ANOMALI

U.S. RANSOMWARE INDUSTRY TARGETING REPORT

DECISION-MAKER INDUSTRY TARGETING VIEW

REPORT RELEASE DATE: SEPTEMBER 2026

SCOPE AND METHODOLOGY

This report summarizes observed ransomware targeting across US industries based on ransomware entity-to-industry mappings. The dataset measures observed targeting presence only; it does not represent confirmed compromise, attack frequency, victim count, operational impact, severity, or real-world dangerousness.

The dataset comprises 200 distinct ransomware entities across 8 analyzed industries. The term ransomware entities is used throughout as a neutral umbrella term for organized operations, malware families, and named activity clusters tracked through the same targeting model.

Country/location entries are country- or territory-level values from the source location field, not different sites within the United States. U.S. industry targeting is the primary analysis; country/location breadth is context for the same ransomware entities and helps identify broad observed footprint, not confirmed incident volume, victim count, or severity. Appendix A, located at the end of the report, contains the full ransomware-by-industry targeting matrix for all 200 entities across the 8 analyzed US industries and is positioned there to preserve the readability of the main analysis.

EXECUTIVE SUMMARY

Observed ransomware targeting pressure across the United States is broad, consistent, and not bounded by industry sector. All eight analyzed industries exceed 50% targeting presence. Technology leads at 86%, followed by Manufacturing at 83% and Healthcare at 77%. The decision-relevant signal for security leaders is not whether a given sector is in scope, it is the relative pressure each sector faces and which entities are driving the widest exposure.

The dataset reveals a clear pattern: entities with the broadest geographic footprint also carry the broadest industry targeting. Of the 26 most geographically active entities, all target every analyzed US industry. This reflects the affiliate-driven ransomware-as-a-service model, where operators such as Qilin, LockBit3, RansomHub, and Akira combine global reach with cross-sector targeting, collapsing the distance between initial access and full extortion pressure.

Sector-specific framing understates the exposure. The entities generating the largest observed footprint in this dataset operate without industry boundaries, and the continued growth of double extortion means disruption and data theft now arrive together. Security leaders should treat identity hardening, internet-facing exposure reduction, and ransomware-resilient recovery as the non-negotiable baseline for 2026.

DECISION - MAKER ANSWER

86%

HIGHEST INDUSTRY PRESSURE

Technology leads the U.S. dataset with 172/200 ransomware entities showing observed targeting presence.

99

BROADEST ENTITY FOOTPRINT

Qilin has the highest observed country/location breadth and targets 8/8 analyzed U.S. industries.

