## blackhať ASIA 2021 May 6-7, 2021 BRIEFINGS

# **Disappeared Coins: Steal** Hashrate in Stratum Secretly

Xin Liu, Rui Chong, Yuanyuan Huang, Yingli Zhang, Qingguo Zhou





# Content

### Mining and Pool

Mining pool

What's the proof of work(PoW)

Introduce the concept of transaction and coinbase in Blockchain

## ()2

### Stratum Protocol

Stratum V2 is rarely used so we still aim at Stratum V1 The features and communication process in Stratum V1

## ()

### Steal Hashrate in Stratum Secretly

A direct job insertion attack model proposed by others before and the reason why the attack failed. Purpose of our attack models Job injection based on set\_extranonce attack model Time segment attack model

### Proof of Concept

Tools and equipment we used for PoC

Shows the execution of attack scripts of the two model through screenshots and videos





# **1 Mining and Pool**

### Minging Pool

It is already difficult for a single independent miner to stably mine a block to obtain revenue, so many miners combine their computing power in the form of cooperative mining to establish a mining pool.

### Assign Jobs

According to the computing ability of miners, each miner is assigned a share target with different difficulty (which is far less than the bitcoin network difficulty)

### **Distribute Profit**

Every miner who joins the mining pool can get profit according to the contribution to the mining pool.

Settlement Strategy PPLNS (Pay Per Last N Shares), PPS (Pay Per Share), PPS+ (Pay Per Shares Plus), FPPS (Full Pay Per Shares)





## **1 Mining and Pool** Proof of Work

Nakamoto consensus:

every miner try to figure out the solution of the Bitcoin puzzle. If someone finds out the solution, the block he mined will be the next block in blockchain after other participants verify that his block is valid.

**Proof of Work** 





## **1 Mining and Pool** Transaction

All transactions need to be verified whether they are valid by *miners*, then the valid transactions are packaged into a block.

And the new block is generated through proof of work(PoW) and added to the blockchain.



Used to deal with the Bitcoin puzzle

List of valid transaction



## **1 Mining and Pool** Transaction

Each block will collect a set of pending transactions in the Bitcoin network. But the first transaction in each block is special, called *coinbase* transaction.

It is used to specify that when the current block is mined through the proof of work, the miner will receive the corresponding block reward (currently 6.25 BTC) and fees.





## **1 Mining and Pool** Coinbase Transaction

The coinbase transaction can be divided into 4 parts: coinbase1, extranonce1, extranonce2, coinbase2

**Coinbase1**: covers the first 5 fields of coinbase transaction and part of the script. Except for the version number, other fields are meaningless for all mining machines, because there is no input party for the coinbase transaction.

Extranonce1: covers a small part of the script in the coinbase transaction.
It is specified by the mining pool and is unique for each connection
between the mining pool and the mining machine.





### coinbase1

### extranonce1

extranonce2

### coinbase2



## **1 Mining and Pool** Coinbase Transaction

The coinbase transaction can be divided into 4 parts: coinbase1, extranonce1, extranonce2, coinbase2

**Extranonce2**: covers a small part of the script in the coinbase transaction, immediately after extranonce1. When miner solves Bitcoin puzzle with proof-of-work, if the *nonce* is exhausted, extranonce2 will be incremented to figure out the puzzle.

Coinbase2: covers the rest of coinbase transaction





### coinbase1

### extranonce1

extranonce2

### coinbase2



The communication between miners and mining pool needs to follow mining protocols, such as Stratum protocol, GetBlockTemplate protocol and GetWork protocol.

Stratum protocol is widely used, and Braiins put forward an upgraded version at the end of 2019, called Stratum V2.

Stratum protocol is based on TCP/IP plaintext transmission protocol, using JSON-RPC data format.











Mining Pool	Stratum V1	Stratum V2
F2Pool	$\checkmark$	×
Poolin	$\checkmark$	×
Btc.com	$\checkmark$	×
AntPool	$\checkmark$	×
SlushPool	$\checkmark$	$\checkmark$

The Stratum V2 has not yet been widely used and we don't have the corresponding mining machine which supports Stratum V2. Mainstream mining machine (e.g. Antminer and Whatsminer) and mining software (e.g. Cgminer and Ccminer) currently do not support Stratum V2.

Since Stratum V2 has not yet been widely popularized, our attack models are only aimed at Stratum V1.

Next, the communication process of Stratum V1 will be introduced in detail.





Step 1.1: First, miner initiates a subscription request to the mining pool to establish a connection through the mining.subscribe method

### mining.subscribe("user agent/version", "extranonce1")

Step 1.2: After receiving the above subscription message, the mining pool will return the subscription\_id, extranonce1 and extranonce2\_size (unit: byte)







Step 2.1: Miners use the *mining.authorize* method to send authorization request to the mining pool

mining.authorize("username", "password")

Step 2.2: mining pool returns true or false to notify miner whether authorization is successful







Step 2.3: After that, the miner will use the mining.extranonce.subscribe method to inform the mining pool that it supports the *mining.set extranonce* method

### mining.extranonce.subscribe()





**Step 3.1**: After successful subscription and authorization, the pool will negotiate the difficulty value with miner through *mining.set\_difficulty* method.

The difficulty needs to be compatible with the computing power of mining machine.

**Step 3.2**: Mining Pool assigns jobs to miner through *mining.notify* method.







### mining.set\_difficulty(difficulty)

mining.notify(Job ID, Hash of previous block, coinbase1, coinbase2, List of merkle branches, version, nBits, nTime, **Clean Jobs**)

- □ Job ID: the id number of job
- □ Hash of previous block: used to build the block header
- coinbase1, coinbase2: two unchangeable parts in coinbase transaction
- □ List of merkle branches: used to build the final merkle root
- □ Version: bitcoin block version
- nBits: the encoded bitcoin network difficulty
- **D** nTime: the current time
- Clean Jobs: if true, it means that the miner needs to stop the current work and execute this new work







Step 4.1: When a miner finds out a result that matches the difficulty that mining pool set, miner use the *mining.submit* method to submit the result, which called *share*.

mining.submit("username", "Job ID", "extraNonce2", "nTime", "nonce")





Step 5.1: using *mining.set\_extranonce* method reset the value of extrance1 and bytes of extraonce2 saved by miner during the subscription phase (step 1.2)



### mining.set\_extranonce("extranonce1", extranonce2\_size)





## 3.1 Why direct job insertion is not feasible

Direct job insertion based on TCP hijacking is not feasible in our situation.

The adversary hijacks the communication between the miner and the normal mining pool, and inserts the job of the malicious mining pool built by the adversary directly into the job flow between the normal mining pool and the miner.



Direct job insertion attack model proposed by others before





## 3.1 Why direct job insertion is not feasible

Miner will save extranonce1 specified by normal mining pool during subscription in Stratum. And extranonce1 is used to construct *coinbase* and calculate the *share*.

The extranonce1 specified by normal pool must be different from the one specified by malicious mining pool.

### extranonce1\_normal != extranonce1\_malicious

So that the *share* calculated by miner based on extranonce1\_normal is different from the one calculated with extranonce1\_malicious





## 3.1 Why direct job insertion is not feasible

Therefore, the *share* belonging to the malicious pool however calculated with extranonce1\_normal will be rejected by the malicious pool in verification for *share* in Stratum.

That's the reason why the attack cannot be successfully implemented.



Direct job insertion attack model proposed by others before





## **3 Steal Hashrate in Stratum Secretly** 3.3 Preconditions of attack

### The purpose of the two man-in-the-middle attacks we proposed is to steal the hashrate of the miners to work for the malicious mining while the miner and the normal mining pool are barely aware of it.

**Key: FIX extranonce1** 

Malicious pool: the bitcoin mining pool built by the adversary Normal pool: the bitcoin mining pools maintained by company





## 3.2 Preconditions of attack

### **Under normal conditions:**

the miner sends subscription and authorization requests to the mining pool.

Once subscription and authorization is successful, the mining pool will allocate work to the miner. When the miner finds out the *share*, it will submit it.









## **3 Steal Hashrate in Stratum Secretly** 3.2 Preconditions of attack

Using man-in-the-middle attack to hijack the communication between miners and mining pools:

The adversary server hijacks the TCP communication between the miner and the mining pool and then maintains the TCP connections with the miner and the mining pools.







### 3.3 Job injection based on set extranonce

The adversary inserts the job from the malicious pool into the job flow of the normal pool.









### 3.3 Job injection based on set extranonce

The adversary establishes a connection with the malicious mining pool, and then listens to the subscription and authorization message of the miner and forwards them to the normal mining pool.









## 3.3 Job injection based on set\_extranonce

After receiving the subscription message, the mining pools will respond to miner with extranonce1 and extranonce2\_size which will be saved by the adversary. What's more, the adversary will save the difficulty and job information sent by the mining pools.





### **#BHASIA @BLACKHATEVENTS**

Malicious Pool



•••

Mine

## 3.3 Job injection based on set\_extranonce

When the miner works for the normal pool for a period of time, the adversary will reset extranonce with extranonce1 and extranonce2\_size of the malicious pool, and construct set difficulty and notify message, and then sends them to miner to make miner work for malicious pool.





### **#BHASIA @BLACKHATEVENTS**

Malicious Pool



## 3.3 Job injection based on set extranonce

Then, the adversary forwards *shares* to malicious pool.

After completing all the above steps, the *mining.set\_extranonce* method will be used again to switch the miner to work for the normal mining pool, and repeat all the above steps.





**bláck hať** ASIA 2021



## Sequence diagram

If attackers only steal 5% of the hashrate, it will be very unobvious. The miners and the pool can hardly find these attacks.

Besides, it has really good performance.



## **3 Steal Hashrate in Stratum Secretly** 3.4 Time segment

The adversary hijacks the TCP communication between the miner and the normal pool, and make it work for two mining pool respectively at different time periods.







blackhat ASIA 2021



## Sequence diagram

This method is based on the reconnection scheme.

At the end of the first time segment, the adversary disconnects from the miner and the normal pool.

In the second time segment, the adversary is waiting for reconnection from the miner. And then, make a new connection to the malicious pool.

The extranoce1 is refreshed.





## **4 Proof of Concept** 4.1 BTCPool

BTCPool is backend system of <u>https://pool.btc.com</u>.

It's an open source project on Github. <u>https://github.com/btccom/btcpool</u>

We built two mining pool to simulate the normal pool and the malicious pool using BTCPool on servers.

OS: Ubuntu 16.04 64 bits





# 4 Proof of Concept 4.1 BTCPool

C wr	hy GitHub? 🗸 Team Enterprise	Explore $\vee$ Marketplace Pricing $\vee$	Search	7 Sign in Sign up	)
🖟 btccom / <b>btcpool</b>				⊙ Watch	73 🖧 Star 526 😵 Fork 359
<> Code (!) Issues 30 % Pull requests 4	) Actions III Projects	Wiki 🕕 Security 🗠 Insights			
		<b>Join GitHul</b> GitHub is home to over 50 million developers w manage projects, and buil Sign u	o today vorking together to host and review code, d software together.	Dismiss	
្រ ma	aster - 24 branches 525 tag uguyifang Merge pull request #466 fro	s n de1acr0ix/ckb-async-await	Go to file	About backend of pool.btc.com	
.ci	ircleci	fixed bsv-1.0.1 dockerfile	11 months ago		
📄 3r	rdparty	[GRIN] fixed cuckarooz29	5 months ago	blockchain mine decred	
cn	make/Modules	tools/kafka_repeater: add libsasl2 as dependency	17 months ago	🛱 Readme	
de de	ocker	sserver: log chain name when finding blocks	7 months ago	ৰ্টুয় MIT License	
do	ocs	Update INSTALL-BTCPool.md	8 months ago		
go	olang	Using golang to implement orphan block monitorin	g script 7 months ago	Releases 25	
in and the second secon	nstall	add docker file for tools/worker_update	6 months ago	Fix #450: jobmaker may not (Latest) on 9 Jun	
pr	rebuild/bytom	Use tokio-compatito drive CKB podebridge	2 years ago	+ 24 releases	
sr.	rc	IGRINI support orin cuckarooz	5 months ago		
te	est	[GRIN] support grin cuckarooz	5 months ago	Packages No packages published	





## **4 Proof of Concept** 4.2 Ceminer

Cominer is a kind of mining software that needs to be installed in miner's machine.

It's an open source software on Github. <u>https://github.com/tpruvot/ccminer/tree/linux</u>

Version: tpruvot linux





# **4 Proof of Concept**

### 4.2 Ccminer









## **4 Proof of Concept** 4.3 GPU

### GeForce RTX 2080 Ti \* 3 (ASIC Miners are SOLD OUT >.<)

		<b>∷~</b> \$ I	nvidia-s	smi							
Wed De	ec 16 10	6:59:3	4 2020								
+	DIA-SMI	440.3	3.01	Driver	Version:	440.	33.01	CUDA Ve	ersio	n: 10.2	-+
GPU   Fan	Name Temp	Perf	Persist Pwr:Usa	tence-M  age/Cap	Bus-Id	Мето	Disp.A ry-Usage	Volat   GPU-L	ile Util	Uncorr. ECC Compute M.	
0   30%	GeFore 32C	ce RTX P8	208 18W ,	On   / 250W	00000000 1M <sup>1</sup>	9:19:0 iB / 1	00.0 Off 11019MiB		0%	N/A Default	
1   0%	GeFore 43C	ce RTX P8	208 1W ,	On   / 260W	00000000 1M <sup>+</sup>	9:1B:0 iB / 1	00.0 Off 11019MiB		0%	N/A Default	
2   31%	GeFore 36C	ce RTX P8	208 20W ,	On   / 250W	0000000 59M	9:68:0 iB / 1	00.0 Off 11016MiB		0%	N/A Default	
+											-+
Proc   GPU	esses: J	PID	Туре	Process	s name					GPU Memory Usage	
2	2	1631 1663	G G	/usr/li /usr/bi	b/xorg/Xo Ln/gnome-	org shell				39MiB 17MiB	

[2020-12-14	09:31:41]	GPU	#1:	Intensity set to :
[2020-12-14	09:31:41]	GPU	#2:	Intensity set to :
[2020-12-14	09:31:41]	GPU	#0:	Intensity set to :
[2020-12-14	09:31:42]	GPU	#1:	Gigabyte RTX 2080
[2020-12-14	09:31:42]	GPU	#0:	Zotac RTX 2080 Ti
[2020-12-14	09:31:42]	GPU	#2:	Zotac RTX 2080 Ti
[2020-12-14	09:31:46]	GPU	#1:	Gigabyte RTX 2080
[2020-12-14	09:31:46]	GPU	#2:	Zotac RTX 2080 Ti
[2020-12-14	09:31:46]	GPU	#0:	Zotac RTX 2080 Ti
[2020-12-14	09:31:50]	GPU	#2:	Zotac RTX 2080 Ti
[2020-12-14	09:31:50]	GPU	#1:	Gigabyte RTX 2080
[2020-12-14	09:31:50]	GPU	#0:	Zotac RTX 2080 Ti
[2020-12-14	09:31:54]	GPU	#1:	Gigabyte RTX 2080
[2020-12-14	09:31:54]	GPU	#0:	Zotac RTX 2080 Ti
[2020-12-14	09:31:54]	GPU	#2:	Zotac RTX 2080 Ti

```
25, 33554432 cuda threads
25, 33554432 cuda threads
25, 33554432 cuda threads
25, 33554432 cuda threads
7 Ti, 1007.25 MH/s
4, 981.97 MH/s
5, 979.54 MH/s
6, 2859.03 MH/s
6, 2855.05 MH/s
6, 2838.45 MH/s
7 Ti, 2841.18 MH/s
6, 2829.64 MH/s
7 Ti, 2561.23 MH/s
6, 2530.67 MH/s
6, 2842.83 MH/s
```



# **4 Proof of Concept**

## 4.4 Job injection based on set extranonce

During job injection based on set extranonce attack, the adversary needs to keep three TCP connections to miner, the normal pool and the malicious pool at the same time. All of the messages between them will be forwarded by adversary.

- □ In the initial stage of the attack, the adversary will save extranonce1 and extranonce2\_size from malicious pool. And the adversary will forward the subscription and authorization message to the normal pool.
- □ Next, the adversary will forward jobs sent by the normal pool to miner and send *shares* submitted by miner to the normal pool.
- After 10 shares being submitted to the normal pool, the adversary constructs fake set\_extranonce message with extranonce1 and extranonce2\_size from malicious pool and send it to miner. And then the adversary inserts the latest difficulty and job of the malicious pool into the job flow, and the miner will complete the job of malicious pool.



**@BLACKHATEVENTS #BHASIA** 



### 4.4 Job injection based on set extranonce

The right half of the image is the output of the attack script.

The left part is the output of the ccminer.

The miner received the job message and difficulty negotiation message hijacked and forwarded by the adversary successfully.

Last login: Thu Dec 17 17:14:19 on ttys003 https://microk8s.io/high-availability L'De' :. ZE o's password: Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86\_64) \* Canonical Livepatch is available for installation. - Reduce system reboots and improve kernel security. Activate at: https://ubuntu.com/livepatch \* Documentation: https://help.ubuntu.com \* Management: 316 packages can be updated. \* Support: 59 updates are security updates. New release '20.04.1 LTS' available. Run 'do-release-upgrade' to upgrade to it. https://microk8s.io/high-availability \*\*\* System restart required \*\*\* \* Canonical Livepatch is available for installation. hte mysice -1 minor/cominer\$ ./ccminer -o stratum+tcp://i/2.iu.z -3 --userpass jack:3 -Ph :~/miner/ccminer\$ ./ccminer -o stratum+tcp://\_\_\_\_\_333 --userpass jack:3 -P -a sha256 -i 25 https://ubuntu.com/livepatch \*\*\* ccminer 2.3.1 for nVidia GPUs by tpruvot@github \*\*\* Built with the nVidia CUDA Toolkit 10.0 64-bits 316 packages can be updated. 59 updates are security updates. Originally based on Christian Buchner and Christian H. project Include some kernels from alexis78, djm34, djEzo, tsiv and krnlx. New release '20.04.1 LTS' available. Run 'do-release-upgrade' to upgrade to it. BTC donation address: 1AJdfCpLWPNoAMDfHF1wD5y8VgKSSTHxPo (tpruvot) \*\*\* System restart required \*\*\* Last login: Thu Dec 17 16:20:43 2020 from 115.155.80.94 [2020-12-17 17:48:17] Starting on stratum+tcp://172.16.20.16:3333 \* Rebuilt URL to: http://172....1.:3333/ ....jl\_\_\_\_\_:~\$ cd lstm\_classfication/ \* Trying 172. 1.1 ... illogoul-1:~/lstm\_classfication\$ source bin/activate \* TCP\_NODELAY set \* Connected to 172. 0.2 .1, (1/2.10.20.10) port 3333 (#0) Connection #A to host 1 [2020-12-17 17:48:17] > {"id": 1, "method": "mining.subscribe", "params": ["ccminer/2.3.1"]} [2020-12-17 17:48:17] NVML GPU monitoring enabled. [2020-12-17 17:48:17] 3 miner threads started, using 'sha256d' algorithm. [2020-12-17 17:48:17] < {"id":1,"result":[[["mining.set\_difficulty","01000006"],["mining.notify", "01000006",8],"error":null} 1000006 [2020-12-17 17:48:17] > {"id": 2, "method": "mining.authorize", "params": ["jack", "3"]} [2020-12-17 17:48:17] < {"id":2,"result":true,"error":null} [2020-12-17 17:48:17] > {"id": 3, "method": "mining.extranonce.subscribe", "params": []} [2020-12-17 17:48:18] < {"id":null,"method":"mining.set\_difficulty","params":[16384]} [2020-12-17 17:48:18] < {"id":null,"method":"mining.notify","params":["0","7e13c2153453397973dc59 000ffffffff2d0388150a044e29db5f726567696f6e312f50726f6a65637420425443506f6f6c2f' 00017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db58700000 0000266a24 21a9edb8ac82c15cf4a2c84710c0f5efa8df563cd7ffb14c6f5cee908b95e1f7302a0100000000" 91fe9d27c6557649aec3ce2cb4cd94fe7765a57e2258e6fc","83ea1a0b03422003df348522b343e1a9bc9ee74eff921 57fab385c850d0ffb","d140c425b156f112b002545a7f82d3d8c686ae1d94c4a4f2643a6495b018899e","80d4fc763 b1c97611ecf6a5333e3a1a2d7c6f454d944bdd8260171378126ac","83047415d3be61b00af1b1fd3bccc780fdb5bbfd 57c1a1c943a7d80bcc53e2","6b9abcf55eabddf4b5faddfb0e476e08d5a460cad12ce265d1a3425ac0d57c98","3282 d9137047eb61daf81693a95b6857d8e939e62dfcaf400c77c2e7eb4c3b","c7af0b0b3ad52a65f02d77d2355b67d9863 426151fd320d56e9c8d6948c782","d54d3c3dea51f4fb251e479a2601f01b3fb8a6d0562c70722296f4d2ef2d043a" 099fe9a21f41e412d4faabc33a5d5429c7b17e5f7794caf2bcc29198ac518f7","5e028ff9ff05a85f962ddfe825d5fb 57c504ee914477fe05a98cb80dd94c291","a4fc39c052ebd597e07cadeff18b2e43ec91dc45c1984c0c0b3e757e8c5b95 "],"20000000","170eb156","5fd31d5e",true]} [2020-12-17 17:48:18] Stratum difficulty set to 16384 [2020-12-17 17:48:18] sha256d block 660872, diff 19157154724710.137 [2020-12-17 17:48:19] GPU #0: Intensity set to 25, 33554432 cuda threads [2020-12-17 17:48:19] GPU #1: Intensity set to 25, 33554432 cuda threads [2020-12-17 17:48:19] GPU #2: Intensity set to 25, 33554432 cuda threads [2020-12-17 17:48:19] GPU #0: Zotac RTX 2080 Ti, 1208.28 MH/s [2020-12-17 17:48:19] GPU #2: Zotac RTX 2080 Ti, 1141.56 MH/s [2020-12-17 17:48:19] GPU #1: Gigabyte RTX 2080 Ti, 1139.11 MH/s



```
https://landscape.canonical.com
               https://ubuntu.com/advantage
* Introducing self-healing high availability clusters in MicroK8s.
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.
  - Reduce system reboots and improve kernel security. Activate at:
(lstm_classfication) _____L-1:~/lstm_classfication$ python3 proxy_11.py
                          ATTACK START
SEND JOB FROM NORMAL_POOL TO MINER
```



### 4.4 Job injection based on set extranonce

After the miner submitted several shares to the normal mining pool, it received the *mining.set\_extranonce* message constructed by the adversary, and it can be seen that the *share* submitted by the miner for the malicious pool was accepted by the malicious pool.

[2020-12-17 18:01:31] accepted: 11/22 (diff 162.740), 5813.20 MH/s boooco 200D ::~/lstm\_classfication [2020-12-17 18:01:31] reject reason: Time too new (lstm\_classfication) \_\_\_\_\_20\_\_\_\_ [2020-12-17 18:01:31] GPU #1: Gigabyte RTX 2080 Ti, 2432.19 MH/s [2020-12-17 18:01:31] GPU #2: Zotac RTX 2080 Ti, 940.18 MH/s [2020-12-17 18:01:32] < {"id":null,"method":"mining.set\_difficulty","params":[64]} [2020-12-17 18:01:35] GPU #1: Gigabyte RTX 2080 Ti, 2413.88 MH/s [2020-12-17 18:01:35] GPU #2: Zotac RTX 2080 Ti, 707.10 MH/s SEND JOB FRO [2020-12-17 18:01:35] GPU #0: Zotac RTX 2080 Ti, 2418.06 MH/s [2020-12-17 18:01:37] < {"id":null,"method":"mining.notify","params":["27","24106a54ae8333c80ffcd9 GOT THE )0000000ffffffff2d0300170a046f2cdb5f726567696f6e312f50726f6a65637420425443506f6f6c2f" ff0140be40250000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db58700000000",[],"20000000 NUMBER "170eb156","5fd69569",false]} [2020-12-17 18:01:39] GPU #0: Zotac RTX 2080 Ti, 2426.19 MH/s GOT THE [2020-12-17 18:01:39] GPU #2: Zotac RTX 2080 Ti, 704.12 MH/s [2020-12-17 18:01:39] GPU #1: Gigabyte RTX 2080 Ti, 2448.14 MH/s NUMBER [2020-12-17 18:01:42] GPU #2: 517 MHz 7707.75 kH/W 117W 88C FAN 61% [2020-12-17 18:01:42] < {"id":null,"method":"mining.set\_difficulty","params":[64]} GOT THE [2020-12-17 18:01:43] GPU #1: Gigabyte RTX 2080 Ti, 2466.09 MH/s [2020-12-17 18:01:43] GPU #0: Zotac RTX 2080 Ti, 2439.83 MH/s NUMBER [2020-12-17 18:01:43] GPU #2: Zotac RTX 2080 Ti, 681.67 MH/s [2020-12-17 18:01:47] GPU #1: Gigabyte RTX 2080 Ti, 2432.29 MH/s GOT THE [2020-12-17 18:01:47] GPU #0: Zotac RTX 2080 Ti, 2425.72 MH/s [2020-12-17 18:01:47] < {"id":null,"method":"mining.notify","params":["27","24106a54ae8333c80ffcd9 NUMBER GOT THE "fffffff0140be40250000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db58700000000",[],"20000000 "170eb156", "5fd69569", false]} NUMBER [2020-12-17 18:01:47] GPU #2: Zotac RTX 2080 Ti, 681.64 MH/s [2020-12-17 18:01:51] GPU #1: Gigabyte RTX 2080 Ti, 2463.50 MH/s GOT THE [2020-12-17 18:01:51] GPU #0: Zotac RTX 2080 Ti, 2425.27 MH/s 2020-12-17 18:01:51] GPU #2: Zotac RTX 2080 Ti. 687.61 MH/s NUMBER [2020-12-17 18:01:51] > {"method": "mining.submit", "params": ["jack", "27", "56000000000000" fd69569", "b390b6f2" GOT THE 2020-12-17 18:01:51] < {"id": null, "method": "mining.set\_extranonce", "params": ["01000006", 2020-12-17 18:01:51] < {"id":11, "result":true, NUMBER 2020-12-17 18:01:51] accepted: 12/23 (diff 71.298), 5729.37 MH/s yes! [2020-12-17 18:01:51] < {"id":11,"result":null,"error":[32,"Time too new",null]} GOT THE [2020–12–17 18:01:51] accepted: 12/24 (diff 71.298), 5729.37 MH/s booooo 2020-12-17 18:01:51] reject reason: Time too new NUMBER [2020-12-17 18:01:55] GPU #1: Gigabyte RTX 2080 Ti, 2429.49 MH/s GOT THE [2020-12-17 18:01:55] GPU #0: Zotac RTX 2080 Ti, 2430.18 MH/s [2020-12-17 18:01:56] GPU #2: Zotac RTX 2080 Ti, 681.85 MH/s NUMBER [2020-12-17 18:01:57] < {"id":null,"method":"mining.notify","params":["28","7e13c2153453397973dc5 e1afc9b7b868aa42b100059a400000000000000000", "020000000100000000000 GOT THE 00000000000000000000000000ffffffff2d0388150a04852cdb5f726567696f6e312f50726f6a65637420425443506f6f6c2f" ,"ffffffff02bec7fb28000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db5870000000000000000266a24 NUMBER aa21a9edb8ac82c15cf4a2c84710c0f5efa8df563cd7ffb14c6f5cee908b95e1f7302a0100000000 ====== 2191fe9d27c6557649aec3ce2cb4cd94fe7765a57e2258e6fc", "83ea1a0b03422003df348522b343e1a9bc9ee74eff921 SEND JOB ERO 7a57fab385c850d0ffb","d140c425b156f112b002545a7f82d3d8c686ae1d94c4a4f2643a6495b018899e","80d4fc763 39b1c97611ecf6a5333e3a1a2d7c6f454d944bdd8260171378126ac", "83047415d3be61b00af1b1fd3bccc780fdb5bbf cf57c1a1c943a7d80bcc53e2", "6b9abcf55eabddf4b5faddfb0e476e08d5a460cad12ce265d1a3425ac0d57 GOT THE 27d9137047eb61daf81693a95b6857d8e939e62dfcaf400c77c2e7eb4c3b", "c7af0b0b3ad52a65f02d77d2355b67d9863 b1426151fd320d56e9c8d6948c782","d54d3c3dea51f4fb251e479a2601f01b3fb8a6d0562c70722296f4d2ef2d043a" NUMBER "2699fe9a21f41e412d4faabc33a5d5429c7b17e5f7794caf2bcc29198ac518f7", "5e028ff9ff05a85f962ddfe825d5fb 967c504ee914477fe05a98cb80dd94c291", "a4fc39c052ebd597e07cadeff18b2e43ec91dc45c1984c0c0b3e757e8c5b9 GOT THE 579"],"20000000","170eb156","5fd31d5e",false]} [2020-12-17 18:01:59] GPU #0: Zotac RTX 2080 Ti, 2436.65 MH/s NUMBER [2020-12-17 18:01:59] GPU #1: Gigabyte RTX 2080 Ti, 2453.64 MH/s \_\_\_\_\_ [2020-12-17 18:02:00] GPU #2: Zotac RTX 2080 Ti, 682.47 MH/s SEND JOB FROM NORMAL\_POOL TO MINER [2020-12-17 18:02:02] < {"id":null,"method":"mining.set\_difficulty","params":[64]} 

<pre>\$ source bin/activate .~/lstm_classfication\$ python3 proxy_11.py</pre>	
ATTACK START	
M NORMAL_POOL TO MINER	-
SHARE FOR NORMAL_POOL	+
OF SHARES : 1	
SHARE FOR NORMAL_POOL	ļ
OF SHARES : 2	
SHARE FOR NORMAL_POOL	ļ
OF SHARES : 3	•
SHARE FOR NORMAL_POOL	
OF SHARES : 4	•
SHARE FOR NORMAL_POOL	
OF SHARES : 5	•
SHARE FOR NORMAL_POOL	
OF SHARES : 6	•
SHARE FOR NORMAL_POOL	
OF SHARES : 7	•
SHARE FOR NORMAL_POOL	
OF SHARES : 8	•
SHARE FOR NORMAL_POOL	
OF SHARES : 9	•
SHARE FOR NORMAL_POOL	
OF SHARES : 10	ł
M SELF_POOL TO MINER	-
	+
SHARE FOR SELF_POOL	+
	+
SHAKE FUR SELF_PUUL	+
UF SHAKES : Z	



### 4.4 Job injection based on set\_extranonce

https://www.youtube.com/watch?v=ZvpdOj6U0vM

<b>&gt;</b> YouTube	搜索
elcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86_64)	https://ubuntu.com/livepatch
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre>	337 packages can be updated. 57 updates are security updates.
* Introducing self-healing high availability clusters in MicroKBs. Simple, hardened, Kubernetes for production, from RaspberryPi to DC.	*** System restart required *** Last login: Sun Mar 21 17:36:15 202  huangyy1900L-1:~\$ widia-smi Sun Mar 21 19:08:40 2021
<pre>https://microk8s.io/high-availability * Canonical Livepatch is available for installation Reduce system reboots and improve kernel security. Activate at: https://ubuntu.com/livepatch</pre>	HVIDIA-SMI 440.33.01 Driver Ve GPU Name Persistence-M B Fan Temp Perf Pwr:Usage/Cap
37 packages can be updated. 7 updates are security updates.	0 GeForce RTX 208 On   0   33% 46C P8 19W / 250W
ew release '20.04.2 LTS' available. un 'do-release-upgrade' to upgrade to it. 	1 GeForce RTX 208 On   0   42% 52C P8 1W / 260W   
Istm_classfication) maj1200DL-1:~/lstm_classfication\$ python3 proxy_self_to_non ATTACK START	rmal.py 36% 56C P8 21M / 256W
SEND JOB FROM NORMEPOOL MINER	Process : GPU PID yps woess 2 1631 G wsr/lib 2 1633 G /wsr/bin/ Huangy1900L-1:-/miner\$ cd ccminer huangy1900L-1:-/miner\$ cd ccminer huangy1900L-1:-/miner\$ccminer\$./C huangy1900L-1:-/miner\$ccminer\$./C sha256 -1 25devices-1,2 *** ccminer 2.3.1 for NVidia GPUs b Built with the nVidia CUDA Tool Originally based on Christian Buc Include some kernels from alexis7 BTC donation address: IAJdfCpLWPNOA [2021-03-21 19:11:41] Starting on s * Rebuilt WL to: http://172.16.20. * Trying 172.16.20.16 * TCP_NOELY set * Connected to 172.16.20.16 (172.16 * Connection #0 to host 172.16.20.1 [2021-03-21 19:11:41] * ("id": 1, " [2021-03-21 19:11:41] Z miner three 8046*1], "01000004", 81, "error";null
▶ ▶  <b>↓</b> 0:01 / 1:38	0004"]],"01000004",8],"error":null} [2021-03-21 19:11:41] > {"id":2, " [2021-02-11 19:11:41] > {"id":2, "

Job injection based on set\_extranonce







## **4 Proof of Concept** 4.5 Time segment

During the time segment attack, the adversary needs to switch the connection to different pools at a fixed time segment. We set the time segment to 10 minutes.

- In the first 10 minutes, the adversary will forward the subscription and authorization message to the normal pool. The miner will only work for the normal pool in the remaining time. At the end of the ten minutes, the adversary will disconnect from the normal pool.
- In the next 10 minutes, the miner will reconnect to the pool, and the adversary will hijack the TCP connection to the malicious pool. The miner will only work for the malicious pool in the remaining time until the time segment ends.



### black hat ASIA 2021

### 4.5 Time segment

The miner received the job message and difficulty negotiation message hijacked and forwarded by the adversary successfully.

Last login: Sun Dec 20 18:04:57 on ttys001 New release '20.04.1 LTS' available. shenqijiadexiaolilideMacBook-Pro:~ nct\$ ssh majl20@172.16.20.16 Run 'do-release-upgrade' to upgrade to it. [maj120@172.16.20.16's password: Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86 64) \*\*\* System restart required \*\*\* [huangyy19@DL-1:~/miner/ccminer\$ ./ccminer -o stratum+tcp://172.16.20.16:3333 --userpass jack:3 -P \* Documentation: https://help.ubuntu.com [huanhuangyy19@DL-1:~/miner/ccminer\$ ./ccminer -o stratum+tcp://172.16.20.16:3333 --userpass jack:3 \* Management: https://landscape.canonical.com \* Support: -P -a sha256 -i 25 https://ubuntu.com/advantage \*\*\* ccminer 2.3.1 for nVidia GPUs by tpruvot@github \*\*\* \* Introducing self-healing high availability clusters in MicroK8s. Built with the nVidia CUDA Toolkit 10.0 64-bits Simple, hardened, Kubernetes for production, from RaspberryPi to DC. Originally based on Christian Buchner and Christian H. project Include some kernels from alexis78, djm34, djEzo, tsiv and krnlx. https://microk8s.io/high-availability BTC donation address: 1AJdfCpLWPNoAMDfHF1wD5y8VgKSSTHxPo (tpruvot) \* Canonical Livepatch is available for installation. - Reduce system reboots and improve kernel security. Activate at: 2020-12-20 18:05:34] Starting on stratum+tcp://172.16.20.16:3333 https://ubuntu.com/livepatch Rebuilt URL to: http://172.16.20.16:3333/ Trying 172.16.20.16... 325 packages can be updated. TCP\_NODELAY set 59 updates are security updates. Connected to 172.16.20.16 (172.16.20.16) port 3333 (#0) Connection #0 to host 172.16.20.16 left intact New release '20.04.1 LTS' available. 2020-12-20 18:05:34] > {"id": 1, "method": "mining.subscribe", "params": ["ccminer/2.3.1"]} Run 'do-release-upgrade' to upgrade to it. 2020-12-20 18:05:34] < {"id":1,"result":[[["mining.set\_difficulty","01000007"],["mining.notify","6 000007"]],"01000007",8],"error":null} \*\*\* System restart required \*\*\* [2020-12-20 18:05:34] > {"id": 2, "method": "mining.authorize", "params": ["jack", "3"]} Last login: Sun Dec 20 15:56:31 2020 from 115.155.66.142 [2020-12-20 18:05:34] NVML GPU monitoring enabled. maj120@DL-1:~\$ cd lstm\_classfication/ [2020-12-20 18:05:34] 3 miner threads started, using 'sha256d' algorithm. majl20@DL-1:~/lstm\_classfication\$ source bin/activate [2020-12-20 18:05:34] < {"id":2,"result":true,"error":null} (lstm classfication) maj1200DL-1:~/lstm\_classfication\$ python3 time finish.py [2020-12-20 18:05:34] > {"id": 3, "method": "mining.extranonce.subscribe", "params": []} 2020-12-20 18:05:35] < {"id":null,"method":"mining.set\_difficulty","params":[16384]} STRAT TO WORK FOR NORMAL POOL [2020-12-20 18:05:35] < {"id":null,"method":"mining.notify","params":["0","c3625bf105f1a760dc4179cb 00000000ffffffff2d036d190a04e121df5f726567696f6e312f50726f6a65637420425443506f6f6c2f","ff TEN MINUTES PASSED ffff02d5324d2e0000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db58700000000000000000266a24aa21a ed27f4a00f9453d307b963558a52895c58937641dce59e8b040d0ccc68dc4102bd00000000",["27c68af4bbcf94a7c52f 20cefed99118840b397655afb7b0d3f5a4fbdc0a2ab", "2b0a0e3e8bf5b9adb3c6cf2b0446cc848858f7a729eb27a3a7d8 STRAT TO WORK FOR MALICIOUS POOL 6b2262a1e9f", "a97b57f5f09f84c5c49c8500a37fd348191df57b54f095b9c4ac9e051ae14727", "aa1d803966b3214f2 451a2bf9eebc784191552805b57059ecef85776832117b", "da1c257dbc31fece3c87956b10505f9fd2f264a45f7d75957 2d45de4f14c6e5","918fbdf6840ae2e0e3a0c0ec0c7c106244f8632fe9ef9e005399048d1402cec0","c3e87179a655a0 b98940d5c6e0edd7957c476c027d9aa0715522f747b7b5724","dbda7bfa02b635e5e6392e2d01f8fd23fec75e70668242 a388a4a072213ff69","ca1a4cd4cbda824fe1d1ef56a8fce864f70131f9111bbd6f60a029665c9814d6","ab716be1b3c c10e242b998c4ca8d766f58b023dd5caf354861fd2621779436c","e2ac2151c29a37c71f88170cb7d03ca6d8446748aa3 cb5a81e27e9d39ad4988","5cb81f104123c3fa1b73d69c18886678f6b310c5f9c8806242c25dd9166a5f37"],"2000000 ."170f1372","5fdc73dc",true]} [2020-12-20 18:05:35] Stratum difficulty set to 16384 [2020-12-20 18:05:35] sha256d block 661869, diff 18670168558399.586 [2020-12-20 18:05:36] GPU #0: Intensity set to 25, 33554432 cuda threads [2020-12-20 18:05:36] GPU #2: Intensity set to 25, 33554432 cuda threads [2020-12-20 18:05:36] GPU #1: Intensity set to 25, 33554432 cuda threads [2020-12-20 18:05:37] GPU #0: Zotac RTX 2080 Ti, 1073.64 MH/s [2020-12-20 18:05:37] GPU #2: Zotac RTX 2080 Ti, 1041.37 MH/s [2020-12-20 18:05:37] GPU #1: Gigabyte RTX 2080 Ti, 1029.75 MH/s [2020-12-20 18:05:41] GPU #0: Zotac RTX 2080 Ti, 2826.53 MH/s [2020-12-20 18:05:41] GPU #1: Gigabyte RTX 2080 Ti, 2823.21 MH/s [2020-12-20 18:05:41] GPU #2: Zotac RTX 2080 Ti, 2651.19 MH/s [2020-12-20 18:05:45] GPU #0: Zotac RTX 2080 Ti, 2808.94 MH/s [2020-12-20 18:05:45] GPU #2: Zotac RTX 2080 Ti, 2626.82 MH/s [2020-12-20 18:05:45] GPU #1: Gigabyte RTX 2080 Ti, 2779.41 MH/s [2020-12-20 18:05:49] GPU #2: Zotac RTX 2080 Ti, 2568.34 MH/s [2020-12-20 18:05:49] GPU #0: Zotac RTX 2080 Ti, 2790.49 MH/s [2020-12-20 18:05:49] GPU #1: Gigabyte RTX 2080 Ti, 2790.82 MH/s [2020-12-20 18:05:53] GPU #1: Gigabyte RTX 2080 Ti, 2755.12 MH/s





## 4.5 Time segment

The adversary successfully

forwarded the *shares* submitted by

the miner to the normal mining

pool.

c8c10e242b998c4ca8d766f58b023dd5caf354861fd2621779436c","e2ac2151c29a37c71f88170cb7d03ca6d8446748aa 🗏 Last login: Sun Dec 20 18:04:57 on ttys001 37cb5a81e27e9d39ad4988", "5cb81f104123c3fa1b73d69c18886678f6b310c5f9c8806242c25dd9166a5f37"], "200000 shenqijiadexiaolilideMacBook-Pro:~ nct\$ ssh majl20@172.16.20.16 00"."170f1372","5fdc73dc",false]} maj1200172.16.20.16's password: [2020-12-20 18:11:57] GPU #0: Zotac RTX 2080 Ti, 2429.15 MH/s Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86\_64) [2020-12-20 18:11:57] GPU #1: Gigabyte RTX 2080 Ti, 2497.16 MH/s [2020-12-20 18:11:59] GPU #2: Zotac RTX 2080 Ti, 1007.52 MH/s \* Documentation: https://help.ubuntu.com [2020-12-20 18:12:01] GPU #0: Zotac RTX 2080 Ti, 2419.58 MH/s \* Management: https://landscape.canonical.com [2020-12-20 18:12:01] GPU #1: Gigabyte RTX 2080 Ti, 2510.13 MH/s \* Support: https://ubuntu.com/advantage 2020-12-20 18:12:03] GPU #2: Zotac RTX 2080 Ti. 1006.68 MH/s [2020-12-20 18:12:04] > {"method": "mining.submit", "params": ["jack", "13", "200000000000000", \* Introducing self-healing high availability clusters in MicroK8s. dc73dc", "616dc14d"], "id":10} Simple, hardened, Kubernetes for production, from RaspberryPi to DC. 2020-12-20 18:12:04] < {"id":10,"result":true,"error":null} [2020-12-20 18:12:04] accepted: 4/4 (diff 64.538), 5921.71 MH/s yes! https://microk8s.io/high-availability 2020-12-20 18:12:05] GPU #1: Gigabyte RTX 2080 Ti, 2525.02 MH/s 2020-12-20 18:12:05] GPU #0: Zotac RTX 2080 Ti, 2425.88 MH/s \* Canonical Livepatch is available for installation. 2020-12-20 18:12:06] > {"method": "mining.submit", "params": ["jack", "13", "260000000000000", "5 - Reduce system reboots and improve kernel security. Activate at: dc73dc", "f9a3d611"], "id":11} https://ubuntu.com/livepatch 2020-12-20 18:12:06] < {"id":11,"result":true,"error":null} 2020-12-20 18:12:06] accepted: 5/5 (diff 108.894), 5922.53 MH/s yes! 325 packages can be updated. 2020-12-20 18:12:08] GPU #2: Zotac RTX 2080 Ti, 1009.53 MH/s 59 updates are security updates. 2020-12-20 18:12:09] GPU #1: Gigabyte RTX 2080 Ti, 2500.26 MH/s 2020-12-20 18:12:09] GPU #0: Zotac RTX 2080 Ti, 2415.32 MH/s New release '20.04.1 LTS' available. 2020-12-20 18:12:12] GPU #2: Zotac RTX 2080 Ti, 1008.21 MH/s Run 'do-release-upgrade' to upgrade to it. 2020-12-20 18:12:13] GPU #0: Zotac RTX 2080 Ti, 2426.38 MH/s [2020-12-20 18:12:13] GPU #1: Gigabyte RTX 2080 Ti, 2493.01 MH/s \*\*\* System restart required \*\*\* 2020-12-20 18:12:16] GPU #2: Zotac RTX 2080 Ti, 1006.54 MH/s Last login: Sun Dec 20 15:56:31 2020 from 115.155.66.142 2020-12-20 18:12:17] GPU #0: Zotac RTX 2080 Ti, 2415.21 MH/s [maj120@DL-1:~\$ cd lstm\_classfication/ 2020-12-20 18:12:17] GPU #1: Gigabyte RTX 2080 Ti, 2525.26 MH/s [maj120@DL-1:~/lstm\_classfication\$ source bin/activate 2020-12-20 18:12:20] > {"method<sup>"</sup>: "mining.submit", "params": ["jack", "13", "620000000000000", " [(lstm\_classfication) majl20@DL-1:~/lstm\_classfication\$ python3 time\_finish.py dc73dc", "91a3d058"], "id":12} STRAT TO WORK FOR NORMAL POOL 2020-12-20 18:12:20] < {"id":12,"result":true,"error":null} [2020-12-20 18:12:20] accepted: 6/6 (diff 71.134), 5934.60 MH/s yes! 2020-12-20 18:12:20] GPU #2: ZOTAC RIX 2080 11, 1006.19 MH/s [2020-12-20 18:12:21] GPU #1: Gigabyte RTX 2080 Ti, 2522.46 MH/s TEN MINUTES PASSED [2020-12-20 18:12:21] GPU #0: Zotac RTX 2080 Ti, 2423.98 MH/s [2020-12-20 18:12:25] GPU #2: Zotac RTX 2080 Ti, 1007.23 MH/s [2020-12-20 18:12:25] GPU #1: Gigabyte RTX 2080 Ti, 2499.49 MH/s STRAT TO WORK FOR MALICIOUS POOL [2020-12-20 18:12:25] GPU #0: Zotac RTX 2080 Ti, 2428.29 MH/s [2020-12-20 18:12:26] < {"id":null,"method":"mining.notify","params":["14","c3625bf105f1a760dc4179c 0000000000000000ffffffff2d036d190a048623df5f726567696f6e312f50726f6a65637420425443506f6f6c2f"," fffffff02d5324d2e0000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db5870000000000000000266a24aa21 a9ed27f4a00f9453d307b963558a52895c58937641dce59e8b040d0ccc68dc4102bd00000000",["27c68af4bbcf94a7c52 f420 cefed 99118840 b397655 af b7b0d3 f5a4 fbdc0 a2 ab", "2b0a0 e3e8 bf5b9 ad b3c6 cf2b0446 cc848858 f7a729 eb27a3 a7d b3c6 cf2b0446 cc848858 f7a728 ab27a3 a7d b3c6 cf2b0446 cc848858 f7a728 ab27a3 ab27866b2262a1e9f", "a97b57f5f09f84c5c49c8500a37fd348191df57b54f095b9c4ac9e051ae14727", "aa1d803966b3214f 23451a2bf9eebc784191552805b57059ecef85776832117b", "da1c257dbc31fece3c87956b10505f9fd2f264a45f7d7595 742d45de4f14c6e5", "918fbdf6840ae2e0e3a0c0ec0c7c106244f8632fe9ef9e005399048d1402cec0", "c3e87179a655a 00b98940d5c6e0edd7957c476c027d9aa0715522f747b7b5724", "dbda7bfa02b635e5e6392e2d01f8fd23fec75e7066824 2da388a4a072213ff69", "ca1a4cd4cbda824fe1d1ef56a8fce864f70131f9111bbd6f60a029665c9814d6", "ab716be1b3 c8c10e242b998c4ca8d766f58b023dd5caf354861fd2621779436c", "e2ac2151c29a37c71f88170cb7d03ca6d8446748aa 37cb5a81e27e9d39ad4988", "5cb81f104123c3fa1b73d69c18886678f6b310c5f9c8806242c25dd9166a5f37"], "200000 00","170f1372","5fdc73dc",false]} [2020-12-20 18:12:29] GPU #0: Zotac RTX 2080 Ti, 2409.62 MH/s [2020-12-20 18:12:29] GPU #1: Gigabyte RTX 2080 Ti, 2502.63 MH/s [2020-12-20 18:12:29] GPU #2: Zotac RTX 2080 Ti, 1003.10 MH/s [2020-12-20 18:12:33] GPU #0: Zotac RTX 2080 Ti, 2429.10 MH/s [2020-12-20 18:12:33] GPU #1: Gigabyte RTX 2080 Ti, 2497.83 MH/s [2020-12-20 18:12:33] GPU #2: Zotac RTX 2080 Ti, 1004.05 MH/s [2020-12-20 18:12:37] GPU #1: Gigabyte RTX 2080 Ti, 2502.19 MH/s [2020-12-20 18:12:37] GPU #0: Zotac RTX 2080 Ti, 2422.44 MH/s [2020-12-20 18:12:38] GPU #2: Zotac RTX 2080 Ti, 1007.34 MH/s [2020-12-20 18:12:41] GPU #1: Gigabyte RTX 2080 Ti, 2526.08 MH/s [2020-12-20 18:12:41] GPU #0: Zotac RTX 2080 Ti, 2416.28 MH/s





## 4.5 Time segment

At the end of the first 10 minutes, the Stratum connection interrupted because the adversary disconnect from the miner and the normal pool.

And then the miner reconnect to the pool, and the adversary hijacks the connection to the malicious pool.

[2020-12-20 18:20:37] GPU #0: Zotac RTX 2080 Ti, 2414.51 MH/s Last login: Sun Dec 20 18:04:57 on ttys001 [2020-12-20 18:20:39] GPU #2: Zotac RTX 2080 Ti, 948.30 MH/s shenqijiadexiaolilideMacBook-Pro:~ nct\$ ssh maj120@172.16.20.16 [2020-12-20 18:20:41] GPU #0: Zotac RTX 2080 Ti, 2421.65 MH/s mail200172.16.20.16's password: [2020-12-20 18:20:41] GPU #1: Gigabyte RTX 2080 Ti, 2415.07 MH/s Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86\_64) [2020-12-20 18:20:43] GPU #2: Zotac RTX 2080 Ti, 935.79 MH/s [2020-12-20 18:20:45] GPU #1: 1481 MHz 12.10 MH/W 200W 86C FAN 98% \* Documentation: https://help.ubuntu.com [2020-12-20 18:20:45] GPU #0: Zotac RTX 2080 Ti, 2416.53 MH/s \* Management: [2020-12-20 18:20:45] GPU #1: Gigabyte RTX 2080 Ti, 2435.25 MH/s \* Support: https://ubuntu.com/advantage [2020-12-20 18:20:47] GPU #2: Zotac RTX 2080 Ti, 934.86 MH/s [2020-12-20 18:20:49] GPU #1: Gigabyte RTX 2080 Ti, 2422.72 MH/s [2020-12-20 18:20:49] GPU #0: Zotac RTX 2080 Ti, 2416.83 MH/s [2020-12-20 18:20:52] GPU #2: Zotac RTX 2080 Ti, 940.06 MH/s [2020-12-20 18:20:53] GPU #1: Gigabyte RTX 2080 Ti, 2404.63 MH/s https://microk8s.io/high-availability [2020-12-20 18:20:53] GPU #0: Zotac RTX 2080 Ti, 2409.76 MH/s 2020-12-20 18:20:561 GPU #2: Zotac RTX 2080 Ti. 936.73 MH/s Canonical Livepatch is available for installation. 2020-12-20 18:20:56] Stratum connection interro Rebuilt URL to: http://172.16.20.16:3333/ https://ubuntu.com/livepatch Trying 172.16.20.16... TCP\_NODELAY set 325 packages can be updated. Connected to 172.16.20.16 (172.16.20.16) port 3333 (#0) 59 updates are security updates. Connection #0 to host 172.16.20.16 left intact 2020-12-20 18:20:56] > {"id": 1, "method": "mining.subscribe", "params": ["ccminer/2.3.1", "010000 New release '20.04.1 LTS' available. Run 'do-release-upgrade' to upgrade to it. 2020-12-20 18:20:56] < {"id":1,"result":[[["mining.set\_difficulty","0100002e"],["mining.notify","0 ,"0100002e",8],"error":null} \*\*\* System restart required \*\*\* 00002e" 2020-12-20 18:20:56] > {"id": 2, "method": "mining.authorize", "params": ["jack", "3"]} Last login: Sun Dec 20 15:56:31 2020 from 115.155.66.142 2020-12-20 18:20:56] < {"id":2,"result":true,"error":null} maj120@DL-1:~\$ cd lstm\_classfication/ [2020-12-20 18:20:56] > {"id": 3, "method": "mining.extranonce.subscribe", "params": []} majl20@DL-1:~/lstm\_classfication\$ source bin/activate 2020-12-20 18:20:57] < {"id":null,"method":"mining.set\_difficulty","params":[16384]} 2020-12-20 18:20:57] < {"id":null,"method":"mining.notify","params":["0","08966f1329a827384bf463e0 00000000fffffffff2d0369190a048525df5f726567696f6e312f50726f6a65637420425443506f6f6c2f","ff fff028cf0e32a0000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db58700000000000000000266a24aa21a d512522b362407f8894a0c4e4e02682501b91638e4f54cbe2345a50cf9f85f14500000000".["fb98974dc1672d6367e9 893e7eaa835a60778ebfd3c64748f98098e72ec4466","642e2a98cfd974df8b3b0304e1c87bb00b3d473683a1d0075231 92a69b8ef4", "b2b0e842896748f5b994eac84249ca564a96bc8b881097f35a6b07eabc1a2584", "54430b8bfd6d830ca 9286a1f5c6fbaf4b2b752276176c3af6f041fe960ca32", "913a7f9e79c5bf5966215c5877d176d2e0f678942bc31dea4 2157e80099e4f", "41ded323384322b68c7c8ba27330c80fdde0cb31b6beb54416f9b51cdfb0e84b", "62a615752be4e7 4cd9b92d15afdfda3b05bd4eeaae01f2fee","3ae9607820045fd5022213b216b74d63d19f665e4a23f0 e3db545f5","caedd5a227cf9f61ae762fa5a3002ad36aece58561196a4a4b5e2f76a2f7d1d0","e51becf0604 176a0799f607d55588197aa71b5c6c0688dbcba69f6f6e0dba15","86595604199719622d005d2c9039bd1beb11641694e 396af07e72eb3ff1613","ed17401a126036590d29a3ef7c5db74a172d1bc3749cfa1569c3fcea231bc2a4"],"2000000 "5fdc69ce",true]} 2020-12-20 18:20:57] Stratum difficulty set to 1638 [2020-12-20 18:20:57] sha256d block 661865, diff 18670168558399.586 [2020-12-20 18:20:59] GPU #0: Zotac RTX 2080 Ti, 2648.35 MH/s [2020-12-20 18:20:59] GPU #1: Gigabyte RTX 2080 Ti, 2505.89 MH/s [2020-12-20 18:21:00] GPU #2: Zotac RTX 2080 Ti, 1088.54 MH/s [2020-12-20 18:21:02] < {"id":null,"method":"mining.notify","params":["1","08966f1329a827384bf463e0 00000ffffffff2d0369190a048525df5f726567696f6e312f50726f6a65637420425443506f6f6c2f"."f ffffff028cf0e32a0000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db5870000000000000000266a24aa21a 9ed512522b362407f8894a0c4e4e02682501b91638e4f54cbe2345a50cf9f85f14500000000".["fb98974dc1672d6367e9 f893e7eaa835a60778ebfd3c64748f98098e72ec4466","642e2a98cfd974df8b3b0304e1c87bb00b3d473683a1d0075231 de92a69b8ef4", "b2b0e842896748f5b994eac84249ca564a96bc8b881097f35a6b07eabc1a2584", "54430b8bfd6d830ca 819286a1f5c6fbaf4b2b752276176c3af6f041fe960ca32", "913a7f9e79c5bf5966215c5877d176d2e0f678942bc31dea4 e22157e80099e4f","41ded323384322b68c7c8ba27330c80fdde0cb31b6beb54416f9b51cdfb0e84b","62a615752be4e7 e4a75d7d94f5bb54cd9b92d15afdfda3b05bd4eeaae01f2fee", "3ae9607820045fd5022213b216b74d63d19f665e4a23f0 da47186d6e3db545f5","caedd5a227cf9f61ae762fa5a3002ad36aece58561196a4a4b5e2f76a2f7d1d0","e51becf0604 da76a0799f607d55588197aa71b5c6c0688dbcba69f6f6e0dba15","86595604199719622d005d2c9039bd1beb11641694e 79396af07e72eb3ff1613", "ed17401a126036590d29a3ef7c5db74a172d1bc3749cfa1569c3fcea231bc2a4"], "2000000 0","170f1372","5fdc69ce",false]} [2020-12-20 18:21:03] GPU #0: Zotac RTX 2080 Ti, 2474.31 MH/s



https://landscape.canonical.com

\* Introducing self-healing high availability clusters in MicroK8s. Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

- Reduce system reboots and improve kernel security. Activate at:

TEN MINUTES PASSED

TEN MINUTES PASSED

### (lstm\_classfication) maj1200DL-1:~/lstm\_classfication\$ python3 time\_finish.py STRAT TO WORK FOR NORMAL POOL STRAT TO WORK FOR MALICIOUS POOL \_\_\_\_\_ STRAT TO WORK FOR NORMAL POOL

### blackhat ASIA 2021

## 4.5 Time segment

The malicious pool has received and accepted the *share* submitted by the miner.

As the second ten minutes ends, the adversary disconnects from the miner and the malicious pool, and will be waiting for the reconnection of miner.

a9ed512522b362407f8894a0c4e4e02682501b91638e4f54cbe2345a50cf9f85f14500000000",["fb98974dc1672d6367e 🔳 Last login: Sun Dec 20 18:04:57 on ttys001 9f893e7eaa835a60778ebfd3c64748f98098e72ec4466", "642e2a98cfd974df8b3b0304e1c87bb00b3d473683a1d007523 shengijiadexiaolilideMacBook-Pro:~ nct\$ ssh maj1200172.16.20.16 1de92a69b8ef4", "b2b0e842896748f5b994eac84249ca564a96bc8b881097f35a6b07eabc1a2584", "54430b8bfd6d830c maj120@172.16.20.16's password: a819286a1f5c6fbaf4b2b752276176c3af6f041fe960ca32","913a7f9e79c5bf5966215c5877d176d2e0f678942bc31dea Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86\_64) 4e22157e80099e4f", "41ded323384322b68c7c8ba27330c80fdde0cb31b6beb54416f9b51cdfb0e84b", "62a615752be4e 7e4a75d7d94f5bb54cd9b92d15afdfda3b05bd4eeaae01f2fee","3ae9607820045fd5022213b216b74d63d19f665e4a23f \* Documentation: https://help.ubuntu.com 0da47186d6e3db545f5","caedd5a227cf9f61ae762fa5a3002ad36aece58561196a4a4b5e2f76a2f7d1d0","e51becf060 \* Management: https://landscape.canonical.com 4da76a0799f607d55588197aa71b5c6c0688dbcba69f6f6e0dba15", "86595604199719622d005d2c9039bd1beb11641694 \* Support: https://ubuntu.com/advantage e79396af07e72eb3ff1613", "ed17401a126036590d29a3ef7c5db74a172d1bc3749cfa1569c3fcea231bc2a4"], "200000 00","170f1372","5fdc69ce",false]} \* Introducing self-healing high availability clusters in MicroK8s. [2020-12-20 18:25:32] Stratum difficulty set to 64 [2020-12-20 18:25:35] GPU #0: Zotac RTX 2080 Ti, 2434.52 MH/s [2020-12-20 18:25:35] GPU #1: Gigabyte RTX 2080 Ti, 2488.09 MH/s https://microk8s.io/high-availability [2020-12-20 18:25:35] GPU #2: Zotac RTX 2080 Ti, 911.10 MH/s [2020-12-20 18:25:37] > {"method": "mining.submit", "params": ["jack", "10", "130000000000000", "5 Canonical Livepatch is available for installation. dc69ce", "f9093451"], "id":10} - Reduce system reboots and improve kernel security. Activate at: 2020-12-20 18:25:37] < {"id":10,"result":true,"error":null} https://ubuntu.com/livepatch [2020-12-20 18:25:37] accepted: 8/8 (diff 2348.196), 5806.93 MH/s yes! [2020-12-20 18:25:39] GPU #0: Zotac RTX 2080 Ti, 2440.88 MH/s 325 packages can be updated. 2020-12-20 18:25:39] GPU #1: Gigabyte RTX 2080 Ti, 2512.05 MH/s 59 updates are security updates. [2020-12-20 18:25:39] > {"method": "mining.submit", "params": ["jack", "10", "1c00000000000000", "5 dc69ce", "bfc04025"], "id":11} New release '20.04.1 LTS' available. [2020-12-20 18:25:39] < {"id":11,"result":true,"error":null} [2020-12-20 18:25:39] accepted: 9/9 (diff 112.260), 5804.80 Run 'do-release-upgrade' to upgrade to it. [2020-12-20 18:25:40] GPU #2: Zotac RTX 2080 Ti, 909.83 MH/s \*\*\* System restart required \*\*\* [2020-12-20 18:25:43] GPU #1: Gigabyte RTX 2080 Ti, 2484.80 MH/s Last login: Sun Dec 20 15:56:31 2020 from 115.155.66.142 [2020-12-20 18:25:43] GPU #0: Zotac RTX 2080 Ti, 2440.06 MH/s [maj120@DL-1:~\$ cd lstm\_classfication/ [2020-12-20 18:25:45] GPU #2: Zotac RTX 2080 Ti, 908.63 MH/s [maj120@DL-1:~/lstm\_classfication\$ source bin/ [2020-12-20 18:25:47] GPU #1: Gigabyte RTX 2080 Ti, 2473.93 MH/s (lstm\_classfication) maj120@DL-1:~/lstm\_class [2020-12-20 18:25:47] GPU #0: Zotac RTX 2080 Ti, 2433.20 MH/s [2020-12-20 18:25:49] GPU #2: Zotac RTX 2080 Ti, 911.58 MH/s STRAT TO WORK FOR NORMAL [2020-12-20 18:25:51] GPU #0: Zotac RTX 2080 Ti, 2433.07 MH/s [2020-12-20 18:25:51] GPU #1: Gigabyte RTX 2080 Ti, 2480.92 MH/s [2020-12-20 18:25:53] GPU #2: Zotac RTX 2080 Ti, 910.91 MH/s [2020-12-20 18:25:55] GPU #0: Zotac RTX 2080 Ti, 2433.00 MH/s [2020-12-20 18:25:55] GPU #1: Gigabyte RTX 2080 Ti, 2473.60 MH/s [2020-12-20 18:25:57] GPU #2: Zotac RTX 2080 Ti, 928.97 MH/s STRAT TO WORK FOR MALICIO [2020-12-20 18:25:59] GPU #0: Zotac RTX 2080 Ti, 2451.92 MH/s [2020-12-20 18:25:59] GPU #1: Gigabyte RTX 2080 Ti, 2513.96 MH/s [2020-12-20 18:25:59] > {"method": "mining.submit", "params": ["jack", "10", "6c000000000000", "5 fdc69ce", "0a56c88f"], "id":12} [2020-12-20 18:25:59] < {"id":12,"result":true,"error":null}
[2020-12-20 18:25:59] accepted: 10/10 (diff 85.405), 5847.19 MH/s yes!</pre> \_\_\_\_\_ STRAT TO WORK FOR NORMAL [2020-12-20 18:26:02] GPU #2: Zotac RTX 2080 Ti, 908.35 MH/s [2020-12-20 18:26:02] < {"id":null,"method":"mining.notify","params":["11","08966f1329a827384bf463e fffffff028cf0e32a0000000017a9143edc44cdf9bbf7d5e722345d5bd576de5be72db5870000000000000000266a24aa21 a9ed512522b362407f8894a0c4e4e02682501b91638e4f54cbe2345a50cf9f85f14500000000",["fb98974dc1672d6367e 9f893e7eaa835a60778ebfd3c64748f98098e72ec4466", "642e2a98cfd974df8b3b0304e1c87bb00b3d473683a1d007523 1de92a69b8ef4", "b2b0e842896748f5b994eac84249ca564a96bc8b881097f35a6b07eabc1a2584", "54430b8bfd6d830c a819286a1f5c6fbaf4b2b752276176c3af6f041fe960ca32", "913a7f9e79c5bf5966215c5877d176d2e0f678942bc31dea 4e22157e80099e4f","41ded323384322b68c7c8ba27330c80fdde0cb31b6beb54416f9b51cdfb0e84b","62a615752be4e 7e4a75d7d94f5bb54cd9b92d15afdfda3b05bd4eeaae01f2fee", "3ae9607820045fd5022213b216b74d63d19f665e4a23f 0da47186d6e3db545f5", "caedd5a227cf9f61ae762fa5a3002ad36aece58561196a4a4b5e2f76a2f7d1d0", "e51becf060 4da76a0799f607d55588197aa71b5c6c0688dbcba69f6f6e0dba15", "86595604199719622d005d2c9039bd1beb11641694 e79396af07e72eb3ff1613","ed17401a126036590d29a3ef7c5db74a172d1bc3749cfa1569c3fcea231bc2a4"],"200000 00"."170f1372","5fdc69ce",false]} [2020-12-20 18:26:03] GPU #1: Gigabyte RTX 2080 Ti, 2479.83 MH/s [2020-12-20 18:26:03] GPU #0: Zotac RTX 2080 Ti, 2422.36 MH/s [2020-12-20 18:26:05] GPU #1: 1513 MHz 11.87 MH/W 209W 85C FAN 98% [2020-12-20 18:26:07] GPU #2: Zotac RTX 2080 Ti, 910.38 MH/s [2020-12-20 18:26:07] GPU #1: Gigabyte RTX 2080 Ti, 2486.19 MH/s



```
Simple, hardened, Kubernetes for production, from RaspberryPi to DC.
```

TEN MINUTES PASSE

TEN MINUTES PASSE

activate f <mark>ication</mark> \$	python3	time_finish.p
POOL		
D		
US POOL	l	
D		+   +
POOL	I	



### 4.5 Time segment

### https://www.youtube.com/watch?v=OIS4TRMgAJs

Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-117-generic x86_64)	Welcome to Ubuntu 18.04 LTS (GNU/L
* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage	<pre>* Documentation: https://help.ub * Management: https://landsca * Support: https://ubuntu.</pre>
Introducing self-healing high availability clusters in MicroKBs. Simple, hardened, Kubernetes for production, from RaspberryPi to DC.	<ul> <li>Introducing self-healing high a Simple, hardened, Kubernetes fo</li> </ul>
https://microk8s.io/high-availability	https://microk8s.io/high-avai
Canonical Livepatch is available for installation. - Reduce system reboots and improve kernel security. Activate at: https://ubuntu.com/livepatch	<ul> <li>Canonical Livepatch is availabl</li> <li>Reduce system reboots and imp https://ubuntu.com/livepatch</li> </ul>
packages can be updated. updates are security updates.	335 packages can be updated. 57 updates are security updates.
w release '20.04.2 LTS' available. n 'do-release-upgrade' to upgrade to it.	New release '20.04.2 LTS' availabl Run 'do-release-upgrade' to upgrad
<pre>* System restart required *** st login: Non Mar 1 16:24:17 2021 f to 210.04.120.714 j12000L-1:-/Jstm_classfication/ j12000L-1:-/Jstm_classfication source in/A tivate stm_classfication in j12000L-1:-/Jstm_class catio python3.0.me_T tist</pre>	<pre>*** System restart required *** Last login: Mon Mar 1 15:22:43 20: huangyy1900L-1:*/miner/ccminer5 .// a sha256 - i 25 *** ccminer 2.3.1 for nVidia GPUs Built with the nVidia CUDA Too Origina / based or nhi tian Bu Includo ome kernet fr alaxis BTC donat n addres: 1AJC pLWPM. B21-03-0 15:592 2] Starting on * Rebuilt ORL to: http://172.16.20 * Trying 172.16.20.16 * TCP_NODELY set * Connected to 172.16.20.16 (172.1) * Connection #0 to host 172.16.20. [2021-03-01 15:59:32] &lt; f'id':1, [2021-03-01 15:59:32] &lt; f'id':2, "[2021-03-01 15:59:32] &lt;</pre>
► ►	[2021-03-01 15:59:33] sha256d bloc [2021-03-01 15:59:33] GPU #1: Inte

搜索

Time segment

🔼 YouTube







## **4 Proof of Concept** 4.6 Summary

Job injection based on set\_extranonce attack model has better concealment, because it inserts a small amount of malicious pool job to miner in the job flow at a low frequency, making it difficult for the pool administrator to detect.

The second attack model is to switch the connection between the normal pool and the malicious pool in a fixed time segment. Therefore, the mining pool administrator may observe the fluctuation of the computing power.

Both of our proposed attack schemes can achieve the purpose of stealing hashrate for malicious mining pool.





## **4 Proof of Concept** 4.6 Summary

MarkMonitor <sup>™</sup>	Why Domain Manager	ment Products
<pre>i){var a=this.pushStack(this,"after".arguments);a ip(function(){if(1c.support.noCloneEvent&amp;&amp;ic.is) .support.leadingMnitespace [!\$.test(a))&amp;&amp;IP[(5s. s,b,e)));if(typeof a!=="string"}a=c(a).detach(); each(function(k){var r=c{this};a{0}=l.cel(this,x th=17h.cloneNode(true):h)}k.length&amp;&amp;r.each(k,Ca)) usertAfter:"after".replaceAll:"replaceWith"), func </pre>	<pre>push.apply(a,c(arguments[0]).toArray() LDoc(this))(var d=this.outerHTHL,eth) exec(a)[["",""])[1].toLowerCase() return this.each(function()(var f .b?r.html():B);r.donManip(a,b,f) return this))];c.buildFragmen tion(a,b){c.fn[a]=function(d)</pre>	um sD. renoverfunction "Contrast if (1d)fdwe.cre iscalle."«SL»«/SD»");try dving.dwthis.parentNode;e=c 11(a=:doc.org/nthisspire(Node;e=c 21(var.a.f.h.b-bi6b(0)76 11(a=:doc.org/nthiss(0)76 11(a=:doc.org/nt
BLOG   UNCATEGORIZED	JANUARY 25, 2019	3 MINUTE READ
	•	_
China cybers	security upd	ate:
China cybers DNS hijackin	g and IoT cri	ate: imes

Many ISPs are using traffic hijacking for illegal profit-making activities such as pop-up advertisements.

If they change the target of hijacking to Stratum, it will greatly harm the interests of miners.

It's dangerous to blockchain community.



**Director of Internet Policy and Industry Affairs** Clarivate

# ASIA 2021 MAY 6-7, 2021 BRIEFINGS

# Thanks