

The background of the entire page is a light purple color. It features several large, dark purple, organic, and flowing shapes that overlap each other, creating a sense of depth and movement. These shapes are primarily located in the top left, middle, and bottom right areas.

Securin

2024

Ransomware Index

A threat and vulnerability management perspective.

When Gen-AI Met Ransomware:

The Year the Machines Joined the Mayhem

Ransomware in 2024 was no longer *just* about encryption: it was about control, persistence, and maximum disruption. It was also the year that artificial intelligence (AI) entered the chat: while security teams were busy training it to detect threats, the ultimate plot twist saw attackers using it to create malware that other AI systems couldn't detect. Overall, Securin's research shows that 2024 was a year of sophistication, collaboration, evolution, and strategic thinking – for ransomware attackers.

What's Keeping Us Up at Night:

Key Findings & Trends



AI-Assisted Ransomware Ops

RansomAI was the evolution of a nightmare scenario. The ransomware group **FunkSec** provided a compelling example of how generative artificial intelligence (GenAI) is lowering the barrier to entry for sophisticated attacks.



2. Old Groups, New Tricks

Cross-collaboration between ransomware groups, multi-stage attack strategies, and sophisticated persistence mechanisms are the new normal.



3. Healthcare Feels the Pain

With **14.5% of attacks**, healthcare bore the brunt of the ransomware pain as attackers turned their attention to critical sectors.



4. APT is a PITA

Attackers adopted an '**Advanced Persistent Threat**' strategy, seeking lateral movement and persistence, with more strategic targeting making it more difficult for security teams to cover defenses.



5. Access All Areas

Authentication and access control vulnerabilities dominated the ransomware exploit toolkit.

Bottom Line: This evolution represents a significant challenge for defenders, as it combines the persistence of ransomware groups with increasingly sophisticated exploitation techniques. Attackers are no longer simply looking for ways in; they're strategically selecting vulnerabilities that provide the broadest possible access, and the greatest chance of success.

What's In This Report?

**01**

Generative AI as both tool and target, and the emergence of RansomAI.

02

Profile of the main threat actors, their tactics and techniques.

03

Top weaknesses being exploited - and which sectors are under fire.

04

Most common attack patterns - and what we can learn from them.

05

Best practices for mitigating the threats.

Dr. Srinivas Mukkamala | Securin Advisor



AI-generated polymorphic ransomware, paired with adaptive exploit code, poses a severe threat by evading current EDRs and security tools. This fast-evolving malware chains CVEs into complex attack sequences, exploiting system weaknesses at scale and risking massive financial losses.

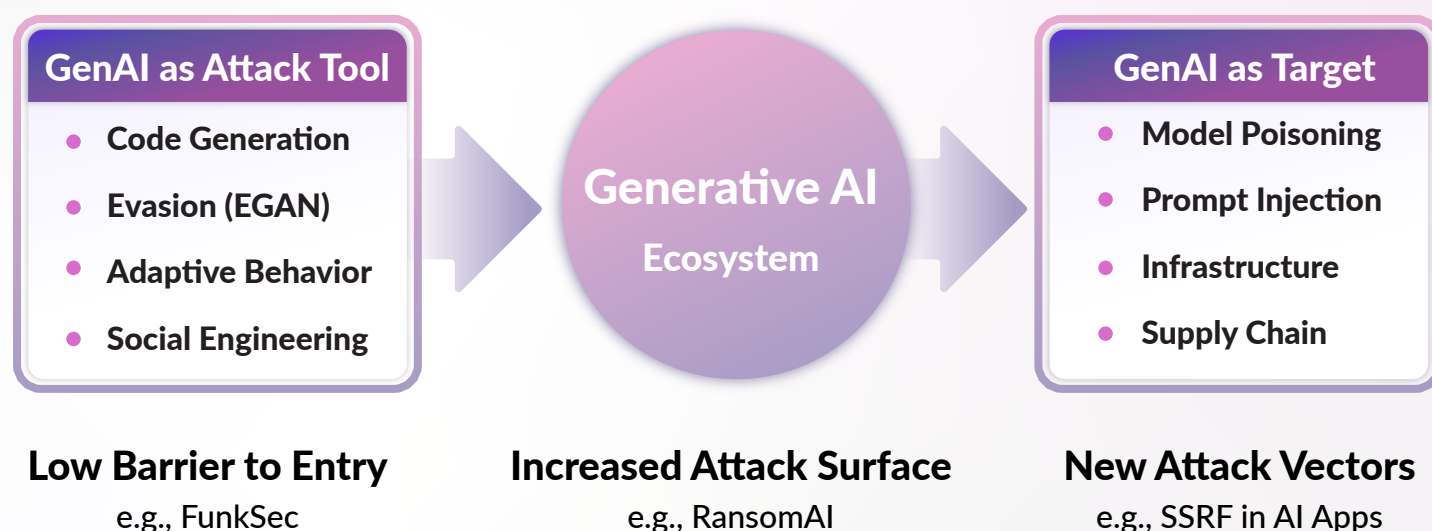
Preemptive security is critical—proactively remediating vulnerabilities before they're hit. We must shift from prioritizing single CVEs to analyzing CVE chains, using machine learning to predict attack paths and bolster defenses.

