This Threat Intelligence Product (TIP) is the sixth in a series assessing adversarial use of generative artificial intelligence that results in harm to investors, broker-dealers and the securities market.

Suggested Routing: *Anti-Money Laundering, Compliance, Cyber, Financial Crimes, Fraud, Information Technology, Operations, Risk and Senior Management.*

Adversarial Use of Generative Artificial Intelligence: GenAI–Enhanced Ransomware Attacks

August 28, 2025

The integration of generative artificial intelligence (GenAI)[1] into the ransomware lifecycle represents a progression by bad actors to leverage emerging technology to enable and further facilitate their nefarious activity. Ransomware typically involves bad actors, including state-sponsored actors, gaining unauthorized access to systems, encrypting and/or exfiltrating data and then demanding payment in return for the decryption key.[2] Bad actors may also use extortion tactics, such as harassing employees, suppliers, and threats to publicly release or sell the victim's data unless a ransom payment is made.

As outlined in FINRA's Regulatory Notice 22-29, ransomware could result in reputational harm, federal and state legal and regulatory consequences, operational disruption and significant financial loss.[3] According to the FBI's Internet Crime Complaint Center (IC3), ransomware complaints rose approximately 32 percent from 2022 to 2024, though many incidents likely go unreported.[4] Reports predict the global damage cost of ransomware attacks will reach $57 billion by 2031.[5] GenAI increases the speed and effectiveness of the cyberattack lifecycle and is changing the cybersecurity threat landscape facing FINRA member firms as well as their customers.

This TIP describes how bad actors can leverage GenAI to conduct targeted ransomware attacks on member firms and offers strategies to mitigate this evolving threat.

Threat Overview

The FBI has warned the public[6] that bad actors are already incorporating GenAI to facilitate financial fraud, and cybersecurity firms have already identified GenAI as being used in malware development.[7] Within the ransomware attack lifecycle, bad actors are likely to leverage GenAI's capabilities to: (1) develop malware; (2) engage in reconnaissance; (3) gain initial access of a firm's system or data through advanced social engineering tactics; (4) establish persistence and spread laterally; (5) locate and exfiltrate data; and (6) deploy the ransomware payload, encrypt data and demand ransom.

GenAI-Enhanced Ransomware Attack Lifecycle

1. *Malware Development*
   Bad actors with novice technical skills might seek to leverage commercial GenAI tools to learn about and develop ransomware, including the entire ransomware attack lifecycle. This could involve the use of "jailbreak" techniques to circumvent controls within consumer-facing Large Language Models (LLMs) to assist in malware development. Less technologically sophisticated bad actors can also purchase malware from Ransomware-as-a-Service (RaaS) providers while focusing on other areas of the ransomware attack lifecycle.[8] More sophisticated bad actors may seek tools on the dark web such as "dark LLMs"—specialized LLMs used to develop malicious code, software and exploits.[9] These bad actors may also use GenAI to develop either polymorphic or metamorphic malware that evade antivirus security by changing either part of the code or creating an entirely new code with each iteration.

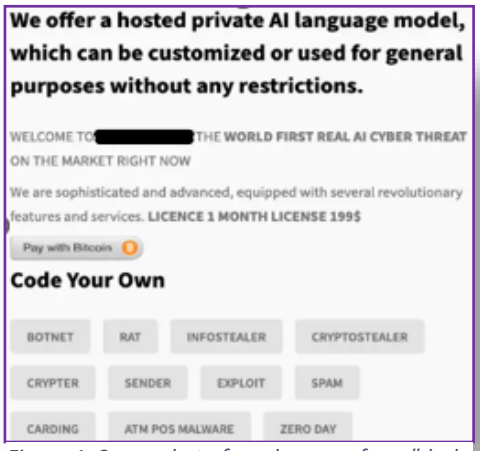

Figure 1. Screenshot of a sales page for a "dark LLM."

