Point Wild

Point Wild Q2 2026 Malware Trend Analysis Report

Quarterly Threat Intelligence Report | April–June 2026

PREPARED BY

Lat61 Threat Intelligence Team

RELEASE DATE

July 2026

Table of Contents

Executive Summary

During Q2 2026, the cyber threat landscape continued to evolve, with attackers increasingly shifting their focus from traditional system exploitation to identity compromise, sophisticated malware, ransomware, and software supply chain attacks. Threat actors increasingly target saved browser passwords, authentication tokens, session cookies, and personal cloud accounts to hijack trusted access to victims' online lives, email, banking, social media, and digital wallets, enabling stealthier account takeovers and more persistent fraud.

This report presents Point Wild's analysis of the evolving malware landscape, combining internal threat research, reverse engineering, detection telemetry, and publicly available threat intelligence to provide actionable insights into emerging threats. Throughout the quarter, Trojans remained the most prevalent malware category. At the same time, infostealers continued to serve as a primary initial-access vector by harvesting browser credentials, session cookies, authentication tokens, and cloud artifacts. The report also examines the evolution of prominent malware families such as XWorm and Vidar, ransomware activity, software supply chain compromises, regional threat distribution, and industry targeting trends observed during the reporting period.

By combining Point Wild's threat intelligence with real-world attack observations, this report provides organizations with actionable insights into the evolving threat landscape, helping security teams strengthen detection capabilities, improve defensive strategies, and make informed decisions to enhance overall cyber resilience.

Malware Landscape Overview

During Q2 2026, Point Wild observed a dynamic and increasingly sophisticated threat landscape affecting both consumer and enterprise environments. Analysis of malware samples and detection telemetry showed that Trojans remained the dominant malware category, accounting for 45.4% of all detections, followed by Infostealers (20.9%), Adware (11.8%), Potentially Unwanted Applications (PUA) (10.9%), Backdoors (8.4%), and Droppers (2.7%). This distribution reflects the continued shift toward attacks focused on credential theft, unauthorized access, malware delivery, and long-term persistence within compromised environments.

Figure 1. Malware categories detected and processed by Point Wild during Q2 2026

Prominent Malware Families Observed by Point Wild in Q2 2026

Remote Access Trojans (XWorm)

XWorm RAT has established itself as one of the most consistently observed RAT families heading into Q2 2026. First emerging in 2022 as a Malware-as-a-Service offering, XWorm is a modular remote access trojan capable of keylogging, credential theft, webcam access, DDoS attacks, clipboard hijacking, and ransomware deployment. It spread rapidly through phishing campaigns and the widespread circulation of cracked builds, gaining adoption among both low-skilled threat actors and advanced persistent threat (APT) groups. Point Wild observed sustained XWorm activity throughout Q2 2026. The release of XWorm V7.4 in this quarter marked a significant evolution, introducing encrypted C2 communications and an updated plugin architecture development that has continued to drive its prevalence through the first half of 2026, underscoring its status as a persistent, adaptive, and high-priority threat to monitor.

