2024 Cybercrime Activity Report

Trends, Insights & Predictions

TLP:CLEAR

FEBRUARY 2025

INCD
Israel National
Cyber Directorate

Table of Contents

Executive Summary

This report provides a comprehensive analysis of cybercrime-related attacks observed throughout 2024, focusing on ransomware incidents and infostealer infections. The report highlights significant trends, victimology, and insights from both global and Israeli perspectives, offering a forward-looking view with valuable predictions for 2025. The information presented has been corroborated by industry insights and multiple external sources.

Part 1: Global Cyber Crime Roundup

INCD
Israel National
Cyber Directorate

Global Ransomware Trends

Globally, ransomware attacks affected 6,133 organizations in 2024[1], representing a 15% increase compared to 2023. Key targeted sectors included:

Healthcare: Consistently targeted due to the critical nature of medical data.

Public entities: Including government and municipal services, often vulnerable due to legacy systems.

Manufacturing: Disruptions in production lines lead to high-pressure ransom payments.

Technology: Targeted for intellectual property theft and value of data for potential espionage purposes of buying

[1] Based on data from ransomware.live

A notable trend was the rise of new ransomware groups, with 48 new groups emerging in 2024. This brings the total number of active groups to over 130. Interestingly, 24 of these groups were responsible for more than 60% of reported attacks, underscoring the dominance of key players in the ransomware landscape.

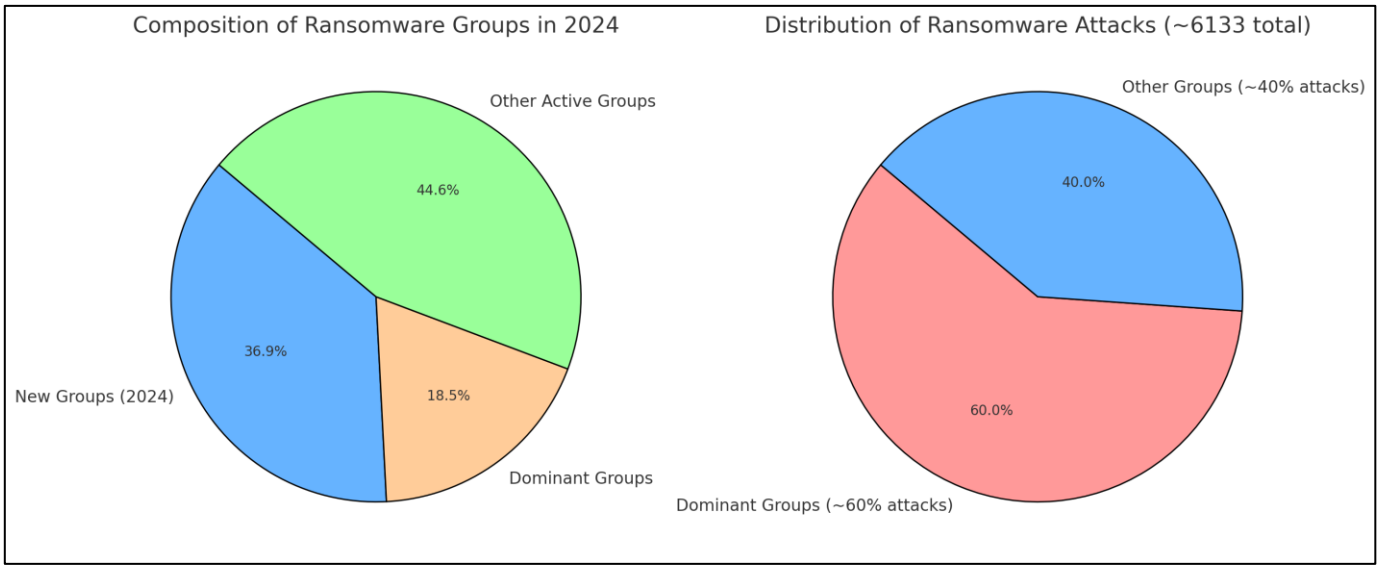


Figure 1: Ransomware group activity status vs. disribution of responisiblity of activity in victim volume

Global Infostealer Infections

Worldwide, infostealer infections reached 39,119,905 cases in 2024. These infections played a pivotal role in ransomware campaigns, with logs from compromised systems being sold on dark web markets for prices ranging from $1 to $10 per system. The low cost and high utility of these logs make infostealers a vital component of the cybercrime ecosystem.