Adaptive security technology that learn ransomware's tricks are key. Without this evolution in cybersecurity, AI-driven ransomware will outpace us, turning vulnerabilities into weapons. Vigilance and innovation are non-negotiable.

AI-Powered Ransomware: The Democratization of Ransomware Development

The emergence of AI-assisted ransomware operations in 2024 represented a significant shift in the cybercrime ecosystem. As GenAI is increasingly integrated into both offensive and defensive operations, the threat landscape is being transformed in ways that demand immediate attention.

Dual Impact of GenAI on Ransomware Operations



SPOTLIGHT: FunkSec - All of the Damage, None of the Experience

The emergence of FunkSec – an AI-assisted ransomware operation – provided a compelling example of how GenAI lowers the barrier to entry for sophisticated attacks. Despite evidence that it's operated by relatively inexperienced actors, FunkSec showed remarkable effectiveness, claiming over 100 victims with its double-extortion tactics and AI-assisted tool development – maximizing impact, maintaining low operational costs and surpassing the efforts of established groups like ClOp and Akira.

If many questioned the credibility of FunkSec's claims, the EGAN framework showed us just how bad things could get...



AI vs AI: The EGAN Framework

Documented by researchers, the [Evolutional Generative Adversarial Network \(EGAN\) framework](#)¹ demonstrates the power of adversarial machine learning in creating highly evasive, polymorphic ransomware variants. **For threat actors and defenders alike, this is next level: it's not just about avoiding detection, it's about learning from each encounter and becoming more effective.**

EGAN's success in bypassing AI-powered antivirus systems highlighted GenAI's capacity to automate the process of creating detection-evasive malware. The framework demonstrates how reinforcement learning can be used to create ransomware that dynamically adjusts its behavior to maximise damage, while retaining stealth. The researchers' success in bypassing commercial security solutions underlines the growing sophistication of AI-assisted malware development

RansomAI: Testing Out Your Worst Nightmares

Perhaps even more concerning than automated malware development is the emergence of adaptive ransomware systems like RansomAI. Created for research purposes, in controlled experiments, it gave some insight into what an AI-powered ransomware future could look like, and it's not pretty:

- 90% success rate in evading detection while encrypting files.
- Adaptive encryption where RansomAI learned to optimize itself.
- Automated attack process from reconnaissance to execution.
- Intelligent detection evasion used to avoid dynamic defenses, mechanisms, and anomaly detection systems.

AI Systems as High-Value Targets

The proliferation of AI systems has created new attack surfaces that ransomware operators are beginning to exploit. Microsoft's red team identified several critical vulnerabilities in AI infrastructure that could be leveraged by ransomware operators:

Cross-Prompt Injection Attacks

Cross-Prompt Injection Attacks pose a particular threat to AI systems, allowing malicious actors to bypass security controls and manipulate AI systems into performing unauthorized actions. Microsoft's success in creating an automated scamming system using a combination of large language models (LLM) and text-to-speech technologies illustrates how these vulnerabilities could be weaponized at scale.

Supply Chain Attacks

Supply chain attacks against AI systems represent another emerging threat vector. The discovery of a Server-Side Request Forgery (SSRF) vulnerability in a video-processing GenAI application demonstrates an uncomfortable new truth: traditional security vulnerabilities don't just persist in AI systems, they get amplified. This finding underscores the importance of maintaining robust security practices even as organizations rush to adopt AI technologies.

