Scottish
Cyber
Coordination
Centre

UK Ransomware Report, August 2024

17 September 2024

This report describes the ransomware threat landscape for the UK. It can help senior leaders, cyber security professionals, and those outside the cyber profession who have an interest in business continuity understand trends in ransomware attacks and the threat actors who may target their organisations.

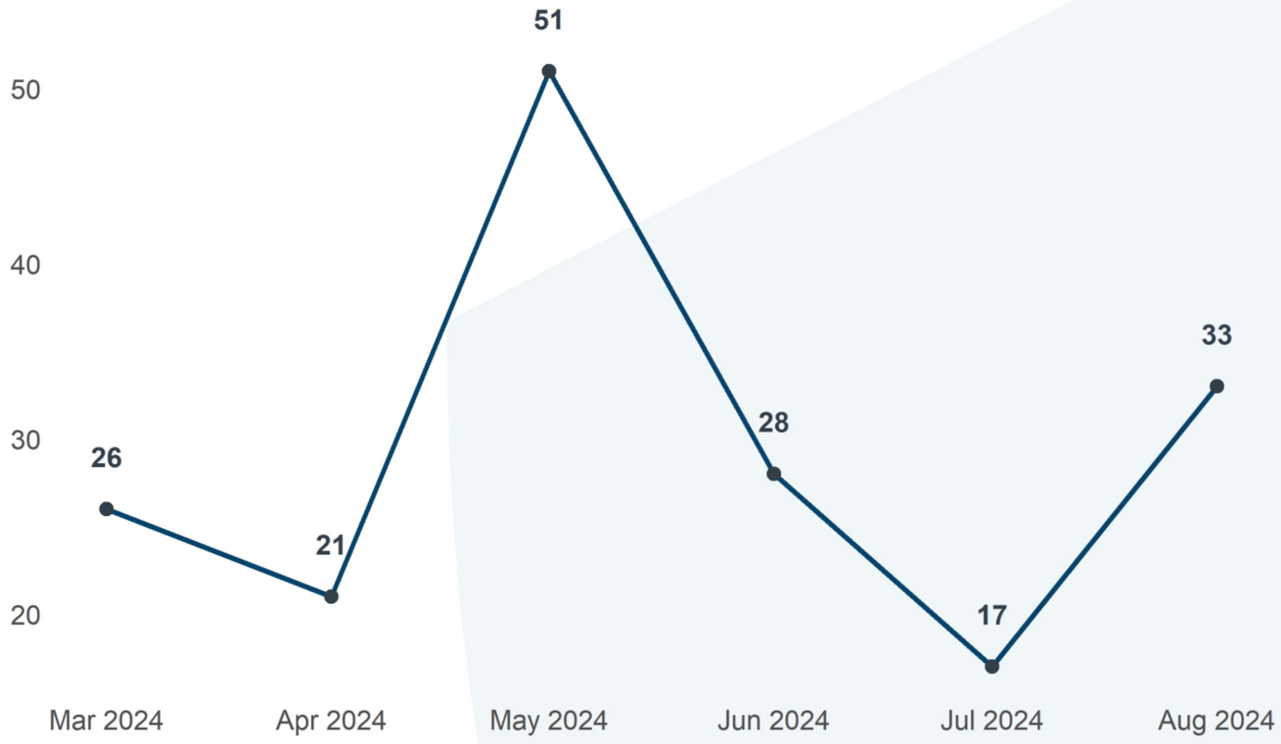
Ransomware attacks are disruptive to organisations and recovery costs can be significant. For more information on ransomware, read the latest **guidance** from the UK National Cyber Security Centre (NCSC).

This report is produced by the Scottish Cyber Coordination Centre (SC3) by drawing on open-source ransomware data and other threat intelligence sources. For more information please contact **SC3@gov.scot**

