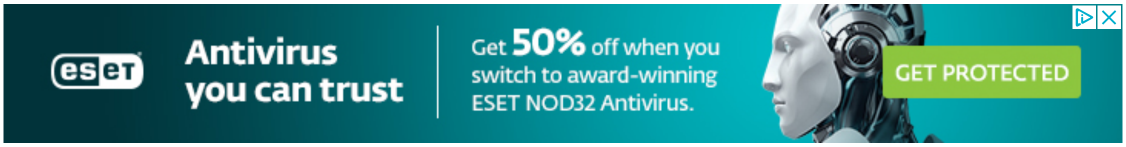
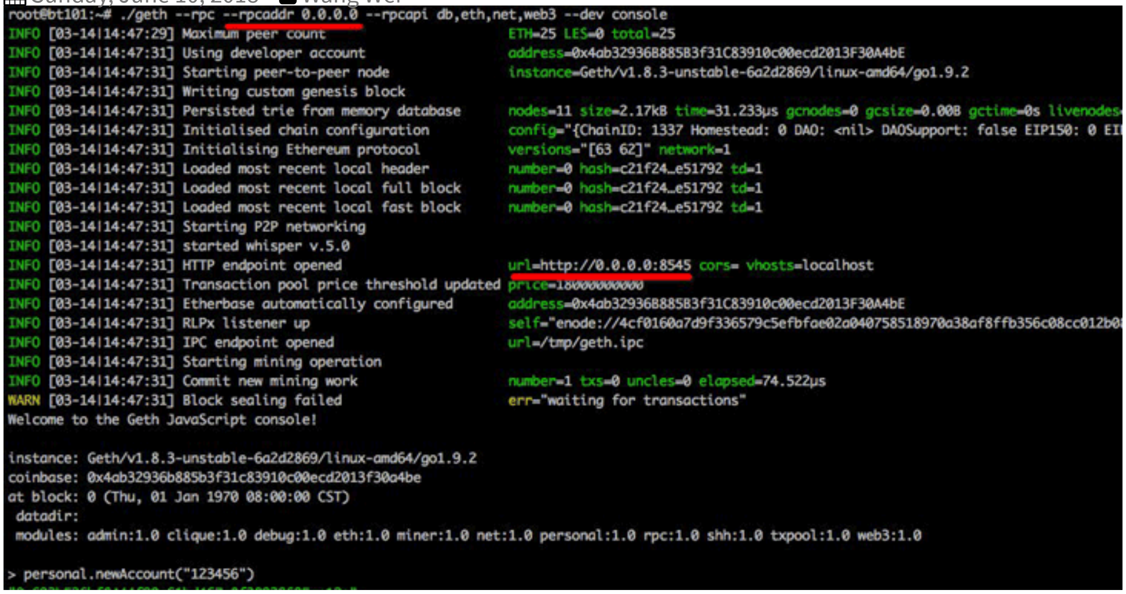
The Hacker News™
Security in a serious way