Evolving Defense Strategies to Meet Emerging AI Threats

The cybersecurity community's response to emerging AI-ransomware and malware threats must be multifaceted. Microsoft's open-source [Python Risk Identification Tool for generative AI \(PyRIT\) framework](#)² is helping standardize AI red teaming practices, enabling organizations to adopt a proactive approach. But, as Microsoft notes: "The work of securing AI systems will never be complete."

Reality Check: For every AI model there's a prompt that can elicit undesired behavior. Perfect security isn't the goal – making attacks economically unfeasible is.

Key Defensive Approaches to AI-Generated Threats

In 2024, the AI threat landscape evolved beyond theory, underlining the real-world implications of AI-powered ransomware. Best defense approaches include:

- 1. Developing comprehensive strategies to understand and address both AI-enabled attacks and AI-specific vulnerabilities.**
- 2. Combining automated testing frameworks with human expertise and continuous security improvement.**
- 3. Maintaining strict security practices during AI adoption, recognizing that speed of implementation should not compromise security.**

While this technology enables more sophisticated attacks with lower barriers to entry, it also provides new opportunities for defense. Proper security practices, continuous testing, and adaptive defense strategies are key to taking a proactive approach to emerging and evolving threats.

Ransomware Main Players

The Usual Suspects? Who's Attacking?

While AI was busy moving the goalposts, the established ransomware groups were also upping their game. 2024 saw all of the major groups demonstrate increasing sophistication. Despite law enforcement disruption, LockBit maintained its position as a dominant threat in ransomware. The group's rapid recovery following significant global crackdown showed worrying levels of resilience and de-centralized infrastructure. Meanwhile, new ransomware groups like RansomHub and MedusaLocker emerged, while established actors like Cl0p continued their pattern of exploiting file transfer vulnerabilities. We also saw the emergence of groups focused specifically on cloud environments, software supply chains and crypto exchanges. Here's our analysis of the major players:

2024's Most Wanted: The Top Six Notable Ransomware Operators



Primary Targets:
Government | Manufacturing | Financial



Primary Targets:
IT | Manufacturing | Energy



Primary Targets:
Education | Financial | Healthcare



Primary Targets:
Healthcare | Manufacturing | Infrastructure



Primary Targets:
Water Systems | Healthcare | Government



Primary Targets:
Healthcare | Financial

In The Firing Line: Which Sectors Are Under Attack

As [Securin's in-depth report](#)³ on critical sector attacks revealed, 2024 marked a deeply concerning pattern of threats to essential services. Our ransomware data underlines this trend, with healthcare the most vulnerable sector at 14.5% of attacks. The sophistication of attacks, exemplified by groups like LockBit and Black Basta, suggests an evolution in tactics that poses an unprecedented challenge to national security and public safety.

2024 Ransomware Attacks By Industry

 Healthcare & Public Health	14.5% of attacks	 Communications	1.6% of attacks
 Information Technology	10.3% of attacks	 Defense	1% of attacks
 Manufacturing	9.1% of attacks	 Entertainment	1% of attacks
 Government & Public Sector	8.5% of attacks	 Food & Agriculture	0.9% of attacks
 Education	5.5% of attacks	 Hospitality	0.4% of attacks
 Transportation & Logistics	5.3% of attacks	 Water & Wastewater Systems	0.3% of attacks
 Financial Services	5.2% of attacks	 Chemical	0.1% of attacks
 Energy	2.6% of attacks	 Dams	0.1% of attacks

Severity Scale:  High → Low

Ripple Effects Across Interconnected Infrastructure

While healthcare bears the brunt of these attacks, the ripple effects extend throughout our interconnected infrastructure. Information technology firms, the backbone of digital services, faced 10.3% of attacks that threatened to disrupt countless downstream organizations. Manufacturing facilities experienced 9.1% of attacks, creating supply chain vulnerabilities that reach far beyond factory walls. The targeting of government facilities (8.5%) and transportation systems (5%) completes a troubling picture of comprehensive threats to critical infrastructure. These aren't isolated incidents, but rather a co-ordinated assault on fundamental systems. The energy sector, though experiencing fewer attacks, faces some of the most sophisticated threats. Notable incidents like the [Schneider Electric breach, where 1.5TB of corporate data was stolen](#)⁴, demonstrate how these attacks could potentially disrupt power distribution and critical energy infrastructure.