2. *Reconnaissance*
   In addition to the reconnaissance tactics covered in prior TIPs addressing the adversarial use of GenAI,[10] bad actors can leverage agentic AI[11] to automate, scale and accelerate their attacks.[12] For example, they may use an ensemble of AI agents to:

   - scrape company websites, LinkedIn posts, and press releases to generate organizational charts, identify email formats (*e.g.,* jane.doe@domain.com), and discover high-value roles that could be targeted;
   - pass information learned to other agents to identify likely passwords for brute force attacks (*e.g.*, jane.doe@domain.com → try JaneDoeNY2025!); or
   - scrape a targets' social media to identify travel-related posts, for example, that would alert the bad actor to an ideal time to execute an attack.

   This automated, multi-pronged approach is feasible with commercial GenAI tools and publicly available workflow automation platforms.

3. *Attempts to Gain Initial Access to Firm's Systems or Data*
   Methods for bad actors to use GenAI to gain initial access include:

   - personalizing phishing emails, and eliminating grammatical errors and awkward phrasing, especially for non-native speakers;
   - creating obfuscated malicious links that bypass email security while adaptively generating phishing campaigns that evolve based on effectiveness; and
   - identifying and exploiting vulnerabilities in Remote Desktop Protocols (RDPs), Server Message Block (SMB) protocols, and Managed Service Providers (MSPs), including zero-day or recently identified vulnerabilities.[13]

4. *Establish Command and Control, Privilege Escalation, and Persistence*

Once bad actors establish control, they might use GenAI to maintain long-term system access through multiple persistence techniques, including:

- generating obfuscated scripts that create randomized scheduled tasks and install disguised Remote Monitoring and Management (RMM) tools that evade traditional security monitoring;
- identifying and exploiting legitimate native tools and processes already present on a victim's system to conduct malicious activity while blending in with routine administrative tasks ("Living-Off-the-Land" techniques); and
- analyzing directory services (*e.g.,* Windows Active Directory) to identify security gaps and circumvent remediation efforts by dynamically adapting to network changes.

5. *Data Targeting and Exfiltration*
   Bad actors might leverage GenAI to identify high-value data containing sensitive customer information or internal records and develop code to exfiltrate it. This data can be later used for double or triple extortion attacks.[14]

6. *Deploy Ransomware Payload, Encrypt Data and Demand Ransom*
   Bad actors might deploy and then execute the ransomware payload across systems in the network, whereby the targeted files would be encrypted. The ransomware payload might clear event logs and disable recovery mechanisms (*e.g.,* Windows Volume Shadow Copy Service).[15]

   To maximize likelihood of payment, bad actors can leverage GenAI to craft multilingual, personalized ransom notes that reference specific stolen files and demonstrate intimate knowledge of the compromised data.

Strategies to Mitigate These Threats

To help mitigate the potential impacts of GenAI–enabled ransomware attacks, member firms may consider taking the following measures:

<u>Education, Training and Business Process Improvements</u>

- Review supervisory procedures and include GenAI-related risks in risk assessments where appropriate.[16]
- Foster a comprehensive cybersecurity culture through regular, mandatory security awareness training, focusing specifically on recognizing GenAI-enhanced threats including sophisticated phishing attempts,[17] voice and video deepfakes, suspicious multi-factor authentication (MFA) requests and early ransomware indicators.[18] This might include tabletop exercises focused on ransomware attacks designed to test your firm's preparedness.[19]
- Update incident response plans and related playbooks to address GenAI-enhanced threats while regularly assessing your firm's resilience against ransomware attacks.[20]
- Proactively engage with your firm's vendors to understand their security capabilities regarding GenAI-enabled ransomware attacks, including their threat detection protocols, incident response procedures, and how they are adapting their mitigation tactics to address evolving GenAI-enabled threats.

