MDR CYBER
Part of the Mishcon de Reya Group

July 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

July 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
TeamViewer corporate IT environment compromised by Russian state actors	TeamViewer was compromised after threat actors leverage employee's standard account to access corporate directory data such as names and encrypted passwords	While limited information has been shared by TeamViewer, it advised to ensure MFA has been enforced for corporate users and TeamViewer hosts placed under heightened monitoring.
The Ghostscript toolkit, commonly pre-installed on Linux systems, was actively exploited, allowing remote code execution.	Attackers exploited the vulnerability by disguising EPS files as JPGs to execute commands and gain shell access to systems with Ghostscript versions 10.03.0 and earlier.	Businesses using Ghostscript in production should upgrade to version 10.03.1 or apply patches if available. There is a test script to detect system vulnerabilities.

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:

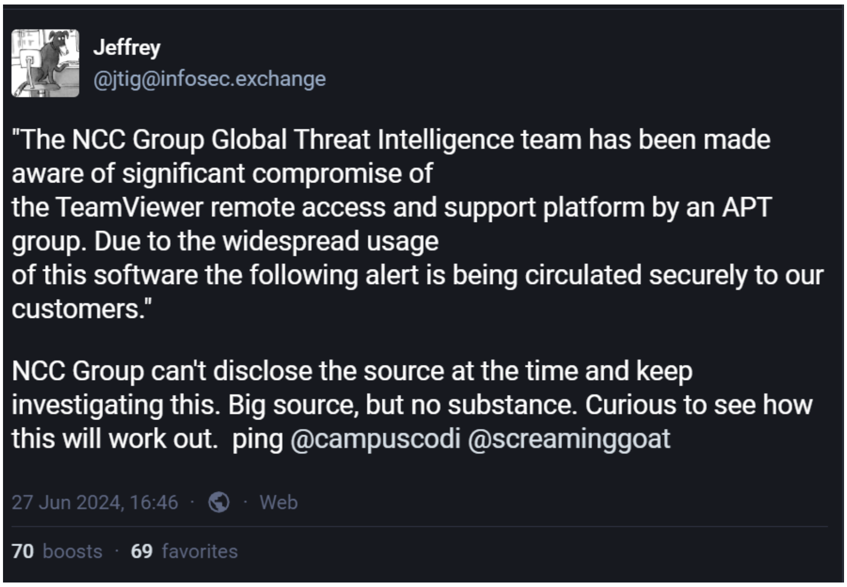
1. To be 'threat-led' and help prioritise defences against particular types of attackers
2. To justify business decisions on cybersecurity changes, technology or services
3. To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status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

Russian attackers cause limited intrusion at TeamViewer

What happened?

On 26 June 2024, TeamViewer – one of the most popular remote access and control software providers – reported that they had detected an intrusion after unusual behaviour was detected on an employee's standard account. Statements issued by the company confirmed that the breach had only impacted their internal corporate IT environment.[1]

There was limited information about the compromise, however TeamViewer revealed that the attackers gained access to their systems after obtaining credentials for a standard employee account which had access to the corporate IT environment. The employee account was used to access employee directory data such as corporate contact information, encrypted employee passwords and names.[2]



Jeffrey
@jtig@infosec.exchange

"The NCC Group Global Threat Intelligence team has been made aware of significant compromise of
the TeamViewer remote access and support platform by an APT group. Due to the widespread usage
of this software the following alert is being circulated securely to our customers."

NCC Group can't disclose the source at the time and keep investigating this. Big source, but no substance. Curious to see how this will work out. ping @campuscodi @screaminggoat

27 Jun 2024, 16:46 · · Web

70 boosts · 69 favorites

Figure 1 - Early warning of the vulnerability (source: infosec.exchange)

TeamViewer noted that the attack was limited to the corporate IT environment due to strong segregation, and did not affect any customer data, product environment or the TeamViewer connectivity platform.

TeamViewer confirmed that the threat actor behind this attack was the Russian-linked APT29, also known as 'Midnight Blizzard' and 'Cozy Bear'. This state sponsored cyberespionage group is known to target military, government and organisations globally.[3]

[1] TeamViewer Hack Officially Attributed to Russian Cyberspies, https://www.securityweek.com/teamviewer-hack-officially-attributed-to-russian-cyberspies/

[2] APT29 Blamed for TeamViewer Intrusion, https://insight.scmagazineuk.com/apt29-blamed-for-teamviewer-intrusion

[3] TeamViewer employee data, passwords exposed in APT29 attack, https://www.scmagazine.com/brief/teamviewer-employee-data-passwords-exposed-in-apt29-attack

So what?

There was limited information about the damage caused by the attack. However, the compromise highlighted the importance of network segregation, as the attack was prevented from affecting customer data, and the importance of securing authentication methods, as the attackers gained access through the compromised employee credentials.

Implementation of Multi-factor authentication (MFA) will enhance authentication security making it difficult for threat actors to find possible entry vectors. TeamViewer administrators can enforce company-wide MFA by following the guidance provided by TeamViewer.[4]

The NCC Group Threat intelligence team advised to remove TeamViewer until further details had been share about the type of compromise TeamViewer was subjected to. However, if removing TeamViewer is not a feasible option, we recommend placing the hosts under heightened monitoring.[5]

[4] Enforce Two-factor Authentication for your Company Members, https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/enforce-two-factor-authentication-for-your-company-members/

[5] Threat Intelligence: TeamViewer compromised by APT29, https://www.nccgroup.com/uk/newsroom/threat-intelligence-teamviewer-compromised-by-apt29/

Commonly pre-installed 'Ghostscript' Linux software actively exploited

What?

