Trend Research

TREND MICRO

THE EASY WAY IN/OUT

Securing The Artificial Future

Trend Micro Security Predictions for 2025

Published by
Trend Research

Stock images used under the license from Shutterstock

Consumer data will be the hot commodity in the underground for 2025, with cybercrime expected to cost over $10 trillion[1] this coming year. Criminals will continue to develop new ways to exploit vulnerable areas, increasing enterprise risk as the attack surface expands. Our research[2] points to artificial intelligence (AI) as a major propulsor for criminal schemes,[3] using it to enhance, speed up, and improve operations[4] and schemes to exploit what remains the most vulnerable avenue — the user.

Criminals will also continue to pursue avenues of least resistance and most accessibility — taking the easiest route, for what continues to be the greatest motivator: profit. Publicly accessible data storage and misusing legitimate tools will be hot targets and techniques. The following sections highlight the top issues that will disrupt enterprise operations and user security in 2025.

RISK ASSESSMENT

Assessing the risk of what's coming

This section summarizes our predictions for 2025 alongside our experts' assessment on their expected risk severity and scope. Severity refers to the level of impact in case of a successful attack, while scope refers to the amount of people likely to be affected in a successful attack. We also list the industries and groups that should be on the lookout for these kinds of attacks.

SEVERITY	SCOPE	INDUSTRY OR GROUP	PREDICTION
MEDIUM	NARROW	• Financial sector • Insurance sector	Bypass-KYC-as-a-service sustained by unintentionally exposed biometrics, leaked and breached PII
HIGH	WIDE	• ALL • Consumer	Hyper-personalized deepfake-enabled scams using LLM trained on existing writing style, knowledge, and personality
MEDIUM	NARROW	• Technology industry • Other enterprises adopting agents (making its scope of risk grow)	AI agent vulnerability exploits
MEDIUM	NARROW	ALL (depending on software adoption)	AI supply chain attacks
HIGH	WIDE	ALL	BEC and fake employee scams
LOW	NARROW	AI industry	AI model web-scraping
HIGH	NARROW	Enterprises adopting agentive AI	Agentive AI hijacking
MEDIUM	NARROW	Enterprises adopting the use of LLMs in the operations	Sensitive information disclosure by LLMs during employee and customer interactions
HIGH	WIDE	ALL	Exploitation of memory management vulnerabilities
HIGH	NARROW	Automotive companies adopting centralized ECUs and their customers	Attacks across various OEM platforms that share components from centralized ECUs
MEDIUM	WIDE	• Automotive companies and their customers • Power grid and system operators and authorities	Targeted attacks on EV charger and vehicle communications
MEDIUM	NARROW	• Government organizations • Enterprises that publicly express their political leaning/ideologies	Increase in hacktivist attacks
HIGH	NARROW	Organizations of interest to National Governments	Espionage attacks by groups like Void Rabisu, DaVinci Group, and other mercenary groups

SEVERITY	SCOPE	INDUSTRY OR GROUP	PREDICTION
HIGH	NARROW	• Government organizations handling diplomatic information, military technology • Supply chain enterprises	Attacks on cloud environments by nation-state threat actors
MEDIUM	WIDE	General Population	Disinformation campaigns
LOW	WIDE	• General Populations devices • Can be used as enabling infrastructure to attack others	Attacks on public-facing servers and internet-facing routers
HIGH	WIDE	ALL	Continued attacks exploiting vulnerabilities in BYOVD
MEDIUM	NARROW	ALL	Attacks redirecting Windows subsystem execution to compromise EDR/AV detection
HIGH	WIDE	ALL	Attacks enabled by techniques disabling or evading EDR/AV
HIGH	WIDE	ALL	Attacks that leverage locations that most enterprises do not have centralized security such as the cloud, mobile, voice calls, and IoT
HIGH	NARROW	ALL	Data exfiltration for attackers facilitated by simulation devices and other cloud-connected IoT devices