Part 2: Israeli Cyber Crime Roundup

INCD
Israel National
Cyber Directorate

Ransomware Victims in Israel

INCD recorded over 300 ransomware attacks targeting Israeli organizations in 2024, marking a sharp rise from 2023. The increase in ransomware incidents reflects both the global rise in such attacks and the particular vulnerabilities of Israeli organizations. The primary ransomware strains observed were:

1. **STOP/DJVU strains:** Known for targeting small businesses and individual users, often leveraging file encryption to demand ransom payments.
    a. The malware is mainly delivered through dubious files downloaded from, in most cases, illegal sites that contain software cracks, etc.
    b. This activity can be identified mainly by the usage of a seemingly-random 4 letter file extension.
    c. Ransom demand is usually on the very lower-end of the spectrum, being merely a few hundred USD at most.
2. **LockBit-Builder strains:** A variant of the well-known LockBit ransomware, widely used in RaaS (Ransomware-as-a-Service) operations.
    a. Worth to mention, most of the activity observed from ransomware activity utilizing LockBit 3.0 in Israel was in an "unofficial" way, i.e., various threat actors that have no stated affiliation to the LockBit group, relying on the leaked builder to generate their ransomware binaries.
    b. The global law enforcement efforts have significantly hindered the activity of the "official" LockBit group. Nonetheless, their activity was still slightly persistent after being impaired by the global law enforcement measures.
3. **Phobos strains:** Notorious for their persistence and ability to adapt, targeting a broad range of sectors.
    a. Different variants of Phobos were observed, while some are just differently known by the file extensions used by them. The variants include: elbie; devos; faust; makop; nigra.
    b. In most (if not all) cases observed, the initial access was through RDP connections, whether them being inadequately secured or using credentials harvested from users of the network.

Several new ransomware groups, like Brain Cipher, Alpha Locker, Fog, etc. were more active than others in Israel in the past year. And some of them being interesting in and of themselves.

Brain Cipher is a group that was very active that leveraged the LockBit ransomware software. In Israel, several victims were observed, and from the experience and knowledge obtained about LockBit, it provided a lot of information and possibilities against it.

Alpha Locker is interesting for that there was a single victim, in Israel, that was attacked by them but posted on their DLS that was created in January of 2024 while the entity was attacked more than half a year prior to that. It seemed to be somewhat of a resurrection of their efforts.

Infostealer Infections in Israel

In addition to ransomware, 52,913 cases of infostealer malware infections were reported.[2] Infostealers are often used as the initial access vector for ransomware deployment, making them a critical part of the cybercrime ecosystem. The most common variants in 2024 were:

1. **RedLine:** A widely used infostealer that targets credentials and browser data.
2. **Generic Stealer:** Low-cost, customizable infostealers available on underground markets.
3. **Lumma:** Known for its fast spread and ability to evade detection.
4. **Raccoon:** Highly popular among cybercriminals due to its ease of use and efficient credential harvesting.
5. **StealC:** A relatively new infostealer with advanced capabilities, including keylogging and screen capture.

** Further information regarding the different info-stealers and hunting techniques can be found here[3].*

[2] Cavalier.hudsonrock.com
[3] https://www.gov.il/he/pages/alert_1848

Impacted Business Sectors

While there are not a few similarities between global trends and victimization profiles, especially in targeting manufacturing and health care organizations, the overall ransomware activity in Israel showed a few different and more unique sectors being targeted and trends, them being:

Law firms: Often targeted for sensitive client information.

Auditing firms: Holding critical financial data attractive to attackers.

Dental clinics: Small healthcare providers with limited cybersecurity budgets.

Car garages: Often targeted for financial and customer data.

Small-medium logistics companies: Vulnerable due to supply chain dependencies.

Manufacturing factories: A prime target due to the potential for operational disruption.

An interesting insight is that most of the "unique" organizations being targeted, like car garages and law and audit firms, were being targeted primarily by a specific group mentioned in a previous report[4].

INCD noted that small and medium businesses (SMBs) remain prime targets due to weaker cybersecurity postures and a lack of regulatory oversight. The persistence of these attacks underscores the urgent need for stronger cybersecurity frameworks and improved incident response mechanisms.

2024 is a turning point in terms of how much impact can be made, with minimum effort. This statement will reoccur in every trend observed throughout the year – echoing the psychological aspect of ransomware attacks. In a domain driven by financial gain, there is nothing that can't be bought. And in a fast-paced world, which has proven this year more than the previous ones – those cyber-attacks play a significant role on the psychological domain. There is no meaning to whether a claim is real or bogus. The only meaning is the one given when something is blown-out of proportion. The following are trends observed throughout 2024 – based on reports made to the INCD, as well as internationally observed trends.

