Scottish Cyber Coordination Centre

UK Ransomware Report, December 2024

13 January 2025

This report describes the ransomware threat landscape for the UK in December 2024. 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.

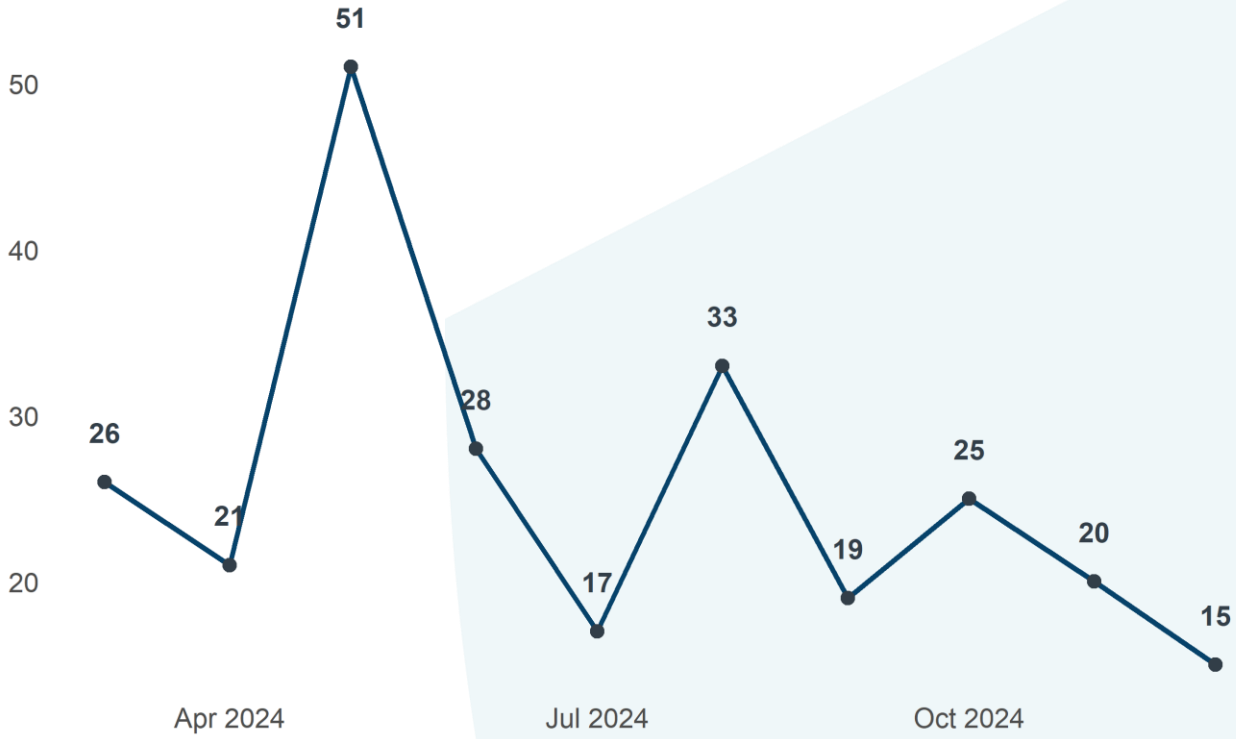
Ransomware attacks are disruptive to organisations and recovery costs can be significant. For more information on ransomware, read the latest **guidance** from the UK National Cyber Security Centre (NCSC).

