Trout

# RANSOMWARE OF 2025: WHO'S MAKING THE HEADLINES?

trout.software

# Executive Summary

The year 2025 has barely begun, yet ransomware groups have wasted no time in making their presence felt. Cybercriminals are executing increasingly sophisticated attacks, leveraging zero-day vulnerabilities, and shifting towards novel extortion models. The rapid rise in ransomware incidents targeting critical infrastructure and high-value sectors demands immediate attention from security professionals.

This report examines the leading ransomware groups dominating the landscape, their evolving tactics, and law enforcement's responses. From Clop's encryption-free extortion to RansomHub's safe-mode exploits, attackers are refining their techniques to evade detection and maximize payouts. Meanwhile, authorities are striking back, with multinational operations leading to key arrests and infrastructure takedowns.

Beyond highlighting the latest threats, this report provides actionable defensive strategies to bolster cybersecurity resilience. Organizations must adopt multi-layered security, network segmentation, and proactive threat monitoring to stay ahead of the evolving ransomware menace.

# Contents

# Ransomware Evolution

## Introduction

As of early 2025, ransomware activity has already intensified, demonstrating an alarming escalation in both frequency and sophistication. In this report, we assess the state of ransomware threats, providing historical context, an analysis of recent trends, and statistical insights into the evolving cyber extortion landscape.

Ransomware is a type of malware designed to encrypt files on a target system, rendering them inaccessible. Cybercriminals then demand a ransom in exchange for decryption keys, often leveraging additional extortion techniques such as data leaks to increase pressure on victims.

## Historical Context and Evolution of Ransomware

The first documented case of ransomware dates back to 1989 with the AIDS Trojan (PS Cyborg). This early example, created by Harvard-trained evolutionary biologist Joseph L. Popp, was distributed via 20,000 infected diskettes labeled “AIDS Information – Introductory Diskettes” at a World Health Organization (WHO) conference. Victims were asked to send a $189 payment to a post office box in Panama to regain access to their data. However, due to flaws in the encryption mechanism, recovery was possible without the attacker’s involvement. Popp was ultimately arrested, marking one of the first cases of cyber extortion.

Since then, the internet has expanded from an academic and military network into a ubiquitous global infrastructure, and cybercriminals have capitalized on this growth. Ransomware has evolved significantly, transitioning from isolated attacks to an industrialized cybercrime model.

## Key Milestones in Ransomware Evolution

- 2000s: Early RSA-based ransomware variants such as Archiveus and GPCode emerged.