[4] https://www.gov.il/he/pages/alert_1709

Part 3: Trends Observed in 2024

INCD
Israel National
Cyber Directorate

1. 'Think Green'

Recycling leaked or breached data from previous attacks is a 'quick-win' method to gain a following, establish your brand, and portray a false narrative. INCD has observed several instances where ransomware groups re-use old, previously leaked data from organizations and market it as a product of their own work. By cross-referencing data, our teams can raise a 'false flag' and categorize various 'hacked' claims as false. This proactive approach helps maintain the integrity of affected organizations and ensures that cybercriminals are not rewarded for false claims. While this method is not unique to cybercrime actors, false claims can significantly damage a brand's public image. The reputational harm caused by such claims is often difficult to repair due to the scarcity of professionals dedicated to verifying and fact-checking criminal assertions.

Moreover, a brand's recovery from a cyber-attack can be further delayed if the public narrative surrounding the incident is controlled by threat actors. In such cases, timely identification and public disclosure of the truth are essential to minimize long-term damage. Organizations should invest in partnerships with cybersecurity firms that specialize in forensic analysis and threat intelligence to counter these tactics effectively.

2. Info Stealers + Initial Access Brokers – An Integral Part of the Ransomware Kill Chain & An Effective Way to Monitor and Boost Resilience

In the scope of cyber-attacks reported to INCD in 2024, one consistent trend alongside 'old players' is the use of info stealers. Info stealers have become a core component in successful ransomware and general cyber-attacks. The sheer

number of infected machines globally this year demonstrates the vast scope of this threat. These malicious programs are designed to exfiltrate sensitive information, including login credentials, cookies, and personal data, which are later sold or used for unauthorized access.

The low cost of logs (ranging from $1 to $10 per infected machine's credentials and cookies) makes cyber-attacks cost-effective in the long run. Combining sensitive login credentials to corporate environments with credentials to bank accounts simplifies an adversary's task, allowing them to achieve multiple objectives with a single attack. Additionally, the availability of automated tools and marketplaces where these logs are traded contributes to the growing prevalence of such attacks.

The ecosystem surrounding info stealers and initial access brokers is highly organized, with dedicated actors specializing in various roles. These actors include developers of malware, distributors, and resellers who profit by offering access to compromised systems. This highly specialized division of labor makes it challenging for defenders to disrupt the entire chain of operations.

3. Child's Play: 'Pass the Parcel' – Passing Access from Hand to Hand (Meow Leaks)

Many cybercrime groups today collaborate by passing access to organizations among themselves. Affiliates often work with preferred service providers, such as reliable access brokers, hosting providers, and money-laundering professionals. This networked approach enables them to maximize their profits by leveraging each other's expertise.

In one case investigated by INCD, an access broker sold access to an Israeli tax-auditing firm. Approximately two months later, this firm was claimed as a victim by the ransomware group 'Meow Leaks.' The incident underscores the complexity of the cybercrime ecosystem, where access once obtained can change hands multiple times before a final attack is launched.

INCD has identified at least one other instance where both 'Meow Leaks' and private brokers sold access to the same organization at different prices. This highlights a recurring trend of overlapping threat actors targeting the same victims through different channels. Such incidents emphasize the importance of continuous monitoring and incident response readiness for organizations that may find themselves repeatedly targeted by different groups.

Furthermore, the practice of passing access among different threat actors complicates attribution efforts. It becomes difficult to determine the exact sequence of events leading up to a breach, making forensic investigations more time-consuming and resource-intensive.

4. Presumed Prevalence in Abusing Smart Contracts as C2 and Exfiltration Infrastructure[5]

Although relatively under the radar in past years, recent campaigns highlight an emerging trend: the abuse of smart contracts as C&C infrastructure in deeper supply chain attacks. This tactic involves leveraging the decentralized and immutable nature of smart contracts to communicate with malware and exfiltrate data.

[5] https://thehackernews.com/2024/11/malware-campaign-uses-ethereum-smart.html
[5] https://thehackernews.com/2023/10/binances-smart-chain-exploited-in-new.html

So far, this type of activity has primarily been attributed to Russian-speaking actors. However, the rapid adoption of Web3 technologies underscores the potential for these technologies to play an integral role in future cyber-attacks. As more organizations adopt blockchain-based solutions, the risk of exploitation by adversaries increases.

Integrating smart contract attributes into an adversary's attack chain marks an interesting development in the threat landscape. This approach allows attackers to exploit the trust inherent in decentralized technologies, making detection and mitigation more challenging. The immutable nature of blockchain transactions further complicates efforts to shut down malicious operations.

Notably, this TTP aligns with known Russian-nexus activity, as demonstrated by Glupteba malware in 2021[6]. The parallels suggest that actors leveraging smart contracts for C2 infrastructure may be following a broader strategy observed in previous campaigns. Glupteba's use of blockchain technology to evade takedowns set a precedent for future campaigns, and the ongoing adoption of similar tactics indicates that this trend is likely to grow.

