dti.domaintools.com /inside-a-crypto-scam-nexus/

Inside a Crypto Scam Nexus

⋮ 10/9/2025

Cybercriminals are orchestrating a cryptocurrency “wallet drain” conspiracy that spans sketchy browser extensions, mobile profile phishing, and sham cryptocurrency trading platforms, all tied together by a single web of infrastructure. In this investigative deep dive, we expose how multiple scam websites such as medaigenesis[.]cc, novacrypt[.]net, and zzztd[.]com were hosted on the same server IP address, 8.221.100[.]222. These sites formed a coordinated infrastructure used to steal cryptocurrency from unsuspecting users. As of September 25, the A record for novacrypt[.]net stopped resolving to this IP address, which could indicate that the attackers have shifted infrastructure or that the domain has been taken down. The scams range from browser extension popups and iPhone configuration profile traps to fraudulent web trading apps, all of which are backed by clever social engineering. Below, we break down each component of this operation, provide code snippets and network maps, and outline Indicators of Compromise (IOCs) to help you recognize and avoid these threats.

MedAI Genesis – A Fake Medical DAO With a Draining Agenda

One of the more elaborate fronts in this scam network is **medaigenesis[.]cc**, which presents itself as a next generation healthcare initiative powered by blockchain and artificial intelligence. Styled as “MedAI Genesis,” the site promotes itself as the future of personalized health management, backed by buzzwords such as AI 5.0, on chain biometric data, and health NFTs.

“Redistribution of medical resources,” it claims. “Rise of the health currency.”

At first glance, it reads like a cryptocurrency investor’s dream married to a healthcare revolution. The platform boasts features like:

- AI-driven medical consultation,
- NFT-based health records,
- On-chain health governance voting,
- A utility token called MDAI.

But under the hood, this is a scam in a lab coat.

Instead of delivering health features, the site launches a wallet connect popup through a browser extension. Its objective is to drain cryptocurrency holdings under the guise of activating access features. The scam blends health tech themes with cryptocurrency mechanics to create a believable front that convinces victims to interact with their wallets, triggering the theft.

How it works: The CSS from Trust Wallet’s Chrome extension (ID egjidjbpglichdcondbcbdnbeeppgdph) is a key mechanism to provide styling and fonts. The risk arises when scammers replicate this styling to create a phishing site that appears identical to a legitimate Trust Wallet connect prompt. On a fake site, clicking “Connect” does not trigger a secure wallet handshake, instead, the site can hide code that makes your wallet approve a dangerous transaction. It may look like you are just connecting, but if you click approve, the scammer could get permission to take your money.

Scam in Action: Imagine visiting a new cryptocurrency platform and seeing a familiar professional-looking “Connect Trust Wallet” dialog. Believing it is safe, you click connect only to be asked to sign a transaction that silently hands control of your wallet to the scammer. Functions like setApprovalForAll or direct transfers can then be abused to drain assets if you approve.

Notably, the extension’s ID corresponds to a Trust Wallet extension listed on the official Chrome Web Store, which raised alarms. The extension’s review page is filled with reports of stolen funds, scam, and backdoors. It appears scammers either published a fake but convincing “Trust Wallet” extension or leveraged the legitimate one. Either way, its presence in the victim’s browser is what enables the “Fake Wallet Connect” popup to appear.

This tactic is especially dangerous because the CSS makes the interface appear authentic, while the real attack would occur in the underlying JavaScript. In this case, the phishing site (for example, a staged platform like “MedAI Genesis”) appears to still be under construction. The look-alike Trust Wallet pop-up is present in the code but not fully functional, as several links return errors or placeholders, and even the Telegram channel is commented out. These indicators suggest the threat actor could be staging the site for a future campaign. In the meantime, the page is decorated with fake features such as “AI-Powered diagnostic service payments” and “Global health data NFTization,” along with unverifiable profiles and logos from real companies like Pinksale and Binance Smart Chain. These credibility tricks are designed to lower a victim’s guard once the phishing flow is fully enabled.

Cleverly, the phishing kit may even embed Trust Wallet style fonts via chrome extension:// URLs to mimic the look of the genuine extension UI. This does not grant access to the real extension but enhances the deception.

```HTML
@font-face { font-family: 'Binance'; src:
url(chrome-extension://egjidjbpglichdcondbcbdnbeeppgdph/fonts/BinancePlex-Regul
ar.otf) format('opentype'); }
```

