TRAVELERS

Q1 CYBER THREAT REPORT

# Record Activity Driven by Array of Options for Attackers

2025

# Table of Contents


Executive Summary 03

Overview of Global Ransomware Activity in Q1 04

How Automation Amplifies the Ransomware Ecosystem 07

Social Engineering Beyond Email 09

Briefing: The New AI Tools Driving Social Engineering Activity 10

Industry Spotlight: Healthcare 13

Conclusion 14


## Published by Travelers with contributions from:


**Ryan Bell**
Director, Threat Intelligence – Cyber Risk Services, *Travelers*

**Nicholas Kelley-Ossey**
Sr. Director, Cybersecurity, *Travelers*

**Kevin Sherry**
Founder and CEO, *Darkweb IQ*

**Courtney Hassenfeldt**
Cybersecurity Technologist, *Travelers*

**Aleesha Quintana**
Cybersecurity Technologist *Travelers*

**Alex Pinto**
Sr. Director of Product Marketing – Cyber, *Travelers*

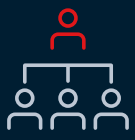
# Executive Summary

For the second quarter in a row, we've noted a new record high in the number of ransomware victims posted on leak sites (a method we've used to track ransomware activity since 2021). While the saying goes that three makes a trend, two quarters of precipitous rises in activity seems like enough reason to dig deeper into the dynamics at play in the ransomware ecosystem.

Over that time period we did not witness the kind of far-reaching vulnerability that in the past has affected thousands of organizations and generated headlines beyond the world of cybersecurity. So how is it that threat actors are gaining access to victims' systems, *en masse*, month after month?

There is not a singular answer. In fact, there are an array of options now available to gain access to systems – even for threat actors who aren't particularly skilled or experienced. From automated tools that can guess passwords to unrestricted AI chatbots that can adapt phishing email content on the fly, there are more diverse, accessible and effective options for threat actors than ever to break past an organization's defenses.

**Ransomware spiked (again) in Q1:** Over 2,200 victims were listed on leak sites in Q1, a 35% jump from the previous quarter.