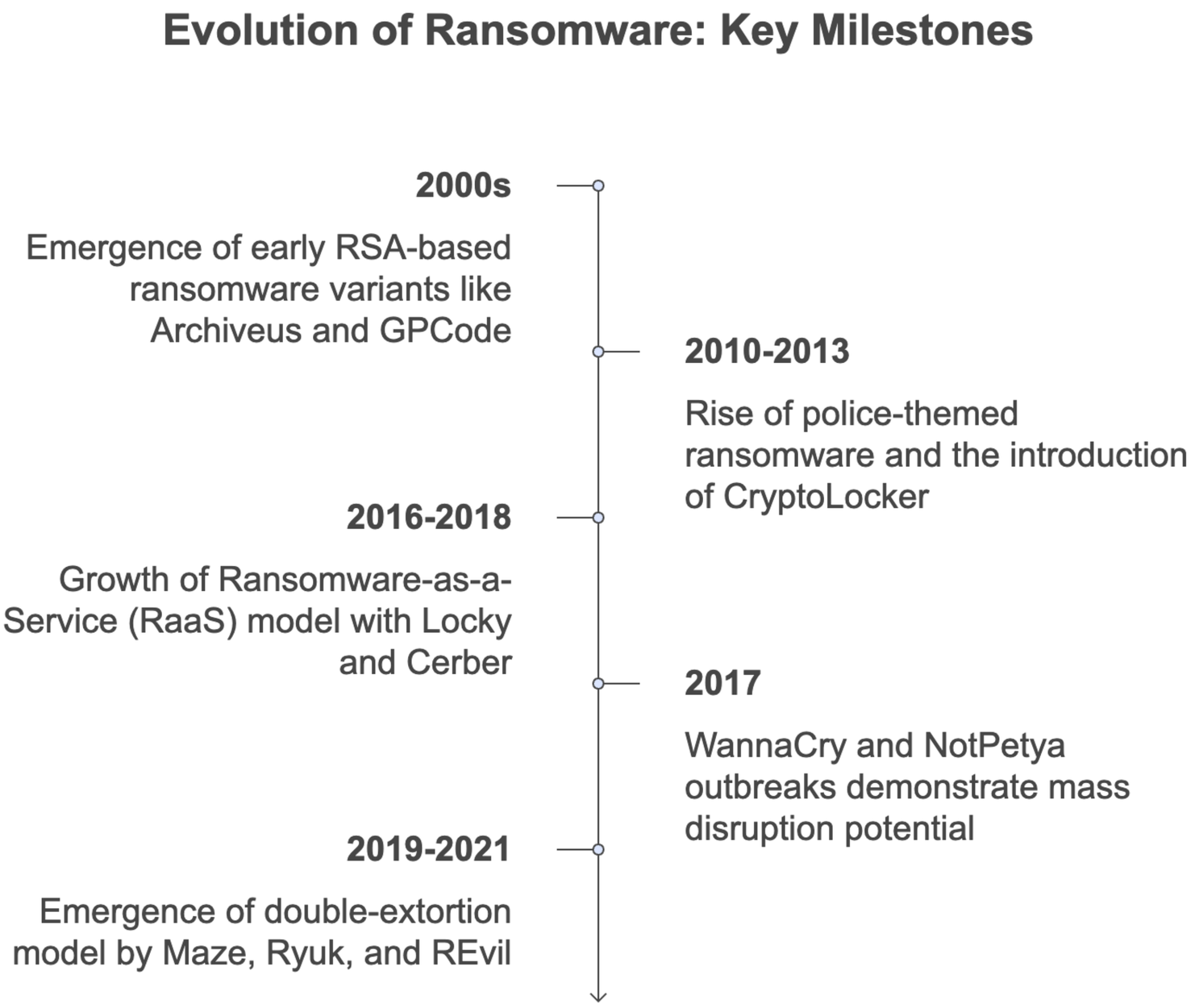
- 2010-2013: The rise of police-themed ransomware (e.g., WinLock, Reveton) introduced scare tactics, often impersonating law enforcement. The emergence of cryptocurrency facilitated untraceable ransom payments, leading to the development of CryptoLocker, one of the first large-scale Bitcoin-powered ransomware campaigns.

- 2016-2018: The Ransomware-as-a-Service (RaaS) model gained traction with groups like Locky and Cerber, allowing cybercriminals to distribute ransomware on a global scale.

- 2017: The WannaCry and NotPetya outbreaks highlighted ransomware's potential for mass disruption, affecting critical infrastructure and global enterprises.

- 2019-2021: The double-extortion model emerged, pioneered by ransomware groups such as Maze, Ryuk, and REvil. These groups not only encrypted victims' data but also threatened to leak it publicly, increasing the pressure to pay.

- Today: Modern ransomware groups operate as organized cybercrime syndicates, employing sophisticated tactics, automation, and supply chain attacks. The ransomware ecosystem is now driven by highly structured criminal enterprises, with affiliates and monetization strategies resembling legitimate businesses.