Technical Solutions

- Immediately isolate infected systems while maintaining multiple, physically separate backups of sensitive data—this strategy enabled nearly half of ransomware victims to successfully recover in 2024 without paying ransom.[21] Firms might consider cloud backups and physical backups in multiple geographic locations.
- Implement password protection measures such as encrypting employee passwords and implementing MFA for employees and administrator accounts to systems.
- Keep all operating systems, software and firmware up to date to minimize exposure to cybersecurity threats. Implement robust perimeter and endpoint protection through advanced antivirus, endpoint detection and response (EDR) solutions that integrate with network detection and response (NDR) capabilities.[22]
- Implement zero-trust architecture, which would require firms to continuously verify all users, devices and applications while enforcing context-aware least-privilege access controls based on identity, device posture and data sensitivity.[23]
- Deploy centralized log management with extended retention periods and automated correlation rules to quickly identify and review connections between endpoint alerts and network-level compromise indicators. This approach should include a baseline reference point of normal activity to detect deviations.[24]
- Implement solutions to secure environment files (.env), regularly rotate cloud access keys and API credentials, and use vault services to prevent exposure of sensitive authentication information.[25]

Resources and Engagement

- Review FINRA's Cybersecurity page to assist your firm in identifying and mitigating risks and learning about effective controls to protect customer and firm confidential data.
- Attend FINRA-hosted cybersecurity events, including cyber workshops and tabletop exercises as part of FINRA's initiative to combat cybersecurity and fraud risks.
- Continuously engage and share information with your firm's Risk Monitoring Analyst regarding cyber events affecting your firm.
- Develop relationships with your local FBI field office personnel, incorporate them into your incident response plan, and leverage their specialized tools and resources, including potential access to decryption keys that may assist in ransomware recovery efforts.
- Participate in information-sharing communities including Cybersecurity and Infrastructure Security Agency (CISA), SysAdmin, Audit, Network, and Security (SANS), Financial Services Information Sharing and Analysis Center (FS-ISAC), InfraGard, and The National Cyber-Forensics and Training Alliance (NCFTA) to gain early intelligence on emerging threats and access to specialized ransomware mitigation resources.
- Participate in FinCEN's 314(b) information-sharing program to exchange critical threat intelligence with other financial institutions, enhancing collective defense capabilities against sophisticated AI-enhanced ransomware attacks.

- Report attempted and successful attacks to law enforcement at the FBI's Internet Crime Complaint Center (IC3.gov), which also includes an inventory of the FBI's latest threat advisories.

Conclusion

Member firms may consult FinCEN's "Advisory on Ransomware and Use of the Financial System to Facilitate Ransom Payment," for guidance on when ransomware incidents must be reported to FinCEN on a Suspicious Activity Report and reported immediately to appropriate law enforcement authorities.

FINRA encourages member firms and their customers to report any cyber events, including ransomware to:

- FINRA using the Regulatory Tip Form found on FINRA.org;
- The SEC using the Tips, Complaints, and Referrals form or by calling (202) 551-4790; and
- The FBI using its Internet Crime Complaint Center or by calling 1-800-CALLFBI (1-800-225-5324).

We value your input!

How are FINRA's Threat Intelligence Products serving your firm's needs? What risks to your firm, your customers or the markets do you find of greatest concern? Send us your feedback and/or your ideas for topics for future Threat Intelligence Products here.

FINRA's Financial Intelligence Unit (FIU) supports the protection of investors and markets by identifying and assessing threats and trends impacting the financial and securities industry and disseminating actionable intelligence. This TIP was prepared by FINRA's FIU. It is based on internal data and open-source information. Questions may be directed to FIU@finra.org.

This TIP does not create new legal or regulatory requirements or new interpretations of existing requirements, nor does it relieve firms of any existing obligations under federal securities laws, regulations and FINRA rules. Member firms may consider the information in this TIP in developing new, or modifying existing, policies and procedures that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model. Moreover, some information may not be relevant due to certain firms' models, sizes or practices.

In citing various industry publications, FINRA is not endorsing any commercial product or service. Any reference in cited articles to specific commercial products, processes, or services does not constitute or imply their endorsement, recommendation or favoring by FINRA.