Scottish
Cyber
Coordination
Centre

Section 1: Ransomware Trends

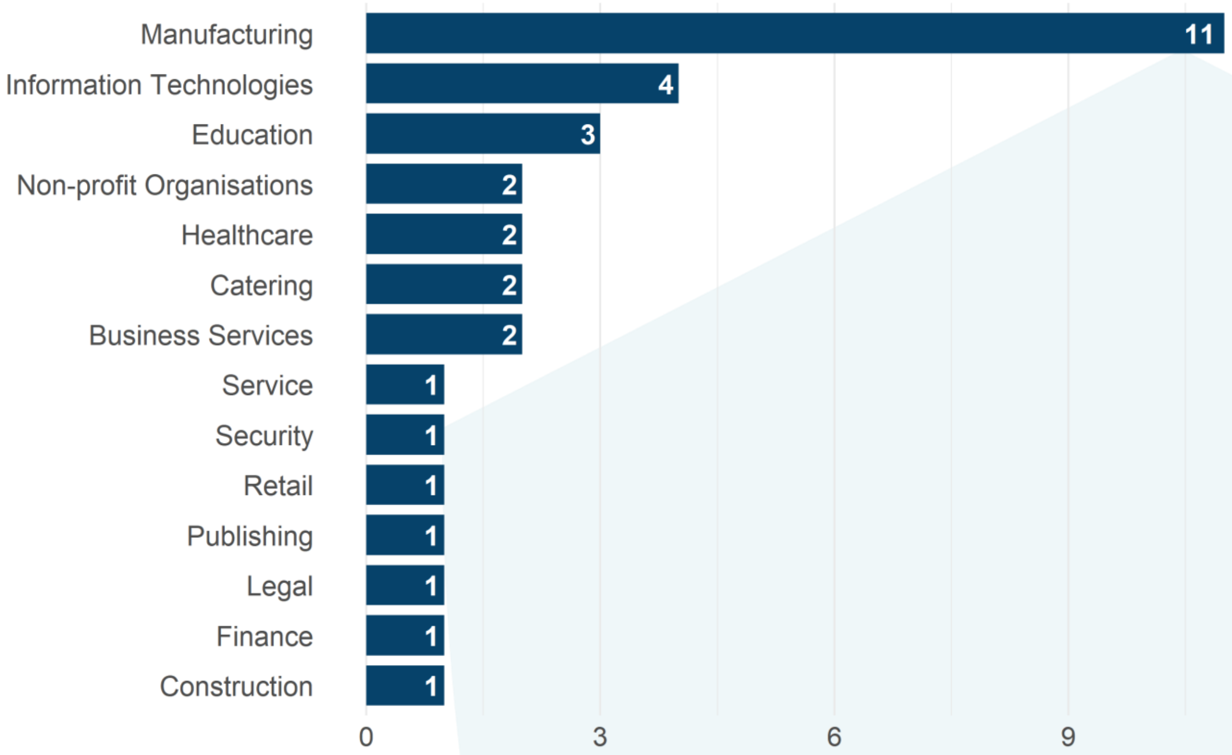
UK ransomware incidents by month, March-August 2024



In August 2024, there were 33 known ransomware incidents targeting UK organisations.[1] This was almost twice as many compared to July when there were 17 incidents. However, the available data does not yet indicate any clear, long-term trend.

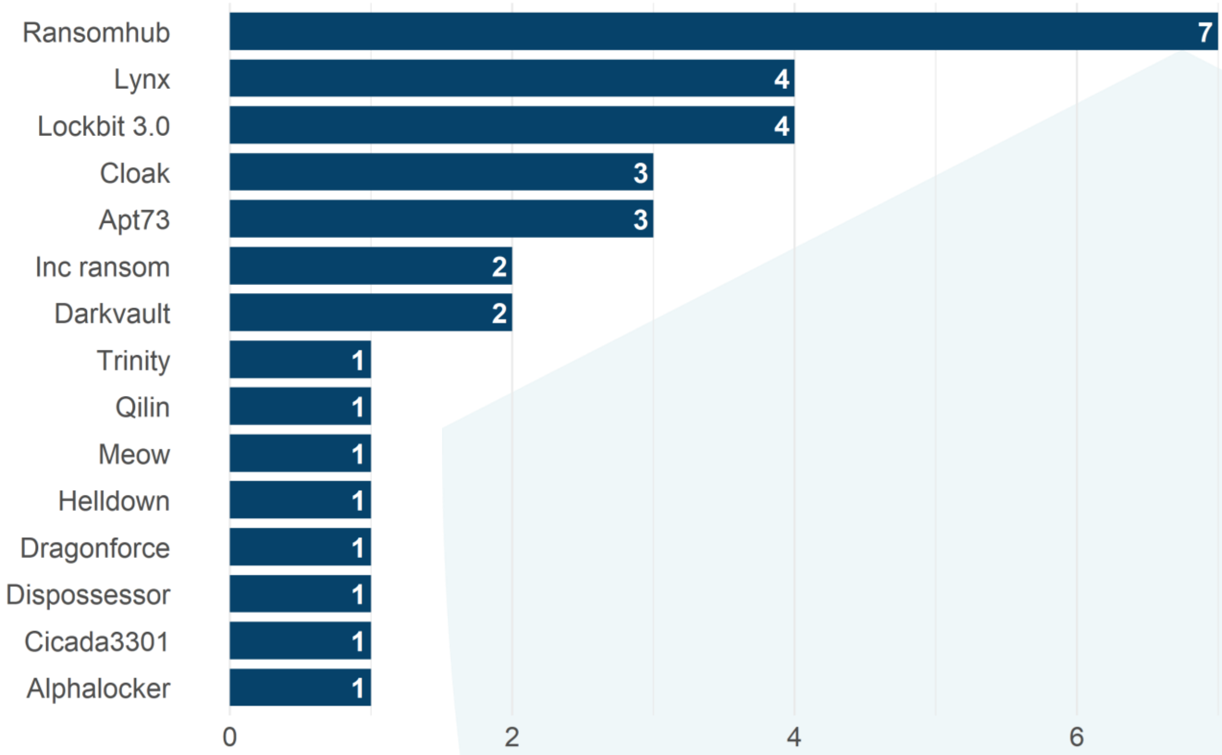
[1] The number of ransomware incidents reported may not reflect the actual number of incidents because some will not be publicly known.

