






# Mamont and Million Short: Cybersecurity Tools Report

Intern: Anoop Shivadas



ID: 129

## Table of Contents

1. Introduction 
2. Mamont Banking Trojan 
3. Million Short Search Engine 
4. Conclusion 
5. References 

## Introduction

This report examines two seemingly unrelated **cybersecurity tools** – *Mamont* and *Million Short* – each of which plays a unique role in the digital domain. **Mamont** is a recently discovered Android banking trojan (malicious software) used by cybercriminals to steal financial information. Its name is Russian for “mammoth,” reflecting its goal of massive financial theft [cybersecurityinformer.com](https://cybersecurityinformer.com). Security researchers have documented Mamont spreading via phishing on messaging platforms (like Telegram) or fake apps, and then siphoning off victims’ SMS codes and banking credentials [therecord.media/securelist.com](https://therecord.media/securelist.com). In contrast, **Million Short** is an unconventional *search engine* designed for discovery. Launched in 2012 by Exponential Labs, it allows users to **exclude** the top *N* websites (up to one million) from search results, revealing obscure or “long-tail” content [en.wikipedia.org/wired.com](https://en.wikipedia.org/wired.com). This is intended to combat SEO dominance by filtering out highly ranked, often SEO-optimized sites, making room for hidden gems.

-  **Mamont:** An Android banking trojan (Russian “mammoth”) that infects devices via deceptive apps, enabling attackers to hijack SMS-based banking transactions [cybersecurityinformer.com](https://cybersecurityinformer.com) [therecord.media](https://therecord.media).
-  **Million Short:** An experimental web search engine that *removes* the most popular sites from results (e.g. top 1 million), offering a “discovery” experience of content missed by Google/Bing [en.wikipedia.org/wired.com](https://en.wikipedia.org/wired.com).

The following sections explore each tool in depth. **Mamont** will be analyzed in terms of its infection methods, capabilities, and mitigation, while **Million Short** will be detailed

regarding its features, use cases, and impact on search practices. The report uses credible sources to ensure accuracy.