You received this email because you are designated as your firm's AML Compliance Contact, Chief Compliance Officer, Chief Information Security Officer, Chief Risk Officer or Regulatory Inquiries contact person in the FINRA Contact System (FCS). While TIPs are not published publicly, we encourage you to forward this TIP on to others within your organization who may benefit and be able to assist in mitigating this threat. Please see suggested routing at the top of this message for potential applicable business areas.

---

[1] Gen AI is a type of artificial intelligence that, based on a user's prompt, will create content, such as text, computer code, audio and video.

[2] *See* CISA's #StopRansomware Guide, https://www.cisa.gov/stopransomware/ransomware-guide.

[3] *See* In the Matter of Industrial and Commerce Bank of China Financial Services LLC (ICBC), Admin. Proc. File No. 3-22335 (Dec. 2, 2024) (finding that ICBC's failure to maintain accurate books and records during and after a ransomware attack violated recordkeeping requirements).

[4] *See* FBI, 2024 Annual Crime Report, April 23, 2025.

[5] *See* Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Exceed $275 Billion By 2031, April 2, 2025.
[6] *See* FBI, PSA: Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud, Dec. 3, 2024.
[7] *See* Raconteur, What we know about the AI-powered ransomware group, Jan. 30, 2025.
[8] *See* IBM, What is ransomware as a service (RaaS)?, Sep. 5, 2024.
[9] *See* Barracuda, LLMs gone bad: The dark side of generative AI, June 20, 2025.
[10] *See* FINRA, Adversarial Use of Generative Artificial Intelligence: Gen AI–Enhanced Business Email Compromise Scams, Feb. 27, 2025 (describing how bad actors might use GenAI to review publicly available information, including social media posts, press releases, and news articles to find the most vulnerable targets or identify exploitable information); *See also* FINRA, Adversarial Use of Generative AI: Gen AI-Enhanced New Account Fraud and Account Takeover, Nov. 21, 2025 (describing a bad actor analyzing social media posts to create highly personalized phishing schemes to be used later in the scheme).
[11] *See* IBM, Agentic AI vs. generative AI (defining agentic AI as AI systems that are designed to autonomously make decisions and act, with the ability to pursue complex goals with limited supervision).
[12] *See* SC Media, How 'Agentic AI' will drive the future of malware, March 19, 2025.
[13] *See* FBI, PSA: High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations, Oct. 2, 2019.
[14] Double extortion tactics involve the unauthorized exfiltration of data in conjunction with encryption, followed by threats of public disclosure on the dark web should the affected party fail to make the ransom payment. Triple extortion tactics include additional coercive measures, including communication with the affected party's customers and supply chain partners to inform them that their data has been compromised.
[15] *See* VMWare, Threat Report: Illuminating Volume Shadow Deletion, Sep. 20, 2022.
[16] *See* NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), Jan. 2023.
[17] *See* CISA, Phishing Guidance: Stopping the Attack Cycle at Phase One, Oct. 2023.
[18] *See* Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017), Training to Mitigate Phishing Attacks Using Mindfulness Techniques. Journal of Management Information Systems, 34(2), 597–626 (teaching individuals to dynamically allocate attention during message evaluation, increase awareness of context, and forestall judgment of suspicious messages).
[19] *See* CISA, CISA Tabletop Exercise Packages.
[20] *See* CISA, Cybersecurity Incident & Vulnerability Response Playbooks.
[21] *See* Palo Alto Networks, Global Incident Response Report 2025
[22] *See* FBI, Ransomware Prevention and Response for CISOs
[23] CISA #StopRansomware Guide, supra note 2.
[24] The process of baselining typically involves collecting data from system logs, network traffic, and user behavior over a defined period, analyzing that information to establish patterns, and then using these patterns to define normal operations against which anomalies can be detected.
[25] *See* Palo Alto Networks, Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments, Aug. 15, 2024.