

Yoroi Wallet Phishing Abuses GoTo Resolve and ScreenConnect for Device Takeover – Malware Analysis, Phishing, and Email Scams

 malwr-analysis.com/2026/03/02/yoroi-wallet-phishing-abuses-goto-resolve-and-screenconnect-for-device-takeover

Anurag Gawande

March 2, 2026

Overview

I recently came across a phishing campaign impersonating the Yoroi Desktop Wallet, targeting cryptocurrency users with what looked like a legitimate upgrade.

The email itself was clean and well-written. It talked about improved security, hardware wallet support, and even AI-based scam detection. Nothing immediately stood out as suspicious. The landing page looked polished too, with proper branding and a familiar layout.

Hello,

We're excited to introduce Yoroi Desktop, a desktop-first evolution of Yoroi designed for long-term Cardano users who demand stronger security, deeper visibility, and smarter decision-making.

Yoroi Desktop moves critical wallet activity out of the browser and into a hardened desktop environment. This reduces attack surfaces while unlocking advanced capabilities that simply aren't possible in extensions. Your keys remain fully non-custodial, with seamless migration from Yoroi Extension or Mobile—no new seed phrases required.

What's new in Yoroi Desktop

* Improved Hardware Compatibility

Native desktop support for Ledger and Trezor with secure USB/Bluetooth handling, multi-device signing workflows, and hardware health checks.

* Advanced Scam Detection

Pre-sign transaction simulation, phishing and malicious dApp detection, and clear, human-readable transaction explanations—before you approve anything.

* Built-in AI Support

AI-assisted risk scoring, staking insights, and governance previews that help you understand what's happening on-chain in real time.

* Full On-Chain Visibility

Portfolio flows, staking performance, rewards forecasting, and governance readiness—all in one place.

Yoroi Desktop is built for holders, stakers, governance participants, and institutions who treat security as non-negotiable and want intelligent guardrails without sacrificing control.

Download Yoroi Desktop today: <https://download.v1desktop-yoroiwallet.com/> and upgrade your Cardano experience with desktop-grade security and AI-powered clarity.

— Yoroi Wallet Team

The Setup

The phishing email redirects users to a domain:

| `hxxps://download[.]v1desktop-yoroiwallet[.]com/`

the domain was recently registered (Feb 2026), yet it was already indexed on Google, meaning users could also land on it via search results, not just email.

v1desktop-yoroiwallet.com



Domain Information

Domain: v1desktop-yoroiwallet.com

Registered On: 2026-02-09

Expires On: 2027-02-09

Updated On: 2026-02-09

Status: client delete prohibited
client transfer prohibited

Name Servers: clarissa.ns.cloudflare.com
isaac.ns.cloudflare.com

AI Mode **All** Shopping Images Short videos Forums News More ▾ Tools ▾

Google promotion

Try Google Search Console

www.google.com/webmasters/

Do you own **v1desktop-yoroiwallet.com**? Get indexing and ranking data from Google.



v1desktop-yoroiwallet.com

<https://v1desktop-yoroiwallet.com>

Yoroi Desktop Wallet - Light Wallet For Cardano

Yoroi Desktop moves critical wallet activity out of the browser into a hardened desktop environment—with AI-powered clarity and advanced scam detection. [Read more](#)