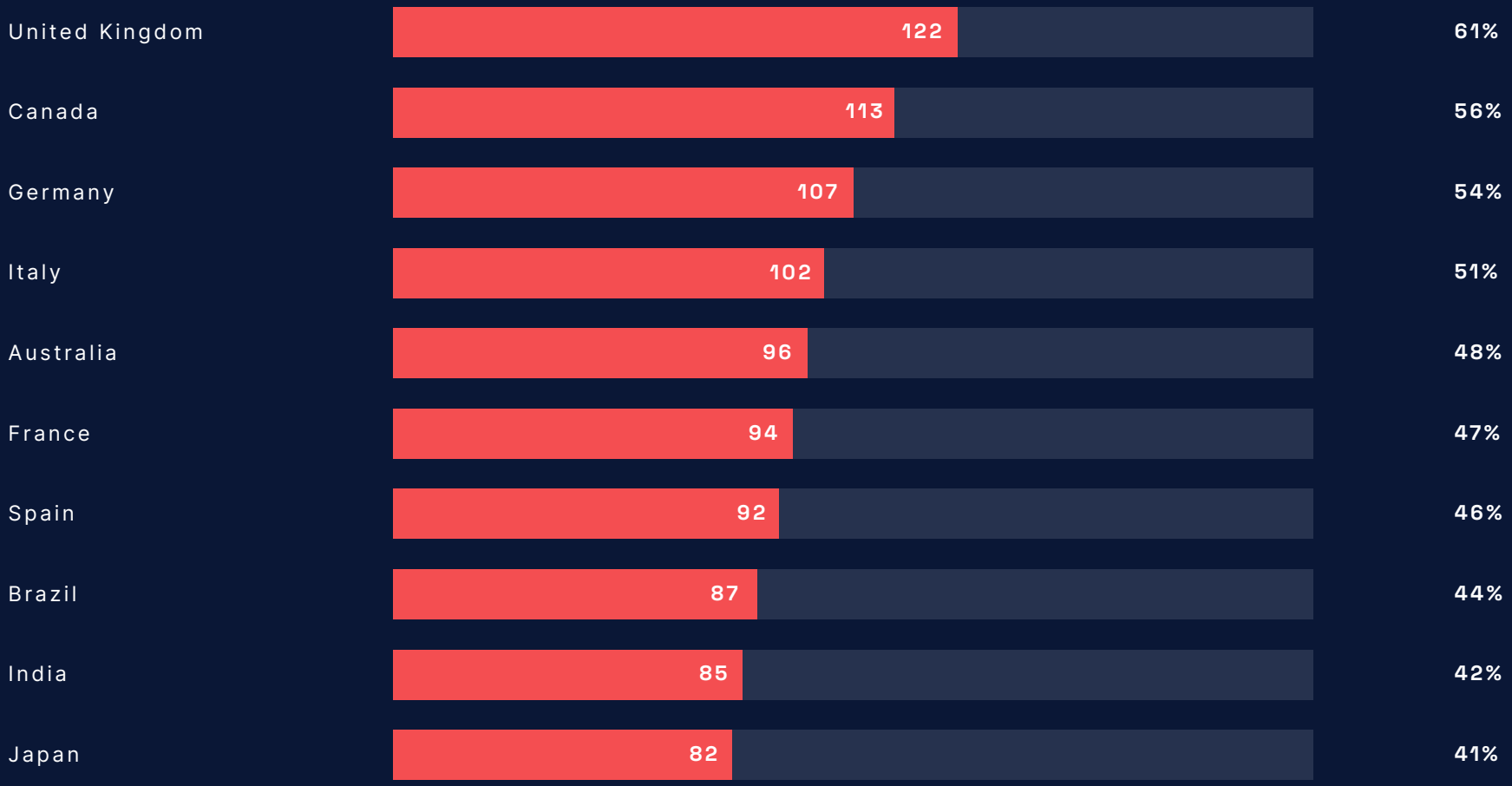
INDUSTRY TARGETING PRESSURE

There is no safe sector in this dataset: all eight analyzed U.S industries exceed 50% observed targeting presence. Technology is the clearest pressure signal at 86%, leading all sectors and reinforcing that digitally central industries face especially broad ransomware attention. The ranking below is best read as a measure of relative exposure, not sector inclusion versus exclusion.

GEOGRAPHIC CONTEXT

Of the 200 ransomware entities in the U.S. industry report set, 189 also list at least one non-U.S. country/location entry. The most common co-targeted locations are major allied and global economies, including the United Kingdom, Canada, Germany, Italy, Australia, France, Spain, Brazil, India, and Japan.

The co-targeting bars show that many of the same ransomware entities targeting U.S. industries also operate across other major allied and global economies. For decision-makers, this makes cross-border ransomware activity directly relevant to U.S. defensive planning.



HIGHEST-BREADTH U.S.-TARGETING RANSOMWARE ENTITIES

Because 70 of the 200 entities in the U.S. dataset already target all 8 analyzed industries, U.S. industry scope alone does not sufficiently distinguish the broadest operators. Country/location breadth adds a second axis that helps separate these full-scope entities by a wider observed footprint. What emerges is a practical priority watchlist of generalized ransomware operations that align with the broader threat landscape, including large-scale affiliate and double-extortion or multiple-extortion models, making them relevant to U.S. defenders regardless of industry.

RANK	ENTITY	OBSERVED COUNTRY/ LOCATIONENTRIES	U.S. INDUSTRY SCOPE
1	Qilin	99	8/8
2	Lockbit3	96	8/8
3	Thegentlemen	75	8/8
4	Ransomhub	73	8/8
5	Akira	71	8/8
6	Incransom	69	8/8
7	Lockbit5	63	8/8
8	Alphv	59	8/8
9	Dragonforce	59	8/8
10	Funksec	59	7/8 (Missing Construction)

Country/location entries are country- or territory-level source values, not different locations within the U.S.

Qilin's combined 99 country/location entries and 8/8 U.S. industry scope is the clearest data-derived signal of generalized ransomware targeting breadth in this dataset.

CROSS-AXIS EXPOSURE: GEOGRAPHY BREADTH VS INDUSTRY BREADTH

The broadest ransomware entities in this dataset are also the broadest across U.S. industries. As country/location reach increases, industry targeting widens with it. In practice, the broadest operators look less like sector-specific threats and more like generalized threats to U.S. organizations.