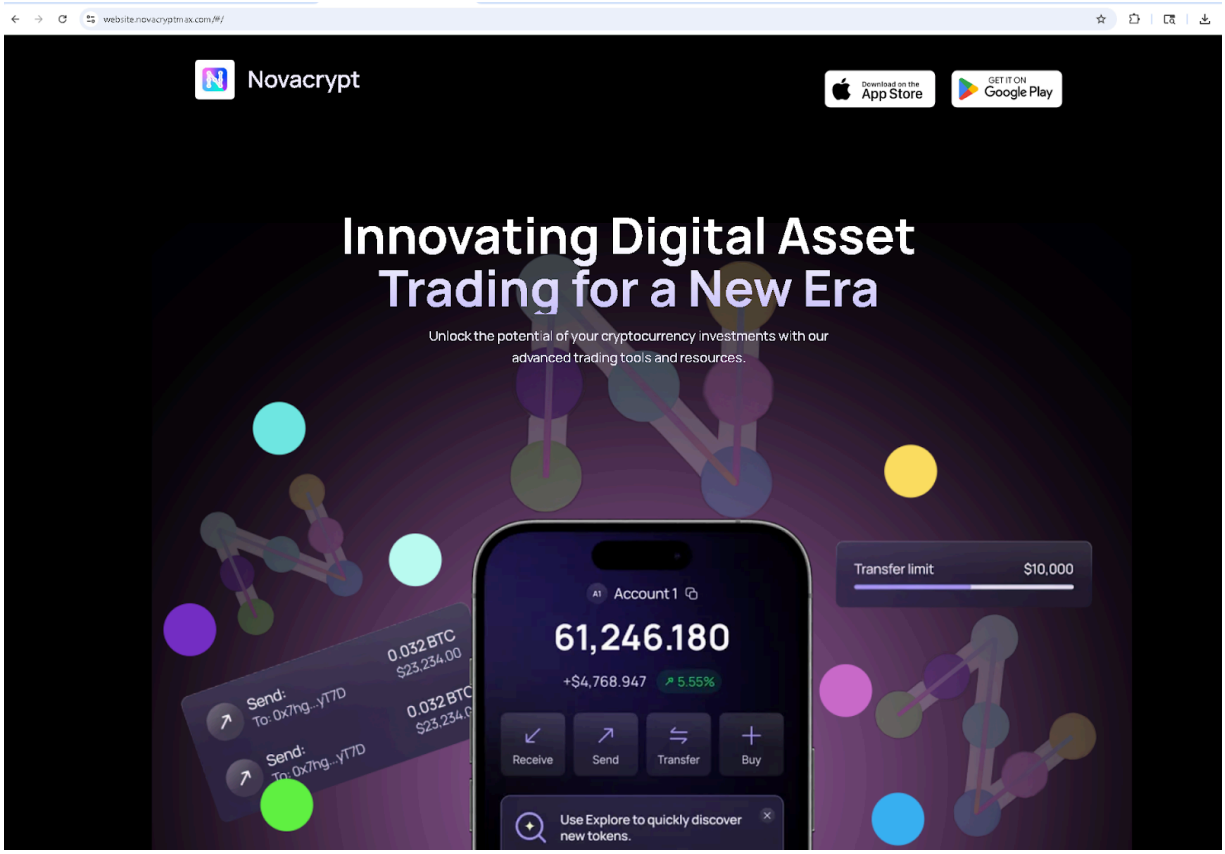
Figure: CSS from the fake Trust Wallet extension loading a Binance font – indicating the extension is active on the page

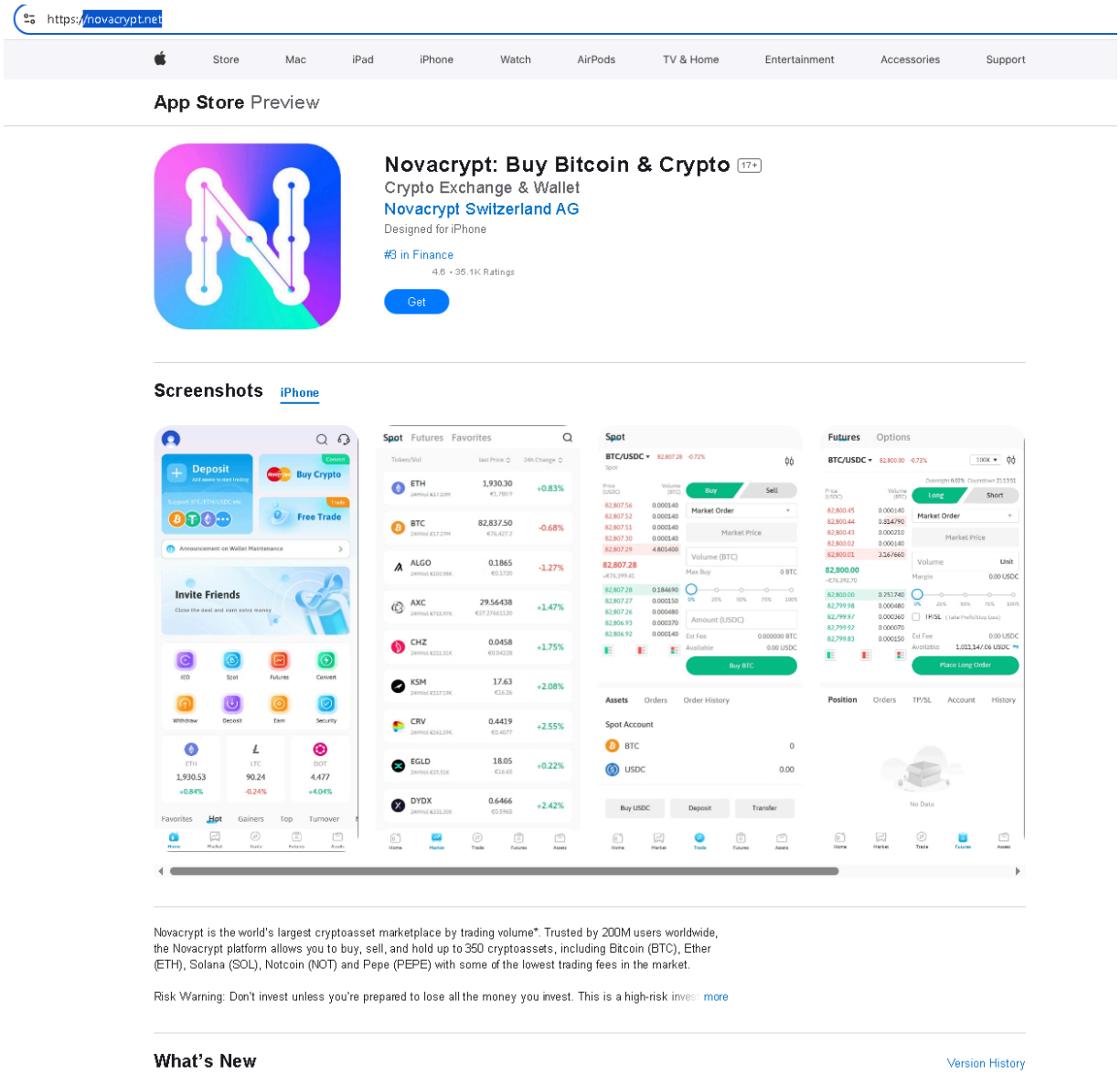
Endgame: Once a victim signs the malicious transaction, the attacker has the permissions needed to siphon cryptocurrency assets at will. This is a classic wallet drain; a convincing façade powered by copied CSS and branding, but with the theft executed entirely by malicious JavaScript hidden beneath.

