Executive summary
Cyberthreat trends in the dark web: AI, blockchain, and the infrastructure crisis in the first half of 2026

Drawing on monitoring of open and closed sources—including private Telegram channels, relevant accounts on X (Twitter), specialized hacker forums, and leaked source code and data from the reporting period—this report examines how advances in artificial intelligence and blockchain infrastructure are shaping threat actors' methods, tools, and tactics. We focus specifically on changes in the cybercriminal underground ecosystem: the use of smart contracts in botnet infrastructure and the crisis of trust in bulletproof hosting providers. These changes could shorten attack preparation times, make tools more accessible to new threat groups, and make criminal infrastructure harder to detect and disrupt. Identifying trends early gives defenders time to refine monitoring, reassess priorities, and prepare for scenarios that are not yet widespread.

Trend 1. AI: expanding attackers' capabilities

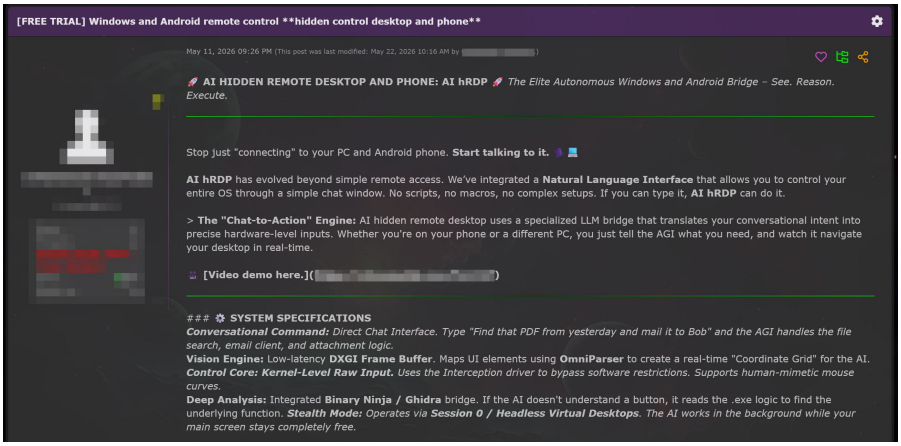
AI as a malware module: just marketing?

AI integration has long been a marketing tactic for malware developers seeking to capitalize on emerging trends. XIRA RAT includes the following intelligent features:

- Keylogging with automatic identification of sensitive data
- Analysis of user activity to identify peak productivity periods and habits

These features can readily be implemented using conventional algorithms without neural networks. Although threat actors still frequently invoke AI to attract attention, this trend is gradually changing. Offerings increasingly feature AI not just as a selling point but also as a practical tool for experimentation during attack preparation and execution. One example is an advertisement offering a free trial of a new tool for threat actors, AI hRDP. AI is the core component of AI hRDP, short for "AI hidden Remote Desktop and Phone." The operator does not need to write scripts or control the device manually. A dedicated LLM bridge translates text commands into specific actions at the hardware input level, effectively functioning as an AI agent. This changes the malware paradigm itself: instead of a hard-coded set of scripts, malware becomes an autonomous agent capable of **making its own decisions based on the host environment**.

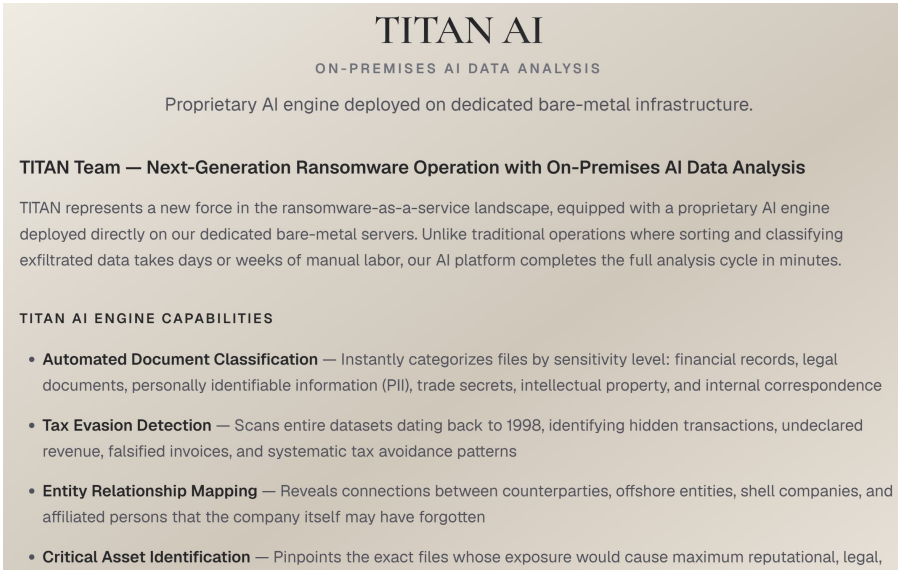
Figure 1. Underground forum post advertising AI hRDP for sale



