMDMyNDg0OS4yMC4wLjA.

[6] https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

[7] https://services.google.com/fh/files/misc/connectwise-screenconnect-remediation-hardening-guide.pdf

Lockbit Ransomware returns after successful disruption

What?

On February 20, 2024. The National Crime Agency (NCA) published details of an operation to take control of LockBit ransomware's primary administration environment, compromising their entire criminal enterprise, calling it Operation Cronos.[8]

Billed as "*the world's most harmful cybercriminal group*", Lockbit have been in operation for the last four years and have been successful with their attacks, previously targeting thousands of victims around the world including in the UK and are responsible for losses of billions of dollars as a cost of recovery and payment of ransoms.[9]

The group provides ransomware-as-a-service (RaaS) to a global network of affiliates supplying them with infrastructure and tools to carry out attacks. Once a victim's network was compromised by LockBit's software, data was stolen, using their bespoke data extraction tool called Stealbit and systems were encrypted. Ransoms were demanded in cryptocurrency and paying victims could decrypt the files and prevent the data from getting published.

Despite the disruption, the ransomware gang attempted a "comeback" a few days after the international operation. A new site was set-up on the dark web sharing a statement that their previous website was compromised due to a vulnerability in the PHP programming language, which is largely used to create websites, and not all servers had PHP installed.[10]

So what?

This is an example of a successful law enforcement operation, and the efforts will undoubtedly disrupt this group and may lead to arrests and further enforcement. It may take some time for this group to rebuild its infrastructure and gain the confidence of their affiliates. However, the threat of other ransomware groups persists.

As with other ransomware, to combat the threat of LockBit ransomware, organisations must adopt a comprehensive and proactive security strategy.

Comprehensive advice for ransomware prevention, protection, monitoring, response, and recovery is available from guides published by the UK's National Cyber Security Centre.[11]

Best practice includes:

- Making regular and appropriate backups of systems
- Filtering and inspecting content to prevent it reaching devices
- Take actions to prevent malware from executing on devices, including patching known vulnerabilities

[8] International investigation disrupts the world's most harmful cyber crime group, https://nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

[9] Russia-based LockBit ransomware hackers attempt comeback, https://www.theguardian.com/technology/2024/feb/26/russian-based-lockbit-ransomware-hackers-attempt-comeback

[10] Law enforcement disrupt world's biggest ransomware operation, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[11] https://www.ncsc.gov.uk/ransomware/home

- Preparing for an incident by creating incident response plans, assigning responsible teams and enlisting external incident response and legal services

We have provided further details around general guidance below:

- Organisations should ensure that all systems are up to date with the latest security patches. Endpoint protection solutions are also crucial, as they can detect and stop ransomware before it can cause harm.

- Employee training and awareness is essential to defend against ransomware. By educating staff on how to identify and report phishing attempts and other social engineering tactics, organisations can significantly reduce the risk of an employee inadvertently allowing ransomware to infiltrate the network, or quickly remediate.[12]

- Access controls and password policies must be robust, limiting the damage that can be done with compromised credentials. The implementation of multi-factor authentication (MFA) adds a critical layer of security, making it more difficult for attackers to gain unauthorised access.

