CyberMaxx

Q4 2024

Ransomware Research Report

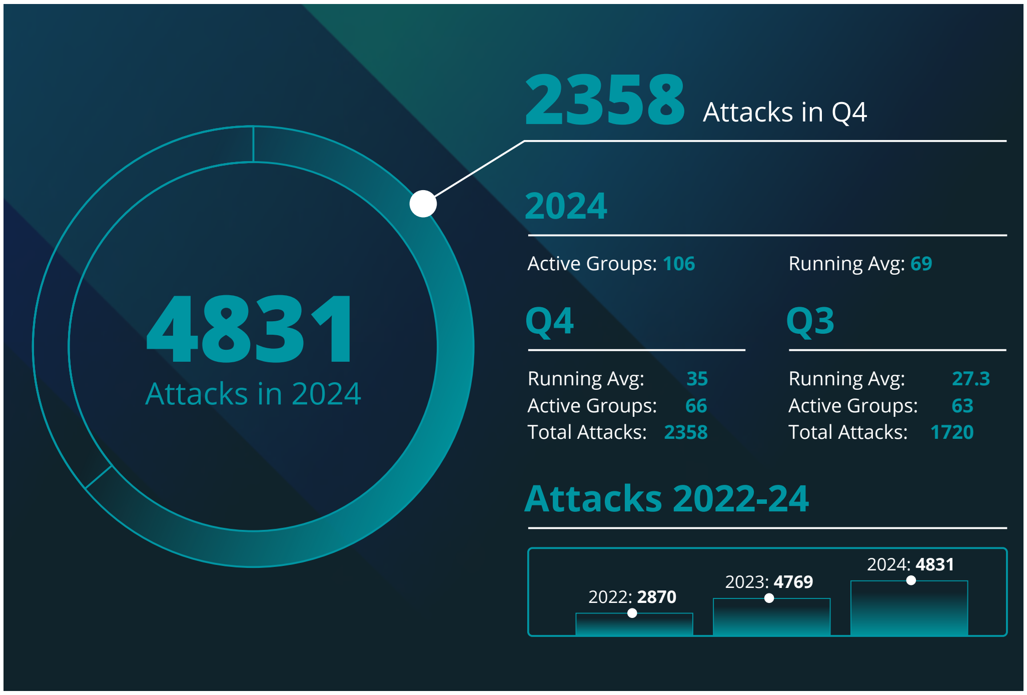
Throughout 2024, ransomware and data extortion attacks have continued to rise.

The total number of ransomware and data extortion attacks this year was 4831, the highest year on record. The total number of attacks this quarter was 2358, the highest quarter on record. 137% more attacks in Q4 than there were in Q3 2024. An observed 37% growth in 90 days.

There was almost double the number of successful attacks in the final 90 days of 2024 than there were in Q4 2023. 2023's final quarter saw 1218 attacks, vs 2024's 2358, at 193%.

Looking at the volume of attacks throughout the year, we can see a clear upward trend month-to-month.

2024 Totals



Q4 Attacks:

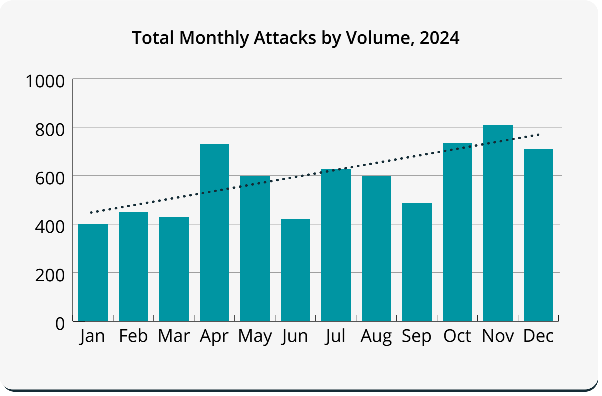
Q4 had the most attacks in any quarter that the CyberMaxx team has observed.
Looking at the distribution by date, we see the largest spike on November 18th, which coincided with two notable vulnerabilities:

