Information Security Education Journal (ISEJ)

DLINE JOURNALS

Print ISSN: 2349-8161
Online ISSN: 2349-817X

ISEJ 2026:13 (2)
https://doi.org/10.6025/isej/2026/13/2/51-83

Statistical Overview of Cyberattack Characteristics, Initial Access Mechanisms, Attack Progression, Extortion Strategies, and Security Exposure

Nguyen Minh Tuan,
Posts and Telecommunications Institute of Technology
Ho Chi Minh City, Vietnam

ABSTRACT

The modern cyber threat landscape is characterized by highly interconnected, multi-stage attack trajectories that exploit functional dependencies across an organization's infrastructure. This analysis systematically examines the statistical overview of cyberattack characteristics, initial access mechanisms, attack progression, extortion strategies, and security exposure based on empirical data from the Unit 42 Global Incident Response Report 2026. Drawing on aggregate statistics from over 750 incident-response engagements across more than 50 countries (October 2024 – September 2025), this study employs a descriptive analytical methodology to map adversarial behaviors and organizational vulnerabilities.

The findings reveal a paradigm shift toward identity-centric warfare, with identity weaknesses materially involved in approximately 90% of investigations and 99% of analyzed cloud identities exhibiting excessive permissions. Furthermore, 87% of intrusions span multiple attack surfaces, underscoring the inadequacy of siloed defenses. Attack velocity has accelerated dramatically, with the fastest-quartile time to exfiltration plummeting to just 72 minutes, severely limiting response windows. Extortion tactics are also evolving; while encryption remains prevalent, its use declined to 78% in 2025 as data theft and harassment increasingly serve as standalone pressure mechanisms. Additionally, the analysis highlights escalating supply chain and SaaS risks, with SaaS application data involvement rising to 23%, and over 60% of cloud native vulnerabilities residing in transitive libraries. Mapping these incidents to the MITRE ATT&CK framework highlights the dominance of techniques such as Valid Accounts, Phishing, and Remote Services. Ultimately, the study concludes that surviving the contemporary threat environment necessitates a transition from reactive, perimeter-based models to proactive, identity centric, and cross-surface defense architectures, underpinned by automated detection and immutable recovery capabilities.

Keywords: Cyberattack Trajectories, Incident Response, Identity-Centric Security, Attack Velocity, Extortion Tactics, MITRE ATT&CK, SaaS and Supply-Chain Security, Multi-Surface Warfare

Received: 3 June 2026, Revised: 31 August 2026, Accepted: 4 September 2026

Copyright: DLINE

1. Introduction

This digital frontier, once a niche for academics and specialists, has evolved into the central nervous system of modern society, underpinning global commerce, critical infrastructure, national security, and interpersonal communication [1, 2]. However, this increased connectivity has concurrently created an ever expanding attack surface, transforming cyberspace into a contested environment where malicious actors (including nation-states, transnational criminal organizations, and politically motivated hacktivists) operate with increasing sophistication and impact [3, 1, 4]. The current era is defined by the pervasiveness of ransomware, the strategic exploitation of supply chains, and the nascent use of artificial intelligence in attack campaigns, with ransomware attacks alone rising by 62% worldwide between 2019 and 2020 [5, 6, 7]. Amid this complex and evolving threat landscape, a fundamental challenge for cybersecurity leaders, policymakers, and researchers is to move beyond reactive incident response and develop proactive, data-driven defense strategies [1].

2. Related work

Cyberattacks rarely manifest as isolated actions; rather, they unfold as sequences in which each stage enables the next, forming trajectories that require relational and contextual analysis [8, 9]. However, most current taxonomies are limited to classifying behaviours in a segmented manner, without representing the functional interdependencies between consecutive techniques [10]. This fragmentation constrains their utility in anticipating complex attack patterns or designing effective reactive defences [11].

In initial phases, threats typically exploit social engineering techniques such as phishing or vishing, which allow attackers to obtain credentials or introduce malware into target systems [12, 13, 14]. Subsequently, many campaigns combine multiple vectors, as seen in the case of the Lucifer malware, which integrates cryptojacking, DDoS attacks, and vulnerability exploitation within a single attack flow [15]. IoT botnets represent another case, where compromised devices are used to structure large-scale distributed attacks [16, 17].

Threat classification in cybersecurity has been an essential tool for structuring the technical and operational knowledge associated with digital risks [18]. Over the past two decades, numerous taxonomies have been proposed to organise incidents according to criteria such as initial vectors, attacker objectives, types of techniques employed, or the impact generated [19]. This systematisation has improved communication among security teams, facilitated risk analysis, and laid the groundwork for coordinated incident response in complex environments [20].

One of the most influential reference frameworks has been MITRE ATT&CK [21], which catalogues tactics and techniques used in adversarial campaigns, structured according to the phases an attacker may follow after initial access. Its adoption has become widespread across both public and private sectors, consolidating its position as a de facto standard in many cyber intelligence operations [22]. However, limitations have been identified regarding its applicability to non-linear, scalable attack chains or those combining techniques from different vectors [23].

In this context, recent proposals have introduced automated methods to enrich these static taxonomies with dynamic operational data [24, 25]. For instance, an approach has been developed to map CVE vulnerabilities directly to ATT&CK tactics using machine learning models, enabling automated identification of security gaps and reducing reliance on manual intervention in the analysis process [26].

MITRE ATT&CK (orAdversarial Tactics, Techniques, and CommonKnowledge) is a curated knowledge base that details cyber adversary behavior across various domains, including enterprise, mobile, and industrial control systems (ICS) [27, 28]. Organized into matrices, ATT&CK outlines specific adversarial tactics (high-level objectives) and techniques (specific actions) that describe how an attacker seeks to compromise or persist in a system. [29] categorize 50 research contributions based on various use cases, including behavioral analytics, red teaming, defensive gap assessment, and CTI enrichment. This categorization highlights different

applications, methodologies, and data sources in the implementation of ATT&CK, with a focus on adversarial behavior modeling, automated threat detection, and framework enhancements. The categorization draws from a white paper [28] discussing the design philosophy, structure, and use cases of MITRE ATT&CK, and a similar white paper [31] on the development and application of the ATT&CK for ICS framework.

2.1 Problem Statement

The modern digital ecosystem, which underpins global commerce, critical infrastructure, and national security, has evolved into a highly contested environment characterized by an ever-expanding and interconnected attack surface. Contemporary cyberattacks are no longer isolated events but complex, multi stage trajectories that exploit functional interdependencies across an organization's infrastructure. A fundamental challenge in current cybersecurity paradigms is that traditional defense strategies and threat taxonomies often treat security domains in silos, failing to account for the non-linear, multi-surface nature of modern intrusions.

Specifically, the current threat landscape is defined by three critical vulnerabilities:

1. Identity as the Primary Target: Identity-related weaknesses are the central enabler of modern breaches, with compromised credentials and social engineering bypassing traditional perimeter defenses.

2. Accelerated Attack Velocity: The time window for detection and response has shrunk drastically, with attackers capable of exfiltrating data in under 72 minutes, rendering manual, reactive incident response obsolete.

3. Evolving Extortion and Supply-Chain Risks: Threat actors are increasingly leveraging data theft and harassment for extortion without relying solely on encryption, while simultaneously exploiting the transitive dependencies within cloud-native and SaaS supply chains.

The core problem is that cybersecurity leaders and policymakers lack a cohesive, data-driven understanding of how these interconnected vectors—identity, endpoints, networks, and cloud/SaaS environments—converge in real world incidents, hindering the development of proactive, resilient defense strategies.

2.2 Motivation

The motivation for this analysis stems from the urgent need to transition cybersecurity postures from reactive incident response to proactive, data-driven risk management. As cyberspace becomes the central nervous system of modern society, the cost of failure extends beyond financial loss to encompass national security and public safety.

This study is driven by the necessity to decode the shifting tactics of sophisticated threat actors including nation states and transnational criminal organizations who are exploiting the rapid adoption of cloud services, SaaS platforms, and remote work infrastructures. By analyzing empirical data from over 750 global incident-response engagements, this research aims to:

- Highlight the critical shift toward identity-centric attack vectors, emphasizing the urgent need for Zero Trust and phishing-resistant authentication.

- Quantify the alarming acceleration of attack velocity, demonstrating why continuous monitoring and automated containment are mandatory.

- Expose the hidden risks within software supply chains and SaaS integrations, which often fall outside traditional security visibility.

- Provide actionable, statistically grounded insights that enable organizations to design defense in depth

architectures, prioritize security investments, and build resilient recovery mechanisms (such as immutable backups) capable of withstanding modern multi vector extortion campaigns.

2.3 Methodology

This research employs a systematic data extraction, structuring, and descriptive analytical methodology based on the Unit 42 Global Incident Response Report 2026 (Palo Alto Networks). The methodology is structured into the following phases:

• **Data Sourcing & Scope:** The primary dataset comprises aggregate statistics from over 750 incident-response engagements handled between October 1, 2024, and September 30, 2025, representing organizations headquartered across more than 50 countries.

• **Structured Transcription & Categorization:** Numerical data, trend points, and statistical distributions explicitly stated in the source report were extracted and organized into thematic domains. These domains include Executive Indicators, Attack Surfaces, Initial Access Vectors, Identity-Driven Routes, Attack Velocity, Extortion Tactics, Ransom Economics, and MITRE ATT&CK Technique Prevalence.

