Scottish Cyber Coordination Centre

UK Ransomware Report, November 2024

16 December 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.

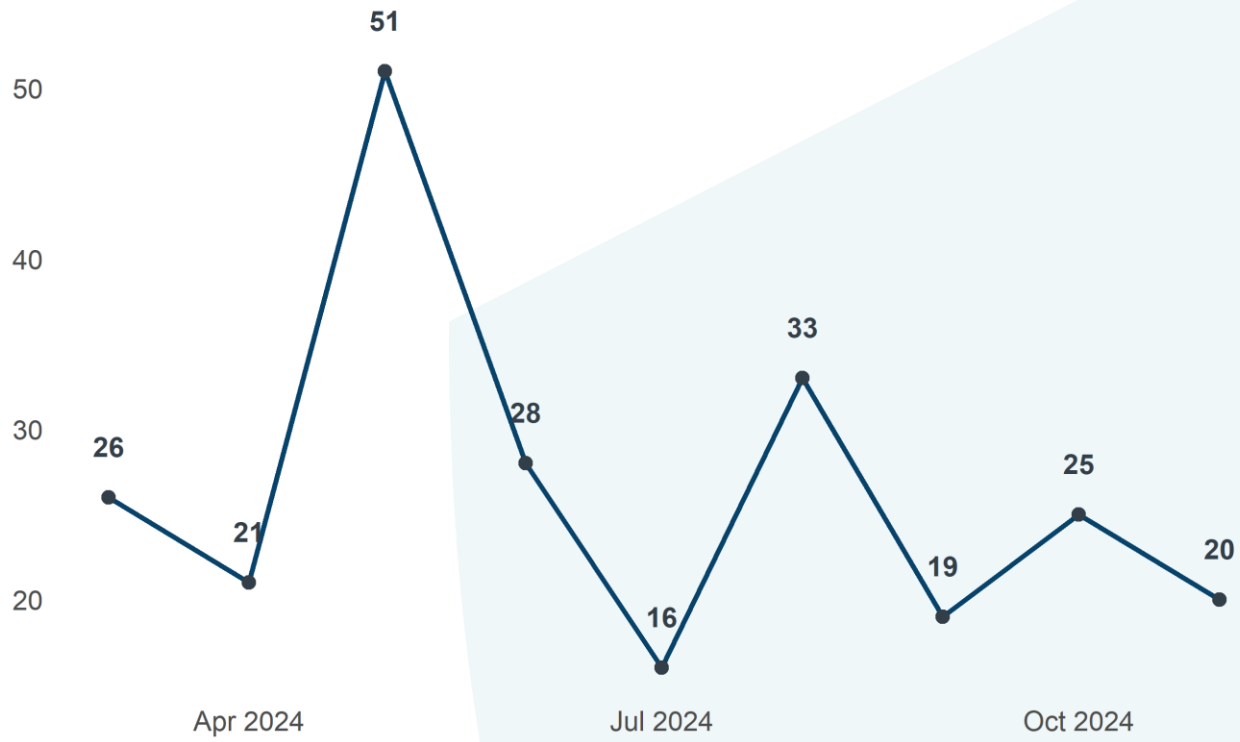
Ransomware attacks are disruptive to organisations and recovery costs can be significant. For more information on ransomware, read the latest **guidance** from the UK National Cyber Security Centre (NCSC).