73

BROAD + GLOBALIZED

This is the widest-footprint subset in the report: U.S.-targeting entities with 16 or more country/location entries.

66

7+ INDUSTRIES

Most broad/globalized entities also target 7 or more U.S. industries, showing that wider geography usually coincides with wider industry scope.

52

BROADEST ENTITY FOOTPRINT

This is the strongest cross-sector signal: broad/globalized entities targeting every one of the 8 analyzed U.S. industries.

14

SINGLE-INDUSTRY ENTITIES

14 single-industry entities target exactly one U.S. industry. Of these, 4 are United States-only, 9 are narrow geography, and 1 is moderate geography. This shows sector-specific targeting exists, but mostly outside the broad/globalized population.

Band definitions: U.S.-only = 1 country/location entry; narrow = 2-5; moderate = 6-15; broad = 16-40; globalized = 41+.

COUNTRY/LOCATION BREADTH ENTITIES BAND		TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	AVR INDUSTRY
US-only	11	55%	64%	45%	55%	36%	27%	18%	18%	3.2
Narrow geography	49	63%	53%	47%	47%	47%	37%	31%	22%	3.5
Moderate geography	67	94%	91%	81%	76%	54%	64%	52%	54%	5.7
Broad geography	47	98%	98%	98%	96%	89%	83%	87%	91%	7.4
Globalized geography	26	100%	100%	100%	100%	100%	96%	96%	100%	7.9

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services |GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

DECISION-MAKER SIGNAL

Within the 26 globalized entities, each target Technology, Manufacturing, Healthcare, Financial Services, Government Public Services, and Energy, while 25 of 26 also target Construction and Education. The operational takeaway is that the broadest geographic entities in this dataset function as generalized ransomware operators whose relevance extends across nearly the full U.S. industry set.

CROSS-AXIS EXPOSURE: GEOGRAPHY BREADTH VS INDUSTRY BREADTH

The United States-only population is included as a contrast group because it is small and materially narrower than the multi-country/location population. It strengthens the main finding: narrow observed scope exists, but the dominant pattern in this report is cross-country/location, cross-sector targeting breadth.

UNITED STATES-ONLY ENTITIES

Observed Industry Targeting | Not Observed

RANSOMWARE ENTITY	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
OMEGA	○	●	●	○	○	○	○	○	2
BLACKMATTER	●	●	●	●	○	●	○	○	5
GRIEF	○	○	○	○	○	○	●	○	1
KITTYKATKREW	○	○	○	●	○	○	○	○	1
LINKC	●	●	○	○	○	○	○	○	2
MARKETO	●	●	●	●	●	○	○	●	6
PROLOCK	○	○	○	●	●	○	○	○	2
SECPO	●	○	○	○	○	○	○	○	1
SICARII	○	●	○	○	○	○	○	○	1
SUNCRYPT	●	●	●	●	●	●	●	○	7
XINGLOCKER	●	●	●	●	●	●	○	●	7

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

These entities are currently observed only in the United States within the location dataset. That should be read as a present-state observation, not as a claim that they cannot expand elsewhere. The contrast is still useful: SUNCRYPT and XINGLOCKER remain broad across 7 U.S. industries each despite their current U.S.-only location scope, while KITTYKATKREW is narrow in both geography and industry scope, appearing only in the U.S. financial services sector.

Public reporting adds context for some members of this group. BLACKMATTER was widely described as a DarkSide successor and was linked to disruptive 2021 attacks affecting U.S. food and agriculture operations. PROLOCK was associated with QakBot-enabled ransomware intrusions and later named by FBI leadership among the major ransomware groups supported by that botnet ecosystem.

STRATEGIC CONTEXT: WHY THESE SECTORS ARE TARGETED

This section focuses on the four highest-pressure sectors in the dataset. Government Public Services, Construction, Education, and Energy are also above the 50% observed targeting threshold, but the strategic rationale for the top tier is treated first because it carries the strongest concentration signal.

TECHNOLOGY

The U.S. technology sector is strategically important because much of the country depends on major software, cloud, platform, and infrastructure providers. Silicon Valley and the wider Bay Area remain a symbolic and operational center of U.S. technology, with firms such as Apple, Alphabet/Google, Meta, and Nvidia anchoring parts of the ecosystem. That concentration may create extortion pressure because disruption at a technology provider can affect customers, hosted data, identity services, software delivery, or downstream operations. For decision-makers, the pressure point is trust: technology firms are targeted not only for their own data, but because other organizations depend on them.

