RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HTA-F01

The New Gold Rush: How to Hack Your Own Best Mining Rig

Roy Katmor

CEO and Co-Founder
enSilo
@RoyKatmor

Udi Yavo

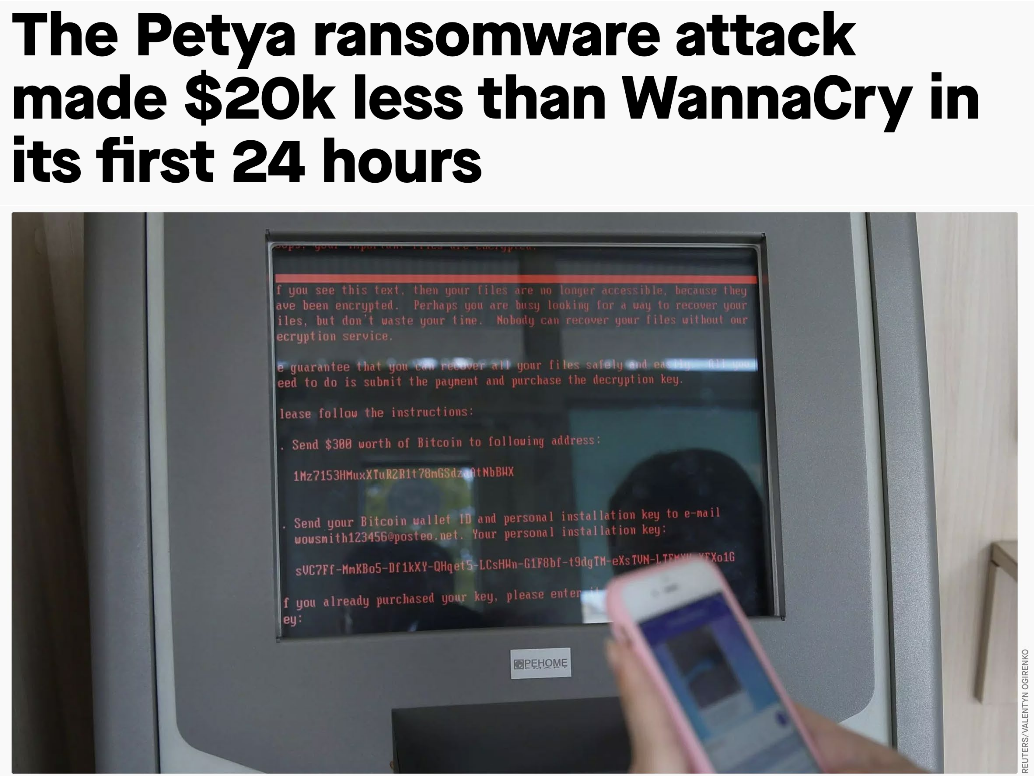
CTO and Co-Founder
enSilo
@UdiYavo

Agenda

- What is crypto-currency mining?
- Miners vs Ransomware
- Hacking your own mining rig
- Detection techniques
- Demo
- Summary

Cryptomining is Big Busine$$

Petya Grossed $132K USD in six weeks



The Petya ransomware attack made $20k less than WannaCry in its first 24 hours

```
f you see this text, then your files are no longer accessible, because they
ave been encrypted.  Perhaps you are busy looking for a way to recover your
iles, but don't waste your time.  Nobody can recover your files without our
ecryption service.

e guarantee that you can recover all your files safely and easily.  All you
eed to do is submit the payment and purchase the decryption key.

lease follow the instructions:

. Send $300 worth of Bitcoin to following address:

  1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

. Send your Bitcoin wallet ID and personal installation key to e-mail
  wowsmith123456@posteo.net. Your personal installation key:

  sVC7Ff-MmKBo5-Df1kXY-QHqet5-LCsHWn-G1F8bf-t9dgTM-eXsTVN-LT[illegible]FXo1G

f you already purchased your key, please enter [illegible]
ey:
```

REUTERS/VALENTYN OGIRENKO

Cryptomining = $100M in One Year

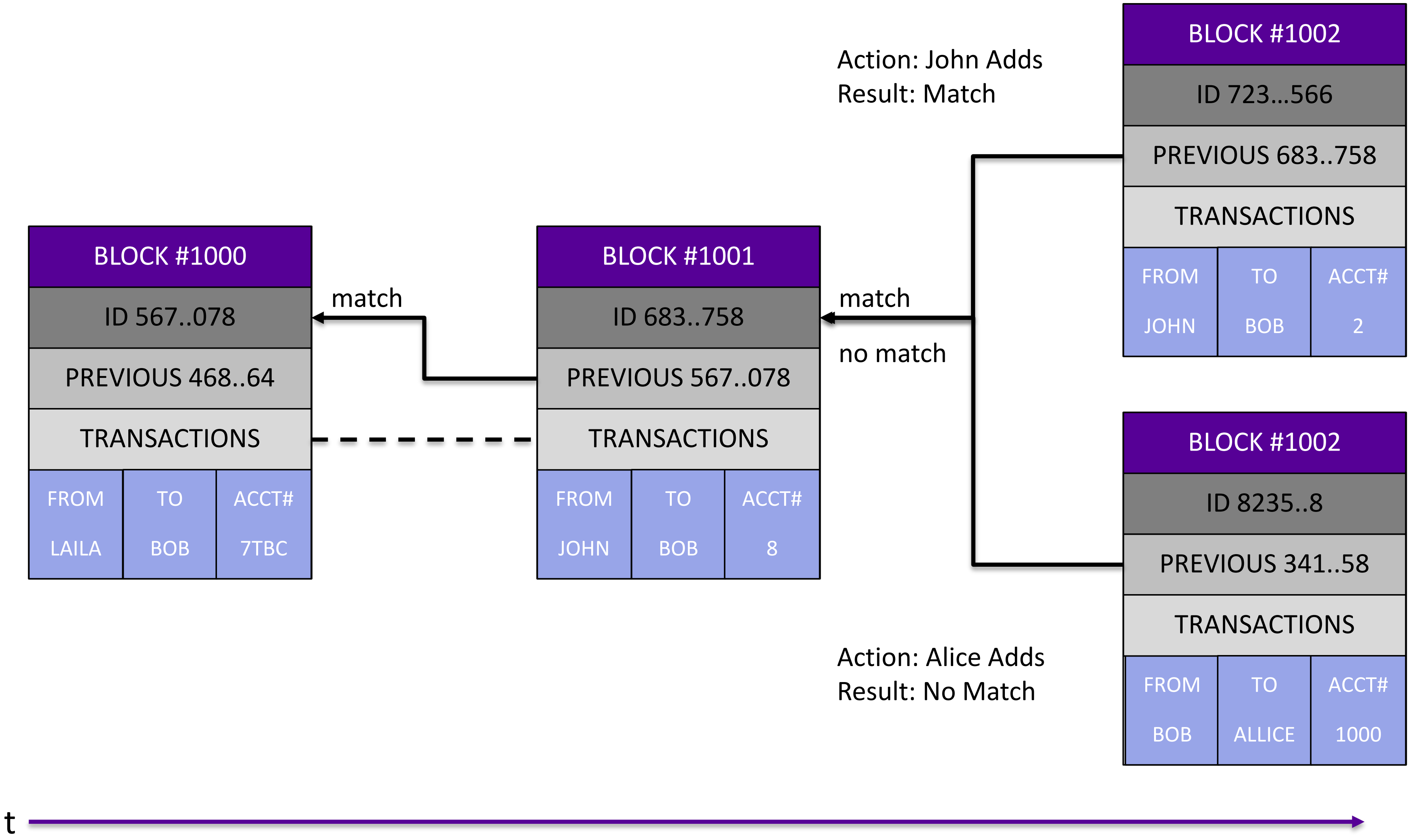
One Hacker Can Make $100M A Year With Evil Cryptocurrency Miners

WHAT IS CRYPTO-CURRENCY MINING?

