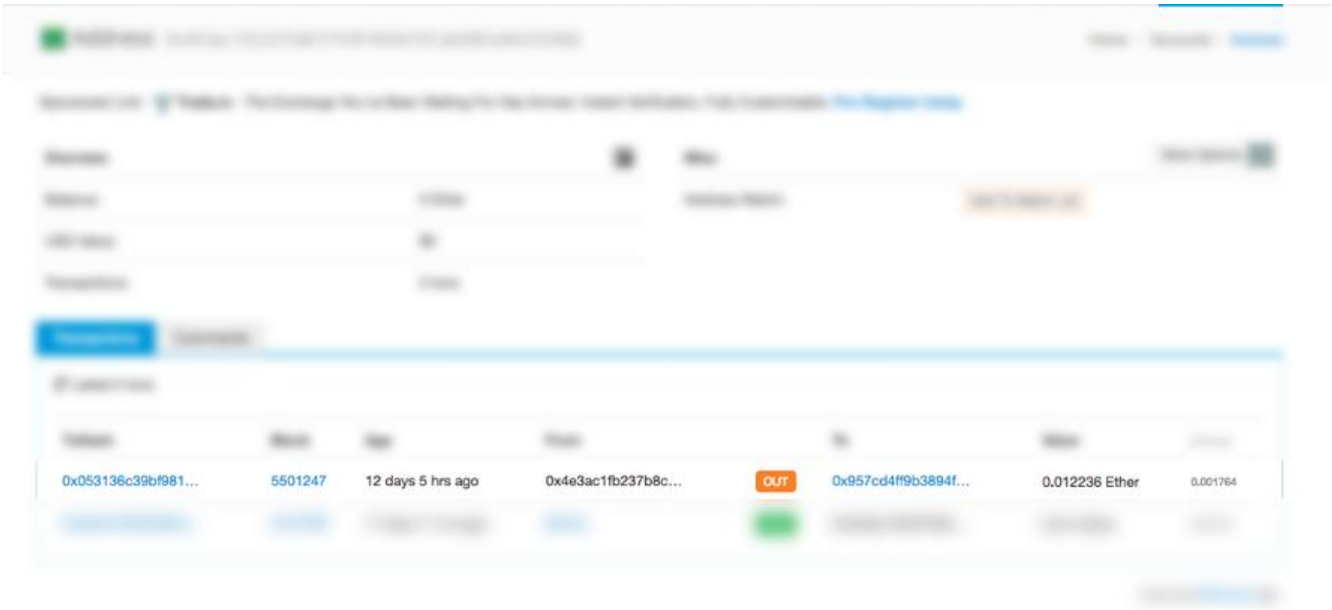
# 如何保护你的以太网节点 RPC 免受黑客攻击？

作者：hb01

原文链接：https://ld246.com/article/1557801575044

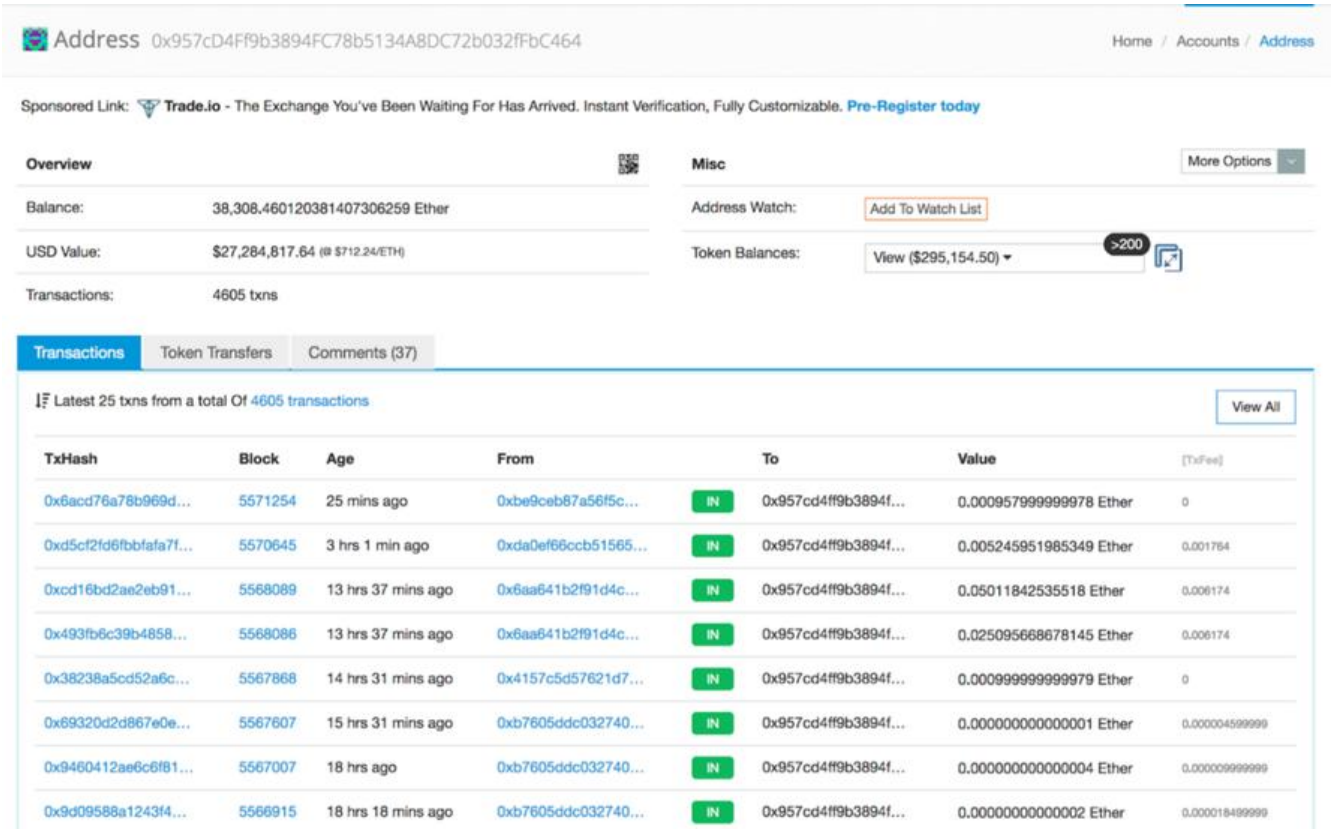
来源网站：链滴

最近朋友的以太坊节点遭到黑客攻击，存储在Geth钱包中的以太币通过暴露的RPC端口命令被转移出，Transfer可以在下面看到。



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0x053136c39bf981... | 5501247 | 12 days 5 hrs ago | 0x4e3ac1fb237b8c... | OUT | 0x957cd4ff9b3894f... | 0.012236 Ether | 0.001764 |

下图显示了最近向黑客帐户的转移：



Address 0x957cD4Ff9b3894FC78b5134A8DC72b032fFbC464

Home / Accounts / Address

Sponsored Link: **Trade.io** - The Exchange You've Been Waiting For Has Arrived. Instant Verification, Fully Customizable. **Pre-Register today**

**Overview**

| | |
|---|---|
| Balance: | 38,308.460120381407306259 Ether |
| USD Value: | $27,284,817.64 (@ $712.24/ETH) |
| Transactions: | 4605 txns |

**Misc**

More Options

| | |
|---|---|
| Address Watch: | Add To Watch List |
| Token Balances: | View ($295,154.50) >200 |

Transactions | Token Transfers | Comments (37)

