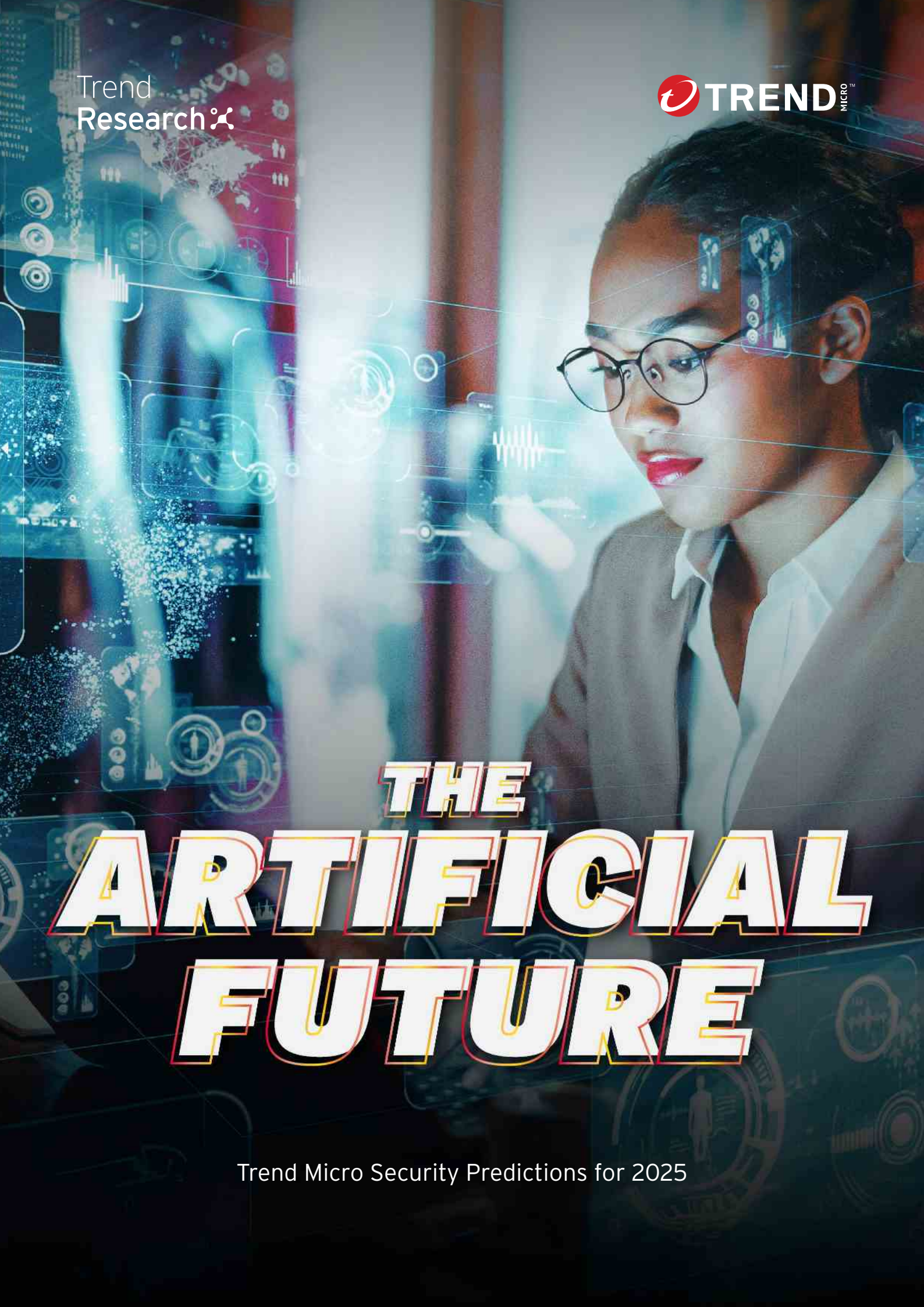
Trend Research

TREND MICRO™



THE ARTIFICIAL FUTURE

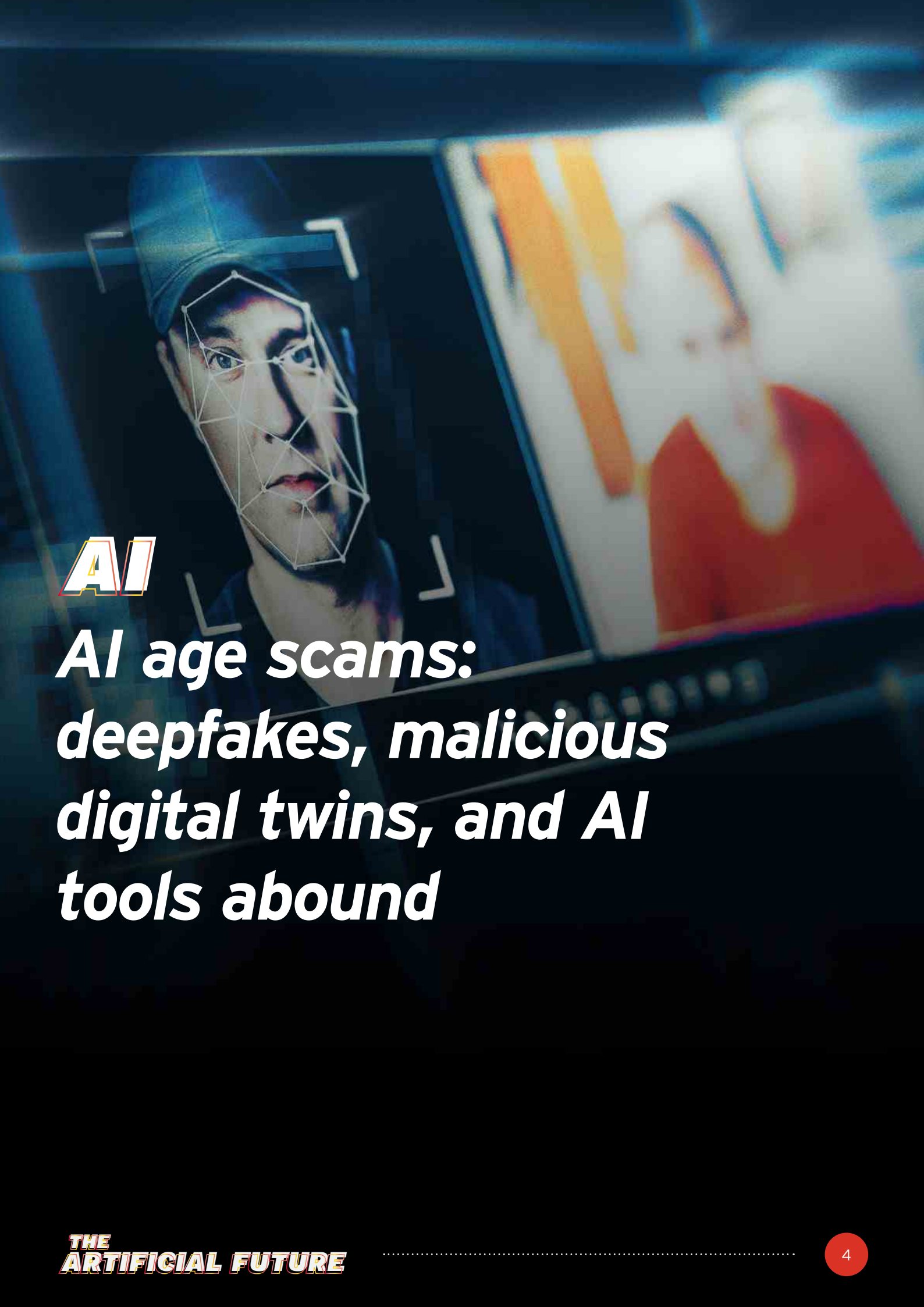
Trend Micro Security Predictions for 2025

Published by
Trend Research

THE ARTIFICIAL FUTURE

In 2025, consumer data will be a hot commodity in the underground, and cybercrime is expected to cost organizations around $10 trillion.[1] 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] that 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. In the sections below we highlight the top issues that will disrupt enterprise operations and user security in 2025.



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 plumb their full potential, and we predict they will use deepfakes in new scams and criminal schemes in 2025. 'Hot' social engineering scams will be 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 - AI agents are increasingly deployed to perform specific tasks or roles, and they will become more attractive targets for malware authors. 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.

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 MODEL WEB 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.

AGENTIC AI

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 chat bots can also work for cybercriminals in helping them understand the company's defenses after being compromised.

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.

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 use by criminals only need to get it right once, but defenders utilizing AI for security need to get it right every time.

