

RMM Abuse in a Crypto Wallet Distribution Campaign – Malware Analysis, Phishing, and Email Scams

 malwr-analysis.com/2025/12/31/rmm-abuse-in-a-crypto-wallet-distribution-campaign

Anurag Gawande

December 31, 2025

Analysis of a Suspicious “Eternl Desktop” MSI Installer Dropping LogMeln Resolve

Overview

A professionally written announcement email titled “**Eternl Desktop Is Live — Secure Execution for Atrium & Diffusion Participants**” is currently circulating within the Cardano community.

Dear Community,

We are pleased to announce the launch of Eternl Desktop — a dedicated, local-first desktop application designed for users who require greater assurance, clarity, and control when interacting with the Cardano network.

As Cardano evolves, participation is no longer limited to holding ADA or delegating to a single pool. Identity, governance, and value-aligned staking are becoming first-class primitives.

Eternl Desktop was built to support this shift by providing:

1. A non-browser signing environment with explicit transaction visibility
2. Advanced delegation and staking controls
3. Hardware wallet–first security controls
4. A professional-grade interface for high-conviction Cardano users

All keys remain local.
All approvals are explicit.
All actions are under your control.

Recent developments across the Cardano ecosystem highlight a growing focus on purpose-driven delegation.

Through Atrium, initiatives such as the Diffusion Staking Basket allow users to delegate ADA across a curated set of stake pools aligned with decentralization, resilience, and long-term network health.

Importantly: Users staking through the Diffusion Basket continue to earn standard ADA staking rewards

In addition, Diffusion participants are earning NIGHT and ATMA tokens as ecosystem incentives

Over \$24,000 worth of NIGHT was distributed in the previous epoch, with a further \$40,000 in NIGHT scheduled for the next epoch.

Eternl Desktop is now available to download below for Windows, macOS, and Linux
<https://download.eternldesktop.network>

Eternl Desktop is where Cardano decisions are finalized.

Thank you for continuing to build, stake, and govern with intent.

—
The Eternl Team

At first glance, the email appears legitimate and well aligned with Cardano’s governance narrative promoting security, decentralization, and staking incentives. However, deeper inspection of the download mechanism and installer behavior raises significant red flags.

Email Social Engineering Highlights

The email leverages high trust messaging and ecosystem specific incentives.

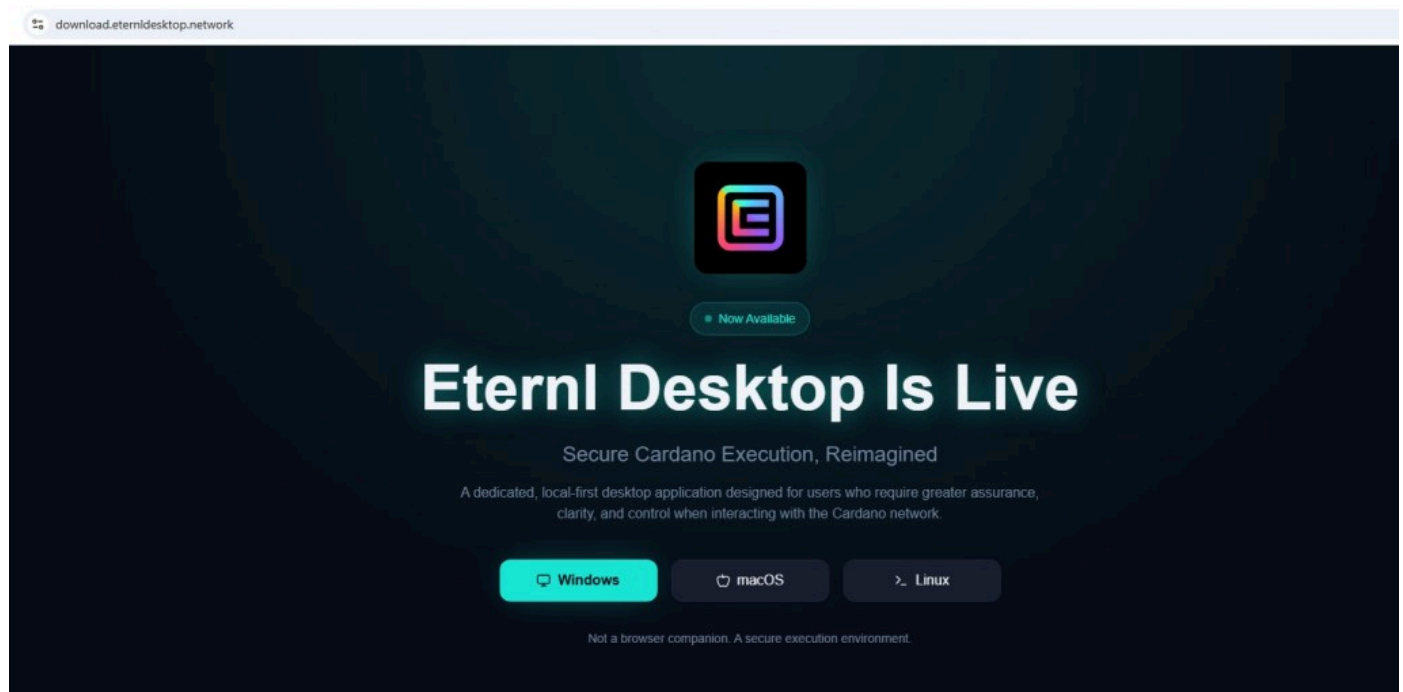
The email strategically references **Atrium** and the **Diffusion Staking Basket** to establish legitimacy within the Cardano ecosystem, while also making enticing claims of **NIGHT** and **ATMA** token rewards to drive user interest. It reinforces trust by emphasizing “**local-first, non-browser signing,**” positioning the application as a more secure alternative to browser based wallets. The overall messaging maintains a polished, professional tone with no visible spelling or grammatical

issues, lending credibility to the communication. This is capped with a strong, authoritative call to action “**Eternl Desktop is where Cardano decisions are finalized.**” designed to create urgency and frame the software as an essential tool for serious Cardano participants.

Download Infrastructure Red Flags

The provided download URL, `hxxps://download[.]eternldesktop[.]network`, raises immediate concerns, as the domain appears to be newly created and lacks any established historical reputation. There is no independent verification or announcement from official, well known Eternl communication channels to validate its legitimacy. Additionally, the software is distributed as a direct MSI installer without publicly available checksums, digital signature transparency, or formal release notes, preventing users from independently verifying the integrity and authenticity of the installer before execution.

New infrastructure + wallet software + MSI installer is a high-risk combination.



Domain Information

 Domain Information	
Domain:	eternldesktop.network
Registered On:	2025-12-21
Expires On:	2026-12-21
Updated On:	2025-12-21
Status:	client delete prohibited client transfer prohibited add period
Name Servers:	isaac.ns.cloudflare.com clarissa.ns.cloudflare.com

MSI Installer Analysis

File Name: Eternl.msi

File Size: 23.3MB

File Type: Windows Intaller (MSI)

Hash: **8fa4844e40669c1cb417d7cf923bf3e0**

Title: LogMeIn Resolve Unattended

Comments: LogMeIn Resolve Unattended v1.30.0.636

Using CFF Explorer, I identified an embedded executable within the MSI file. I then used LessMSI to extract the executable for further analysis.

```

0000EFF0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | MZ .....yy..
0000F000 | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | .....@.....
0000F010 | B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 | .....(.....
0000F020 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0000F030 | 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 | .....
0000F040 | 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 | 0 20 . . i ! , 0 L i ! Th
0000F050 | 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F | is program.canno
0000F060 | 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t.be.run.in.DOS.

```

Extracted Executable File

File Name: unattended-updater.exe

File Type: PE32

File Size: 23.35MB

Original File Name: GoToResolveUnattendedUpdater.exe

File Hash: **3f317e17741122cd4ea30123ba241cd0**

File Description: LogMeIn Resolve

File Type	Portable Executable 32
File Info	Microsoft Visual C++ 8
File Size	23.35 MB (24488968 bytes)
PE Size	23.34 MB (24473088 bytes)
Created	Saturday 13 December 2025, 13.18.00
Modified	Saturday 13 December 2025, 13.18.00
Accessed	Tuesday 30 December 2025, 20.54.36
MD5	3F317E17741122CD4EA30123BA241CD0
SHA-1	76E4DF51CD8D5AEDD265144006D1FF374BD7F1D7
Property	Value
CompanyName	GoTo, Inc.
FileDescription	LogMeIn Resolve
FileVersion	1.30.0.636
InternalName	GoToResolveUnattendedUpdater.exe
LegalCopyright	Copyright © 2016-2025 GoTo, Inc. US patents pending.
OriginalFilename	GoToResolveUnattendedUpdater.exe
ProductName	GoTo Resolve

During dynamic analysis, the sample was observed writing log files and JSON artifacts to disk.

GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\unattended.json.tmp
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log
GoToResolveU...	3184	WriteFile	C:\Program Files (x86)\GoTo Resolve Unattended\937825596157721385\appdata\GoToResolveUnattended.log

It also tried to connect to below domains.

```
[ HttpQuery ] url: "http://ip.zscaler.com/" network error: QNetworkRe
[ HttpQuery ] url: "https://zerotrust.services.gotoresolve.com/health
[ HttpQuery ] url: "https://dumpster.console.gotoresolve.com/api/live
[ HttpQuery ] url: "https://sessions.console.gotoresolve.com/api/heal
[ HttpQuery ] url: "https://devices-iot.console.gotoresolve.com/" net
```

- hxx://ip.zscaler.com
- hxx://zerotrust.services.gotoresolve.com
- hxx://dumpster.console.gotoresolve.com/api/live
- hxx://sessions.console.gotoresolve.com
- hxx://devices-iot.console.gotoresolve.com/

- `hxxps://devices.console.gotoresolve.com/properties`
- `hxxps://applet.console.gotoresolve.com`
- `hxxps://custombranding.console.gotoresolve.com`

The executable is placed within a uniquely identified folder created under “**C:\Program Files (x86)\GoTo Resolve Unattended**”. All executables, along with JSON configuration files related to the RMM setup, are stored in this directory.

 <code>logger.json</code>	JSON Source File
 <code>mandatory.json</code>	JSON Source File
 <code>pc.json</code>	JSON Source File
 <code>unattended.json</code>	JSON Source File

The **unattended.json** configuration file enables unattended access, allowing a technician to connect to the remote system without the end user being physically present.

```

1  {
2      "publickey": "181e652afa0047e8de852ce025d62da0f7192f0e05d7dd3f560",
3      "WebsiteUrl": "devices-iot.console.gotoresolve.com",
4      "BaseUrl": "https://devices-iot.console.gotoresolve.com/",
5      "CompanyId": "937825596157721385",
6      "Product": 6,
7      "LogLevel": 2,
8      "Offline": 0,
9      "FleetTemplateName": "syn-prd-ava-unattended",
10     "Namespace": "syn-prd-ava-unattended",
11     "HealthCheckUrl": "https://devices.console.gotoresolve.com/health",
12     "CreatedAt": "1766123623235",
13     "SessionBackendUrl": "https://sessions.console.gotoresolve.com",
14     "AppletGeneratorUrl": "https://applet.console.gotoresolve.com",
15     "Region": "global",
16     "CustomBranding": 1,
17     "CustomBrandingTitle": "",
18     "CustomBrandingUrl": "https://custombranding.console.gotoresolve.com",
19     "Lang": "en",
20     "SessionType": "Unattended",
21     "WorkFolder": "C:\\Program Files (x86)\\GoTo Resolve Unattended\\937825596157721385",
22     "ApplicationType": 4,
23     "Salt": "w38czV9HEaJ7plmW",
24     "ServiceName": "GoToResolve 937825596157721385",
25     "HostName": "",
26     "Environment": "Production",
27     "WtsStartingSessionId": 1,
28     "RegisteredProcess": 1,
29     "Uuid": "1FA8B563-13ED-4588-BE83-25E1CE682744",
30     "CredentialProviderInstalled": 1
31 }

```

The application attempts to connect to **hxxps://dumpster.console[.]gotoresolve[.]com/api/sendEventsV2** to transmit event information in JSON format. The connection fails, and the application retries the request multiple times.

```
POST /api/sendEventsV2 HTTP/1.1
Host: dumpster.console.gotoreolve.com
Content-Type: application/json
Authorization: API-KEY cn16269ktie1dcpmz8y2ddxhjhhgi0nebxwpr4a3c711bfwnubk2[REDACTED]
Content-Length: 2553
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-IN,*
User-Agent: Mozilla/5.0
```

```
{
  "Records": {
    "companyId": "937825596157721385",
    "component": "Unattended",
    "computerId": "ef2f58fcbd2bf32db9c5a1d46d559b66",
    "deviceId": "",
    "events": [
      {
        "app": "Unattended",
        "facility": "SimpleConnectionController",
        "level": "info",
        "message": "onConnectionDisconnected, reason: ReconnectNeeded",
        "processId": "3184",
        "sessionId": "",
        "threadId": "Main",
        "time": "[REDACTED]",
        "utcTime": "[REDACTED]"
      }
    ],
  },
}
```

Why This Is Concerning

This behavior is concerning because Remote Monitoring and Management (RMM) tools inherently provide powerful capabilities such as remote command execution, system monitoring, persistent access, and unattended control. While legitimate in enterprise environments, these features are frequently abused by threat actors during initial access operations, particularly in crypto themed malware campaigns and fake wallet or airdrop lures, where RMM software is leveraged to establish long-term post exploitation persistence on compromised systems.

While **LogMeIn** Resolve itself is a legitimate product, its silent delivery inside a wallet installer is not legitimate behavior.

Detection Summary

- Flagged as PUA / Riskware
- Behavioral indicators consistent with remote management agents
- Not a known component of any official Eternl wallet release

Threat Assessment

Indicator	Risk
Newly registered download domain	High
MSI installer for wallet software	High
Drops RMM tool	Critical
PUA classification	Confirmed

HIGHLY SUSPICIOUS – DO NOT INSTALL

This campaign exhibits multiple overlapping indicators consistent with supply-chain abuse and trojanized wallet distribution, combined with pre positioning techniques that leverage RMM tools to establish persistent access. Together, these behaviors suggest preparation for potential follow on activity, including future credential harvesting or cryptocurrency wallet compromise.

Indicators of Compromise (IOCs)

Domains:

download[.]eternldesktop[.]network

Files

- etrnl.msi
- unattended-updater.exe

Product Identifiers

- LogMeIn Resolve
- GoTo Resolve

Hash

- 8fa4844e40669c1cb417d7cf923bf3e0
- 3f317e17741122cd4ea30123ba241cd0

This campaign demonstrates how crypto governance narratives are increasingly weaponized to distribute **covert access** tooling under the guise of professional software.