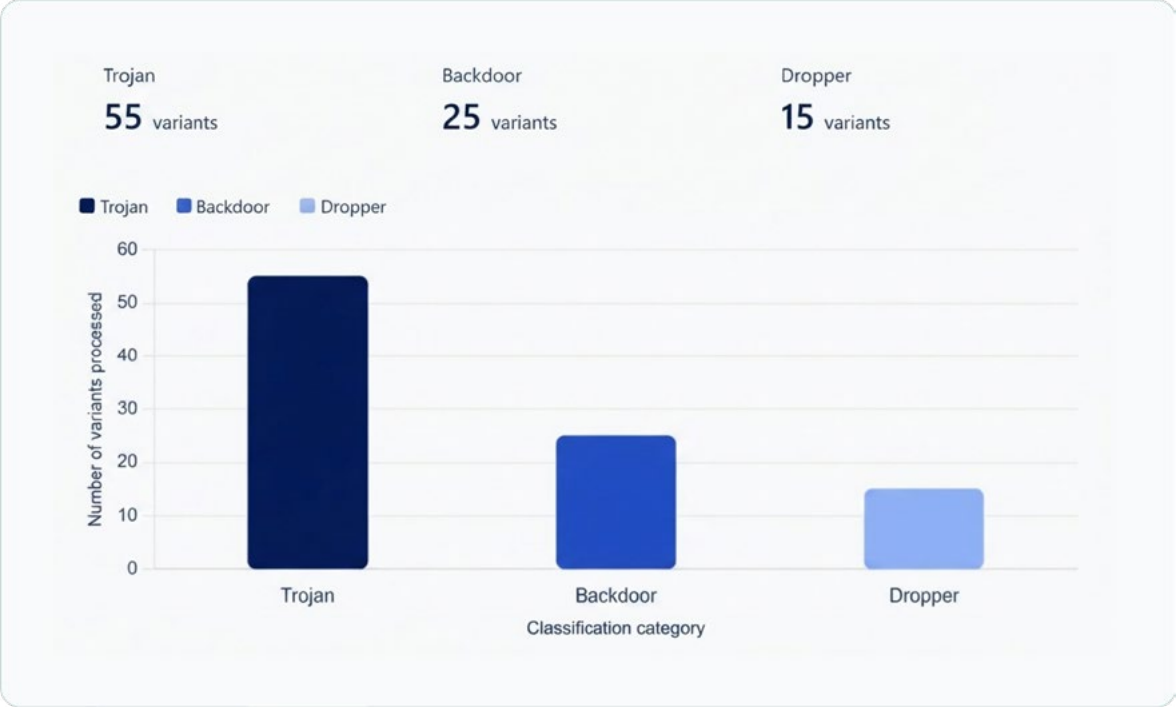

Figure 2. XWorm variants processed by Point Wild Q2 2026

Infostealers

Infostealers have become one of the most common tools used by cybercriminals to gain access to organizations in 2026. These threats are no longer limited to stealing passwords. Modern infostealers can collect session cookies, cloud account credentials, authentication tokens, and other sensitive information stored in web browsers and applications.

By stealing this data, attackers can often gain access to accounts and systems without needing a password, and in some cases, even bypass multi-factor authentication (MFA). Once inside a network, cybercriminals may use the access to steal data, commit fraud, or launch further attacks, including ransomware incidents. This makes infostealers a key threat to both individuals and organizations.

In the wild, the most prominent infostealer families in Q2 2026 are Lumma, RisePro, Vidar, StealC, RedLine, AgentTesla, and Formbook.

