



| Flash |

AI-Powered Tool to Target Cryptocurrency Wallets in Development

F-2024-08-01a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor,
Cryptocurrency

August 1, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on August 1, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | AI-Powered Tool to Target Cryptocurrency Wallets In Development

> Key Findings

- On July 25, 2024, untested threat actor “Michelangelo” posted in a dark web forum advertising a new artificial intelligence (AI)-powered malicious tool designed to facilitate attacks targeting cryptocurrency wallets.
- The tool lists an array of features that enable various methods of obtaining passwords associated with victims’ cryptocurrency wallets. An emphasis is also placed upon user convenience, flexibility, and management of attack processes.
- While tools with brute-forcing and password-mining capabilities are not new, this tool allegedly contains innovative features that reflect an appetite amongst cybercriminals to develop and commercialize malicious techniques able to target the growing cryptocurrency economy.

| Details

On July 25, 2024, untested threat actor Michelangelo posted in the primarily Russian-speaking dark web forum Exploit advertising a new AI-powered tool designed to facilitate “complex, sophisticated, and large-scale” attacks targeting cryptocurrency wallets. Rather than searching for buyers, Michelangelo appears to be seeking other

threat actors able to cooperate in development—particularly those able to integrate the tool into their own projects.

- A list of features is included in the advertisement, the majority of which are centered around user convenience, flexibility, and the ability to manage and monitor attacks in real time. These include command line and web interfaces, task scheduling, and real-time monitoring and analytics.
- Other details specify the tool's ability to facilitate and enhance password-checking and brute-forcing processes. Among these is the use of machine learning algorithms to conduct AI-enhanced password prediction and automate password spraying leveraging previously-obtained information, as well as the ability to use chosen rules and custom dictionaries.



Hub for sophisticated complex attacks on crypto wallets using AI and optimized distributed computing

By Michelangelo, Thursday at 04:22 PM in [Other] - everything else

About the project:

- **CLI and web interface**: Convenient tools for launching and managing attacks, as well as monitoring the process in real time.
- **Cloud Integration**: Support for AWS, Google Cloud and Azure to scale attacks and securely store data and configurations.
- **Support for various wallets and files**: MetaMask, Exodus, Electrum, Bitcoin Core, Blockchain, etc.
- **Task Scheduler and Notifications**: Ability to schedule attacks, notification system (mail, SMS, messengers) and logging with analytics.
- **Manage and distribute tasks between GPUs**: Support and optimize GPU utilization and maximize performance.
- **Password Storage Database**: Utilize password database, automatically update and manage the database.
- **Monitoring and analytics**: Real-time attack tracking via web interface and CLI, generate reports on attack results.
- **Intelligent password mining**: Using machine learning algorithms to analyze and adapt attacks, predicting passwords based on big data analysis.
- **Adaptive Attacks**: Changing attack strategy in real time, dynamic resource reallocation.
- **Team Management**: Task allocation and collaboration on attacks, ability to share dictionaries and configurations.
- **Automated Recovery**: Automatic data recovery after successful password cracking, integration with backup systems.
- **Attacks using known data (Password Spraying)**: Using information about previous passwords to generate additional variants.
- **Integration with external data sources**: Analyzing leaked databases to update password dictionaries, integration with data leak analysis services.
- **Parallel attack execution**: Support for multi-threaded attacks, optimize resource allocation.
- **Custom dictionaries and rules**: Create and use custom dictionaries, set of instructions for generating additional password variants.
- **Computing Resources**: Utilize powerful computing resources and the ability to manage all aspects of the farm.
- **Scalable Attack Vector**: Realization of more than 16 types of attacks.

And this is not the whole list of functions, we are actively working 24/7 and expanding the functionality.

Exploit post by Michelangelo advertising new tool

Source: ZeroFox Intelligence

The advertisement does not specify exactly how the tool enables attacks or the necessary prerequisites, but it is likely that a threat actor would first need to obtain initial network access. Once established, the tool likely leverages the victim's hardware resources to conduct password mining and spraying processes, attempting to gain access to local crypto wallets.

- The “Passwords” that Michelangelo claims the tool can obtain could relate to those guarding an account, the private keys associated with cryptocurrencies, or the recovery seeds associated with security codes used to perform recovery efforts.
- However, given the tool’s apparent reliance upon optimized GPU utilization, it is very likely that it seeks to obtain private keys able to grant full access to the cryptocurrency.

Upon gaining access to the victim’s cryptocurrency, the funds can be transferred to a wallet owned by the attacker before various laundering techniques, such as the use of tumblers, obfuscate the funds.

The tool is currently under development, and its completion timeline is not specified. Given its likely need to be deployed to victim networks, Michelangelo’s sought-after collaborators almost certainly include threat actors able to provide initial network access, malware operators able to embed the tool within malicious software (thereby providing a delivery method), or botnet operators who are seeking to exploit large numbers of compromised credentials. It is unknown if the tool will be sold to a single buyer, multiple buyers, or provided as a subscription-based service.

While tools with brute-forcing and password-mining capabilities are not new, this tool allegedly contains innovative features that reflect an appetite amongst cybercriminals to develop and commercialize malicious techniques able to target the growing cryptocurrency economy.

Recommendations

- Always use reputable, well-established cryptocurrency platforms, exchanges, and wallet services. Avoid those that are unfamiliar, especially if they appear to contain design errors that arouse suspicion.
- When visiting cryptocurrency platforms, be sure that the web page is legitimate before entering sensitive information. Some phishing scams target these pages specifically, using brand impersonation and web page cloning to target users.
- Be aware of cryptocurrency scams that leverage social engineering hooks, such as the endorsement of a given platform by a celebrity or the promise of a “giveaway” in exchange for a small upfront cost.
- Ensure network and cryptocurrency wallet passwords are complex, not repeated, stored securely, and changed regularly.
- Passwords, private keys, and seed phrases should be stored offline where possible and should not be shared or stored via web browser-saving tools.
- Where possible, cryptocurrency wallets should employ phishing-resistant multi-factor authentication (MFA) protocols.
- Consider the use of cold cryptocurrency wallets such as paper and hardware wallets, which offer heightened security. Multiple cryptocurrency wallets should be used for the storage of significant funds.
- Ensure that software updates and security patches relating to operating systems, security software, and cryptocurrency wallets are kept up to date.
- Only access cryptocurrency services via private Wi-Fi networks, and consider the use of a Virtual Private Network (VPN).
- Organizations should adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (R&DE) threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%