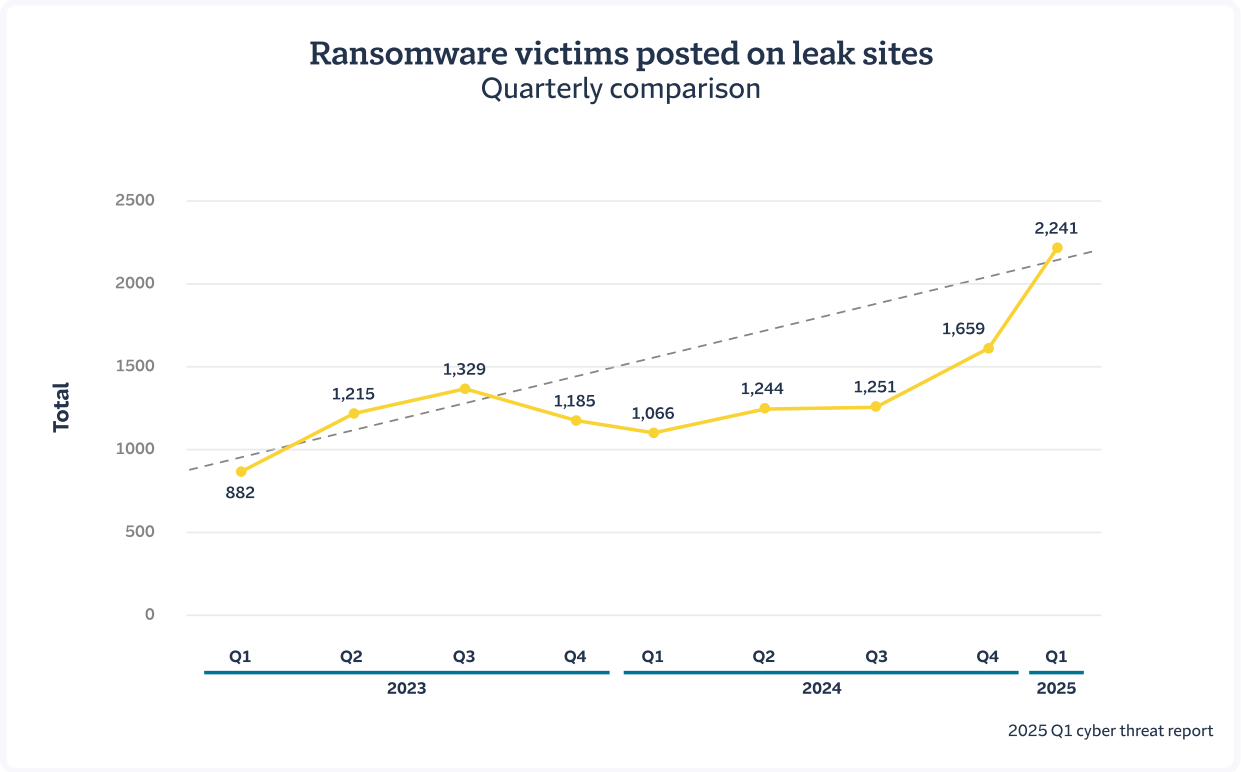


**Growth in activity was widespread:** The Cl0p ransomware group posted hundreds of victims following their use of a mass exploit, but the bigger story was the continued rise of repeatable initial access methods by a variety of groups.

**Social engineering evolves:** New tactics include Microsoft Teams impersonation, deepfakes and even physical mail scams.

# Ransomware in Q1 2025: Persistent Threats at a New, Higher Level

The first quarter of 2025 has seen ransomware attacks continue growing in frequency, with the number of victims seen posted on leak sites* rising to 2,241 between January 1st and March 30th of 2025. This marks a 35% increase in activity since last quarter and is more than double the level seen in the first quarter last year.




Those of us who watch this space closely are accustomed to seeing varying levels of ransomware activity from quarter to quarter. But a substantial increase like the one revealed in this data still has the capacity to raise eyebrows, particularly as it comes when the previous quarter (Q4 2024) had also seen a substantial increase. Together, the data from the past two quarters represent a break from the pattern of less-dramatic movements (both up and down) over several previous quarters.

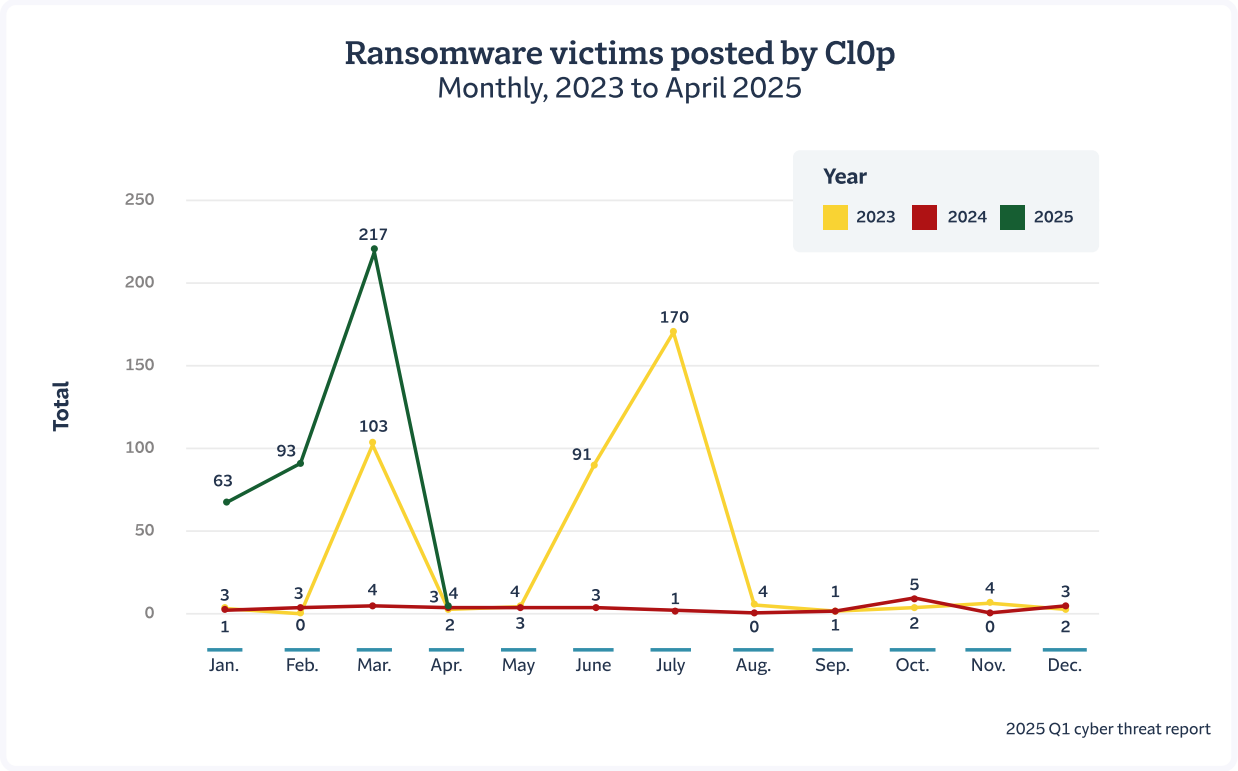
What's driven this increase in activity? From what we can see in the data there are two major drivers: a single group executing a mass exploit, and a continued rise in the use of "repeatable" initial access tactics by several active groups.

