CyberMaxx

Q1 2025
Ransomware Research Report

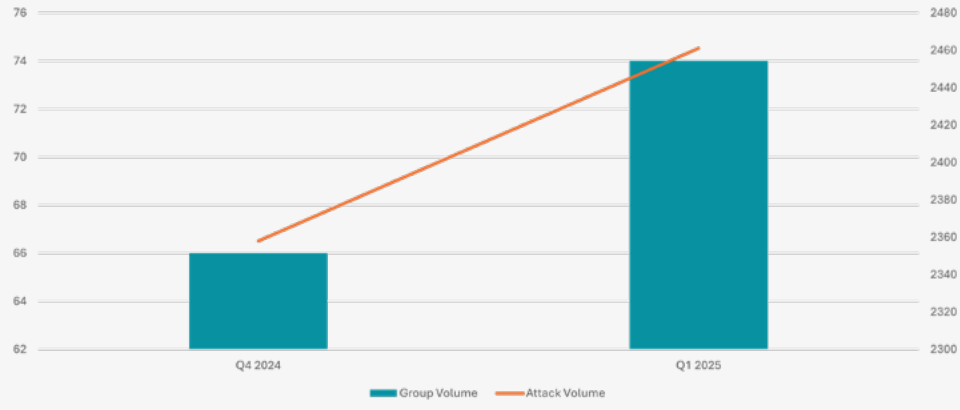
The first quarter of 2025 has set a new record for ransomware attacks, with 74 active groups responsible for 2,461 recorded incidents.