UK ransomware incidents by sector, August 2024



Manufacturing was the most frequently targeted sector. There were 11 known ransomware incidents against manufacturing organisations in August. This represented one third of the total incidents in August – a larger proportion than in recent months. For example, in July just 1 of 17 incidents related to an organisation in the manufacturing sector.

UK ransomware incidents by threat actor, August 2024



15 different threat actors were responsible for all known UK ransomware incidents in August. The most prolific group was **Ransomhub** which was responsible for 7 ransomware attacks. This was more than any other threat actor during this period.

High profile victims of RansonHub include Planned Parenthood in the United States in September 2024.[2] The group exfiltrated sensitive data, including patient records, before demanding a ransom. Christie's Auction House was also attacked in May 2024.[3] The exfiltrated data allegedly contained names, dates of birth and nationalities of victims.

[2] Bleeping Computer, **Planned Parenthood confirms cyberattack as RansomHub claims breach** (5 September 2024)
[3] SC Media, **RansomHub threatens to leak data of Christie's auction house clients** (28 May 2024)

Section 2: Analysis of RansomHub

RansomHub is a malware family and ransomware group first identified in February 2024 which is a variant of Cyclops/Knight ransomware. It operates a Ransomware-as-a-Service (RaaS) model and its affiliates have already compromised over 210 victims internationally.

This section describes some of the tactics and techniques observed in RansomHub affiliates. The sources SC3 consulted to compile this information is listed at the end of this section.

Indicators of Compromise (IoCs) associated with RansomHub can be found in the appendix to this report. Further analysis and IoCs are available in the **CISA Cybersecurity Advisory**.

Initial access

- Phishing emails
- Exploitation of known vulnerabilities including:
  - **CVE-2023-3519** (Citrix ADC)
  - **CVE-2023-27997** (FortiOS)
  - **CVE-2023-46604** (Java OpenWire protocol marshaller)
  - **CVE-2023-22515** (Atlassian Confluence Data Centre and Server)
  - **CVE-2023-46747** (BIG-IP)
  - **CVE-2023-48788** (Fortinet FortiClientEMS)
  - **CVE-2017-0144** (Microsoft SMB)
  - **CVE-2020-1472** (Netlogon Remote Protocol)
  - **CVE-2020-0787** (Zerologon)
- Brute Force/Password spraying
- Compromising a Virtual Private Network (VPN)

Execution

- Using Secure Shell (SSH) protocol to access an organisation's NetApp Active IQ Unified Manager instance.
- Using the Unified Manager's default diagnostics account, diag, to execute the command su to switch to the user account root, then modified the file sshd_config to allow SSH logins to the root account.

- Using SSH to log into the root account from an external IP address and a customer's VPN IP address.

Defence Evasion

- Renaming the ransomware executable files with different names such as 'Windows.exe'
- Clearing logs on Windows and Linux systems
- Disabling antivirus software using Windows Management Instrumentation
- Using TDSSKiller (a legitimate tool from Kaspersky to remove rootkits) with the -dcsvc command to disable endpoint detection and response (EDR) systems.
- Using the Windows Control Panel (CPL) file appwiz.cpl to try to uninstall security software.
- Trying to modify registry settings, probably to try to use RansomHub's safeboot parameter to restart the system in safe mode.