## Mamont Banking Trojan 🐘

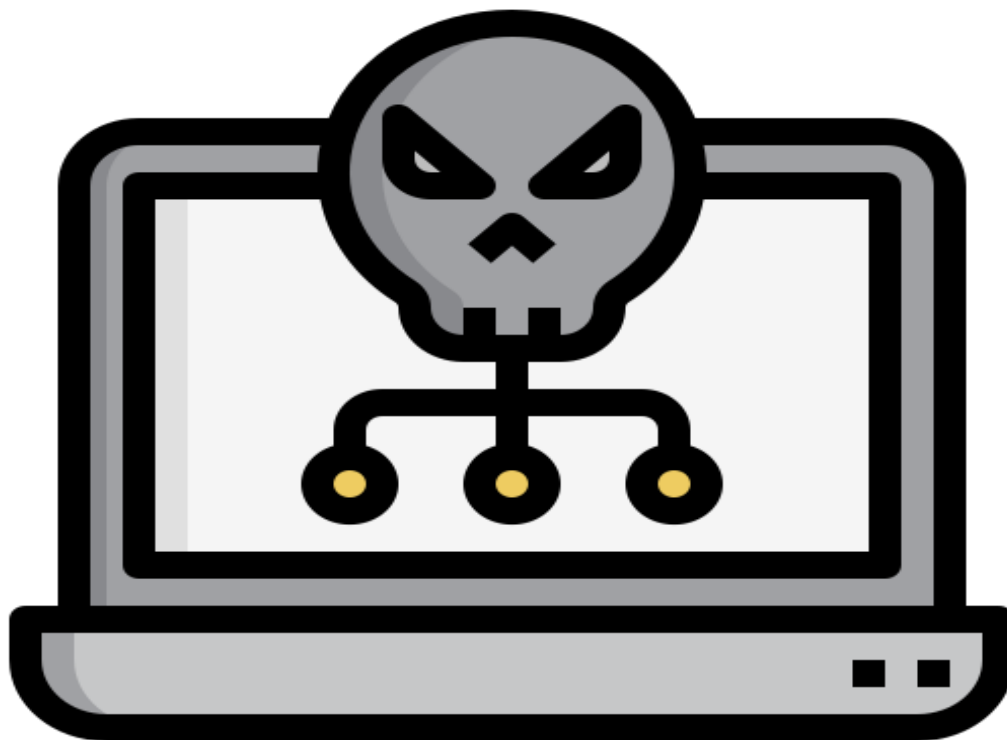







Figure 1: **Mamont** (Russian for “mammoth”) banking trojan – an Android malware targeting financial accounts [cybersecurityinformer.com/therecord.media](https://cybersecurityinformer.com/therecord.media). Mamont is a sophisticated mobile banking trojan first identified in late 2024 [cybersecurityinformer.com](https://cybersecurityinformer.com). It is designed to steal money by intercepting SMS-based two-factor authentication and banking credentials. Russian authorities have linked it to hundreds of cybercrime incidents and even arrested developers of the malware [therecord.media/cybersecurityinformer.com](https://therecord.media/cybersecurityinformer.com). According to security reports, Mamont is often **distributed via Telegram** and other messaging platforms. Attackers lure victims with fake offers (e.g. cheap bulk-priced goods) and then send a malicious app to track the “parcel” – a decoy that actually installs Mamont on the device [securelist.com/therecord.media](https://securelist.com/therecord.media). Once installed, the trojan asks for extensive permissions (background operation, SMS, notifications, calls) and then begins exfiltrating sensitive data. Notably, Mamont requests the user’s *tracking number* (from the fake order), which it forwards along with device info to the attackers’ server – a tactic used for victim identification [securelist.com/therecord.media](https://securelist.com/therecord.media). This elaborate scam (see Figure 1) has proven very convincing, as noted by Kaspersky researchers [securelist.com](https://securelist.com).

Key characteristics of **Mamont** include:

-  **Name & Type:** Android banking trojan; the name “Mamont” literally means “mammoth” in Russian [cybersecurityinformer.com](https://cybersecurityinformer.com). It focuses on financial theft and credential capture.
-  **Spread & Infection:** Delivered via Telegram channels or instant messages. Victims receive fraudulent prompts (e.g. clicking a video link or special “tracker” app) that lead to a phishing site. For example, users might see a message saying their order has shipped with a link to download an Android *tracking app* – but this app is Mamont in disguise [securelist.com/therecord.media](https://securelist.com/therecord.media). The malware has also been packaged as a fake Google Chrome installer in some cases [therecord.media](https://therecord.media).
-  **Functionality:** Once running, Mamont steals two-factor SMS codes and intercepts push notifications. It can forward all incoming SMS/call data to the attackers and execute fraudulent bank transfers via mobile banking systems [therecord.media/securelist.com](https://therecord.media/securelist.com). The trojan’s code includes customizable text overlays, allowing it to pop up fake login windows to harvest passwords. It also has a self-propagation feature, sending the malware to contacts in the victim’s messenger apps [therecord.media/securelist.com](https://therecord.media/securelist.com).
-  **Impact:** The malware has been tied to over 300 attacks, enabling criminals to siphon funds from victims’ accounts. In a typical scheme, stolen money is routed through phone numbers and e-wallets controlled by the attackers [therecord.media](https://therecord.media). The use of trust-building tactics (like no prepayment for goods) has made it especially effective against both individuals and businesses [securelist.com](https://securelist.com).
-  **Detection & Protection:** Security products (e.g. Kaspersky) detect this threat as *Trojan-Banker.AndroidOS.Mamont* [securelist.com](https://securelist.com). To stay safe, users should **never click unknown links** or download apps outside official stores. The experts strongly advise against trusting unsolicited offers or installing apps from unofficial sources [securelist.com](https://securelist.com). Using a reputable mobile security solution is recommended to block trojans like Mamont. Key prevention rules include:
  - Don’t click links in messages from strangers [securelist.com](https://securelist.com).
  - Be skeptical of offers that seem “too good to be true” [securelist.com](https://securelist.com).
  - Only download apps from official app stores (Google Play) [securelist.com](https://securelist.com).
  - Keep the device updated and protected with antivirus software [securelist.com](https://securelist.com).