G+ +1,699,980
480,100
2,090,300



Hackers Stole Over $20 Million in Ethereum from Insecurely Configured Clients

Sunday, June 10, 2018 Wang Wei



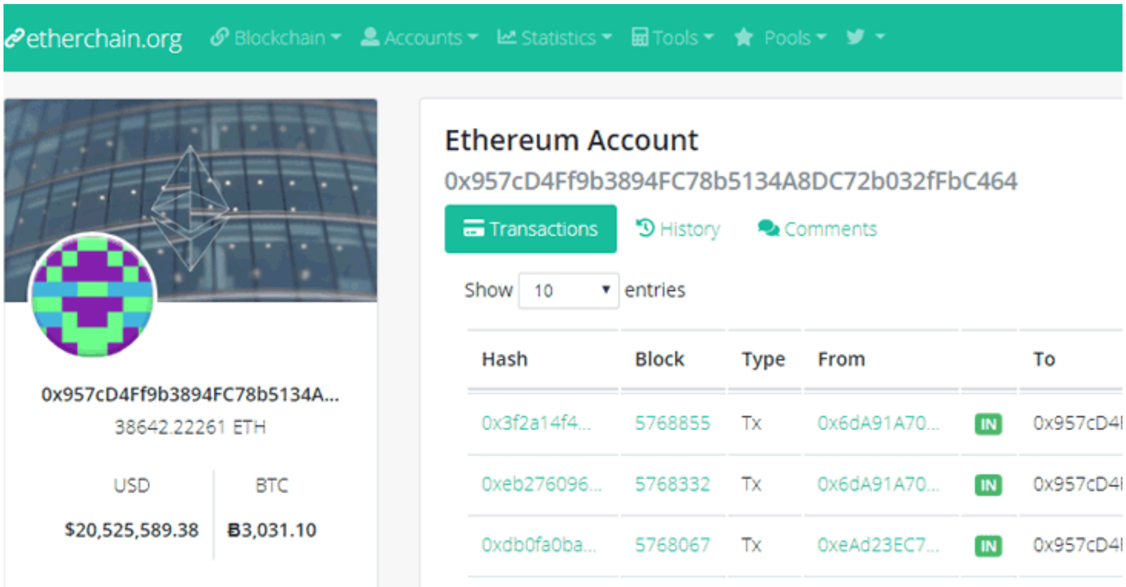
```
root@bt101:~# ./geth --rpc --rpcaddr 0.0.0.0 --rpcapi db,eth,net,web3 --dev console
INFO [03-14|14:47:29] Maximum peer count                       ETH=25 LES=0 total=25
INFO [03-14|14:47:31] Using developer account                  address=0x4ab32936B885B3f31C83910c00ecd2013F30A4bE
INFO [03-14|14:47:31] Starting peer-to-peer node               instance=Geth/v1.8.3-unstable-6a2d2869/linux-amd64/go1.9.2
INFO [03-14|14:47:31] Writing custom genesis block
INFO [03-14|14:47:31] Persisted trie from memory database      nodes=11 size=2.17kB time=31.233µs gcnodes=0 gcsize=0.00B gctime=0s livenodes
INFO [03-14|14:47:31] Initialised chain configuration          config="{ChainID: 1337 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: 0 EI
INFO [03-14|14:47:31] Initialising Ethereum protocol           versions="[63 62]" network=1
INFO [03-14|14:47:31] Loaded most recent local header          number=0 hash=c21f24…e51792 td=1
INFO [03-14|14:47:31] Loaded most recent local full block      number=0 hash=c21f24…e51792 td=1
INFO [03-14|14:47:31] Loaded most recent local fast block      number=0 hash=c21f24…e51792 td=1
INFO [03-14|14:47:31] Starting P2P networking
INFO [03-14|14:47:31] started whisper v.5.0
INFO [03-14|14:47:31] HTTP endpoint opened                     url=http://0.0.0.0:8545 cors= vhosts=localhost
INFO [03-14|14:47:31] Transaction pool price threshold updated price=18000000000
INFO [03-14|14:47:31] Etherbase automatically configured       address=0x4ab32936B885B3f31C83910c00ecd2013F30A4bE
INFO [03-14|14:47:31] RLPx listener up                         self="enode://4cf0160a7d9f336579c5efbfae02a040758518970a38af8ffb356c08cc012b0
INFO [03-14|14:47:31] IPC endpoint opened                      url=/tmp/geth.ipc
INFO [03-14|14:47:31] Starting mining operation
INFO [03-14|14:47:31] Commit new mining work                   number=1 txs=0 uncles=0 elapsed=74.522µs
WARN [03-14|14:47:31] Block sealing failed                     err="waiting for transactions"
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.3-unstable-6a2d2869/linux-amd64/go1.9.2
coinbase: 0x4ab32936b885b3f31c83910c00ecd2013f30a4be
at block: 0 (Thu, 01 Jan 1970 08:00:00 CST)
 datadir:
 modules: admin:1.0 clique:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 shh:1.0 txpool:1.0 web3:1.0

> personal.newAccount("123456")
```

Security researchers have been warning about cybercriminals who have made over 20 million dollars in just past few months by hijacking insecurely configured Ethereum nodes exposed on the Internet.

Qihoo 360 Netlab in March tweeted about a group of cybercriminals who were scanning the Internet for port 8545 to find insecure geth clients running Ethereum nodes and, at that time, stole 3.96234 units of Ethereum cryptocurrency (Ether).

However, researchers now noticed that another cybercriminal group have managed to steal a total 38,642 Ether, worth more than $20,500,000 at the time of writing, in past few months by hijacking Ethereum wallets of users who had opened their JSON-RPC port 8545 to the outside world.

Geth is one of the most popular clients for running Ethereum node and enabling JSON-RPC interface on it allows users to remotely access the Ethereum blockchain and node functionalities, including the ability to send transactions from any account which has been unlocked before sending a transaction and will stay unlocked for the entire session.



Ethereum Account

0x957cD4Ff9b3894FC78b5134A8DC72b032fFbC464

0x957cD4Ff9b3894FC78b5134A...

