Scottish Cyber Coordination Centre

UK Ransomware Report, September 2024

14 October 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.

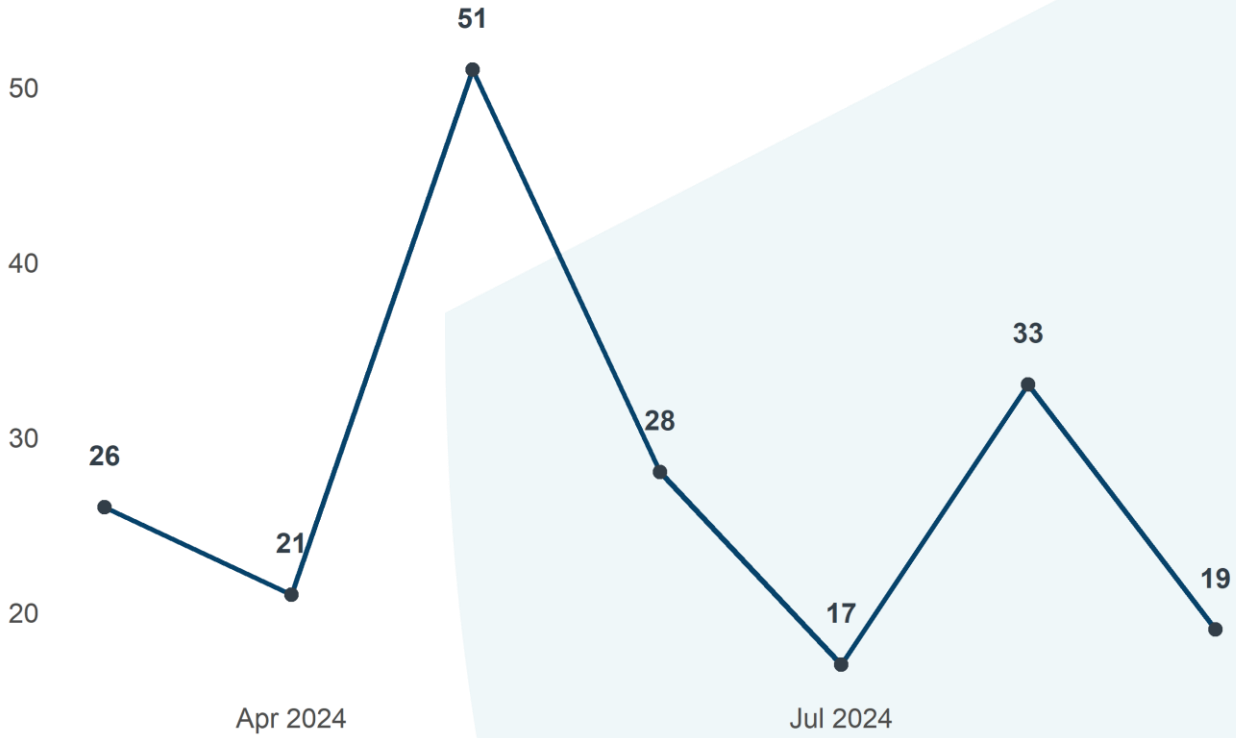
Ransomware attacks are disruptive to organisations and recovery costs can be significant. For more information on ransomware, read the latest guidance from the UK National Cyber Security Centre (NCSC).