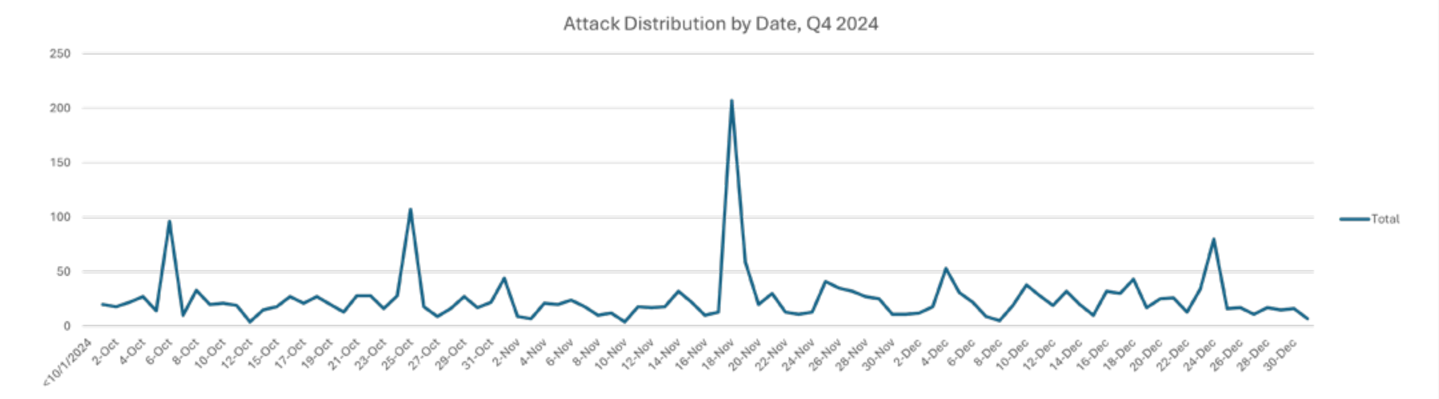
- CVE-2024-0012: 9.3, Palo Alto PAN-OS RCE
- CVE-2024-9474: 6.9, Palo Alto PAN-OS Privilege Escalation

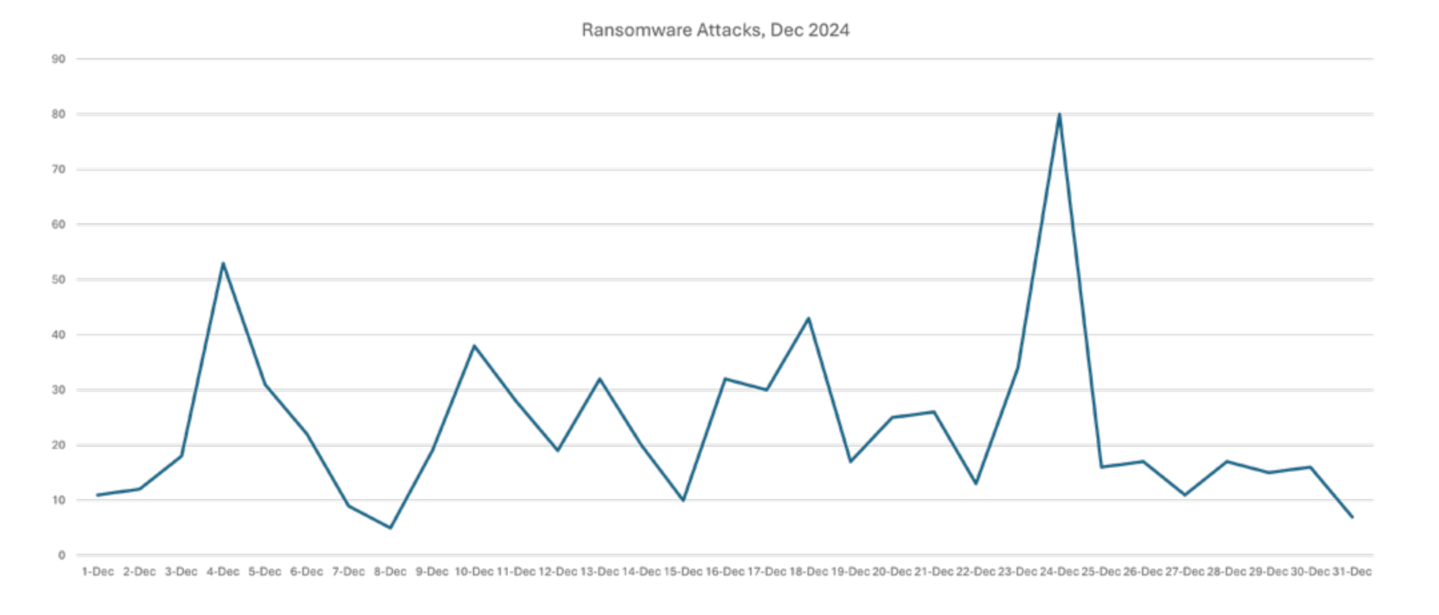
CVE-2024-0012 and CVE-2024-9474 are both known to have been exploited in-the-wild at this time, which may have contributed to this spike in activity.