MANUFACTURING

U.S. manufacturing carries ransomware pressure because it connects production, logistics, critical infrastructure, and national supply chains. CISA identifies critical manufacturing outputs as essential to sectors such as transportation, defense, electricity, and major construction. That means downtime can move beyond an internal IT problem and affect plant scheduling, supplier coordination, quality processes, and delivery commitments. Lean inventories and complex supplier networks can reduce tolerance for prolonged disruption. For decision-makers, the pressure point is operational continuity: manufacturing organizations may need to restore safe, trusted production quickly because delays can cascade into customers, suppliers, and infrastructure dependencies.

HEALTHCARE

U.S. healthcare is a high-pressure extortion environment because it combines patient care, protected health information, insurance, payments, and clinical operations. CMS estimates national health expenditures reached $5.3 trillion in 2024, or 18.0% of GDP, making healthcare one of the country's largest economic systems. The Change Healthcare incident also showed how one major health technology and payment intermediary can create nationwide pressure across providers and patients. For decision-makers, healthcare ransomware risk should be framed around clinical continuity, payment disruption, privacy obligations, and public trust.

FINANCIAL SERVICES

U.S. financial services face extortion pressure because availability and confidence are central to the sector. New York remains a core financial hub, and the New York Fed has unique responsibilities in global market operations, monetary policy implementation, and financial services. Banks and financial institutions depend on payment systems, telecommunications, customer portals, third-party providers, and transaction integrity. FFIEC warns that disruption or unauthorized alteration of systems supporting financial services can undermine sector confidence. For decision-makers, the pressure point is confidence: ransomware can turn technical disruption into regulatory, market, customer, and reputational exposure.

FEATURED PROFILES

These four profiles are representative, not exhaustive. They were selected from the highest-breadth entities to illustrate the dominant affiliate-driven ransomware-as-a-service and double-extortion model visible across the dataset.

QILIN

Category: Ransomware-as-a-service / double-extortion operator

Primary malware/platform: Qilin/Agenda ransomware; Windows and ESXi-capable builds

Active since: Observed in 2022

Operating model: Affiliate-driven RaaS with customizable ransomware and leak infrastructure

Overview: Qilin's risk is conversion speed: common access exposure can quickly become data theft, encryption, and public leak pressure.

Common tradecraft themes: Phishing, compromised remote access, exposed services, lateral movement, process/service termination, exfiltration, and leak-site extortion.

Representative ATT&CK techniques: Phishing (T1566); Exploit Public-Facing Application (T1190); Valid Accounts (T1078); External Remote Services (T1133); Data Encrypted for Impact (T1486)

LOCKBIT3

Category: High-volume ransomware-as-a-service / double-extortion operator

Primary malware/platform: LockBit 3.0 / LockBit Black; Windows, Linux, and ESXi impact

Active since: LockBit since 2020; LockBit3 emerged in 2022

Operating model: Large affiliate ecosystem using shared LockBit tooling and infrastructure

Overview: LockBit3's risk is scale: many affiliates can turn varied access paths into fast theft, recovery sabotage, and encryption.

Common tradecraft themes: Phishing, exposed RDP/VPN, valid account abuse, credential dumping, SMB/PsExec-style movement, exfiltration, and shadow-copydeletion.

Representative ATT&CK techniques: Phishing (T1566); External Remote Services (T1133); Valid Accounts (T1078); SMB/ Windows Admin Shares (T1021.002); Inhibit System Recovery (T1490)

THEGENTLEMEN

Category: Emerging ransomware-as-a-service / double-extortion operation

Primary malware/platform:The Gentlemen RaaS; reported multi-platform enterprise lockers

Active since: Observed in mid-2025

Operating model: Affiliate-driven RaaS with financially motivated, opportunistic targeting

Overview: The Gentlemen's risk is rapid enterprise takeover, especially when edge access or credentials lead to domain-wide deployment.

Common tradecraft themes: VPN/firewall exposure, credential abuse, Active Directory discovery, remote execution, Group Policy deployment, SystemBC tunneling, and defense impairment.