Latest 25 txns from a total Of 4605 transactions — View All

| TxHash | Block | Age | From | | To | Value | [TxFee] |
|---|---|---|---|---|---|---|---|
| 0x6acd76a78b969d... | 5571254 | 25 mins ago | 0xbe9ceb87a56f5c... | IN | 0x957cd4ff9b3894f... | 0.000957999999978 Ether | 0 |
| 0xd5cf2fd6fbbfafa7f... | 5570645 | 3 hrs 1 min ago | 0xda0ef66ccb51565... | IN | 0x957cd4ff9b3894f... | 0.005245951985349 Ether | 0.001764 |
| 0xcd16bd2ae2eb91... | 5568089 | 13 hrs 37 mins ago | 0x6aa641b2f91d4c... | IN | 0x957cd4ff9b3894f... | 0.05011842535518 Ether | 0.006174 |
| 0x493fb6c39b4858... | 5568086 | 13 hrs 37 mins ago | 0x6aa641b2f91d4c... | IN | 0x957cd4ff9b3894f... | 0.025095668678145 Ether | 0.006174 |
| 0x38238a5cd52a6c... | 5567868 | 14 hrs 31 mins ago | 0x4157c5d57621d7... | IN | 0x957cd4ff9b3894f... | 0.000999999999979 Ether | 0 |
| 0x69320d2d867e0e... | 5567607 | 15 hrs 31 mins ago | 0xb7605ddc032740... | IN | 0x957cd4ff9b3894f... | 0.000000000000001 Ether | 0.000004599999 |
| 0x9460412ae6c6f81... | 5567007 | 18 hrs ago | 0xb7605ddc032740... | IN | 0x957cd4ff9b3894f... | 0.000000000000004 Ether | 0.000009999999 |
| 0x9d09588a1243f4... | 5566915 | 18 hrs 18 mins ago | 0xb7605ddc032740... | IN | 0x957cd4ff9b3894f... | 0.000000000000002 Ether | 0.000018499999 |

保护计算机系统传统上是一场斗智斗勇，Gosser说”穿透者试图找到漏洞，设计师试图关闭它们。”

与大多数比特币客户端不同，默认情况下，大多数以太坊客户端RPC不受密码保护。

尽管如此，有多种方法可以保护以太坊节点RPC。

其中一些方法包括：

原文链接：如何保护你的以太网节点 RPC 免受黑客攻击?

- 1.为帐户选择一个强密码。
- 2.使用Nginx作为反向代理和HTTP基本身份验证。
- 3.使用UFW设置防火墙。

## 安装以太坊客户端

以太坊有两个主要客户Parity和Geth。安装任何一个都可以很好地与以太坊网络进行交互。

你可以通过以下任一文章安装：

- https://github.com/ethereum/go-ethereum/wiki/Installing-Geth
- https://wiki.parity.io/Setup

## 配置节点

从来没有这样做过!!!

在GETH节点上启用RPC访问时，不允许在解锁帐户的情况下允许对RPC进行外部访问。例如：

$ geth — rpc — rpcaddr 0.0.0.0 — rpcport 8545 — rpcapi “db, eth, net, web3, personal” — pcapi “admin,eth,debug,personal,web3” — unlock <addrs>

你基本上允许外部访问你的以太坊帐户，并且当你解锁帐户时，攻击者可以轻松转出存储在你钱包中以太币。

由于此错误而被黑客入侵的示例：

https://ethereum.stackexchange.com/questions/3887/how-to-reduce-the-chances-of-your-ehereum-wallet-getting-hacked?utm_medium=organic&utm_source=google_rich_qa&utm_cmpaign=google_rich_qa

- 还有我的朋友:)

## 保护你的以太坊节点

### 1.为帐户选择强随机密码

在Parity或Geth上创建帐户时，请选择一个强大的随机密码。可以从以下站点生成密码：

- https://passwordsgenerator.net/
- https://lastpass.com/generatepassword.php
- https://www.random.org/passwords/

### 2.使用Nginx HTTP基本身份验证

- 安装Nginx

你需要在服务器上安装和配置Nginx，你可以按照此Nginx文章进行操作。

- 设置HTTP Auth基本凭据

在此步骤中，你将为运行该节点的用户创建密码。

该密码和关联的用户名将存储在你指定的文件中。密码将被加密，文件名可以是你喜欢的任何名称。

```
$ sudo htpasswd -c /etc/nginx/.htpasswd nginx
```

