PICOT QUENTIN
Groupe 1A
24/10/2025

Rapport d’analyse

SOMMAIRE

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**

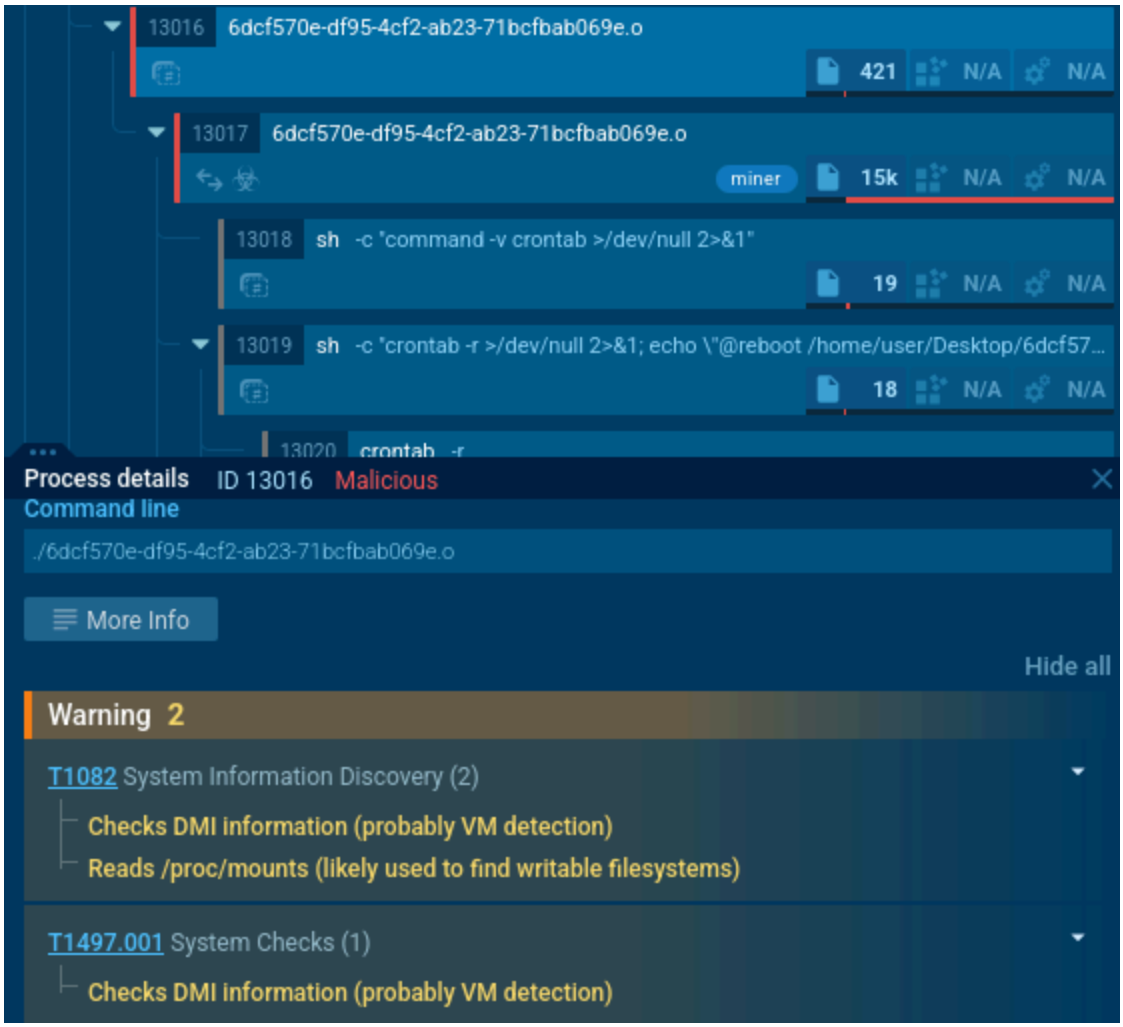
ETAPES

Analyse du réseau

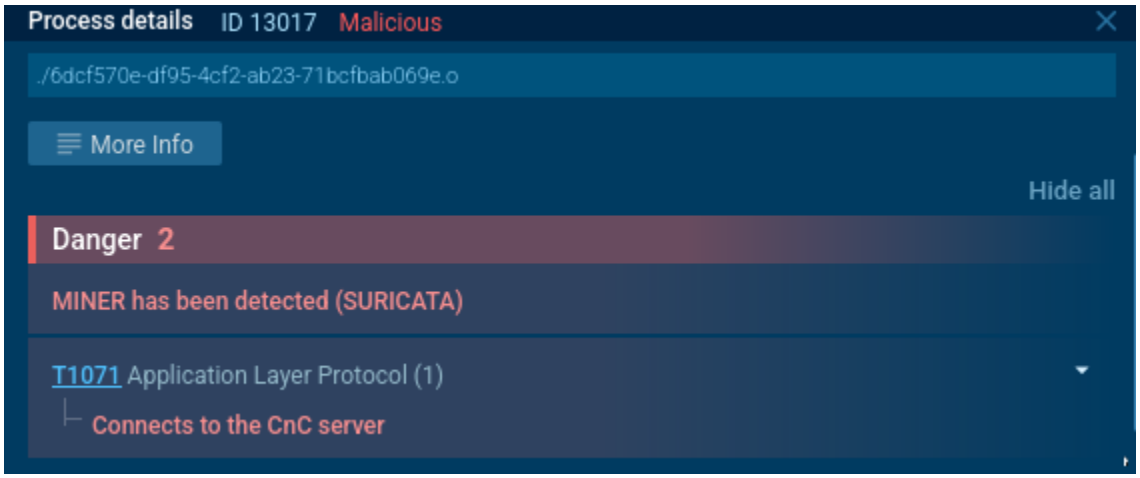
Nous commençons par regarder les processus malveillant ainsi que leur detail