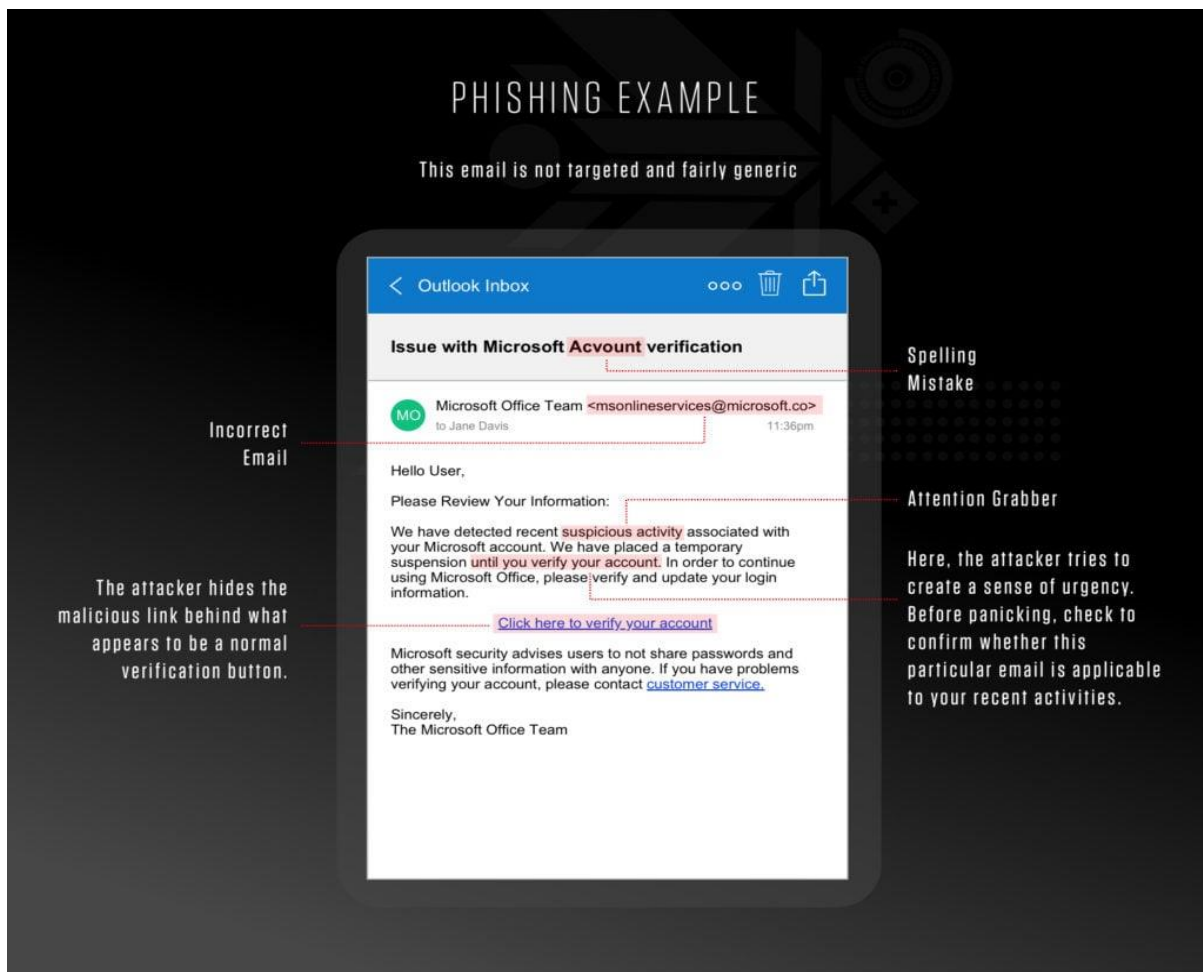


Figure 2: Phishing message from a fake online store. The victim is told their order can be tracked via a special app. In reality, the link downloads Mamont malware to the Android device [securelist.com](https://securelist.com). The scam in Figure 2 shows an example message sent by the fraudsters. Once the user clicks the “Tracker” link and installs the app, the Mamont trojan takes over the device. As Kaspersky notes, the trojan then continuously communicates with its command-and-control (C2) server to exfiltrate data and receive commands [securelist.com/therecord.media](https://securelist.com/therecord.media).