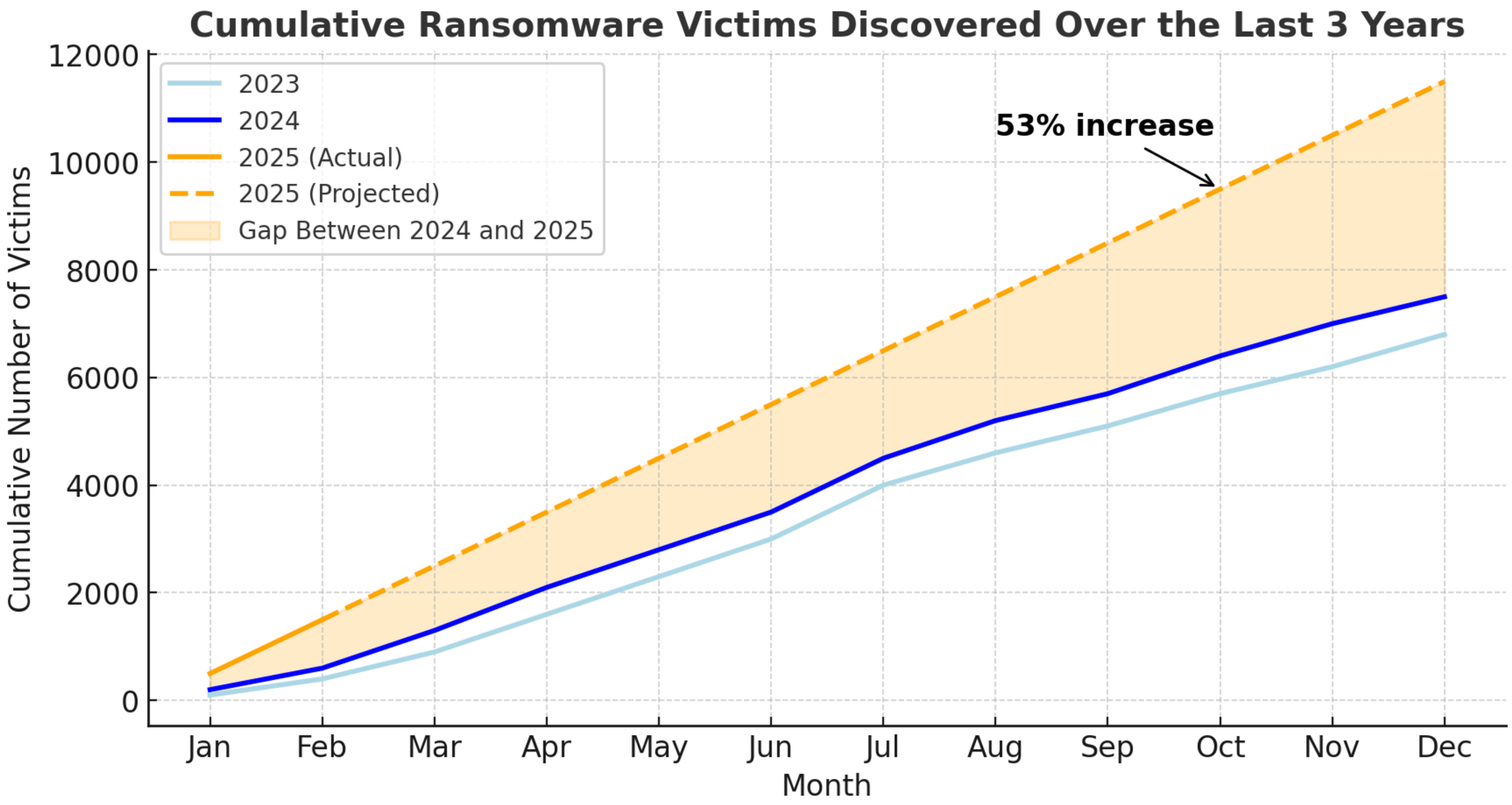


# Ransomware Trends in 2025

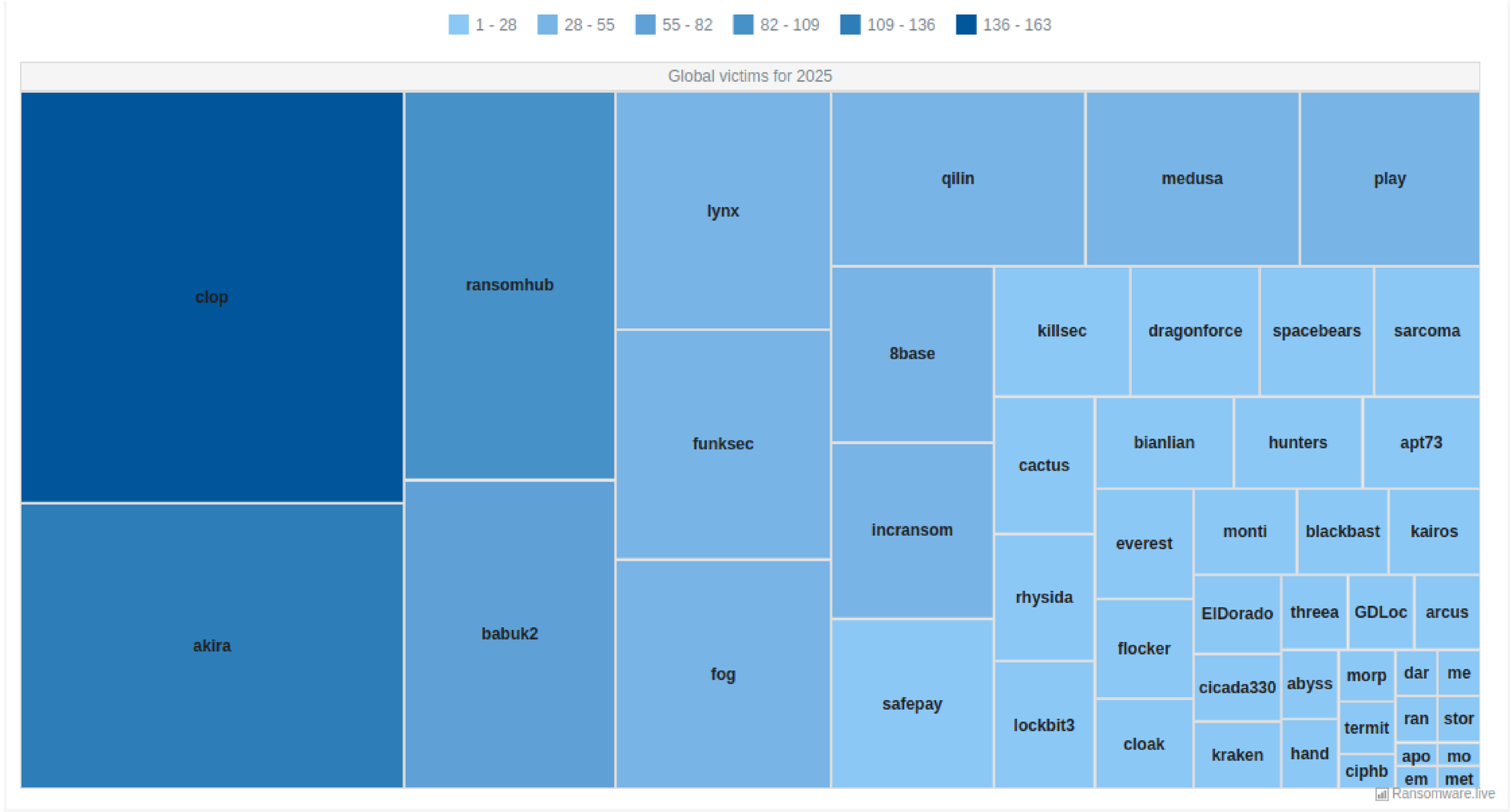
## Overall trend

To monitor the evolving ransomware landscape, we utilized Ransomware.live, a ransomware leak site monitoring tool. Originally a fork of ransomwatch and inspired by ransomlook, this tool aggregates data from various ransomware leak sites, tracking victim disclosures and attack trends in real time.

- According to Ransomware.live statistics, the number of reported ransomware attacks in early 2025 has already surpassed the previous year's figures within the first quarter.
- The increasing sophistication of ransomware operations, combined with geopolitical tensions and economic incentives, suggests that this trend will continue to escalate.