To counter these threats, organizations should stay informed about emerging attack vectors and invest in advanced monitoring tools capable of detecting anomalies in blockchain interactions. Additionally, fostering collaboration between the cybersecurity community and blockchain developers will be crucial in building resilience against these novel attack methods.

[6] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/glupteba-malware/

5. State-Sponsored Crime

2024 emphasized the natural connection between state and crime. The financially-driven crime ecosystem remains accessible to actors with varying motivations, including those sponsored by or aligned with nation-states. This dynamic ecosystem blurs the lines between state activity and independent criminal enterprises. Whether through moonlighting by state-sponsored actors or hiding in plain sight under the guise of legitimate businesses, the integration of state interests with financially motivated crime continues to evolve.

Iranian adversaries have resurfaced on the dark web[7], rebranding themselves as new personas and collaborating with established ransomware groups and affiliates. Their persistent re-emergence highlights the adaptive nature of state-sponsored threat actors in exploiting criminal networks to achieve geopolitical goals. This convergence amplifies the risks faced by both public and private sector organizations.

6. Virtual Insanity

Cloud-based ransomware attacks continue steadily, primarily due to misconfigurations. Misconfigured cloud environments create vulnerabilities that are readily exploited by attackers. The complexity of cloud infrastructure, combined with rapid adoption rates, increases the likelihood of oversight and errors, which can serve as entry points for ransomware operators.

There has been a stable shift towards targeting ESXi and Linux-based environments. As observed in previous years, this trend continues to pose significant risks. Business owners must take additional precautions when deploying

[7] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

these environments, as they offer a broader attack surface and are often less rigorously defended than traditional Windows-based systems. Effective monitoring and configuration management are essential to mitigate these risks.

7. TTPs

7.1 RMM + MFT Is Here to Reign

Criminals are increasingly abusing Remote Monitoring and Management (RMM) tools and Managed File Transfer (MFT) vulnerabilities. This trend mirrors tactics employed by groups such as Cl0p, who have effectively exploited MFT systems to exfiltrate sensitive data. The abuse of legitimate RMM tools provides attackers with persistent access to compromised environments, allowing them to execute ransomware operations while bypassing traditional detection methods. Given the widespread use of these tools in enterprise settings, organizations must adopt stringent access controls and continuous monitoring to detect unauthorized activity.

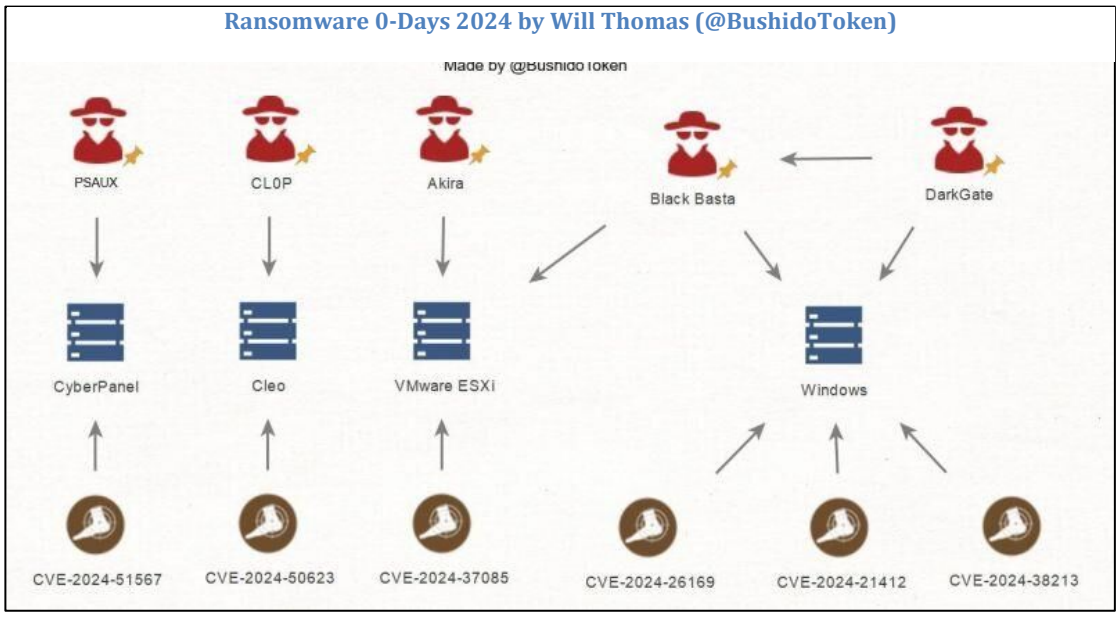
** Further information regarding the different info-stealers and hunting techniques can be found here*[8].