Hacker Hotspots:

Top Weaknesses Being Exploited by Ransomware Actors

Securin’s analysis of weaknesses exploited by ransomware in 2024 reveals a clear focus on authentication and access control vulnerabilities. Improper Authentication (CWE-287) emerges as the most commonly exploited weakness, often paired with Authentication Bypass (CWE-288) and Missing Authentication (CWE-306), indicating that ransomware attackers are primarily targeting vulnerabilities that allow them to circumvent security controls rather than exploit memory corruption issues. The next most significant clusters of weakness are:

Memory-Related Vulnerabilities

Including buffer operations and out-of-bounds writes (CWE-119, CWE-787). These are particularly concerning because they often lead to code execution capabilities. The presence of Use After Free (CWE-416) vulnerabilities in multiple security products suggests that ransomware operators are also targeting more sophisticated memory corruption vulnerabilities that require deeper technical expertise to exploit.

Misconfiguration and Design Flaws

The exploitation of Path Traversal (CWE-22) and Incorrect Default Permissions (CWE-276) shows that ransomware groups are leveraging misconfigurations and design flaws in addition to implementation vulnerabilities.

Evolving Defense Strategies to Meet Emerging AI Threats

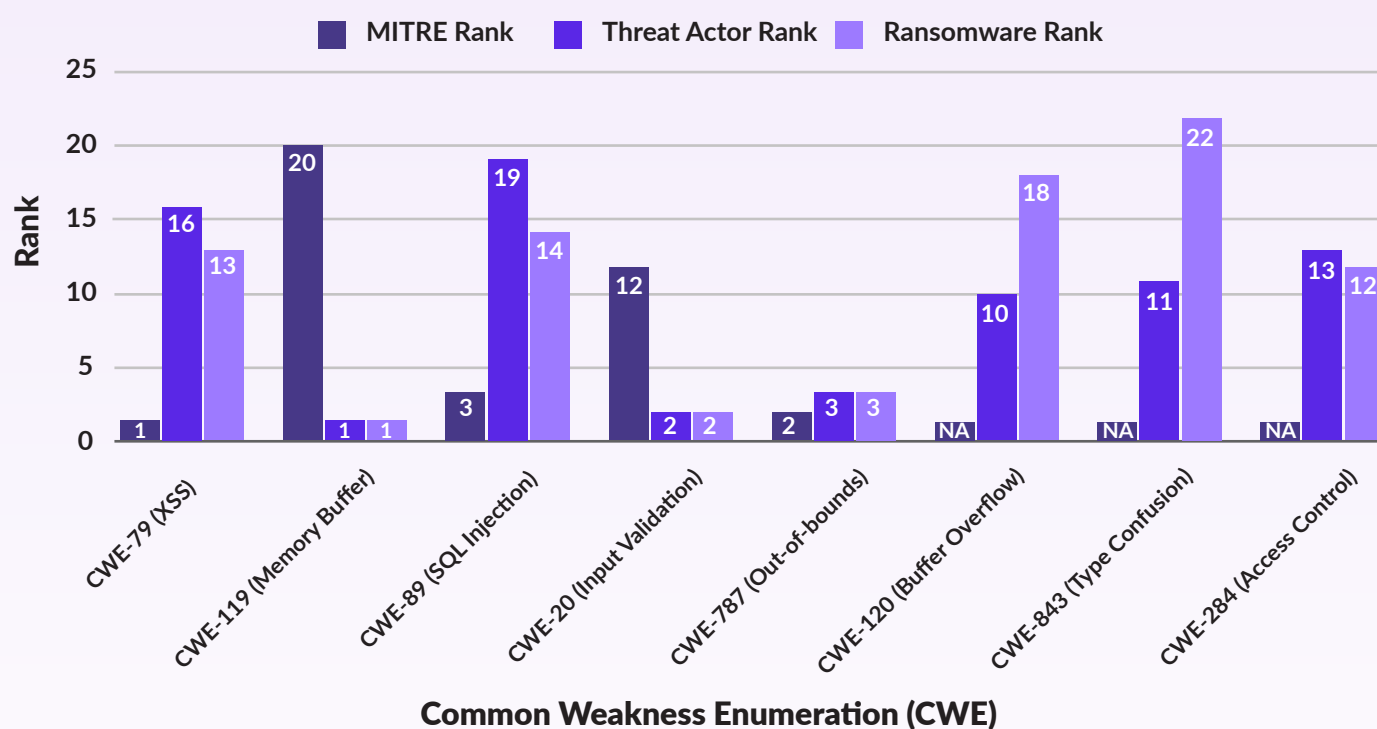
CWE ID	Weakness Name	Count
CWE-287	Improper Authentication	5
CWE-119	Improper Restriction of Operations within Memory Buffer	3
CWE-787	Out-of-Bounds Write	3
CWE-288	Authentication Bypass Using Alternative Path	3
CWE-276	Incorrect Default Permissions	2
CWE-306	Missing Authentication for Critical Function	2
CWE-416	Use After Free	2
CWE-22	Path Traversal	2
CWE-94	Code Injection	2