Representative ATT&CK techniques: Exploit Public-Facing Application (T1190); Valid Accounts (T1078); Remote Desktop Protocol (T1021.001); Group Policy Modification (T1484.001); Impair Defenses: Disable or Modify Tools (T1562.001)

RANSOMHUB

Category: High-volume ransomware-as-a-service / double-extortion operator

Primary malware/platform: RansomHub ransomware with affiliate-supplied intrusion and exfiltration tooling

Active since: Observed in February 2024

Operating model: Affiliate-driven RaaS with leak-site pressure and variable intrusion tradecraft

Overview: RansomHub's risk is affiliate portability: operators bring different access methods but converge on theft, EDR disruption, and encryption.

Common tradecraft themes: Phishing, public-facing exploitation,password spraying, compromised accounts, credential dumping, EDR-killer tooling, exfiltration, and recovery sabotage.

Representative ATT&CK techniques: Phishing (T1566); Exploit Public-Facing Application (T1190); Password Spraying (T1110.003); Impair Defenses: Disable or Modify Tools (T1562.001); Data Encrypted for Impact (T1486)

RANSOMWARE THREAT PROJECTIONS: U.S. 2026

1

INITIAL ACCESS BROKERS WILL SHORTEN THE PATH TO RANSOMWARE

Initial access brokers will continue industrializing the commercial supply chain of ransomware access. Affiliates can buy or trade compromised credentials, VPN/RDP access, exposed enterprise-service footholds, and already-compromised networks, lowering the time and skill required to move from access to extortion.

2

EXPLOITED VULNERABILITIES WILL DRIVE MORE INTRUSIONS

Exploited vulnerabilities will remain the technical entry surface that feeds that access market. Unpatched VPNs, firewalls, edge devices, and internet-facing enterprise applications create high-value footholds in U.S. healthcare, manufacturing, technology, government, and financial services environments.

3

EDR-KILLER TOOLING WILL BECOME A STANDARD RAAS ENABLER

Ransomware-as-a-service operators and affiliates are likely to rely more heavily on EDR-killing tools before encryption or data theft. Recent reporting shows ransomware groups using vulnerable or signed drivers, modified legitimate utilities, and shared EDR-disabling tooling, suggesting EDR evasion is becoming a more common part of the affiliate playbook.

4

DOUBLE EXTORTION WILL BECOME THE DEFAULT PRESSURE MODEL

Ransomware attacks are likely to continue moving toward double extortion, where operators both disrupt systems and steal sensitive data before demanding payment. Even when organizations can restore from backups, attackers can still use leaked data, regulatory exposure, customer notification pressure, and reputational harm to force negotiations.

STRATEGIC RECOMMENDATIONS

1
HARDEN IDENTITY AND REMOTE ACCESS FIRST

Treat identity as the primary ransomware boundary. Require phishing-resistant MFA for remote access, administrators, SSO, VPN, and privileged service accounts; remove exposed RDP; review stale accounts; and monitor credential exposure and anomalous logins.

2
CLOSE INTERNET-FACING EXPOSURE BEFORE AFFILIATES EXPLOIT IT

Prioritize VPNs, firewalls, edge devices, backup platforms, RMM tools, and externally reachable applications. Use exploit intelligence and CISA KEV-style prioritization over generic severity scoring, shorten emergency patch timelines, and remove exposed services that are not mission-critical.

3
BUILD RECOVERY THAT RANSOMWARE CANNOT REACH

Maintain offline or immutable backups for critical systems and data, test restoration under ransomware conditions, and separate backup administration from the main identity environment. Pair recovery planning with segmentation so one compromise cannot disable production and backups together.

4
DETECT, CONTAIN, AND PREPARE FOR DOUBLE EXTORTION

Assume affiliates will try to disable security tools, move laterally, and steal data before encryption. Preserve centralized logs, enable EDR tamper protections, monitor PowerShell/RMM/exfiltration behavior, and rehearse legal, communications, regulatory, and law enforcement decisions before an extortion deadline.

This report is based on structured ransomware targeting analysis for U.S. The recommendations above are intended as a baseline operating model, not a one-time checklist. Continuous monitoring is required because ransomware access paths, affiliate tooling, and extortion pressure change quickly.