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.

Enterprises will be introducing AI agents to mainstream to remain competitive; agents might themselves 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 to protect against such threats. 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. Outside of organizations, the growing prevalence of AI-generated content continues to demand user education for better discernment when consuming and interacting with content online.

APT

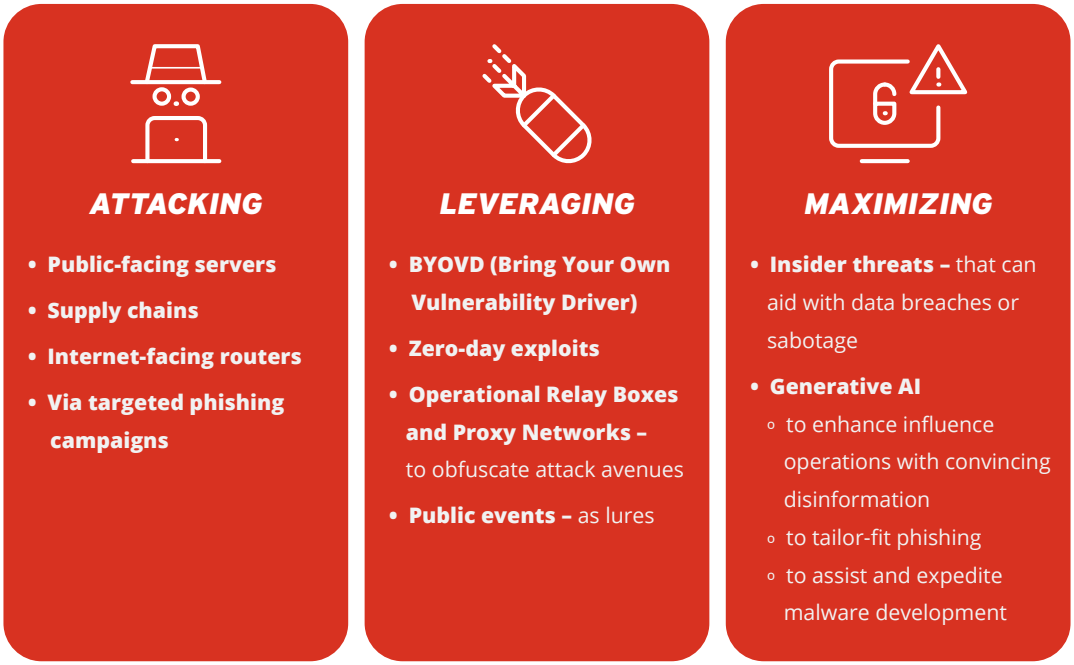
Advanced criminal groups will hammer away at cloud environments and supply chains

Nation-state threat actors such as Lazarus,[5] Turla,[6] and Pawn Storm[7] 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 doing a significant amount of espionage too, such as Void Rabisu[8] and the DaVinci Group.[9] Operations aligned with Russian propaganda like Doppelganger and pro-China networks such as Spamouflage have been seen continually leveraging disinformation to deepen societal divisions. Salt Typhoon's[10] recent attack that siphoned phone call audio and data could suggest that nation-state threat actors are exploring audio deepfakes. Earth Hundun[11] 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.

APT groups are expected to persist



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[12] before conflict begins, when it erupts and throughout its duration, and in its wake in preparation for future attacks.

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.

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.

RANSOMWARE

Ransomware groups will double down on exploiting widely used legitimate tools and applications

2024 saw a rise in ransomware groups leveraging legitimate tools for data exfiltration,[13] credential collection[14] 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 in 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.

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.*

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 safeguarded against malicious attacks and vulnerabilities by implementing rigorous security measures to protect AI models and data.