Q1 2025 Totals

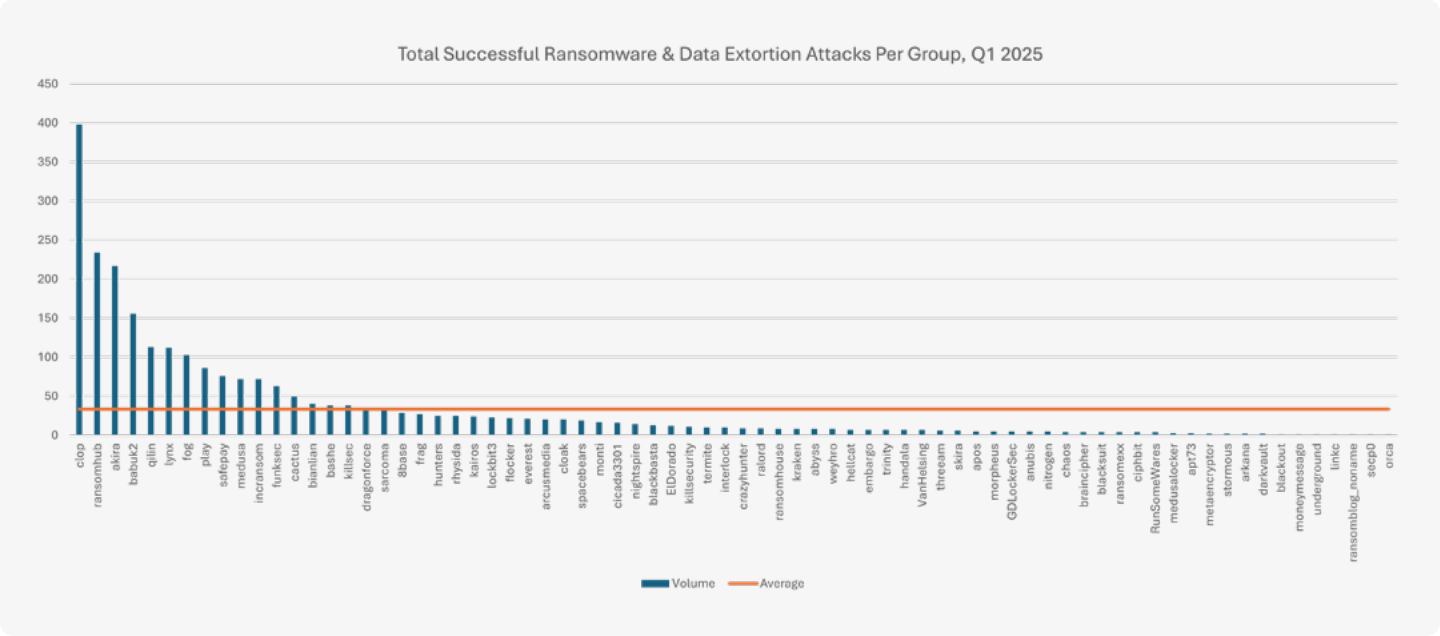
2461 Attacks in Q1 2025

2358 Attacks in Q4 2024

This makes Q1 2025 the quarter with the highest number of recorded attacks so far, beating out Q4 2024, and making Q1 2025 the most prolific quarter for ransomware activity to date.



On average, ransomware groups achieved 33.2 successful attacks per group during Q1 2025. The increased number of active groups and overall attacks highlights the persistence and diversification of threat actors within the ransomware ecosystem.



cl0p Dominates the Quarter

The most active group during Q1 2025 was Cl0p, responsible for 398 attacks, accounting for approximately 16% of all successful attacks observed during the quarter.

Cl0p's dominance this quarter is attributed to their exploitation of two critical vulnerabilities:

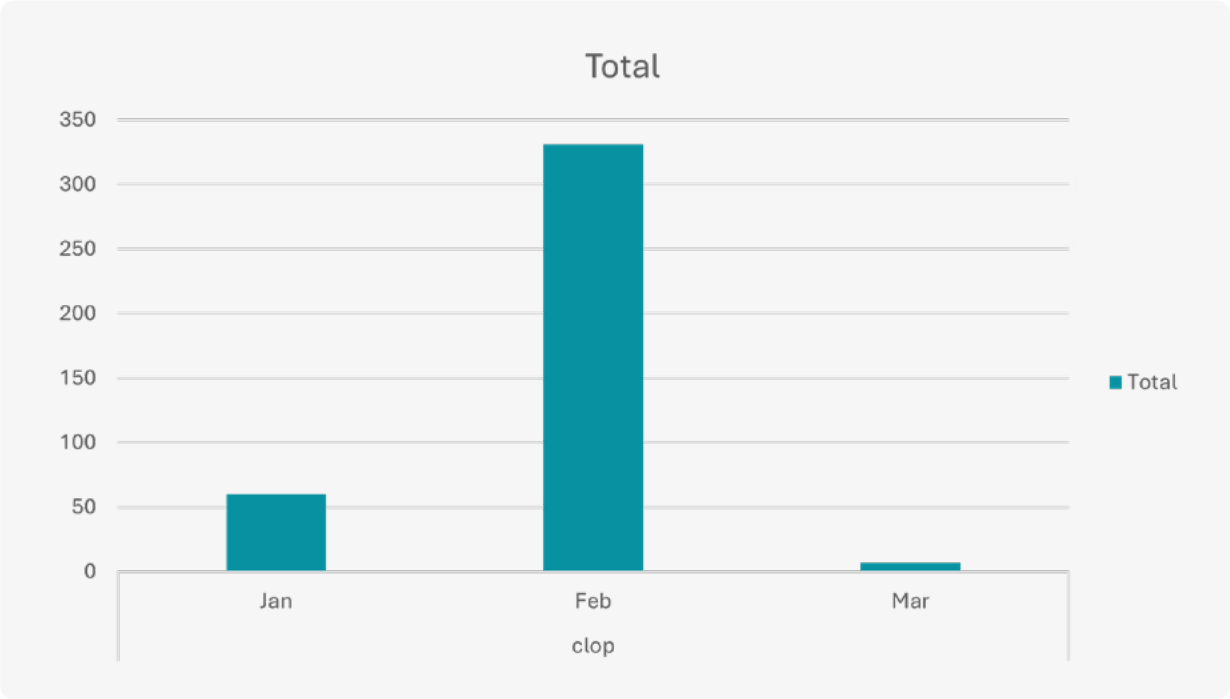
- **CVE-2024-50623:** An unrestricted file upload vulnerability affecting Cleo Harmony and VLTrader.
- **CVE-2024-55956:** Unauthenticated command execution enabled by leveraging the default configuration on the Autorun directory within Cleo Harmony.