MODERNIZE YOUR SECURITY

PLEASE CONTACT JEAN CREECH AVENT FOR ADDITIONAL INFORMATION

jcreechavent@anomali.com | +1 843-986-8229 | WhatsApp: +1 843-986-8229

ANOMALI

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 1. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
0APT	●	●	●	●	●	●	●	●	8
0DAYSYNDICATE	●	○	○	○	○	○	○	○	1
0MEGA	○	●	●	○	○	○	○	○	2
8BASE	●	●	●	●	●	●	●	●	8
ABYSS	●	●	●	●	●	●	○	●	7
AILOCK	●	●	●	●	●	●	○	○	6
AKIRA	●	●	●	●	●	●	●	●	8
ALP-001	●	●	○	○	○	○	○	○	2
ALPHALOCKER	●	●	●	●	○	●	○	●	6
ALPHV	●	●	●	●	●	●	●	●	8
ANUBIS	●	●	●	●	●	●	○	●	7
APOS	●	●	●	●	○	●	○	○	5
APT73	●	●	●	●	●	●	●	●	8
ARCUSMEDIA	●	●	●	●	●	●	●	●	8

Actively Targeting | Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
ARGONAUTS	●	●	●	○	○	○	○	○	3
ARKANA	●	○	○	●	○	○	○	●	3
AURORA	○	●	●	●	○	○	○	○	3
AVADDON	●	●	●	●	●	●	●	●	8
AVOSLOCKER	●	●	●	●	●	●	●	●	8
BABUK	○	○	●	○	●	●	○	○	3
BABUK2	●	●	●	●	●	●	●	●	8
BAVACAI	●	●	○	○	●	●	●	○	5
BEAST	●	●	●	●	●	●	○	●	8
BERT	●	○	●	○	○	●	○	○	3
BIANLIAN	●	●	●	●	●	●	●	●	8
BLACKBASTA	●	●	●	●	●	●	○	●	7
BLACKBYTE	●	●	●	●	●	●	●	●	8
BLACKLOCK	●	●	●	●	●	●	●	●	8

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 2. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
BLACKMATTER	●	●	●	●	○	●	○	○	5
BLACKNEVAS	●	●	●	●	○	●	●	●	7
BLACKSHRANTAC	●	●	●	●	●	●	○	●	7
BLACKSUIT	●	●	●	●	●	●	●	●	8
BLACKWATER	○	●	●	○	●	○	○	○	3
BQTLOCK	●	○	○	○	●	○	●	○	3
BRAINCIPHER	●	●	●	●	●	○	●	●	7
BRAVOX	●	●	●	●	○	○	○	●	5
BROTHERHOOD	●	●	○	○	●	●	○	●	5
CACTUS	●	●	●	●	●	●	●	●	8
CEPHALUS	●	●	●	●	●	●	○	○	6
CHAOS	●	●	●	●	●	●	○	●	7
CHORT	●	○	○	○	○	○	●	○	3

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
CICADA3301	●	●	●	●	●	●	●	●	8
CIPHBIT	●	●	●	●	●	●	○	●	7
CIPHERFORCE	●	○	○	○	○	○	○	○	1
CLOAK	●	●	●	●	●	●	●	●	8
CLOP	●	●	●	●	●	●	●	●	8
CMDORGANIZATION	●	●	●	○	○	●	●	○	5
COINBASECARTEL	●	●	●	●	●	●	●	●	8
CONTI	●	●	●	●	●	●	●	●	8
CRAZYHUNTER	●	●	●	○	○	○	●	○	4
CRYP70N1C0D3	●	●	○	○	●	○	●	○	4
CRYPTBB	○	○	○	○	○	●	●	○	2
CRYPTO24	●	●	●	●	○	●	●	○	6
CUBA	●	●	●	●	●	●	●	●	8
D4RK4RMY	●	●	○	●	○	○	●	●	5
DAIXIN	○	●	●	●	●	○	○	●	5

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 3. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
DAN0N	●	○	●	●	○	○	○	○	3
DARKSIDE	○	●	○	○	○	●	○	●	3
DARKVAULT	●	○	●	●	●	○	●	○	5
DESOLATOR	●	○	○	●	○	●	○	○	3
DEVMAN	●	●	●	●	●	●	●	●	8
DIREWOLF	●	●	●	●	●	●	●	●	8
DISPOSSESSOR	●	●	●	●	●	●	●	●	8
DONEX	●	○	○	○	○	○	○	○	1
DONUTLEAKS	●	●	●	●	●	●	○	○	6
DOPPELPAYMER	●	●	○	○	●	○	●	○	4
DRAGONFORCE	●	●	●	●	●	●	●	●	8
DRAGONRANSOMWARE	●	●	●	●	○	○	●	●	6
DUNGHILL	●	●	○	○	○	●	○	○	3
ELDORADO	●	●	●	●	●	○	●	●	7