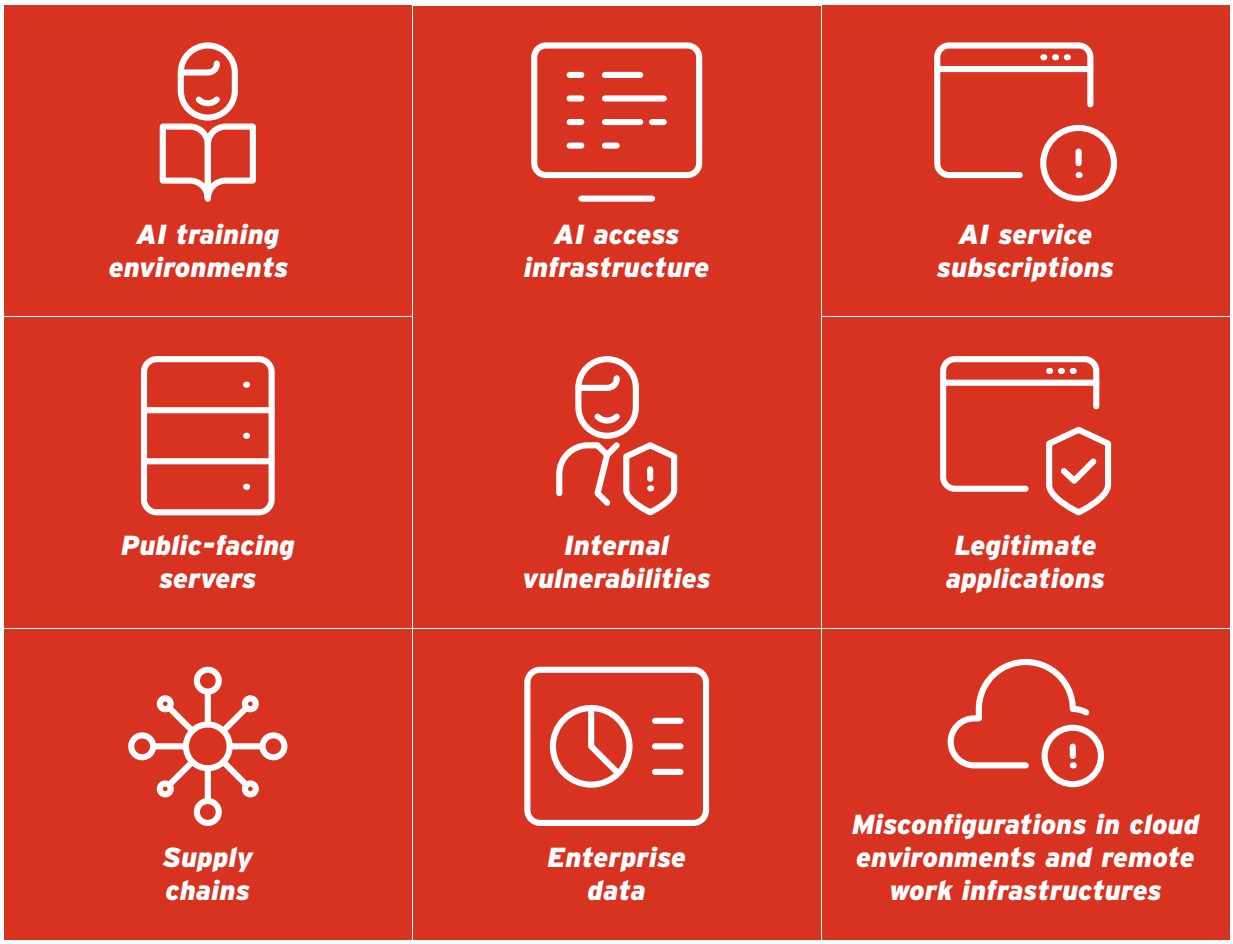
ATTACK TOOL TRENDS

Enterprises: beware of information harvesting and malvertising

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.