*Data shared on leaksites provides a proxy for overall ransomware activity. A victim's information will typically be posted if the victim has refused to pay a ransom. This means that the data should be viewed as a fraction of overall activity, but one that can provide a longitudinal comparison of activity over longer time frames.

## Cl0p drives recent spike in ransomware activity

The first driver of note for Q1 2025 was the mass-exploit of a vulnerability by the Cl0p ransomware gang. The initial attacks exploiting the vulnerability took place in December 2024 and led to at least 373 victims being posted on leak sites in the following months, including **over 200 in March alone**, making it the most active month in our records dating back to 2021.

Cl0p is a specialized gang whose activity tends to come in short (but dramatic) bursts. Based on previous activity, Cl0p was "overdue" for an appearance, having remained relatively dormant since the summer of 2023 with their infamous MOVEit attack. The December exploit matched the group's past patterns in that respect, with a sudden drop-off in new victims in April, as well as with their choice of target being a specific managed file transfer and storage solution (a type of technology Cl0p has targeted in the past). In this case the attack leveraged two severe vulnerabilities, CVE-2024-50623 and CVE-2024-55956 – each carrying a Common Vulnerability Scoring System (CVSS) score of 9.8 out of 10, indicating nearly the highest possible level of risk and urgency – which allowed attackers to perform unrestricted file uploads/downloads and execute arbitrary commands on vulnerable systems.




Bear in mind that the nearly 400 victims shown in our data are only those who likely refused some element of a demand by the group. Adding the (unknown) number of victims who chose to quickly pay a ransom would push the victim count higher.

## Diverse initial access tactics drive consistent drumbeat of activity

The other main driver of ransomware in Q1 was the continued trend toward a more "organic" style of ransomware, which was highlighted in our last quarterly report.

With this strategy, rather than exploiting one major vulnerability at a time – the approach taken by Cl0p and many other prolific groups in the past – threat actors instead use tactics that can repeatedly and reliably provide initial access to victims' systems. That often means breaking in by brute-forcing passwords and weak credentials, using social engineering, or exploiting an array of older, less well-known vulnerabilities.

> One revealing fact: **even if you remove the hundreds of victims from Cl0p's mass-exploit, last quarter would still have seen the most ransomware victims we've recorded** in a single quarter since we began measuring leak site victims in 2021. That is largely due to this trend in initial access tactics.