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-September 2024

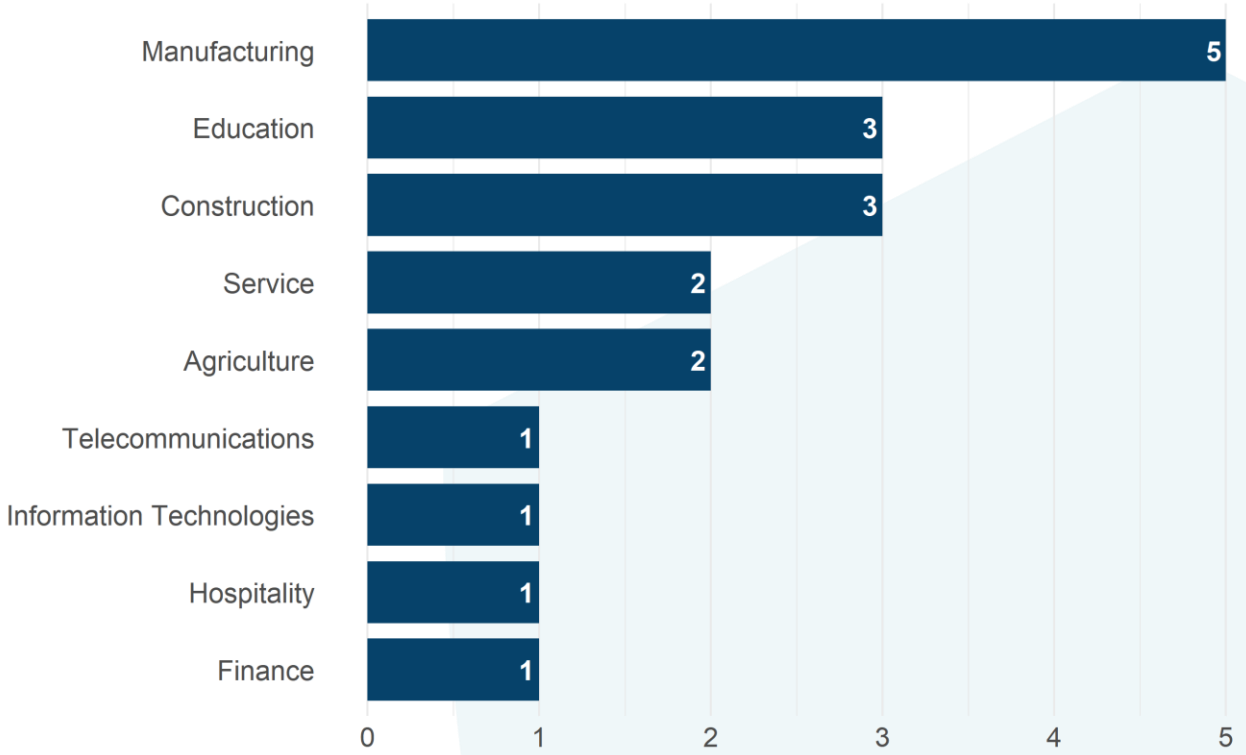


In September 2024, there were 19 known ransomware incidents targeting UK organisations.[1] This was a decrease from the 33 incidents recorded in August. The available data does not yet indicate any clear, long-term trend.

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

Scottish Cyber Coordination Centre

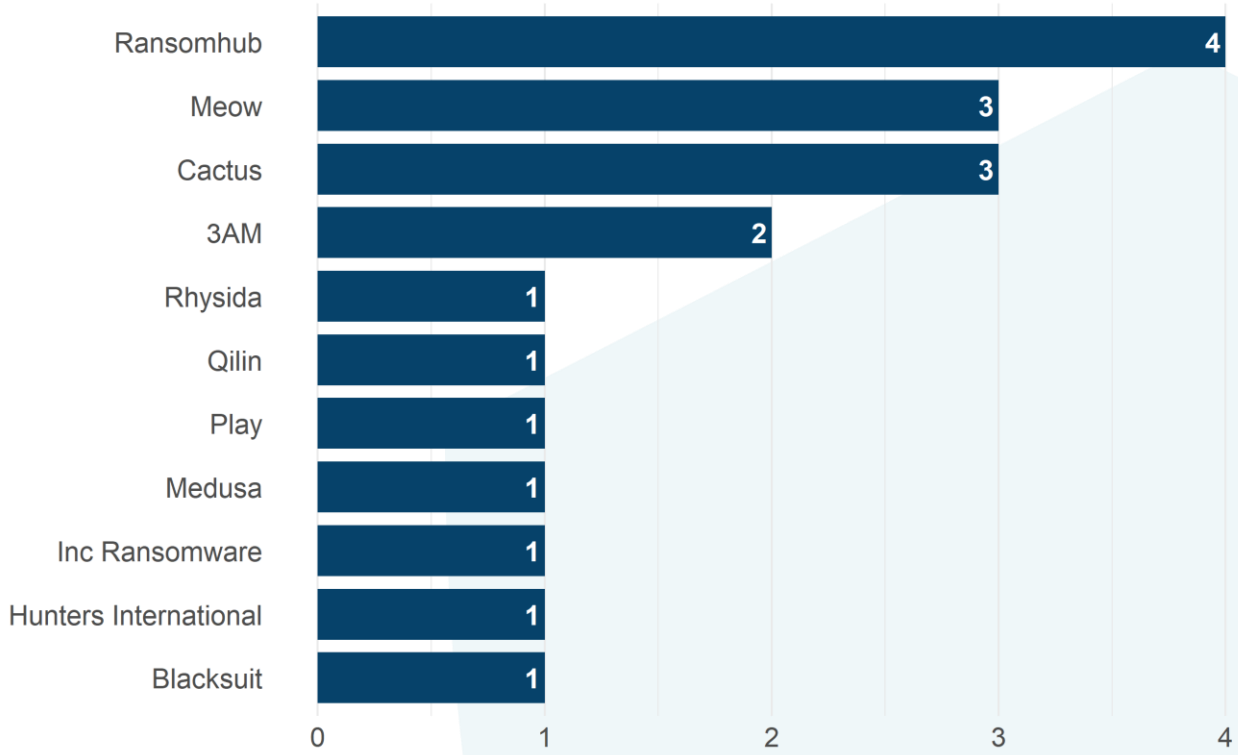
UK ransomware incidents by sector, September 2024