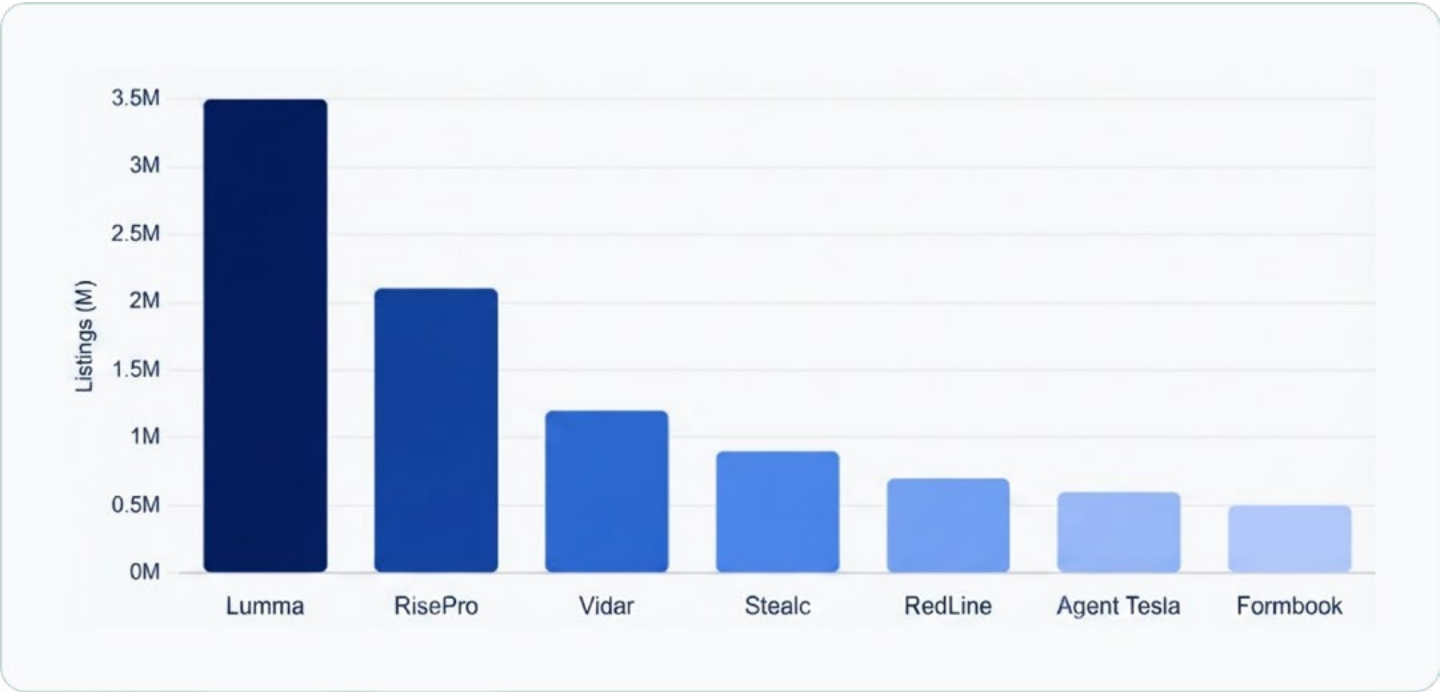

Figure 3: Top infostealer families

Vidar

Vidar remained a notable Malware-as-a-Service (MaaS) infostealer throughout 2026, continuing to target sensitive user and organizational data. The malware is designed to steal browser-stored credentials, session cookies, authentication tokens, cryptocurrency wallet information, and cloud account credentials. Recent campaigns have distributed Vidar through phishing emails, fake software downloads, malicious GitHub repositories, and other trusted platforms, highlighting the growing use of trust-based social engineering techniques.

Despite not being among the most dominant malware families observed during the period, Vidar continues to pose a significant threat due to its credential theft capabilities. Stolen credentials can provide unauthorized access to corporate networks and cloud environments, and are frequently sold to Initial Access Brokers (IABs) and ransomware operators, enabling subsequent attacks such as data breaches, business email compromise, and ransomware deployment.

During Q2 2026, Point Wild's Reverse Engineering Team documented an advanced Vidar campaign that utilized a multi-stage infection chain, trusted Windows utilities, and memory-based execution techniques to evade traditional detection mechanisms, demonstrating the malware's ongoing evolution and effectiveness.

Ransomware Trends

Ransomware remained one of the most disruptive threats in Q2 2026, with claims of attacks consistently high throughout the quarter. Qilin emerged as the most consistent and prolific group, maintaining its lead position throughout both months. Newer groups, such as The Gentlemen, rapidly scaled operations, capturing a significant share of all ransomware activity within months of launching. The USA continued to bear the heaviest global impact, while Healthcare, Manufacturing, and IT sectors remained the most frequently targeted industries.

Top 10 Ransomware Groups by Reported Victims (Q2 2026)

Publicly reported victims from April-June 2026 based on ransomware leak site tracking and industry reporting.