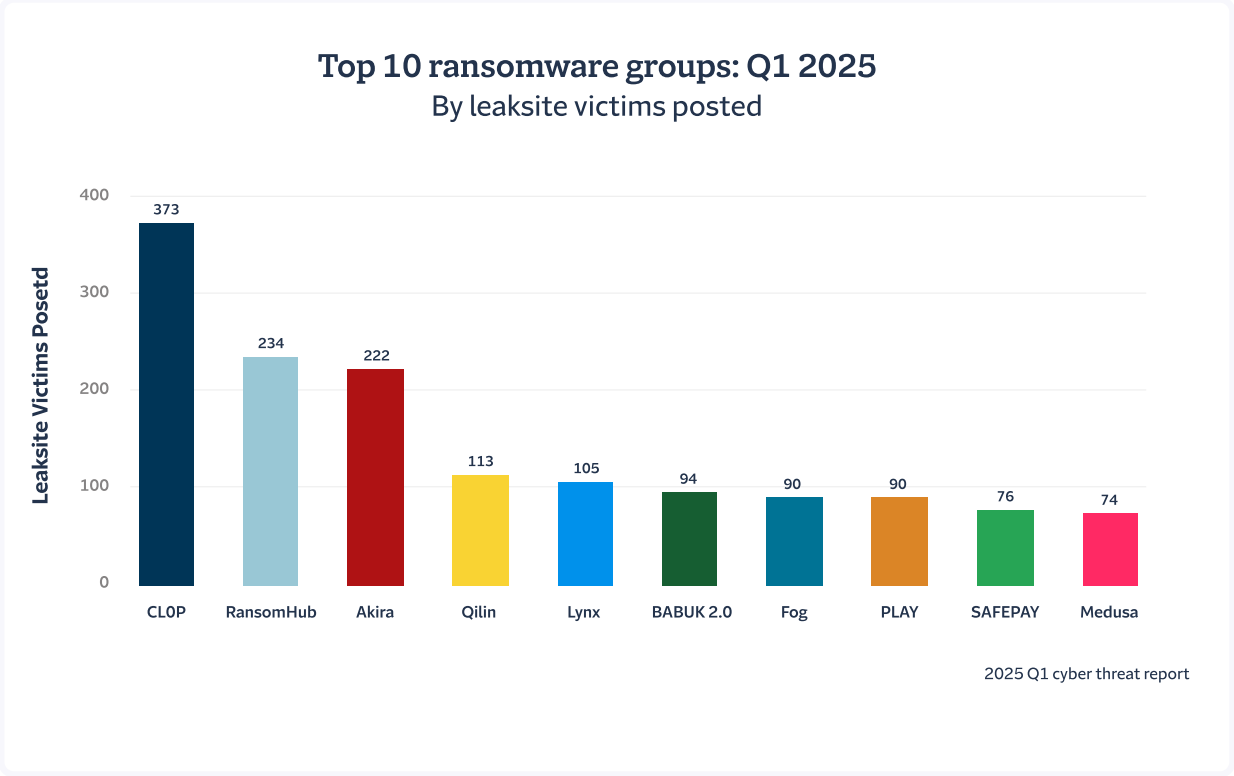
We've continued to gain insight into how threat actors are operationalizing this approach and what kinds of attacks result. A few observations from this quarter:

- Researchers found that the Black Basta group has developed an automated tool called "BRUTED" to conduct large-scale brute-force attacks on enterprise virtual private networks (VPNs) and firewalls, exploiting weak or reused credentials to gain unauthorized access. The group also is known to employ social engineering through common communications apps used by many companies (see page 9 of this report).

- While it appears to have shut down at the end of March (or perhaps merged with another group), Ransomhub was a particularly prolific ransomware-as-a-service (RaaS) operation in early 2025, attacking over 200 victims. The attacks were spread across a variety of types of internet-facing infrastructure and hit a variety of industries, suggesting these were opportunistic targets drawn in by casting a wide net, rather than a targeted strategy against a known weakness.

- We also saw continued targeting of managed service providers (MSPs) and their remote management tools. In one recent case, the Qilin ransomware actors gained access to an MSP administrator's ScreenConnect credentials through a well-crafted phishing email, subsequently launching ransomware attacks on the MSP's customers.

Looking across the top groups by activity, the large number of groups with significant levels of activity suggests a strong "ecosystem" of ransomware at work driving all this activity.