7.2 Abused 2024 CVEs by Cyber Criminals

2024 has shown a consistent pattern of exploiting zero-day vulnerabilities as a force multiplier. Attackers aim to maximize their victim count by rapidly leveraging newly discovered vulnerabilities before patches are widely applied.

[8] https://www.gov.il/he/pages/alert_1849

Trends from 2023 have carried into 2024, with many of the same software products being targeted and the same active groups responsible for exploiting zero-days. This continuity underscores the technical sophistication of these groups, whose capabilities rival those of state-sponsored adversaries.



Defense evasion tools have continued to proliferate throughout 2024, with at least a dozen new tools being marketed and discussed in underground forums during the first half of the year. The sale and development of evasion tools, particularly those designed to bypass Endpoint Detection and Response (EDR) systems, remain a thriving business model. This trend highlights the ongoing arms race between attackers and defenders in the cybersecurity landscape.

8. Post LockBit 3.0 Era?

Operation Cronos in February 2024 disrupted the underground community by dismantling LockBit's infrastructure. This takedown had a significant impact, creating a temporary void that other groups attempted to fill. The operation served

as a warning to cybercriminals, prompting some to reconsider their strategies. Despite this disruption, LockBit resurfaced with a new variant, LockBit 4.0, marking a revival of activity and innovation in ransomware operations.

8.1 Encryption-Less Ransomware Attacks

The trend towards encryption-less ransomware attacks continues to gain traction. Many cybercrime groups now favor the breach-extort-leak model, which achieves the same impact without the complexity of implementing robust encryption schemes. This shift reduces the operational overhead for attackers and accelerates the timeline from initial compromise to extortion.

8.2 Increased Emphasis on Leak and Shame Tactics

There is a growing focus on information leakage and public shaming. A larger percentage of victims reporting to INCD in 2024 experienced data leakage without encryption. This tactic pressures victims to comply with extortion demands, as the public exposure of sensitive data can be devastating to an organization's reputation.

8.3 Small Strains, Big Damage

Smaller ransomware groups continue to cause significant harm despite receiving less attention. INCD's analysis indicates that most ransomware incidents are attributed to lesser-known variants, such as Phobos[9] and STOP/DJVU. These smaller strains lack media coverage and a formal Data Leak Site (DLS), yet

[9] https://www.justice.gov/opa/pr/phobos-ransomware-administrator-extradited-south-korea-face-cybercrime-charges

they inflict considerable damage. Organizations must remain vigilant against these seemingly minor threats, which often fly under the radar.

8.4 BitLocker Attacks

The last quarter of 2024 saw an uptick in ransomware attacks leveraging the BitLocker feature. This tactic involves encrypting victims' systems using built-in operating system features, making detection and mitigation more difficult. The abuse of legitimate system tools continues to challenge traditional cybersecurity defenses.

8.5 Code Similarity Across Ransomware Families

A significant portion of newly emerged ransomware groups share code similarities with older strains. While this does not necessarily affect differences in TTPs between affiliates, it provides valuable intelligence for defenders. Code-based connections can reveal the lineage of ransomware families and offer insights into the decision-making processes of developers. In certain cases, such as with Shinra ransomware [10], identifying shared code elements has enabled the development of potential vaccines capable of neutralizing entire families of variants.

This code-sharing trend highlights the collaborative nature of the cybercrime ecosystem, where developers borrow and build upon existing codebases to create new variants. Understanding these connections enhances resilience by enabling more effective threat intelligence and response strategies.

[10] https://www.gov.il/BlobFolder/reports/alert_1815/he/ALERT-CERT-IL-W-1815.pdf

9. Adversaries Leveraging AI for Malware Development and Operations

An emerging trend in 2024 was the use of artificial intelligence by cyber adversaries to enhance their malware and operational capabilities. However, analysis of these AI-driven threats revealed significant shortcomings. Attackers often implemented AI without performing adequate integrity checks, resulting in non-functional or poorly optimized code. This indicates that while adversaries are experimenting with AI, they lack the expertise or resources to fully harness its potential.

Despite these early failures, the growing interest in AI-driven cyber operations underscores the need for vigilance. As adversaries gain more experience and improve their AI implementations, it is likely that these tactics will evolve into a more significant threat. Organizations should prepare by investing in AI-driven defense mechanisms capable of detecting and neutralizing such advanced threats.

10. Evolving Law Enforcement Operations Against Cyber Criminals

2024 marks a significant shift in law enforcement operations targeting cybercriminals.[11],[12] While traditional operations focused primarily on arresting individual criminals, there is now an increasing emphasis on dismantling the infrastructure and ecosystem that enable these actors to operate. This includes taking down dark web marketplaces, seizing servers used for command and

[11] https://www.europol.europa.eu/crime-areas/cybercrime
[12] https://www.fbi.gov/investigate/cyber/news

control, and disrupting the financial networks that facilitate money laundering for ransomware payments.