What can we learn from the data? This multi-vectored approach to weakness exploitation suggests that attackers have a mature understanding of enterprise software vulnerabilities - and the ability to exploit both simple and complex weaknesses.

Mind the Gap(s): Discrepancies Between MITRE Rankings and Real-World Attacks

Securin's analysis of MITRE's 2024 Top 25 Common Weakness Enumerations (CWEs) reveals a striking misalignment between standardized rankings and real-world exploitation.

Top Discrepancies: MITRE vs Threat Actor & Ransomware Rankings



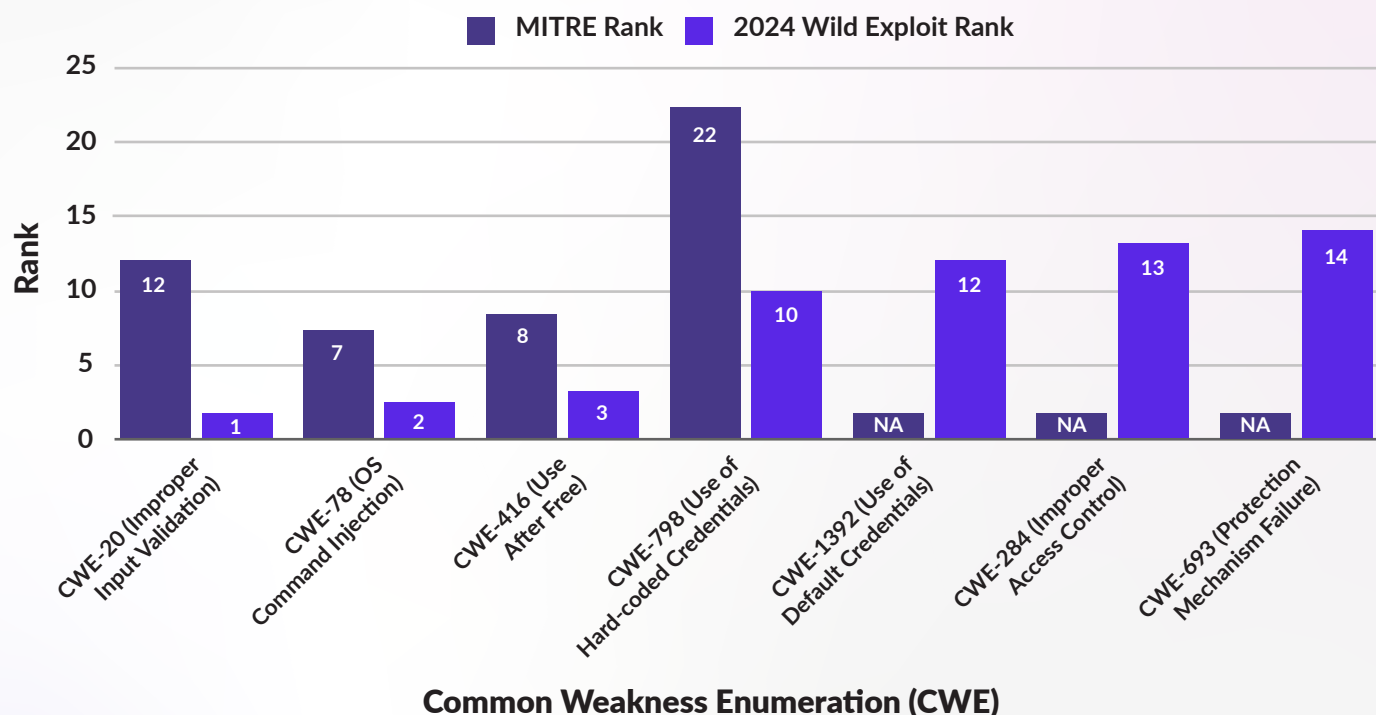
For example, vulnerabilities such as Memory Buffer Operations and Improper Input Validation are under-represented in MITRE's Top 25, but dominate real-world attack patterns and exploitation. In fact, Memory Buffer Operations is the most dramatic under-ranking in the MITRE list: this weakness consistently ranks as the #1 target for both threat groups and ransomware operators.