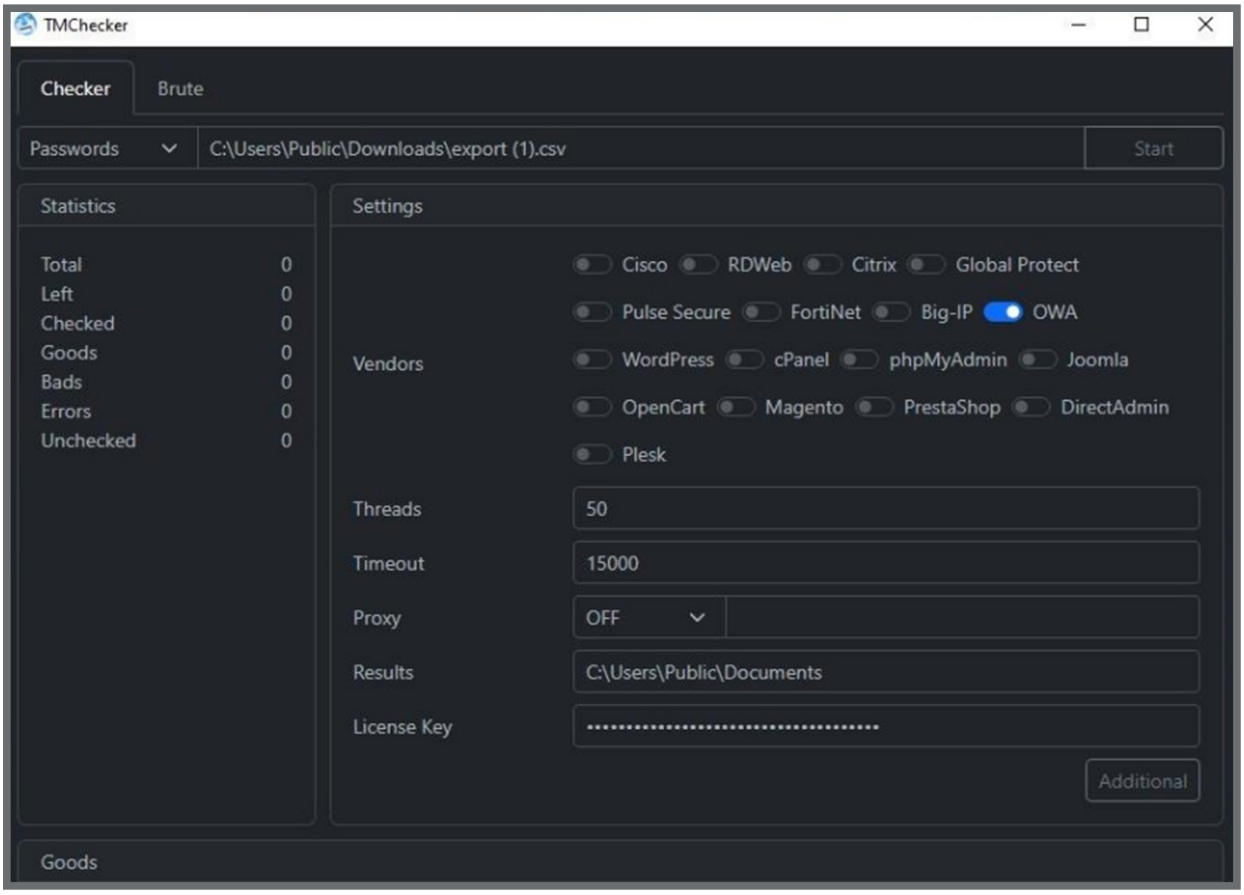



# How Automation Amplifies the Ransomware Ecosystem

We attribute much of the increase in repeatable initial access tactics discussed in the previous section to the introduction of automation.

One example can be seen in the popularity of a specific tactic: compromising user credentials on enterprise VPNs. In our last report we commented on the fact that this tactic became more widespread after a training manual, which was developed by an initial access broker, was leaked and passed around among threat actors. While some followed the guide's methods to compromise VPNs one by one, others saw the effectiveness of this approach and "productized" it.