• **Contextual Interpretation & Metric Validation:** Because the source data represents aggregate industry metrics rather than a raw, machine-readable incident database, the analysis focuses on descriptive statistics and year-over-year trend comparisons (e.g., calculating the 74.7% reduction in fastest-quartile exfiltration time, or tracking SaaS data involvement from 6% in 2022 to 23% in 2025).

• **Analytical Caveats & Limitations:** The methodology strictly adheres to the interpretive boundaries of the source data. Overlapping categories (such as multi-surface attack involvement) are treated as non-mutually exclusive. Furthermore, MITRE ATT&CK metrics are analyzed strictly as *relative prevalences* among identified techniques within specific tactics, rather than absolute probabilities of incident occurrence. Inferential statistics, predictive modeling, and confidence intervals are intentionally excluded due to the aggregate nature of the source report.

3. Data Source

This companion report [32] reorganizes numerical information explicitly stated in the source PDF. It is a transcription and structured presentation of report statistics, not a reconstruction of the underlying incident-level dataset.

3.1 Data extraction and interpretation notes

• The report describes more than 750 incident response cases handled from October 1, 2024, through September 30, 2025, with comparisons to earlier case data for selected metrics.

• Percentages across attack surfaces and several tactic categories are not mutually exclusive; they should not be summed to 100%.

• For Figure 3 (initial access vectors, 2021–2025), the PDF provides a plotted chart but does not tabulate all annual point values in its text. This package reports only annual values explicitly stated in narrative text and marks unreported cells as NR rather than digitizing by guesswork.

• MITRE ATT&CK percentages in the appendix are relative prevalence among techniques identified for each tactic, not the percentage of incidents involving each technique.

Some report statements use approximate or threshold wording (for example, >90%, about 35%, nearly 100). Those forms are preserved rather than converted into false precision.

The PDF is an aggregate threat intelligence report. It does not provide row level incident records, sample sizes for every sub group, or enough information to independently recalculate inferential statistics.

4. Analysis

4.1 Modern Cyber Threat Landscape

The digital frontier has evolved from a niche domain for academics and specialists in to the central nervous system of modern society. It now underpins global commerce, critical infrastructure, national security, and interpersonal communication. However, this unprecedented connectivity has concurrently created an ever-expanding and highly contested attack surface. Malicious actors ranging from nation states and transnational criminal organizations to politically motivated hacktivists operate with increasing sophistication, leveraging advanced capabilities to disrupt and exploit target environments.

The current era of cyber conflict is defined by several converging trends: the pervasiveness and financial impact of ransomware, the strategic exploitation of global software supply chains, and the nascent integration of artificial intelligence into attack campaigns. To illustrate the scale of this escalation, ransomware attacks alone rose by 62% worldwide between 2019 and 2020. Amid this complex and rapidly evolving threat landscape, a fundamental challenge for cybersecurity leaders, policymakers, and researchers is to move beyond reactive incident response and develop proactive, data driven defense strategies capable of addressing interconnected organizational risks.

4.2 Attack Trajectories and the Evolution of Threat Taxonomies

Cyberattacks rarely manifest as isolated actions; rather, they unfold as complex sequences in which each stage enables the next. These multi stage trajectories require relational and contextual analysis to fully understand. However, a significant limitation in current cybersecurity paradigms is that most threat taxonomies classify behaviors in a segmented manner, failing to represent the functional interdependencies between consecutive techniques. This fragmentation constrains the utility of traditional frameworks in anticipating complex attack patterns or designing effective, reactive defenses.

The MITRE ATT&CK framework has emerged as the *de facto* standard for cataloging adversarial tactics and techniques across enterprise, mobile, and industrial control systems. Its widespread adoption has improved communication among security teams and facilitated coordinated incident response. Nevertheless, limitations have been identified regarding its applicability to non linear, scalable attack chains or those combining techniques from disparate vectors (e.g., integrating crypto jacking, DDoS, and vulnerability exploitation into a single flow). Consequently, modern threat analysis requires supplementing static taxonomies with dynamic operational data to map vulnerabilities directly to adversarial behaviors and identify hidden security gaps.

4.3 Data Source and Analytical Scope

This analysis is grounded in the empirical data presented in the Unit 42 Global Incident Response Report 2026 (Palo Alto Networks, February 2026). The dataset encompasses aggregate statistics from more than 750 incident response engagements handled between October 1, 2024, and September 30, 2025, representing organizations headquartered across more than 50 countries.

The objective of this analysis is to systematically transcribe, structure, and interpret the numerical information explicitly stated in the source report. It provides a comprehensive statistical overview of cyberattack characteristics, initial access mechanisms, attack progression, extortion strategies, and security exposure, translating aggregate threat intelligence into actionable insights regarding multi surface warfare, identity centric exploitation, and attack velocity.

4.4 Interpretive Framework and Limitations

To ensure analytical rigor and prevent misinterpretation of the aggregate data, the following interpretive rules and limitations govern the subsequent tables and figures:

Non-Mutually Exclusive Categories: Percentages across attack surfaces and several tactic categories represent overlapping conditions. Because a single intrusion frequently affects multiple surfaces (e.g., identity, endpoint, and network), these percentages must not be summed to 100%.

Relative vs. Absolute Prevalence: In the context of the MITRE ATT&CK technique mappings, the reported percentages represent the *relative prevalence* among the specific techniques identified for a given tactic. They do not represent the absolute percentage of total incidents involving each technique.

Preservation of Approximate Wording: Where the source report utilizes threshold or approximate wording (e.g., “>90%”, “about 35%”, “nearly 100”), these forms are preserved to avoid introducing false precision.

Absence of Row-Level Data: The source material is an aggregate threat-intelligence report. It does not provide row-level incident records, exhaustive sample sizes for every subgroup, or the underlying raw data required to independently recalculate inferential statistics. Therefore, this analysis is strictly descriptive and does not compute confidence intervals, significance tests, or predictive regression models.

Trend Data Constraints: For certain longitudinal metrics (such as the 2021–2025 initial access vectors), the source provides plotted charts but does not tabulate all annual point values in the narrative text. This analysis reports only the annual values explicitly stated in the text, marking unreported cells as “NR” (Not Reported) rather than estimating or digitizing by guesswork.

Indicator	**Value**	**Unit**	**Population / context**
Incident response engagements	>750	cases	2025 report dataset
Countries represented	>50	countries	Organizations headquartered across more than 50 countries
Intrusions spanning 2+ attack surfaces	87	%	Incidents
Intrusions spanning 3+ attack surfaces	67	%	Incidents
Intrusions spanning 4+ attack surfaces	43	%	Incidents
Browser activity	48	%	Investigations; 44% in 2024
Preventable gaps materially enabled breaches	>90	%	Breaches/incidents as described in report
Identity weaknesses materially involved	~90	%	Investigations
Cloud identities with excessive permissions	99	%	More than 680,000 identities analyzed

Cloud or SaaS assets involved	~35	%	Investigations
SaaSapplication data relevant	23	%	2025 cases; 18% 2024, 12% 2023, 6% 2022
Fastest quartile time to exfiltration	72	minutes	2025; 285 minutes in 2024
Median time to exfiltration	2	days	Full dataset
Incidents with exfiltration under 1 hour	22	%	2025; 19% in 2024
Backup restoration possible without paying	41	%	Extortion victims
Extortion cases where backups were impacted	26	%	2025
Threat actors fulfilled promises	68	%	Cases where actors made a promise

Table 1. Executive cybersecurity indicators

Table 1 presents the principal cybersecurity indicators reported by Unit 42, providing an overview of the scale, characteristics, and operational consequences of the investigated incidents. The report covers more than 750 incident-response engagements across more than 50 countries. A prominent finding is the extensive involvement of multiple attack surfaces: 87% of intrusions affected at least two surfaces, 67% involved three or more, and 43% extended across four or more surfaces. These results indicate that contemporary cyber incidents frequently involve interconnected organizational resources rather than isolated technical components.

Identity-related weaknesses were particularly prominent, being materially involved in approximately 90% of investigations. In addition, 99% of more than 680,000 examined cloud identities had excessive permissions, indicating substantial exposure associated with identity and access-management practices. Browser activity was identified in 48% of investigations, while cloud or SaaS assets were involved in approximately 35%. The table also highlights the increasing relevance of SaaS application data, which was involved in 23% of cases in 2025, compared with 6% in 2022.

The operational indicators further demonstrate the speed and impact of modern intrusions. The fastest-quartile time to exfiltration decreased from 285 minutes in 2024 to 72 minutes in 2025, while 22% of incidents involved exfiltration within one hour. In extortion-related cases, 41% of victims could restore from backups without paying, although backups were impacted in 26% of cases. Overall, the indicators demonstrate the importance of identity security, cross-surface visibility, cloud governance, and rapid incident detection and recovery.

Attack surface	Incidents affected (%)
Identity	89
Endpoints	61
Network	50
Human	45
Email	27
Applications	26
Cloud	20
SecOps	10
Database	1

Table 2. Attack surfaces involved in intrusions

Identity was the most frequently involved surface (89%), followed by endpoints (61%) and network activity (50%). Categories overlap because a single intrusion can affect multiple surfaces.

Table 2 summarizes the distribution of incidents across nine organizational attack surfaces. Identity was the most frequently affected surface, accounting for 89% of incidents, followed by endpoints (61%) and networks (50%). Human-related factors were involved in 45% of incidents, while email and applications accounted for 27% and 26%, respectively. Cloud environments were involved in 20% of incidents, whereas security operations and database-related surfaces accounted for 10% and 1%.