AI

AI age scams: deepfakes, malicious digital twins, and AI tools abound

Deepfakes are poised to be the biggest AI-related threat because of the vast potential for misuse. Criminals have yet to reach their full potential, and we predict they will use deepfakes in new scams and criminal schemes in 2025. Popular or common social engineering scams will become even more believable with the use of deepfakes, while LLM trained on a person's public posts can mimic their writing style, knowledge and personality. These AI-enabled techniques make for dangerously convincing impersonations to target unwitting victims. We also predict the continuation of AI-based semi-automated scams. For corporations, BEC and "fake employee" scams should be the most concerning. Bypass-KYC-as-a-service has been popular in the underground for a few years already, sustained by three elements: unintentionally exposed biometrics, leaked and breached PII (particularly from ransomware attacks), and the growing capabilities of AI. This avenue of attack will continue for scammers.

In terms of AI targets – malicious individuals are likely to exploit vulnerabilities in AI systems to manipulate them into carrying out harmful or unauthorized actions with the appearance of digital entities based on persons impersonated without their awareness, or even with entirely new identities. We will keep seeing new uses for this new technology as it advances, and as criminal actors keep finding new social engineering uses for it, such as building phishing kits that are tailored to specific events. AI helps attackers be more efficient and timelier with the delivery of these toolkits. We have seen it with the recent US elections, and it will likely get more common.

For consumers, the growing prevalence of AI-generated content continues to demand user education for better discernment when consuming and interacting with content online.

> *Imagine by how much scams could scale up with automation brought by an LLM. The usage of AI is still limited, but it is easy to imagine the next iteration will depend on it to automate everything. AI used by criminals only need to get it right once, but defenders utilizing AI for security need to get it right every time.*

AI-enabled cybercrime and malicious activity to watch out for:

PIG BUTCHERING

- Identify profiles of lonely vulnerable people
- Contact and start romancing them
- Hook victims and pass them to human operators that can deepen the relationship through personality filters of an LLM that allows for scalability
- Lure victims into trading and investment chatrooms
- Get victims to invest their money into a fake site

MIS/DISINFORMATION CAMPAIGNS

- Create authentic appearing social media personas en masse
- Deploy content as typical social media users would
- Mirror disinformation of other bot personas
- Perpetuate pre-existing false narratives to amplify malign foreign influences
- Formulate messages, to include the topic and framing, based on the specific archetype of the bot.

Other AI-enabled activities to watch out for:

AI MODELWEB SCRAPING

Web scrapers for AI models will continue for websites of companies worldwide, particularly online media and newspapers

AI SOFTWARE ENGINEERS

AI evolution will likely include AI software engineers from models with advanced reasoning and scaled-up inference

IMPROVED SCALABILITY OF CYBER ATTACKS

AI will allow criminals to interact using foreign languages and with the understanding of local and regional culture without the knowledge previously necessitated.

AI SUPPLY CHAIN ATTACKS

This will become even more mainstream when LLM models are used as basis for agents and as we see agents proliferation.

> *AI paves the way potentially for hyper personalized attacks (phishing, public opinion manipulation, scam) which consider the habits and known needs of the targeted individual. More complex cyberattacks and scams could potentially lead to situations where traditional security measures are insufficient."*

AI FOR ENTERPRISES

Automation will cloak flaws from human eyes

As AI becomes more agentive and begins using enterprise tools and computers autonomously, it creates a chain of events and interactions that are invisible to human operators. This lack of visibility can be a security concern as it will be a struggle to monitor and control the agents' actions in real time.

As enterprises inevitably enter the AI race, they may expose themselves to more vulnerabilities and flaws.[5] Sensitive information disclosure[6] is a growing concern in that LLMs risk exposing sensitive data during interactions with employees and customers, including personal identifiable information and intellectual property.

More companies are using AI to discover infrastructure vulnerabilities, increasing both the number of identified vulnerabilities, and, potentially, the risk of exploitation. The AI agents will also become more attractive to malware authors. There is great potential for unauthorized or malicious activities carried out by misguided autonomous agents, including "agent hijacking" by external actors. Traditional malware and known threat detection will shift left toward vulnerability and attack surface management, while also shifting right towards leveraging foundational data intelligence.