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

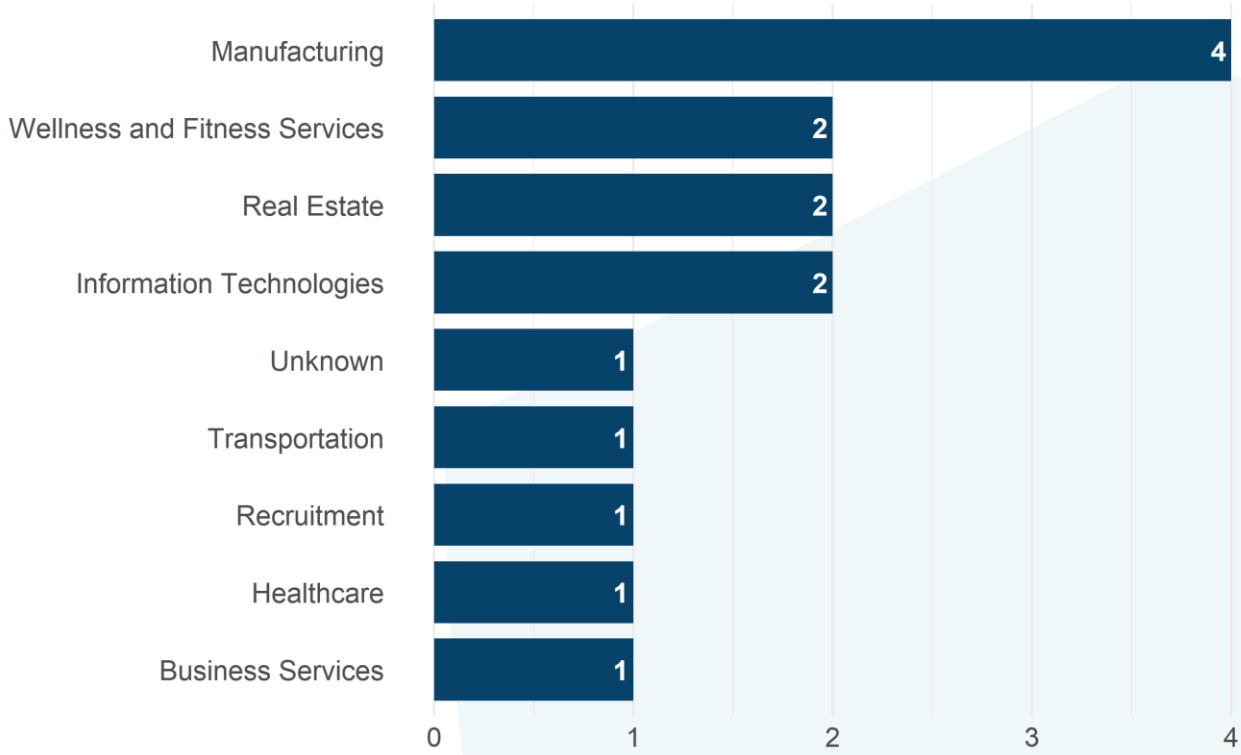
UK ransomware incidents by month



In December 2024, there were 15 known ransomware incidents targeting UK organisations. This was five fewer than the previous month. However, the available data does not yet indicate any clear, long-term trend.

Scottish Cyber Coordination Centre

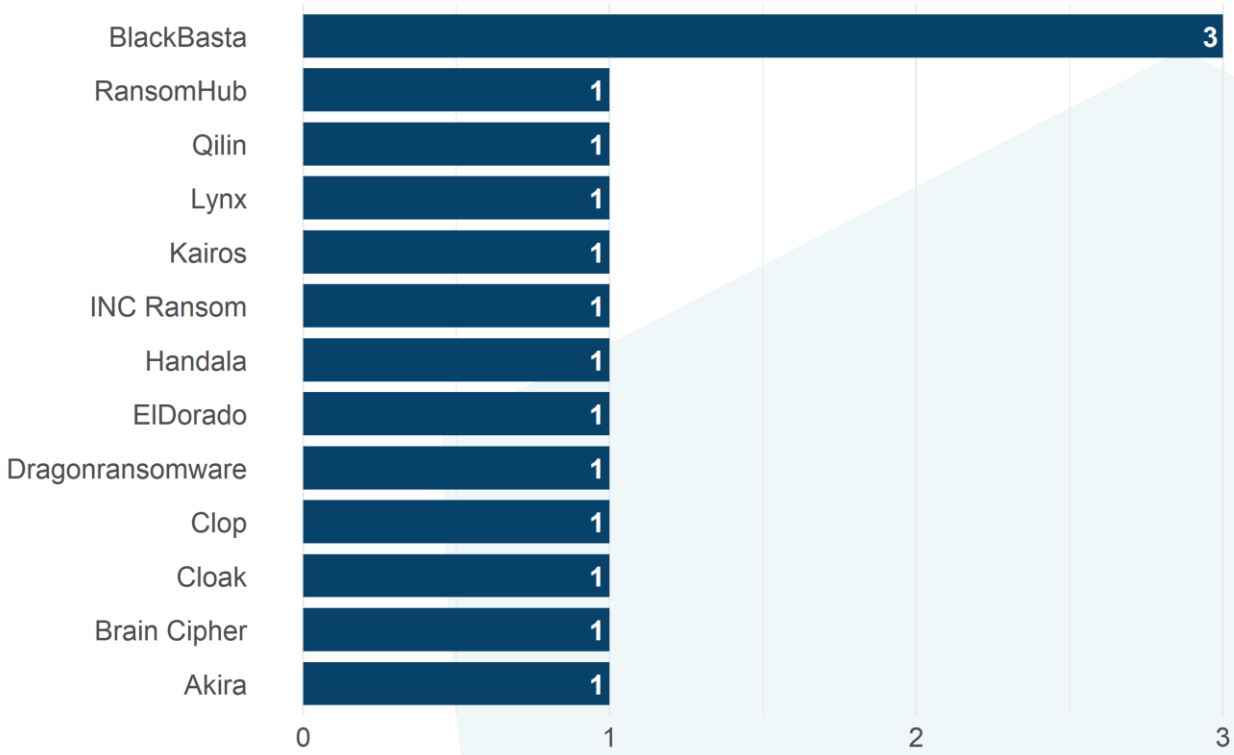
UK ransomware incidents by sector, December 2024