The findings demonstrate the central role of identity infrastructure in contemporary cyberattacks. The high proportion of identity-related incidents, together with the substantial involvement of endpoints and networks, suggests that attackers commonly exploit interconnected access and infrastructure components. The involvement of human factors in 45% of incidents also emphasizes the importance of addressing social engineering and user-related security weaknesses alongside technical controls.

These percentages should be interpreted as overlapping categories rather than mutually exclusive incident classifications. A single intrusion may involve several attack surfaces; consequently, the percentages should not be summed to estimate the total number of incidents.

Interpretation: The three reported identity-driven route groups total 65% of initial access. Identity-related social engineering was the largest group (33%), followed by credential misuse/brute force (21%) and identity policy/insider risk (11%).

Table 3 examines the principal routes through which identity-related weaknesses contributed to initial access. The three reported route groups collectively accounted for 65% of initial access. Identity-related social engineering represented the largest group at 33%, comprising identity based phishing (22%) and other forms

of social engineering (11%). Credential misuse and brute-force attacks accounted for 21%, including previously compromised credentials (13%) and brute force (8%). Identity policy and insider risks represented a further 11%, comprising IAM misconfigurations (3%) and insider threats (8%).

Identity-driven initial access route	**Share (%)**	**Definition / note**
Identity-related social engineering	33	Identity-based phishing + other social engineering
Identity-based phishing	22	Subcategory
Other social engineering	11	Subcategory
Credential misuse and brute force	21	Previously compromised credentials + brute force
Previously compromised credentials	13	Subcategory
Brute force	8	Subcategory
Identity policy and insider risk	11	IAM misconfigurations + insider threats
IAM misconfigurations	3	Subcategory
Insider threats	8	Subcategory

Table 3. Identity-driven initial access routes

The distribution indicates that identity-driven compromise occurs through several complementary mechanisms. Social engineering represents the largest reported route, highlighting the continuing importance of phishing-resistant authentication, user awareness, and identity verification. The contribution of previously compromised credentials and brute-force attacks further demonstrates the risks associated with weak authentication controls, password reuse, and inadequate protection against automated login attempts. The presence of IAM misconfigurations and insider threats indicates that weaknesses in access governance and internal controls also contribute to initial compromise.

Collectively, these results suggest that identity protection requires a combination of technical and organizational safeguards, including multifactor authentication, privileged-access management, continuous identity monitoring, and effective access-policy enforcement.

Unit42_Global_Incident_Response_2026_Tables_Figures_Report(1).

Phishing and software/API vulnerabilities tied at 22%. Previously compromised credentials (13%) and other social engineering (11%) were also prominent. The report's identity based phishing subcategory is included within phishing and must not be added again to this table.

Initial access vector	Share (%)	Year
Phishing	22	2025
Software/API vulnerabilities	22	2025
Previously compromised credentials	13	2025
Other social engineering	11	2025
Brute force	8	2025
Insider threat	8	2025
IAM misconfigurations	3	2025

Table 4. Leading initial access vectors in 2025

Table 4 compares the principal initial access vectors identified in the 2025 incident response data. Phishing and software/API vulnerabilities were jointly the most frequently reported vectors, each accounting for 22% of initial access. Previously compromised credentials represented 13%, followed by other social engineering at 11%. Brute-force attacks and insider threats each accounted for 8%, while IAM misconfigurations represented 3%.

The equal contribution of phishing and software/API vulnerabilities demonstrates that initial compromise can arise through both human-oriented attack techniques and technical weaknesses in software infrastructure. The proportion associated with previously compromised credentials also highlights the importance of credential protection and continuous authentication monitoring. Meanwhile, the contributions of social engineering, brute force, and insider threats indicate that organizations must address a broad range of access-related vulnerabilities.

The results support a defense in depth approach in which email and user protection are combined with vulnerability management, secure software development, credential monitoring, and identity governance. The identity based phishing value is already represented within the phishing category and should not be added separately when interpreting the table

Initial access vector	2021 (%)	2025 (%)	Source note
Other social engineering	3.0	11.0	2021 to 2025; report explicitly states increase
Brute force	13.0	8.0	2021 to 2025; report explicitly states decline
Previously compromised credentials	NR	13.0	2025 value reported; earlier annual values not transcribed in narrative
Phishing	NR	22.0	2025 value reported; Figure 3 provides annual chart but not tabulated values

Software/API vulnerabilities	NR	22.0	2025 value reported; Figure 3 provides annual chart but not tabulated values
IAM misconfigurations	NR	NR	Reported range across five years: 1%–4%; year-specific values not tabulated

Table 5. Explicitly reported initial-access trend points

The report explicitly states that other social engineering rose from 3% in 2021 to 11% in 2025, while brute force declined from 13% to 8%. The source's plotted annual series is not fully tabulated in the text, so intermediate values are not fabricated.

Table 5 presents the year specific initial-access values that are explicitly stated in the report narrative for the period 2021–2025. Other social engineering increased from 3% in 2021 to 11% in 2025, representing an eight-percentage-point increase. In contrast, brute force attacks declined from 13% to 8% over the same period, representing a five-percentage point reduction. The report also indicates that IAM misconfigurations remained within a range of 1%–4% across the five-year period.

For previously compromised credentials, phishing, and software/API vulnerabilities, the table provides the reported 2025 values but does not assign values to 2021 because the corresponding annual figures are not tabulated in the report narrative. These entries are therefore marked as not reported (NR). This distinction is important because the source includes a plotted annual trend but does not provide all underlying numerical observations in tabular form.

The findings suggest a growing contribution from other social engineering and a declining contribution from brute force attacks in the explicitly reported comparison. However, the available values are insufficient to establish a complete annual trend for every attack vector. Accordingly, the table supports a descriptive comparison of reported endpoints rather than a comprehensive time-series analysis.

Metric	**2024**	**2025**	**Unit**	**Note**
Fastest quartile time-to-exfiltration	285.0	72	minutes	2024 vs 2025
Incidents exfiltrating in under 60 minutes	19.0	22	%	2024 vs 2025
Median time-to-exfiltration	NR	2	days	Full dataset; not an annual comparison

Table 6. Attack velocity and time-to-exfiltration

The fastest quartile's time to exfiltration fell from 285 to 72 minutes (a 74.7% reduction, calculated from the two reported values). The share of incidents exfiltrating in under one hour rose from 19% to 22%. The median across the full dataset was two days.

Table 6 presents indicators of attack velocity by comparing selected exfiltration metrics for 2024 and 2025. The fastest-quartile time to exfiltration decreased from 285 minutes in 2024 to 72 minutes in 2025, corresponding to a reduction of approximately 74.7%. At the same time, the proportion of incidents involving

exfiltration within 60 minutes increased from 19% to 22%. The report also provides a median time to exfiltration of two days for the full dataset.

These findings indicate that although the overall median time to exfiltration was two days, a subset of incidents progressed much more rapidly. The substantial reduction in the fastest quartile time suggests that organizations may have increasingly limited opportunities to identify and contain attacks before sensitive information is removed. The increase in incidents involving exfiltration within one hour reinforces the need for continuous monitoring, rapid detection, and automated response capabilities.

The median value applies to the full dataset and should not be interpreted as a separate annual median for either 2024 or 2025.

Extortion tactic	2021	2022	2023	2024	2025
Encryption	96	90	89	92	78
Data theft	53	59	53	60	57
Harassment	5	9	8	13	10

Table 7. Extortion tactics, 2021–2025

Encryption fell to 78% in 2025 from 92% in 2024, while data theft remained at 57% and harassment at 10%. The report emphasizes that extortion is increasingly possible without encryption.

Table 7 describes changes in the use of three extortion tactics encryption, data theft, and harassment between 2021 and 2025. Encryption was the most frequently reported tactic throughout the period, although its reported prevalence decreased from 96% in 2021 to 78% in 2025. A notable decline occurred between 2024 and 2025, when encryption decreased from 92% to 78%. Data theft remained comparatively stable, varying between 53% and 60% and reaching 57% in 2025. Harassment was less frequently reported, increasing from 5% in 2021 to 10% in 2025, with a peak of 13% in 2024.

The results suggest that extortion strategies are not limited to encrypting organizational data. The continued prevalence of data theft indicates that attackers can exert pressure through the threat of information disclosure, even when encryption is not the primary mechanism. Harassment represents a less common but persistent complementary tactic.

The reduction in encryption prevalence, alongside the continued presence of data theft and harassment, is consistent with the report's observation that extortion can occur without encryption. These findings highlight the importance of data loss prevention, sensitive-data monitoring, backup protection, and incident communication planning in addition to conventional ransomware defenses.

Median initial demands rose from $1.25 million to $1.5 million, and median payments increased from $267,500 to $500,000. However, both demand and payment as a share of perceived annual revenue declined.

Table 8 compares ransom demands, payments, and negotiation-related indicators for 2024 and 2025. The median initial ransom demand increased from USD 1.25 million in 2024 to USD 1.5 million in 2025. Median ransom payments also increased, rising from USD 267,500 to USD 500,000. Despite these increases in absolute monetary values, the median initial demand as a proportion of perceived annual revenue declined from 2.0% to 0.55%. Similarly, ransom payments as a proportion of perceived annual revenue decreased from 0.6% to 0.26%.

The median reduction between the initial demand and final payment increased from 53% in 2024 to 61% in 2025. This indicates a larger reported percentage reduction during negotiations in 2025, even though the median payment amount was higher than in the previous year.