Manufacturing continues to be the most frequently targeted sector. There were 5 known ransomware incidents against UK based manufacturing organisations in September. These accounted for just over a quarter of total UK incidents reported during September.

Scottish Cyber Coordination Centre

UK ransomware incidents by threat actor, September 2024



11 different threat actors were responsible for all known UK ransomware incidents in September. The RansomHub group claimed responsibility for 4 attacks, while both Cactus and Meow each took credit for 3.

SC3 have already published a profile on Ransomhub in the August 2024 UK Ransomware Report. This month's report will focus on Cactus.

High-profile victims of Cactus include Schneider Electric in January 2024. The attack resulted in the exfiltration of terabytes of data, used to extort the company. Schneider Electric is a French multinational company, specialising in energy management and automation, with a revenue of £23.4 billion in 2023, and is headquartered in Rueil-Malmaison, France.[2] Chubb Bulleid, a prominent law firm based in Somerset, UK, has recently fallen victim to a ransomware

[2] Bleeping Computer, Energy giant Schneider Electric hit by Cactus ransomware attack (29 January 2024)

attack orchestrated by the Cactus ransomware group. The attack, disclosed in July 2024, has led to the exposure of a significant amount of sensitive and confidential information.[3]

Section 2: Analysis of Cactus

Cactus ransomware is a malware family first identified in early 2023. It operates a Ransomware-as-a-Service (RaaS) model, targeting primarily large organisations by exploiting known vulnerabilities and leveraging encryption techniques to evade detection. Cactus is noted for its unique self-encryption feature, which encrypts its own payload to bypass security systems. Since its discovery, it has been used in multiple high-profile attacks affecting various sectors, predominantly in the manufacturing sector.

This section outlines the tactics, techniques, and procedures (TTPs) observed in Cactus ransomware campaigns, compiled from several sources including CrowdStrike, SOC Radar and Bitdefender. Indicators of Compromise (IoCs) related to Cactus ransomware are provided in the appendix.

Resource Development (TA0042)

- The Cactus ransomware group appears to have custom-built its self-encrypting payload to evade detection. This capability suggests that the group invests in tool development to enhance its effectiveness and stealth.

Initial Access (TA0001)

- Exploits known vulnerabilities in popular software and hardware systems including:
  - **CVE-2023-41266**, **CVE-2023-41265** & **CVE-2023-48365** (Qlik Sense Enterprise for Windows)
  - **CVE-2023-38035** (Ivanti)
- Targets unpatched or misconfigured VPNs followed by the creation of an SSH backdoor

[3] Halcyon, Chubb Bulleid Law Firm targeted by Cactus Ransomware Group (30 July 2024)

Scottish Cyber Coordination Centre

Execution (TA0002)

- Uses Windows Scheduled Tasks to delay execution
- Uses a batch script to execute the ransomware with 7-Zip – this technique allows the ransomware to self-encrypt and evade detection by many security tools, which would typically scan the ransomware executable.
- The ransomware operators simulate attacks using Cobalt Strike, which is often used for executing payloads, deploying backdoors, or gaining additional privileges on the system.

Persistence (TA0003)

- Cactus Ransomware ensures its persistent presence within the compromised system by creating a scheduled task named “Updates Check Task” that runs every 5 minutes, thereby running the ransomware as SYSTEM and ensuring that its malicious activities continue without a problem.
- The attackers employ legitimate tools like Splashtop and AnyDesk to maintain persistent access to compromised systems, blending in with legitimate software and bypassing traditional defences.

Defence Evasion (TA0005)

- Cactus encrypts its ransomware payload to evade detection by endpoint security solutions.
- The ransomware decrypts itself upon execution using a specific command-line argument, bypassing traditional antivirus scanning during deployment.
- Cactus affiliates rename ransomware files to appear as legitimate system processes (e.g., "update.exe").
- System event logs are cleared to remove traces of malicious activity.
- Leveraging tools like Windows Defender’s MpCmdRun.exe to disable or impair security solutions.

