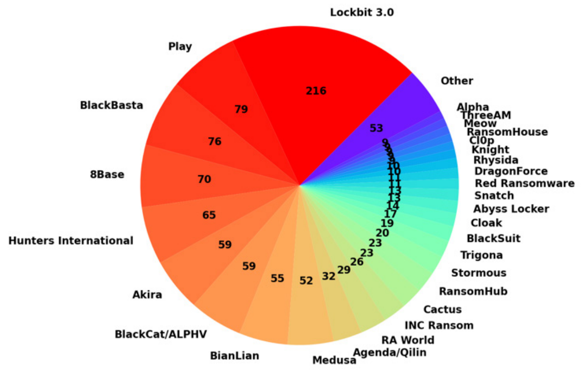
KEY PLAYERS IN RANSOMWARE-AS-A-SERVICE

Q1 2024

RaaS Operations with the Most Global Victims

Announced via Leak Site in Q1 2024

Distribution of Global Victims by Ransomware Group with Victim Counts



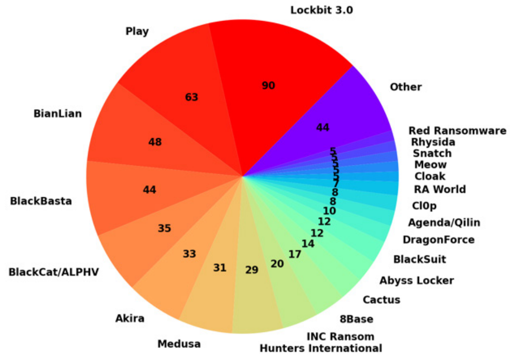
1. Lockbit 3.0
2. Play
3. BlackBasta
4. 8Base
5. Hunters International
6. Akira
7. BlackCat/ALPHV
8. BianLian
9. Medusa
10. Agenda/Qilin

RaaS Operations with the Most American Victims

Announced via Leak Site in Q1 2024

1. Lockbit 3.0
2. Play
3. BianLian
4. BlackBasta
5. BlackCat/ALPHV
6. Akira
7. Medusa
8. Hunters International
9. INC Ransom
10. 8Base

Distribution of Victims in the USA by Ransomware Group with Victim Counts



LOCKBIT 3.0

Ransomware-as-a-Service Operator

AKA

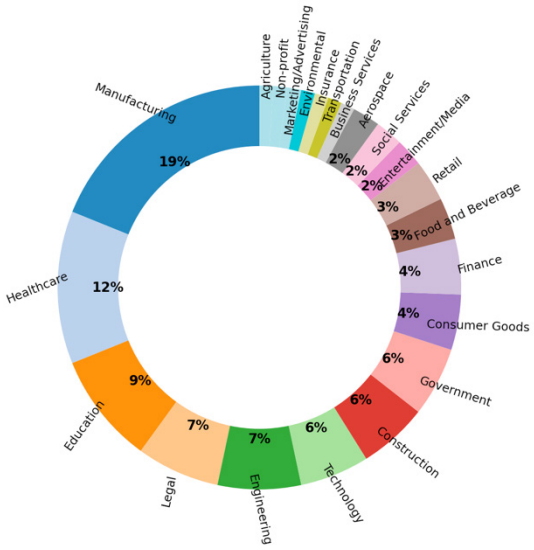
- Gold Mystic
- Water Selkie
- Bitwise Spider
- ABCD Ransomware

History

First appearing in 2019, this popular, innovative and business-savvy RaaS group would be designated an unparalleled, cyber criminal threat by international law enforcement less than five years later. In early 2024, a global law enforcement action, Operation Cronus, led to the seizure of the group's infrastructure, the arrest of two of its affiliates, and U.S. indictments and sanctions for two Russian nationals alleged to be members of the group. In the aftermath of Cronus, despite reportedly recycling older victims on their leak site, the group appears to have rebounded, and is continuing the Lockbit brand and operation for now.

In the wake of the 2022 shutdown of Conti's RaaS, Lockbit became the ransomware service with the most victims (in the U.S. and elsewhere) that same year. They've maintained supremacy in quarterly counts of victims since that time.

Innovations of this RaaS include their affiliate payment system, Stealbit, a bespoke exfiltration tool developed for Lockbit 2.0, a bug bounty program to encourage improvement of their ransomware, tattoo-based and other marketing ploys, among others.