Researchers at Darkweb IQ, an offensive cybercrime interception firm, have been tracking the rise of new, easy-to-use tools to conduct brute force attacks, as well as a style of attack known as password spraying, against various types of public-facing enterprise accounts. One of these is called TMChecker, designed to simplify and automate the process of compromising accounts. TMChecker has built-in compatibility to attack several widely used enterprise tools.




A screenshot of TMChecker provided by researchers at Darkweb IQ shows the tool that attackers can use to conduct brute force attacks against widely used software.

More recently, Darkweb IQ obtained and analyzed a new credential checking and brute-forcing tool, "Golden Checker," which represents a continued trend in the modularization and commodification of credential validation tooling — where infrastructure, credential parsing and brute-force orchestration are bundled to simplify the process for threat actors. Like TMChecker, Golden Checker utilizes a web-based interface that makes it easy to use. It can quickly test large numbers of usernames and passwords on various online login pages, such as remote desktops, websites, and virtual private network (VPN) devices.

What started as an insider secret has now become a widely automated and productized operation, keeping ransomware groups busy with a steady supply of new victims.

# Social Engineering Goes Broader and Deeper

Major zero-day vulnerabilities naturally grab headlines. But as any practitioner in cyber insurance or incident response knows all too well, exploiting weaknesses in software is far from the only way that a threat actor can break into an organization's system.

After more than three decades of widespread use of the internet, social engineering remains one of the most effective tools in a threat actor's arsenal. Recently, threat actors have expanded their tactics to go broader – increasingly leveraging communication avenues other than email – and deeper, with AI tools that enable new approaches to classic email phishing.

## Microsoft Teams Exploitation

The targeting of organizations using Microsoft products by threat actors is not a new phenomenon. However, recent reports indicate that multiple groups have used Microsoft Teams to impersonate IT help desks in the past quarter. Research published by Sophos highlights two groups that initiated attacks by inundating users' inboxes with spam emails, subsequently following up on Teams while posing as help desk personnel offering to resolve the issue.

Later in the quarter a threat actor was observed, again, posing as help desk support and sending a Teams message to targets, which contained a malicious PowerShell command. These attacks showcase a continued trend in the abuse of Teams and the default setting of allowing external calls, and messages. If an organization requires the use of these features it is best for employees to be trained on the threats associated with it.

This activity has been observed in Travelers claims, as shown in this anonymized excerpt from a claim report:

> "User received an MS Teams call at 10:45am EST from a threat actor. The threat actor claimed to be calling regarding a SPAM Bomb event from Feb 14th. The threat actor impersonated the helpdesk and convinced the user to download software, Quick Assist, that enabled remote access her PC. The threat actor then downloaded malware onto the user's computer."

## "Snail Mail" Threats

In February, organizations began receiving physical letters claiming to be from the threat actor BianLian. These letters stated that a ransom payment was required to prevent the exposure of data that had supposedly been exfiltrated from the targeted organization. Upon investigation, none of the targeted organizations found any evidence of actual data theft or system breaches, which limited the impact of the letters – although the novelty of the attack style generated widespread interest. Recently physical mail has also been used to target individuals, with fake letters sent impersonating The Swiss National Cyber Centre and packages supposedly coming from Amazon, in each case containing a malicious QR codes.

These types of attacks are not as common, but due to the widespread publication of the fake BianLian letters organizations should be aware of the threat. It is important people are aware not to access links or scan QR codes of unknown origin.

## Briefing: The New AI Tools Driving Social Engineering Activity

In the past few years there has been a persistent mismatch between the world-changing possibilities embodied by new AI tools and the reality of the as-yet-limited impact these tools are having on things like corporate financial results and employment numbers. It's been a similar story in the world of cybercrime: though it does not take a strong imagination to think of a scenario where threat actors use AI to massively increase their efficiency and capability at little cost, evidence of major changes in the patterns and habits of threat actors has been scarce.

That mismatch may be starting to break down. New research from the past quarter has shed light on the ways AI is making its way into the efforts of threat actors on several fronts. The following are a sample of the recent findings from security researchers around the industry, including at Travelers, on the frontier of AI usage.