Optimizing extortion

This points to an emerging trend: ransomware groups are developing **proprietary AI modules** tailored to their specific needs. The ransomware group TITAN AI claims its tool can classify corporate documents by confidentiality level, pinpoint files that could cause the greatest reputational damage, and even identify tax evasion. They claim that the AI runs on their own infrastructure and can process up to 700 GB of data in less than an hour. The system can calculate the optimal ransom demand by determining the maximum amount a victim can afford to pay. Figure

Figure 2. Description of TITAN AI's capabilities on the group's data leak site (DLS)



Without manual intervention, TITAN AI compiles evidence, calculates regulatory fines, and queues data for publication. Rather than simply threatening to publish data, the attackers present a fully developed case outlining the legal and reputational damage the victim faces, taking psychological pressure to a new level. More ransomware-as-a-service (RaaS) groups will openly acknowledge **using AI to analyze stolen information**, adopting TITAN AI's tactics.

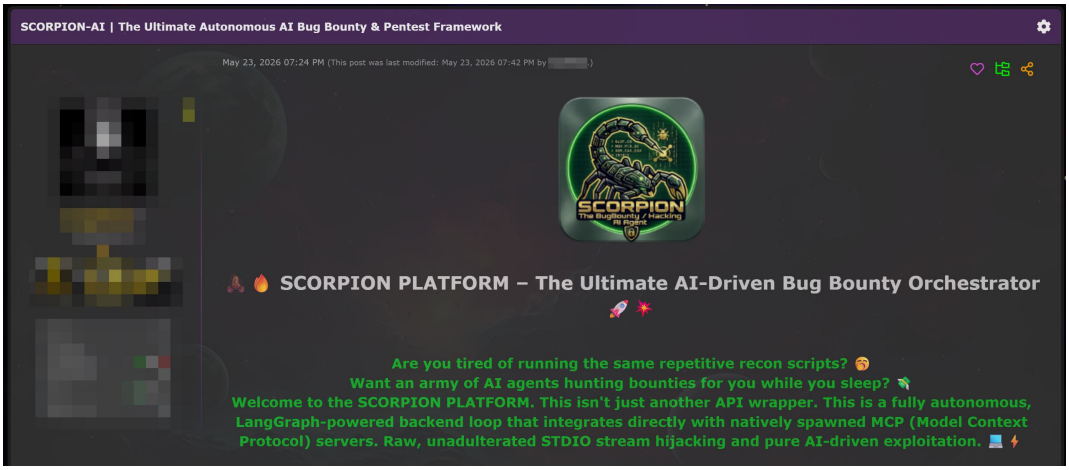
Automating vulnerability discovery with AI

The use of autonomous agents and orchestrators to automate vulnerability discovery and penetration testing is becoming a significant new application of AI. Platforms such as Scorpion, which use AI agents to **automate reconnaissance and penetration testing**, clearly illustrate the current trend. Along with high-speed scanning, such platforms also produce large numbers of false positives and vulnerabilities with limited exploitation potential. Nevertheless, tools that use AI agents eliminate routine tasks, accelerate vulnerability discovery, and make penetration testing easier to automate, **becoming a new standard for both security researchers and cybercriminals**.

AI-assisted malware development

Generative AI is widely used to write malware, but the underground community discourages this practice because it compromises the secrecy of the development process and makes it easier to detect. Malware developers who rely on AI models face not only criticism from their own community and declining code quality, but also risks to their infrastructure, which becomes vulnerable to attacks by fellow cybercriminals.