Lockbit US Victims' Q1 2024 Industry Verticals

Attack Vectors (Initial Access)

- Phishing
- Remote Desktop Protocol Brute Force
- Drive-by Compromise
- Valid Accounts
- External Remote Services
  - Remote Desktop Protocol Brute Force
  - Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)
  - Citrix Bleed Vulnerability (CVE 2023-4966)
  - ConnectWise ScreenConnect Vulnerability (CVE-2024-1709)
  - F5 iControl REST unauthenticated Remote Code Execution Vulnerability (CVE-2021-22986)

- Exploit Public-Facing Application
  - F5 iControl REST unauthenticated Remote Code Execution Vulnerability (CVE-2021-22986)
  - Fortra GoAnyhwere Managed File Transfer (MFT) Remote Code Execution Vulnerability (CVE-2023-0669)
  - PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350)
  - Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228)
  - F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability (CVE-2021-22986)
  - Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability (CVE-2018-13379)

Tools

- AnyDesk
- Atera Remote Monitoring & Management (RMM)
- Bloodhound
- Choclately
- Defender Control
- ExtPassword
- FileZilla
- FreeFileSync
- Impacket
- LaZagne
- Ligolo
- LostMyPassword
- MEGA Ltd MegaSync
- Microsoft Sysinternals ProcDump
- Microsoft Sysinternals PsExec
- Mimikatz
- Ngrok
- PasswordFox
- PCHunter
- PowerTool
- Rclone
- Seatbelt
- ScreenConnect
- Splashtop
- TDSSKiller
- TeamViewer
- ThunderShell
- WinSCP

Noteworthy Incidents

- 2023 Boeing Breach
- 2023 Industrial and Commercial Bank of China Breach
- 2024 Fulton County, Georgia Breach

PLAY

Ransomware-as-a-Service Operator

AKA

- Recess Spider
- PlayCrypt

History

Play RaaS emerged around mid-2022 and quickly became known for its aggressive attack tactics and rapid proliferation. The group behind Play RaaS has been active in continuously updating the ransomware's capabilities and targeting various sectors worldwide, focusing on maximizing revenue through extortion.

Attack Vectors (Initial Access)

- Phishing
- Exploit of Public-Facing Applications
- Credential Stuffing
- Supply Chain Attacks

Tools

- AdFind
- BloodHound
- GMER
- IOBit Software
- PowerShell
- Cobalt Strike
- Mimikatz
- WinPEAS
- WinRAR and WinSCP

Noteworthy Incidents

- **Attack on the City of Oakland**
  In one of the more publicized incidents, the City of Oakland in California was a victim of Play ransomware. This attack caused significant disruptions to the city's services, including systems related to payments and communications (BleepingComputer).
- **Infiltration of Globant**
  Globant, a prominent software development firm, experienced a significant breach attributed to Play ransomware. This incident highlighted the ransomware's capability to exploit vulnerabilities in corporate networks, particularly leveraging critical flaws in Microsoft Exchange known as ProxyNotShell for initial access (Avertium).

BIANLIAN

Independent Ransomware and Data Extortion Group

AKA

- Masked Spider

History

BianLian initially appeared as a banking Trojan around 2018, primarily targeting Android devices. However, it has evolved significantly since its inception. Around mid-2022, BianLian transitioned into a fully-fledged ransomware operation, shifting its targeting focus towards enterprises across various sectors globally. The group behind BianLian is known for its rapid development cycle and adaptation of new techniques, which suggests a high level of technical expertise.

Attack Vectors (Initial Access)

- Phishing
- Exploit of Public-Facing Applications
- Credential Stuffing
- Supply Chain Attacks

Tools

- Custom Exfiltration Tools
- FTP and SFTP Protocols
- Rclone

Noteworthy Incidents

- **Exploitation of JetBrains TeamCity:**
  BianLian actors were observed exploiting vulnerabilities in JetBrains TeamCity, a continuous integration/continuous deployment server. This allowed them to gain initial access to victim networks, particularly targeting the software development industry. The utilization of such a specific tool underscores the group's sophisticated approach to selecting and exploiting enterprise software vulnerabilities that provide broad network access **(**Security Affairs).
- **Targeting Critical Infrastructure:**
  The group has significantly impacted critical infrastructure sectors in the U.S. and Australia. This includes a range of industries from healthcare and manufacturing to professional services. BianLian's tactics involve not just data encryption but also data exfiltration, shifting towards a model that emphasizes extortion by threatening to leak stolen data unless a ransom is paid. This shift reflects a broader trend among ransomware groups adapting to more resilient network defenses against file encryption (CISA) (SecurityWeek)