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

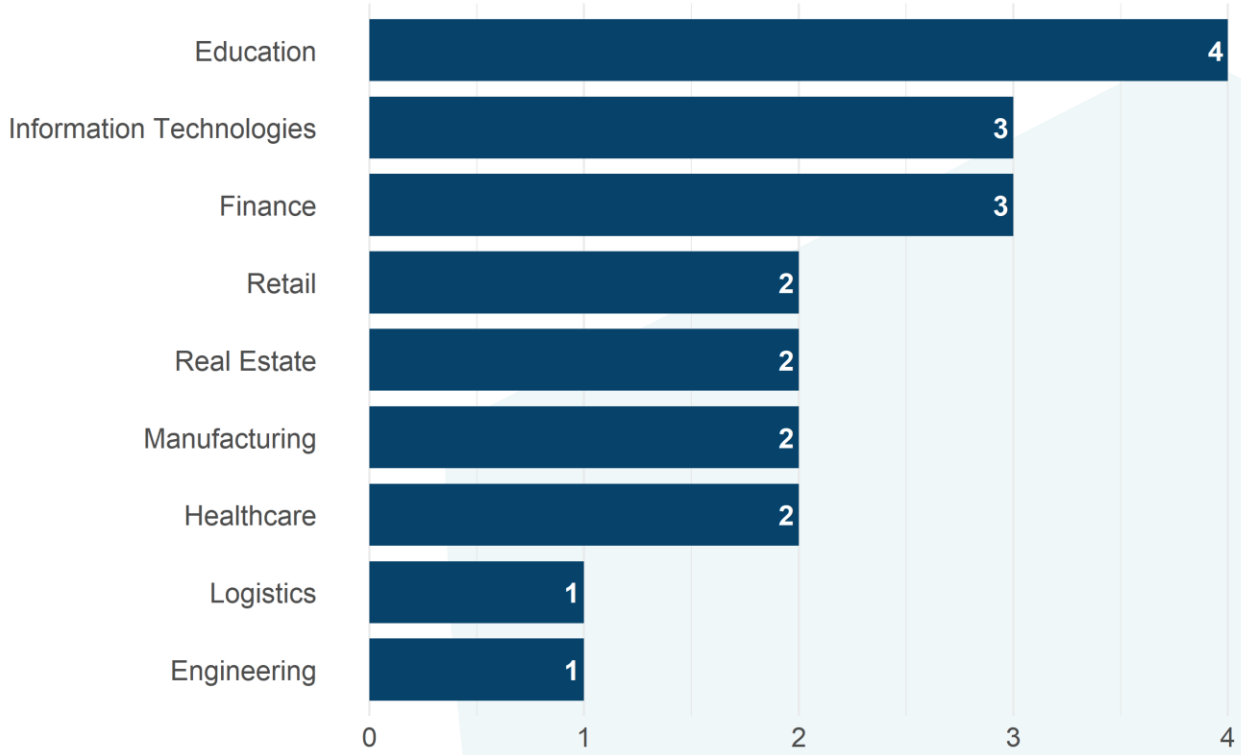
UK ransomware incidents by month, March-November 2024



In November 2024, there were an estimated 20 ransomware incidents targeting UK organisations. For context, the average number of monthly incidents since March is 27, 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