Taken together, the findings show that ransom economics cannot be understood solely through absolute monetary values. The relationship between the demand, payment, and perceived organizational revenue provides additional context for interpreting the financial pressure imposed by attackers. However, these are descriptive comparisons; the table does not establish why ransom amounts changed or whether the differences are statistically significant.

Ransom metric	2024	2025	Unit	Note
Median initial ransom demand	1250000.0	1500000.0	USD	2024 to 2025
Median ransom payment	267500.0	500000.0	USD	2024 to 2025
Initial demand as share of perceived annual revenue	2.0	0.55	% PAR	2024 to 2025
Payment as share of perceived annual revenue	0.6	0.26	% PAR	2024 to 2025
Median reduction from demand to payment	53.0	61.0	% reduction	2024 to 2025

Table 8. Ransom economics

Recovery / negotiation indicator	Share (%)
Victims able to restore from backup without paying	41
Extortion cases in which attackers impacted backups	26
Actors fulfilled promises when made	68

Table 9. Recovery and negotiation indicators

41% of victims could restore systems from backup without paying, but attackers impacted backups in 26% of extortion cases. Actors fulfilled promises in 68% of cases in which they made a promise; this should not be interpreted as evidence that promises are reliable.

Table 9 summarizes three indicators relating to organizational recovery and negotiation outcomes. The results show that 41% of victims were able to restore their systems from backups without paying the ransom. However, attackers impacted backups in 26% of extortion cases, demonstrating that recovery resources may themselves become targets during an intrusion. The report also states that threat actors fulfilled their promises in 68% of cases in which they made a promise.

The findings emphasize the operational importance of backup resilience and recovery preparedness. The proportion of victims able to restore from backups demonstrates that recovery capabilities can provide an alternative to ransom payment. Nevertheless, the reported impact on backups indicates that merely maintaining backup copies may be insufficient unless those copies are isolated, protected, and regularly tested.

The promise fulfilment figure requires careful interpretation. It refers only to cases in which threat actors made promises and does not demonstrate that such promises are dependable or that negotiation is a reliable risk-management strategy. Overall, the results support the development of resilient backup architectures and tested recovery procedures rather than reliance on attacker assurances.

Year	Cases involving SaaS application data (%)
2022	6
2023	12
2024	18
2025	23

Table 10. SaaS and software supply-chain exposure

Table 10 presents the year-by-year proportion of cases involving SaaS application data from 2022 to 2025. The reported share increased consistently from 6% in 2022 to 12% in 2023, 18% in 2024, and 23% in 2025. The increase from 2022 to 2025 represents a rise of 17 percentage points, indicating that SaaS application data became increasingly relevant to the investigated incidents during the reporting period.

This pattern highlights the growing importance of cloud-hosted applications and externally managed software services in organizational cybersecurity. As organizations rely more heavily on SaaS platforms for communication, collaboration, data storage, and business operations, these environments can become important components of the attack surface. Consequently, security monitoring should extend beyond traditional endpoints and on-premises infrastructure to include SaaS identities, application permissions, integrations, and data-access activities.

The table demonstrates an increase in the proportion of investigations involving SaaS application data. It does not, by itself, establish that SaaS adoption caused an increase in incidents or that the absolute number of SaaS-related attacks increased at the same rate.

Indicator	Value	Unit	Source
C2 techniques related to remote access tools (T1219)	39	%	PDF p. 14
Cloud-native application vulnerabilities in transitive libraries	>60	%	PDF p. 14
Additional Salesforce integrations discovered in one case	nearly 100	count	PDF p. 13; case example, not prevalence

Table 11. Additional supply-chain indicators

Investigations involving SaaS application data rose from 6% in 2022 to 23% in 2025. The report also states that more than 60% of vulnerabilities in cloud-native applications reside in transitive libraries.

Table 11 presents three additional indicators concerning software and cloud supply-chain exposure. Remote access tools accounted for 39% of the reported command-and-control technique prevalence. The report also indicates that more than 60% of vulnerabilities in cloud-native applications were located in transitive libraries. In addition, nearly 100 additional Salesforce integrations were discovered in one investigated case.

These findings illustrate different dimensions of supply-chain and application exposure. The remote-access-tool indicator highlights the relevance of legitimate or dual-use remote administration capabilities in attacker command-and-control activity. The transitive-library finding points to the security implications of dependencies that are incorporated indirectly through other software components. The Salesforce example illustrates how integrations can expand the number of connections and potential access paths within a business application environment.

The indicators collectively emphasize the importance of software composition analysis, dependency monitoring, application integration inventories, and restrictions on remote access tools. The Salesforce figure is a single case example rather than a prevalence estimate and should not be generalized to all investigated organizations.

Security gap / evidence indicator	Value	Unit	Context	Source
Investigations requiring evidence from 2+ distinct sources	87	%	Some complex cases drew on as many as 10 sources	PDF p. 29
Breaches materially enabled by misconfiguration / coverage gaps	>90	%	Report level finding	PDF p. 29
Cloud identities with excessive permissions	99	%	Across > 680,000 identities	PDF p. 11

Table 12. Security gaps and investigative visibility

Table 12 summarizes findings relating to security control weaknesses and the information required to investigate incidents. Approximately 87% of investigations required evidence from at least two distinct sources, while some complex investigations used evidence from as many as ten sources. The report further states that more than 90% of breaches were materially enabled by misconfiguration or security coverage gaps. In addition, 99% of the more than 680,000 cloud identities examined had excessive permissions.

These findings reveal two interconnected cybersecurity challenges. First, effective incident investigation depends on correlating information from multiple sources, including identity systems, endpoints, network infrastructure, cloud platforms, and security-monitoring tools. Limited visibility across these sources may hinder the reconstruction of attack sequences and the identification of compromised resources. Second, the high reported prevalence of misconfiguration and excessive permissions indicates that weaknesses in security governance and access control can materially increase organizational exposure.

The findings support integrated security monitoring, centralized evidence collection, configuration assessment, and continuous identity permission reviews. The percentages should be interpreted within the contexts specified by the report, rather than as independently measured rates for a common population.

MITRE tactic	Technique	Relative prevalence (%)	PDF page	Interpretation note
Initial access	T1078 Valid Accounts	39	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Initial access	T1566 Phishing	29	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Initial access	T1190 Exploit Public-Facing Application	21	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Initial access	T1133 External Remote Services	6	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Initial access	T1189 Drive-by Compromise	5	37	Relative prevalence among techniques identified for this tactic; not case prevalence

Initial access	T1091 Replication Through Removable Media	<1	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1059 Command and Scripting Interpreter	58	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1053 Scheduled Task/Job	14	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1204 User Execution	13	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1569 System Services	10	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1072 Software Deployment Tools	2	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1047 Windows Management Instrumentation	2	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1203 Exploitation for Client Execution	<1	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Execution	T1675 ESXi Administration Command	<1	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1078 Valid Accounts	19	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1543 Create or Modify System Process	16	37	Relative prevalence among techniques identified for this tactic; not case prevalence

Persistence	T1053 Scheduled Task/Job	15	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1136 Create Account	13	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1098 Account Manipulation	10	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1505 Server Software Component	7	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1547 Boot or Logon Autostart Execution	5	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1133 External Remote Services	3	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1112 Modify Registry	3	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1574 Hijack Execution Flow	3	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1556 Modify Authentication Process	3	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1546 Event Triggered Execution	2	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Persistence	T1037 Boot or Logon Initialization Scripts	1	37	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1003 OS Credential Dumping	32	38	Relative prevalence among techniques identified for this tactic;

Credential access	T1110 Brute Force	30	38	not case prevalence
Credential access	T1555 Credentials from Password Stores	11	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1552 Unsecured Credentials	6	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1558 Steal or Forge Kerberos Tickets	6	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1556 Modify Authentication Process	4	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1212 Exploitation for Credential Access	3	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1621 MFA Request Generation	3	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1557 Adversary-in-the-Middle	1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1056 Input Capture	1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1040 Network Sniffing	1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Credential access	T1649 Steal or Forge Authentication Certificates	<1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1021 Remote Services	85	38	Relative prevalence among techniques identified for this tactic; not case prevalence

Lateral movement	T1570 Lateral Tool Transfer	4	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1550 Use Alternate Authentication Material	4	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1072 Software Deployment Tools	2	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1563 Remote Service Session Hijacking	2	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1210 Exploitation of Remote Services	1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1534 Internal Spearphishing	<1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1091 Replication Through Removable Media	<1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Lateral movement	T1080 Taint Shared Content	<1	38	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1074 Data Staged	33	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1560 Archive Collected Data	21	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1213 Data from Information Repositories	15	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1039 Data from Network Shared Drive	6	39	Relative prevalence among techniques identified for this tactic; not case prevalence

Collection	T1005 Data from Local System	5	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1119 Automated Collection	4	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1113 Screen Capture	4	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1056 Input Capture	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1114 Email Collection	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1557 Adversary in the Middle	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1530 Data from Cloud Storage	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1123 Audio Capture	1	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Collection	T1602 Data from Configuration Repository	1	39	Relative prevalence among techniques identified for this tactic; not case prevalence

Command and control	T1219 Remote Access Tools	39	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Command and control	T1105 Ingress Tool Transfer	25	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Command and control	T1071 Application Layer Protocol	19	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Command and control	T1572 Protocol Tunneling	8	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Command and control	T1090 Proxy	6	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Command and control	T1102 Web Service	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1095 Non-Application Layer Protocol	<1	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1567 Exfiltration Over Web Service	62	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1048 Exfiltration Over Alternative Protocol	14	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1011 Exfiltration Over Other Network Medium	7	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1052 Exfiltration Over Physical Medium	7	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1041 Exfiltration Over C2 Channel	5	39	Relative prevalence among techniques identified for this tactic; not case prevalence

Exfiltration	T1020 Automated Exfiltration	3	39	Relative prevalence among techniques identified for this tactic; not case prevalence
Exfiltration	T1537 Transfer Data to Cloud Account	2	39	Relative prevalence among techniques identified for this tactic; not case prevalence

Table 13. Selected MITRE ATT&CK technique prevalence

Valid Accounts (39%) and Phishing (29%) were the leading listed initial-access techniques. Remote Services (85%) dominated the listed lateral-movement techniques; Exfiltration Over Web Service (62%) led the exfiltration group. These are within-tactic relative prevalence figures, not case rates.

Table 13 provides a structured overview of selected MITRE ATT&CK techniques across several adversarial tactics, including initial access, execution, persistence, credential access, lateral movement, collection, command and control, and exfiltration. The values represent relative prevalence among the techniques identified within each tactic; they are not percentages of incidents involving those techniques.

Within initial access, Valid Accounts (T1078) represented 39% of the listed technique prevalence, followed by Phishing (T1566) at 29% and Exploit Public-Facing Application (T1190) at 21%. These findings indicate the importance of account compromise, social engineering, and exploitation of externally accessible applications in the initial-access technique profile. For execution, Command and Scripting Interpreter (T1059) was the leading listed technique at 58%, suggesting a substantial role for command- and script-based execution activity among the techniques identified.

The persistence category included Valid Accounts (19%), Create or Modify System Process (16%), Scheduled Task/Job (15%), and Create Account (13%) as prominent techniques. This distribution illustrates the range of mechanisms through which attackers may maintain access. In the credential-access category, OS Credential Dumping (32%) and Brute Force (30%) were the two leading listed techniques, followed by Credentials from Password Stores (11%). These results reinforce the importance of protecting authentication material and monitoring suspicious credential-related activity.

Remote Services (T1021) dominated the listed lateral-movement techniques, accounting for 85% of the relative prevalence in that tactic. For collection, Data Staged (33%), Archive Collected Data (21%), and Data from Information Repositories (15%) were the leading listed techniques. In command and control, Remote Access Tools (T1219) represented 39%, followed by Ingress Tool Transfer (25%) and Application Layer Protocol (19%). Finally, Exfiltration Over Web Service (T1567) was the leading listed exfiltration technique at 62%, followed by Exfiltration Over Alternative Protocol (14%).

Overall, the table demonstrates that the reported technique profile spans the full progression of an intrusion, from initial access and execution to persistence, credential access, lateral movement, collection, command and control, and data exfiltration. The prominence of account-related techniques, remote services, remote-access tools, and web service based exfiltration suggests that identity controls, remote-access governance, endpoint monitoring, and outbound data monitoring are important defensive priorities. Because the percentages are relative to techniques identified within each tactic, they should not be interpreted as incident-level probabilities or compared as though all tactics share a common denominator.

Figure 1 illustrates the relative involvement of different organizational attack surfaces in the investigated incidents. Identity represents the most frequently affected surface, at 89%, followed by endpoints at 61% and networks at 50%. Human related factors account for 45%, while email and applications contribute 27% and 26%, respectively. Cloud environments, security operations, and databases show lower reported involvement, at 20%, 10%, and 1%.

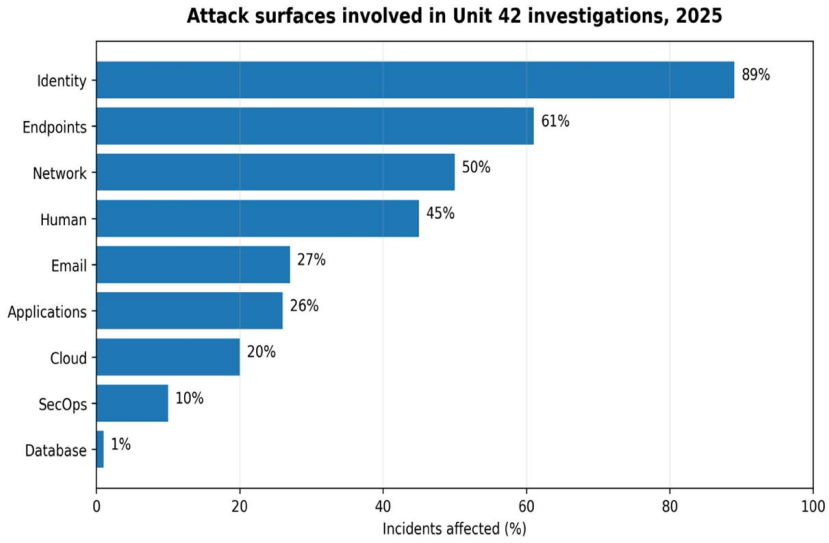

Figure 1. Attack surfaces involved in Unit 42 investigations in 2025. The bars show the percentage of incidents involving each surface; overlap is expected

The figure visually emphasizes the predominance of identity related exposure and the interconnected nature of organizational attack surfaces. The substantial involvement of endpoints and networks suggests that identity compromise may occur alongside activity across devices and communication infrastructure. The contribution of human-related factors also indicates that technical controls need to be complemented by user focused security measures. Since an intrusion may involve multiple surfaces, the bars represent overlapping categories and do not constitute mutually exclusive portions of a whole.

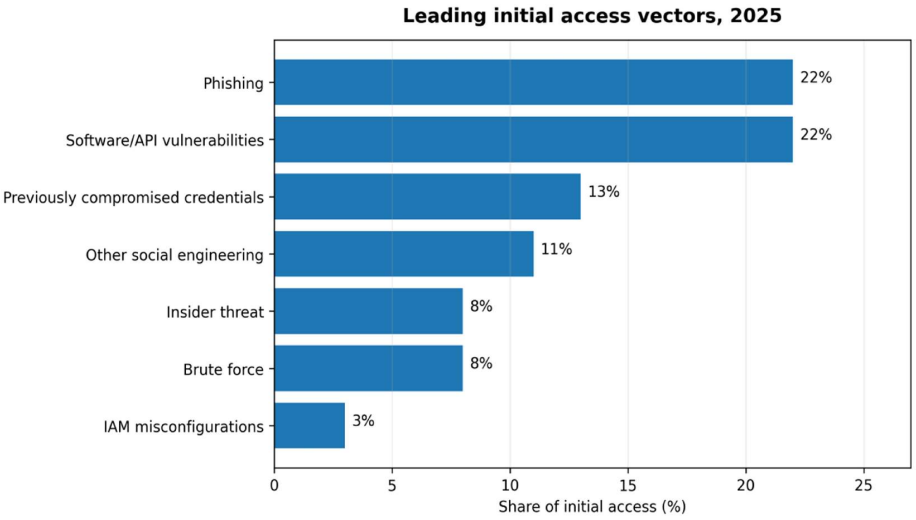

Figure 2. Leading initial access vectors in 2025. Phishing and software/API vulnerabilities each accounted for 22%

Figure 2 compares the leading vectors used to obtain initial access in 2025. Phishing and software/API vulnerabilities share the highest reported proportion, with each accounting for 22%. Previously compromised credentials represent 13%, while other social engineering accounts for 11%. Brute-force attacks and insider threats each contribute 8%, and IAM misconfigurations account for 3%.

The figure demonstrates that initial access is associated with both human-oriented and technology oriented

weaknesses. The equal contribution of phishing and software/API vulnerabilities indicates that organizations need to address user-facing attack pathways as well as weaknesses in externally accessible software and interfaces. The remaining categories highlight the importance of credential security, authentication protections, and access governance. The figure supports a multi-layered prevention strategy rather than a defense approach focused exclusively on phishing or malware

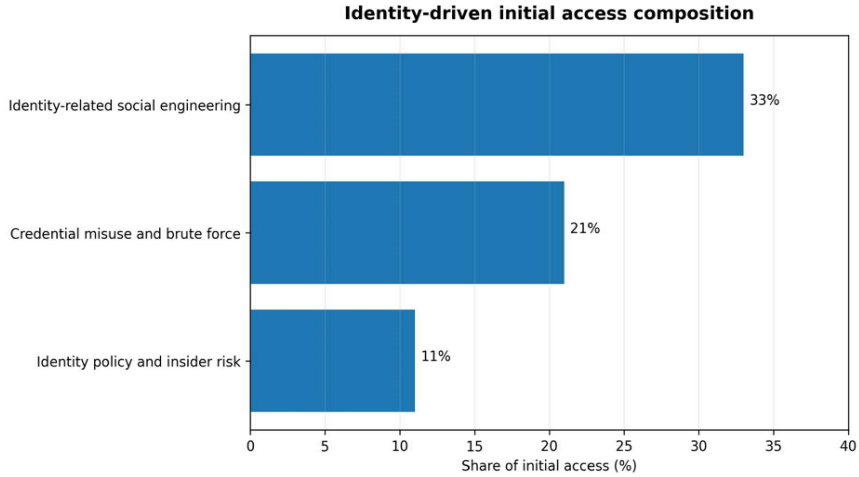

Figure 3. Composition of identity-driven initial access. The three route groups sum to the report's 65% identity-driven initial-access estimate

Figure 3 presents the composition of identity-driven initial access, which collectively accounts for 65% of the reported initial-access activity. Identity-related social engineering is the largest component at 33%, followed by credential misuse and brute force at 21%, and identity policy and insider risk at 11%. The social engineering component includes identity-based phishing (22%) and other social engineering (11%). Credential misuse and brute force comprise previously compromised credentials (13%) and brute force (8%), while identity policy and insider risk include IAM misconfigurations (3%) and insider threats (8%).