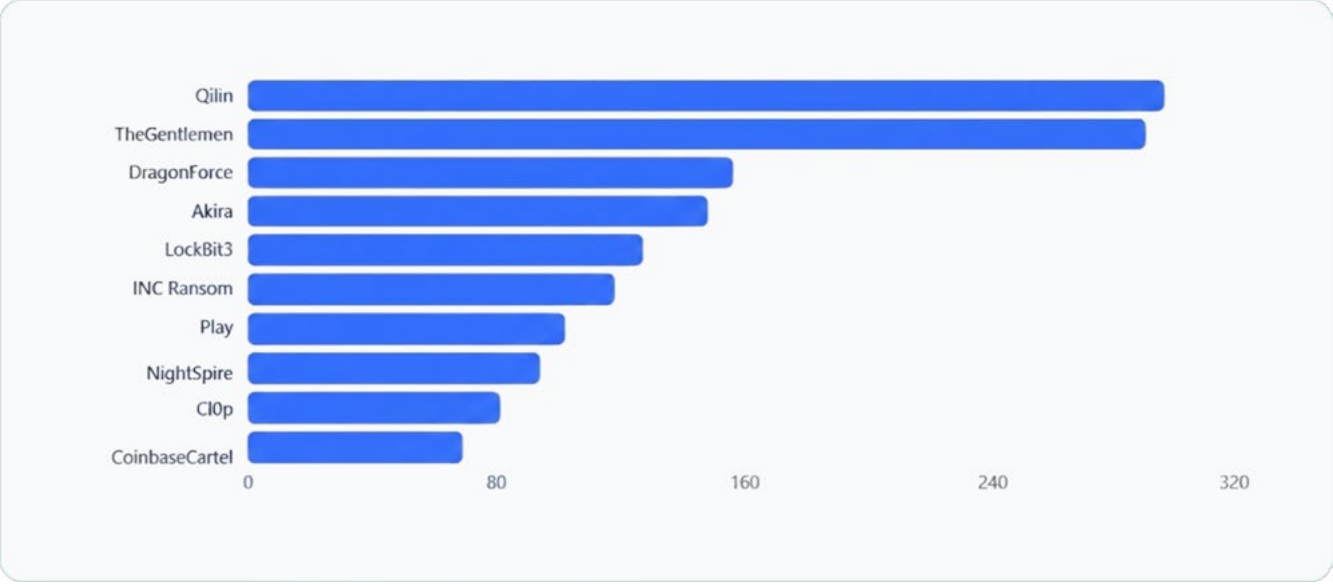

Figure 4. Ransomware groups by reported victims

Source: Publicly disclosed ransomware victim claims collected from ransomware leak sites and analyzed using Ransomfeed. Victim counts represent publicly claimed incidents and may not reflect verified compromises.

In May 2026, the Qilin ransomware group claimed responsibility for compromising Sysco, the Houston-based global food distribution company, adding the organization to its dark web leak site. As evidence of the alleged breach, Qilin published samples of purportedly stolen data, including a customer invoice and a tax-related document. According to CyberNews reports, Sysco declined to pay

the ransom demand, prompting the threat actors to release the stolen data after the payment deadline expired. The incident underscores the continued use of double-extortion tactics by ransomware groups, where data theft and public disclosure are leveraged to increase pressure on victims beyond file encryption alone.