Manufacturing was the most frequently targeted sector. There were 4 known ransomware incidents against manufacturing organisations in December.

Scottish Cyber Coordination Centre

UK ransomware incidents by threat actor, December 2024



13 different threat actors were responsible for all known UK ransomware incidents in December. The most prolific group was BlackBasta which was responsible for 3 attacks.

High-profile victims of Black Basta include several notable organisations. The UK-based telecommunications giant BT Group experienced a ransomware breach in December 2024, leading its BT Conferencing business division to shut down servers.[1] Ascension, one of the largest private U.S. healthcare providers, was attacked and had the personal and healthcare data of 5.6 million patients and employees stolen in May 2024. The scale of the cyber attack is estimated to cost approximately $1.3 billion.[2]

---

[1] Bleeping Computer, **BT unit took servers offline after Black Basta ransomware** breach (4 December 2024)
[2] HealthcareITNews, **Ascension confirms data breached in Black Basta ransomware attack** (13 June 2024)

Scottish Cyber Coordination Centre

Section 2: Analysis of Black Basta Ransomware

Black Basta is a Ransomware-as-a-Service (RaaS) group which emerged in April 2022. Operating under a tightly controlled affiliate model, the group has had a significant impact across multiple sectors, primarily targeting industrial, engineering, and manufacturing organisations.

To date, Black Basta's dedicated leak site has featured 578 posts, exposing sensitive data from 31 distinct sectors. Most of Black Basta's victims are based in the United States, accounting for 340 of the total posts, followed by entities in Germany and the United Kingdom, with 43 UK-based victims identified. This distribution highlights the group's focus on Western economies and high-value industries.

Despite their extensive operations, Black Basta maintains a selective affiliate base. WANDERING SPIDER, a highly active adversary group, has been responsible for over 90% of observed Black Basta incidents. Other actors, such as TUNNEL SPIDER, have also been identified deploying the ransomware. [1]

Analysis of blockchain transactions reveals a direct connection between Black Basta and the Conti Group, a Russian ransomware gang that ceased operations in 2022. The timing of Conti's dissolution coinciding with Black Basta's emergence suggests a possible evolution or rebranding of the group.[2]

Black Basta employs a dual-extortion model, encrypting victim data while threatening to publish exfiltrated information to pressure organisations into paying ransoms. Ransom notes from Black Basta lack initial ransom demands or payment instructions, instead giving victims a unique code and an Onion URL for contact via the Tor browser. Victims usually have 10-12 days to pay before their data is published on the Black Basta TOR site, Basta News.[3]

---

[1] CrowdStrike Intelligence Reports
[2] Elliptic, **Black Basta ransomware victims have paid over $100 million** (29 November 2023)
[3] CISA, **#StopRansomware: Black Basta** (8 November 2024)

Black Basta's use of innovative social engineering has also set them apart from other ransomware groups. Recent incidents highlight their impersonation of IT support personnel via platforms like Microsoft Teams, tricking employees into granting access to sensitive systems.[1] This method complements their technical arsenal, illustrating their ability to exploit human vulnerabilities alongside technological flaws.

Black Basta employs a blend of advanced malware techniques and sophisticated social engineering. Their relentless targeting of high-value assets and critical sectors underscores their status as a significant threat to organisations in Western countries, especially within the industrial and healthcare sectors.

Initial Access (TA0001)

Black Basta affiliates primarily use spear phishing to gain initial access. They have also leveraged Qakbot during this phase. In February 2024, Black Basta began exploiting the ConnectWise vulnerability CVE-2024-1709. Additionally, affiliates have been observed conducting social engineering by impersonating IT support personnel on Microsoft Teams to trick employees into granting system access.

Discovery (TA0007) and Execution (TA0002)

Black Basta affiliates utilise tools like the SoftPerfect network scanner (netscan.exe) for network scanning. Cybersecurity experts have identified affiliates performing reconnaissance with utilities disguised under innocuous file names such as Intel or Dell, placed in the root directory.