What is crypto-currency mining?

- Crypto-currencies use block-chains to create a ledger of transaction
- Adding a transaction is done a solving a math problem
  - A miner needs to find a nonce that will generate a hash lower than a predefined target hash
  - For example, a target hash must contain X number of leading 0
  - Computationally, it's a hard problem to solve
- Mining is essentially process of verification and adding of transactions to a block-chain
  - Each time a miner adds a block it get crypto-currency for it's efforts
  - Transaction can also specify a "reward" for the miner that adds it to the blockchain

What is crypto-currency mining?



Action: John Adds
Result: Match

BLOCK #1000

ID 567..078

PREVIOUS 468..64

TRANSACTIONS

FROM	TO	ACCT#
LAILA	BOB	7TBC

BLOCK #1001

ID 683..758

PREVIOUS 567..078

TRANSACTIONS

FROM	TO	ACCT#
JOHN	BOB	8

BLOCK #1002

ID 723...566

PREVIOUS 683..758

TRANSACTIONS

FROM	TO	ACCT#
JOHN	BOB	2

BLOCK #1002

ID 8235..8

PREVIOUS 341..58

TRANSACTIONS

FROM	TO	ACCT#
BOB	ALLICE	1000

Action: Alice Adds
Result: No Match

What is crypto-currency mining?

But Crypto-mining is hard – very hard

Can take years for slow miners…

Mining Pools

- Basically means “mining together”

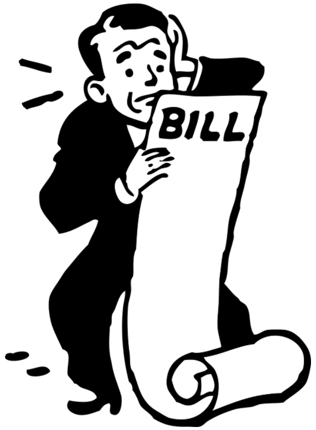
- The profit is distributed between the miners in pool based on their amount of work – Or shares
  - Miners need to present “proof-of-work” to get their shares

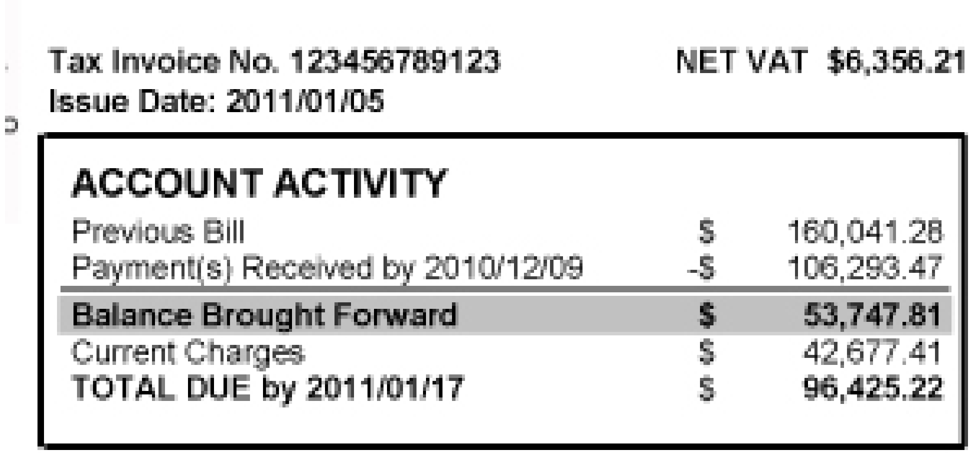
Mining Pools – Proof of Work

- All miners in a pool constantly try to “strike gold”
- Only one miner will actually find it
- The “gold” needs to be distributed to workers based on their efforts or “shares”
- Shares are gained by finding “easier” to find nounce
  - Basically hashes that are “close” to the target are considers shares
  - This is fair since the chance to find a share is equal
  - The difficulty can be set based on how close to the target it needs to be
  - Work is not wasted and the pool can validate shares
- Payment methods are different between pools

Mining Costs

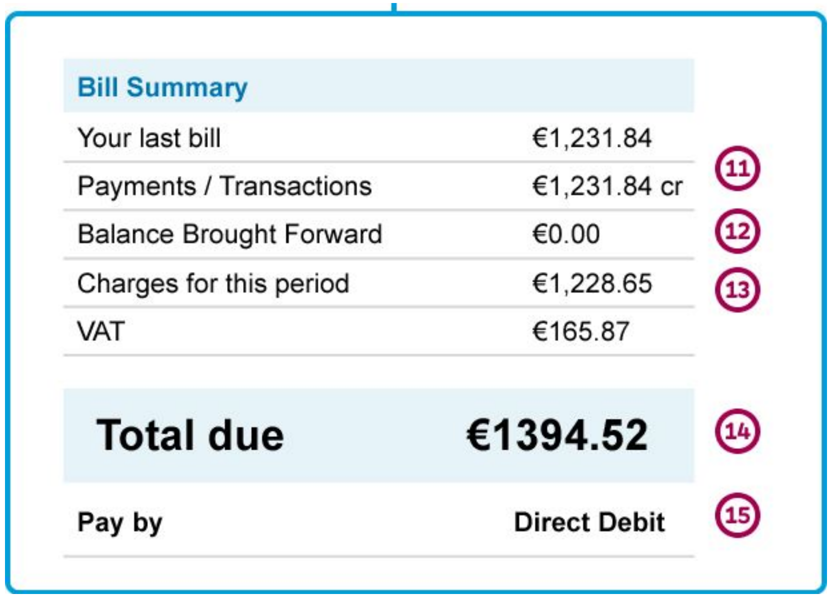
- Requires significant amounts of electricity
- Unless you’re like Facebook and can cool your server farm with cold air from the artic circle, this is what your electricity bill will look like….