Around 8 July 2024, the Ghostscript document conversion toolkit, widely used and commonly pre-installed on Linux systems, was under active exploitation for remote code execution. The software is used is used by multiple document conversion software, including ImageMagick, LibreOffice, GIMP, Inkscape, Scribus, and the CUPS printing system.

The vulnerability which allows the exploitation impacts all Ghostscript 10.03.0 and earlier installations and was tracked as CVE-2024-29510. Exploitation enabled attackers to perform activities such as command execution using the Ghostscript Postscript interpreter.[6]

Attackers had been observed exploiting the vulnerability using EPS (PostScript) files disguised as JPG (image) files to get shell access to vulnerable systems.

So what?

Some web applications and other services which provide document conversion and preview functionalities use Ghostscript, meaning that these may be impacted by the bug.

Businesses are advised to review if they are using the software in production systems and if so, either upgrade to the latest version (10.03.1) or remove it from systems, if practical.

Codean Labs published a Postscript file[7] to help detect if the vulnerability is present in systems. Users should run the command: "ghostscript -q -dNODISPLAY -dBATCH CVE-2024-29510_testkit.ps"

If the distribution that is used did not provide an option to use the latest version, there may be patches available.[8][9][10]

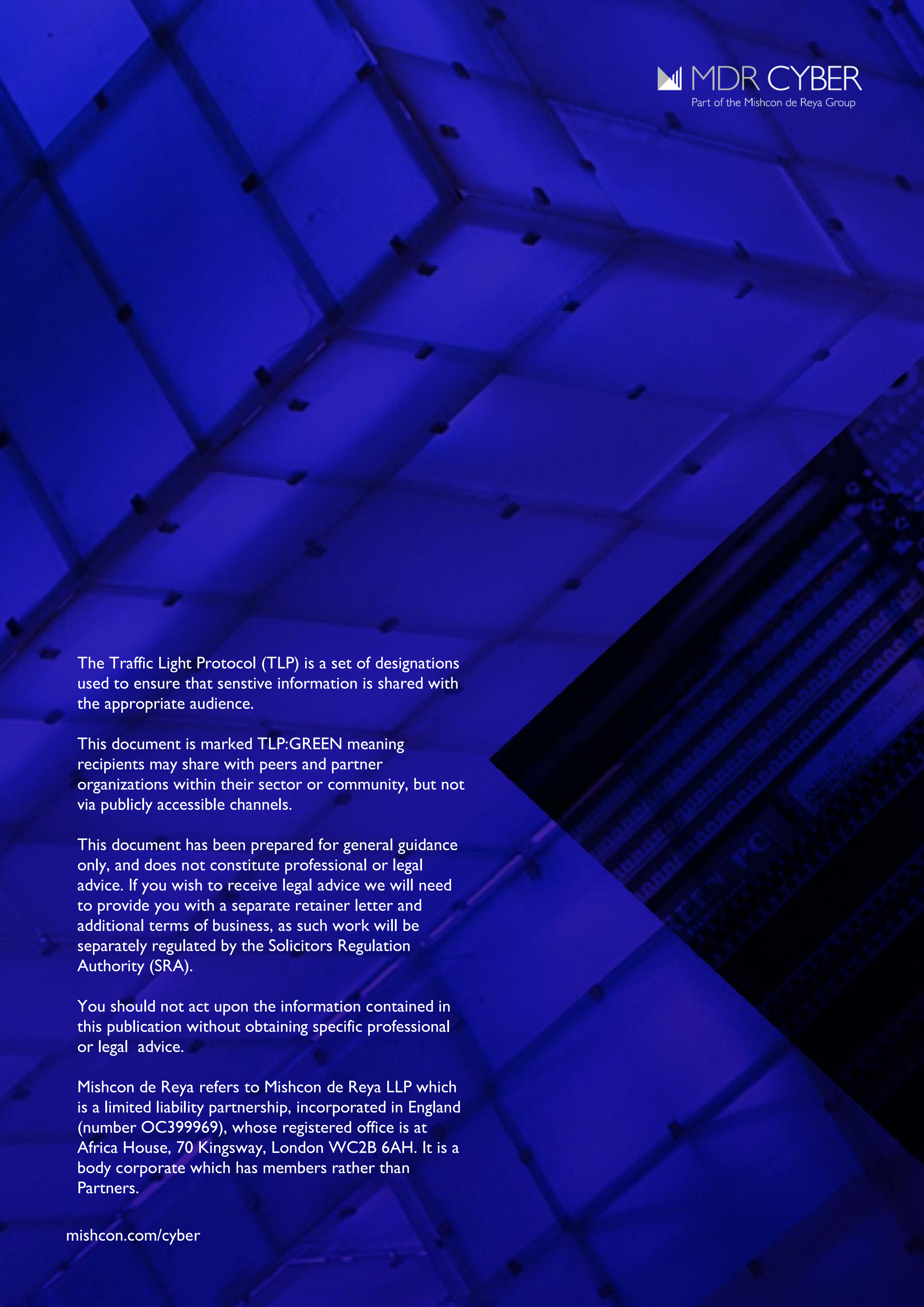
[66] CVE-2024-29510 – Exploiting Ghostscript using format strings, https://codeanlabs.com/blog/research/cve-2024-29510-ghostscript-format-string-exploitation/

[7] https://codeanlabs.com/wp-content/uploads/2024/06/CVE-2024-29510_testkit.ps

[8] Package Ghostscript, https://packages.debian.org/search?keywords=ghostscript

[9] USN-6835-1: Ghostscript vulnerabilities, https://ubuntu.com/security/notices/USN-6835-1

[10] Information for build ghostscript-10.02.1-5.fc39, https://koji.fedoraproject.org/koji/buildinfo?buildID=2480001



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