System resource consumption by AI agents, whether benign or malicious, can also lead to denial-of-service when resources are overwhelmed.

Threats posed by agentive AI will be harder to detect using traditional statistical anomaly detection methods. Enterprises will be introducing AI agents to mainstream to remain competitive; agents might itself be malicious because of their autonomy and logic errors or execution errors. The growing reliance on AI Agents underscores the urgent need for robust security measures that give security teams end-to-end visibility on these Agent's operations, while also harnessing the power of AI to counter and protect from the vulnerabilities its convenience creates for itself.

> *Companies will experiment a lot in 2025 and figure out how much hallucinations they can tolerate. Malware authors will likely attack these frameworks, look for possible vulnerabilities, and exploit them. Internal helper chatbots can also work for cybercriminals in helping them understand the company's defenses after being compromised.*

Enterprises adopting agentive AI should beware of:

- Data theft
- Data breaches caused by coding errors
- Model misalignment
- Infrastructure-based DDoS attacks
- Compromise from third-party libraries or code

> *Users might happily shoot themselves in the foot experimenting with AI agents, and that will remain a threat until better guidelines and execution guide rails are created. The limited number of agent and model providers also means that one flaw in a popular provider can create a persistent vulnerability across numerous organizations.*

APT

Maximum impact: Advanced criminal groups versus cloud environments and supply chains

Nation-state threat actors such as Lazarus,[7] Turla,[8] and Pawn Storm[9] were particularly active in 2024 and are expected to increase their activity in 2025. These groups will continue to target diplomatic information and military technologies as well as their supply chains for maximum impact. Other criminal and mercenary groups are now carrying out espionage too, such as Void Rabisu[10] and the DaVinci Group.[11] Operations aligned with Russian propaganda like Doppelganger and pro-China networks such as Spamouflage are seen to continue leveraging disinformation to deepen societal divisions. Salt Typhoon's[12] recent attack that siphoned phone call audio and data could suggest that nation-state threat actors are exploring audio deepfakes.

Earth Hundun[13] and other nation-state threat actors with similar geopolitical alignments will continue their speedy evolution. Meanwhile, North Korean groups will likely keep focusing on cryptocurrency to help bypass sanctions. APT29 has been targeting cloud environments, an activity expected to rise. Sandworm, primarily involved in operations related to the invasion of Ukraine, could expand its operations depending on future geopolitical developments. The same geopolitical developments will continue to see hacktivist groups impacting enterprises they see as linked to their political or ethical ideals; and in the act are influenced by state actors looking to make use of the free energy they provide.

Organizations must understand their position within the supply chain, address vulnerabilities in public-facing servers, and implement multi-layered defenses within internal networks. It is advisable to require background checks for certain roles during recruitment as state actors have recently leveraged this to place insiders within a target network. Furthermore, collaboration among governments, private companies, and media is essential to uncover the full scope of influence operations. Attack Path Prediction will be critical for enterprises as cloud instances can allow for multi-step kill chain; being able to predict and disrupt these attack paths will boost an organization's defenses.

> *Geopolitical tensions and conflicts bring new levels of risks to enterprises within and outside of conflict zones. Organizations should execute proactive, future-proof, sustained and sustainable strategies[14] before conflict begins, when it erupts and throughout its duration, and in its wake in preparation for future attacks.*

APT groups are expected to persist

ATTACKING

- **On public-facing servers**
- **On supply chains**
- **On-Internet-facing routers**
- **Via targeted phishing campaigns**

LEVERAGING

- **BYOVD (Bring Your Own Vulnerable Driver)**
- **Zero-day exploits**
- **Operational Relay Boxes and Proxy Networks –** to obfuscate attack avenues
- **Public events –** as lures

MAXIMIZING

- **Insider threats –** that can aid with data breaches or sabotage
- **Generative AI**
  - to enhance influence operations with convincing disinformation
  - to tailor-fit phishing
  - to assist and expedite malware development

Throughout 2024, generative AI was utilized in content creation, dissemination, and in the development of fake personas and misleading information. It is predicted that the use of generative AI will be further enhanced to increase the credibility of disseminated content and improve operational efficiency in disinformation campaigns. The social impact should not be underestimated. It is important for governments, private companies, media and other organizations to collaborate in uncovering the full scope of malicious influence operations.