Palo Alto's UNIT42 dubbed this "Operation Lunar Peek", and have a detailed writeup available here. Other notable vulnerabilities that were actively exploited during this same timeframe are listed below:

- CVE-2024-11667: Vulnerabilities in Zyxel, ProjectSend, and CyberPanel
- CVE-2024-41713: Critical Vulnerability in Mitel MiCollab
- CVE-2024-11680: Critical Vulnerability in ProjectSend"



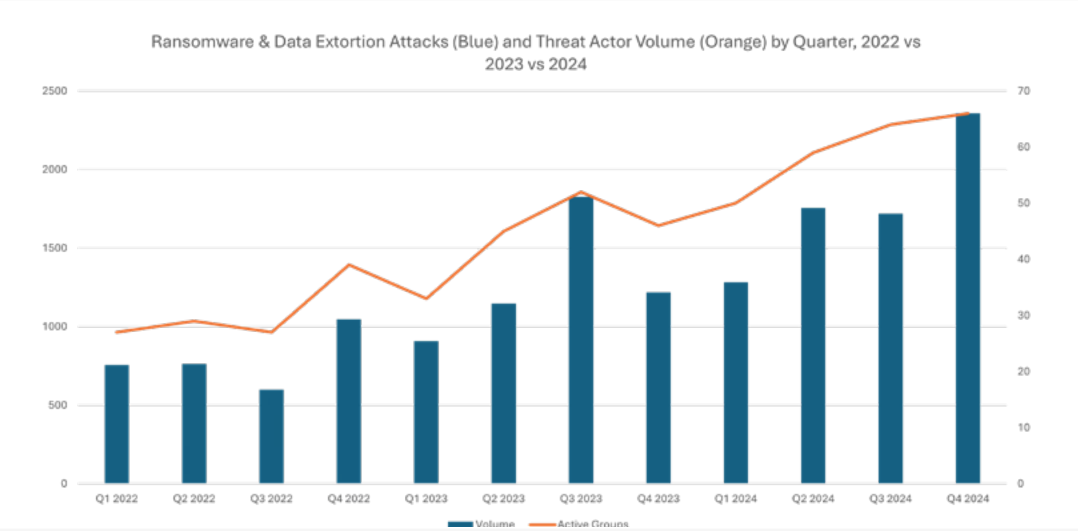




Threat Actors

Another notable spike was on December 24th. As Security teams in the west wrap up the year for the holiday season and take PTO; Threat Actors leverage this to exploit the smaller team footprints and often increased response times – allowing them an improved success rate of actions-on-objectives.

