Scottish Cyber Coordination Centre

UK Ransomware Report, October 2024

15 November 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.

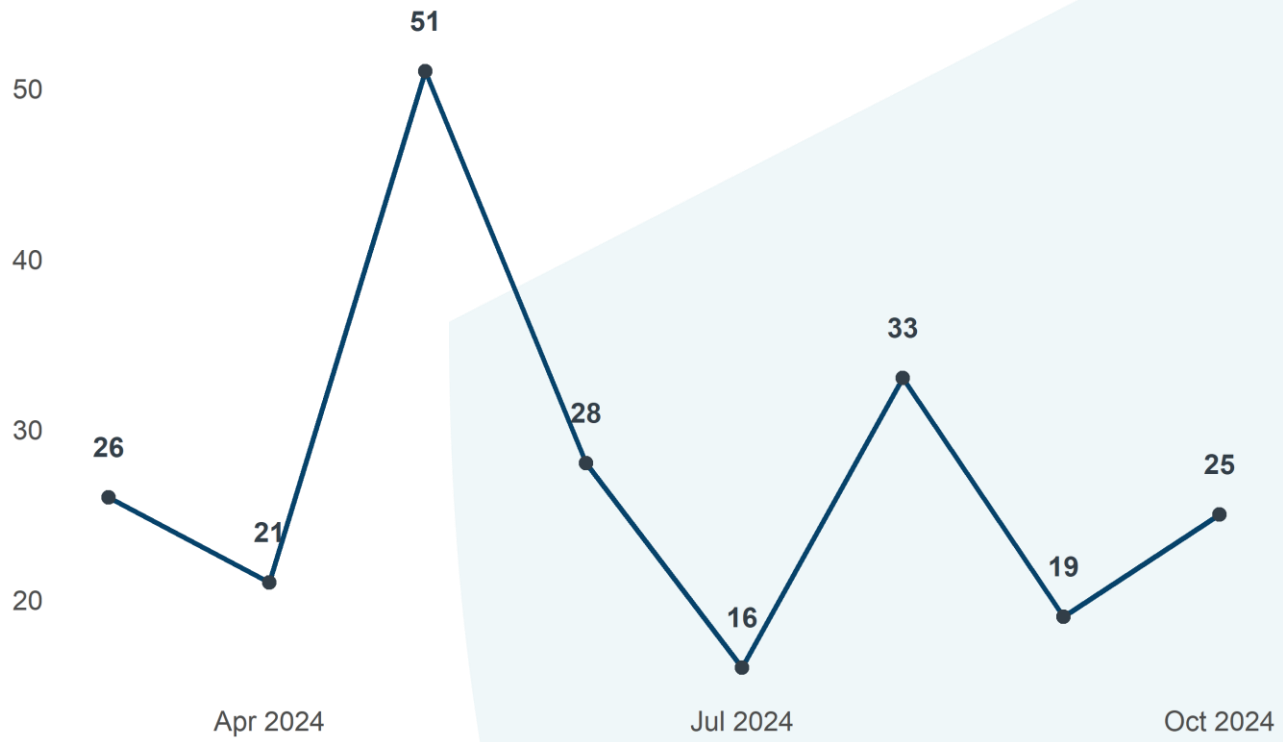
Ransomware attacks are disruptive to organisations and recovery costs can be significant. For more information on ransomware, read the latest **guidance** from the UK National Cyber Security Centre (NCSC).