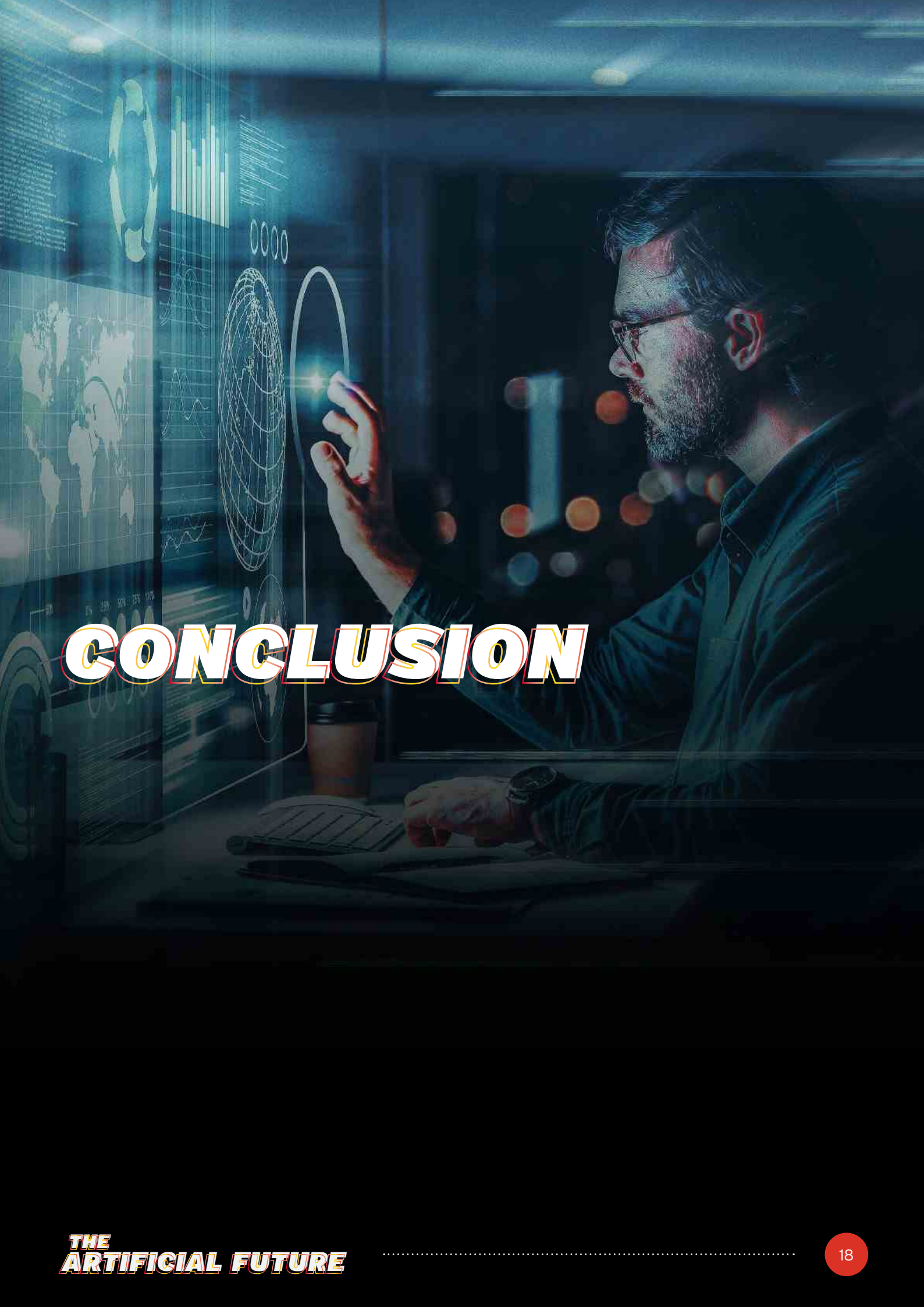
Malvertising threats have been thrust into the spotlight partly because of the widespread proliferation of infostealers that use this arrival technique,[15] which could lead to attackers seeing its potential for other campaigns. We have already seen ransomware groups[16] use this to get a foothold in 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. In 2025 we predict this trend will continue.

What will attackers be targeting?



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.

Enterprises should make sure that they comply with new security standards outlined by legal experts. The European Union's (EU) NIS2[17] 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[18]) 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.



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.

The attack surface continues to expand and become more complex, and so traditional security measures will be increasingly challenged to comprehensively manage all risks. 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 get access to your network could also start to use your own AI agents and AI subscriptions for their own benefit or to 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 Jai Vijayan. (Oct. 25, 2023). *Dark Reading*. "Lazarus Group Exploits Chrome Zero-Day Campaign. "Accessed on Nov. 15, 2024, at link.

6 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.

7 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.

8 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.

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

10 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.

11 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.

12 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.

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

14 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.

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

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

17 NIS2Directive. (n.d.). *NIS2Directive.com*. Accessed on Nov. 13, 2024, at link.

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

TREND MICRO™

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, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

Trend Micro's global threat research team delivers unparalleled intelligence and insights that power our cybersecurity platform and help protect organizations around the world from 100s of millions of threats daily.

We have 7,000 employees across 65 countries, singularly focused on security and passionate about making the world a safer and better place.

Trend Micro enables organizations to simplify and secure their connected world.

trendmicro.com