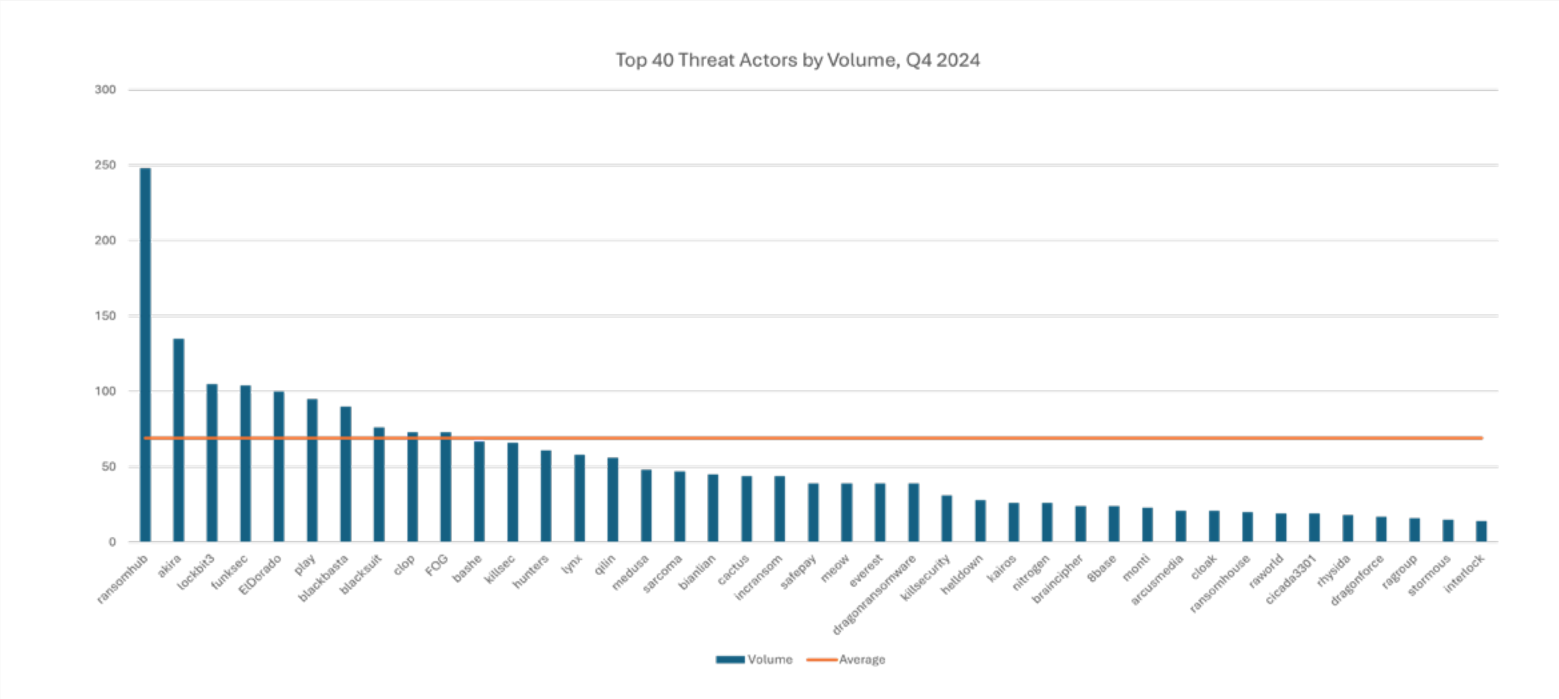
Threat actors are following the adoption of cloud in 2024. We saw a 39% increase in attacks against cloud environments over 2023, making this a common initial access vector for threat actors. Together Identity attacks and exploiting misconfigurations were the main attack vectors utilized. The CyberMaxx team published a non-disruptive tool to test your environment against password spraying attacks, [find it here](#).


Ransomware & Data Extortion Attacks (Blue) and Threat Actor Volume (Orange) by Quarter, 2022 vs 2023 vs 2024

We saw a

39%

increase in attacks against cloud environments over 2023, making this a common initial access vector for threat actors.


Top 40 Threat Actors by Volume, Q4 2024

We have continued to observe new Threat Actors enter the space, with Q4 having 66 active groups participating in successful ransomware and data extortion attacks.