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

Scottish Cyber Coordination Centre

Section 1: Ransomware Trends

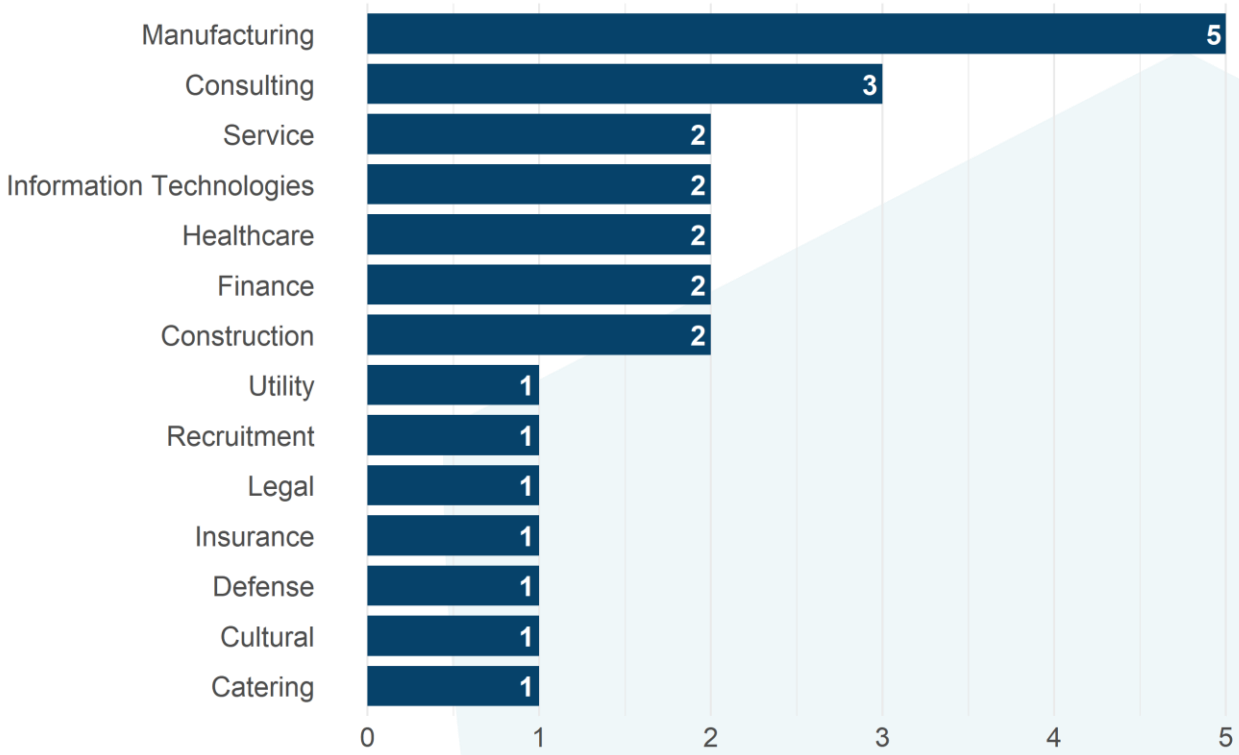
UK ransomware incidents by month, March-October 2024



In October 2024, there were an estimated 25 known ransomware incidents targeting UK organisations. To put this into context, the average number of monthly incidents since March 2024 is 26, although there are often considerable fluctuations in the monthly count. The current data does not yet highlight a clear, long-term trend.