In summary, Mamont is a **malicious tool** that exploits social engineering and mobile banking vulnerabilities. It illustrates how threat actors blend seemingly legitimate services (parcel tracking, chat apps) with malware distribution. The comprehensive analysis by security researchers and law enforcement underscores the importance of user vigilance and good security hygiene to counter such threats [therecord.media/securelist.com](https://therecord.media/securelist.com).

## Million Short Search Engine 🔍





Million Short is an **alternative web search engine** focused on exploring the “long tail” of the internet. Launched on April 30, 2012, by Toronto startup Exponential Labs [en.wikipedia.org](https://en.wikipedia.org), it allows users to **filter out** the top  $N$  (up to one million) most popular

websites from their search results [en.wikipedia.orgwired.com](https://en.wikipedia.org/wired.com). In other words, Million Short literally *removes* the web's biggest sites (e.g. Wikipedia, Amazon) from the result set, letting lesser-known pages surface. The idea is to present a more *discoverable* set of results rather than the same mainstream sites that dominate Google or Bing. As Wired described it:



“Want to see the web’s long tail? Just cut out the top 1 million websites and search through what’s left. That’s exactly what the aptly named Million Short search engine promises to do.”[wired.com](https://wired.com)

The search engine’s emphasis on discovery is by design. According to Wikipedia, Million Short brands itself as “more of a discovery engine,” since it “allows users to filter the top million websites on the internet out of their search, resulting in a unique set of results and placing an emphasis on content discovery”[en.wikipedia.org](https://en.wikipedia.org). This mechanism also **counteracts SEO bias**: by excluding the heavily SEO-optimized sites, Million Short helps users find content that might otherwise be buried deep in conventional search results. Tech media noted that this approach is “designed to combat the impact that aggressive black and grey hat SEO practices have on mainstream search results”[en.wikipedia.orgwired.com](https://en.wikipedia.org/wired.com).

Key features of **Million Short** include:

-  **Core Concept:** Excludes popular domains from results. Users can choose to remove the top 100, 1,000, 10,000, 100,000 or 1,000,000 sites from their queries [en.wikipedia.orgwired.com](https://en.wikipedia.org/wired.com). For example, removing the “top 100” will skip the 100 most visited websites, while “top 1,000,000” skips the top million. This simple slider gives control over how narrow or broad the filter is.
-  **Technical Approach:** According to its Wikipedia entry and media interviews, Million Short initially worked by combining the Bing search API with its own crawl data to identify and exclude top-ranked sites [en.wikipedia.orgwired.com](https://en.wikipedia.org/wired.com). The engine constantly crawls the web and maintains its own ranking list to know which domains to omit.
-  **Customization & Add-ons:** Beyond filtering by popularity, Million Short offers extra tools for customizing results. Users can “boost” or “block” specific sites they want to see more or never see [millionshort.com](https://millionshort.com). It also has “Topicals” – mini-search engines dedicated to specific topics (e.g. “Egyptian History”) – allowing curated searches on sub-fields. Other filters include shopping results, advertising, and country-specific domains. The interface is designed to be ad-free and privacy-friendly.
-  **Privacy & Business Model:** Million Short prides itself on being **ad-free and private**. For over a decade it was offered free of charge with no ads [millionshort.com](https://millionshort.com). (In 2023, due to rising costs, Million Short introduced a paid subscription option to keep the service running, but basic functionality remains

available.) The site's own manifesto emphasizes that it remains a "*private search experience*" where results are not SEO-driven [millionshort.com](http://millionshort.com).