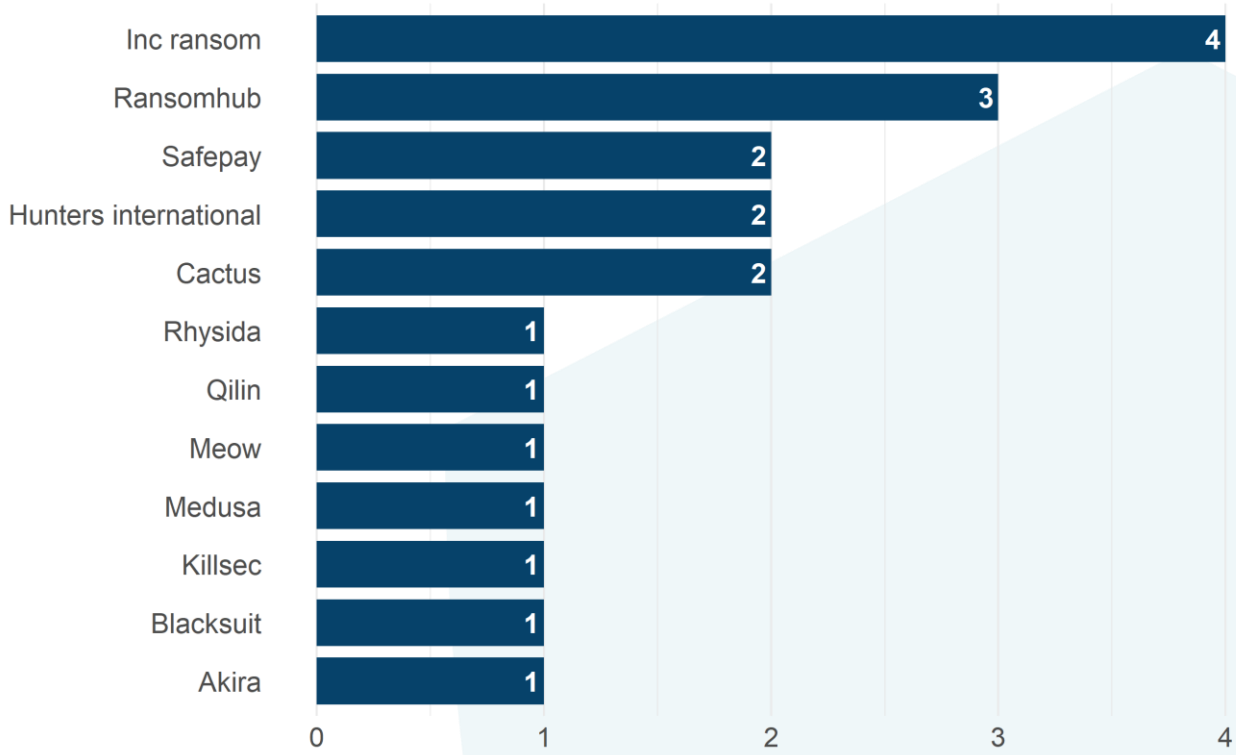
UK ransomware incidents by sector, November 2024



Education has been the most frequently targeted sector in the UK, with private schools predominantly named as victims. Additionally, the UK IT sector has consistently faced cyber incidents, experiencing between 1-4 incidents in each month since March 2024.

Scottish Cyber Coordination Centre

UK ransomware incidents by threat actor, November 2024



INC ransomware has increased its activity with 4 confirmed cases in November. RansomHub continues to be a prolific group, with 3 incidents in November, bringing their total to 23 since March 2024.

INC Ransomware has targeted high-profile victims, including NHS Dumfries and Galloway, claiming responsibility for the attack earlier this year, during which 3 terabytes of data were stolen.[1] Additionally, in November, they claim to have breached the Alder Hey Children's Hospital Trust, one of Europe's largest children's hospitals. They posted on their data leak site that they obtained large-scale patient records, donor reports, and procurement data.[2]

[1] UK Defence Journal, **Hackers threaten to release huge amount of NHS Scotland data** (27 March 2024)
[2] InfoSecurity Magazine, **INC Ransom Claims Cyber-Attack on UK Children's Hospital** (29 Nov 2024)

Scottish Cyber Coordination Centre

Section 2: Analysis of INC ransomware

This profile outlines the evolution of INC ransomware, including its rebranding as Lynx Ransomware, the developer behind it, and the tactics, techniques, and procedures (TTPs) observed in its campaigns.

Detected in July 2023, INC ransomware is a sophisticated variant developed by a criminal group that CrowdStrike tracks as TRAVELING SPIDER, operating under a Ransomware-as-a-Service (RaaS) model. It targets victims indiscriminately, including sectors such as healthcare, finance, and technology in the UK and the US.