Scottish Cyber Coordination Centre

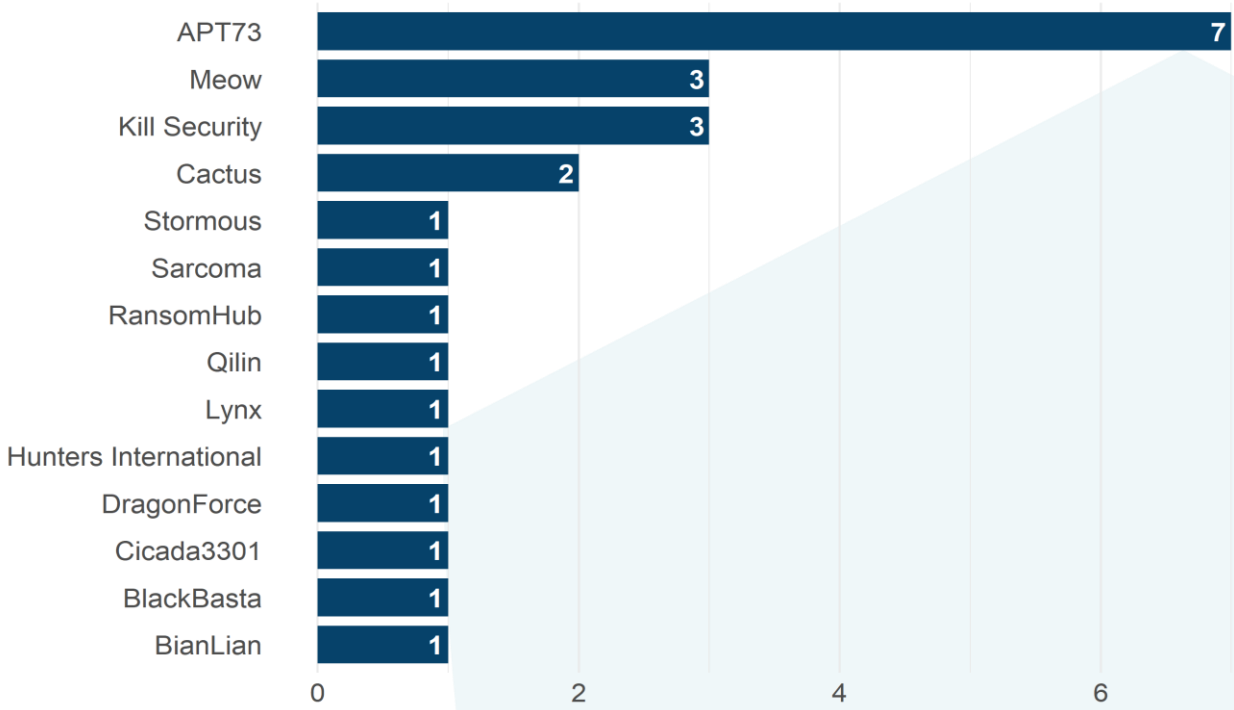
UK ransomware incidents by sector, October 2024



The manufacturing sector remains the most frequently targeted. There were an estimated 5 ransomware incidents affecting manufacturing organisations in October, which accounted for one-fifth of all incidents this month. The consulting sector saw a notable increase in incidents with 3 cases this month, despite none being observed since June 2024.

Scottish Cyber Coordination Centre

UK ransomware incidents by threat actor, October 2024



14 different threat actors were responsible for the ransomware attacks observed in October. ATP73 was responsible for 7 of these incidents, more than any other group. Additionally, both Cactus and Meow remained active; each group carried out between 2 or 3 attacks in September and October.

Notable victims of APT73 include CDS, a subsidiary of Hewlett Packard Enterprise, from which approximately 500GB of sensitive company data, including confidential and employee documents, was exfiltrated.[1] APT73 also targeted Gannons Solicitors, a UK-based commercial law firm, extracting 2.3MB of data comprising sensitive legal documents and client information.[2]

Section 2: Analysis of ATP73

[1] Ransomlook, **Group Profile: APT73** (2024)
[2] Halycon, **Ransomware on the Move: Play, APT73, BlackSuit, Hunters International** (2024)

Scottish Cyber Coordination Centre

APT73 is a ransomware group that emerged in late April 2024 and has quickly positioned itself as a significant cyber threat. Believed to be a spinoff from LockBit, APT73's tactics and the design of its Data Leak Site (DLS) closely resemble those of its predecessor, suggesting shared techniques and infrastructure.[3]

Operating a Ransomware-as-a-Service (RaaS) model, APT73 primarily targets large enterprises, exploiting vulnerabilities through spear-phishing and infrastructure breaches. Despite its recent formation, the group has rapidly expanded its influence through dual-extortion tactics, encrypting sensitive data and threatening to leak exfiltrated information.[4]

After initial attacks in June 2024, APT73 went offline, decommissioning its older DLS domains in July and August. The group resurfaced in September 2024 with an expanded victim list, naming three victims in September and six in October. To date, APT73 has listed approximately 20 verified victims, primarily targeting UK-based organisations.[5]

Resource Development (TA0042)

- APT73's development efforts include custom ransomware payloads, possibly adapted from LockBit's base code. This adaptation suggests an investment in creating malware suited to its operational style and deployment methods.