你可以检查新创建的文件的内容以查看用户名和哈希密码。

```
$ cat /etc/nginx/.htpasswd
```

- 更新Nginx配置

现在我们已经创建了HTTP基本身份验证凭据，下一步是更新Nginx配置以查看它。

```
$ sudo nano /etc/nginx/sites-available/default
```

更新文件以包含这些内容：

```
server {
 listen 80;
 listen [::]:80;
 # ADDED THESE TWO LINES FOR AUTHENTICATION
auth_basic  “Protected Ethereum client”;
auth_basic_user_file /path/to/passwords;
 server_name example.com;
 location / {
      proxy_pass http://localhost:8545/;
      proxy_set_header Host $host;
 }
}
```

- 测试

要应用更改，请先重新加载Nginx。

```
$ sudo service nginx reload
```

你现在可以访问RPC URL

**http://<USERNAME>:<PASSWORD>@mydomain.com**

你还可以安装可以从letsencrypt获得的免费SSL证书，你可以在此处找到该教程。

## 3.使用UFW设置防火墙

UFW或Uncomplicated Firewall是iptables的一个接口，旨在简化配置防火墙的过程。

- 安装UFW

```
$ sudo apt-get install ufw
```

- 设置默认策略

```
$ sudo ufw default deny incoming
$ sudo ufw default allow outgoing
```

- 允许以太网网络端口

我们还将启用以太坊网络，以便我们的节点能够与公共区块链网络进行通信和同步。

以太坊网络端口是30303，

```
$ sudo ufw allow 30303
```

- 启用RPC端口

我们只允许从我们的可信节点连接到我们的以太坊客户端。以太坊端口的默认RPC端口为8545。

```
$ sudo ufw allow from <IP addr> to any port 8545
```

例如，如果我的外部服务器IP地址是192.148.16.1，设置：

```
$ sudo ufw allow from 192.148.16.1 to any port 8545
```

如果你使用的是与8545不同的不同RPC端口，则应指定它。

- 启用UFW

启用UFW

```
$ sudo ufw enable
```

- 允许其他连接

你也可以根据需要启用其他端口，例如：HTTP 端口80，使用此命令可以允许HTTP连接（未加密的Web服务器使用的连接）：

```
$ sudo ufw allow http
```

你的防火墙现在应配置为允许连接到以太坊RPC和网络端口。确保允许服务器需要的任何其他传入连，同时限制任何不必要的连接，以便你的服务器功能和安全。

## 结论

安全性是区块链生态系统中的一个主要讨论。到处都有黑客想要偷走你的硬币。

如果你想学习区块链并在Blockchain Technologies建立职业生涯，那么请查看我们分享的一些以太区块链相关的交互式在线编程实战教程：

- java以太坊开发教程，主要是针对java和android程序员进行区块链以太坊开发的web3j详解。
- python以太坊，主要是针对python工程师使用web3.py进行区块链以太坊开发的详解。
- php以太坊，主要是介绍使用php进行智能合约开发交互，进行账号创建、交易、转账、代币开以及过滤器和交易等内容。
- 以太坊入门教程，主要介绍智能合约与dapp应用开发，适合入门。
- 以太坊开发进阶教程，主要是介绍使用node.js、mongodb、区块链、ipfs实现去中心化电商D

原文链接：如何保护你的以太网节点 RPC 免受黑客攻击?

pp实战，适合进阶。

- ERC721以太坊通证实战，课程以一个数字艺术品创作与分享DApp的实战开发为主线，深入讲以太坊非同质化通证的概念、标准与开发方案。内容包含ERC-721标准的自主实现，讲解OpenZeppeln合约代码库二次开发，实战项目采用Truffle，IPFS，实现了通证以及去中心化的通证交易所。

- C#以太坊，主要讲解如何使用C#开发基于.Net的以太坊应用，包括账户管理、状态与交易、智合约开发与交互、过滤器和交易等。