By focusing on the broader ecosystem, law enforcement agencies aim to create long-term disruption and reduce the overall profitability of cybercrime. Recent coordinated international efforts have shown promising results, such as the shutdown of several major underground forums and hosting providers. These actions not only remove key resources from cybercriminals but also send a strong message to would-be offenders about the risks of participating in such activities.

This strategic pivot is critical, as targeting the enablers of cybercrime can have a cascading effect, limiting the ability of threat actors to regroup and launch new campaigns. Moreover, enhanced collaboration between law enforcement, private sector entities, and cybersecurity researchers has proven essential in identifying and neutralizing these critical components of the cybercrime ecosystem.

JANUARY 24

- Nineteen Individuals Worldwide Charged in Transnational Cybercrime Investigation of the xDedic Marketplace
- Russian National Sentenced for Involvement in Development and Deployment of Trickbot Malware Cryptojacker arrested in Ukraine over EUR 1.8 million mining scheme

FEBRUARY 24

•Warzone RAT infrastructure dismantled Operation Cronos – LockBit disruption

MARCH 24

- Moldovan National Sentenced to Federal Prison for Operating Websites Involved in the Illicit Sale of Compromised Computer Credentials (E-Root Marketplace)

APRIL 24

- LabHost PhaaS disruption
- Justice Department Seizes Four Web Domains Used to Create Over 40,000 Spoofed Websites and Store the Personal Information of More Than a Million Victims

MAY 24

- Operation Endgame: IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee infrastructure takedown
- Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme
- 911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation

JUNE 24

- Operation First Light 2024: Conducted between May and June 2024, targeting online scammers involved in phishing, romance scams, investment scams, and fake shopping websites Four Members of
- Notorious Cybercrime Group 'FIN9' Charged for Roles in Attacking U.S. Companies

JULY 24

- 2024 Operation MORPHEUS to takedown malicious Cobalt Strike infrastructure

AUGUST 24

- Disruption of Radar/Dispossessor Ransomware Group
- Leader of International Malvertising and Ransomware Schemes Extradited from Poland to Face Cybercrime Charges

SEPTEMBER 24

- Dismantling an international criminal network engaged in unlocking stolen or lost mobile phones through a phishing platform
- Russian and Kazakhstani Men Indicted for Running Dark Web Criminal Marketplaces, Forums, and Trainings (WWH Club administrators)

OCTOBER 24

- Additional arrests against LockBit personas
- Doxing of DDoS group Anonymous Sudan
- Ukrainian National Pleads Guilty to "Raccoon Infostealer" Cybercrime

NOVEMBER 24

- Phobos Ransomware Administrator Extradited from South Korea to Face Cybercrime Charges

DECEMBER 24

- Operation PowerOFF: Dismantling services known as 'booter' and 'stresser' websites
- Romanian National Sentenced to 20 Years in Prison in Connection with NetWalker Ransomware Attacks
- Rydox Cybercrime Marketplace Shut Down and Three Administrators Arrested

Part 4: Predictions for 2025

INCD
Israel National
Cyber Directorate

Based on observed trends and expert insights, the following predictions outline the expected cybercrime landscape for 2025:

1. Improved AI-Driven Cybercrime Tactics

Although initial attempts at using AI in malware have been flawed, adversaries are expected to refine their methods. Public reporting[13] have provided the public a glimpse as to how adversaries from all sides of the road (both financially and state motivated) leveraged the accessibility and power of public-use AI tools such as ChatGPT and Gemini. INCD has observed adversaries of hacktivist nature targeting the Israeli cyber-space providing DDoS scripts generated by AI and conducting reconnaissance on potential targets to assess the probability of a victim to pay ransom. By mid-2025, more advanced AI-driven malware with improved functionality and evasion capabilities could emerge. Organizations should prioritize research and development in AI-powered threat detection.

2. Proliferation of Low-Cost, High-Impact Cyberattacks

The trend of leveraging inexpensive, widely available tools for cyberattacks will continue to grow. With the cost of initial access logs and infostealer infections remaining low, attackers can easily mount large-scale operations. This will necessitate better endpoint security and incident response strategies.

[13] https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai , https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

3. Increased Cloud Exploitation Due to Misconfigurations

Cloud adoption is set to expand further in 2025, with more organizations migrating critical workloads to cloud environments. This trend will be accompanied by an increase in attacks exploiting cloud misconfigurations. Emphasis on cloud security training and automated configuration management will be crucial to mitigate this threat.