### AI-Driven Polymorphic Phishing

A notable evolution in phishing tactics is the rise of AI-powered polymorphic phishing – a technique that uses generative AI to craft and continuously modify phishing emails in real time. These polymorphic characteristics make it exceedingly difficult for conventional filters and static rule-based security systems to detect malicious content. In fact, Knowbe4, a security training firm, has predicted that by 2027, the traditional method of classifying phishing incidents into discrete campaigns may become obsolete, as polymorphic attacks will continue to evolve independently, rendering static categorizations ineffective.

**GhostGPT: A New Frontier in AI-Enabled Phishing**

One of the most notable tools fueling the recent spike in AI-enabled phishing is GhostGPT – an uncensored AI chatbot specifically tailored for cybercriminal use. Unlike mainstream AI platforms, GhostGPT operates no safeguards, allowing users to generate phishing emails, malware, and exploit code on demand.

In January 2025, researchers from Abnormal Security identified GhostGPT as the source behind a rise in suspicious phishing emails targeting clients. In one test, the AI was prompted to generate a DocuSign phishing email, which it executed with a degree of realism and deception that made it suitable for immediate deployment in real-world attacks. This easy accessibility may lower the barrier to entry for less-skilled threat actors, accelerating the production and personalization of phishing lures across industries.

**The Rise of Criminal AI Ecosystems**

GhostGPT is part of a broader trend of malicious AI platforms that began emerging shortly after OpenAI released ChatGPT in late 2022. WormGPT, introduced in early 2023, was among the first AI models explicitly designed for malicious purposes. It was soon followed by other variants like WolfGPT and EscapeGPT.

These tools are not isolated developments. Researchers have now observed advertisements for GhostGPT on dark web forums, complete with subscription models, user guides and customer support – mirroring legitimate software-as-a-service (SaaS) offerings. This shift indicates that cybercriminals are building full-scale business infrastructures to support and monetize AI-driven attacks.

Even legitimate large language models (LLMs) are in the cross hairs. Research from Cisco reveals that fine-tuning LLMs for specific tasks significantly compromises their safety and security features. Models fine-tuned for domains like biomedicine, finance and law exhibited a much greater likelihood of generating harmful responses compared to their original versions. This vulnerability is exploited by cybercriminals by weakening guardrails and opening the door to jailbreaks, prompt injections and model inversion.

**Deepfake-Driven Attacks**

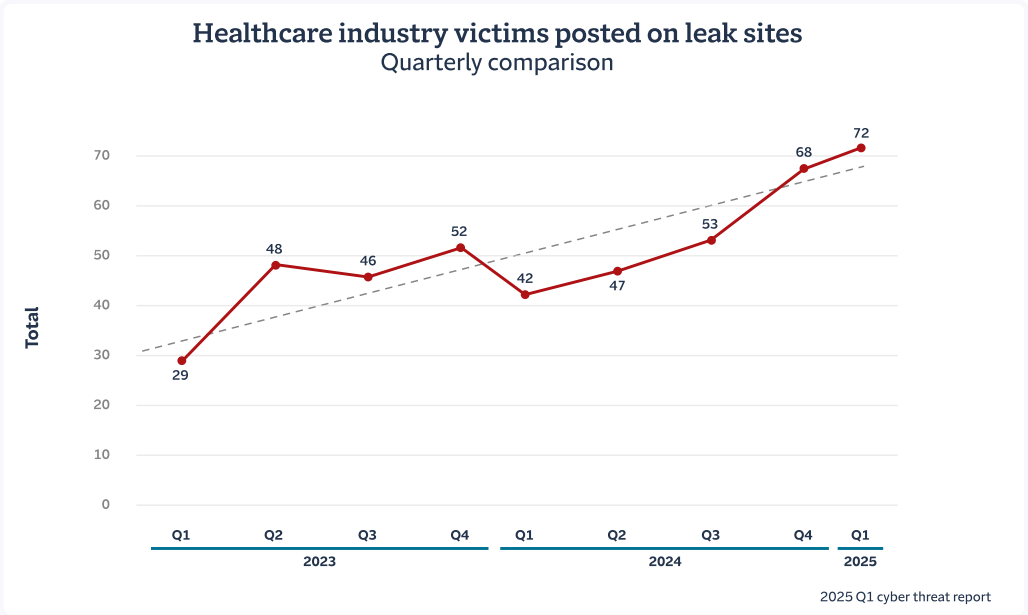
While it's still early in the evolution of deepfakes, they continue to be observed as tactics used for social engineering. For example, last quarter saw a phishing campaign that targeted YouTube creators using videos impersonating YouTube's CEO to steal credentials. There have also been reports of successful attacks on executives resulting in the fraudulent transfer of funds.