Figure 3. Underground forum post advertising Scorpion-AI for sale



AI as a preferred target

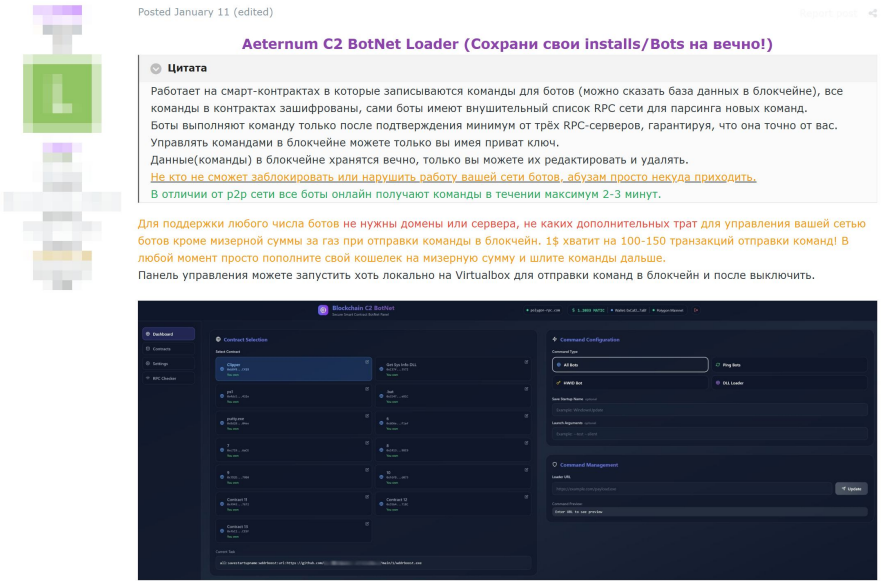
That risk is already visible in the wild: **KAIDO RAT specifically targets the local environments of developers who use AI tools**. It also uses the Claude command-line interface (CLI) as a control channel, accepting commands through Discord or Telegram, and intercepts Model Context Protocol (MCP) communications in the Claude desktop application.

Trend 2. Blockchain as the new standard for botnets

Botnets are beginning to use blockchain infrastructure in place of traditional DNS and command-and-control (C2) mechanisms, making their control infrastructure more resilient. Kimwolf's developers use unconventional techniques, including manipulating DNS settings to interact with internal networks and using the Ethereum Name Service (ENS), built on the Ethereum blockchain, to locate command-and-control (C2) servers. In early 2026, financially motivated threat actors adopted this approach, replacing conventional C2 servers entirely with smart contracts.

Aeternum's defining feature is the complete replacement of traditional C2 servers with decentralized infrastructure based on smart contracts on the Polygon blockchain. Infected devices retrieve and parse new instructions through public remote procedure call (RPC) nodes, which are servers that enable interaction with a blockchain network by processing queries and submitting transactions. This design significantly reduces operating costs: $1 worth of the MATIC cryptocurrency covers 150 transactions, and the attacker does not need to pay for hosting.

Figure 4. Underground forum post describing the Aeternum botnet's functionality

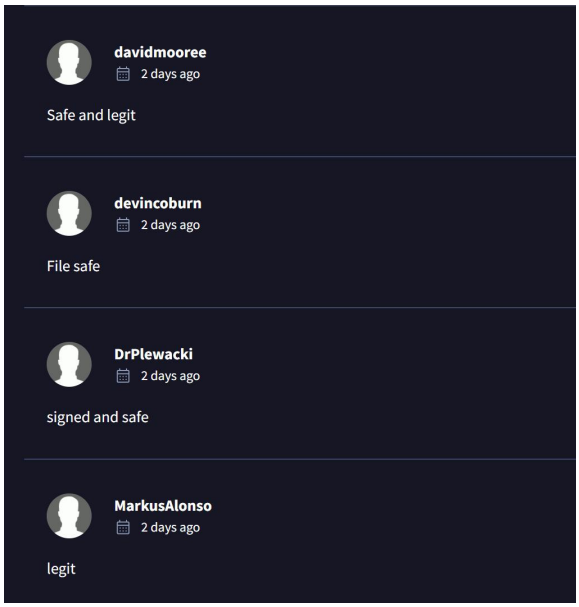


The release of another project, Void Botnet, on March 7, 2026, provides further evidence that blockchain is becoming a new standard in the botnet market. We expect **blockchain adoption in botnets to become widespread in the near term**, although it will not fully replace conventional C2 servers.

Trend 3. Evolution of cybercriminal tools

Threat actors are increasingly **targeting business logic and decision-making processes rather than code vulnerabilities**. Examples include tools that automate attacks on interactive voice response (IVR) systems and techniques that manipulate the reputation of malicious files on VirusTotal to bypass security filters. To counter these threats, organizations need to complement traditional defenses, such as file detection and signature-based blocking, with in-depth behavioral analysis and monitoring of transaction sequences.