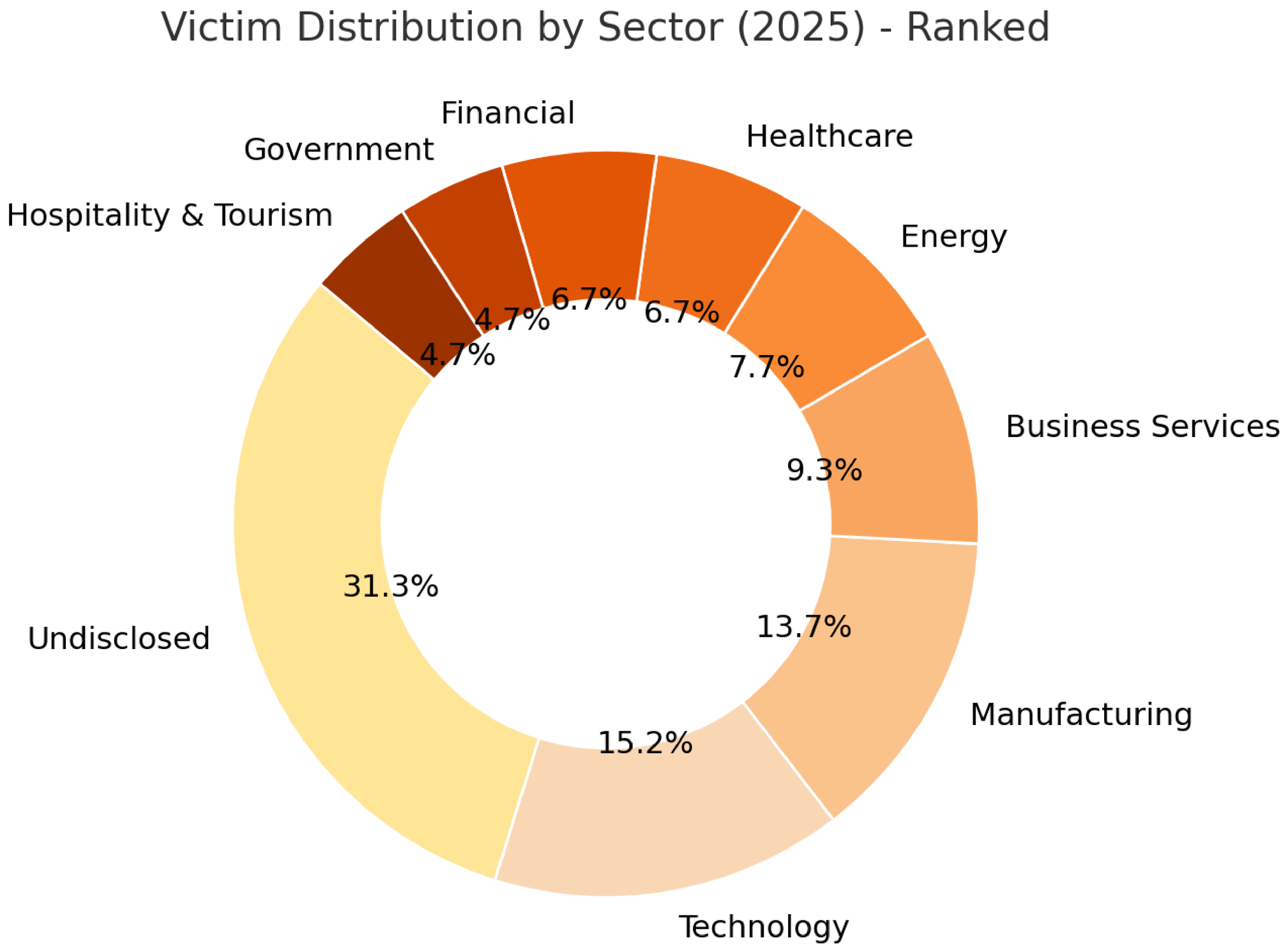
# Attack groups




Clop (23.3%), RansomHub (13.4%), and Akira (12.9%) are the dominant ransomware groups, collectively accounting for nearly 50% of all reported incidents. This suggests a high concentration of attacks led by a few major players, reinforcing the industrialization of ransomware operations.

Smaller groups like Medusa, Qilin, and Play still contribute significantly, indicating a fragmented but highly active cybercrime ecosystem.

## Vertical trends




Among disclosed cases, technology (15.2%) and manufacturing (13.7%) are top targets, likely due to their reliance on interconnected systems, intellectual property, and critical supply chains—making them prime candidates for disruption.

Business services (9.3%), energy (7.7%), healthcare (6.7%), and financial institutions (6.7%) also face persistent threats, reflecting attackers' focus on high-value data and essential services. Attacks on government (4.7%) and hospitality (4.7%) further highlight how ransomware is being used for espionage, disruption, and financial extortion.

These trends reinforce the need for sector-specific cybersecurity measures, mandatory reporting policies, and proactive defense strategies to mitigate operational and economic risks.

# Most Active Ransomware groups

## Clop

### What is Clop?

Clop is a ransomware variant associated with TA505, a cybercriminal group active since at least 2014. TA505 is known for compromising over 3,000 U.S.-based organizations and 8,000 global organizations. The group frequently changes its malware and drives global trends in criminal malware distribution, including ransomware campaigns involving Clop.

Emerging in February 2019 from the CryptoMix ransomware variant, Clop was used as a Ransomware as a Service (RaaS) in large-scale spear-phishing campaigns. These campaigns utilized verified and digitally signed binaries to bypass system defenses. Clop initially employed a 'double extortion' tactic, stealing and encrypting victim data, and publishing exfiltrated data on the Tor network via the CL0P^_-LEAKS website if the ransom was not paid.

In 2023, Clop increasingly adopted pure extortion methods with "encryption-less ransomware," which skips the encryption process but still threatens to leak data if the ransom is not paid. This approach allows threat actors to achieve the same results and generate larger profits.

### Technical Overview

The Clop ransomware group is known for evolving its tactics, techniques, and procedures (TTPs). They typically gain initial access through phishing emails containing the Get2 Loader, which downloads the SDBot and FlawedAmmy RAT. They also use valid credentials or exploit various CVEs over time, as shown in the graph below:

In late January 2023, the Clop ransomware group launched a campaign using a zero-day vulnerability, now cataloged as CVE-2023-0669, to target the GoAnywhere MFT platform. There is speculation about the use of a Cleo product vulnerability tracked as CVE-2024-55956, which Clop claimed to have exploited.