These two vulnerabilities were exploited in tandem, providing Cl0p with a powerful exploit chain that they leveraged to devastating effect. The exploitation of unpatched systems continues to be a favored technique for initial access among ransomware groups.

February 2025: Cl0p's Record-Breaking Month

Cl0p's use of the exploit chain was particularly effective in February 2025, resulting in 331 individual attacks—the highest number ever recorded by a single group in a single month. This relentless activity underscores Cl0p's aggressive targeting and highly efficient exploitation tactics.

cl0p Activity by Volume



The top 5 groups of this quarter are listed below:

Group Name	Attacks
cl0p	398
RansomHub	234
Akira	217
Babuk2	156
Qilin	113

Notably, Lockbit, once a prominent ransomware group, did not make the top five list this quarter. With only 23 known attacks, they have fallen to 24th place.

Conclusion

The record-breaking activity in Q1 2025 signals an escalation in ransomware threats, with Cl0p setting new benchmarks for attack volume and efficiency. Their successful exploitation of critical vulnerabilities highlights the need for organizations to prioritize patch management and improve their overall security posture.

Black Basta

Black Basta Leak: Revelations from Internal Chat Logs

In February 2025, a major leak of internal chat logs from the Black Basta ransomware group provided unprecedented insights into their operations, target selection criteria, exploitation tactics, and the tools they employed.

This leak has sparked considerable interest among cybersecurity researchers and law enforcement agencies alike, as it offers a rare glimpse into the inner workings of one of the most notorious ransomware gangs currently active.

Target Selection

According to the leaked logs, Black Basta demonstrated a clear preference for targets with low tolerance for operational downtime. This strategic focus suggests that Black Basta sought to exploit the urgency and critical nature of these industries to increase the likelihood of ransom payments.

Healthcare facilities, in particular, are especially vulnerable due to the potential life-or-death consequences of operational disruptions. Financial services and critical infrastructure entities are similarly attractive targets, given their dependency on constant availability and the potentially catastrophic outcomes of prolonged downtime.

High-priority targets included **healthcare institutions, financial services, and critical infrastructure entities.**

Exploitation Methods

The logs reveal that Black Basta primarily favored exploiting known vulnerabilities, rather than investing in costly zero-day exploits. A notable complaint among members of the group was the high price of zero-day exploits, with one specific reference to a privilege escalation exploit priced at $10,000 USD.

Despite their reluctance to invest heavily in zero-days, the group was confirmed to have purchased one for privilege escalation on Windows systems. This exploit was later identified as CVE-2024-26169, which was patched by Microsoft on March 12, 2024. At the time, Microsoft stated that there was no evidence of exploitation in the wild.

Discovery of Tools

Two variants of a tool attributed to Black Basta were discovered from a failed operation by Symantec's cybersecurity team. The first variant, compiled on December 18, 2023, is available on VirusTotal with the following hash:

- **b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0** (VirusTotal Link)

The second variant, compiled on February 27, 2024, has the hash:

- **4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63**

Interestingly, the latter file does not appear in sandbox results, suggesting it may have been distributed or tested privately. The compilation dates precede Microsoft's patching of CVE-2024-26169, indicating Black Basta had access to the exploit prior to its disclosure. While timestamps can be modified, experts have noted there is little reason for the attackers to do so in this instance.

Credential Harvesting

A large number of credentials were discovered within the leaked chat logs, highlighting the group's extensive credential harvesting operations. This tactic is commonly employed to gain initial access or escalate privileges within compromised networks.

Use of Exploit.in and Additional Exploits

Furthermore, evidence from the leak points to Black Basta's usage of forums such as exploit.in to acquire or trade vulnerabilities.

Conclusion

The Black Basta leak provides valuable insights into the group's modus operandi, with a clear focus on exploiting vulnerabilities in critical sectors and leveraging credential harvesting to facilitate their attacks. As more details emerge from the leaked logs, organizations must remain vigilant and proactive in addressing potential vulnerabilities before they can be exploited by other threat actors.

