

# Rapport d'analyse

## SOMMAIRE

<b>INTRO</b>	<b>2</b>
<b>ACCORD</b>	<b>2</b>
Notre mission	2
L'équipe	2
<b>ETAPES</b>	<b>3</b>
analyse du réseau	3
actions	4
<b>CONCLUSION</b>	<b>5</b>
<b>CONSEIL</b>	<b>5</b>

---

## INTRO

nous allons analyser un malware

## ACCORD

### Notre mission

Notre mission analyser et comprendre le problème ce qu'il fait ?,sont origine ?,d'où vient il ?

### L'équipe

Travail à 2 avec tom pouyez (problème accès site)  
rendu individuel

## ETAPES

### Analyse du réseau

Nous commençons par regarder les processus malveillant ainsi que leur detail

### Actions

on est sur le processus du malware

Process details ID 13016 Malicious

Command line

./6dcf570e-df95-4cf2-ab23-71bcfbab069e.o

More Info

Hide all

**Warning 2**

[T1082](#) System Information Discovery (2)

- Checks DMI information (probably VM detection)
- Reads /proc/mounts (likely used to find writable filesystems)

[T1497.001](#) System Checks (1)

- Checks DMI information (probably VM detection)

on analyse les dangers

Process details ID 13017 Malicious

Command line

./6dcf570e-df95-4cf2-ab23-71bcfbab069e.o

More Info

Hide all

**Danger 2**

MINER has been detected (SURICATA)

[T1071](#) Application Layer Protocol (1)

- Connects to the CnC server

on observe Le port 853 est un port réservé pour DNS-over-TLS

# Behavior activities

(PID: 13017) 6dcf570e-df95-4cf2-ab23-71bcfbab069e.o

Source: networkFirst seen: 45303 ms

 **Danger / Known Threat**  
**MINER has been detected (SURICATA)**

Process:

/home/user/Desktop/6dcf570e-df95-4cf2-ab23-71bcfbab069e.o

IpDst:

194.59.30.110

IpSrc:

192.168.100.44

PortDst:

43782

PortSrc:

57452

on va dans l'arbre des processus



on observe que le malware lance plusieurs processus afin de reprendre la main sur le pc pour rester présent continuellement

PID	Process	Class	Message
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Misc Attack	ET COMPROMISED Known Compromised or Hostile Host Traffic group 7
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 38
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Misc Attack	ET 3CORESec Poor Reputation IP group 6
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Crypto Currency Mining Activity Detected	MINER [ANY.RUN] CoinMiner Agent CnC Initial Connection
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Potential Corporate Privacy Violation	ET POLICY Cryptocurrency Miner Checkin
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 14
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Misc Attack	ET 3CORESec Poor Reputation IP group 12
13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	Potential Corporate Privacy Violation	ET POLICY Cryptocurrency Miner Checkin
13147	http	Not Suspicious Traffic	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management

+6232 ms	ET COMPROMISED Known Compromised or Hostile Host Traffic group 7 <b>Misc Attack</b>	2500012	194.59.30.110	57452	192.168.100.44	57452
+6235 ms	ET DROP Spamhaus DROP Listed Traffic Inbound group 38 <b>Misc Attack</b>	2400037	194.59.30.110	57452	192.168.100.44	57452
+6238 ms	ET 3CORESec Poor Reputation IP group 6 <b>Misc Attack</b>	2525005	194.59.30.110	57452	192.168.100.44	57452
+6244 ms	MINER [ANY.RUN] CoinMiner Agent CnC Initial Connection <b>Crypto Currency Mining Activity Detected</b>	8001332	192.168.100.44	43782	194.59.30.110	43782
+8769 ms	ET POLICY Cryptocurrency Miner Checkin <b>Potential Corporate Privacy Violation</b>	2024792	192.168.100.44	2137	93.123.39.174	2137
+8770 ms	ET DROP Spamhaus DROP Listed Traffic Inbound group 14 <b>Misc Attack</b>	2400013	93.123.39.174	50240	192.168.100.44	50240
+8771 ms	ET 3CORESec Poor Reputation IP group 12 <b>Misc Attack</b>	2525011	93.123.39.174	50240	192.168.100.44	50240
+63550 ms	ET POLICY Cryptocurrency Miner Checkin <b>Potential Corporate Privacy Violation</b>	2024792	192.168.100.44	2137	93.123.39.174	2137

On observe que le cpu est utilisé.

## Threat details

Here are the details of the threat

Main
Stream data
Suricata rule

The data provided by [Suricata IDS](#)