Memory-related weaknesses, such as buffer overflows and use-after-free issues, are frequently leveraged in sophisticated attacks due to their potential for arbitrary code execution and privilege escalation. Adversaries exploit these flaws to gain footholds in systems, deploy ransomware, and execute remote code with elevated privileges. Security teams need to prioritize vulnerabilities based on real-world exploitation data rather than relying solely on predefined lists.

The Implications of MITRE Ranking Disparities for Ransomware

The tech world has moved beyond simple web applications, and the cybercriminals have followed suit. Their focus is on weaknesses that allow direct pathways to privilege escalation, and remote code execution. Securin's analysis of MITRE's top 25 CWEs in their real-world context underlines this reality: as the graph below shows, Buffer Overflow, Type Confusion, and Access Control weaknesses have become more lucrative for threat actors than XSS and SQL Injection.

Top Discrepancies: MITRE vs 2024 Exploited-in-the-Wild



What's notable here is the significant discrepancy between the MITRE ranking and the real-world threat and ransomware target. Again, we see how the concept of severity vs risk comes into play when we're looking at MITRE Top 25 rankings whose core calculation relies on the Common Vulnerability Scoring System (CVSS). For example, remote code execution vulnerabilities often operate as ransomware – doubling the likelihood of exploitation. And ransomware-associated vulnerabilities themselves are often part of broader campaigns leveraging multiple Known Exploited Vulnerabilities (KEVs).

The disparity between MITRE rankings and real-world exploitation patterns suggests a need for more dynamic and context-aware security prioritization frameworks. They also underline challenges around the need for context-aware rankings, resource allocation, and the evolution of security programs that are flexible enough to adapt to emerging threats.

Cracking the Code:

Key Trends in Patterns, Tactics, & Techniques

New CVEs Exploited by Ransomware in 2024



CVE-2024-51568 (CyberPanel) and **CVE-2024-1709 (ConnectWise ScreenConnect)** were among the most exploited vulnerabilities.



Multiple ransomware groups, including LockBit, Black Basta, and BlackCat, targeted **CVE-2024-1709**, indicating a rapid exploit-sharing culture.



JetBrains TeamCity (CVE-2024-27198) was exploited to compromise software development and deployment pipelines, shifting towards software supply chain attacks.



Cleo Harmony (CVE-2024-55956) exploitation by Clap reflects a continued focus on file transfer system vulnerabilities

Most Common Attack Patterns (CAPECs) Referenced in 2024 Ransomware CVEs

The attack patterns for ransomware in 2024 were characterized by sophisticated exploitation strategies, focused on circumventing authentication and gaining remote code execution capabilities.

CAPEC ID	Attack Pattern Name	Count
CAPEC-22	Exploiting Trust in Client	6
CAPEC-88	OS Command Injection	6
CAPEC-127	Directory Indexing	5
CAPEC-242	Code Injection	4
CAPEC-114	Authentication Abuse	4
CAPEC-115	Authentication Bypass	4
CAPEC-76	Manipulating Web Input to File System Calls	4
CAPEC-79	Using Slashes in Alternative Encoding	4
CAPEC-650	Upload a Web Shell to a Web Server	4
CAPEC-43	Exploiting Multiple Input Interpretation Layers	4

The prominence of “Exploiting Trust in Client” and “OS Command Injection” (see table above) indicates that attackers are primarily targeting vulnerabilities that allow them to bypass security controls and execute malicious commands with elevated privileges.

Key Trends in Ransomware Attack Patterns 2024

Securin's research reveals additional significant attack pattern trends:

1. Manipulation of Web-Based Inputs and Directory Traversal Techniques:



An emerging trend, with attackers leveraging multiple encoding methods to bypass security controls. The combination of Directory Indexing attacks with Web Shell uploads suggests a systematic approach to persistence once initial access is gained.