Credential Access (TA0006)

- Use of tools like Mimikatz to extract passwords from compromised systems.
- Brute-forcing administrative credentials and exploiting weak authentication mechanisms.

Scottish Cyber Coordination Centre

Discovery (TA0007)

- Conducts network scanning using tools such as Nmap and PowerShell commands to identify lateral movement opportunities
- Performs System Network Connection Discovery to gather information on all connected devices

Lateral Movement (TA0008)

- Uses SSH and RDP protocols to move laterally within compromised environments
- Ransomware was deployed to other machines using PsExec

Command and Control (TA0011)

- Access to the target computer was obtained using Splashtop or AnyDesk
- SOCK5 proxy between infected hosts was created using Chisel

Exfiltration (TA0010)

- Encrypts exfiltrated data and sends it through encrypted channels to evade detection
- Sensitive data and files were exfiltrated to cloud storage using Rclone

Impact (TA0040)

- Deploys ransomware to encrypt data on critical systems using AES and RSA encryption
- Deletes volume snapshots to prevent recovery using built-in system tools
- Shuts down systems to prevent response teams from interrupting encryption processes
- Threatens double extortion by threatening to leak exfiltrated data on Tor-hosted DLS sites, if the ransom is not paid

Mitigations

- Ensure that all VPN software and devices are patched and updated to shield against vulnerabilities exploited by Cactus.
- Employ robust antivirus and EDR/EPP solutions capable of detecting and mitigating threats posed by self-encrypting ransomware.

Scottish Cyber Coordination Centre

- Monitor suspicious behaviour looking for specific commands such as 'Invoke-Mimikatz' or PowerShell sessions executing with unusual privileges.
- Implement multi-factor authentication (MFA) to reduce the risk of brute force attacks being successful.
- Enable multi-factor authentication (MFA) and implement network segmentation to limit lateral movement.
- Implement network segmentation to isolate critical systems and sensitive data from less secure areas, reducing the potential impact of a ransomware breach.
- Ensure that data is backed up regularly and that backup systems are isolated from the network to safeguard against encryption.
- Educate employees on ransomware threats, phishing tactics, and cybersecurity best practices to minimise the likelihood of falling victim to attacks.

Sources

1. CrowdStrike intelligence reports
2. SOC Radar, **Dark Web Profile: Cactus Ransomware** (2 Jan 2024)
3. Bitdefender, **CACTUS: Analyzing a Coordinated Ransomware Attack on Corporate Networks** (28 Feb 2024)
4. Logpoint, Cactus Ransomware: How it works and how to respond? (24 Nov 2023)
5. Kroll, **CACTUS Ransomware: Prickly New Variant Evades Detection** (10 May 2023)

Scottish Cyber Coordination Centre

Appendix

Indicators of Compromise (IoCs) associated with Cactus

Indicator	Type
d9f15227fefb98ba69d98542fbe7e568	hash_md5
3adc612b769a2b1d08b50b1fb5783bcf	hash_md5
be7b13aee7b510b052d023dd936dc32f	hash_md5
26f3a62d205004fbc9c76330c1c71536	hash_md5
b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b	hash_sha256
5b70972c72bf8af098350f8a53ec830ddbd5c2c7809c71649c93f32a8a3f1371	hash_sha256
78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17	hash_sha256
248795453ceb95e39db633285651f7204813ea3a	hash_sha1
6715b888a280d54de9a8482e40444087fd4d5fe8	hash_sha1
78aea93137be5f10e9281dd578a3ba73	hash_md5
39fe99d2250954a0d5ed0e9ff9c41d81	hash_md5
0e4ee38fe320cfb573a30820198ff442	hash_md5
8d2e4bef47e3f2ee0195926bbf4a25d5	hash_md5
f7a6d1e6e5436bd3c10f3a26f3e9b9b9	hash_md5
fb467a07f44e8d58e93e3567fd7ff016	hash_md5
be139fc480984eb31de025f25a191035	hash_md5
08d2c800c93015092e14738c941ac492	hash_md5
02e4da16377fc85e71a8c8378b2a8a96	hash_md5
8b37df9d295bbc2906961f72b7cdc5fb	hash_md5

Scottish Cyber Coordination Centre

8af259ad55c3746926e992c82bc7e850	hash_md5
55e42014424c0d120ff17f11e207e4f0	hash_md5
5f7c3cda7759ef6e577552ad322c1f64	hash_md5
64.52.80.252	C2
162.33.177.56	C2
45.61.138.99	C2
206.188.196.20	C2
45.61.136.79	C2
45.61.136.127	C2
85.206.172.127	Attacker IP
192.227.190.11	Attacker IP
154.18.12.125	Attacker IP