Credential Access

- Using Mimikatz on Windows systems to gather credentials.

Discovery

- Conducting network scanning with tools like AngryIPScanner, Nmap, and PowerShell

Lateral Movement

- The affiliate moved laterally via Remote Desktop Protocol (RDP)
- Using SSH (Secure Shell Protocol) from NetApp Active IQ Unified Manager to move laterally to several NetApp storage clusters.

Command and Control

- Using Anydesk, a legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks.

Exfiltration

- Exfiltrating data over an asymmetrically encrypted network protocol other than that of the existing command and control channel
- Exfiltrating data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

Impact

- Attempting to execute a RansomHub Windows version (amd64.exe) to encrypt data on compromised devices
- Using *RansomHub* to encrypt NetApp ONTAP systems
- The ransomware deployment script deletes volume snapshots
- The ransomware deployment script shuts down targeted systems

Mitigations

- Apply patches promptly, particularly for known vulnerabilities such as those in Citrix and Fortinet.
- Enable multi-factor authentication (MFA) and implement network segmentation to limit lateral movement.
- Educate employees on ransomware threats, phishing tactics, and cybersecurity best practices to minimise the likelihood of falling victim to attacks.
- Implement network segmentation to isolate critical systems and sensitive data from less secure areas, reducing the potential impact of a ransomware breach.
- Implement multi-factor authentication (MFA) to reduce the risk of threat actors successfully leveraging compromised credentials
- When users do not manage their own applications, search for user sessions loading appwiz.cpl
- Use application allowlisting to ensure only pre-approved tools can be executed in the organization's network, which can prevent adversaries from executing unapproved tools2
- Search for commands featuring regex pattern -pass\s[a-z0-9]{64}, which RansomHub uses for execution

Sources

1. CrowdStrike intelligence reports
2. CISA, **#StopRansomware: RansomHub Ransomware** (29 August 2024)
3. Security Affairs, **RansomHub Ransomware Gang Relies on Kaspersky TDSKiller Tool to Disable EDR** (11 September 2024)

Appendix

Indicators of Compromise (IoCs) associated with RansomHub

Indicator	Type
37990333d47f8566710b609456500583	hash_md5
6290c21095d627fb86f1e4ac01a502cd	hash_md5
3b077778bef985761666aa6c5f5072d8	hash_md5
be510bba25a26936c283a3a870c2f763	hash_md5
41c5da33552e3f4a62fb3ef23d708561	hash_md5
5705b15c79a2e25e5893ad44124a650a	hash_md5
a0d8c263cb0c8a368f946d6ab96af506	hash_md5
354610622a0044d74b0ddd31fce9b3b4	hash_md5
faba9c27ccb5a525e72da3d86f72a7e045fb3a70	hash_sha1
2a2e15ae89f8b9809740c8e510ebb428c5caea9f	hash_sha1
773e8c8ddd69f3da588eb14f240d01fa710325a0	hash_sha1
22bc44cdf90ed069cc6d40fbff8ddeba4ba5db60	hash_sha1
8702fcbb6add93a54976594842515f91f8c1aa7e	hash_sha1
ad9510d111c66db851964792c0f5d834451e37bc	hash_sha1
3d29350a14c8d3e848f6d0503e27da4228f04260	hash_sha1
75a06569ecb6427dd1914f6e1fec3a889d92d075	hash_sha1
4f6a795b340ac74584165f4006f07522383dd93698f826fb9b40d7d719a2824d	hash_sha256
abf312f6f87ccc6ccc777a0b3c2ac21ff6475451572d579840099fe323fb4aa5	hash_sha256
e904e1407844eb35e74ef70064e8c6facd32fca0f4e1e87c8a32827413610d4e	hash_sha256

a7e57f8b533401decd14849be1b934197c72435187b55305bc566cac6444bd7c	hash_sha256
c6ac071aa3b2703281f38eb92b25e574d1fea4d01f5c18be2110e7adfdc84c7d	hash_sha256
2c7b45efd12ce63a4d702e67813dac885d8dff96c4d5eb03a00de0d9acbc154f	hash_sha256
586edbee968fc2eb2cf2495b218336c99f496fa83e48eeb255e3af17aa84a8c5	hash_sha256
f0982c63b5006fdcfed5b582b5df500b27033ecea5cba5e09886a816ece6058c	hash_sha256