At Travelers, we took the opportunity to test this out for ourselves. Using widely available tools, we set out to see if we could develop a convincing deepfake of an executive. Using only a few minutes of audio from an interview given by a Travelers executive, coupled with a still image taken from the video of the interview, we were able to generate a reasonably convincing video-animated deepfake.

Gartner forecasts that by next year, 30% of enterprises will view identity verification and authentication solutions as unreliable when used alone, due to the prevalence of AI-generated deepfakes. It is anticipated that the use of deepfakes to target organizations will persist, manifesting through methods such as fraud, phishing, smishing or vishing.

Although identifying manipulated videos, images or voices can be challenging, recognizing unusual email addresses, links or phone numbers as potential red flags is a critical first step. Providing employees with cyber awareness training and keeping them informed about ongoing threats is essential for mitigating these risks.

# Industry Spotlight: Healthcare




Cyberattacks on the healthcare industry have increased in recent years. In 2024 alone, approximately 276 million patient records were compromised in the U.S., far more than any prior year. One of the primary drivers of these attacks is ransomware. According to a joint study by Michigan State, Yale, and Johns Hopkins universities, ransomware was behind only 11% of healthcare industry breaches by count in 2024, but those incidents accounted for a staggering 69% of all compromised patient records that year. While some ransomware groups prohibit attacks against targets in healthcare, there is a substantial minority that actively target the sector: in Q1 2025 35% of active ransomware groups were observed attacking healthcare organizations according to a Travelers analysis of victims posted on leak sites.

The attack surface for healthcare is vast, and cybercriminals are increasingly targeting not just patient records but also medical software and systems. In one example, recent research uncovered malware campaigns that disguise malicious code as legitimate healthcare applications, including imaging viewer tools commonly used by patients. DICOM — the protocol used by imaging devices to exchange information — has not been directly exploited in these recent attacks, however, threat actors have infected software linked to DICOM viewers. This highlights how attackers are identifying ways to gain a foothold that can become entry points into larger healthcare networks.

Operational challenges heighten risk exposure. Many healthcare organizations operate with limited budgets and staffing, which can lead to gaps in cybersecurity training and defenses. The urgent, life-critical nature of healthcare services also increases the pressure to pay ransoms quickly, making providers more attractive targets in addition to the high value of patient data. As ransomware toolkits become easier to access and deploy, the healthcare industry remains one of the most exposed sectors.

# Conclusion

The first quarter of 2025 has confirmed what many in the cybersecurity community have been anticipating: ransomware activity is not just persisting—it's evolving. This maturing threat landscape is fueled by increasingly repeatable access methods, widespread use of automation, and the emergence of new AI-enabled tactics. Threat actors are operating with greater efficiency and reach, supported by a growing ecosystem of tools and services designed to lower barriers and scale up attacks. With the volume and variety of tactics expanding, organizations must be prepared for a threat environment where high levels of activity are not the exception—they're the baseline.

### Recommendations from the Travelers Cyber Risk Services Team

To mitigate these risks, organizations should adopt a strong cyber prevention program, including the following recommendations detailing the top security investments with the greatest return on investment.

These recommendations will help increase the bar required for ransomware actors to successfully carry out an attack on an organization.

**They include:**

- Implement phishing-resistant MFA for all remote access and email.
- Run an effective vulnerability management program to quickly patch critical vulnerabilities in edge devices, such as VPNs.
- Ensure you have reliable backups and have a resilient disaster recovery and business continuity plan
- Run EDR solutions with 24x7 active monitoring

travelers.com

One Tower Square
Hartford, CT 06183

Travelers analysis was made possible with supporting data from eCrime.ch.