Security and Threats
Cryptocurrency Miners
INDEX

- Who am I?
- OSINT and Cryptocurrency
- Hacking Cryptocurrency Miners with OSINT Techniques
- Next Generation Phishing Attacks
- Web Browser Mining Attacks
- Smart-Contract Vulnerabilities
HELLO!

Seyfullah KILIÇ
Software Engineer
Security Researcher
since 2008
Listed Google Hall of Fame
Founder of @SwordSec
1. OSINT and Cryptocurrency

Open Source Intelligence...
What is Open-Source Intelligence

- Information gathering from public sources
- Gather Intelligence for both Offensive & Defensive Strategies
- Analysis of data or attackers
OSINT and Cryptocurrency

Relations between OSINT and Cryptocurrency
Using **OSINT** and Cryptocurrency

- Tracking Wallet
- Discovering Private Keys
- Exploring Miners Hardware
## BITCOIN ADDRESS REPORT

**Scan Alert:** This address has been reported as fraudulent (1 time)

### BTC Address
- **Address:** 366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG

### Wallet Details
- **Current Balance:** 0.01805590
- **Last Transaction:** 17 Mar 18
- **Last Known Input:** None
- **Last Known Output:** 1ERAvbYfew...

### Transaction Details
- **Total Received:** 3.84352509
- **# Transactions:** 238
- **# Output Transactions:** 114

### Scam Alert
- **Thomas Max Willam:** wmax908 - Instagram account
- **Reported Date:** Mar 29th, 18

### Website Appearances/Public Sightings
- **URL:** http://bitcoinwhoswho.com/address/366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG

### Transaction History

<table>
<thead>
<tr>
<th>Date Found</th>
<th>Description</th>
<th>More Detail</th>
<th>Website URL</th>
<th>URL Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 Mar 18</td>
<td>366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG</td>
<td>366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG</td>
<td><a href="http://bitcoinwhoswho.com/address/366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG">http://bitcoinwhoswho.com/address/366jyjTPhq8xuMJ6YVafQbPb2qHzSySpSxKG</a></td>
<td>-</td>
</tr>
</tbody>
</table>
Searching for Bitcoin Private Keys in GitHub repositories with Google BigQuery
Searching in Shodan and Censys

**Shodan**
is the world's first search engine for Internet-connected devices.

**Censys**
Finding and analyzing every reachable server and device on the Internet.
2. Hacking Cryptocurrency Miners with OSINT Techniques
Hacking “antMiner s9”

Discovering antMiner mining hardware and accessing to them...
(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"
Default root password: root

Step 2. Connect miner and your PC via network cable.
Step 3. Enter miner’s IP address into your web browser, then login miner management interface, both of username and password is ‘root’ by default.
Step 4. Set LAN as DHCP client. Click “Network->Interface->LAN”, select DHCP client as the following page, and then click “Switch Protocol”, and then click “Save & Apply”. The default LAN value of the first several batch is fixed to 192.168.1.1, and WAN address can’t be set as 192.168.1.x, otherwise the AntMiner can’t be accessed. If your miner’s LAN is set as DHCP by default, please ignore this step.
## Miner General Configuration

**Pool 1**
- URL
- Worker
- Password

**Pool 2**
- URL
- Worker
- Password

**Pool 3**
- URL
- Worker
- Password

**Setup**
- Search Frequency From: 550.00M
Hacking "Claymore Software"

Discovering Ethereum mining rigs and exploit them...
“ETH - Total Speed.”
Pool's Ethereum wallet address
What more can be done?

You can improve search techniques with OSINT for gathering **massive data**

You can even **damage all GPUs** by controlling the fans after editing the config.txt
Protection Methods

Setup a **firewall** in front of Mining Rig

Change **root** password

Close write **permission**
3. Next Generation Phishing Attacks
~ $4,782 Tokens
ICO CROWDFUNDING IS NOW OPEN!

After much waiting, The Bee Token is proud to announce that our crowdfund is NOW OPEN! You're so this address to register for our newsletter so we thought we'd give you some instructions on how to participate.

Firstly, we have modified your contribution maximum limit to be **104.43 ETH** so please don't send more than this or you won't be compensated. If you are receiving this email then you are permitted to join the ICO but your contribution limit is only guaranteed for 24 hours so don't miss out!

Secondly, to celebrate our NEW partnership with Microsoft thought we'd give you a **100% BONUS** on all tokens sent within the next 6 hours. We guarantee that The Bee Token will double in value within 2 months or we'll give you your Ethereum back!

Our Ethereum ICO address is:

`0xdf1ec2e44a8b1774b068ecfc5ef1c937a86bafe3e`

The ICO sale will close upon reaching our hard cap of 5,000 Ethereum so act fast before we run out of room!

Kind regards,
The Bee Token Team
**eth-phishing-detect**

Utility for detecting phishing domains targeting Ethereum users.

**basic usage**
4. Web Browser Based Mining Attacks
What is Browser Mining

- Generally Used Javascript API to mine the Monero
- Most Popular website is CoinHive.com
- CoinHive is blocked by TURKEY ISP
Browser Mining Attack Vectors

- MITM Attack and Injecting the Javascript Codes
- Injecting html codes by hacking popular websites
- DNS Hijacking
GET https://coinhive.com/lib/coinhive.min.js
Protection Methods

- Use "Mining Blocker" on Chrome
- Use Updated Antivirus
- Check Processes and CPU Usage
5. Ethereum Smart-Contract Vulnerabilities
function initWallet(address[] _owners, uint _required, uint _daylimit) {
    initDaylimit(_daylimit);
    initMultiowned(_owners, _required);
}
### Transaction Information

**Transaction Hash:** 0x9dbf0326a03a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec

**Block Height:** 4043800 (1310724 block confirmations)

**Timestamp:** 254 days 22 hrs ago (Jul-19-2017 12:18:15 PM +UTC)

**From:** 0x0e7647e1e397c0f121e79d3aa0620bc1dbbb3d02 (Multisig Exploit-Hacker)

**To:** 0xdeb65419e75b868a32a52f0734298822d8bcfe007e

**Value:**
- 0 Ether ($0.00)
- 0.000000021 Ether (21 Gwei)
- 0.001403619 Ether ($0.57)

**Gas Limit:** 82703

**Gas Used By Tx:** 66839

**Execution Fee:** 0.000000021 Ether (21 Gwei)

**Actual Tx Cost:** 0.001403619 Ether ($0.57)

**Contract:** 0xdeb65419e75b868a32a52f0734298822d8bcfe007e

---

**Function:** `initWallet(address[] _owners, uint256 _required, uint256 _default)` ***

**MethodID:** 0x6e460cfe

**Data:**

```
[0]: 0x0000000000000000000000000000000000000000000000000000000000000000
[1]: 0x0000000000000000000000000000000000000000000000000000000000000000
[2]: 0x0000000000000000000000000000000000000000000000000000000000000000
[3]: 0x0000000000000000000000000000000000000000000000000000000000000000
[4]: 0x0000000000000000000000000000000000000000000000000000000000000000
```

**Convert to Add**

*To access the private Note feature, you must be logged in*
~$33,424,300
Protection Methods

- Detect Overflows & Underflows
- Visibility & Delegatecall
- Reentrancy
Thank you for listening...

http://swordsec.com
info@swordsec.com
twitter.com/Sword_Sec