Known for its double extortion strategy of encrypting data while threatening to leak it, the group emerged by exploiting vulnerabilities in remote desktop protocols (RDP) and running spear-phishing campaigns. These initial efforts laid the groundwork for its rise as a significant threat actor within the cybercriminal ecosystem. [3]

In mid-2024, INC rebranded as Lynx Ransomware, enhancing its code to be more elusive and destructive. Concurrently, the INC ransomware source code was listed for sale on darknet forums for about $300,000, raising concerns about other groups or affiliates adopting it. [4] Notably, the TTPs of INC ransomware incidents show significant overlaps with those of Nokoyawa ransomware, which was previously operated as a RaaS. TRAVELING SPIDER is also attributed as the developer and vendor of various other ransomware variants like Nemty, Nemty X, Karma, and Nokoyawa, consistently retiring previous variants with each new development. Initially targeting smaller entities, TRAVELING SPIDER and its affiliates shifted to larger organisations with higher ransom demands, adopting a big game hunting tactic. INC and Nokoyawa ransomware samples, along with their DLS portals, show significant technical similarities, highlighting the ongoing evolution of TRAVELING SPIDER's ransomware development.[5]

---

[3] Palo Alto Networks, **Lynx Ransomware: A Rebranding of INC Ransomware** (10 October 2024)
[4] Bleeping Computer, **INC ransomware source code selling on hacking forums for $300,000** (13 May 2024)
[5] CrowdStrike Intelligence Reports

Scottish Cyber Coordination Centre

Initial Access (TA0001)

- INC ransomware gains initial access by using spear-phishing campaigns to compromise targeted systems. Additionally, they exploit known vulnerabilities in public-facing applications, such as CVE-2023-3519 in Citrix ADC and Gateway systems, along with the widespread exploitation of CVE-2024-1709, a ConnectWise vulnerability that allows authentication bypass.

Defence Evasion (TA0005)

- INC ransomware uses HackTool.ProcTerminator and ProcessHacker to evade detection. The group were observed employing these tools to terminate processes running in their victim's system.

Credential Access (TA0006)

- The ransomware uses tools such as HackTool.PS1.VeeamCreds.A and Mimikatz to dump credentials from Veeam Backup and Replications Managers.

Discovery (TA0007)

- INC ransomware employs NetScan and Advanced IP Scanner to gather network information that can subsequently facilitate lateral movement. Notably, the attackers have been seen using legitimate tools like Notepad, Wordpad, and Paint to examine files. It downloads tools for lateral movement, such as Mimikatz and Advanced IP Scanner, from an open directory.

Lateral Movement (TA0008)

- INC ransomware uses PSexec, AnyDesk, and TightVNC to move through its victim’s system.

Scottish Cyber Coordination Centre

Exfiltration (TA0010)

- INC ransomware utilises MEGAsyncSetup64.EXE, a desktop application for MEGA file sharing, synchronization, and cloud services, to facilitate the exfiltration of data.

Impact (TA0040)

- INC ransomware uses 7-Zip to compress data before sending it out via MegaSync. It also employs the AES algorithm for file encryption with two modes: fast and medium mode. Following successful data encryption, INC ransomware will leave a ransom note stating demands and contact instructions.

Mitigations

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

- Enhancing employee awareness through training to recognise phishing emails, malicious links, and suspicious attachments, ensuring they report such threats promptly.
- Enforcing strong password policies, including regular updates, unique combinations of characters, and preventing reuse across multiple accounts.
- Implementing Multi-Factor Authentication (MFA) for all user accounts to provide additional protection against credential theft.
- Regularly updating and patching systems to address vulnerabilities, including operating systems, applications, firmware, and disabling unnecessary services.
- Using anti-malware solutions capable of identifying and blocking ransomware through advanced detection methods such as heuristics and machine learning.
- Monitoring network traffic for unusual patterns or communication with known command-and-control servers to detect potential compromises.

- Maintaining secure backups of critical data, stored offline or in a separate network environment, and regularly testing recovery processes to ensure rapid restoration.