Initial Access (TA0001)

- APT73's preferred initial access tactic involves phishing emails, which trick victims into downloading malware or entering credentials that allow attackers to infiltrate the network.

[3] Cyfirma, **Tracking Ransomware: April 2024** (2024)
[4] Halycon, **Ransomware on the Move: Play, APT73, BlackSuit, Hunters International** (2024)
[5] Medium, **APT73/Eraleig News: Unveiling New Ransomware Group** (2024)

Scottish Cyber Coordination Centre

Exfiltration (TA0010)

- The group exfiltrates via encrypted channels from where it can be accessed for extortion. The encryption of exfiltrated data provides an added layer of security, making it harder for detection tools to identify the activity.

Impact (TA0040)

- APT73's ransomware encrypts vital data rendering critical files inaccessible to the victim without decryption keys. To amplify its impact, APT73 threatens double extortion, pressuring victims by threatening to release sensitive information on the dark web if the ransom goes unpaid.

Mitigations

To defend against APT73 and similar threats, organisations should focus on:

- Enhancing email security and training to prevent employees from engaging with phishing emails.
- Deploying endpoint detection and response (EDR) solutions that can detect abnormal activities associated with ransomware.
- Reinforcing access controls with Multi-Factor Authentication to mitigate risks associated with credential theft and brute-force attacks.
- Ensuring that critical data backups are kept offline or in a separate network environment to prevent encryption by ransomware.

Sources

1. Halycon, **Emerging Ransomware Threat Actors** (2024)
2. Ransomlook, **Group Profile: APT73** (2024)
3. Medium, **APT73/Eraleig News: Unveiling New Ransomware Group** (2024)
4. AlienVault, **APT73/Eraleig news: unveiling new ransomware group** (2024)

Scottish Cyber Coordination Centre

Appendix

Indicators of Compromise (IoCs) associated with APT73

Indicator	Type
6d170d36a4d6b47987f51445b24e587c	hash_md5
94895ed0dc352981fbec38b5348ec3ae3be26371	hash_sha1
f1a00e2fe86455b9d1a384d5e96185e016816acd1d7ef3460e232e9ecb9da79	hash_sha256
176.97.75.205	IPv4
http://qcgv5tfer4f46ns6ohh72zeyyh5uavoiybypzpt3lmwk5ecyqykptgqd.onion/files/trifecta.zip	URL
eraleignews.com	Domain
qcgv5tfer4f46ns6ohh72zeyyh5uavoiybypzpt3lmwk5ecyqykptgqd.onion	Domain
qku4reiyfcs2vqq5tow2uprhyqhweo56lrgs6457svr3ej4ton5frkad.onion	Domain
http://wn6vonooq6fggjdgyocp7bioykmfjket7sbp47cwhgubvowwd7ws5pyd.onion/	Domain
http://basheqtvzqwz4vp6ks5lm2ocq7i6tozqgf6vjcasj4ezmsy4bkpshhyd.onion/	Domain
http://bashe4aec32kr6zbifwd5x6xgjsmhg4tbowrbx4pneqhc5mqooyifpid.onion/	Domain
http://basheqtvzqwz4vp6ks5lm2ocq7i6tozqgf6vjcasj4ezmsy4bkpshhyd.onion	Domain
http://basherq53eniermxovo3bkduw5qqq5bkqcml3qictfmamgvmzovykyqd.onion	Domain
http://basherykagbxoaiaxkgqhmhd5gbmedwb3di4ig3ouovziagosv4n77qd.onion	Domain
http://bashete63b3gcijfofpw6fmn3rwnmyi5aclp55n6awcfbexivexbhyad.onion	Domain

Scottish Cyber Coordination Centre

http://bashex7mokreyoxl6wlswxl4foi7okgs7or7aergnuiockuoq35yt3ad.onion	Domain