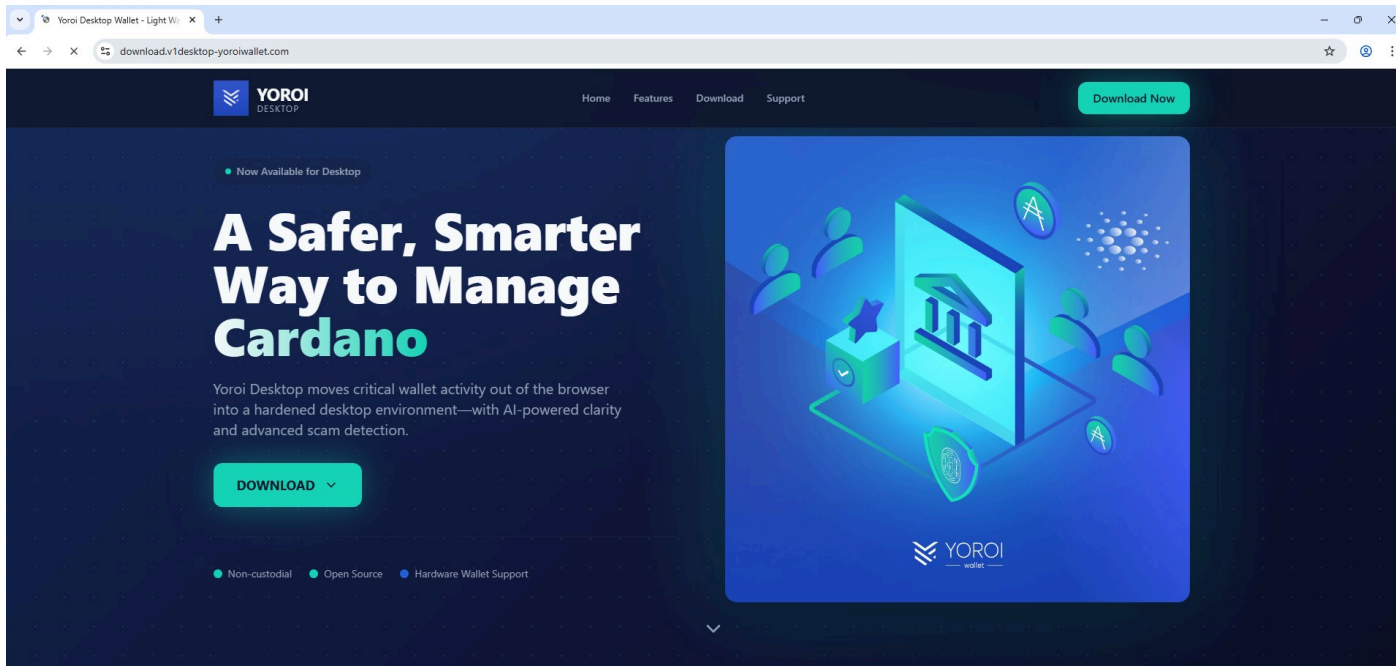
The Download That Isn't a Wallet

The site promotes a “**Yoroi Desktop**” download, but instead of hosting anything legitimate, it redirects to a file-sharing service and delivers an MSI file:

hxxps://store-na-phx-1.gofile.io/download/direct/900a7e14-a15a-41f6-94fb-c88603d09463/YoroiDesktop-installer.msi

hxxps://cold8[.]gofile[.]io/download/direct/900a7e14-a15a-41f6-94fb-c88603d09463/YoroiDesktop-installer.msi

hxxps://store-na-phx-5[.]gofile[.]io/download/direct/87c6015b-8a47-4cde-9e31-aaacd3f4193c/YoroiDesktop-installer.msi



Running the installer doesn't give you a wallet. It installs GoTo Resolve (LogMeIn) in unattended mode.

Silent Remote Access via GoTo Resolve

File name: YoroiDesktop-installer.msi

File hash: 8634AD3C6488D6A27719C5341E91EEB9

File name: unattended-updater.exe

File hash: 2A2D9B03AA6185F434568F5F4C42BF49

Once executed, the system is quietly enrolled into a remote access setup. There's no obvious warning, no suspicious pop-ups, just a legitimate tool being used in the wrong way.

Looking at the configuration reveals what's happening behind the scenes:

CompanyId: 5504330483880245799

Namespace: syn-prd-ava-unattended

FleetTemplateName: syn-prd-ava-unattended

This isn't random. It shows the machine is being registered into a pre-configured remote access fleet, controlled by whoever owns that GoTo Resolve tenant.