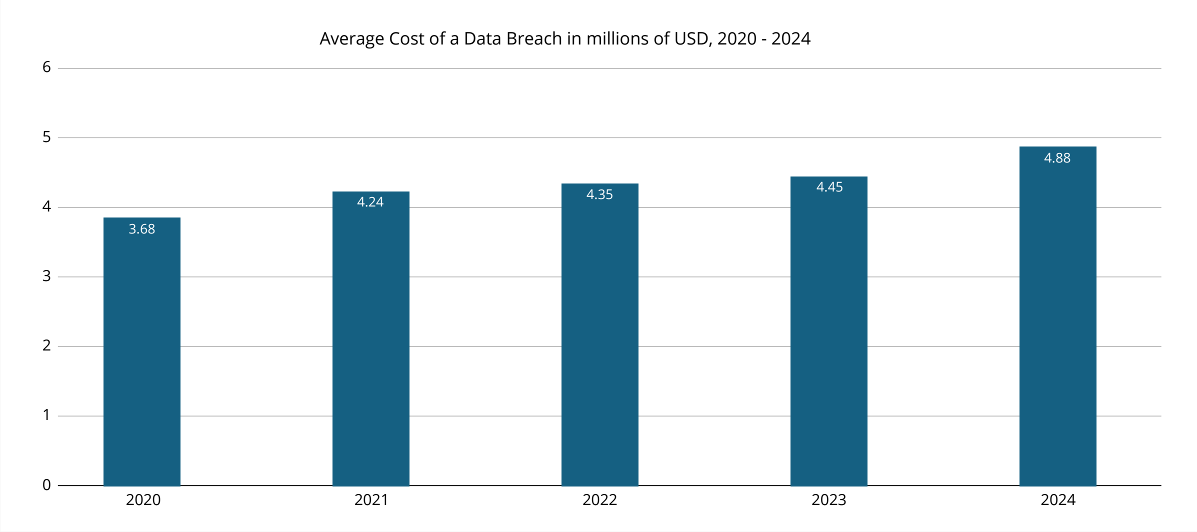
We have continued to observe new Threat Actors enter the space, with Q4 having **66 active groups** participating in successful ransomware and data extortion attacks.

Quarter	Volume	Active Groups
Q1 2022	756	27
Q2 2022	764	29
Q3 2022	599	27
Q4 2022	1047	39
Q1 2023	909	33
Q2 2023	1147	45
Q3 2023	1826	52
Q4 2023	1218	46
Q1 2024	1283	50
Q2 2024	1755	59
Q3 2024	1720	64
Q4 2024	2358	66

Average Cost of a Data Breach

The average cost of a data breach for an organization continues to grow year over year, as measured by IBMs “Cost of a Data Breach”, through 2020 until today in 2024, rising from $3.86M to $4.88M in 4 years. This data shows that incidents are getting more expensive and more frequent as time goes on.

Security costs continue to go up to combat the increasing likelihood of a successful attack. The data and statistics detailed above are only the tip of the iceberg, as with cyber security incidents there are multiple other factors depending on industry which can impacts an organizations bottom line.


Average Cost of a Data Breach in millions of USD, 2020 - 2024

Source: https://www.ibm.com/reports/data-breach

2024 Wrap Up

CrowdStrike

In July of 2024, a faulty update from CrowdStrike caused a global IT outage affecting Windows systems. The issue stemmed from a signature update, which incorrectly identified key operating systems files as malicious, creating a boot loop and constantly crashing. Many systems had to manually updated to prevent this loop and become operational again.

The aviation industry was severely affected, with Delta Air Lines cancelling 7,000 flights and suffering over $500 million in losses. Hospitals experienced system failures, disrupting patient care, while banks and emergency services also faced major operational breakdowns.

Delta Air Lines has since filed a lawsuit against CrowdStrike, seeking over $500 million in damages for alleged negligence. The incident has raised concerns about the risks of third-party software with deep access to operating systems, prompting discussions on redesigning products to prevent similar disruptions.