Fake Trust Wallet CSS code snippet for a popup:

```
.trust-wallet-one-tap .body .right-items .wallet-title {
        color: #1e2329;
        font-size: 16px;
        font-weight: 600;
        line-height: 20px;
}

.trust-wallet-one-tap .body .right-items .wallet-subtitle {
        color: #474d57;
        font-size: 14px;
        line-height: 20px;
}

.trust-wallet-one-tap .connect-indicator {
        gap: 15px;
        padding: 8px 0;
}

.trust-wallet-one-tap .connect-indicator .flow-icon {
        color: #474d57;
}

.trust-wallet-one-tap .loading-color {
        color: #fff;
}

.trust-wallet-one-tap .button {
        border-radius: 50px;
        outline: 2px solid transparent;
        outline-offset: 2px;
        background-color: rgb(5, 0, 255);
        border-color: rgb(229, 231, 235);
        cursor: pointer;
        text-align: center;
        height: 45px;
}

.trust-wallet-one-tap .button .button-text {
        color: #fff;
        font-size: 16px;
        font-weight: 600;
        line-height: 20px;
}

.trust-wallet-one-tap .footer {
        margin: 20px 30px;
}

.trust-wallet-one-tap .check-icon {
        color: #fff;
}

@font-face {
        font-family: 'Binance';
        src: url(chrome-extension://egjidjbpglichdcondbcbdnbeeppgdph/fonts/BinancePlex-Regular.otf) format('opentype');
        font-weight: 400;
        font-style: normal;
}

@font-face {
        font-family: 'Binance';
        src: url(chrome-extension://egjidjbpglichdcondbcbdnbeeppgdph/fonts/BinancePlex-Medium.otf) format('opentype');
        font-weight: 500;
        font-style: normal;
}
```

Phishing via iPhone Profile: The Novacrypt “App”


website.novacryptmax.com/#/
Novacrypt
Download on the App Store
GET IT ON Google Play
Innovating Digital Asset Trading for a New Era
Unlock the potential of your cryptocurrency investments with our advanced trading tools and resources.
Account 1
61,246.180
+$4,768.947
5.55%
Receive
Send
Transfer
Buy
Use Explore to quickly discover new tokens.
Transfer limit
$10,000
0.032 BTC
$23,234.00
Send:
To: 0x7hg...yT7D
0.032 BTC
Send:
To: 0x7hg...yT7D



Another facet of this scam nexus targets mobile users, especially iPhone owners, by distributing a malicious Apple configuration profile (.mobileconfig) that masquerades as a new cryptocurrency trading app called Novacrypt. Instead of a real app, victims end up installing a WebClip – essentially a fake app icon that opens a phishing site. This is a stealthy method to phish cryptocurrency exchange credentials via what appears to be a standard app installation.

How it works: The scammers set up a fake "App Store" download page prompting users to install the Novacrypt app for iOS. When the user agrees, they receive a .mobileconfig file from the Novacrypt site (e.g., novacrypt.net/…/Novacrypt.mobileconfig). This configuration profile, when opened on an iPhone, prompts the user to install a new profile, which most users interpret as installing an app or enabling certain functionality.

Let's break down key parts of the Novacrypt mobileconfig payload:

```
HTML
<key>PayloadDisplayName</key>
<string>Novacrypt</string>
...
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
...
<key>Label</key>
<string>Novacrypt</string>
...
<key>URL</key>
<string>https://h5.novacryptmax[.]com/#/pages/auth/sign-in</string>
```

Figure: Excerpt from the Novacrypt.mobileconfig file, showing it creates a WebClip named "Novacrypt" that opens a URL to h5.novacryptmax[.]com.