At this point, the attacker doesn't need to trick the user anymore. They already have what they need, persistent access to the device.

```
[REDACTED]
SessionBackendUrl: https://sessions.console.gotoresolve.com
SessionType: Unattended
[REDACTED]
WebsiteUrl: devices-iot.console.gotoresolve.com
WorkFolder: [REDACTED]
WtsStartingSessionId: 1
publickey: [REDACTED]295b38afb9966304dd47c3d39a72db79
Param layer Id: 1
HostId: [REDACTED]
Param layer Id: 0
AppletGeneratorUrl: https://applet.console.gotoresolve.com
ApplicationType: 4
BaseUrl: https://devices-iot.console.gotoresolve.com/
CompanyId: 5504330483880245799
CreatedAt: [REDACTED]
Environment: Production
FleetTemplateName: syn-prd-ava-unattended
HealthCheckUrl: https://health.console.gotoresolve.com/devices
HostId: [REDACTED]
InstallationId: [REDACTED]
Lang: en
```

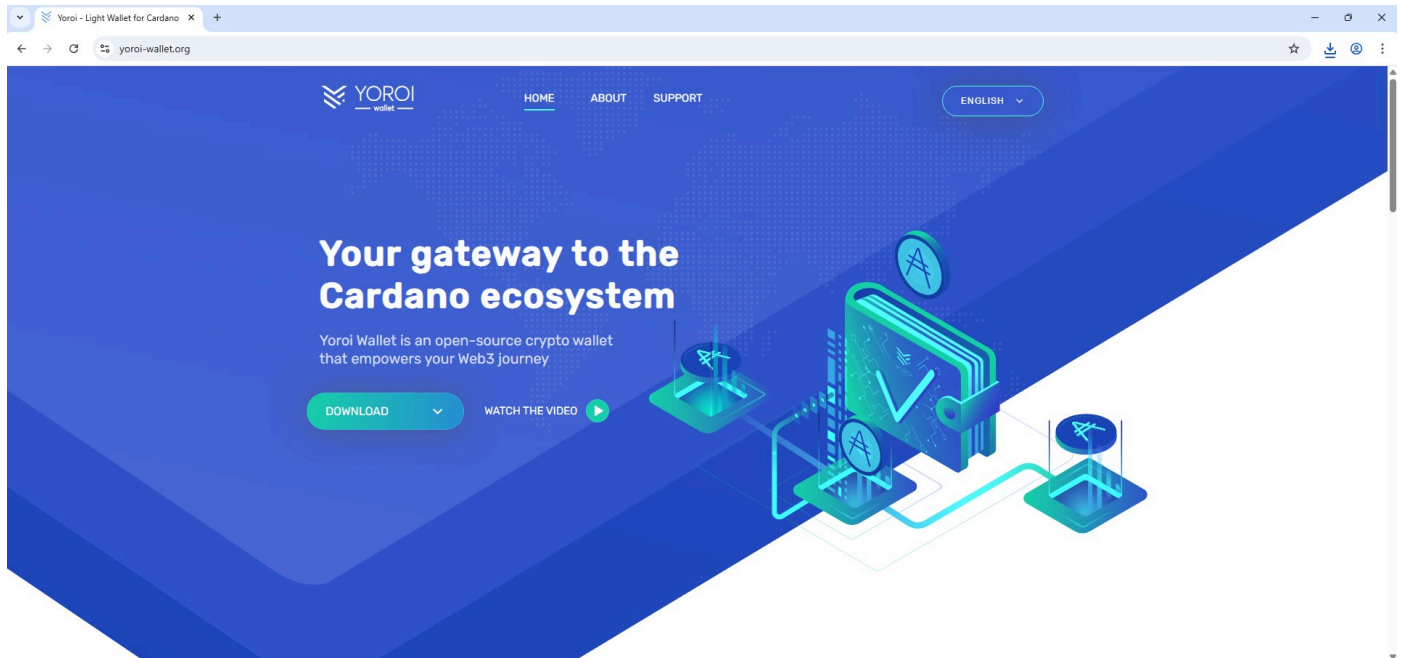
A Second Variant: ScreenConnect

File hash: e79a47fc85955123f0821223a4cf2595

File name: yoroi-wallet.msi

While pivoting on this activity through URLScan, I came across another domain following the same theme:

| yoroi-wallet[.]org



yoroi-wallet.org

Updated 7 hours ago ↻



Domain Information

Domain:	yoroi-wallet.org
Registered On:	2026-01-06
Expires On:	2027-01-06
Updated On:	2026-01-11
Status:	client transfer prohibited
Name Servers:	monika.ns.cloudflare.com tony.ns.cloudflare.com

This one doesn't use GoTo Resolve. Instead, it delivers a payload based on ConnectWise ScreenConnect, another legitimate remote access tool.

Inside the dropped configuration file, the intent becomes clear:

```
<configuration>
  <configSections>
    <section name="ScreenConnect.ApplicationSettings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral,
      PublicKeyToken=b77a5c561934e089" />
  </configSections>
  <ScreenConnect.ApplicationSettings>
    <setting name="ClientLaunchParametersConstraint" serializeAs="String">
      <value>?h=instance-plb26i-relay.screenconnect.com&amp;p=443&amp;
        k=BgIAAACKAABSU0ExAAgAA
        IDWQnRBmzjKAj*2f41Ecc5T
        UT%2fRLh0DG1d5BgZ8q1B0D
        1nP8ODSBQFv%2bFZddL5eLTJX6HriyhVXFdY2RaXhcGHrbC
        xDRyaaMXB8SNpr4dDKJwb6RM1RTMeIOAKoEHN6nmzlnY1Fa
      </value>
    </setting>
  </ScreenConnect.ApplicationSettings>
</configuration>
```

The important part here is the relay server:

```
| instance-p1b26i-relay[.]screenconnect[.]com
```

This tells the client exactly where to connect. Once installed, the system reaches out to that server and establishes a remote session.

Again, no exploit, no malware in the traditional sense, just legitimate software used to gain control.

A Familiar Pattern

This isn't the first time I've seen something like this.

It closely resembles a campaign I previously analyzed where RMM tools were abused in a crypto wallet distribution flow:

One thing that stands out across both campaigns is how the payload is delivered.

In all cases, the final MSI files are not hosted directly on the phishing domains. Instead, the sites redirect users to gofile[.]io, a legitimate file-sharing service, to download the installer.

This adds another layer of evasion. Hosting the MSI on a legitimate service like gofile makes it harder to block and also reduces suspicion from users, since the download doesn't come directly from the phishing domain.

While digging further into this, I also noticed that the MSI files are hosted across multiple gofile storage endpoints such as:

```
| store-na-phx-[1/4/5].gofile.io/download/direct/
```

Changing the server index (for example, 1, 4, or 5) reveals similar download paths hosting MSI files that follow the same theme, crypto wallet installers that actually deploy RMM tools.

Combined with the use of legitimate tools like GoTo Resolve (LogMeIn) and delivery through trusted file-sharing services, the overall chain appears clean on the surface but ultimately leads to full remote access.

Indicators

URLs

v1desktop-yoroiwallet[.]com
yoroi-wallet[.]org
instance-p1b26i-relay[.]screenconnect[.]com
YoroiDesktop-installer.msi
yoroi-wallet.msi
CompanyId: 5504330483880245799
Namespace: syn-prd-ava-unattended

File Hash

8634ad3c6488d6a27719c5341e91eeb9
2a2d9b03aa6185f434568f5f4c42bf49
e79a47fc85955123f0821223a4cf2595
be8c2d03333cbd13dab654260c60b025