OpenAI: Influence and Cyber Operations

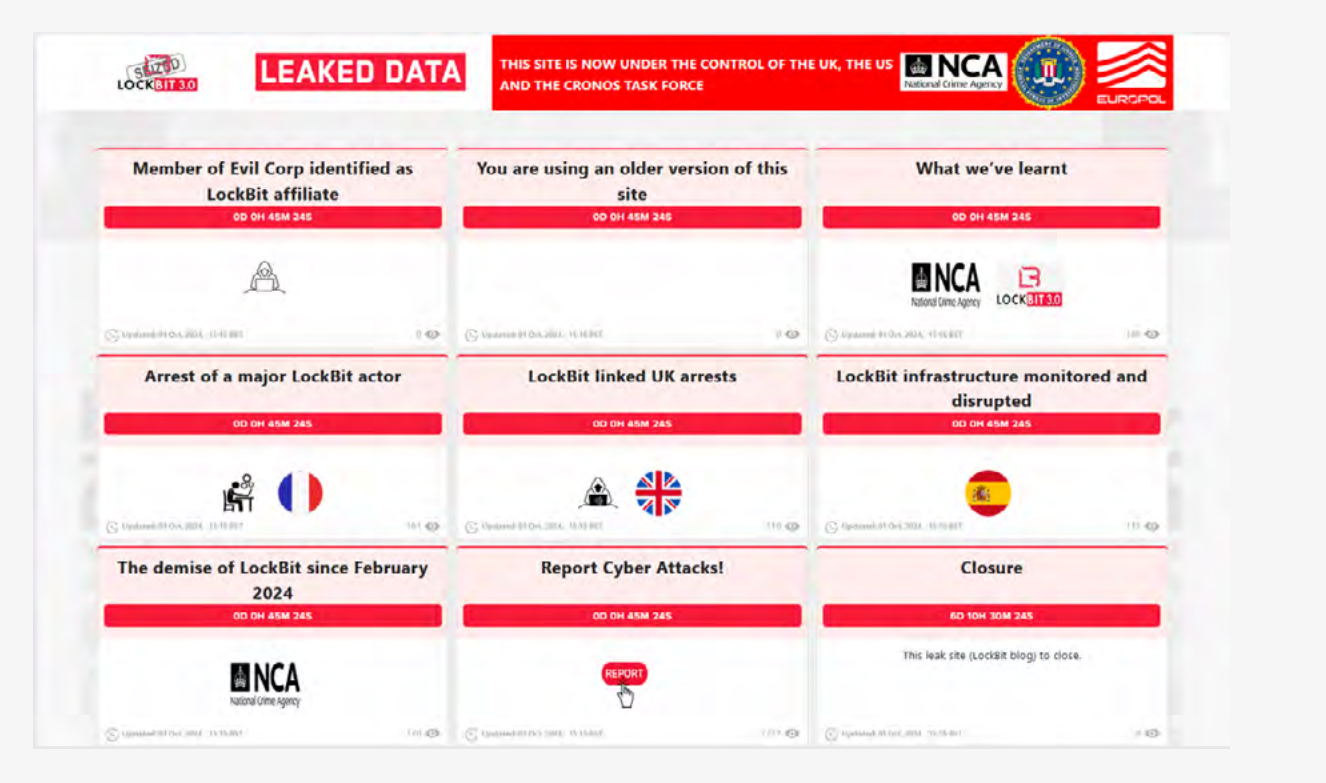
OpenAI have been monitoring threat actors using ChatGPT for malicious purposes, identifying threat actors attempting to use the platform. They claim to have disrupted more than twenty operations and deceptive networks from around the world that were attempting to use their models.

OpenAI observed these threat actors asking questions about specific CVE numbers, asking about how to identify versions of Log4j vulnerable to Log4Shell, how sqlmap is used and many others. The full report from OpenAI is available here.