BLACKBASTA

Ransomware-as-a-Service Operator

AKA

- Storm-0506

History

Black Basta ransomware, identified as a significant cyber threat since its emergence in April 2022, employs a range of tools and techniques that underline its sophistication and targeted approach. The group quickly gained attention due to its aggressive tactics and the rapid proliferation of its attacks.

Tools

- QakBot Trojan
- Mimikatz
- Cobalt Strike
- PowerShell and Windows Management Instrumentation (WMI)
- NetSupport Manager and Other Remote Access Tools

Noteworthy Incidents

- **American Dental Association (ADA) Cyberattack:**
  Shortly after Black Basta was first observed in April 2022, it targeted the American Dental Association, causing substantial disruptions. The group compromised ADA's systems and published stolen data on their leak site just 96 hours following the attack. This incident highlighted the group's rapid operational capabilities and their use of double-extortion tactics (Trend Micro) (Trend Micro).
- **Widespread Corporate Network Compromises:**
  Black Basta has been active in seeking network access credentials through underground forums, aiming to infiltrate corporate networks primarily in English-speaking countries. This approach underscores their strategy to target and monetize access to high-value networks, which was evident when they advertised on forums like XSS.IS and EXPLOIT.IN (Trend Micro) (Trend Micro).
- **Use of Sophisticated TTPs (Tactics, Techniques, and Procedures):**
  The group employs advanced methods like DNS over HTTPS (DoH) to conceal their command and control communications, making their activities harder to detect and mitigate. Such tactics demonstrate Black Basta's sophisticated operational approach and their continuous adaptation to enhance stealth and efficacy of their attacks (Trend Micro).

BLACKCAT

AKA

- ALPHV
- Alpha Spider

History

BlackCat/ALPHV is a sophisticated ransomware variant that first appeared in mid-November 2021. It quickly became notorious for its use of the Rust programming language, making it the first major ransomware family to do so. This choice of programming language allows for enhanced performance and security features, which makes BlackCat particularly effective across different operating systems, including Windows and Linux.

The ransomware is known for its triple extortion technique, which not only involves encrypting and stealing data but also threatening to launch Distributed Denial-of-Service (DDoS) attacks if ransoms are not paid. This makes BlackCat particularly aggressive compared to other ransomware gangs.

BlackCat's method of attack typically involves gaining initial access through compromised credentials, followed by lateral movement within the network to escalate privileges and deploy the ransomware payload. This process often involves disabling security features to avoid detection and maximize the impact of the attack.

Attack Vectors (Initial Access)

- Compromised Credentials
- Exploit of Public-Facing Applications
- Spear Phishing
- Deployment via Malware

Tools

- Powershell
- Cobalt Strike
- MEGAsync
- GOST (GO Simple Tunnel
- Mimikatz
- LaZagne

Noteworthy Incidents

- **Change Healthcare:**
  Blackcat disrupted Change Healthcare's systems leading to significant prescription processing outages across the United States. The incident, which unfolded in February 2024, involved the theft of 6 terabytes of sensitive data including health records, payment information, and personal identifiable information. (Krebs on Security) (SecurityWeek) (BleepingComputer).

8BASE

History

The 8Base ransomware group emerged in 2023 with their adoption of DLS (Data/Dedicated Leak Site) but their operation can be traced to smaller campaigns in 2022. Initially this group reportedly targeted United States and Brazilian entities exclusively, but their targeting has since expanded to encompass organizations across a broad array of nations. In the first quarter of 2024, this group claimed victims in 18 countries.