The distribution demonstrates that identity related compromise is not attributable to a single technique. Social engineering represents the largest reported route, while compromised credentials and weaknesses in identity governance provide additional pathways. This pattern highlights the need to combine phishing-resistant authentication, credential monitoring, privileged access controls, and continuous assessment of identity configurations. The figure should be interpreted as a composition of the reported identity-driven initial access categories, not as an independent estimate of all cyberattack mechanisms.

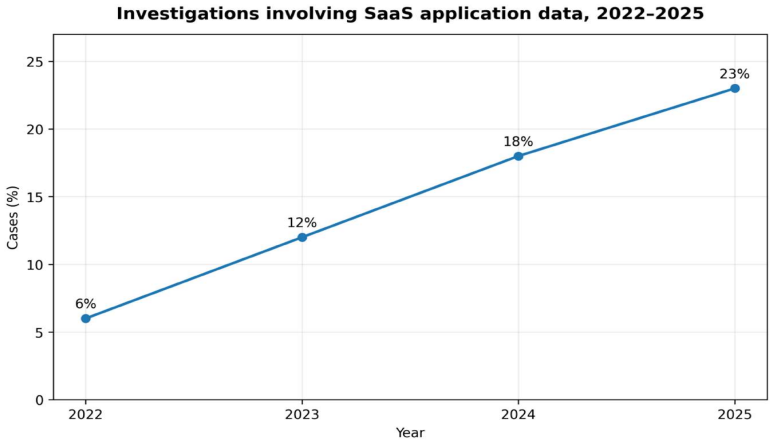

Figure 4. Investigations involving SaaS application data, 2022–2025

Figure 4 depicts the increase in the proportion of investigations involving SaaS application data over four consecutive years. The reported share rose from 6% in 2022 to 12% in 2023, increased further to 18% in 2024, and reached 23% in 2025. This consistent upward pattern represents a 17-percentage point increase between the first and final years shown.

The figure highlights the growing relevance of SaaS environments in incident response investigations. As organizational data and business processes increasingly rely on cloud hosted applications, SaaS platforms and their integrations become important elements of the cybersecurity environment. The trend supports extending monitoring and security governance to application identities, access permissions, connected services, and data movement across SaaS platforms. However, the figure represents the proportion of investigations involving SaaS application data; it does not establish a causal relationship between SaaS adoption and incident occurrence

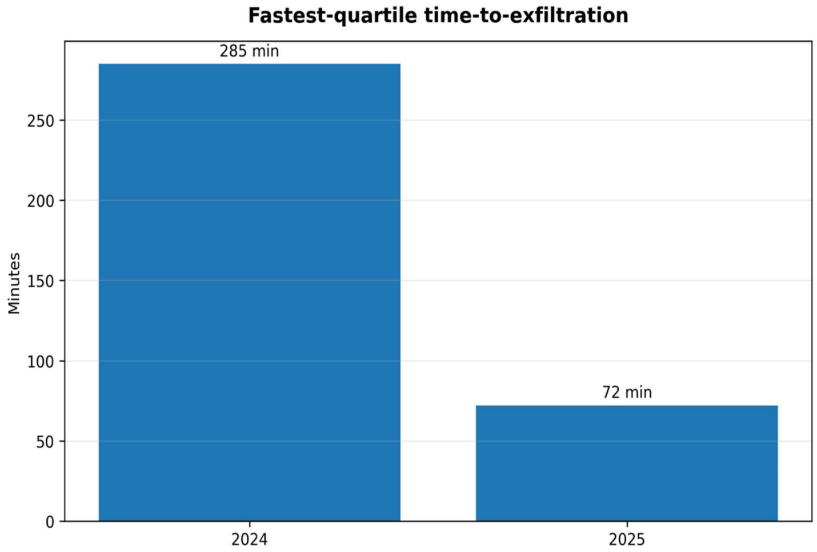

Figure 5. Fastest-quartile time-to-exfiltration in 2024 and 2025

Figure 5 compares the fastest-quartile time-to-exfiltration in 2024 and 2025. The reported value decreased from 285 minutes in 2024 to 72 minutes in 2025, representing an approximately 74.7% reduction. This substantial decline indicates that the fastest-moving incidents in the reported dataset reached the exfiltration stage considerably sooner in 2025 than in the preceding year.

The result has important implications for incident detection and response. Traditional security processes that depend on delayed alert review or manual investigation may provide insufficient response time when data exfiltration occurs rapidly. Organizations therefore require continuous monitoring, timely detection of suspicious access and data transfer behavior, and automated containment mechanisms. The figure concerns the fastest quartile rather than the median or average incident, and its interpretation should remain specific to this segment of the reported cases.

Figure 6 illustrates the changes in three reported extortion tactics encryption, data theft, and harassment between 2021 and 2025. Encryption remained the most frequently reported tactic throughout the period, although its prevalence decreased from 96% in 2021 to 78% in 2025. The most notable recent reduction occurred between 2024 and 2025, when encryption declined from 92% to 78%. Data theft showed comparatively limited variation, ranging from 53% to 60% and reaching 57% in 2025. Harassment remained the least frequently reported tactic, with values between 5% and 13%.

The figure demonstrates that extortion strategies can involve multiple forms of pressure. Although encryption remained prominent, the continued occurrence of data theft indicates that attackers may use the threat of

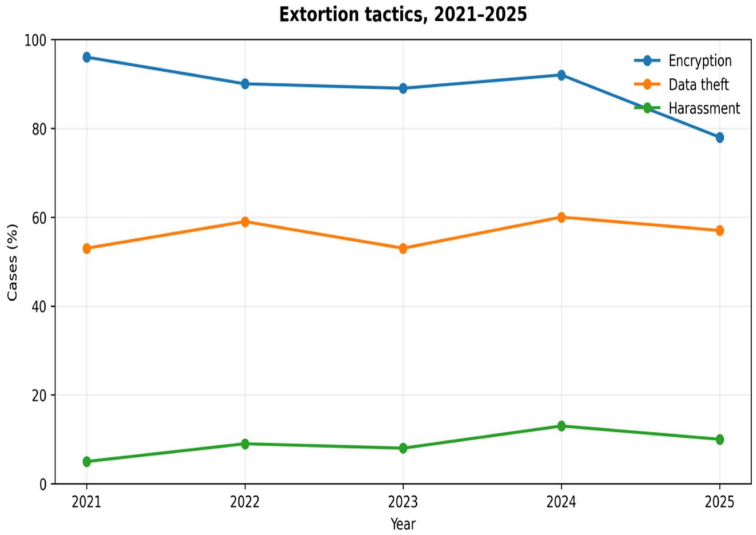

Figure 6. Extortion tactics from 2021 to 2025

information disclosure as an extortion mechanism. Harassment may provide an additional means of pressuring affected organizations. The pattern reinforces the need for organizations to protect sensitive information and prepare for data disclosure threats, rather than treating ransomware defense solely as a matter of preventing file encryption.

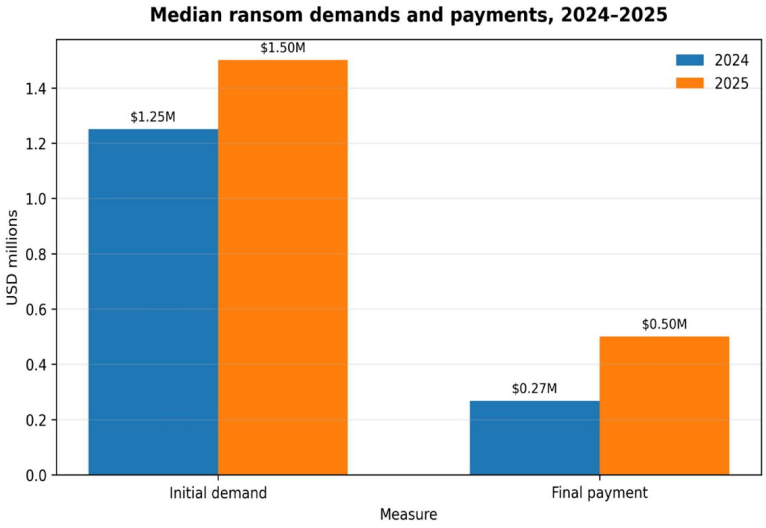

Figure 7. Median ransom demands and payments in 2024 and 2025

Figure 7 compares median initial ransom demands and median ransom payments for 2024 and 2025. The median initial demand increased from USD 1.25 million in 2024 to USD 1.5 million in 2025. Median payments also increased, from USD 267,500 to USD 500,000. The figure therefore demonstrates an increase in both the requested and paid ransom amounts over the two-year comparison.

The difference between initial demands and payments also illustrates the role of negotiation in the reported cases. The associated median reduction from the initial demand to the payment increased from 53% in 2024 to 61% in 2025. However, the monetary increases should be interpreted alongside the report's revenue-normalized indicators: initial demands and payments represented smaller proportions of perceived annual

revenue in 2025 than in 2024. Thus, the absolute amounts and their relative financial burden provide different perspectives on ransom economics.