Persistence (TA0003)

Persistence is maintained using Cobalt Strike beacons and other legitimate tools, enabling long-term access to compromised networks.

---

[1] Bleeping Computer, **Black Basta ransomware poses as IT support on Microsoft Teams to breach networks** (25 October 2024)

Scottish Cyber Coordination Centre

Privilege Escalation (TA0004)

Black Basta exploit known vulnerabilities to escalate privileges within compromised environments, employing tools like Mimikatz to harvest credentials. Black Basta have exploited common vulnerabilities such as **ZeroLogon**, **NoPac** and **PrintNightmare** for local and Windows Active Domain privilege escalation.

Defence Evasion (TA0005)

To evade detection, Black Basta affiliates have named files with innocuous names such as Intel or Dell. They have also deployed a tool called Backstab to disable endpoint detection and response (EDR) tools and used PowerShell to disable antivirus products.

Lateral Movement (TA0008)

Tools like BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), are commonly observed for lateral movement. Additionally, some affiliates employ tools such as Splashtop, Screen Connect, and Cobalt Strike beacons to facilitate remote access and lateral movement.

Collection (TA0009)

Black Basta affiliates gather sensitive data, including intellectual property and financial information, from high-value assets identified during discovery. Data is compressed and encrypted before exfiltration, minimising detection by network monitoring tools.

Exfiltration (TA0010)

Black Basta affiliates use RClone to exfiltrate data before encryption. Before this process, they disable antivirus products and EDR tools.

Impact (TA0040)

Black Basta affiliates have utilised the vssadmin.exe programme to delete shadow copies before using a public key to fully encrypt files. This encryption targets critical systems and data, rendering them inaccessible and causing significant operational disruption. They also employ dual-extortion tactics,

threatening to publish stolen data on their dedicated leak site if ransom demands are not met.

Mitigations

To defend against Black Basta ransomware and similar variants or threats, organisations should focus on:

- Enhancing employee awareness through training to recognise phishing emails, malicious links, and suspicious attachments, including tactics such as impersonation on communication platforms like Microsoft Teams. Encourage employees to report such threats promptly.
- Enforcing robust password policies, requiring complex, unique passwords and preventing reuse across multiple accounts or services.
- Implementing Multi-Factor Authentication (MFA) for all user accounts, including remote access and privileged accounts, to reduce the risk of credential theft or brute-force attacks.
- Regularly updating and patching systems to address vulnerabilities in operating systems, applications, and firmware. Prioritise critical updates, particularly for Known Exploited Vulnerabilities (KEV) such as PrintNightmare and vulnerabilities in VPN appliances. These can be found in CISA's KEV catalog.
- Deploying EDR solutions to detect suspicious activity and halt ransomware execution. Ensure these solutions can identify advanced malware, such as Qakbot, Lumma and DarkGate.
- Implementing network segmentation to limit lateral movement within the organisation. Isolate critical systems, including backups, to reduce the impact of a potential breach.
- Monitoring network traffic for unusual activity or communication with known command-and-control servers. This includes reviewing logs for unauthorised access attempts or anomalous behaviour.

Sources

1. CrowdStrike Intelligence Reports
2. CISA, **#StopRansomware: Black Basta** (8 November 2024)
3. Cyfirma, **Black Basta: Ransomware** (13 November 2024)

4. Qualys, **Black Basta Ransomware: What You Need to Know** (19 September 2024)
5. Rapid7, **Black Basta Ransomware Campaign Drops Zbot, DarkGate, and Custom Malware** (23 December 2024)
6. Bleeping Computer, **Black Basta ransomware poses as IT support on Microsoft Teams to breach networks** (25 October 2024)

Scottish Cyber Coordination Centre

Appendix

Indicators of Compromise (IoCs) associated with Black Basta

Indicator	Type
170.130.165[.]73 45.11.181[.]44 79.132.130[.]211	Likely Cobalt Strike infrastructure
66.42.118[.]54	Exfiltration server
Moereng[.]com	Domain
Exckicks[.]com	Domain
securityadminhelper.onmicrosoft[.]com supportserviceadmin.onmicrosoft[.]com supportadministrator.onmicrosoft[.]com cybersecurityadmin.onmicrosoft[.]com	Fake accounts impersonating help desk addresses
AntispamConnectUS.exe	Malware file name
3ea66e531e24cddcc292c758ad8b51d5	MD5
cf7af42525e715bd77f8465f6ac0fd9e5bea0da0	SHA256
A downloadable list of IOCs, provided as part of a joint cybersecurity advisory, can be found **here**	