Attack Vectors (Initial Access)

- Phishing emails
- Initial Access Brokers (IAB)
- Exploit kits
- Drive-by downloads

Tools

- 8Base Ransomware (Phobos ransomware variant)
- SystemBC
- Exploit kits

Noteworthy Incidents

- 2023 ToyotaLift Northeast Breach

NEW AND EMERGING RANSOMWARE GROUPS (Q1 2024)

RANSOMHUB

This is a new ransomware group that emerged in the first quarter of 2024, when it was noticed after claiming responsibility for an attack on Change Healthcare, where it reportedly obtained 4 TB of highly sensitive data**.** This data breach was initially attributed to an affiliate of the ALPHV/BlackCat ransomware group, but due to a subsequent fallout over ransom payments, RansomHub emerged claiming possession of the stolen data.

This group operates a ransomware-as-a-service (RaaS) model. Despite being new, the group has demonstrated a sophisticated operational capacity, targeting significant entities and managing the stolen data effectively to pressure victims into meeting their demands.

Given its aggressive entry into the ransomware arena and the potential affiliations with former members of other notorious groups, RansomHub is considered a significant threat in the cybersecurity landscape.

TRISEC

Trisec is a new ransomware group that emerged in early 2024, gaining immediate attention with its first attack on an Irish Toyota dealership. The group has positioned itself ambiguously, blending financially motivated attacks with claims of state-sponsored activities, which is unusual for cybercriminal groups that typically prefer to keep such affiliations hidden. Their operations and tactics suggest a high level of confidence and strategic planning, setting longer-than-usual deadlines for ransom negotiations, indicative of their robust operational capabilities.

Trisec's public persona includes references that hint at a possible Tunisian connection, though this could be a deliberate misdirection to confuse law enforcement and cybersecurity researchers. The group's approach includes a mixture of clearnet and darknet activities, and they have shown a tendency to use their own leak sites for communication and threats, typical of ransomware groups aiming to establish a reputation and instill fear among potential targets.

Despite their recent arrival on the cybercrime scene, Trisec has demonstrated a concerning level of proficiency and boldness in their operations. The lack of extensive background information on them and their rapid rise to notice suggests that they could either be a rebranded older group or a new entity formed by experienced cybercriminals from various backgrounds.

SLUG

Slug is a newly emerged ransomware group that first came into the public eye in January 2024 following its attack on AerCap, a major global aircraft leasing firm. The group claimed to have stolen 1TB of data from AerCap, marking this incident as their initial public target. Despite the serious nature of this breach, there was no evidence that Slug had taken control of AerCap's IT systems, and AerCap had moved quickly to involve law enforcement and start an investigation into the extent of the data breach.

Slug has been somewhat enigmatic, with very little information available on its members or its origins. As of the latest reports, Slug's dark web portal remained sparse, offering no further details about the group or its other potential activities. This lack of information could suggest that Slug is either very new to the ransomware scene or is operating with a high level of secrecy, potentially to gauge the response to their initial public activities before escalating their operations.

MYDATA / ALPHA LOCKER

Alpha Locker, also known as MyData or Alpha, is a ransomware group that emerged in the cybersecurity landscape around May 2023. They are notable for their use of a data leak site hosted on a TOR domain, which they use to publish the data of their victims as part of their extortion strategy.

Despite their emerging status, Alpha Locker has been relatively active since their appearance, with a particular focus on tailoring their ransom notes and approach to enhance the effectiveness of their extortion efforts. Their ransomware has been observed affecting a wide range of industry sectors across different countries, underscoring the broad threat they pose.

DONEX

DoNex is a recently identified ransomware strain that has been targeting enterprises across the United States and Europe since its emergence in March 2024. This ransomware group is known for its double-extortion tactic

The group communicates with its victims through Tox messenger, a secure and anonymous peer-to-peer instant messaging service, to negotiate ransom payments. DoNex ransomware employs sophisticated encryption techniques, appending the victim's ID as an extension to all encrypted files, which renders the files inaccessible without the decryption key.