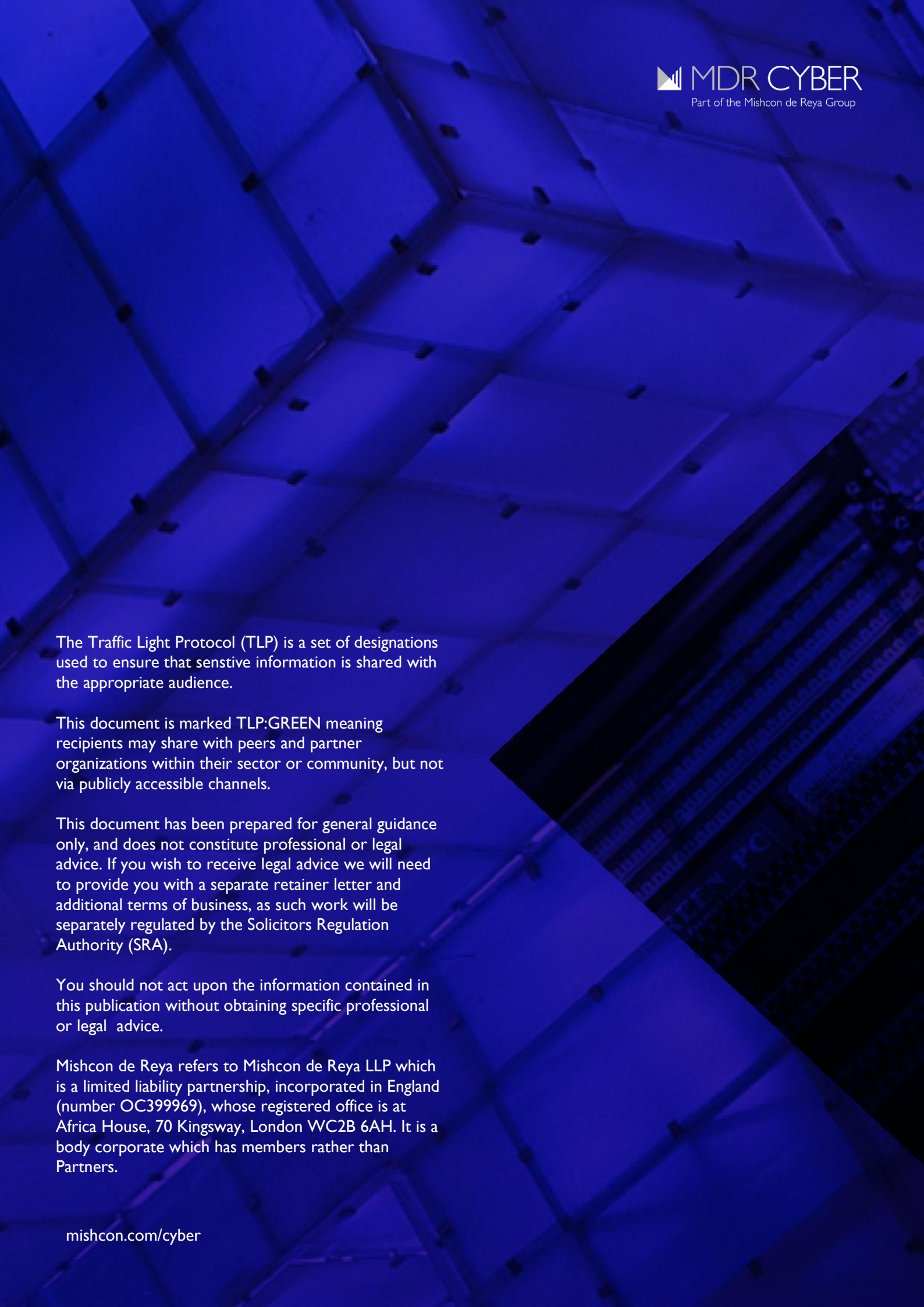
- Regular, secure, and tested backups are indispensable. These backups should be encrypted and stored in a manner that isolates them from the network, such as offsite or in the cloud, ensuring they are not accessible to attackers.

- An incident response should detail how to isolate infected systems, communicate with stakeholders, liaise with external forensic and legal experts and report the incident to authorities. Regular training and simulation exercises can help prepare the response team to act swiftly and effectively in the event of an attack.[13]

By embracing these defensive measures, organisations can not only mitigate the risk of a ransomware attack but also position themselves to respond and recover with resilience. Staying informed about the evolving cyber threat environment and continuously enhancing cyber security practices are essential steps in safeguarding against the sophisticated and ever-changing tactics of ransomware operators.

[12] Tips & advice to prevent ransomware from infecting your electronic devices, https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices

[13] LockBit Attempts to Stay Afloat With a New Version, https://www.trendmicro.com/en_us/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html?utm_source=trendmicroresearch&utm_medium=SEM&utm_campaign=0224_lockbitdisruptionSEM&gad_source=1&gclid=EAIaIQobChMI9bz29MHfhAMVsZdQBh1EtQd1EAAYAyAAEgKyVfD_BwE



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.