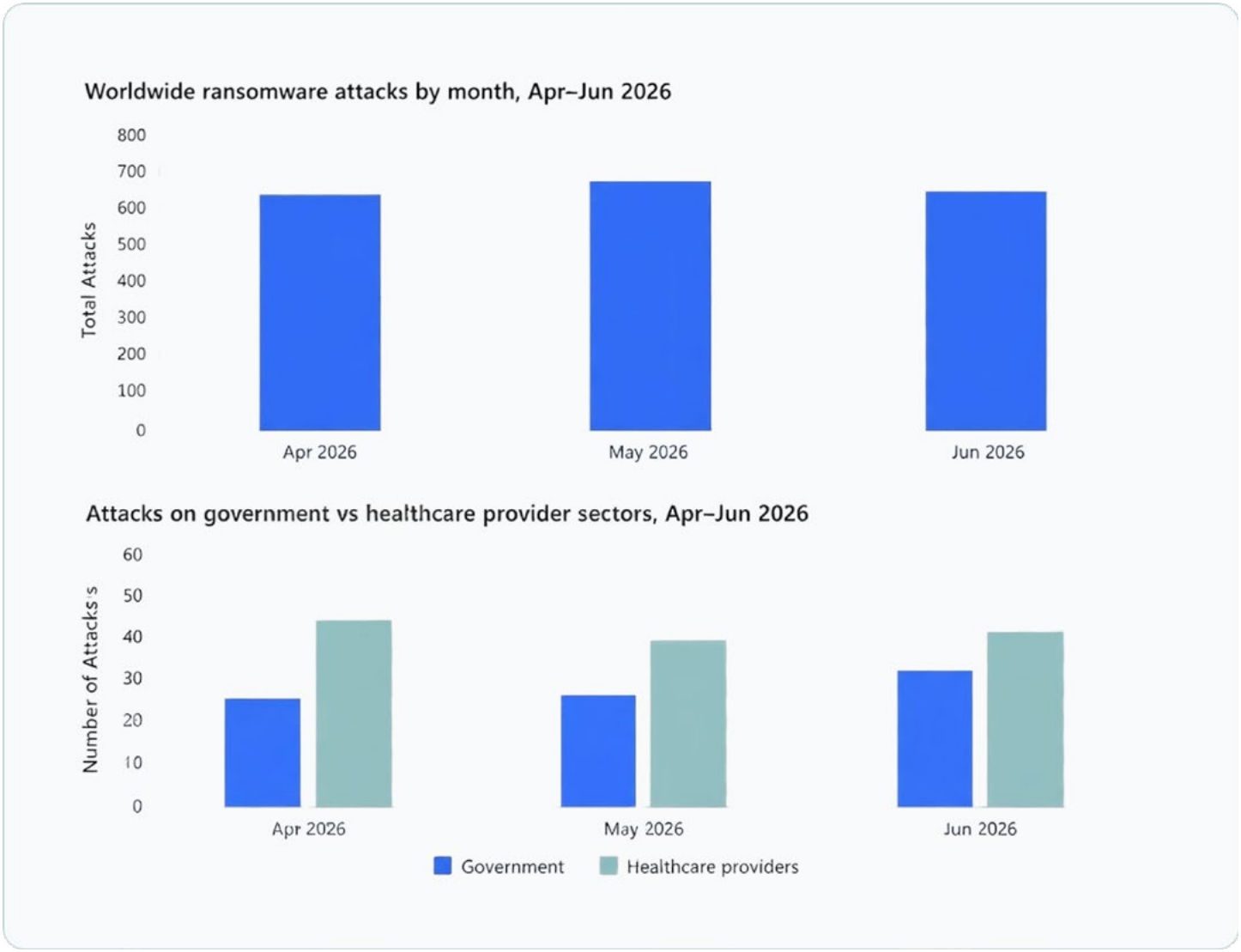

Figure 5. Global Ransomware Activity and Sector-Specific Impact (April–June 2026)

Source: Comparitech Worldwide Ransomware Tracker. Figures represent publicly reported ransomware incidents tracked by Comparitech.

Supply Chain Attacks

Software supply chain attacks continued to evolve during the reporting period, with threat actors increasingly targeting trusted software packages, developer environments, and CI/CD pipelines to compromise downstream organizations at scale. These attacks demonstrate how a single compromised dependency can expose thousands of users and enterprise environments. Point Wild's Research Team analyzed one such campaign, Shai-Hulud 2.0: The Second Coming.