VULNERABILITIES

Vulnerabilities in memory management and mobility innovation

Memory management vulnerabilities, such as Out-of-Bounds (OOB) Write/Reads, continue to be exploited by threat actors; the CISA KEV[15] reported 18 different OOB Write vulnerabilities exploited this year. Memory management bugs (CWE-787 and CWE-125[16]) are among the top most dangerous vulnerabilities based on severity and frequency as analyzed by MITRE. Memory management and memory corruption bugs will likely continue to be favorites of attackers in the coming year. Memory corruption and logic bugs are often combined to create winning Pwn2Own entries.

In 2025, we expect to see bug chains continue to be prevalent while bugs in APIs create problems for cloud resources. We also expect more container escapes.[17] We had a Docker[18] escape demonstrated this year, and more are sure to follow.

However, older, simpler vulnerabilities like cross-site scripting (XSS) and SQL injections continue to be popular and will continue to be targeted for as long as they exist. This is especially true for operational technology devices and services that security experts have yet to scrutinize. Older techniques continue to be effective like simple buffer overflows and command injection exploits remain popular for devices like printers and Wi-Fi cameras, as these devices were not built with security in mind. Despite the advancement that AI offers, these classic avenues of least resistance will continue being useful for cybercriminals who want maximum profit for the least amount of effort.

Meanwhile, security is faced with the challenge of keeping pace with mobility innovation as the path forward continues to unfold. The push for platform standardization in mobility across different platforms means that a single vulnerability in a widely adopted system could cascade across multiple models and manufacturers, leading to large-scale recalls or urgent software updates. Vehicle systems are also transitioning from multiple distributed electronic control units (ECUs) to a few centralized ECUs with higher computational power. While this transition reduces the cost and time required for developing new versions of E/E systems, it in turn lowers the barriers to entry, reduces the learning curve for attackers, and increases the risks of widespread attacks across various OEM platforms that share components.

This year, EV charging and in-vehicle infotainment (IVI) systems were frequently exploited at Pwn2Own, especially during the inaugural Pwn2Own Automotive event. These systems represent a broad attack surface that vendors have yet to thoroughly vet for security gaps. In the future, attackers are likely to target the communication between EV chargers and vehicles, as EV charging stations are connected online and interact with payment systems and the power grid as well as vehicles. If not properly secured, they could be exploited to access in-vehicle systems, steal payment information, and disrupt charging processes.

Cyberthreats to connected cars could lead to serious physical consequences. For example, compromised vehicles could enable criminals to disable brakes or steering. Advanced safeguards and proactive measures are critical to protecting automotive systems from cyber-physical threats that endanger driver, passenger, and pedestrian safety.

Asset detection is crucial for enterprises to detect critical vulnerabilities such as memory management bugs; the sheer number of devices on today's networks makes comprehensive identification challenging. Thorough detection is vital for maintaining these assets through timely patches and updates. Meanwhile, evolving threats in the automotive industry stress the importance of collaborative efforts among OEMs, suppliers, and cybersecurity firms to strengthen collective and holistic defenses. Organizations like Auto-ISAC play a key role by providing platforms that enable the automotive industry to share information and best practices effectively.