Actions

on est sur le processus du malware

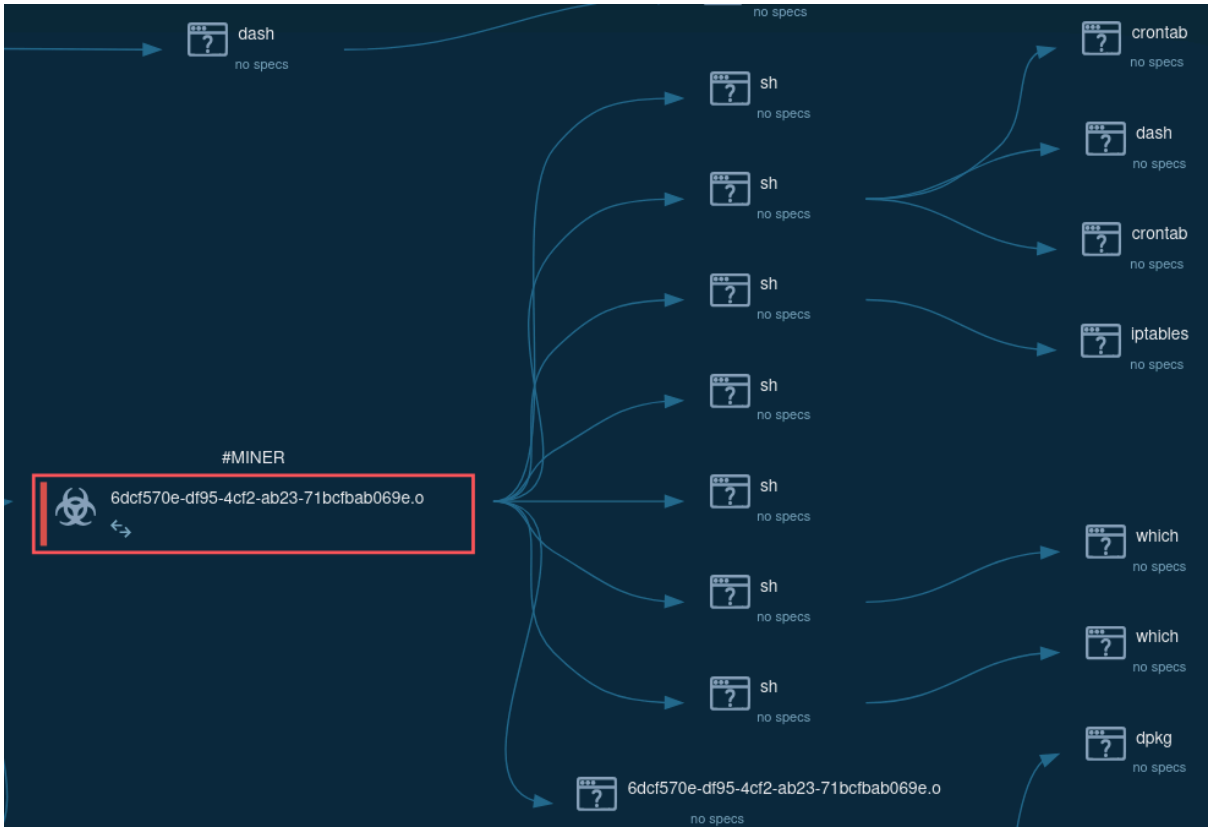


on analyse les dangers



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