Supply Chain Attack Highlights (Q2 2026)

CATEGORY	KEY OBSERVATION
Primary Target	Open-source package ecosystems (npm, GitHub, and third-party dependencies)
Primary Objective	Theft of developer credentials, cloud secrets, API keys, and CI/CD tokens
Common Initial Vector	Compromised npm packages and developer accounts
Most Affected	Software vendors, enterprise developers, and organizations relying on open-source software
Business Impact	Large-scale downstream compromise through trusted software dependencies, potentially affecting thousands of downstream users and enterprise environments

Regional Distribution of Malware Activity

During Q2 2026, North America accounted for the largest share of observed malware and ransomware activity (40%), followed by Europe (25%) and the Asia-Pacific (20%). South America (8%) and the Middle East & Africa (7%) represented smaller proportions of reported activity. This regional distribution reflects trends observed from publicly reported cyber incidents, ransomware disclosures, threat intelligence reporting, and Point Wild's internal malware research. The concentration of activity in North America, Europe, and APAC highlights the continued targeting of economically significant regions by both cybercriminal groups and nation-state actors, reinforcing the need for continuous monitoring and proactive threat detection.

Malware Impacted Region Q2 2026

Distribution of Malware and Ransomware Attacks by Region Based on Threat Intelligence Telemetry