Risks in mobility game changers

CHATBOT INTEGRATION IN VEHICLES CAN BE EXPLOITED TO

- Inject malicious commands
- Manipulate responses
- Access sensitive information through voice interactions

VULNERABILITIES IN IN-VEHICLE PAYMENT SYSTEMS CAN BE EXPLOITED TO

- Steal payment information
- Hijack transactions
- Disrupt services

> *While technological advancements promise efficiency and innovation, they also introduce new risks the industry might not be equipped for or are indeed even aware of. A single breach can ripple across the ecosystem, underscoring the critical need for robust, collaborative defense strategies.*

RANSOMWARE

Secure legitimate tools and applications against fresh torrent of ransomware attacks

2024 saw a rise in ransomware groups leveraging legitimate tools for data exfiltration,[19] credential collection[20] and replication, which can make it easier for attackers to move laterally and escalate privileges. As we move into 2025, legitimate tools will continue to be exploited as cybercriminals realize their potential in disguising attack activity as legitimate and that they already have access to valuable resources, data, and enterprise networks. With the rise of ransomware attacks starting through vulnerabilities or using compromised accounts, attacks that start with phishing will likely go down, suggesting a shift in techniques for ransomware gangs. More successful attacks from our recent investigations used compromised accounts to connect to a machine in the environment, while other cases saw the attacker bypassing multi-factor authentication (MFA) mechanisms. Ransomware attacks could also drift towards business models that no longer necessitate encryption.

As ransomware groups evolve in their technique of leveraging legitimate tools, organizations should not only rely on malicious files and hash detections but also monitor behavior across layers. Enterprises should opt for solutions that provide enhanced visibility and correlated detection across multiple layers, ensuring that incidents with the potential to cause significant system damage can be addressed as early as possible. Organizations can stay on top of threats by subscribing to CTI platforms to gain insights and information on the tactics, techniques, and procedures of cyberattacks, to prepare prevention and mitigation protocols.

As cybercriminals maximize AI, so should organizations: leverage AI to advance threat detection, automate responses, and predict potential security breaches. Ensure that AI systems are protected against malicious attacks and vulnerabilities by implementing rigorous security measures to protect AI models and data.

Ransomware attacks will see a rise in the use of:

More sophisticated and deliberate approaches to target or evade EDR and AV products such as:

- The increased use of BYOVD
- Hiding shellcodes inside inconspicuous loaders
- Multiple techniques to disable EDR/AV, or not disabling them at all
- Redirecting Windows subsystem execution to compromise EDR/AV detection
- Creating kill chains that leverage locations that most enterprises do not have centralized security such as the cloud, mobile, voice calls, and IoT

Artificial intelligence in cases where:

- AI platforms and AI tools are targeted to disrupt the operational supply chain
- GenAI-generated code is used to spread malware, or to recode malware to contain ransomware instead
- AI can be used to generate more convincing phishing emails
- An LLM-created HTML file was used in an NTLM leak attack

IoT equipment for:

- Simulation devices and other cloud-connected IoT devices can facilitate data exfiltration for attackers

> *These new techniques make the attack stealthier and quicker. There are less tools that the attackers need to use: there is no need to attach an intermediate downloader to a phishing mail that will download more tools. Additionally, the stealth provided using legitimate tools makes it a little harder to detect the attack. The fewer steps taken for the attack means that it can be done quicker; we have seen the attack time frame shrink to just a couple of days from at least a whole week.*

ATTACK TOOL TRENDS

More efficient information harvesting and malvertising assaults

In the past, we have seen a one-to-one ratio between loaders and info stealers, where one loader will install just one infostealer, but we have started seeing multiple infostealers installed by a single loader. Information harvested by such threats are useful for threat actors and enable them to carry out other attacks. Ransomware groups will continue to use this as a key part of their attacks: utilize information, such as user accounts harvested by infostealers, in their ransomware attacks.

Malvertising threats have been thrust into the spotlight partly because of the widespread proliferation of infostealers that use this arrival technique[21], which could lead to attackers seeing its potential for other campaigns. We have already seen ransomware groups[22] use this to get a foothold in a target environment. The stealth mechanisms described in the previous section show how threat actors can innovate and elevate the technique to make it more effective in gaining initial access. We predict that this trend will continue in 2025.

Enterprises should make sure that they comply with new security standards outlined by legal experts. The European Union's (EU) NIS2[23] Directive is a new legal directive that will help enterprises improve the security of networks and information systems across the EU by focusing on strengthening cybersecurity risk management and incident reporting. The Digital Operational Resilience Act (DORA[24]) will also be implemented in January 2025, which will require financial institutions to follow stringent guidelines for safeguarding against ICT-related incidents. Enterprises should also address vulnerabilities in public-facing servers and implement multi-layered defenses within internal networks.