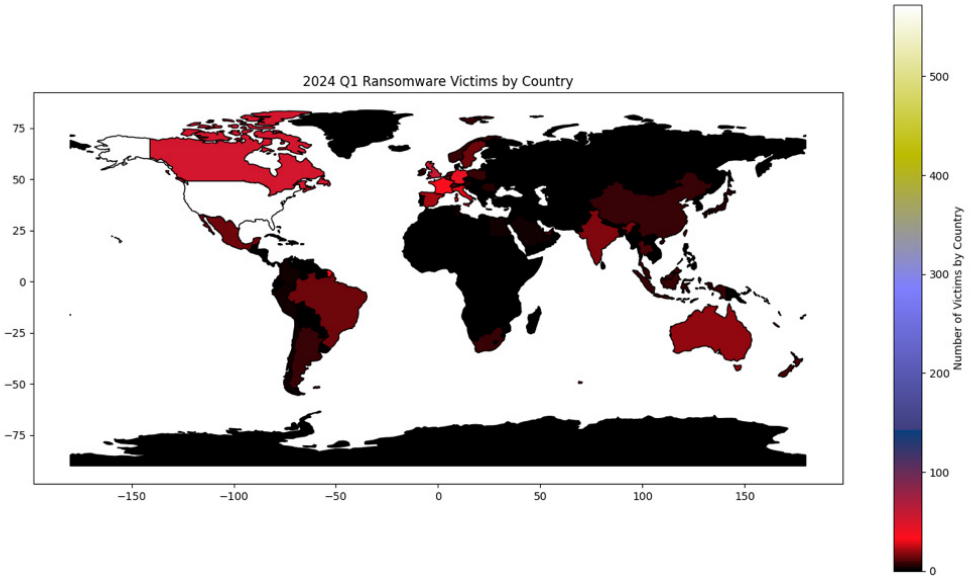
INSANE

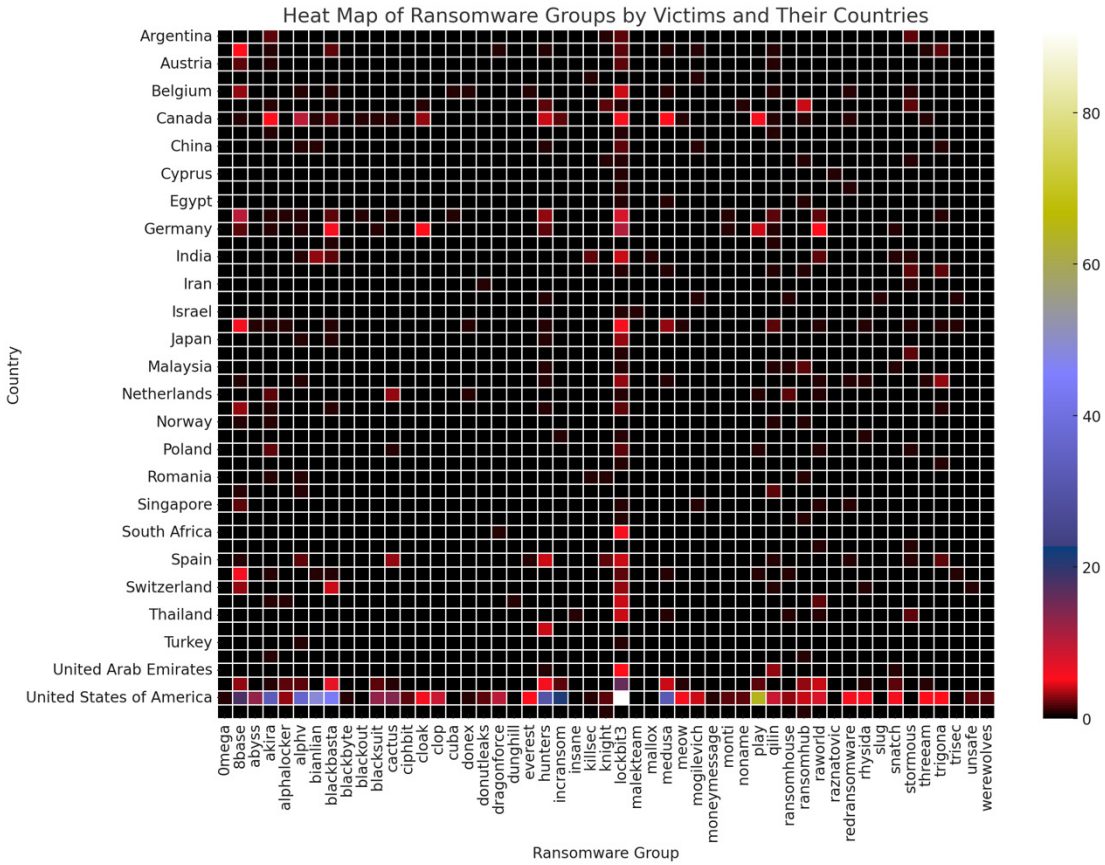
Insane Ransomware, also known as "Going Insane," made a brief appearance in the ransomware scene in January 2024. Originating from Thailand, it claimed a single victim before fading from active visibility. This group has been cryptic about its operations, primarily leaving some information on its data leak site. They assert the use of AES encryption and claim capabilities for information-stealing through their malware.