Sources

1. CrowdStrike Intelligence Reports
2. Sentinel One, **Inc. Ransom** (2024)
3. Trend Micro, **Ransomware Spotlight: INC** (29 Oct 2024)
4. Huntress, **Investigating New INC Ransom Group Activity** (11 August 2023)

Scottish Cyber Coordination Centre

Appendix

Indicators of Compromise (IoCs) associated with INC Ransomware

Indicator	Type
C:\source\INC Encryptor\Release\INC Encryptor.pdb	Exe PDB String
*.inc-readme.txt, *.inc-readme.html	Ransom note file
*.inc	Encrypted File Extension
SHA256 hashes for Lynx ransomware:	
571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b	hash_sha256
82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513	hash_sha256
eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc	hash_sha256
SHA256 hashes for INC ransomware:	
accd8bc0d0c2675c15c169688b882ded17e78aed0d914793098337afc57c289c	hash_sha256
02472036db9ec498ae565b344f099263f3218ecb785282150e8565d5cac92461	hash_sha256
05e4f234a0f177949f375a56b1a875c9ca3d2bee97a2cb73fc2708914416c5a9	hash_sha256
11cfd8e84704194ff9c56780858e9bbb9e82ff1b958149d74c43969d06ea10bd	hash_sha256
1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a	hash_sha256
1a7c754ae1933338c740c807ec3dcf5e18e438356990761fdc2e75a2685ebf4a	hash_sha256
29a25e971dbb87d3adcee75693782d978a3ca9f64df0a59b015ca519a4026c49	hash_sha256
3156ee399296d55e56788b487701eb07fd5c49db04f80f5ab3dc5c4e3c071be0	hash_sha256

36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e	hash_sha256
508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef	hash_sha256
64b249eb3ab5993e7bcf5c0130e5f31cbd79dabdcad972680427807 26e68533f	hash_sha256
7f104a3dfda3a7fbdd9b910d00b0169328c5d2facc10dc17b4378612ffa82d51	hash_sha256
869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947	hash_sha256
9ac550187c7c27a52c80e1c61def1d3d5e6dbae0e4eaeacf1a493908ffd3ec7d	hash_sha256
ca9d2440850b730ba03b3a4f410760961d15eb87e55ec502908d2546cd6f598c	hash_sha256
d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6	hash_sha256
e17c601551dfded76ab99a233957c5c4acf0229b46cd7fc2175ead7fe1e3d261	hash_sha256
ee1d8ac9fef147f0751000c38ca5d72feceeaae803049a2cd49dcce15223b720	hash_sha256
f96ecd567d9a05a6adb33f07880eebf1d6a8709512302e363377065ca8f98f56	hash_sha256
fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced	hash_sha256
fef674fce37d5de43a4d36e86b2c0851d738f110a0d48bae4b2dab4c6a2c373e	hash_sha256
63e0d4e861048f581c9e5c64b28a053eb0023d58eebf2b943868d5f68a67a8b7	hash_sha256
a0ceb258924ef004fa4efeef4bc0a86012afdb858e855ed14f1bbd31ca2e42f5	hash_sha256
c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef	hash_sha256
martina.lestariid1898@proton.me	Email address
Lynxblog.net	Leak site
http[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion	URL
http[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion/disclosures	URL

Scottish Cyber Coordination Centre

http[:]//lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd[.]onion	URL
http[:]//lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd[.]onion	URL
http[:]//lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad[.]onion	URL
http[:]//lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad[.]onion	URL
http[:]//lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad[.]onion	URL
http[:]//lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion	URL
http[:]//lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid[.]onion	URL
http[:]//lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd[.]onion/login	URL
http[:]//lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd[.]onion/login	URL
http[:]//lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd[.]onion/login	URL
http[:]//lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd[.]onion/login	URL
http[:]//lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd[.]onion/login	URL
http[:]//lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad[.]onion/login	URL
http[:]//lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad[.]onion/login	URL
http[:]//lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad[.]onion/login	URL