Ghost Robbers In The Cloud
Finding Crypto Miners

Shira Shamban
Dome9 Security (acquired by CheckPoint)
Money Heist – Let’s Review...
Finders Keepers, Losers Weepers

```json
"sync_down_on Open": true,
"sync_same_age": true,
"host": "c:kr",
"user": "dcc120140248",
"password": "mkw0268",
"port": "22",
"upload_on_save": true,
"remote_path": "/export/dcc_class/dcc/dcc120140248/hw1",
"file_permissions": "664",
"dir_permissions": "775",
"extra_list_connections": 0,
```
“Overtaking Ransomware, Cryptominers affected over 42% of organizations worldwide, compared to 20.5% at the end of 2017”

“During the first six months of 2018, Cryptomining attacks are estimated to have ‘earned’ their users more than $2.5 billion”
It WILL Be Your Fault

“Through 2022, at least 95% of cloud security failures will be the customer’s fault” Gartner
MMM

```
[ec2-user@ip-10-0-1-63 cpuminer-multi]$ sudo ./miner -a cryptonight -o stratum+tcp://pool.minexmr.com:4444 -iQtaPNqaugfr8KZ7adyaSksr4hHEsAW8yxJ8b2R7fRs1VbMm -p 1 -t 3
[2019-01-23 09:44:01] Using JSON-RPC 2.0
[2019-01-23 09:44:02] Pool set diff to 15000
[2019-01-23 09:49:49] Pool set diff to 11407
[2019-01-23 09:51:02] Stratum detected new block
[2019-01-23 09:51:50] Stratum detected new block
[2019-01-23 09:51:57] Stratum detected new block
[2019-01-23 09:52:09] accepted: 1/1 (100.00%), 34.81 H/s at diff 11407 (yay!!!)
[2019-01-23 09:55:32] accepted: 2/2 (100.00%), 34.99 H/s at diff 11407 (yay!!!)
[2019-01-23 09:55:34] Stratum detected new block
[2019-01-23 09:56:22] accepted: 3/3 (100.00%), 35.08 H/s at diff 11407 (yay!!!)
[2019-01-23 09:56:38] Stratum detected new block
[2019-01-23 09:57:18] Stratum detected new block
[2019-01-23 09:58:09] Stratum detected new block
[2019-01-23 10:00:41] accepted: 4/4 (100.00%), 34.85 H/s at diff 11407 (yay!!!)
[2019-01-23 10:01:44] Stratum detected new block
[2019-01-23 10:03:21] accepted: 5/5 (100.00%), 34.54 H/s at diff 11407 (yay!!!)
[2019-01-23 10:05:49] Stratum detected new block
```

How?
Containers!

25% of companies have adopted Docker!
Docker Version: 18.06.1-ce

HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 13 Jan 2019 18:07:51 GMT
Content-Length: 29

Docker Containers:
- Image: karmix/mongo-miner
  Command: /xmrig -o lgo-cryptonight-lite --url pool.aeon.hashvault.pro:3333 --user-kmtnxe1KvV5DA8bfyX1Z2By3a6xHxumanQ42FhGnWf/aM/hKmU8t3s8aL/tOBWgaH47ZxWTD7LlA0B83oG8ecP25b9Jh23mBwv9FtGx/aM/hKmU8t3s8aL/tOBWg

- Image: ubuntu
  Command: /bin/bash

- Image: dev-peer.org.h3c.com-zswl-v1-20171026feu10ecf214f675a2c58699f98795f6ed34549ed5411328b7a5c08
  Command: chaincode -peer.address=peer0.org.h3c.com:7052

- Image: dev-peer.org.h3c.com-zswl-v1-3126741246fe69F3510877c583453d20d44095m190646d952a40e8535ccadfe1
  Command: chaincode -peer.address=peer0.org.h3c.com:7052

- Image: hyperledger/fabric-peer:1.1.0
  Command: peer node start
msf exploit(linux/http/docker_daemon_tcp) >
MVD – minimal viable detection
MVD – minimal viable detection

Production environment –
MVD – minimal viable detection

Miner traffic
Tell-Tale Signs...

- Scan the code
- Monitor CPU
- Monitor the cost
- Ports (Docker, miner)
- First-time asset
- First-time connections
- Mind the socket
Any questions?

Tic-tac, tic-tac, tic-tac.
Thank you!

Shira Shamban
shirasha@checkpoint.com
@ShambanIT