### Impact

As of early 2025, Clop has reportedly targeted 161 victims.

## Attack profile

Clop's toolkit includes several types of malware to collect information:

- FlawedAmmyy/FlawedGrace remote access trojan (RAT) collects information and attempts to communicate with the Command and Control (C2) server to enable the download of additional malware components [T1071], [T1105].

- SDBot RAT propagates the infection by exploiting vulnerabilities and dropping copies of itself in removable drives and network shares [T1105]. It can also propagate through peer-to-peer (P2P) networks. SDBot acts as a backdoor [T1059.001] to execute commands on compromised computers and uses application shimming for persistence and to avoid detection [T1546.011].

- Truebot is a first-stage downloader that collects system information and takes screenshots [T1113]. Developed by the Silence hacking group, Truebot can load shell code [T1055] or DLLs [T1574.002], download additional modules [T1129], execute them, or delete itself [T1070]. TA505 has used Truebot to download FlawedGrace or Cobalt Strike beacons.

- Cobalt Strike is used to expand network access after gaining access to the Active Directory (AD) server [T1018].

- DEWMODE is a PHP web shell designed to target Accellion FTA devices and interact with the underlying MySQL database to steal data from compromised devices [1505.003].

- LEMURLOOT is a C# web shell designed to target the MOVEit Transfer platform. It authenticates incoming HTTP requests via a hard-coded password and can run commands to download files, extract Azure system settings, retrieve detailed record information, and manage user accounts. The web shell returns data in a gzip compressed format.

## Additional Links

For further information, visit the Ransomware.live website, the Mitre&ATTACK groups page associated with Clop, or the CISA report on the topic.

# Akira

## What is Akira?

Akira is a ransomware variant and deployment entity active since at least March 2023. Akira gains initial access by using compromised credentials to exploit single-factor external access mechanisms such as VPNs. It then employs various publicly available tools and techniques for lateral movement within the network. Akira is associated with "double extortion" ransomware activities, where data is exfiltrated from victim environments before encryption, with threats to publish the files if the ransom is not paid. Technical analysis of Akira ransomware reveals multiple overlaps and similarities with Conti malware.

As a Ransomware-as-a-Service (RaaS), Akira has been utilized by several groups, including GOLD SAHARA and PUNK SPIDER.

## Technical Overview

Akira ransomware is a 64-bit Windows binary primarily developed in C++ with extensive use of C++ libraries. It employs the Boost library for its asynchronous encryption functionality and is compiled using Microsoft Linker version 14.35. In June 2023, a security researcher known as "rivitna" published a Linux version of Akira, which is also 64-bit and incorporates the Boost library.

Initially, early versions of Akira ransomware encrypted files with the ".akira" extension. By August 2023, some attacks introduced a variant called Megazord, written in Rust, which encrypts files with the ".powerranges" extension. Despite the introduction of Megazord, Akira threat actors have continued to deploy both the original Akira ransomware, including an updated Akira_v2 variant, and Megazord interchangeably in their campaigns, as confirmed by CISA.

## Impact

As of early 2025, Akira has reportedly targeted 141 victims.

## Additional Links

For further information, you can refer to our report on Akira here. Additional resources are available on the Ransomware.live website, the Mitre&ATTACK groups page associated with Akira, and the CISA report on the topic.

# Ransomhub

## What is Ransomhub?

RansomHub emerged in mid-February 2024 and has already listed several organizations as alleged victims of their attacks, which involve extortion through encryption and data leaks.

The announcement of RansomHub's new Ransomware-as-a-Service (RaaS) was published on RAMP4U (or RAMP), a Russian-origin forum used by cybercriminals to advertise malicious services. A user named 'koley' announced the affiliate program on February 2, 2024.

In the RaaS announcement, it was mentioned that the money laundering of paid ransoms is the responsibility of the affiliate. All communication and sending of the decryptor to the victim are handled through chat. The revenue split for this RaaS is 90% for the affiliate and 10% for the developer, who is identified as 'koley.'