4. Expansion of Leak-Centric Attacks

The breach-extort-leak model, which gained traction in 2024, will become even more prevalent in 2025. This approach bypasses the need for complex encryption schemes and focuses on public shaming and data exposure to compel ransom payments. Organizations must enhance their data leak prevention measures and crisis communication strategies.

5. Broader Exploitation of Decentralized Technologies

The use of decentralized technologies such as blockchain and smart contracts for malicious purposes will continue to rise. Attackers may leverage these technologies for command-and-control (C2) infrastructure and data exfiltration. Advanced monitoring tools that can detect anomalies in blockchain interactions will become essential.

6. Heightened Collaboration Between Law Enforcement and Industry

In response to the evolving threat landscape, law enforcement agencies are likely to strengthen partnerships with private-sector cybersecurity firms. This collaboration will focus on dismantling cybercrime ecosystems, including dark web marketplaces and financial networks that facilitate ransomware

payments. Cross-border cooperation and intelligence sharing will be key to these efforts.

7. **Increased Emphasis on Zero-Day Vulnerability Exploitation**

The exploitation of zero-day vulnerabilities will remain a significant threat in 2025. With attackers seeking to maximize impact before patches are widely applied, organizations must adopt proactive vulnerability management and threat intelligence capabilities to stay ahead of emerging risks.

8. **Rise of AI-Driven Social Engineering**

Advances in AI-driven impersonation and phishing tools will lead to more sophisticated social engineering campaigns. Attackers will be able to craft highly convincing fake communications, increasing the likelihood of successful breaches. Continuous staff training and advanced email filtering technologies will be essential to mitigate this risk.

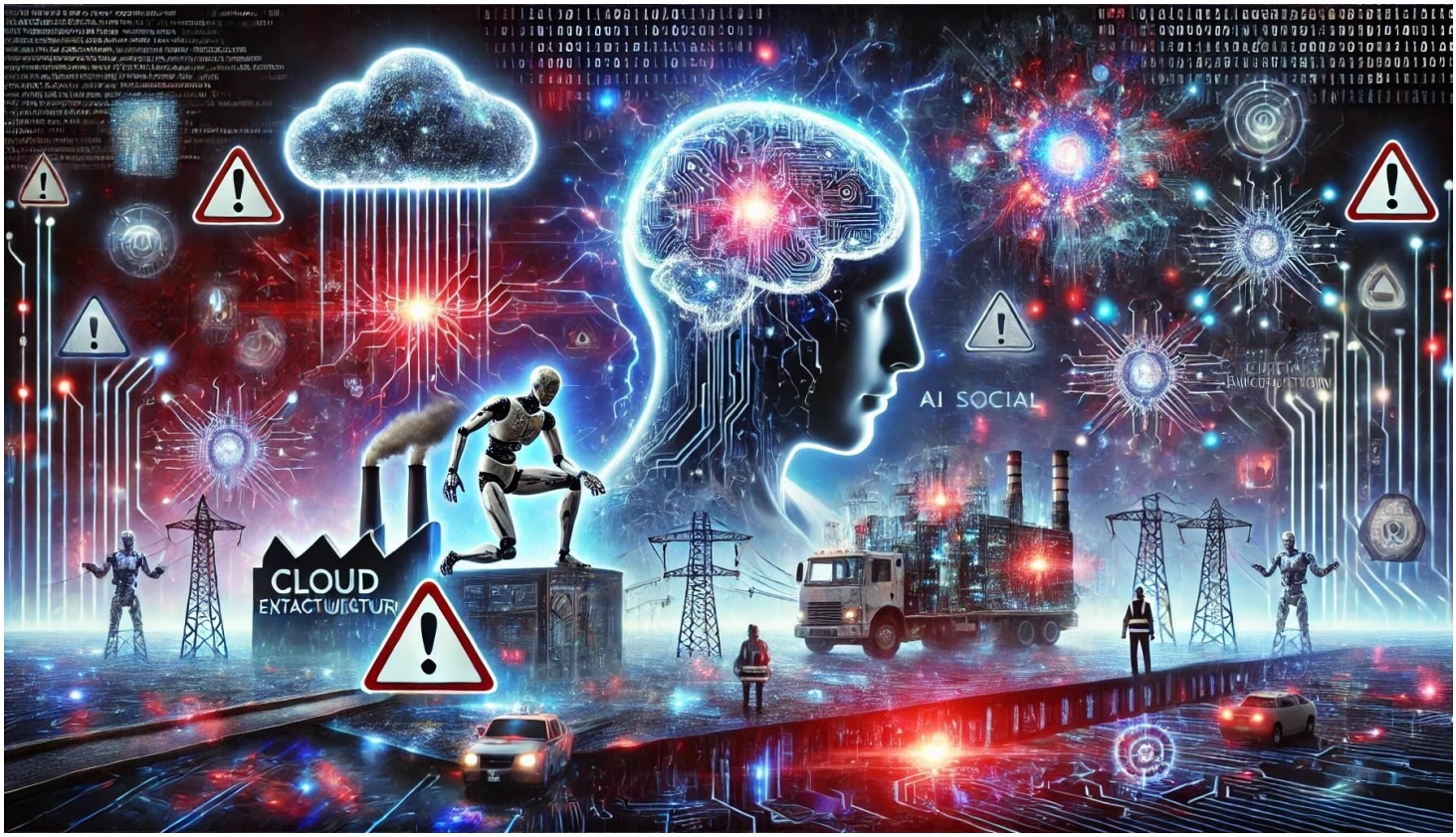
9. **Targeting of Critical Infrastructure with OT-Specific Attacks**