1 of 2
Show all
View
HEX
Text
Highlight chars

Send: 349 b
Timeshift: 47392 ms
Download
Hide

00000000	7B 22 69 64 22 3A 31 2C 22 6A 73 6F 6E 72 70 63	{ "id":1, "jsonrpc
00000010	22 3A 22 32 2E 30 22 2C 22 6D 65 74 68 6F 64 22	":"2.0", "method"
00000020	3A 22 6C 6F 67 69 6E 22 2C 22 70 61 72 61 6D 73	:"login", "params
00000030	22 3A 7B 22 6C 6F 67 69 6E 22 3A 22 78 22 2C 22	":"login":"x", "
00000040	70 61 73 73 22 3A 22 78 22 2C 22 61 67 65 6E 74	pass":"x", "agent
00000050	22 3A 22 58 4D 52 69 67 2F 36 2E 32 31 2E 32 20	":"XMRig/6.21.2
00000060	28 4C 69 6E 75 78 20 78 38 36 5F 36 34 29 20 6C	(Linux x86_64) l
00000070	69 62 75 76 2F 31 2E 34 38 2E 30 20 67 63 63 2F	ibuv/1.48.0 gcc/
00000080	31 31 2E 32 2E 31 22 2C 22 61 6C 67 6F 22 3A 5B	11.2.1", "algo":[
00000090	22 63 6E 2F 31 22 2C 22 63 6E 2F 32 22 2C 22 63	"cn/1", "cn/2", "c
000000a0	6E 2F 72 22 2C 22 63 6E 2F 66 61 73 74 22 2C 22	n/r", "cn/fast", "
000000b0	63 6E 2F 68 61 6C 66 22 2C 22 63 6E 2F 78 61 6F	cn/half", "cn/xao
000000c0	22 2C 22 63 6E 2F 72 74 6F 22 2C 22 63 6E 2F 72	", "cn/rto", "cn/r
000000d0	77 7A 22 2C 22 63 6E 2F 7A 6C 73 22 2C 22 63 6E	wz", "cn/zls", "cn
000000e0	2F 64 6F 75 62 6C 65 22 2C 22 63 6E 2F 63 63 78	/double", "cn/ccx
000000f0	22 2C 22 72 78 2F 30 22 2C 22 72 78 2F 77 6F 77	", "rx/0", "rx/wow

en regardant l'intérieur d'une requête on observe que toutes les connections à des serveurs dns sert à miner de la cryptomonnaie le XMR(monero) qui mine sur le cpu

Pour la partie ROOT :

on observe une connection ssh

# Behavior activities

(PID: 13001) 4088e9a1-d873-4ee0-a773-1714a4b2872e.o

1 of 422

Source: network

First seen: 22300 ms



Warning / Network Activities  
Connects to SSH

T1021 Remote Services

Process: /home/user/Desktop/4088e9a1-d873-4ee0-a773-1714a4b2872e.o  
IpDst: 45.55.201.89  
PortDst: 22  
PortSrc: 50790  
Protocol: tcp

Main

The data provided by sensors is

Potential Corporate Privacy Violation

## POLICY [ANY.RUN] A SSH banner has been detected

Src / Dst ..... 31.220.95.67 : 22 ⇄ 192.168.100.45 : 55226 ↵  
Timeshift ..... 21822 ms  
SID ..... 8001425; rev: 1;  
Transport ..... TCP  
App Protocol ..... SSH  
Src IP ..... 31.220.95.67  
Dst IP ..... 192.168.100.45  
Src Port ..... 22  
Dst Port ..... 55226  
To DstIP Packet ..... 3  
To SrcIP Packet ..... 3  
Total Bytes ..... 501

Potential Corporate Privacy Violation

## POLICY [ANY.RUN] Received Telnet Banner

Src / Dst .....	190.106.79.26 : 23 ⇄ 192.168.100.45 : 49460 ↵
Timeshift .....	24203 ms
SID .....	8001336; rev: 1;
Transport .....	TCP
Src IP .....	190.106.79.26
Dst IP .....	192.168.100.45
Src Port .....	23
Dst Port .....	49460
To DstIP Packet ..	3
To SrcIP Packet ..	2
Total Bytes .....	366



Potential Corporate Privacy Violation

## POLICY [ANY.RUN] A SSH banner has been detected on a non-standard port number

Src / Dst	213.158.95.131 : 2222 ↔ 192.168.100.45 : 47496 ↗
Timeshift	24924 ms
SID	8001327; rev: 1;
Transport	TCP
App Protocol	SSH
Src IP	213.158.95.131
Dst IP	192.168.100.45
Src Port	2222
Dst Port	47496
To DstIP Packet	3
To SrcIP Packet	4
Total Bytes	1312

### IP Details For: 45.55.201.89

Decimal:	758630745
Hostname:	45.55.201.89
ASN:	14061
ISP:	DigitalOcean LLC
Services:	Data Center/Transit
Country:	United States
State/Region:	New Jersey
City:	Clifton
Latitude:	40.8586 (40° 51' 30.91" N)
Longitude:	-74.1636 (74° 9' 48.98" W)



[CLICK TO CHECK BLACKLIST STATUS](#)

## ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)

Src / Dst .....	179.27.97.1 : 443 ➡ 192.168.100.45 : 39582 ↵
Timeshift .....	48869 ms
SID .....	2013659; rev: 6;
Transport .....	TCP
App Protocol .....	TLS
Src IP .....	179.27.97.1
Dst IP .....	192.168.100.45
Src Port .....	443
Dst Port .....	39582
To DstIP Packet ..	5
To SrcIP Packet ..	5
Total Bytes .....	2738

## CONCLUSION

Nous pensons que ce processus malveillant est un malware exécutant des sous processus afin de rester up en permanence , il envoie des requêtes à tous les serveurs dns afin de créer un lien vers le monde extérieur pour accéder à un portail crypto pour miner et envoyer ce qu'il aura pu miner sur le cpu de l'ordinateur.

## CONSEIL

Nous vous conseillons de faire attention à tout processus que vous lancer ainsi à ce qu'y est installé sur les équipements , il faudra isoler la partie touchée par l'attaque et la formater afin de se séparer de ce malware et il faudra faire de la surveillance de réseau afin de savoir si des processus malveillant essaie de communiquer vers l'extérieur ainsi que de surveiller s'y aucun processus malveillant circule sur le réseau local.