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
EMBARGO	●	●	●	●	●	●	○	○	6
EVEREST	●	●	●	●	●	●	●	●	8
EXITIUM	○	○	●	○	●	○	○	●	3
FLOCKER	●	●	●	●	●	○	●	○	6
FOG	●	●	●	●	●	○	●	●	7
FRAG	●	●	●	●	○	●	○	○	5
FULCRUMSEC	●	●	●	●	○	○	●	○	5
FUNKSEC	●	●	●	●	●	○	●	●	7
GDLOCKERSEC	●	○	○	○	●	○	●	○	3
GENESIS	●	●	●	●	●	●	●	●	8
GLOBAL	●	●	●	●	●	●	○	●	7
GRIEF	○	○	○	○	○	○	●	○	1
HANDALA	●	●	●	●	●	●	●	●	8
HELLCAT	●	○	○	●	●	○	●	●	5

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 4. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
HELLDOWN	●	●	●	●	●	○	○	●	6
HELLOGOOKIE	●	○	○	○	○	○	○	○	1
HIVE	●	●	●	●	●	●	●	●	8
HUNTERS	●	●	●	●	●	●	●	●	8
ICARUS	○	○	○	●	○	○	○	○	1
IMNCREW	●	●	●	●	○	○	○	○	4
INCRANSOM	●	●	●	●	●	●	●	●	8
INSOMNIA	●	●	●	●	○	●	○	●	6
INTERLOCK	●	●	●	●	●	●	●	○	7
J	●	●	○	○	●	●	●	●	6
KAIROS	●	●	●	●	●	●	●	●	8
KARAKURT	●	●	●	●	●	●	●	●	8
KAWA4096	○	○	●	●	●	○	○	○	3
KAZU	●	○	●	●	●	●	○	○	5

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
KILLSEC	●	●	●	●	●	●	●	●	8
KITTYKATKREW	○	○	○	●	○	○	○	○	1
KNIGHT	●	●	●	●	●	○	●	○	6
KRAKEN	●	●	●	○	○	●	○	○	4
KRYBIT	●	●	●	●	●	●	●	●	8
KRYPTOS	○	○	○	●	●	●	●	○	4
LAMASHTU	●	●	●	○	○	●	○	●	5
LAPSUS$	●	●	●	●	●	●	●	●	8
LEAKBAZAAR	●	●	●	●	○	●	○	○	5
LINKC	●	●	○	○	○	○	○	○	2
LOCKBIT2	●	●	●	●	●	●	●	●	8
LOCKBIT3	●	●	●	●	●	●	●	●	8
LOCKBIT5	●	●	●	●	●	●	●	●	8
LORENZ	●	●	●	●	●	●	○	○	6

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 5. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
LOSTTRUST	●	●	●	●	●	●	●	●	8
LYNX	●	●	●	●	●	●	●	●	8
M3RX	●	●	●	○	○	○	○	○	3
MADLIBERATOR	●	●	●	●	●	○	○	○	5
MALLOX	●	●	○	○	○	●	○	●	4
MARKETO	●	●	●	●	●	○	○	●	6
MAZE	●	●	●	●	●	●	●	●	8
MEDUSA	●	●	●	●	●	●	●	●	8
MEDUSALOCKER	●	●	●	●	●	●	●	●	8
MEOW	●	●	●	●	●	○	●	●	7
METAENCRYPTOR	●	●	○	●	○	●	●	○	5
MINTEYE	○	○	○	●	○	●	○	○	2
MOGILEVICH	○	○	○	○	●	○	○	○	2
MONEYMESSAGE	●	●	●	●	●	○	●	○	6

Actively Targeting | Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
MONTI	●	●	●	●	●	●	●	●	8
MORPHEUS	●	●	●	●	○	●	○	●	6
MS13089	○	○	●	○	○	○	○	○	1
NETRUNNER	○	●	●	○	○	○	○	○	2
NETWALKER	●	●	●	○	●	○	●	●	6
NIGHTSPIRE	●	●	●	●	●	●	●	●	8
NITROGEN	●	●	●	●	○	●	●	●	7
NOESCAPE	●	●	●	●	●	●	●	●	8
NOKOYAWA	●	●	●	●	●	●	●	●	8
NONAME	●	○	○	○	○	○	○	○	1
NOVA	●	●	●	●	●	●	●	●	8
OBSCURA	●	●	●	○	●	●	○	●	6
OSIRIS	○	●	○	○	○	○	○	○	1
PAYLOAD	○	●	●	●	●	●	●	●	7