What will attackers be targeting?

AI training environments	**AI access infrastructure**	**AI service subscriptions**
Public-facing servers	**Internal vulnerabilities**	**Legitimate applications**
Supply chains	**Enterprise data**	**Misconfigurations in cloud environments and remote work infrastructures**

> *By 2025, it is anticipated that cyberattacks targeting these misconfigurations will become even more sophisticated, with a rise in automated attack methods leveraging AI. Consequently, companies may face severe impacts, including legal liabilities due to information leaks, financial losses, and erosion of trust.*

CONCLUSION

Malicious actors will go full throttle in mining the potential of AI in making cybercrime easier, faster, and deadlier. But this emerging and ever-evolving technology can also be made to work for enterprise security and protection by harnessing it for threat intelligence, asset profile management, attack path prediction and remediation guidance. As SOCs catch up to secure innovations still and yet unraveling, protecting enterprises from tried and tested modes of attack remains essential. While innovation makes for novel ways to strike, criminals will still utilize what is easy and what has worked for them for years.

The attack surface continues to become more complex; as it expands exponentially, it is not wise to assume that time-tested tactics and techniques are in the past. Traditional security measures will be increasingly challenged to comprehensively manage all risks both from novel and known threats. Implementing a risk-based approach to cybersecurity is essential, particularly one that allows organizations to centrally identify these diverse assets and effectively assess and mitigate risks. By simplifying and converging security operations, it will be easier for enterprises to mitigate risks and adopt an outlook on security that is proactive. Update user training and awareness, keeping abreast of recent AI advancements and how they enable cybercrime.

In line with this, enterprises should place safety measures to secure any AI integrations both for pre- and post-implementation; security for input validation, response validation, or actions generated by AI. Monitor and secure your AI technology closely against abuse. Cybercriminals that gain access to your network could also start to use your own AI agents and AI subscriptions for their own benefit or drain your resources.

Enterprises integrating LLMs should prioritize robust security measures, including hardening sandbox environments for code execution, implementing strict data validation to prevent exfiltration and vector store poisoning, and deploying multi-layered defenses against prompt injection. Incorporating a secure development lifecycle with regular threat modeling, red teaming, and continuous monitoring is essential. Educating users on secure LLM usage, limiting exposure to sensitive data, and staying updated on emerging threats will further enhance protection against sophisticated vulnerabilities in AI-driven systems.

Endnotes

1 Steve Morgan. (Nov. 13, 2020). *Cybersecurity Ventures*. “Hackerpocalypse - Cybercrime Report 2016.” Accessed on Oct. 29, 2024, at link.

2 Vincenzo Ciancaglini and David Sancho. (Aug. 31, 2023). *Trend Micro*. “Back to the Hype: An Update on How Cybercriminals are Using GenAI. Accessed on Oct. 29, 2024,” at link.

3 Federal Bureau of Investigation. (July 2, 2023). *FBI*. “FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence.” Accessed on Oct. 29, 2024, at link.

4 National Cyber Security Centre. (Sep. 15, 2023). *NCSC*. “Impact of AI on Cyber Threat”. Accessed on Oct. 29, 2024, at link.

5 NIST. (Jan. 26, 2023). *Information Technology Laboratory (ITL)*. “AI Risk Management Framework”. Accessed on Nov. 27, 2024, at link.

6 OWASP. (March 20, 2023). *OWASP*. “LLM Top 10”. Accessed on Nov. 27, 2024, at link.

7 Jai Vijayan. (October 25, 2023). *Dark Reading*. “Lazarus Group Exploits Chrome Zero-Day Campaign”. Accessed on Nov. 15, 2024, at link.

8 Ravie Lakshmanan. (May 3, 2024). *The Hacker News*. “Turla Group Deploys LunarWeb and MoonBase Malware in Sophisticated Cyber Espionage Operation”. Accessed on Nov. 15, 2024, at link.