38642.22261 ETH

USD	BTC
$20,525,589.38	Ƀ3,031.10

Show 10 entries

Hash	Block	Type	From		To
0x3f2a14f4...	5768855	Tx	0x6dA91A70...	IN	0x957cD4I
0xeb276096...	5768332	Tx	0x6dA91A70...	IN	0x957cD4I
0xdb0fa0ba...	5768067	Tx	0xeAd23EC7...	IN	0x957cD4I

Here's the attackers' Ethereum account address, where all the stolen funds have been collected:

> **0x957cD4Ff9b3894FC78b5134A8DC72b032fFbC464**

By simply searching this address on the Internet, we found dozens of forums and websites where users have posted details of similar incidents happened with them, describing about the same account address hackers used to stole their funds from the insecurely configured Ethereum nodes.

According to an advisory issued by Ethereum Project three years ago, leaving the JSON-RPC interface on an internet-accessible machine without a firewall policy opens up your cryptocurrency wallet to theft "by anybody who knows your [wallet] address in combination with your IP."

NetLab researchers warned that not only the above-mentioned cybercriminal group but other attackers are also actively scanning the Internet for insecure JSON-RPC interface to steal funds from cryptocurrency wallets.

> "If you have honeypot running on port 8545, you should be able to see the requests in the payload. Which has the wallet addresses. And there are quite a few ips scanning heavily on this port now," 360 Netlab tweeted.

Users who have implemented Ethereum nodes are advised only to allow connections to the geth client originating from the local computer, or to implement user-authorization if remote RPC connections need to be enabled.

Share on Facebook Share on Twitter

Wang Wei

Security Researcher and Consultant for the government, Financial Securities and Banks. Enthusiast, Malware Analyst, Penetration Tester.

Cryptocurrency, Cryptocurrency Malware, Cyber Attack, Ethereum, Ethereum Development, Ethereum Wallet, Geth Client, Hacking Ethereum, Hacking News

★ Latest Stories

Cortana Software Could Help Anyone Unlock Your Windows 10 Computer
Cortana, an artificial intelligence-based smart assistant that Microsoft has built into every version of Windows 10, could help...

Special Price Drop—Get Secure VPN Service For Lifetime
PRIVACY – a bit of an Internet buzzword nowadays, because the business model of the Internet has now shifted towards data colle...

Google Blocks Chrome Extension Installations From 3rd-Party Sites
You probably have come across many websites that let you install browser extensions without ever going to the official Chrome w...

Microsoft June 2018 Patch Tuesday Pushes 11 Critical Security Updates
It's time to gear up for the latest June 2018 Microsoft security patch updates. Microsoft today released security patch update...

Signature Validation Bug Let Malware Bypass Several Mac Security Products
A years-old vulnerability has been discovered in the way several security products for Mac implement Apple's code-signing API t...

Thousands of Android Devices Running Insecure Remote ADB Service
Despite warnings about the threat of leaving insecure remote services enabled on Android devices, manufacturers continue to shi...

Best Deals

NaN% OFF

BUY NOW $0.00

...

Comments

1 Comment Sort by Newest ⇕

Add a comment...

Ether Plasmia · Flight Attendant at Toronto Pearson International Airport

ha! i love this man. Love to see that nothing is safe. And rich ppl who thinks they have the world in their hands getting a shot of reality. Here in Brazil we had a truck driver strike, which was better then any hacker attack u could imagine...rich folks standing next to poor folks in gas stations waiting for gasoline for 10 hours or more. A truck driver strike man, the whole nation has stopped. food raise in 100% the tatoes were 10 bucks it went up to 200. I know some rich motherfucker still got money out of this. but the country lost a lot too...this can be a key to global revolution, imagine...worldwide truck driver strike. Police was making security for gas trucks, because some would throw molotovs on the truck. ha! but situation is back on tracks now...u know why? they wanted a 40 cent discount on diesel fuel. But if they had a little bit more knowledge of the situation they caused they could take down all corrupted leaders.

Like · Reply · 2d

Facebook Comments Plugin

POPULAR STORIES

Update Google Chrome Immediately to Patch a High Severity Vulnerability

Marcus Hutchins, WannaCry-killer, hit with four new charges by the FBI

Facebook bug changed 14 million users' default privacy settings to public

Learn Ethical Hacking Online: A to Z Training Courses

Hackers Stole Over $20 Million in Ethereum from Insecurely Configured Clients

Adobe Issues Patch for Actively Exploited Flash Player Zero-Day Exploit

Prowli Malware Targeting Servers, Routers, and IoT Devices

Russia to Fine Search Engines for Linking to Banned VPN services

A New Paradigm For Cyber Threat Hunting

U.S. Builds World's Fastest Supercomputer – Summit