RansomHub appears to have ties to both ALPHV (BlackCat) and Knight Ransomware. Following a February 2024 ransomware attack on Change Healthcare, ALPHV initially claimed responsibility but was later accused by an affiliate, notchy, of withholding their share of a $22 million ransom. After ALPHV's sudden disappearance in March 2024, RansomHub surfaced, claiming possession of the same 4TB of stolen data. Researchers noted strong similarities in tactics, techniques, infrastructure, and code between ALPHV and RansomHub, suggesting RansomHub could be a rebrand or composed of former ALPHV affiliates. Additionally, RansomHub shares significant code overlap with Knight Ransomware (formerly Cyclops), including being written in Go, using Gobfuscate for obfuscation, and employing similar ransom notes and encryption techniques. Both also utilize a strategy of restarting systems in safe mode before encryption. These overlaps imply that RansomHub could be a hybrid operation, merging elements of ALPHV's tactics with Knight's codebase, potentially involving former affiliates from both groups.

## Impact

As of early 2025, RansomHub has reportedly targeted 124 victims.

## Attack profile

So far, no new evidence has emerged that could directly connect RansomHub and ALPHV, especially regarding their code. While ALPHV uses a payload written in Rust, RansomHub employs a payload written in Golang and C++.

The malware employs countermeasures against analysts, such as the use of the "gobfuscate" tool, which makes static analysis complex by adding an additional layer of protection to the payload, requiring a 32-byte password to initiate.

RansomHub affiliates typically gain initial access by targeting internet-facing systems and user endpoints using various methods, including phishing emails [T1566], exploitation of known vulnerabilities [T1190], and password spraying [T1110.003]—the latter often leveraging credentials obtained from data breaches. Proof-of-concept exploits are commonly sourced from platforms like ExploitDB and GitHub [T1588.005]. The following Common Vulnerabilities and Exposures (CVEs) have been observed in their attacks:

- CVE-2023-3519 (CWE-94) – Citrix ADC (NetScaler) Remote Code Execution: This vulnerability allows unauthenticated attackers to trigger a stack buffer overflow in the NetScaler Packet Processing Engine (NSPPE) via a crafted HTTP GET request, enabling remote code execution as root.

- CVE-2023-27997 (CWE-787 | CWE-122) – FortiOS and FortiProxy Heap-Based Buffer Overflow: Affects multiple versions of FortiOS and FortiProxy SSL-VPNs, allowing remote attackers to execute arbitrary code through specially crafted requests.

- CVE-2023-46604 (CWE-502) – Apache ActiveMQ Remote Code Execution: Exploits the Java OpenWire protocol marshaller, allowing attackers to manipulate serialized class types and execute arbitrary shell commands by targeting brokers or clients. Updating to versions 5.15.16, 5.16.7, 5.17.6, or 5.18.3 mitigates this vulnerability.

- CVE-2023-22515 – Confluence Data Center and Server Privilege Escalation: Enables attackers to create unauthorized administrator accounts on publicly accessible Confluence instances, granting full system access. Atlassian Cloud sites are not affected.

- CVE-2023-46747 (CWE-306 | CWE-288) – F5 BIG-IP Authentication Bypass: Allows attackers with network access to bypass authentication on the BIG-IP system, potentially executing arbitrary system commands through the management port or self IP addresses.

- CVE-2023-48788 (CWE-89) – Fortinet FortiClientEMS SQL Injection: A SQL injection vulnerability that enables attackers to execute unauthorized code through specially crafted packets targeting specific FortiClientEMS versions.

## Attack profile - continued

- CVE-2017-0144 – Windows SMBv1 Remote Code Execution: This vulnerability in Microsoft Windows' SMBv1 server allows attackers to execute arbitrary code via maliciously crafted packets. Known as the exploit used in the WannaCry ransomware attack.

- CVE-2020-1472 – Netlogon Privilege Escalation (Zerologon): Allows attackers to establish a vulnerable Netlogon secure channel connection to a domain controller, leading to privilege escalation.

- CVE-2020-0787 – Windows Elevation of Privilege Vulnerability: Often exploited alongside Zerologon, this vulnerability enables attackers to elevate privileges and gain deeper access to compromised systems.

Here is a list of tools used by RansomHub affiliates:

1. BITSAdmin – Command-line utility for managing asynchronous file transfers via the Background Intelligent Transfer Service (BITS).
2. Cobalt Strike [S0154] – Penetration testing tool used for lateral movement and file execution.
3. Mimikatz [S0002] – Credential extraction tool used for privilege escalation.
4. PSExec [S0029] – Remote execution tool for running programs and commands on remote systems.
5. PowerShell – Cross-platform automation framework for scripting, configuration management, and command execution.
6. RClone – Command-line program used to sync files with cloud storage services.
7. Sliver – Penetration testing toolset for remote command and control.
8. SMBExec – Tool for remote code execution by manipulating SMB services.
9. WinSCP – Secure file transfer tool supporting SSH, FTP, WebDAV, and Amazon S3, used to exfiltrate data.
10. CrackMapExec – Penetration testing toolset for network exploitation.
11. Kerberoast – Tool for brute-forcing and exploiting Kerberos authentication.
12. Angry IP Scanner – Network scanner for detecting live hosts and open ports.