Operational Technology (OT) systems in critical infrastructure sectors, such as energy and transportation, will face increased targeting. Adversaries may exploit vulnerabilities in OT environments to disrupt essential services. Enhanced monitoring, segmentation, and incident response plans tailored to OT systems will be necessary to reduce risks.

10. **Emergence of Quantum-Resilient Cryptographic Attacks**

As quantum computing technology advances, cybercriminals may begin to experiment with attacks that attempt to bypass traditional cryptographic

protections. Organizations should start evaluating and adopting quantum-resilient encryption algorithms to future-proof their cybersecurity defenses.



Cybercrime predictions for 2025 - visualized. Generated using DALL-E

References

1. https://www.databreachtoday.com/recapping-2024s-top-attacks-cybercrime-espionage-more-a-27176
2. https://www.zscaler.com/blogs/security-research/threatlabz-ransomware-report-unveiling-75m-ransom-payout-amid-rising
3. https://www.bitdefender.com/en-us/blog/businessinsights/top-ransomware-trends-for-2024-2025-security-teams-cant-ignore
4. https://www.paloaltonetworks.com/why-paloaltonetworks/cyber-predictions
5. https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025
6. https://blog.bushidotoken.net/2024/12/top-10-cyber-threats-of-2024.html

TTP

TTP Description	MITRE ATT&CK Category
Abuse of Remote Monitoring and Management (RMM) tools	TA0003: Persistence
Exploitation of Managed File Transfer (MFT) systems	TA0001: Initial Access
Info stealers for credential theft	TA0006: Credential Access
Initial Access Brokers selling access	TA0001: Initial Access
Use of zero-day vulnerabilities	TA0042: Resource Development
Encryption-less ransomware attacks (breach-extort-leak)	TA0040: Impact
Leak and shame tactics	TA0040: Impact
Code similarity across ransomware families	TA0042: Resource Development
Abuse of cloud misconfigurations	TA0001: Initial Access
Targeting ESXi and Linux-based environments	TA0001: Initial Access
Abuse of BitLocker for encryption	TA0040: Impact
Use of smart contracts as C2 infrastructure	TA0011: Command and Control
State-sponsored actors collaborating with cybercrime groups	TA0042: Resource Development
Advanced AI-driven malware development	TA0042: Resource Development
Exploitation of decentralized technologies	TA0011: Command and Control
Phishing with AI-driven tools	TA0001: Initial Access

Exploitation of Operational Technology (OT) systems	TA0001: Initial Access
Quantum-resilient cryptographic attacks	TA0040: Impact
Defense evasion tools	TA0005: Defense Evasion
Leveraging stolen credentials for access	TA0006: Credential Access
Use of public shaming as extortion	TA0040: Impact

CVEs known to be used in ransomware campaigns - 2024 (based on CISA KEV)[14]

CVE-2024-4577	PHP Group | PHP
CVE-2024-40711	Veeam | Backup & Replication
CVE-2024-6670	Progress | WhatsUp Gold
CVE-2017-1000253	Linux | Kernel
CVE-2024-23897	Jenkins | Jenkins Command Line Interface (CLI)
CVE-2024-37085	VMware | ESXi
CVE-2024-26169	Microsoft | Windows
CVE-2023-24955	Microsoft | SharePoint Server
CVE-2023-48788	Fortinet | FortiClient EMS
CVE-2024-27198	JetBrains | TeamCity
CVE-2024-21338	Microsoft | Windows
CVE-2024-1709	ConnectWise | ScreenConnect
CVE-2020-3259	Cisco | Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
CVE-2023-22527	Atlassian | Confluence Data Center and Server
CVE-2023-35082	Ivanti | Endpoint Manager Mobile (EPMM) and MobileIron Core
CVE-2023-29357	Microsoft | SharePoint Server

***** END OF DOCUMENT *****

[14] https://www.cisa.gov/known-exploited-vulnerabilities-catalog