Bybit Crypto

Bybit Crypto Exchange Hack by Lazarus Group: A $1.5 Billion Breach

In February 2025, the cryptocurrency exchange Bybit experienced a devastating security breach, resulting in the theft of approximately 400,000 ETH tokens valued at $1.5 billion USD. The attack, which has now been attributed to the Lazarus Group (a state-sponsored threat actor group based in North Korea), demonstrates the growing sophistication of cybercriminals targeting digital assets.

Attack Vector: Exploiting Safe{Wallet}

The attack on Bybit was not a direct assault on their infrastructure but rather a calculated exploitation of a third-party multi-signature (multi-sig) platform called Safe{Wallet}. Multi-sig platforms are designed to enhance security by requiring multiple parties to approve transactions before they can be executed. However, the attackers took advantage of an often-overlooked vulnerability in the user interaction process. One common issue with multi-sig platforms is user complacency. Often, users become accustomed to quickly clicking through approval processes, "next, next, next", without adequately reviewing the transactions they are authorizing. This behavioral flaw can render the enhanced security features that multi-sig systems provide ineffective.

Compromising Safe{Wallet}

The attackers reportedly compromised a developer's workstation at Safe{Wallet}, injecting malicious JavaScript code into the frontend interface. This sophisticated

approach allowed the attackers to manipulate the user interface to present what appeared to be a legitimate transaction. In reality, the approval process was being used to authorize a massive unauthorized transfer from Bybit's cold wallet.

By disguising the transfer as a legitimate transaction, the attackers successfully evaded detection during the critical approval stage. This tactic underscores the need for enhanced vigilance and continuous monitoring of third-party systems integrated into cryptocurrency platforms.

Laundering the Stolen Funds

After successfully exfiltrating the 400,000 ETH tokens, the Lazarus Group employed laundering techniques to obscure the origins of the stolen assets. The funds were channelled through numerous intermediary addresses, exchanged for other tokens, and passed through instant swap services designed to facilitate rapid cross-network asset transfers.

As of now, the stolen funds remain dormant across multiple wallets. This strategy of letting assets sit untouched for extended periods is commonly employed by cybercriminals to avoid detection and scrutiny by blockchain monitoring tools. Eventually, these assets may be moved through further laundering processes to be cashed out.

Conclusion

The Bybit hack serves as a stark reminder of the vulnerabilities inherent in complex, interconnected systems within the cryptocurrency space. While multi-sig platforms like Safe{Wallet} are designed to bolster security, user complacency and sophisticated infiltration techniques can render these defenses ineffective. Organizations must continuously evaluate and enhance their cybersecurity measures, particularly when integrating third-party solutions.

Chainalysis

Decline in Ransomware Payments Despite Record Attack Numbers in 2024

According to a recent report by Chainalysis, ransomware payments experienced a significant decline in 2024, despite a record-breaking number of attacks throughout the year. The report reveals that victims paid approximately $813.55 million in cryptocurrency, which marks a 35% decrease from the staggering $1.25 billion extorted in 2023.

This decline in payments comes as a surprising contrast to the sheer volume of attacks reported. CyberMaxx noted that 2024 saw the highest number of attacks ever recorded, with the fourth quarter of the year marking a record-breaking

period for ransomware incidents. Despite this unprecedented activity, the decline in payments suggests a shift in how organizations are responding to ransomware threats.

Factors Contributing to Decline in Payments

The primary factors driving the decline in ransomware payments include increased law enforcement actions and a growing trend among organizations to refuse paying ransoms. These dynamics are reshaping the landscape of ransomware extortion and may indicate that criminals are struggling to adapt to heightened resistance and scrutiny.

Law Enforcement Actions

Throughout 2024, coordinated efforts from international law enforcement agencies have made significant strides in disrupting ransomware operations.

These operations are increasingly aided by blockchain analytics firms like Chainalysis, which provide authorities with tools to trace and track cryptocurrency transactions. As a result, criminals face greater difficulty in laundering funds, making ransomware operations less lucrative and more risky.