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 6. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
PAYLOADBIN	●	●	●	●	●	●	●	●	8
PAYOUTSKING	●	●	●	●	○	●	●	●	7
PEAR	●	●	●	●	●	●	●	○	7
PLAY	●	●	●	●	●	●	●	●	8
PROLOCK	○	○	○	●	●	○	○	○	2
PYSA	●	●	●	●	●	●	●	●	8
QILIN	●	●	●	●	●	●	●	●	8
QUANTUM	●	●	●	●	●	●	●	●	8
RADAR	●	●	●	●	○	●	○	○	5
RADIANT	○	○	●	○	○	○	●	○	2
RAGNARLOCKER	●	●	●	●	○	●	●	●	7
RALORD	●	●	○	○	○	●	●	○	4
RANSOMED	●	●	●	●	●	○	○	●	6
RANSOMEXX	●	●	●	●	●	●	●	●	8

Actively Targeting | Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
RANSOMHOUSE	●	●	●	●	●	●	●	●	8
RANSOMHUB	●	●	●	●	●	●	●	●	8
RAWORLD	●	●	●	●	●	●	●	●	8
REBORNVC	●	○	○	○	○	○	●	○	2
REDRANSOMWARE	●	●	●	●	○	●	○	○	5
REVIL	●	●	●	●	●	●	●	●	8
RHYSIDA	●	●	●	●	●	●	●	●	8
ROYAL	●	●	●	●	●	●	●	●	8
RUNSOMEWARES	●	●	●	●	○	○	○	○	3
SAFEPAY	●	●	●	●	●	●	●	●	8
SARCOMA	●	●	●	●	○	●	●	●	7
SECP0	●	○	○	○	○	○	○	○	1
SECUROTROP	●	●	○	○	○	●	○	○	3
SHADOWBYT3$	●	○	○	○	○	○	●	○	2

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 7. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
SHINYHUNTERS	●	●	●	●	●	○	●	●	7
SICARII	○	●	○	○	○	○	○	○	1
SILENT	●	●	○	○	●	○	○	○	3
SILENTRANSOMGROUP	●	●	○	●	○	●	○	●	5
SINOBI	●	●	●	●	●	●	●	●	8
SKIRA	●	●	○	●	●	●	○	○	5
SNATCH	●	●	●	●	●	●	●	●	8
SPACEBEARS	●	●	●	●	●	●	○	●	7
STORMOUS	●	●	●	●	●	●	●	●	8
SUNCRYPT	●	●	●	●	●	●	●	○	7
TEAMXXX	○	○	●	●	○	○	○	○	2
TENGU	●	●	●	●	●	●	●	●	8
TERMITE	●	●	●	●	●	●	●	●	8
THEGENTLEMEN	●	●	●	●	●	●	●	●	8

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
THREEAM	●	●	●	●	●	●	●	○	7
TITAN	○	●	○	○	○	○	○	○	1
TRIDENTLOCKER	●	●	○	○	●	○	○	●	4
TRIGONA	●	●	●	●	○	●	●	○	6
TRINITY	●	●	●	●	●	○	○	○	5
TRIPLE X	○	○	○	●	○	○	○	○	1
UNDERGROUND	●	●	○	●	○	○	○	○	4
UNSAFE	○	●	○	○	○	○	●	●	3
VALENCIALEAKS	○	●	●	○	●	○	○	○	3
VANHELSING	●	○	●	●	●	○	○	○	4
VECT	●	●	●	●	○	○	●	●	6
VICESOCIETY	●	●	●	●	●	●	●	●	8
WANNACRY	○	●	●	●	●	○	●	●	6
WARLOCK	●	●	●	●	○	●	●	●	7

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology

APPENDIX A: FULL RANSOMWARE-BY-INDUSTRY TARGETING MATRIX

Appendix A matrix segment 8. All rows from the source matrix are preserved across appendix segments and sorted alphabetically by threat actor.

Actively Targeting Not Observed

THREAT ACTOR	TCH	MFG	HLT	FIN	GPS	CON	EDU	NRG	TOTAL
WEREWOLVES	●	●	●	●	○	○	○	●	5
WEYHRO	●	●	○	●	●	○	○	○	4
WORLDLEAKS	●	●	●	●	●	●	●	●	8
XINGLOCKER	●	●	●	●	●	●	○	●	7
TOTAL	172	166	154	151	131	128	118	118	

Column key: CON=Construction | EDU=Education | NRG=Energy | FIN=Financial Services | GPS=Government Public Services | HLT=Healthcare | MFG=Manufacturing | TCH=Technology