on va dans l'arbre des processus

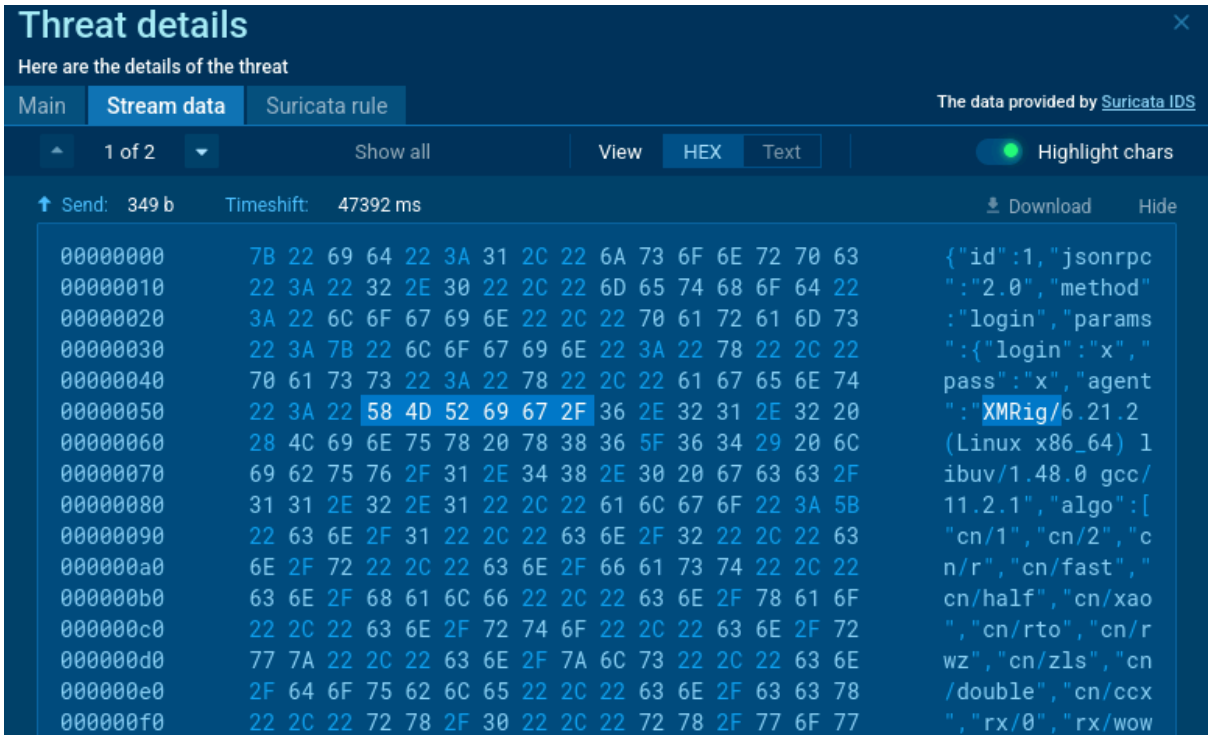


on observe que le malware lance plusieur processus afin de reprendre la main sur le pc pour rester présent continuellement

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

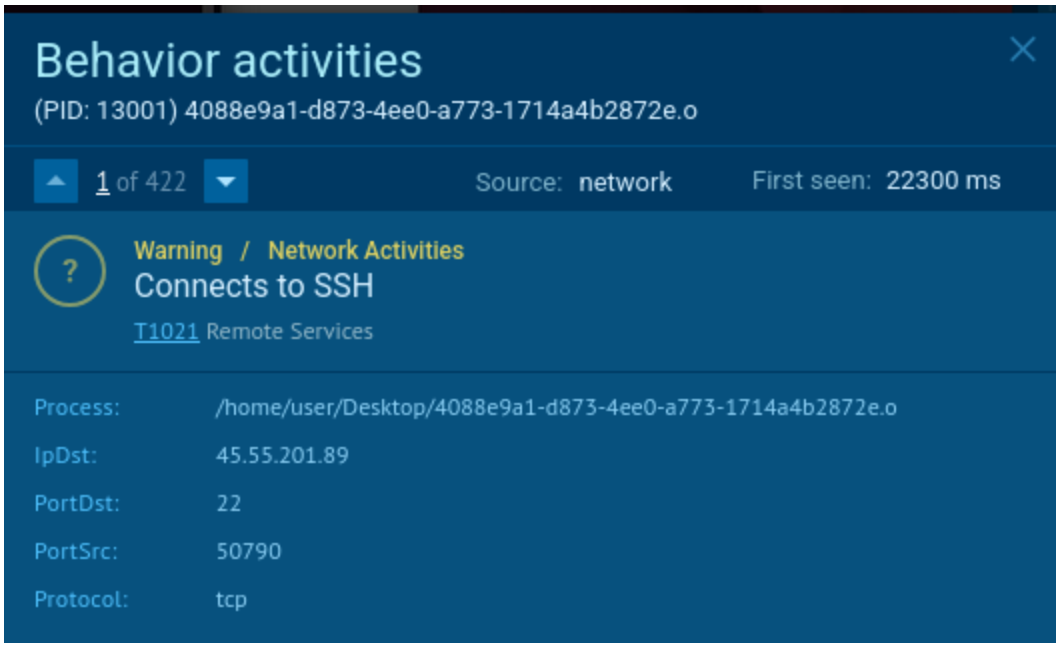
On observe que le cpu est utilisé.

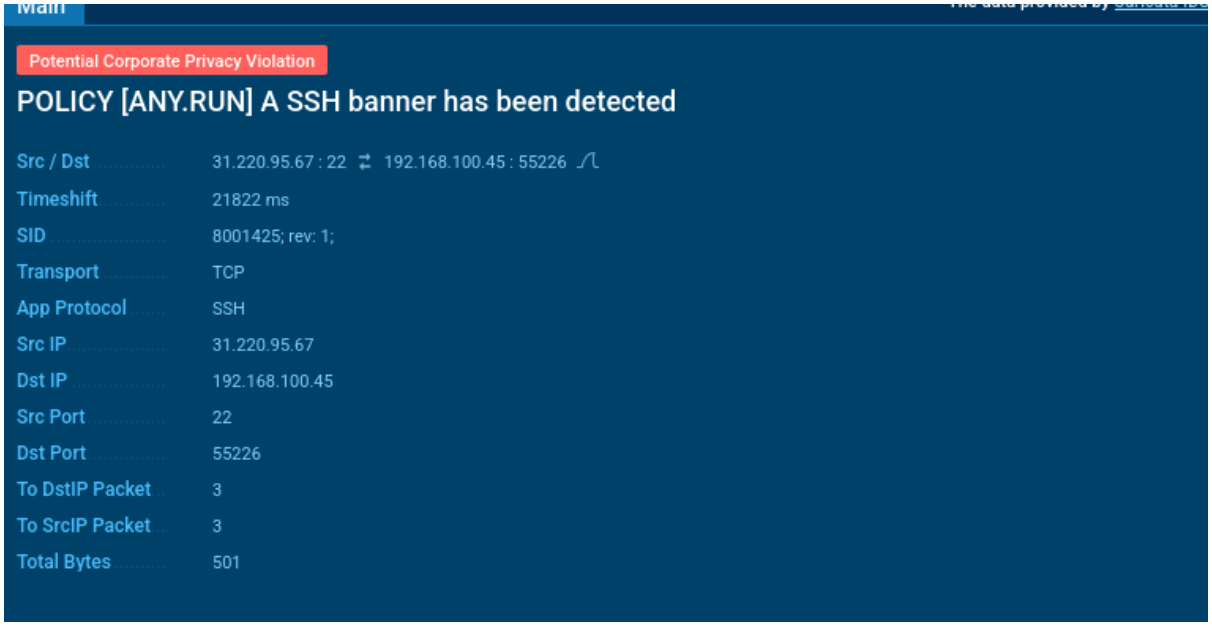


en regardant l'intérieur d'une requête on observe que toutes les connections à des serveurs dns sert à miner de la cryptomonnaie le XMR(monero) qui mine sur le cpu

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
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

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.