Tax Invoice No. 123456789123 NET VAT $6,356.21
Issue Date: 2011/01/05

ACCOUNT ACTIVITY

Previous Bill	$	160,041.28
Payment(s) Received by 2010/12/09	-$	106,293.47
Balance Brought Forward	**$**	**53,747.81**
Current Charges	$	42,677.41
TOTAL DUE by 2011/01/17	$	96,425.22


Bill Summary

Your last bill	€1,231.84	
Payments / Transactions	€1,231.84 cr	11
Balance Brought Forward	€0.00	12
Charges for this period	€1,228.65	13
VAT	€165.87	
Total due	**€1394.52**	14
Pay by	**Direct Debit**	15

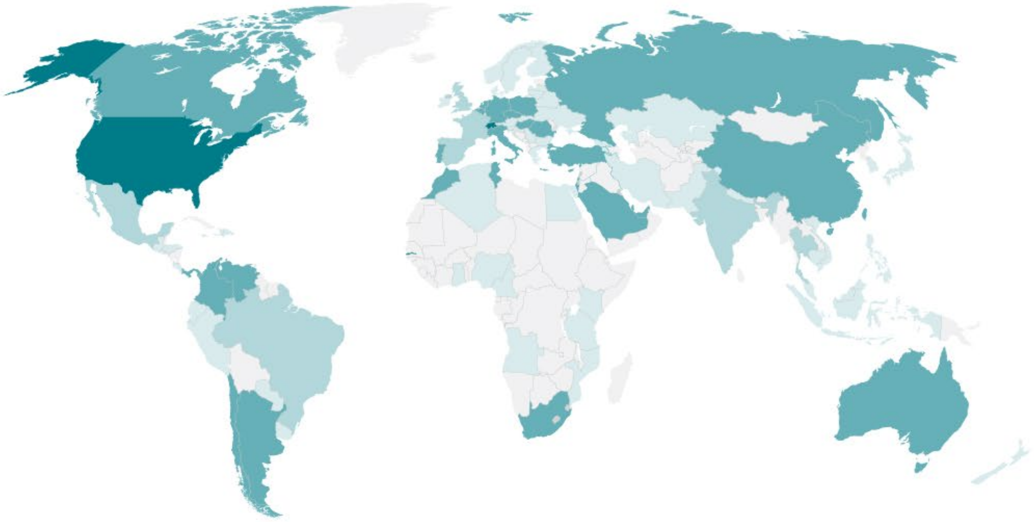
RSAConference2019

Miners vs Ransomware

Miners vs Ransomware - Commonalities

- Tools of choice for threat actors to make money
- Relevant to both Consumers and Enterprises
- Relatively low cost for entry – high ROI
- Are everywhere…

Cryptomining geo-distribution



CRYPTOMINING USERS

Country	Count
United States	37,660
Switzerland	15,154
Brazil	3,937
India	3,916
Spain	3,317
United Kingdom	3,040
Mexico	2,793
Thailand	2,562
France	2,552
Poland	2,277

Source: Zscaler

Miners vs Ransomware - Damage

Ransomware

Ransomware decommissions machines and destroys data – clearly high damage

- Big incentive to track and stop the attacker - Bad for operators

Miners

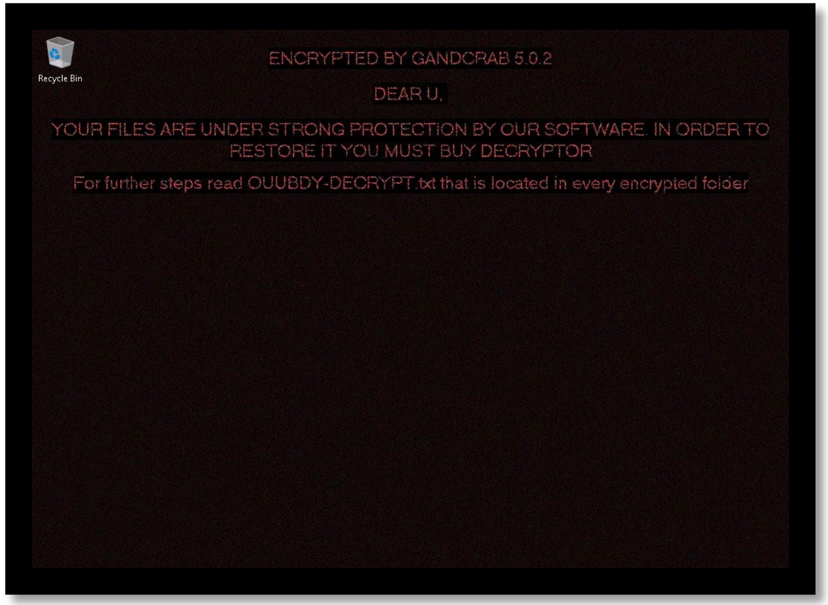
Miners cost is mostly electricity – low damage

- Less incentive to track down the attacker – good for operators
- Many also steal currency and not only mine
- Electricity costs can be significant too
- Many Miners do have ransomware capability
  - Darkgate, Rakhni, Xbash - too name a few
  - Operator can decide what is best Mine/Ransom based on risk/profit

Miners VS Ransomware - Stealth

Ransomware

- Doesn’t hide at all – just encrypts the machine and asks for payout



ENCRYPTED BY GANDCRAB 5.0.2

DEAR U,

YOUR FILES ARE UNDER STRONG PROTECTION BY OUR SOFTWARE. IN ORDER TO RESTORE IT YOU MUST BUY DECRYPTOR

For further steps read OUUBDY-DECRYPT.txt that is located in every encrypted folder

Miners

- Must be hidden to work over time
  - Persistency is important
  - Should not be easy to spot/detect
  - Must have a network connection to make money

Miners VS Ransomware - Payout

Ransomware

- Depends on victim willingness to pay
- Price per-attack is known and controlled by attack

Miners

- Almost certain
- Amount depends on victim machine and time on computer and currency value
- Can work as ransomware too

Miners VS Ransomware – Many Distribution Options

Ransomware

- Phishing
- Exploits
- Operations (RDP password guessing)
- Other Malware

Miners

- Phishing
- Exploits
- Operations (RDP password guessing)
- Other Malware
- Web Mining (Coinhive)
- PUA Installer Bundles

Miners VS Ransomware – Dev Efforts

Ransomware

- Ransomware itself is normally simple
- Backend is required to restore victim files/keys

Miners

- Open-source tools
  - https://github.com/xmrig/xmrig
  - https://github.com/LysanderGG/Simple-XMR-Miner
- No backend needed
  - Mining is decentralized
  - Public mining pools
- More on dev-later

Miners VS Ransomware – Prosecution Risk

Ransomware

- High damage = High incentive to stop actors
- Backend – Ransomware have backends that can potentially tie to the actor

Miners

- Low damage = Low incentive to stop actors
- No backend – decentralized payment system. No way to easily trace to actor