Activity	LLM ATT&CK Framework Category
Asking about vulnerabilities in various applications	LLM informed reconnaissance
Asking how to search for specific versions of Log4j that are vulnerable to the critical RCE Log4Shell	LLM informed reconnaissance
Asking about popular content management systems used abroad	LLM informed reconnaissance
Asking for information on specific CVE numbers	LLM informed reconnaissance
Asking how internet-wide scanners are made	LLM informed reconnaissance
Asking how sqlmap would be used to upload a potential web shell to a target server	LLM assisted vulnerability research
Asking for help finding ways to exploit infrastructure belonging to a prominent car manufacturer	LLM assisted vulnerability research
Providing code and asking for additional help using communication services to programmatically send text messages	LLM enhanced scripting techniques
Asking for help debugging the development of an extension for a cybersecurity tool	LLM enhanced scripting techniques
Asking for help to debug code that's part of a larger framework for programmatically sending text messages to attacker specified numbers	LLM-aided development
Asking for themes that government department employees would find interesting and what would be good names for attachments to avoid being blocked	LLM-supported social engineering
Asking for variations of an attacker-provided job recruitment message	LLM-supported social engineering

Operation Cronos Update

Law Enforcement updated Lockbit’s release pages on the dark web with a countdown timer, replacing posts that were previously made during the disruption operation earlier this year. The posts were titled “Lockbit Linked UK Arrest” and “Lockbit Disruption” amongst others. A screenshot of this can be seen below:



LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Member of Evil Corp identified as LockBit affiliate
0D 0H 45M 24S

You are using an older version of this site
0D 0H 45M 24S

What we’ve learnt
0D 0H 45M 24S

Arrest of a major LockBit actor
0D 0H 45M 24S

LockBit linked UK arrests
0D 0H 45M 24S

LockBit infrastructure monitored and disrupted
0D 0H 45M 24S

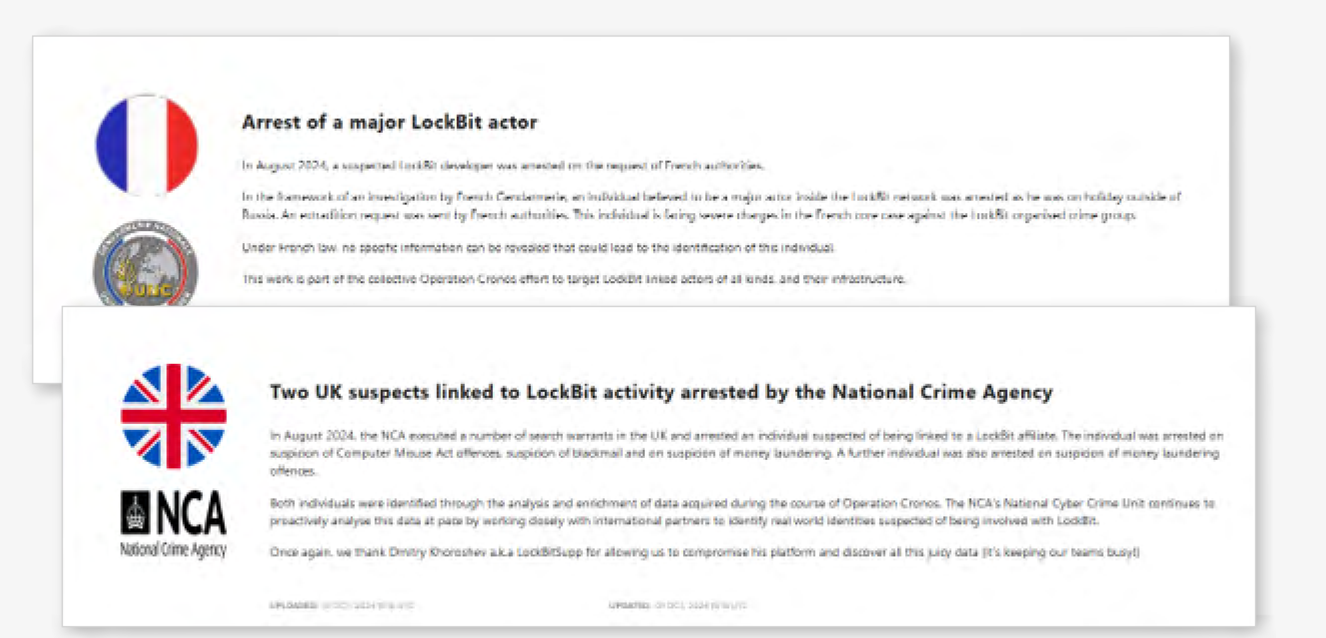
The demise of LockBit since February 2024
0D 0H 45M 24S

Report Cyber Attacks!
0D 0H 45M 24S

Closure
6D 10H 30M 24S
This leak site (LockBit blog) to close.