-  **Use Cases:** The unique nature of Million Short has attracted a niche audience. OSINT researchers and curious users turn to it to uncover content that traditional search hides. By trimming the "head" of the web, Million Short makes it easier to stumble upon obscure blogs, region-specific pages, and newly launched sites. For example, Wired noted that Million Short can reveal personal websites, small forums or niche Q&A pages that Google usually buries [wired.com](http://wired.com). Search Engine Watch similarly observed that it "lets you purge up to 1 million of the web's most prominent sites" to give something new [searchenginewatch.com](http://searchenginewatch.com). In essence, it's often more of a **discovery tool than a precision search**.
-  **History & Impact:** At launch, Million Short generated significant attention online. Tech blogs and forums (Reddit, Hacker News) buzzed about "the search engine that plumbs the web's depths." Major outlets like Wired, TechCrunch and The Verge covered it [wired.com](http://wired.com) [en.wikipedia.org](http://en.wikipedia.org). The novelty of exploring the web's "long tail" spurred research into its relevance, and even academic studies were done on its utility. Although it remains a niche service, Million Short's concepts influenced conversations about search diversity and anti-spam measures. Its related experiments (Million Tall, Million Short "It On" comparisons, DNS filters) also highlighted how search results can be skewed by popularity [en.wikipedia.org](http://en.wikipedia.org).

Million Short's **interface** is straightforward. (Figure 3 illustrates a typical search.) Users enter a query and then select a filter (e.g. "Remove top 10k sites"). The results update accordingly. Because it's relatively simple compared to giant search engines, Million Short's result count may be smaller and its index less comprehensive. But that is by design – the aim is *quality over quantity* for the *uncommon*.



Figure 3: **Million Short** search interface. Users enter keywords and choose how many top sites to exclude (e.g. top 100, top 1k, etc.), yielding results from the long tail [en.wikipedia.org](http://en.wikipedia.org) [wired.com](http://wired.com).

In summary, Million Short is a **cybertool** that inverts standard search logic. Instead of climbing to the top results, it deliberately skips the obvious and shows the rest. For cybersecurity professionals, this can be useful in OSINT (open-source intelligence) investigations: for example, finding less-known domains or pages that might contain intelligence or indicators of compromise that common queries would miss. It is not a replacement for Google, but rather a complementary tool for discovery. The combination of its filter sliders, site boosting/blocking, and privacy stance makes it an interesting *adjunct* in the security research toolkit [en.wikipedia.org/millionshort.com](https://en.wikipedia.org/millionshort.com).

## Conclusion

Both **Mamont** and **Million Short** highlight different facets of the cybersecurity landscape. Mamont, as a malicious **tool used by attackers**, underscores how social engineering and mobile technology can be weaponized to commit fraud. Its emergence and the resulting law enforcement action (three arrests linked to hundreds of crimes [therecord.media/cybersecurityinformer.com](https://therecord.media/cybersecurityinformer.com)) remind us that mobile banking security and user awareness remain critical. In parallel, Million Short represents a **legitimate tool for defenders and analysts**. By filtering out mainstream sites, it helps uncover hidden information and can aid OSINT investigations or SEO research. The two case studies together illustrate a broader principle: the internet contains both threats to guard against and unconventional resources to exploit for security purposes. Understanding Mamont's techniques informs better mobile security practices, while leveraging a search tool like Million Short can broaden the information-gathering horizon. Altogether, these tools – one malicious, one benign – reinforce the importance of continual learning in cybersecurity.

## References

- Kaspersky SecureList. “Download a banker to track your parcel” (analysis of Mamont Trojan). Dec 2024. [securelist.com](https://securelist.com/securelist.com)
- Recorded Future News (The Record). “Russia arrests three for allegedly creating Mamont malware...” Mar 27, 2025. [therecord.media](https://therecord.media)
- CybersecurityInformer.com. “Russian authorities arrest three suspects behind Mamont Android banking trojan.” Mar 28, 2025. [cybersecurityinformer.com](https://cybersecurityinformer.com)
- Wikipedia. “Million Short” (Exponential Labs search engine) [en.wikipedia.org](https://en.wikipedia.org).
- Search Engine Watch. John Rampton, “Million Short Search Engine Serves Up Nothing But Obscure Results,” May 2012 [searchenginewatch.com](https://searchenginewatch.com).
- Wired Magazine. Scott Gilbertson, “Million Short: A Search Engine for the Very Long Tail,” May 2012 [wired.com](https://wired.com).
- MillionShort.com (official site). *Plans & About* pages (ad-free, private search engine) [millionshort.com](https://millionshort.com).