The figure is descriptive and does not establish the factors responsible for changes in ransom demands or payments. It should also be read in conjunction with the revenue-normalized values in Table 8.

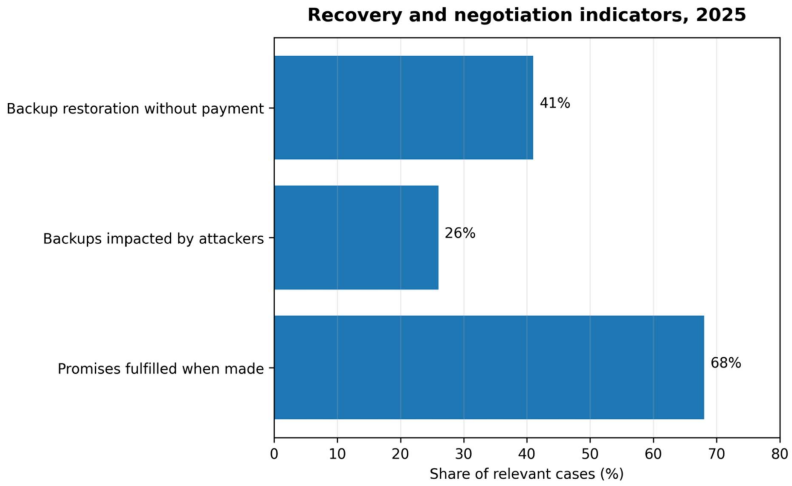

Figure 8. Backup restoration, backup impact, and promise-fulfilment indicators

Figure 8 presents three indicators relating to recovery and extortion negotiations. The figure shows that 41% of victims were able to restore from backups without paying a ransom. At the same time, backups were impacted in 26% of extortion cases. The report further indicates that threat actors fulfilled promises in 68% of cases in which promises were made.

The juxtaposition of backup restoration and backup impact is particularly important. Although backup availability enabled a substantial proportion of victims to recover without paying, the reported impact on backups demonstrates that attackers may also target recovery resources. This supports the use of isolated or immutable backups, regular recovery testing, and clearly defined recovery procedures. The promise-fulfilment indicator provides context about reported negotiation outcomes, but it should not be interpreted as evidence that threat actors can be trusted or that negotiating with them is a dependable recovery strategy.

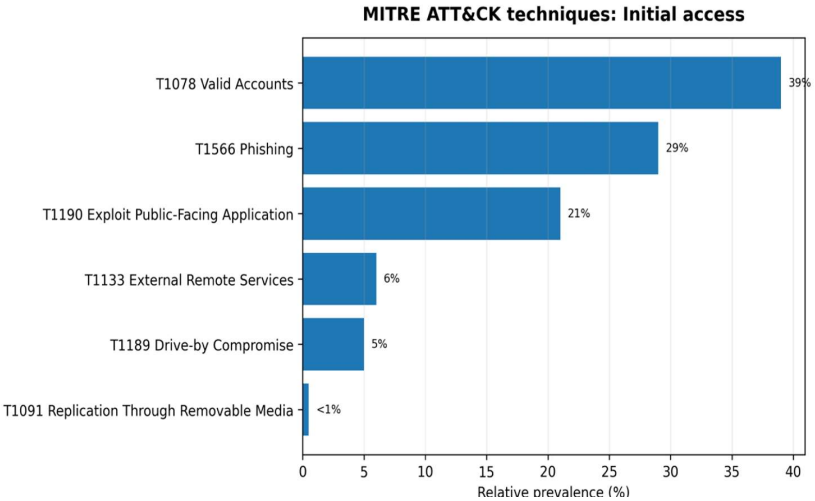

Figure 9. Relative prevalence of MITRE ATT&CK initial-access techniques

Figure 9 presents the relative prevalence of selected MITRE ATT&CK techniques associated with initial access. Valid Accounts (T1078) is the leading listed technique at 39%, followed by Phishing (T1566) at 29% and Exploit Public-Facing Application (T1190) at 21%. External Remote Services (T1133) accounts for 6%, while Drive-by Compromise (T1189) represents 5%. Replication Through Removable Media (T1091) is reported at less than 1%.

The figure emphasizes the importance of account security and phishing defenses within the reported initial-access technique profile. The contribution of exploitation of public-facing applications further indicates that externally accessible software requires continuous vulnerability assessment and timely remediation. These findings suggest that defensive measures should combine strong authentication, monitoring of suspicious account use, phishing protection, and vulnerability management.

Importantly, the displayed percentages represent relative prevalence among techniques identified for the initial-access tactic. They do not indicate the percentage of incidents in which each technique occurred.

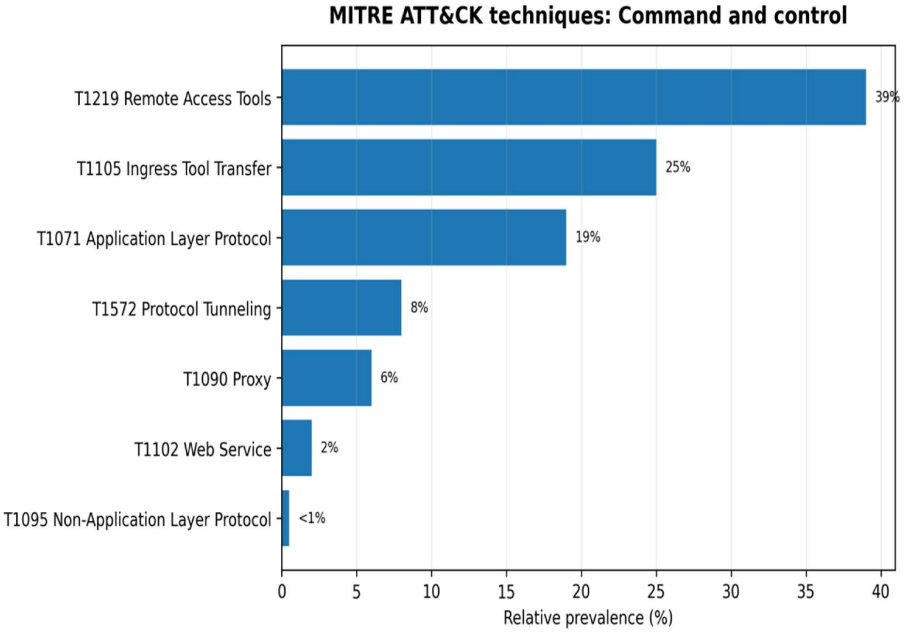

Figure 10. Relative prevalence of MITRE ATT&CK command-and-control techniques

Figure 10 illustrates the relative prevalence of selected command-and-control techniques. Remote Access Tools (T1219) account for the largest reported share at 39%, followed by Ingress Tool Transfer (T1105) at 25% and Application Layer Protocol (T1071) at 19%. Protocol Tunneling (T1572) contributes 8%, while Proxy (T1090) accounts for 6%. Web Service (T1102) represents 2%, and Non-Application Layer Protocol (T1095) is reported at less than 1%.

The results indicate that remote-access tools and the transfer of tools into compromised environments are important elements of the reported command-and-control technique profile. The contribution of application-layer protocols and tunneling also highlights the need to monitor communications that may blend with legitimate network traffic. Organizations should therefore maintain visibility into remote administration utilities, unusual outbound connections, unauthorized tool transfers, and suspicious use of communication protocols.

The percentages represent relative prevalence among techniques identified for the command-and-control tactic, not the proportion of investigated incidents involving each technique.

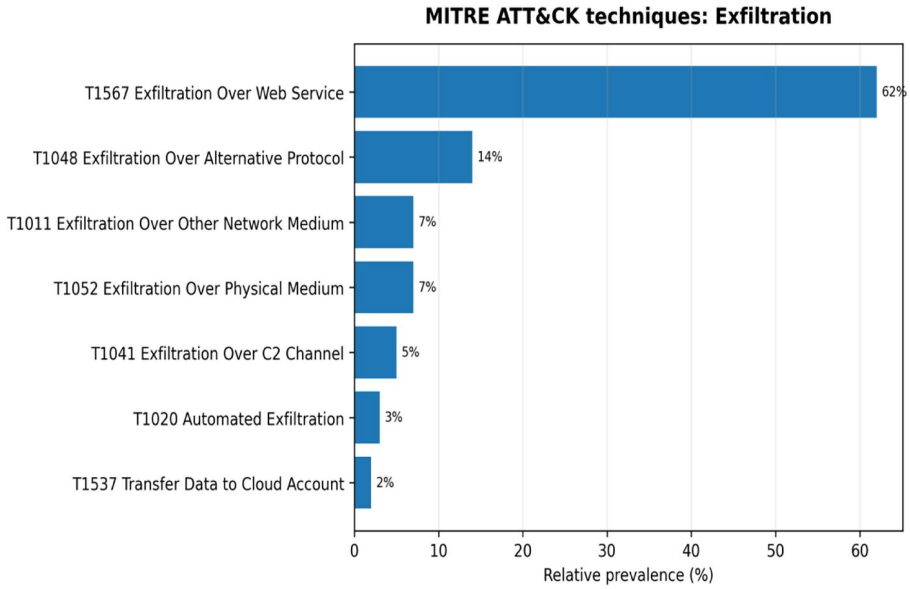

Figure 11. Relative prevalence of MITRE ATT&CK exfiltration techniques

Figure 11 presents the relative prevalence of selected techniques associated with data exfiltration. Exfiltration Over Web Service (T1567) is the most prominent technique, accounting for 62% of the listed relative prevalence. Exfiltration Over Alternative Protocol (T1048) represents 14%, while Exfiltration Over Other Network Medium (T1011) and Exfiltration Over Physical Medium (T1052) each account for 7%. Exfiltration Over C2 Channel (T1041) contributes 5%, Automated Exfiltration (T1020) accounts for 3%, and Transfer Data to Cloud Account (T1537) represents 2%.