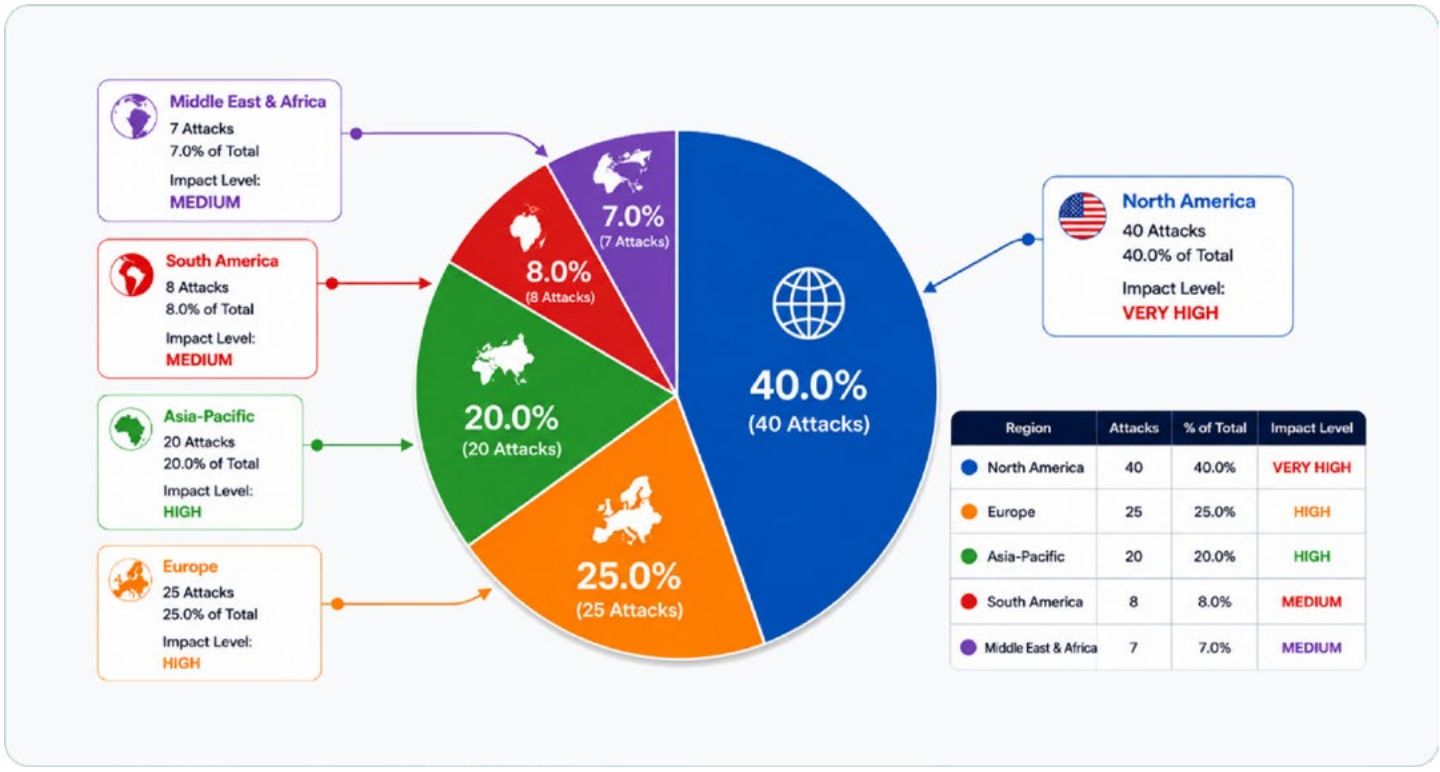

Figure 6. Malware Impacted Region

Source: Regional distribution is derived from publicly available ransomware disclosures, malware campaign reports, and threat intelligence publications for Q2 2026. Figures represent observed incidents during the reporting period.

Industry Impact Analysis

Analysis of publicly available threat intelligence reports and disclosures for Q2 2026 shows that Business Services, Manufacturing, and Healthcare were the most targeted industries, collectively accounting for nearly three-quarters of reported incidents. Financial Services, Power & Energy, and Government also remained key targets, reflecting adversaries' continued interest in sectors where operational disruption and financial impact are highest.