2. Authentication-Related Attack Patterns (Authentication Abuse & Bypass):



The increased frequency of authentication abuse/bypass alongside command injection techniques demonstrates a tactical progression: bypass security controls, then achieve code execution. More complex patterns like "Exploiting Multiple Input Interpretation Layers" indicates that ransomware operators have developed sophisticated technical capabilities and are able to chain multiple attack techniques together effectively.

3. Advanced Persistent Threat (APT) Tactics:



Our analysis suggests ransomware groups are increasingly adopting APT-like tactics, moving beyond simple encryption tools to sophisticated multi-stage attacks that leverage a diverse range of attack patterns.

Top Ransomware ATT&CK Tactics & Techniques 2024

Again, we're seeing a sophisticated attack cycle, combining opportunistic scanning with targeted attacks emphasizing discovery, persistence and evasion of defenses:

Initial Access:

Initial access is primarily gained through exploiting public-facing applications (T1190), followed by the high frequency of stolen/compromised credentials abuse (T1078) and external remote service exploitation (T1133).

Post-Compromise:

Post-compromise activities show a strong emphasis on discovery operations (T1082, T1083), indicating that ransomware groups are spending more time mapping networks before deploying payloads.

Taking Action:

Best Practices to Defend Against Ransomware

With all proactive security strategies, knowing your attack surface is half the battle. Here are seven concrete actions that defenders can take to mitigate the ransomware risks we've just looked at.

1. Prioritize Authentication & Access Control Vulnerabilities:

- Implement MFA across all systems, especially for privileged accounts and remote access.
- Deploy continuous monitoring for suspicious authentication attempts.
- Implement privileged access management (PAM) solutions.
- Consider Zero Trust architecture as a strategic goal.

2. Enhance Memory Protection Mechanisms:

- Deploy exploit prevention systems focused on memory corruption vulnerabilities.
- Implement memory protection tools like Control Flow Guard (CFG) and Address Space Layout Randomization (ASLR).
- Prioritize patching of memory-related vulnerabilities identified in this report (CWE-119, CWE-787, CWE-416).

3. Develop Sector-Specific Defense Strategies:

- Healthcare organizations: Focus on clinical system segmentation and resilience.
- Manufacturing: Implement OT/IT network separation with monitored interfaces.
- Government: Deploy advanced EDR solutions with behavioral analysis.
- Financial services: Enhance monitoring for novel lateral movement techniques.

4. Revise Vulnerability Prioritization Frameworks:

- Move beyond reliance on CVSS/MITRE rankings alone.
- Implement context-aware vulnerability management considering ransomware likelihood.
- Prioritize weaknesses commonly exploited in ransomware attacks in your sector.
- Monitor for exploitation chains rather than isolated vulnerabilities.

Ransomware Best Practices: Strategic Defensive Positioning

Adopt an APT-Focused Defensive Posture:



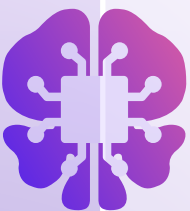
- Implement continuous threat hunting for persistent threats.
- Deploy deception technology to detect stealthy reconnaissance activities.
- Monitor for living-off-the-land techniques using legitimate system tools.
- Enhance visibility into lateral movement and privilege escalation attempts.

Establish Comprehensive Recovery Capabilities:



- Implement immutable backups beyond ransomware reach.
- Conduct regular recovery testing simulating sophisticated ransomware scenarios.
- Develop staged restoration procedures prioritizing critical business functions.
- Create offline incident response playbooks for ransomware scenarios.

Develop GenAI-Aware Security Programs:



- Conduct red team exercises specifically targeting AI systems.
- Implement security controls for AI development and deployment pipelines.
- Establish monitoring for potential prompt injection attacks and AI-targeting.
- Maintain strict access controls on AI training data and model parameters.

References

- 1 **Evolutional Generative Adversarial Network (EGAN):** <https://arxiv.org/pdf/2405.12266>
- 2 **CISA Sectors Critical Infrastructure 2024:** <https://www.securin.io/cisa-sectors-critical-infrastructure-2024-download/>
- 3 **Python Risk Identification Tool for generative AI:** <https://www.securin.io/cisa-sectors-critical-infrastructure-2024-download/>
- 4 **Schneider Electric Breach:** <https://www.bleepingcomputer.com/news/security/cactus-ransomware-claim-to-steal-15tb-of-schneider-electric-data/>

About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Follow Us On



Securin
securin.io