The lack of extensive activity or multiple reported incidents makes Insane Ransomware somewhat enigmatic in the cybercrime landscape. Their approach and sudden disappearance could suggest testing or a demonstration of capabilities rather than an ongoing campaign.

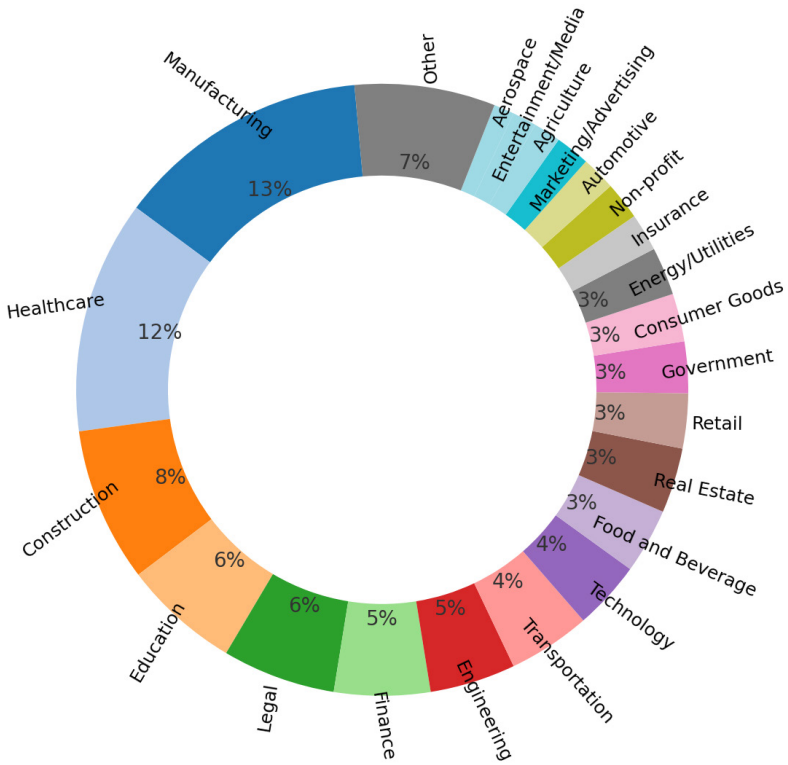
Primary Source:
Mousqueton J. (2022, April). Ransomware.live. https://www.ransomware.live/

Additional Content
Ransomware Groups' Geographic Targeting





Q1 2024 Industry Verticals of Victims in the United States



Industry Vertical	Victim Count
Manufacturing	74
Healthcare	68
Construction	45
Education	34
Legal	33
Finance	28
Engineering	25
Transportation	24
Technology	20
Real Estate	19
Food and Beverage	19
Retail	16
Government	15
Consumer Goods	14
Energy/Utilities	14
Insurance	11
Non-profit	11
Automotive	10
Marketing/Advertising	10
Agriculture	8
Entertainment/Media	7
Aerospace	6
Social Services	5
Business Services	5
Consulting	4
Electronics	4
Telecommunications	4
Hospitality/Leisure	3
Environmental	3
Travel and Tourism	2
Defense	2
Industrial Supplies	2
Financial Services	2

Lockbit Additional Research

Lockbit 3.0's Industry Victims, Pre- and Post- Cronus

Using the date of Operation Cronus as a marker to compare Q1 2024 victims by industry verticals, before and after this date

- **Increased Attacks:**
  - **Healthcare** saw an increase of 3 attacks.
  - **Consumer Goods** increased by 2 attacks.
  - **Transportation, Technology, Insurance,** and **Business Services** each saw a modest increase of 1 attack.
- **Decreased Attacks:**
  - **Manufacturing, Government,** and **Construction** each saw a significant decrease, with 5 fewer attacks after February 20.
  - **Legal** and **Education** decreased by 4 attacks each.
  - Several other industries like **Entertainment/Media, Retail,** and F**ood and Beverage** saw minor decreases.