Malware Activity by Industry Q2 2026

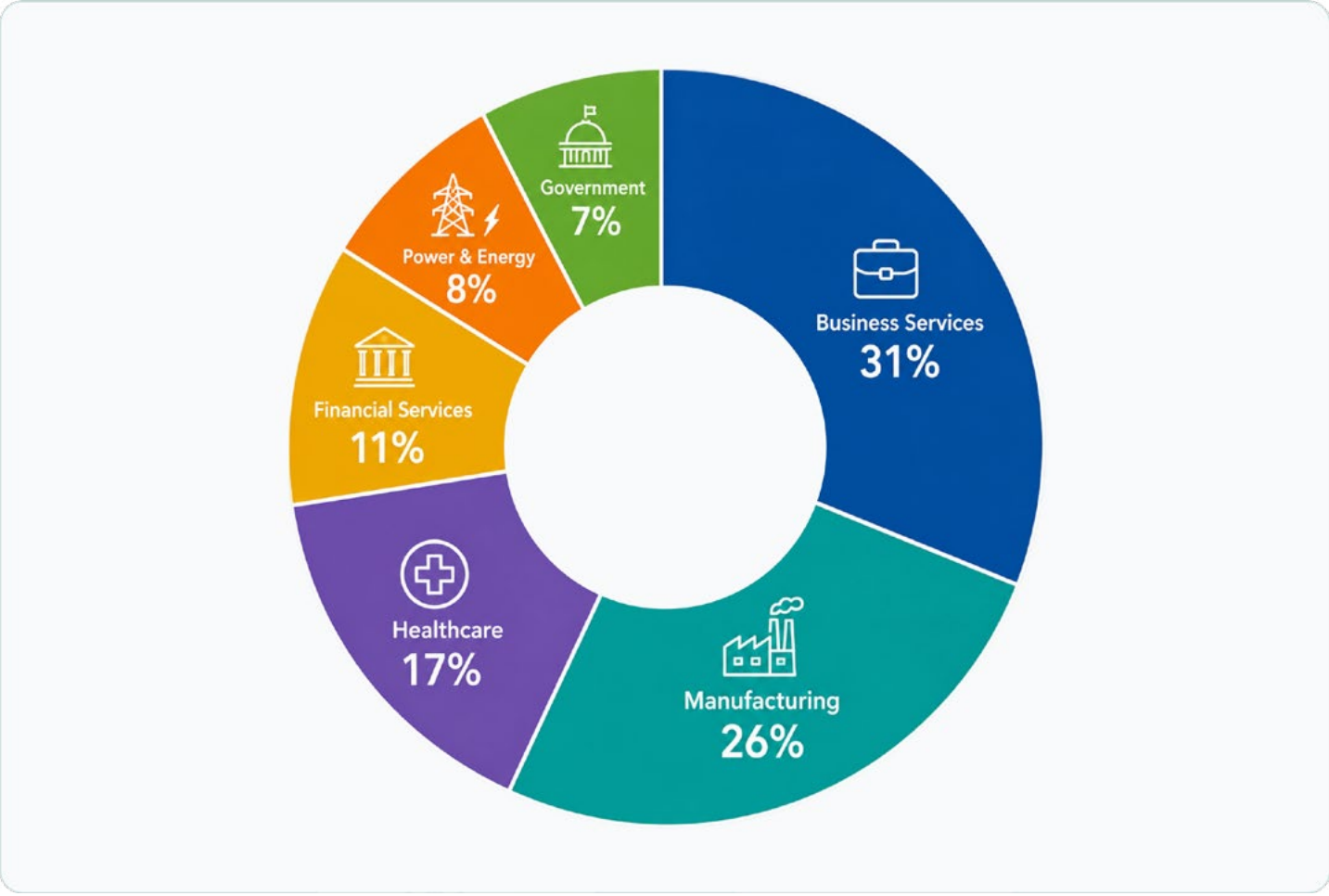

Figure 7. Malware activity by industry

Source: Industry distribution is based on publicly reported ransomware victim disclosures and threat intelligence publications aggregated for Q2 2026. The data represent observed incidents and may not include all global cyber events.

Key Findings

- The Q2 2026 threat landscape continued to shift toward identity-centric attacks, with cybercriminals increasingly targeting credentials, authentication tokens, and cloud identities to gain unauthorized access.
- Trojans (45.4%) remained the most prevalent malware category, followed by Infostealers (20.9%).
- Infostealers, including Lumma, RisePro, Vidar, StealC, RedLine, AgentTesla, and FormBook, remained the leading initial-access vector for compromise.
- Ransomware operators increasingly leveraged stolen credentials and exploited software vulnerabilities to gain initial access.
- Supply chain attacks targeted open-source packages, developer credentials, and CI/CD pipelines, increasing downstream risk.
- North America remained the most targeted region, while Business Services, Manufacturing, and Healthcare experienced the highest levels of malware activity.
- Threat actors increasingly abuse trusted applications and legitimate system tools to evade traditional security controls.

Conclusion

The evolving threat landscape underscores the need for organizations to move beyond traditional, signature-based security approaches. The increasing abuse of developer credentials, trusted software, and legitimate system utilities continues to expand attack surface. To improve cyber resilience, organizations should adopt an intelligence-driven security strategy that prioritizes identity protection, endpoint visibility, software supply chain security, continuous threat monitoring, and rapid incident response. The report also provides practical recommendations to help organizations strengthen their defenses against emerging malware threats.

Methodology

This report analyzes malware and cyber threat activity observed during Q2 2026 using a combination of Point Wild's internal malware research, reverse engineering, detection telemetry, and publicly available threat intelligence sources. Ransomware statistics were derived from publicly disclosed victim claims tracked through ransomware leak sites and industry reporting. Regional and industry impact analysis was based on publicly reported cyber incidents, ransomware disclosures, and threat intelligence publications. The findings presented reflect observed trends during the reporting period and may not represent all cyber incidents globally.

References

Ransomfeed

https://www.cyfirma.com/research/tracking-ransomware-apr-2026/

https://www.fortinet.com/resources/reports/threat-landscape-report

https://www.ibm.com/reports/threat-intelligence

X-Force Threat Intelligence Index 2026 | IBM

https://www.trendmicro.com/en_us/research.html

Ransomware Roundup: H1 2026 stats on attacks, ransoms, and active gangs - Comparitech

ShinyHunters claims 61M Sysco records | Cybernews

The Vercel Breach: OAuth Supply Chain Attack Exposes the Hidden Risk in Platform Environment Variables | Trend Micro (US)