Once the timer reached zero, the posts were released, related to the arrest of multiple individuals worldwide who were related to the Lockbit operation, incl. developers and the owner of the bullet-proof hosting site used by Lockbit’s infrastructure.

Images from the released posts are below:



Arrest of a major LockBit actor

In August 2024, a suspected LockBit developer was arrested on the request of French authorities.

In the framework of an investigation by French Gendarmerie, an individual believed to be a major actor inside the LockBit network was arrested as he was on holiday outside of Russia. An extradition request was sent by French authorities. This individual is facing severe charges in the French core case against the LockBit organised crime group.

Under French law, no specific information can be revealed that could lead to the identification of this individual.

This work is part of the collective Operation Cronos effort to target LockBit linked actors of all kinds, and their infrastructure.

Two UK suspects linked to LockBit activity arrested by the National Crime Agency

In August 2024, the NCA executed a number of search warrants in the UK and arrested an individual suspected of being linked to a LockBit affiliate. The individual was arrested on suspicion of Computer Misuse Act offences, suspicion of blackmail and on suspicion of money laundering. A further individual was also arrested on suspicion of money laundering offences.

Both individuals were identified through the analysis and enrichment of data acquired during the course of Operation Cronos. The NCA’s National Cyber Crime Unit continues to proactively analyse this data at pace by working closely with international partners to identify real world identities suspected of being involved with LockBit.

Once again, we thank Dmitry Khoroshev a.k.a LockBitSupp for allowing us to compromise his platform and discover all this juicy data (it’s keeping our teams busy!)

UPLOADED: [illegible] UPDATED: [illegible]

Other Notable Events

CrowdStrike outage on July 19th 2024. Lead to Microsoft holding a summit to discuss the future of security in the Microsoft kernel.

Health Infrastructure Security and Accountability Act proposed in the US, September 26th 2024. If passed, it would set clearer cyber security standards for the healthcare industry and hold corporation executives accountable.

Conclusion

2024 has been the both the year with the most attacks overall, as well as the year with the largest number of attacks in one quarter, rivalling the previous years in just 90 days. The spike in November can be attributed to several zero-days that were exploited in-the-wild, notably the PAN-OS CVE-2024-0012 & CVE-2024-9474 likely being responsible for at least part of the spike in activity, showing the need for a responsive patching process to avoid exploitation by opportunistic threat actors.

2024 has been the both the year with the **most attacks overall**, as well as the year with the **largest number of attacks in one quarter.**

December 24th showed another spike in activity, highlighting the fact that threat actors are aware that teams are smaller during the holiday season and quickly capitalize on this. The shift towards cloud is following the industry trend to move away from on-prem. Identity-based attacks and exploitation of misconfigurations emerged as primary vectors, emphasizing the need for robust security practices. The number of groups has also risen again; which appears to be an ongoing trend for the past two years. The number of attacks is also increasing as more groups join the ransomware industry looking to profit.

In conclusion, 2024's record-breaking ransomware incidents demand heightened vigilance, proactive vulnerability management, and robust cloud security measures. The increasing scale of these attacks and the cost of an incident continues to climb year-over-year, highlighting the critical need for organizations to adapt swiftly to the evolving threat landscape and invest in comprehensive defensive strategies to mitigate risks effectively.

About:

CyberMaxx provides comprehensive managed detection and response (MDR) services that protect organizations from today's complex cyber threats. With a focus on proactive security measures, CyberMaxx delivers industry-leading technology combined with expert human oversight, offering robust protection and peace of mind to clients across various industries.

References

- IBM, Cost of a Data Breach, 2024
- Unit42, Operation Lunar Peek
- MSSprinkler, Github, Github
- OpenAI, Influence and Cyber Operations (PDF)