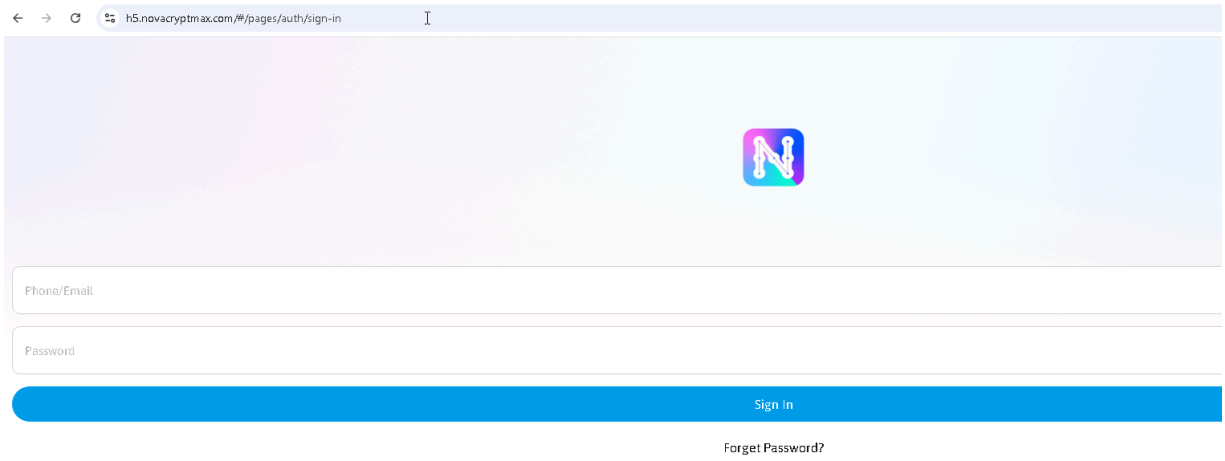
- **PayloadDisplayName** = "Novacrypt" – The name shown to the user during install, making it appear official.
- **PayloadType** = com.apple.webClip.managed – This indicates the profile will install a **Web Clip (shortcut)** on the home screen.
- **Label** = "Novacrypt" – The label under the home screen icon, so it looks like a real app named Novacrypt.
- **URL** = https://h5.novacryptmax[.]com/#/pages/auth/sign-in – The crux of the scam: this is the URL that the WebClip opens. It's a fake login page on a domain (novacryptmax[.]com) that *appears* to be related to Novacrypt but is entirely under the scammer's control.

Additionally, the profile includes a base64-encoded icon image (to make the WebClip icon resemble a legitimate app logo), and it is digitally signed (likely with a self issued certificate). Interestingly, the profile's signature references "Let's Encrypt" and a domain 360[.]icu, suggesting that the threat actor used a free certificate (possibly a deceptive one named to appear trustworthy) and potentially hosted the profile on a domain like 360[.]icu. This shows the lengths to which the scammers go to make the profile appear "verified" to the user.

Step-by-step, the attack unfolds as:

1. **Bait** – The victim receives a link (via email, social media, etc.) to download the *"Novacrypt crypto trading app."* The link directs users to a page that mimics an official app store, prompting the installation of an iOS configuration profile.
2. **Install** – The user installs the profile on their iPhone, ignoring iOS warnings. Because the profile is named "Novacrypt" and has a nice icon, it appears legitimate. A new **"Novacrypt"** icon now appears on the home screen, as if a real app had been installed.
3. **Phishing** – When the victim taps the Novacrypt icon, it doesn't launch a real app; instead, it quietly opens Safari to h5.novacryptmax[.]com/#/pages/auth/sign-in, a phishing webpage. The page likely impersonates a login screen for a cryptocurrency exchange or wallet.
4. **Credentials Theft** – Believing this to be part of setting up the app, the user enters their username, password, 2FA, etc. Those credentials are immediately sent to the attacker. The victim might even be redirected or shown an error after to avoid suspicion. Meanwhile, the attackers can use those stolen logins to empty the victim's accounts or wallets on real exchanges.