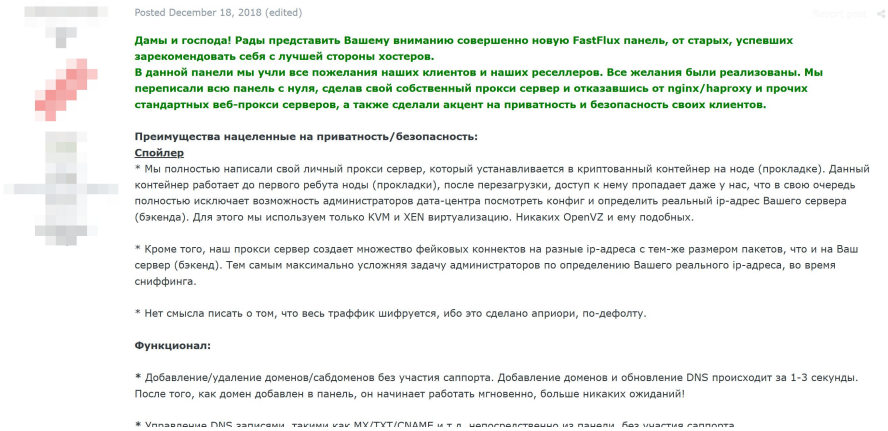
Figure 5. Examples of comments on VirusTotal



Trend 4. Takedowns of hosting providers

Problems affecting several major hosting and VPN providers have triggered a **crisis of trust in the underground community**. 1VPN was dismantled during the international Operation Saffron on May 19–20, 2026. In early May 2026, Yalishanda's fast-flux service suddenly went offline. On May 2, 2026, 4VPS, a service marketing itself as a bulletproof hosting provider, suffered a major attack. These incidents clearly demonstrate that threat actors are also vulnerable to supply chain risks. A vulnerability or hidden backdoor in purchased software, or the **compromise of a service provider, can instantly disrupt the buyer's entire attack chain.**

Figure 6. Advertisement for the service on the dark web



Posted December 18, 2018 (edited)

Дамы и господа! Рады представить Вашему вниманию совершенно новую FastFlux панель, от старых, успевших зарекомендовать себя с лучшей стороны хостеров.
В данной панели мы учли все пожелания наших клиентов и наших реселлеров. Все желания были реализованы. Мы переписали всю панель с нуля, сделав свой собственный прокси сервер и отказавшись от nginx/haproxy и прочих стандартных веб-прокси серверов, а также сделали акцент на приватность и безопасность своих клиентов.

Преимущества нацеленные на приватность/безопасность:
Спойлер
* Мы полностью написали свой личный прокси сервер, который устанавливается в криптованный контейнер на ноде (прокладке). Данный контейнер работает до первого ребута ноды (прокладки), после перезагрузки, доступ к нему пропадает даже у нас, что в свою очередь полностью исключает возможность администраторов дата-центра посмотреть конфиг и определить реальный ip-адрес Вашего сервера (бэкенда). Для этого мы используем только KVM и XEN виртуализацию. Никаких OpenVZ и ему подобных.

* Кроме того, наш прокси сервер создает множество фейковых коннектов на разные ip-адреса с тем-же размером пакетов, что и на Ваш сервер (бэкенд). Тем самым максимально усложняя задачу администраторов по определению Вашего реального ip-адреса, во время сниффинга.

* Нет смысла писать о том, что весь траффик шифруется, ибо это сделано априори, по-дефолту.

Функционал:

* Добавление/удаление доменов/сабдоменов без участия саппорта. Добавление доменов и обновление DNS происходит за 1-3 секунды. После того, как домен добавлен в панель, он начинает работать мгновенно, больше никаких ожиданий!

* Управление DNS записями, такими как MX/TXT/CNAME и т.д. непосредственно из панели, без участия саппорта

Reports that 6 GB of data allegedly belonging to 4VPS had been offered for sale on another platform for $20,000 attracted particular attention. It soon emerged that the dataset included information belonging to the ransomware-as-a-service (RaaS) group The Gentlemen. Analysis of the data showed that, when selecting targets, The Gentlemen prioritize an organization's role in critical infrastructure over its revenue. The leak also highlights the use of Chinese large language models, including Kimi, Ernie, and DeepSeek, to generate and analyze code. The attackers are also considering locally hosted LLMs for processing large volumes of stolen data to identify the most valuable information and increase pressure on victims. The Gentlemen's reliance on AI reinforces the observation that **it is gradually becoming a core component of the toolkit used by modern ransomware groups**.

Cyberthreat trends in the dark web: AI, blockchain, and the infrastructure crisis in the first half of 2026

Learn more about Positive Technologies researches