## Additional Links

For further information, visit the Ransomware.live website or the CISA report on the topic.

# Arrests and Law Enforcement's Reactions

2025 has been a significant year not only for cybercriminals and Advanced Persistent Threats (APTs) but also for law enforcement agencies, which have made notable strides in combating cybercrime.

## Operation Talent (30/01/2025)

The Justice Department announced its participation in a multinational operation involving actions in the United States, Romania, Australia, France, Germany, Spain, Italy, and Greece to disrupt and take down the infrastructure of the online cybercrime marketplaces known as Cracked and Nulled.

The operation was announced in conjunction with Operation Talent, a multinational law enforcement initiative supported by Europol to investigate Cracked and Nulled.

For more information, visit:

- Europol Newsroom
- Operation Talent Video

## Operation Phobos Aetor (10/02/2025)

A coordinated international law enforcement action led to the arrest of four individuals leading the 8Base ransomware group. These Russian nationals are suspected of deploying a variant of Phobos ransomware to extort high-value payments from victims across Europe and beyond. Simultaneously, 27 servers linked to the criminal network were taken down.

This operation follows a series of high-impact arrests targeting Phobos ransomware:

- An administrator of Phobos was arrested in South Korea in June 2024 and extradited to the United States in November of the same year. He is now facing prosecution for orchestrating ransomware attacks that encrypted critical infrastructure, business systems, and personal data for ransom.
- A key Phobos affiliate was arrested in Italy in 2023 on a French arrest warrant, further weakening the network behind this ransomware strain.

For more details, visit:

- Europol Newsroom

# Conclusion

In 2025, ransomware attacks have become more frequent and sophisticated, with a projected 53% year-on-year growth. This surge highlights the increasing threat to organizations, particularly in the manufacturing and technology sectors, which are the main targets due to their reliance on interconnected systems and intellectual property. However, the impact is widespread, affecting various industries and emphasizing the need for robust cybersecurity measures.

Ransomware have evolved from simple attacks to complex, organized cybercrime operations. Groups like Clop, RansomHub, and Akira are at the forefront, using advanced tactics such as encryption-less extortion and exploiting vulnerabilities to maximize their impact.
The increasingly complex geopolitical landscape further complicates the situation, as cybercriminals exploit global tensions/protections and economic incentives to their advantage.

To protect against these threats, organizations must implement strong security measures, including regular system updates, employee training to recognize phishing attempts, and comprehensive backup plans. Law enforcement efforts, such as Operation Talent and Operation Phobos Aetor, have made progress in arresting cybercriminals and shutting down their operations, but continuous effort is needed.

# Additionnal References

- Ransomwarelive:
  - Website: Ransomware.live - http://ransomware.live
  - Description: A ransomware leak site monitoring tool that aggregates data from various ransomware leak sites, tracking victim disclosures and attack trends in real time.

- Mitre & ATTACK Groups
  - Clop: https://attack.mitre.org/groups/G0095/
  - Akira: https://attack.mitre.org/groups/G0135/

- CISA Advisory
  - Clop: https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
  - Akira: https://www.cisa.gov/uscert/ncas/alerts/aa23-123a
  - RansomHub: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

- Europol Newsroom:
  - Operation Talent: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
  - Operation Phobos Aetor: https://www.europol.europa.eu/newsroom/news/operation-phobos-aetor-arrests-and-infrastructure-takedowns

- Operation Talent Video
  - https://youtu.be/OAlnBpgIEKA

- Trout:
  - Website: http://trout.software
  - Contact: hello@trout.software

Trout

**TROUT**

Trout is a leading cybersecurity company specializing in enhancing network performance and security for industrial operations and critical infrastructure. Trout designs and manufactures advanced network hardware in Europe and the USA, utilizing AI and compute optimization to efficiently implement zero-trust architectures.

Trout’s solutions facilitate the secure adoption of digital innovations, automate compliance, and strengthen operational resilience in critical environments.

For more information, visit trout.software or contact hello@trout.software.