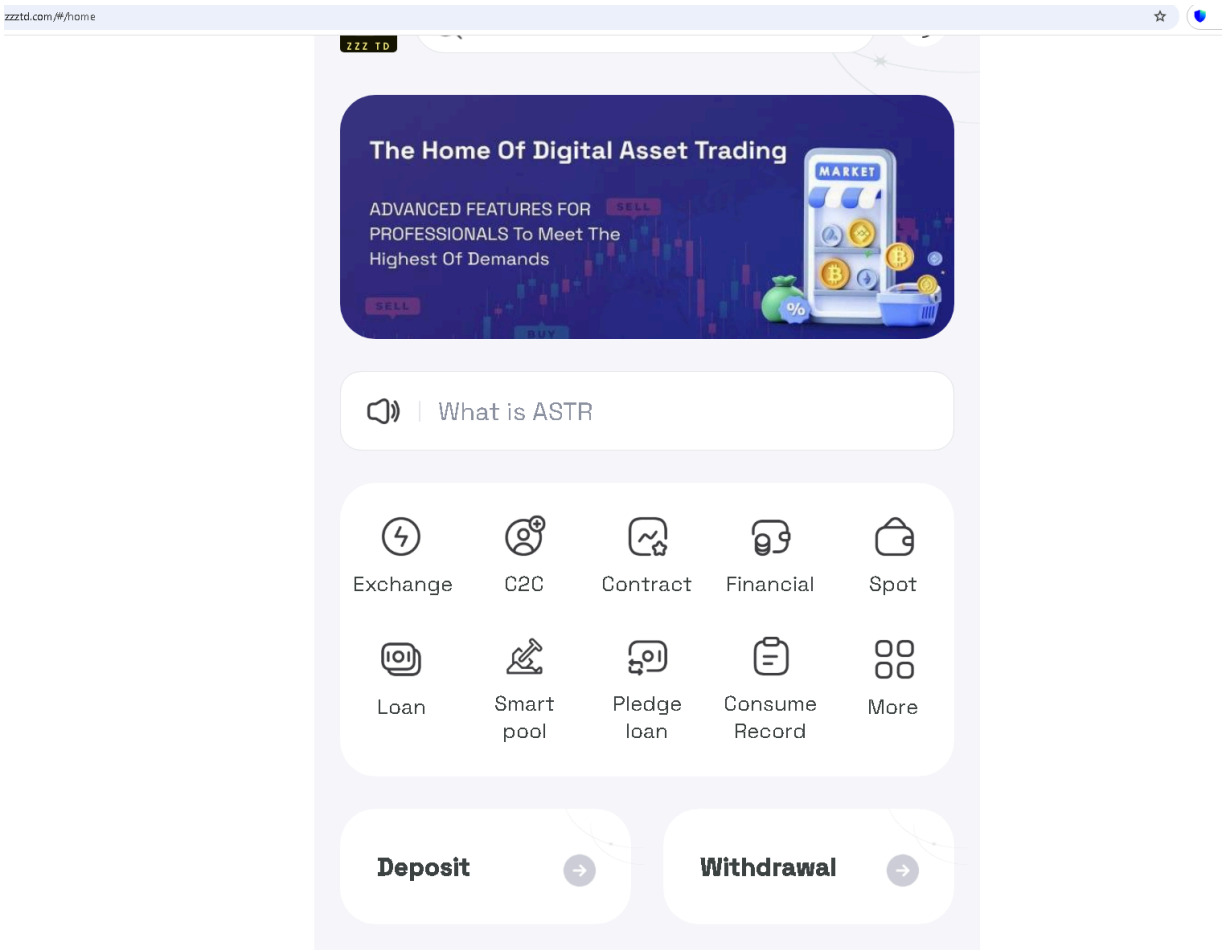
H5.novacryptmax[.]com



This scheme abuses Apple's enterprise device management feature to add a phishing shortcut on the user's phone. It appears to install an app, but in reality it is only a bookmark to a fraudulent site. No malware is installed on the device, the "app" is simply Safari redirected to the attacker's page.

The Novacrypt phish's infrastructure reveals some interesting connections: the phishing site utilizes the domain **novacryptmax[.]com** (with subdomains such as **h5.**, **web.**, etc.), which was registered through the same registrar (Gname) as the other scam domains and hosted behind Cloudflare. The decoy download page was on **novacrypt[.]net** (hosted at 8.221.100[.]222), and its "App Store" button simply served the mobileconfig from that domain. There was even an Android variant attempt – the "Google Play" button on the site pointed to googleplay.nova-reviews[.]com (likely intended to drop an APK or guide Android users, though by the time of analysis, that domain wasn't resolving).

The "ZZZTD" Web Trader – Fake Platform with Malicious Code



The third pillar of this scam nexus is a fake online cryptocurrency trading/investment platform hosted on **zzztd[.]com** (also on 8.221.100].]222). At first glance, zzztd[.]com appears to be a cryptocurrency or financial trading web application. However, buried in its code are suspicious scripts that suggest it may be stealing data or loading malware in the background.

On zzztd[.]com's homepage, researchers found references to two main JavaScript files: chunk-vendors.f0dabee900057778.js and app.46e5246269e54881.js. These appear to be typical for a web app (the former likely containing third party library code, and the latter the app's own code). The HTML uses <script defer> tags to load these, meaning they execute after the page loads:

```HTML
<script defer src="/wap/js/chunk-vendors.f0dabee900057778.js"></script>
<script defer src="/wap/js/app.46e5246269e54881.js"></script>
```

Figure: Code snippet from zzztd[.]com loading JavaScript files for the web application. The defer attribute indicates these scripts run only after the HTML is parsed, ensuring the page renders first.

A VirusTotal scan of the app.46e5246269e54881.js file showed 0 antivirus detections, which isn't uncommon for custom JavaScript (most AV engines don't flag obfuscated JS files). However, the behavioral analysis on VirusTotal yielded a clue: it revealed that this script (or something it loaded) tried to contact a suspicious domain, anedhaude[.]xyz. That domain is not currently publicly active, but further investigation uncovered an Android Trojan sample **("ioeai.apk")** that also communicated with anedhaude[.]xyz. In other words, the zzztd[.]com web app shares

infrastructure or code with known malware, strongly suggesting that if a user interacted with zzztd[.]com (or downloaded anything from it), they could be infected or have their data sent to the attackers' server.

It's possible that zzztd[.]com was set up to either phish for login credentialsto cryptocurrency accounts (by mimicking a trading dashboard and tricking users into inputting private keys or exchange logins) or to deliver malware (like the mentioned Android APK) to users under the guise of a mobile trading app. The site's code, including references to an external C2 domain (anedhaude[.]xyz), is a red flag – legitimate cryptocurrency trading platforms wouldn't embed calls to random .xyz domains. This pattern connects zzztd[.]com back to the same threat actor's toolkit.