> Agencies have successfully dismantled several prominent ransomware gangs, seized cryptocurrency wallets associated with illicit transactions, and apprehended key individuals linked to major attacks.

Organizations Refusing to Pay Ransoms

Another critical factor contributing to the decline in payments is the growing trend of organizations refusing to yield to ransom demands. Many companies are increasingly choosing to absorb the costs of recovery rather than pay criminals. This shift is driven by several factors:

1. **Improved Cybersecurity Measures:** As companies strengthen their defenses and backup systems, they are more capable of recovering from attacks without needing to pay ransoms.
2. **Increased Regulatory Pressure:** Governments and regulatory bodies are discouraging ransom payments to prevent the financing of criminal enterprises.
3. **Greater Awareness:** Public and private sector entities are increasingly aware of the broader implications of paying ransoms, including the potential for future attacks and the ethical considerations of funding criminal groups.

The Paradox of 2024

Interestingly, 2024 stands as the year with the highest number of recorded ransomware attacks but also the year with the largest decline in ransom payments. This paradox highlights the resilience of organizations and the growing effectiveness of law enforcement actions. However, it also suggests that while payment volumes have decreased, the overall threat of ransomware continues to escalate.

Oracle Health Data Breach: Legacy Systems Compromised

In early 2025, Oracle Health, formerly known as Cerner, suffered a significant data breach impacting multiple U.S. hospitals and healthcare providers. The breach occurred due to unauthorized access to legacy data migration servers, using compromised customer credentials. This unauthorized access reportedly began sometime after January 22, 2025, with the attackers exfiltrating patient data to an external location.

Oracle Health became aware of the breach around February 20, 2025, **initiating a comprehensive investigation and response process**.

Notification of affected clients began in March, with Oracle Health striving to provide transparency regarding the extent of the breach.

Nature of the Breach

The stolen data reportedly includes sensitive patient information from electronic health records, though the precise scope and amount of compromised data remain unclear. The use of compromised credentials to access legacy systems underscores a common vulnerability within the healthcare sector, where outdated or insufficiently protected systems remain integrated with modern networks.

Extortion Attempt by "Andrew"

An individual identifying themselves as "Andrew" has attempted to extort the affected healthcare providers, demanding payments in exchange for not releasing the stolen data. Notably, this threat actor does not appear to be affiliated with any known ransomware group, suggesting the possibility of either a lone actor or a new entity entering the scene.

The motivations and capabilities of "Andrew" are still under investigation, but the lack of affiliation with a prominent ransomware group could complicate efforts to track and apprehend the individual. The healthcare sector remains particularly vulnerable to such attacks, given the sensitive nature of patient data and the potential harm that could result from its unauthorized disclosure.

Moving Forward

This breach highlights the ongoing challenge of securing legacy systems and ensuring that customer credentials are adequately protected. As Oracle Health continues to investigate and mitigate the impacts of the breach, healthcare organizations must remain vigilant and proactive in bolstering their own cybersecurity measures.

The incident also serves as a reminder that attackers are increasingly targeting healthcare institutions due to their critical role in society and the high value of the data they possess. Ensuring robust protection of sensitive data should remain a top priority for all entities operating in the healthcare sector.

Q1 2025 Conclusion

Security teams must prioritize patch management and ensure that critical vulnerabilities are addressed promptly. Enhanced monitoring and detection capabilities are essential to identify intrusions before data exfiltration occurs.

Organizations should also emphasize credential protection, implementing multi-factor authentication (MFA) and monitoring for compromised accounts. Finally, proactive threat intelligence gathering and collaboration with law enforcement agencies can help organizations anticipate and mitigate emerging threats.

As ransomware groups continue to adapt their tactics, organizations must remain agile and prepared to respond effectively.

About CyberMaxx

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.

We enable customers to stay ahead of evolving threat landscapes by insights from offensive programs that strengthen their defensive security.

Ready to take the first steps towards a stronger security posture? Schedule an introductory call with one of our solutions experts today.

For more information, call 1-800-897-CYBER (2923) or visit:
cybermaxx.com