NEWS 7 MAR 2025

Ransomware Groups Favor Repeatable Access Over Mass Vulnerability Exploits

James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Ransomware groups have shifted away from mass compromise events from vulnerability exploits towards “reliable and repeatable” methods to gain access to victim networks, according to Travelers’ latest *Cyber Threat Report.*

These tactics include targeting weak credentials on VPN and gateway accounts that are not protected by multifactor authentication (MFA).

The researchers noted that this activity began to take hold in the second half of 2023, and spread widely among ransomware operators and initial access brokers (IAB) throughout 2024.

The report highlighted a ransomware training playbook written by an IAB that was leaked in the Summer of 2023 that emphasized this shift.

The manual advised that instead of focusing on discovering the next zero-day vulnerability, ransomware actors should deploy tools to look for default usernames like “admin” or “test” and to try combinations of common passwords in order to uncover weak credentials to target.

There was not a single vulnerability that led to mass ransomware exploits in 2024.

This is a marked difference from 2023, where a significant portion of the ransomware leak site activity was attributed to exploits in common software products, such as the MOVEit and GoAnywhere file transfer software.

Several ransomware groups pounced on such vulnerabilities to exploit as many victims as possible in a short period of time.

Jason Rebholz, Vice President and Cyber Risk Officer at insurance firm Travelers, commented: “Based on our observations, it’s clear that basic attack techniques are still highly effective for ransomware groups.”

He added: “These groups have been on the offensive, proactively hunting for targets and having significant success. It’s vital that businesses implement proven security controls, such as MFA, to make it far more challenging for malicious actors to carry out an attack on their organization.”

Ransomware Activity Hits Quarterly Record

The report found that ransomware activity reached record levels in Q4 2024, with 1663 new victims posted on leak sites.

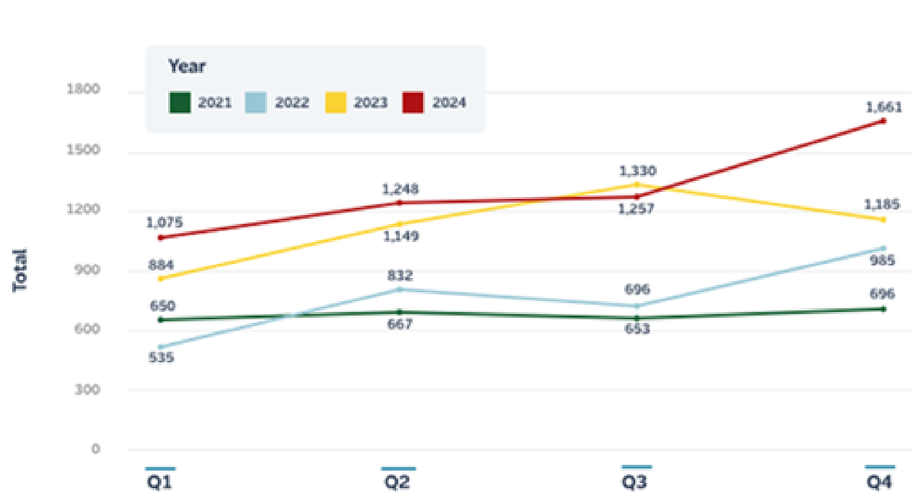
This represents a 32% increase compared to Q3 2024, with Q4 representing the highest level of ransomware activity recorded in any single quarter by the insurer, eclipsing Q3 2023.

November saw the highest number of ransomware leak site victims of the quarter, at 629. This was followed by a relative decline to 516 in December.

The researchers said this pattern aligns with historical trends of increased activity in the early holiday season, followed by a later decrease going into the new year.

Read now: Ransomware Attacks Surge to Record High in December 2024

Throughout 2024, there were 5243 ransomware victims posted on leak sites, a 15% increase from the 4548 incidents recorded in 2023.



Ransomware victims posted on leak sites per quarter, 2021-2024. Source: Travelers

The report also recorded a 67% increase in new ransomware groups formed in 2024 compared to 2023, with 55 new groups observed last year.

This indicates a rapid proliferation of smaller more agile actors in the ransomware ecosystem following the disruption of leading ransomware-as-a-service (RaaS) operators such as LockBit and Clop by law enforcement.

RansomHub accounted for the highest number of attacks in Q4 2024 at 238, making up 14% of the total.

This was followed by Akira and Play, making up 133 and 95 attacks, respectively.

You may also like

OPINION 15 JUL 2019
#HowTo Avoid Common Configuration Sins

NEWS 8 MAR 2024
Dropbox Used to Steal Credentials and Bypass MFA in Novel Phishing Campaign

NEWS 13 JUL 2022
Microsoft Details How Phishing Campaign Bypassed MFA

NEWS 26 FEB 2019
Privileged Credential Abuse a Top Attack Vector

OPINION 6 JUN 2017
Why Two Factors are Better than One

What’s hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1 NEWS 28 MAR 2025
Nine in Ten Healthcare Organizations Use the Most Vulnerable IoT Devices

2 NEWS 28 MAR 2025
Solar Power System Vulnerabilities Could Result in Blackouts

3 NEWS 28 MAR 2025
Trump CISA Cuts Threaten US Election Integrity, Experts Warn

4 NEWS 28 MAR 2025
Morphing Meerkat PhaaS Platform Spoofs 100+ Brands

5 NEWS 29 JAN 2024
Nigerian 'Yahoo Boys' Behind Social Media Sextortion Surge in the US

6 NEWS 27 MAR 2025
CoffeeLoader Malware Loader Linked to SmokeLoader Operations