9 Feike Hacquebord and Fernando Merces. (Jan. 31, 2024). *Trend Micro*. “Pawn Storm Uses Brute Force and Stealth Against High-Value Targets”. Accessed on Nov. 4, 2024, at link.

10 Feike Hacquebord and Fernando Merces. (July 14, 2023). *Trend Micro*. “Void Rabisu Targets Female Leaders with New RomCom Variant”. Accessed on Nov 15, 2024, at link.

11 Daryna Antoniuk. (Sep. 28, 2023). *The Record*. “Hackers Using Remcos Getting Stealthier”. Accessed on Oct. 29, 2024, at link.

12 SecurityWeek News. (Oct. 10, 2023). *SecurityWeek*. “US Gov Agency Urges Employees to Limit Phone Use After China Salt Typhoon Hack”. Accessed on Nov. 13, 2024, at link.

13 Pierre Lee and Cyris Tseng. (May 16, 2024). ***Trend Micro***. “Tracking the Progression of Earth Hundun’s Cyberespionage Campaign in 2024”. Accessed on Oct. 29, 2024, at link.

14 Feike Hacquebord, Stephen Hilt, Vladimir Kropotov, Fyodor Yarochkin. (Oct. 5, 2023). *Trend Micro*.” Cyber Considerations for Organizations During Times of Conflict”. Accessed on Oct. 29, 2024, at link.

15 CISA. (Feb. 1, 2023). *Cybersecurity and Infrastructure Security Agency*. “Known Exploited Vulnerabilities Catalog”. “Accessed on Nov. 27, 2024, at link.

16 Sergiu Gatlan. (Aug. 15, 2024”). *BleepingComputer*. “MITRE shares 2024’s top 25 most dangerous software weaknesses”. “Accessed on Nov. 27, 2024, at link.

17 Trend Micro. (Oct. 4, 2023). *Trend Micro*. “NVIDIA AI Container Toolkit Vulnerability Fix”. “Accessed on Nov. 27, 2024, at link.

18 Sunil Bharti, Ranga Duraisamy. (Oct. 12, 2023). *Trend Micro*. “Attackers Target Exposed Docker Remote API Servers with Perfctl”. “Accessed on Nov. 27, 2024, at link.

19 SC World Staff. (June 19, 2023). *SC World*. "Microsoft Azure Tools Increasingly Leveraged in Ransomware Attacks". Accessed on Oct. 29, 2024, at link.

20 Pierluigi Paganini. (Oct. 20, 2023). *Security Affairs*. "Veeam Backup & Replication Vulnerability CVE-2024-40711: What You Need to Know". Accessed on Oct. 29, 2024, at link.

21 Jaromir Horejsi. (Sep. 12, 2024). *Trend Micro*. "Malvertising Campaign Uses Fake AI Editor Website for Credential Theft". Accessed on Nov. 5, 2024, at link.

22 Lawrence Abrams. (Sep. 15, 2024). *BleepingComputer*. "Ransomware Gang Targets Windows Admins via PuTTY, WinSCP Malvertising". Accessed on Nov. 5, 2024, at link.

23 NIS2Directive. (n.d.). "NIS2Directive.com". Accessed on Nov 13, 2024, at link.

24 DORA. (n.d.). "Digital Operational Resilience Act". Accessed on Nov. 13, 2024 at link.

THE EASY WAY IN/OUT

Securing The Artificial Future

Trend Micro Security Predictions for 2025

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information.

Fueled by decades of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

Trend's platform delivers advanced threat defense techniques, extended detection and response (XDR), attack surface management (ASM), and integration across the IT ecosystem, including AWS, Microsoft, and Google. This enables organizations to better understand, communicate, and mitigate cyber risk.

Trend's global threat research team delivers unparalleled intelligence and insights that power the platform and help protect organizations around the world from hundreds of millions of threats daily.

With 7,000 employees across 70 countries, Trend is singularly focused on cybersecurity by enabling organizations to simplify their connected world. TrendMicro.com.

trendmicro.com

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy