RISKIQ®

10 Things to Know About MEWKit

Cryptotheft's Newest Weapon Highlights the Dangers of Cryptocurrency Landscape

1. MEWKit is more than just a phishing kit.

MEWKit exceeds the capabilities of a typical phishing kit because it consists of two parts: a phishing page mimicking the MyEtherWallet site and a server-side component that handles the wallets to which attackers transfer stolen funds once a phishing attack succeeds.

While typical phishing pages usually redirect to the legitimate version of the website so the victim can log in again, MEWKit simply abuses MyEtherWallet's unique access to the Ethereum network to make the transactions in the background. By leveraging characteristics of automated Transfer System malware actors operating MEWKit can access and steal their phishing victims' Ethereum funds directly from the exchange.

Once a user logs in, MEWKit checks their wallet's balance and requests a receiver address from the server side. It then leverages the standard MyEtherWallet functionality by setting the attacker-owned wallet as the receiving address and transferring out the victim's entire balance.

2. Cryptocurrency exchanges are not always as secure as you think, which makes them a prime target for hackers.

MyEtherWallet is unlike other cryptocurrency exchanges and trading platforms because it does not have internal accounts. Like a bank or typical cryptocurrency exchange, a user creates an account to which they can transfer funds in and out. This way, the exchange has the keys to their wallet with the account providing an additional layer of security and adding controls such as two-factor authentication and security questions. These banks and exchanges are also able to perform analytics to see what device is being used to log in, and from where.

3. Remember the hijack of Amazon Route 53 traffic last month? All that traffic was directed to Russian servers running MEWKit

On April 24th at a little after 11:00 UTC, a border gateway protocol (BGP) hijack was performed targeting IP space associated with Amazon Route 53, which is an Amazon DNS provisioning system.

What this means is that an unauthorized party was able to reroute a portion of the traffic intended to reach Amazon Route 53 to itself and reroute domain resolutions to an endpoint of their own choice. The DNS servers that ended up handling the traffic were set up to only resolve myetherwallet[.]com, and the server responding for the redirected web traffic was operating MEWKit.

The DNS server that responded with a new IP address for MyEtherWallet routed from Russia, which is likely the country from which the actors behind this attack operate.

4. MEWKit is likely extremely lucrative

With close to a hundred domains set up in a period of a few months, the associated costs of carrying out its attacks point to MEWKit being exceptionally successful and, although simple in technical sophistication, efficient at stealing Ethereum and lucrative to operate. It has been reported that on the day of the Amazon DNS hijack, over 100,000 in Ethereum was stolen, although we are unable to corroborate these facts as described in our report.

5. Expect more attacks like the one against Amazon

The internet is old, and some of its core components are not aging gracefully. The Amazon attack is just the latest to involve Border Gateway Protocol (BPS), the technical specification that network operators use to exchange large chunks of Internet traffic.

Despite its crucial function in directing web traffic, BGP still relies on dubious means to determine if participants are trustworthy. In fact, service providers like Amazon have no effective technical means to prevent such attacks. BGP and DNS continue to be a problematic but essential piece of our global internet. The Amazon Route 53 Hijack had a single target in mind and managed to perform a substantial attack to reach their goal. Although the scope of this attack was relatively small, its footprint could have been much, much larger.

6. Direct access to a cryptocurrency network can be like playing with fire

Unlike a bank, which adds additional layers of security to its customers' accounts, MyEtherWallet gives users direct access to the Ethereum network through their browser. This direct access makes MyEtherWallet an extremely transparent experience, but without the added security layers of most banks and exchanges, it also creates some significant risks and puts fewer hurdles between attackers and a payday, which is why MEWKit was purpose-built for MyEtherWallet.

Once a phishing attack is successful on a MEWKit victim thinking they are interacting with the official MyEtherWallet website, funds are directly accessible to the attackers. Because of this, we believe MEWKit was born a phishing ATS build specifically for MyEtherWallet.

7. Hardware wallets are more secure than digital ones

While MyEtherWallet has support for various hardware wallets such as Trezor, Ledger Wallet, Digital Bitbox and Secalot MEWKit does not support stealing keys from these. This inability to steal keys from hardware wallets means those who are phished by MEWKit while using a hardware-based wallet will be affected by MEWKit's ATS but still need to confirm the transaction on their wallet before it processes because hardware wallets' private keys are stored inside and are therefore are not exposed to MEWKit.

Sudden, unexplained transactions are a good sign of hitting MEWKit and, of course, not accepting the transaction is the course to take.

8. Once you're hacked, there's no way to stop the bleeding.

MEWKit attacks, when a user authenticates with certain authentication options, have access to a victim's wallet after phishing them. If they purchase more Ethereum, the attackers can continue to drain their funds.

The authentication methods this will affect are:

- Mnemonic
- PrivateKey
- JSON / KeyFile.

9. Phishing is evolving

The level of sophistication required to pull off this attack—rerouting DNS traffic from a major service provider to a server running MEWKit—shows a new dedicated effort from threat actors to pursue cryptocurrency. Based on this amount of traffic captured in the Amazon DNS attack alone, it's safe to assume MEWKit will continue to be in operation for the foreseeable future.

10. All cryptocurrency exchanges could be at risk from a new version of MEWKit

While MEWKit was targeting only MyEtherWallet, RiskIQ found some direct connections to phishing pages for other cryptocurrency exchanges, which means MEWKit might expand to a catch-all phishing kit.

For the full story of MEWKit, its past and current campaigns, and a complete list of indicators of compromise, download the 30-page report here.

RISKIQ®

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ PassiveTotal could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com
1 888.415.4447 @RiskIQ