The predominance of web service based exfiltration highlights the importance of monitoring outbound data transfers and identifying unusual use of web based services. The presence of alternative protocols, network media, physical media, and command and control channels demonstrates that data removal can occur through multiple technical pathways. Consequently, organizations should implement data loss prevention controls, monitor abnormal outbound traffic, review cloud data-sharing activity, and correlate network events with identity and endpoint telemetry.

The figure describes relative prevalence within the exfiltration tactic, rather than incident-level occurrence rates. Its results should therefore be interpreted as a distribution of the techniques identified in the report, not as the probability that a particular incident will use a given exfiltration method.

5. Overall interpretation

To sum up the tables and figures reveal several interconnected characteristics of the cybersecurity incidents examined in the Unit 42 Global Incident Response Report 2026. First, identity-related weaknesses constitute a major component of the reported threat environment. The high involvement of identity systems, the prevalence of excessive cloud permissions, and the contribution of compromised credentials and social engineering demonstrate the importance of identity-centric security controls.

Second, the findings highlight the increasingly interconnected nature of cyber incidents. The involvement of multiple attack surfaces, the growing relevance of SaaS application data, and the reported supply-chain vulnerabilities indicate that organizational security cannot be addressed exclusively through endpoint protection or perimeter based defenses. Effective protection requires visibility across identity systems, endpoints, networks, cloud environments, SaaS applications, and software dependencies.

Third, the findings demonstrate the importance of attack velocity and data protection. The reduction in fastest quartile exfiltration time suggests that organizations have limited opportunities to detect and contain some incidents before sensitive information is removed. The extortion results further demonstrate that data theft, encryption, and harassment can contribute to attacker pressure, while the backup indicators emphasize the importance of resilient recovery mechanisms.

Finally, the MITRE ATT&CK technique distributions provide a structured view of the reported adversarial activities across different stages of an intrusion. The prominence of Valid Accounts, Phishing, Remote Services, Remote Access Tools, and Exfiltration Over Web Service identifies several areas that deserve attention in defensive monitoring and security control design.

6. Limitations

The source is an industry incident response report rather than a machine readable research dataset. The values are descriptive aggregates selected by the report authors. Some denominators vary by metric, some categories overlap, and the report does not disclose all underlying counts or year by year values in tabular form. Accordingly, this package does not calculate confidence intervals, significance tests, correlations, regressions, or predictive models from these aggregates.

7. Conclusion

The analysis of the 2026 global incident response data reveals a cybersecurity landscape defined by extreme interconnectedness, identity centric exploitation, and blistering attack velocity. The findings lead to several definitive conclusions.

1. Identity is the New Perimeter: With identity involved in 89% of intrusions and 99% of analyzed cloud identities possessing excessive permissions, the traditional network perimeter is irrelevant. Security strategies must pivot to identity centric governance, continuous authentication monitoring, and strict privileged-access management.

2. The Reality of Multi-Surface Warfare: The vast majority of incidents (87%) span multiple attack surfaces. Defenses can no longer rely on isolated endpoint protection or email gateways; they require unified visibility across identity, network, cloud, and human attack surfaces.

3. Speed Dictates Survival: The reduction of the fastest quartile time to exfiltration to just 72 minutes proves that organizations are losing the race against automated and highly optimized threat actors. Defense strategies must incorporate automated detection, behavioral analytics, and rapid containment capabilities.

4. Extortion and Recovery Resilience: The evolution of extortion tactics where data theft and harassment are leveraged alongside or instead of encryption means that data loss prevention and sensitive data monitoring are as critical as anti ransomware tools. Furthermore, while 41% of victims recovered via backups, the fact that attackers targeted backups in 26% of cases underscores the absolute necessity of isolated, immutable backup architectures.

5. Supply Chain and SaaS Blind Spots: The steady rise in SaaS related incidents (reaching 23% in 2025) and the high prevalence of vulnerabilities in transitive cloud native libraries indicate that third party software integrations are major vectors for compromise. Software composition analysis and SaaS identity monitoring must become standard operational practices.

Ultimately, surviving the modern threat landscape requires abandoning fragmented, reactive security models. Organizations must adopt a holistic, proactive, and data-driven approach that assumes identity compromise, monitors for rapid data exfiltration, and guarantees business continuity through rigorously tested, resilient recovery architectures.

References

[1] Foulon, M., Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy, 45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062.

[2] Li, Y., Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126.

[3] Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal, 38*(29). https://doi.org/10.1057/s41284-025-00471-7.

[4] Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology, 9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671.

[5] Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science, 10*, e1772. https://doi.org/10.7717/peerjcs.1772.

[6] Islam, M. S., Xiangdong, L. (2025). *Guardians of the web: The evolution and future of website information security* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2505.04308.

[7] Smith, S. E. (2021). *An analysis of significant cyber incidents and the impact on the past, present, and future* [Undergraduate research project]. ODU Digital Commons. https://digitalcommons.odu.edu/covacci-undergraduateresearch/2021fall/projects/12.

[8] Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., Asif, M. (2020). Man in the middle attacks: Analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security, 8*, 52–58.

[9] Niño, F. Y. Á. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes, 24*, 92–119.

[10] Konsta, A. M., Lafuente, A. L., Spiga, B., Dragoni, N. (2024). Survey: Automatic generation of attack trees and attack graphs. *Computers & Security, 137*, 103602.

[11] Zhang, J., Zheng, J., Zhang, Z., Chen, T., Tan, Y. A., Zhang, Q., Li, Y. (2024). ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. *Computer Networks, 245*, 110376.

[12] Bhardwaj, A., Sapra, V. (2020). Why is phishing still successful *Computer Fraud Security, 2020*, 15–19.

[13] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation. (2021). *TrickBot malware* (AA21-076A). https://www.cisa.gov.

[14] Álvarez, A. L., Cruz, J. A., Cruz, S. B., Gallardo, J. D. C., López, I. M., García, R. E. (2024). El phishing como amenaza en la ciberseguridad corporativa de grandes empresas. *Investigación Latinoamericana en Ingeniería y Arquitectura, 1*, 26–33.

[15] Palo Alto Networks. (2025). *Lucifer: New cryptojacking and DDoS hybrid malware exploiting high and critical vulnerabilities to infect Windows devices*. Unit 42. https://unit42.paloaltonetworks.com.

[16] Gelgi, M., Guan, Y., Arunachala, S., Rao, M. S. S., Dragoni, N. (2024). Systematic literature review of IoT botnet DDoS attacks and evaluation of detection techniques. *Sensors, 24*, 3571.

[17] Wu, Q., Zhang, S., Zheng, B., You, C., Zhang, R. (2021). Intelligent reflecting surface aided wireless

communications: A tutorial. *IEEE Transactions on Communications, 69*, 3313–3351.

[18] de Nobrega, K. M., Rutkowski, A. F., Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *Journal of Strategic Information Systems, 33*, 101861.

[19] Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence, 2*, 455–513.

[20] Rabitti, G., Chokami, A. K., Coyle, P., Cohen, R. D. (2024). A taxonomy of cyber risk taxonomies. *Risk Analysis, 45*, 376–386.

[21] MITRE. (2025). ATT&CK: *Adversarial tactics, techniques, and common knowledge*. https://attack.mitre.org/

[22] Al-Sada, B., Sadighian, A., Oligeri, G. (2023). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *IEEE Access, 11*, 70560–70573.

[23] Al-Sada, B., Sadighian, A., Oligeri, G. (2025). MITRE ATT&CK: State of the art and way forward. *ACM Computing Surveys, 57*, 1–37.

[24] Li, L., Huang, C., Chen, J. (2024). Automated discovery and mapping ATT&CK tactics and techniques for unstructured cyber threat intelligence. *Computers Security, 140*, 103815.

[25] Sun, H., Shu, H., Kang, F., Zhao, Y., Huang, Y. (2024). Malware2ATT&CK: A sophisticated model for mapping malware to ATT&CK techniques. *Computers Security, 140*, 103772.

[26] Branescu, I., Grigorescu, O. C., Dascalu, M. (2024). Automated mapping of CVEs to MITRE ATT&CK tactics. *Information, 15*, 214.

[27] Son, S. B., Park, S., Lee, H., Kim, Y., Kim, D., Kim, J. (2023). Introduction to MITRE ATT&CK: Concepts and use cases. In *2023 International Conference on Information Networking (ICOIN)* (p. 158–161). IEEE.

[28] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy* [Technical report]. The MITRE Corporation.

[29] Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., Sikdar, B. (2025). *MITRE ATT&CK applications in cybersecurity and the way forward* [Preprint]. arXiv. https://arxiv.org/abs/2502.10825.

[30] Al-Sada, B., Sadighian, A., Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. *Computing Surveys, 57*(1), 1–37.

[31] Alexander, O., Belisle, M., Steele, J. (2020). *MITRE ATT&CK for industrial control systems: Design and philosophy*. The MITRE Corporation.

[32] Unit 42. (2026). *Global incident response report 2026*. Palo Alto Networks.