- app.46e5246269e54881.js- https://www.virustotal.com/gui/file/430a73bc2a01dd1c5c84c5cc8bf0c65b163198a39910d66dc93f23fcea458fbe/beha
- ioeai.apk- https://www.virustotal.com/gui/file/884cc0b03fbb7f8282916433987ccd8573460d8c2daa33fe1da211a13331b1e7/beha

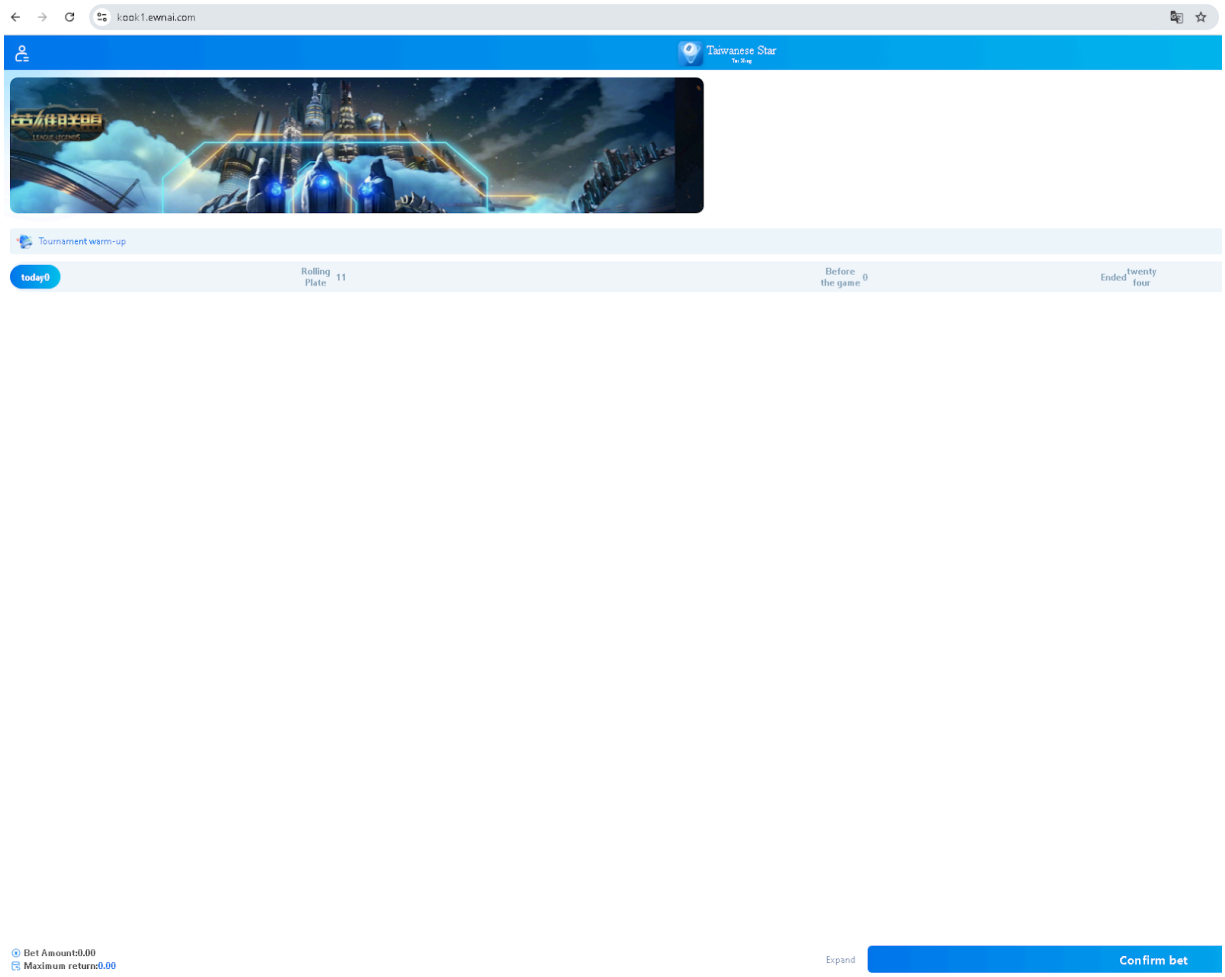
Connecting the Dots: One IP, Many Scams

What ties MedAI Genesis, Novacrypt, and ZZZTD together? The investigation found that all these seemingly disparate scams were hosted on a single IP address**:** 8.221.100[.]222. This IP address (an Alibaba Cloud server in Asia) served as a one stop hosting hub for the scammer, hosting multiple domains for various fraud schemes. At least eight domains sharing this server have been identified, including those involved in the scams above and others:

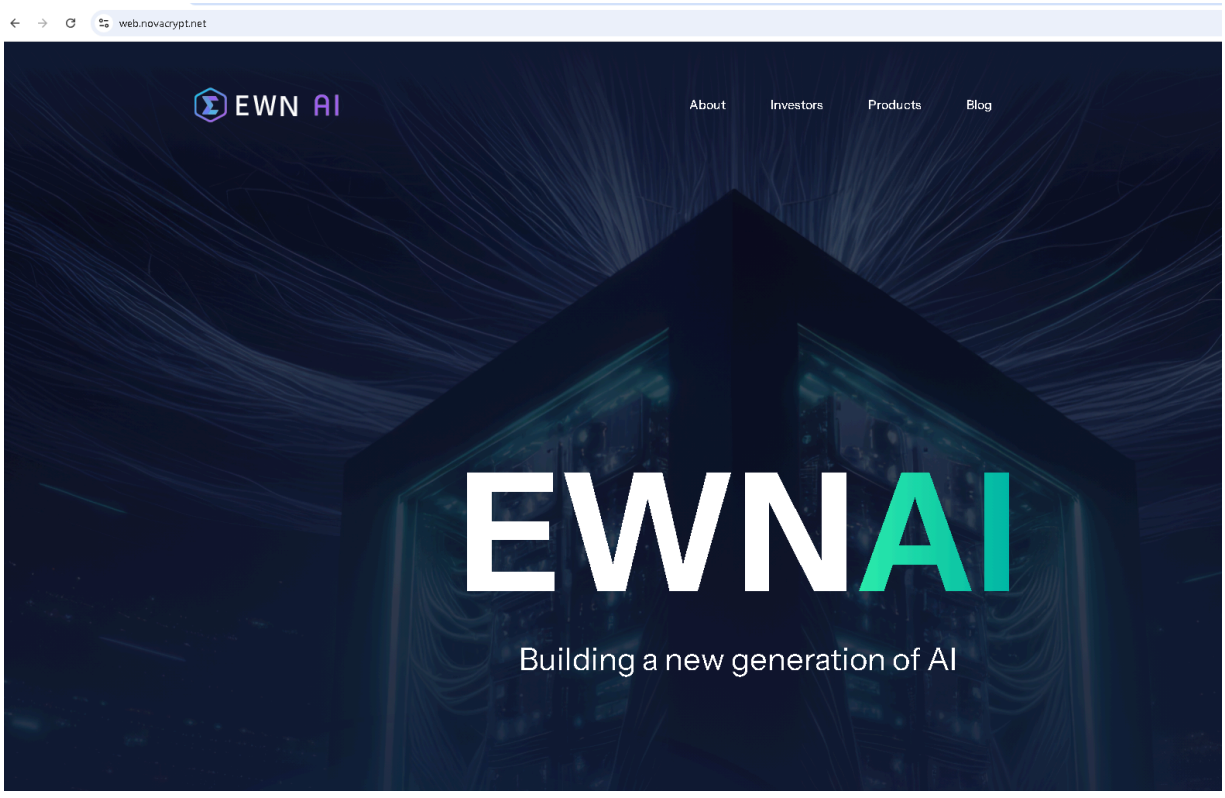
- **medaigenesis[.]cc** – Fake cryptocurrency/AI investment site (wallet drainer stage)
- **novacrypt[.]net** – Host for the fake app mobileconfig and website
- **zzztd[.]com** – Fake cryptocurrency trading platform with malicious JS
- **n58[.]bet** – Likely another scam site (one reference suggests it was a fake gaming site in Chinese)
- **ewnai[.]com** – A fake AI technology site
- **app.tiktoks[.]cc** – A short lived domain
- **admin.zzztd[.]com**, **web.zzztd[.]com** – Subdomains related to zzztd[.]com
- **web.novacrypt[.]net** – Subdomain which, interestingly, was misconfigured to display content from EWN AI (ewnai[.]com), accidentally linking the Novacrypt scam to the EWN AI scam by content reuse.

Subdomain resolving to a different IP, hosting a fake gaming site.

kook1.ewnai[.]com (103.235.174.202)



Web.novacrypt[.]net (misconfigured to display content from EWN AI (ewnai[.]com)



Most of these domains were registered through the same registrar **(Gname.com Pte. Ltd.)**, reinforcing that they are controlled by the same actor or group. Passive DNS records indicate that this infrastructure has been in use since at least April 2025 and remained active until August 2025, suggesting an ongoing campaign.

The threat actor behind this nexus appears to be quite versatile: not only targeting cryptocurrency investors through multiple avenues (sketchy extensions, fake apps, and fake platforms), but also dabbling in other forms of fraud, such as a fake TikTok Shop scam. One of the scam sites was a gaming/gambling site in Chinese, hinting that the operators might be based in or targeting users in East Asia (or trying a variety of lures to see what sticks). The range of themes, from AI startups to cryptocurrency exchanges to e-commerce, shows a wide-reaching fraud operation managed by a single actor.

Below is a network map connecting the key domains and infrastructure:

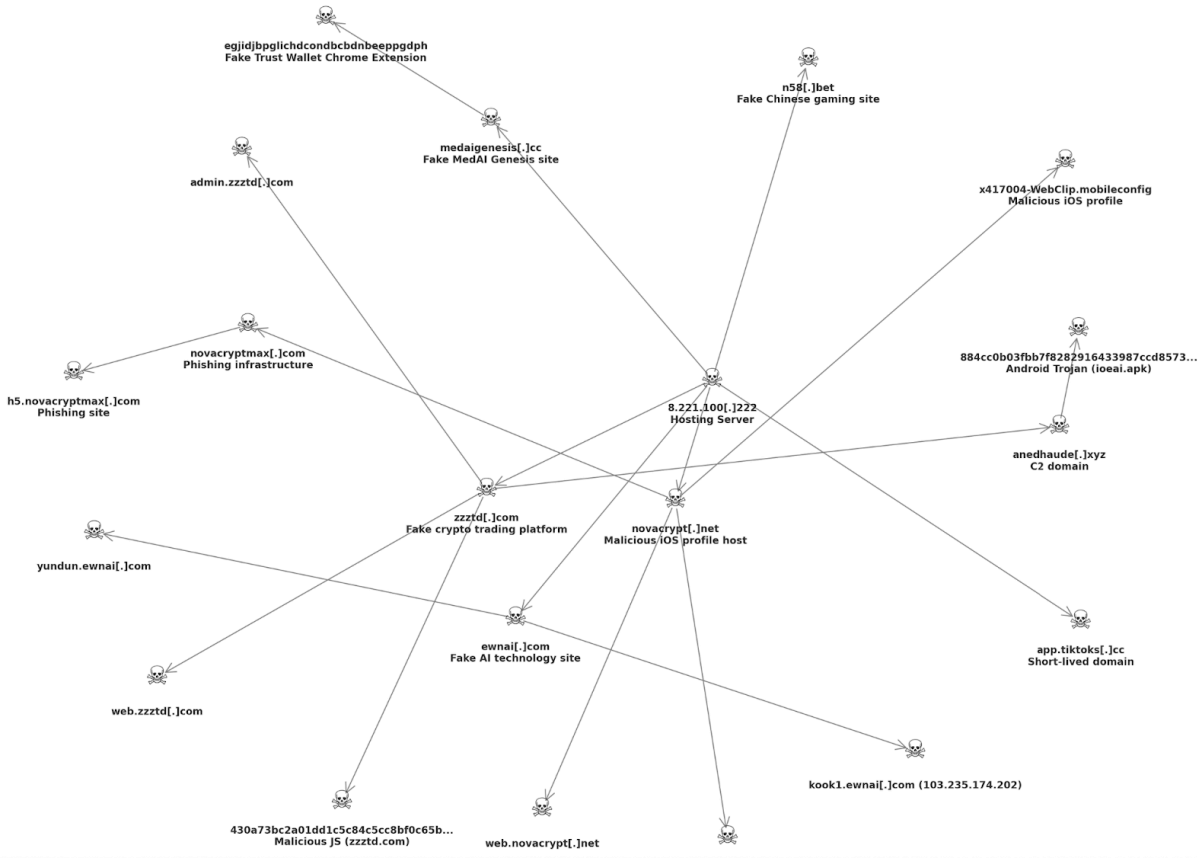


Figure: Network map of the scam nexus, showing domains hosted on 8.221.100[.]222 (center) and their relationships. The fake Trust Wallet popup and external phishing domains (novacryptmax[.]com, etc.) are also linked to the core cluster.

Despite the variety of themes these platforms use (AI token site, trading platform, mobile app), these scams share common tactics. They all rely on social engineering to get the victim to take a harmful action willingly, such as installing an extension or profile, clicking a connect button, or typing in a password. The technical traps (malicious code injection, webclip profiles, obfuscated scripts) are combined with psychological lures (shiny websites, promises of big profits, or urgent investment opportunities). It's a potent mix that has likely claimed many victims.

Conclusion

This cluster of scams demonstrates how threat actors combine technical methods with deception to steal cryptocurrency. By controlling multiple domains and even a browser extension, they exploit trust at several levels: browser add-ons, app installation processes, and convincing web design. The single infrastructure behind these schemes also highlights how a determined attacker can leverage one setup to run multiple scams, from cryptocurrency theft to fake e-commerce.

Staying safe requires a mix of technical defenses and skepticism: avoid installing browser extensions or mobile profiles from unverified sources, double check URLs (a legit project won't ask you to install a profile for an "app"), and be wary of any unexpected wallet transaction requests. As the "Cryptocurrency Drain Conspiracy" shows, even a legitimate looking prompt could be a trap. Always verify through official channels, and when in doubt, **don't click "Connect" or "Install"**, that split second decision can make the difference between keeping your assets secure or seeing them wiped out.

Indicators of Compromise (IOCs)

For quick reference, here is a summary of known indicators associated with this scam nexus. Security teams and vigilant users can use these to detect or block related activity:

Indicator	Type	Description
8.221.100[.]222	IP Address	Hosting server for the scam websites (MedAI, Novacrypt, ZZZTD, etc.
medaigenesis[.]cc	Domain	Fraudulent "MedAI Genesis" cryptocurrency site (wallet drainer lure)
novacrypt[.]net	Domain	Website used to distribute malicious .mobileconfig (fake Novacrypt app)
h5.novacryptmax[.]com	Domain	Phishing site (opened by the iOS WebClip to steal login credentials)
novacryptmax[.]com	Domain	Related phishing domain (multiple subdomains like h5., web., etc. on Cloudflare)
googleplay.nova-reviews[.]com	Domain	Fake Google Play link used on Novacrypt site (intended to target Android users)
zzztd[.]com	Domain	Fake cryptocurrency trading/investment platform (hosts malicious JS)
web.zzztd[.]com / admin.zzztd[.]com	Domain (subdomain)	Subdomains of zzztd.com (likely admin panel or web API)
ewnai[.]com	Domain	Fake "EWN AI" technology site (part of same infrastructure)
kook1.ewnai[.]com / yundun.ewnai[.]com	Domain (subdomain)	Subdomains of ewnai.com (used for a fake gaming site and fake TikTok Shop scam)
n58[.]bet	Domain	Scam site on the same server (reported as a fake Chinese gaming/gambling site)

egjidjbpglichdcondbcbdnbeeppgdph	Chrome Extension ID	sketchy “Trust Wallet” browser extension
Trust Wallet (legitimate extension)	Chrome Extension	*Note: Legit extension used by scammers (bad reviews report theft)*
x417004-WebClip240618-205808-qf0.mobileconfig	File (iOS profile)	Malicious iOS configuration profile for Novacrypt fake app (WebClip installer)
430a73bc2a01dd1c5c84c5cc8bf0c65b (SHA-256)	File Hash	Hash of zzztd.com’s app.46e5246269e54881.js (malicious script file)
884cc0b03fbb7f8282916433987ccd8573460d8c2daa (SHA-256)	File Hash	Hash of ioeai.apk – Android Trojan linked via anedhaude.xyz (related malware in this nexus)
anedhaude[.]xyz	Domain	Suspicious domain used as C2/host by zzztd’s malware (not resolving now)