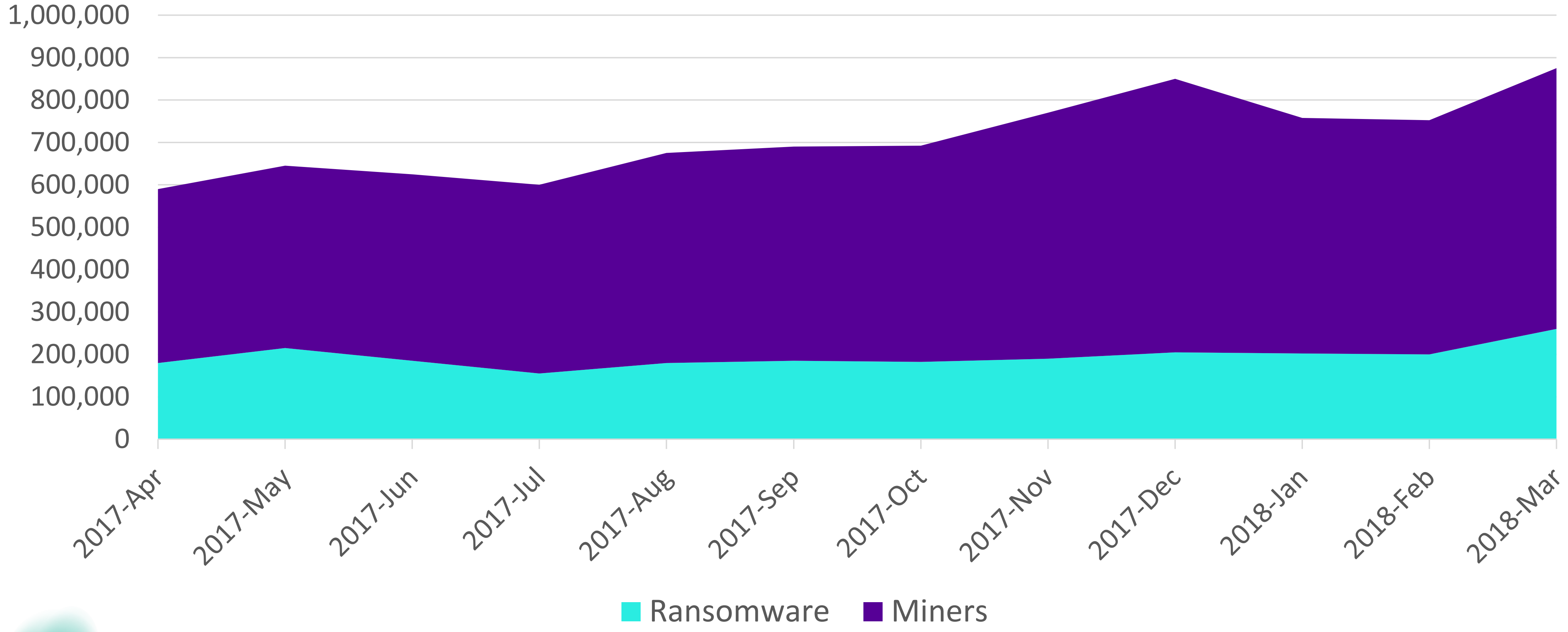
Miners vs Ransomware - Summary

	Ransomware	Miners
Damage	High	Low ✓
Stealth	None ✓	Needs to remain hidden
Payout	Depends on victim =	Very Likely
Distribution	More limited	Many methods ✓
Dev-effort	Medium	Low ✓
Risk	Medium	Low ✓

Miners WIN!

2017-2018 – Miners eclipse ransomware

The number of users encountering either ransomware or miners at least once in the period from April 2017 to March 2018 (Source: Kaspersky)



DarkGate Malware - Awesome Example of a Miner Found in the Wild

- Uses multiple methods for avoiding detection by traditional AV using vendor-specific checks and actions including the use of the process hollowing technique
- Has the ability to evade elimination of critical files by several known recovery tools
- Uses two distinct User Account Control (UAC) bypass techniques to escalate privileges
- Is capable of detonating multiple payloads with capabilities that include cryptocurrency mining, crypto stealing (theft of credentials associated with crypto wallets), ransomware and remote control

RSA®Conference2019

Hacking your own miner rig

Build you own miner – Requirements

Coin

- Anonymity
- Profitable
- Easy Development

Stealth

- Evade detection
- Create variants easily
- Persistency
- Obfuscation

Distribution

- Minimal effort distribution

Build you own miner – Monero, Malware coin of choice

- Anonymity
  - Untraceable – Not possible to know how you use funds
  - Confidential amount – Can't tell which transactions are big/small
- Effective on CPU – Unlike Bitcoin, mining Monero on CPU is almost as effective as GPU/ASIC
  - Means that random targets will generate profit
- Effective for WEB mining
- Easy to use open-source tools
  - https://github.com/emesik/monero-python
  - https://github.com/fireice-uk/xmr-stak
  - https://github.com/xmrig/xmrig - Used by most Monero miners

Build you own miner – Requirements

☑ Coin

- Anonymity
- Profitable
- Easy Development

□ Stealth

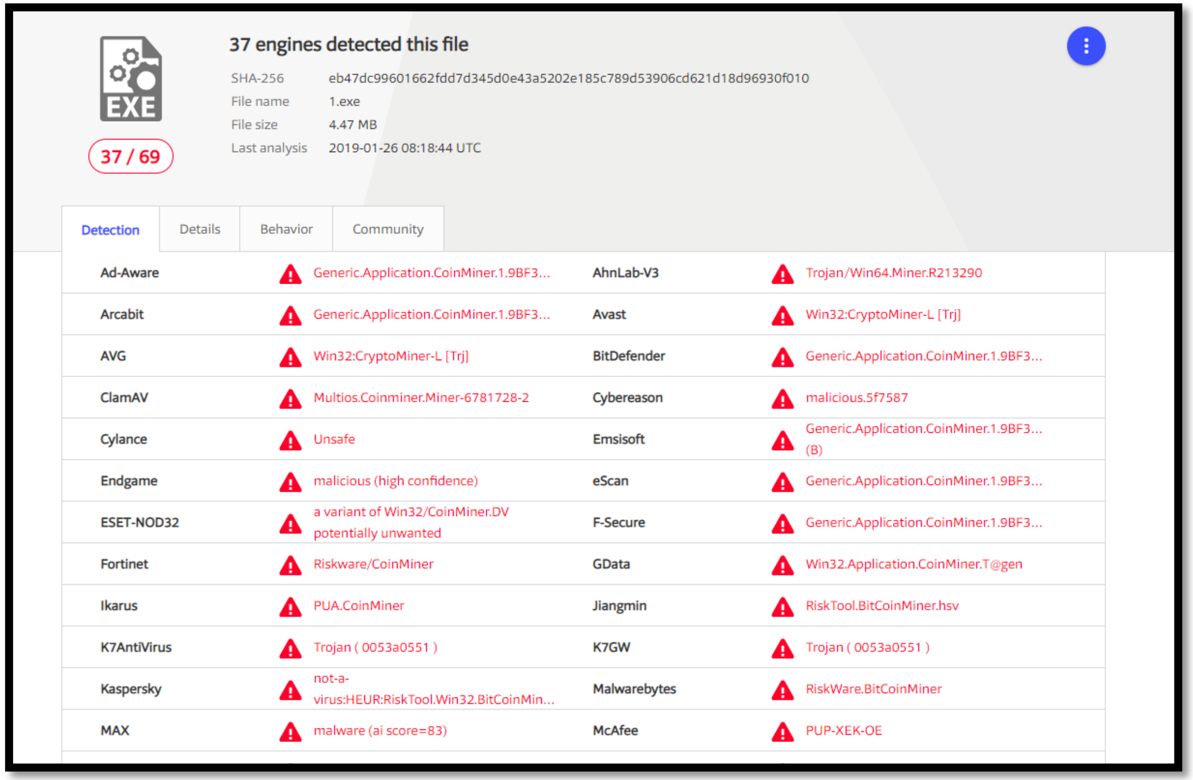
- Avoid simple detection methods
- Easy Variants Creation

□ Distribution

- Minimal effort distribution

Build you own miner – Evade Detection

- XMRIG triggers many Anti-Virus:



37 / 69

37 engines detected this file

SHA-256 eb47dc99601662fdd7d345d0e43a5202e185c789d53906cd621d18d96930f010
File name 1.exe
File size 4.47 MB
Last analysis 2019-01-26 08:18:44 UTC

Ad-Aware	⚠ Generic.Application.CoinMiner.1.9BF3...	AhnLab-V3	⚠ Trojan/Win64.Miner.R213290
Arcabit	⚠ Generic.Application.CoinMiner.1.9BF3...	Avast	⚠ Win32:CryptoMiner-L [Trj]
AVG	⚠ Win32:CryptoMiner-L [Trj]	BitDefender	⚠ Generic.Application.CoinMiner.1.9BF3...
ClamAV	⚠ Multios.Coinminer.Miner-6781728-2	Cybereason	⚠ malicious.5f7587
Cylance	⚠ Unsafe	Emsisoft	⚠ Generic.Application.CoinMiner.1.9BF3... (B)
Endgame	⚠ malicious (high confidence)	eScan	⚠ Generic.Application.CoinMiner.1.9BF3...
ESET-NOD32	⚠ a variant of Win32/CoinMiner.DV potentially unwanted	F-Secure	⚠ Generic.Application.CoinMiner.1.9BF3...
Fortinet	⚠ Riskware/CoinMiner	GData	⚠ Win32.Application.CoinMiner.T@gen
Ikarus	⚠ PUA.CoinMiner	Jiangmin	⚠ RiskTool.BitCoinMiner.hsv
K7AntiVirus	⚠ Trojan (0053a0551)	K7GW	⚠ Trojan (0053a0551)
Kaspersky	⚠ not-a-virus:HEUR:RiskTool.Win32.BitCoinMin...	Malwarebytes	⚠ RiskWare.BitCoinMiner
MAX	⚠ malware (ai score=83)	McAfee	⚠ PUP-XEK-OE

Build you own miner – Evade Detection

Some possibilities:

- Alter the source-code enough to avoid detection
  - Manual changes are lot of work
  - Can use obfuscators but still work
- Pack it
  - Creating a new packer is a lot of work
  - Using existing packer will trigger Anti-Virus
- Execute the payload only in memory
  - Many open-source possibilities:
    - https://github.com/itm4n/VBA-RunPE
    - https://github.com/oueldz4/runpe/blob/master/runpe.py
    - …

Build you own miner – Easy Payload Creation with python

- Quick coding and easy to modify but needs to be installed
  - Use py2exe or PyInstaller to create executable file
- Python RunPE supports payload Encryption OOB
  - Requires minor modification to execute payload with arguments
- Obfuscation – Multiple open-source libraries
  - https://github.com/QQuick/Opy
  - https://liftoff.github.io/pyminifier/
  - …
- Persistency – Easy to add using python

Build you own miner – Python RunPE Modifications

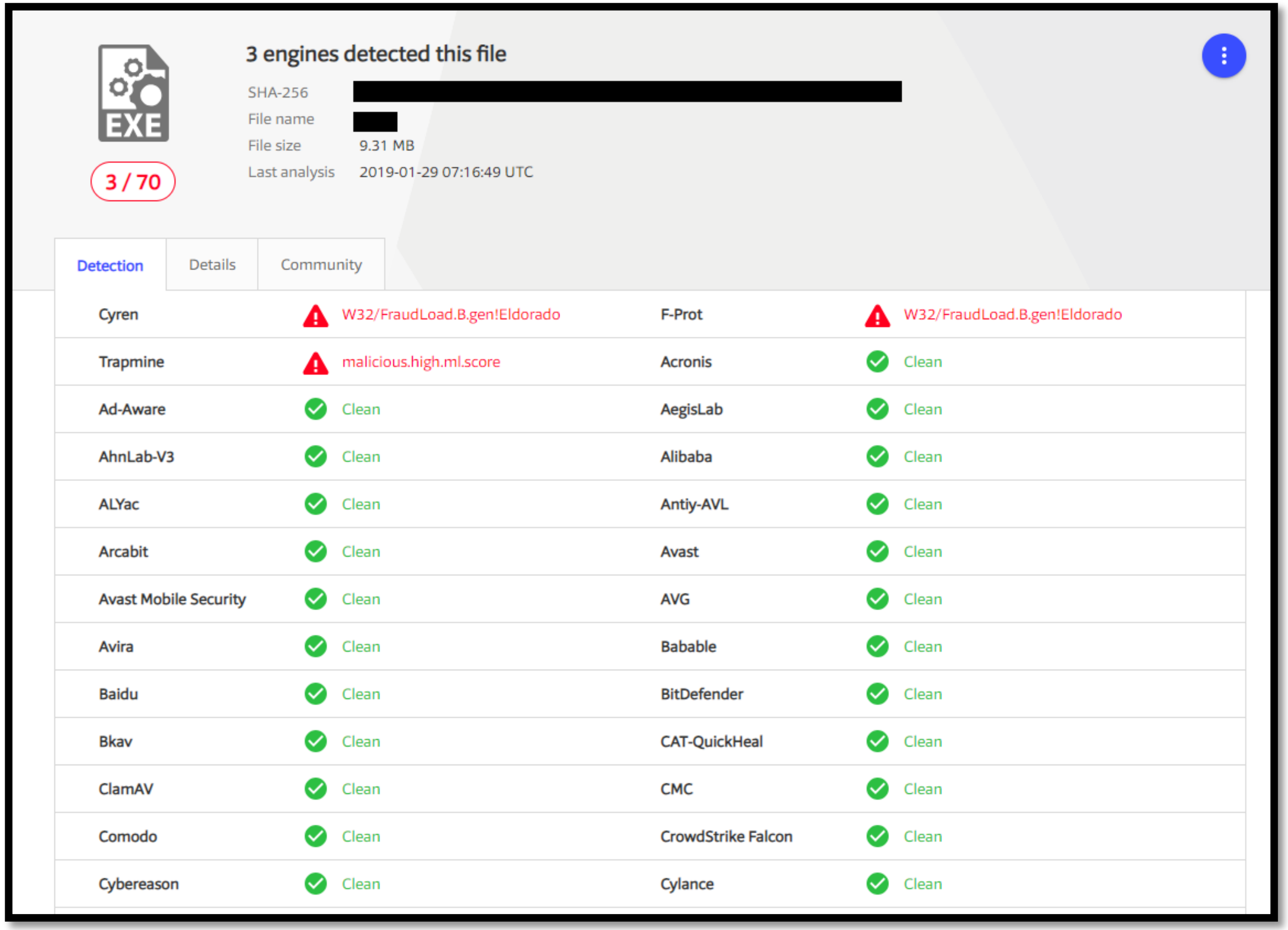
- Support payload compression
- Support 64-bit systems
- Support arbitrary file dropping
  - XMRIG needs configuration file
- Launch as hidden process
- Add persistency
  - Code from stackoverflow
- Support arbitrary payload base address
- 2 Minor bug fix
- Remove prints ☺

Build you own miner – Payload creation Summary

1. Use XMRIG compiled binaries – 0 Work
2. Leveraging python RunPE to execute XMRIG in memory
   - About 30 lines of code + 23 lines from stack overflow for persistency
   - About 3 hours of debugging and modifying the original code

Build you own miner – VT After modifications

- After:



3 engines detected this file

SHA-256 [redacted]
File name [redacted]
File size 9.31 MB
Last analysis 2019-01-29 07:16:49 UTC

3 / 70

Cyren	⚠ W32/FraudLoad.B.gen!Eldorado	F-Prot	⚠ W32/FraudLoad.B.gen!Eldorado
Trapmine	⚠ malicious.high.ml.score	Acronis	✓ Clean
Ad-Aware	✓ Clean	AegisLab	✓ Clean
AhnLab-V3	✓ Clean	Alibaba	✓ Clean
ALYac	✓ Clean	Antiy-AVL	✓ Clean
Arcabit	✓ Clean	Avast	✓ Clean
Avast Mobile Security	✓ Clean	AVG	✓ Clean
Avira	✓ Clean	Babable	✓ Clean
Baidu	✓ Clean	BitDefender	✓ Clean
Bkav	✓ Clean	CAT-QuickHeal	✓ Clean
ClamAV	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	CrowdStrike Falcon	✓ Clean
Cybereason	✓ Clean	Cylance	✓ Clean

Build you own miner – Requirements

☑ Coin

- Anonymity
- Profitable
- Easy Development

☑ Stealth

- Avoid simple detection methods
- Easy Variants Creation

□ Distribution

- Minimal effort distribution

Build you own miner – Distribution

- Any regular malware distribution method
- Using phishing mails is probably the simplest
  - Can use docs with Macros, DDE, Exploits, …
  - Links to malicious executables
    - File-sharing sites
    - Hack web-sites
  - …

Build you own miner – Creating Maldocs

- Lots of source on-line to create malicious macros
  - https://gist.github.com/nopslider/0d48760928642ca190ed
  - https://mikemurr.com/vbscript-download-and-execute-file/
  - https://github.com/itm4n/VBA-RunPE
  - …
- DDE attacks are also a good option
  - https://pentestlab.blog/2018/01/16/microsoft-office-dde-attacks/
  - …
- 1-day exploits
  - Equation editor exploits are popular these days

Build you own miner – Requirements

✓ Coin

- Anonymity
- Profitable
- Easy Development

✓ Stealth

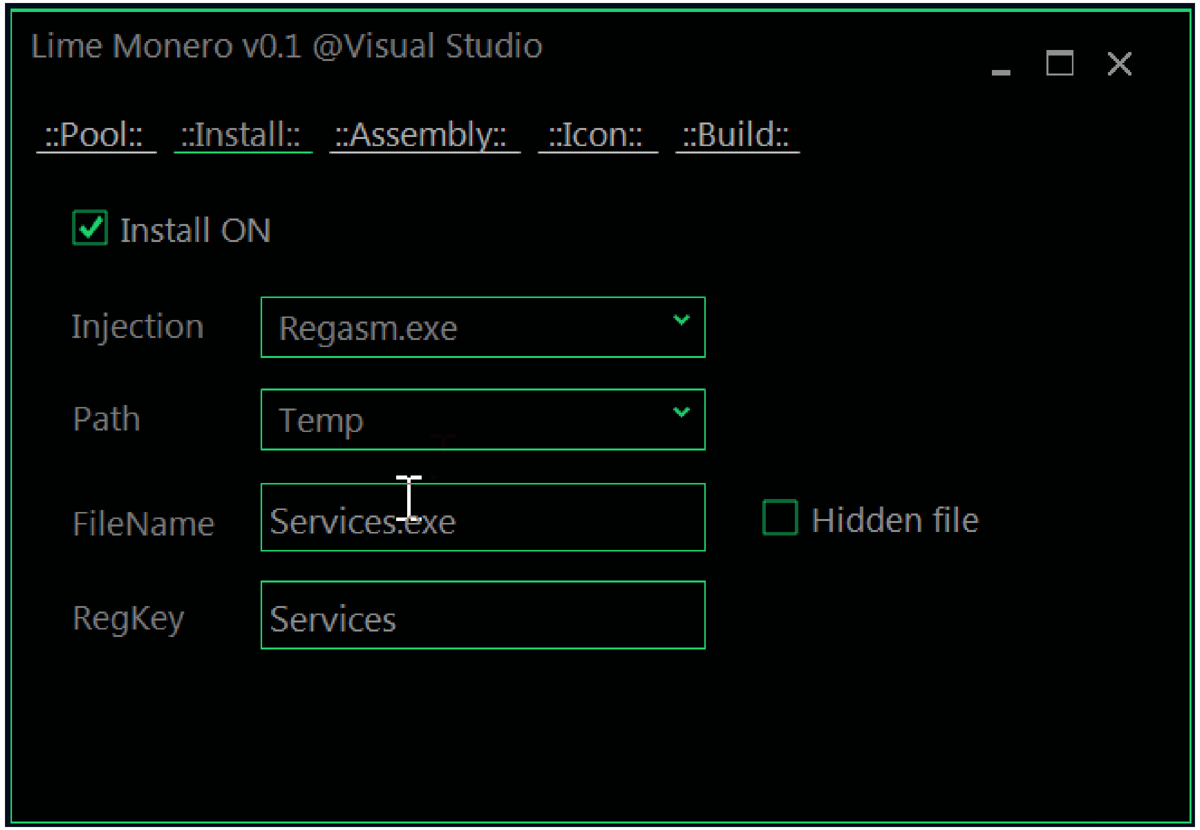
- Avoid simple detection methods
- Easy Variants Creation

✓ Distribution

- Minimal effort distribution

Build you own miner – 0 effort

- There are also open-source miners
- https://github.com/NYAN-x-CAT/Lime-Miner



Lime Monero v0.1 @Visual Studio

☑ Install ON

Injection: Regasm.exe

Path: Temp

FileName: Services.exe

□ Hidden file

RegKey: Services

RSAConference2019

Detection Techniques

Basic Detection Methods

- Monitoring connections to known mining pools
- Use web coin-miners black lists:
  - https://github.com/ZeroDot1/CoinBlockerListsWeb
  - https://github.com/hoshsadiq/adblock-nocoin-list
  - https://v.firebog.net/hosts/static/w3kbl.txt
- Miners IOCs
- CPU Usage statistics
- Looking for XMRIG in memory

Basic Detection Methods - Problems

- Where to look?
  - With tens of thousands of machines it is hard to know where to look
  - Can’t scan memory on every machine…
- URL/IP black lists are less effective in Perimeter less organizations
  - Attackers may use proxies
- IOCs are not effective versus 0-day miners
- Simple CPU usage statistics is False-Positive prone
  - Compilers
  - Hard working servers
  - …

Miner Sweeper – WMI based miner detector

- WMI in a nutshell

  "Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems. You can write WMI scripts or applications to automate administrative tasks on remote computers but WMI also supplies management data to other parts of the operating system and products, for example System Center Operations Manager, formerly Microsoft Operations Manager (MOM), or Windows Remote Management (WinRM)."
  https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmi-start-page

- WMI is a great tool for defenders and attackers:
  - Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asynchronous, and Fileless Backdoor
  - WINDOWS MANAGEMENT INSTRUMENTATION (WMI) OFFENSE, DEFENSE, AND FORENSICS

Miner Sweeper – WMI based miner detector

- WMI queries can provider wealth of information ***remotely***
  - Enumerate AV products
  - Enumerate running processes
  - Enumerate services
  - Check performance counters
  - ...

Checking performance counters ?!?

Miner Sweeper – High level concept

- To be effective Miners must mine
  - CPU statistics must increase significantly
  - No significant mining == No significant ROI for the miner

Al Capone's Empty Vault

- WMI Allows us to remotely collect CPU statistics

Miner Sweeper – High level concept

Agent-less WMI Based remote CPU anomaly detection

1. Periodically retrieve CPU statistics
   - WMI allows machine/process/thread granularity
2. Throw statistics into Big-Data repository for anomaly detection
   - On machines that normally have high CPU do it on process granularity
3. Once we suspect a machine is infected
   - ○ Look for suspicious connections using WMI – known mining pool
   - ○ Home in on specific processes by checking process statistics
   - ○ Run forensics tools to find the culprit – more on this later

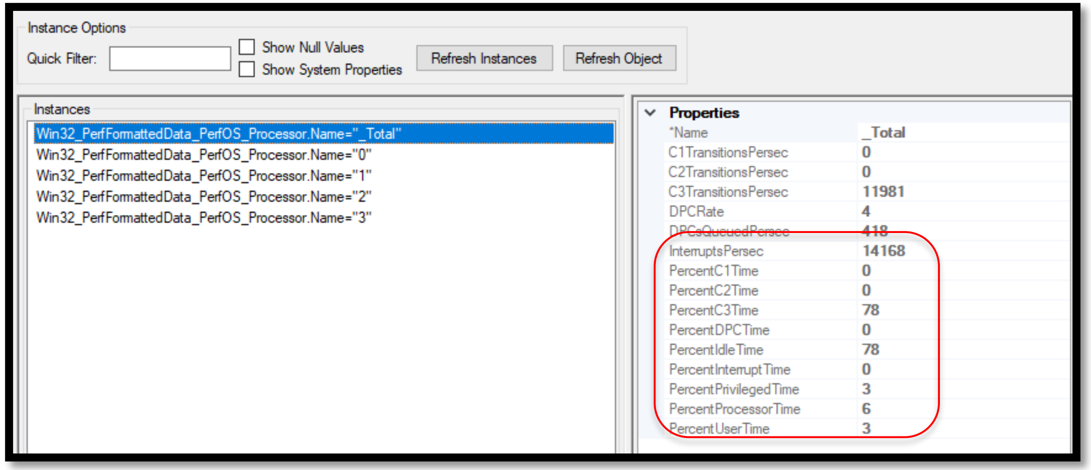
Miner Sweeper – Data Collection

CPU Statistics collection

- Win32_PerfFormattedData_PerfOS_Processor data class
  - Interesting fields – PercentProcessorTime, PercentUserTime, PercentIdleTime
- Win32_PerfFormattedData_PerfProc_Process data class
  - Interesting fields – IDProcess, Name, PercentUserTime, PercentProcessorTime, ElapsedTime
- Win32_PerfFormattedData_PerfProc_Thread
  - Interesting fields – StartAddress, PercentUserTime, PercentProcessorTime, ElapsedTime, IDThread

Miner Sweeper – Data Collection – WMI Explorer

Processor statistics



Instance Options

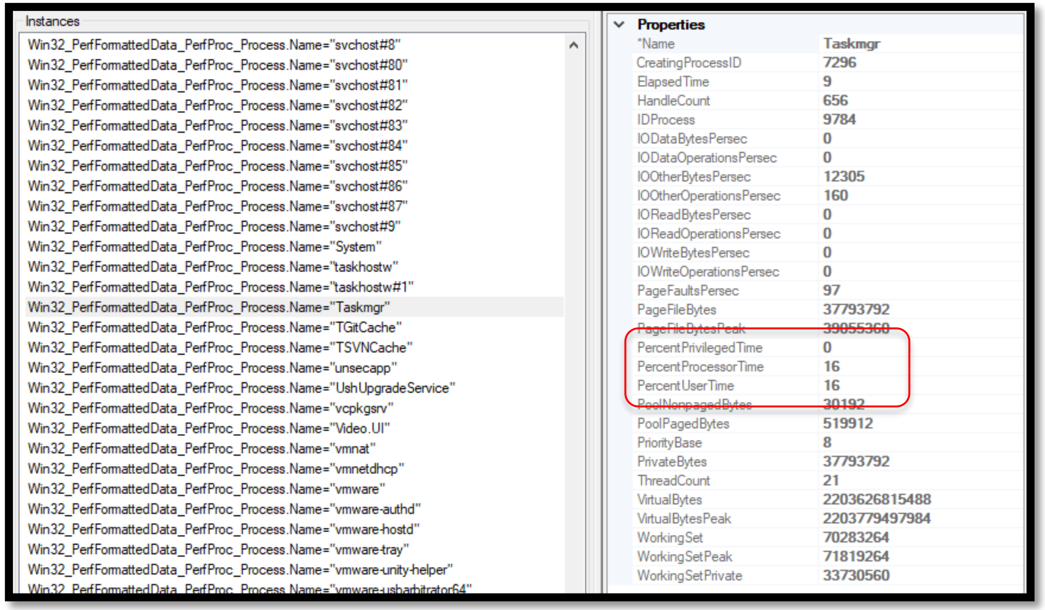
Quick Filter: □ Show Null Values □ Show System Properties

Instances

Win32_PerfFormattedData_PerfOS_Processor.Name="_Total"
Win32_PerfFormattedData_PerfOS_Processor.Name="0"
Win32_PerfFormattedData_PerfOS_Processor.Name="1"
Win32_PerfFormattedData_PerfOS_Processor.Name="2"
Win32_PerfFormattedData_PerfOS_Processor.Name="3"

Properties	
*Name	_Total
C1TransitionsPersec	0
C2TransitionsPersec	0
C3TransitionsPersec	11981
DPCRate	4
DPCsQueuedPersec	418
InterruptsPersec	14168
PercentC1Time	0
PercentC2Time	0
PercentC3Time	78
PercentDPCTime	0
PercentIdleTime	78
PercentInterruptTime	0
PercentPrivilegedTime	3
PercentProcessorTime	6
PercentUserTime	3

Process statistics

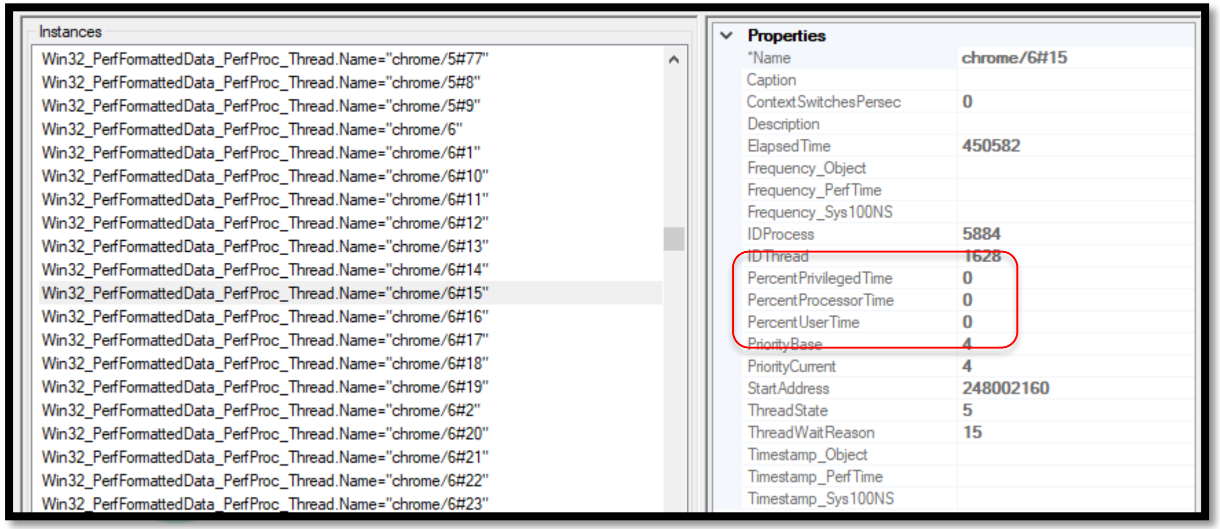


Instances

Win32_PerfFormattedData_PerfProc_Process.Name="svchost#8"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#80"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#81"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#82"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#83"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#84"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#85"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#86"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#87"
Win32_PerfFormattedData_PerfProc_Process.Name="svchost#9"
Win32_PerfFormattedData_PerfProc_Process.Name="System"
Win32_PerfFormattedData_PerfProc_Process.Name="taskhostw"
Win32_PerfFormattedData_PerfProc_Process.Name="taskhostw#1"
Win32_PerfFormattedData_PerfProc_Process.Name="Taskmgr"
Win32_PerfFormattedData_PerfProc_Process.Name="TGitCache"
Win32_PerfFormattedData_PerfProc_Process.Name="TSVNCache"
Win32_PerfFormattedData_PerfProc_Process.Name="unsecapp"
Win32_PerfFormattedData_PerfProc_Process.Name="UshUpgradeService"
Win32_PerfFormattedData_PerfProc_Process.Name="vcpkgsrv"
Win32_PerfFormattedData_PerfProc_Process.Name="Video.UI"
Win32_PerfFormattedData_PerfProc_Process.Name="vmnat"
Win32_PerfFormattedData_PerfProc_Process.Name="vmnetdhcp"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware-authd"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware-hostd"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware-tray"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware-unity-helper"
Win32_PerfFormattedData_PerfProc_Process.Name="vmware-usbarbitrator64"

Properties	
*Name	Taskmgr
CreatingProcessID	7296
ElapsedTime	9
HandleCount	656
IDProcess	9784
IODataBytesPersec	0
IODataOperationsPersec	0
IOOtherBytesPersec	12305
IOOtherOperationsPersec	160
IOReadBytesPersec	0
IOReadOperationsPersec	0
IOWriteBytesPersec	0
IOWriteOperationsPersec	0
PageFaultsPersec	97
PageFileBytes	37793792
PageFileBytesPeak	39055360
PercentPrivilegedTime	0
PercentProcessorTime	16
PercentUserTime	16
PoolNonpagedBytes	30192
PoolPagedBytes	519912
PriorityBase	8
PrivateBytes	37793792
ThreadCount	21
VirtualBytes	2203626815488
VirtualBytesPeak	2203779497984
WorkingSet	70283264
WorkingSetPeak	71819264
WorkingSetPrivate	33730560

Thread statistics



Instances

Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/5#77"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/5#8"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/5#9"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#1"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#10"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#11"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#12"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#13"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#14"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#15"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#16"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#17"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#18"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#19"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#2"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#20"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#21"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#22"
Win32_PerfFormattedData_PerfProc_Thread.Name="chrome/6#23"

Properties	
*Name	chrome/6#15
Caption	
ContextSwitchesPersec	0
Description	
ElapsedTime	450582
Frequency_Object	
Frequency_PerfTime	
Frequency_Sys100NS	
IDProcess	5884
IDThread	1628
PercentPrivilegedTime	0
PercentProcessorTime	0
PercentUserTime	0
PriorityBase	4
PriorityCurrent	4
StartAddress	248002160
ThreadState	5
ThreadWaitReason	15
Timestamp_Object	
Timestamp_PerfTime	
Timestamp_Sys100NS	

Miner Sweeper – Anomaly Detection

For our implementation we used elasticsearch:

- Indexing performance counters is trivial
- Anomaly detection over it is easy
  - https://www.elastic.co/blog/machine-learning-anomaly-scoring-elasticsearch-how-it-works
  - https://www.elastic.co/blog/implementing-a-statistical-anomaly-detector-part-1
  - …

Miner Sweeper – Suspected Device Analysis

1. Find suspicious processes using WMI performance counters
2. For suspicious processes:
   - Scan memory – Implemented simple reflective-PE scanner
   - Send to VT/favorite Sandbox – Implemented VT connector
   - Run favorite forensics tools
   - …
3. Output results

Demo

Takeaways

- Cryptominers offer a better return on the investment of time and resources versus ransomware
- Creating less damage and the decentralized nature of crypto-coins reduces actor's risk which makes it appealing
- One major draw back – effective mining means high CPU which can lead to detection
- Miner Sweeper uses new a novel method leveraging WMI to effectively detect miners across the organization

RSA®Conference2019

Questions?