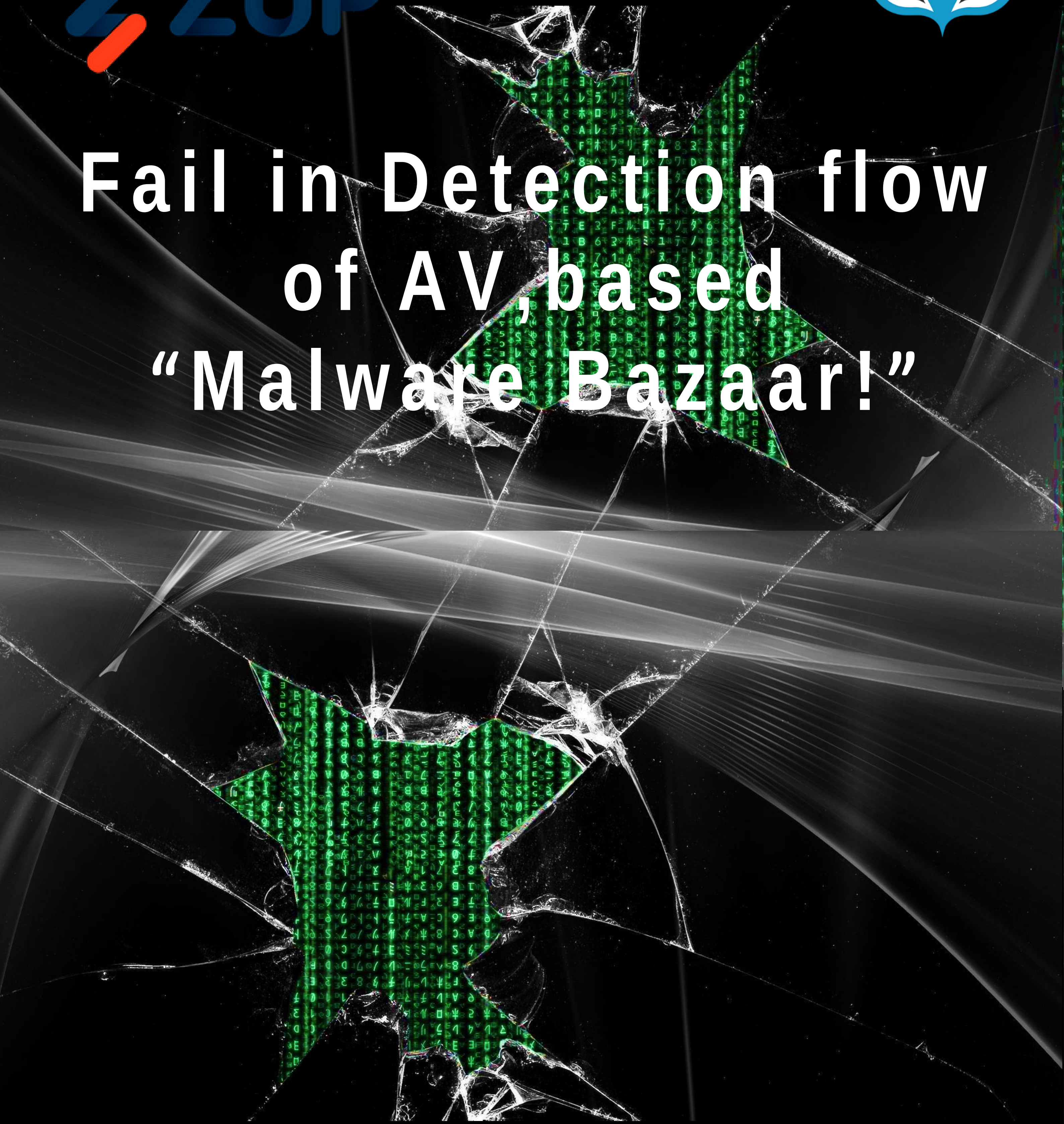
Fail in Detection flow of AV,based “Malware Bazaar!”



ZUP Security Labs at Zup Innovation

Researcher & CyberSecurity Manager: Filipi Pires

Introduction

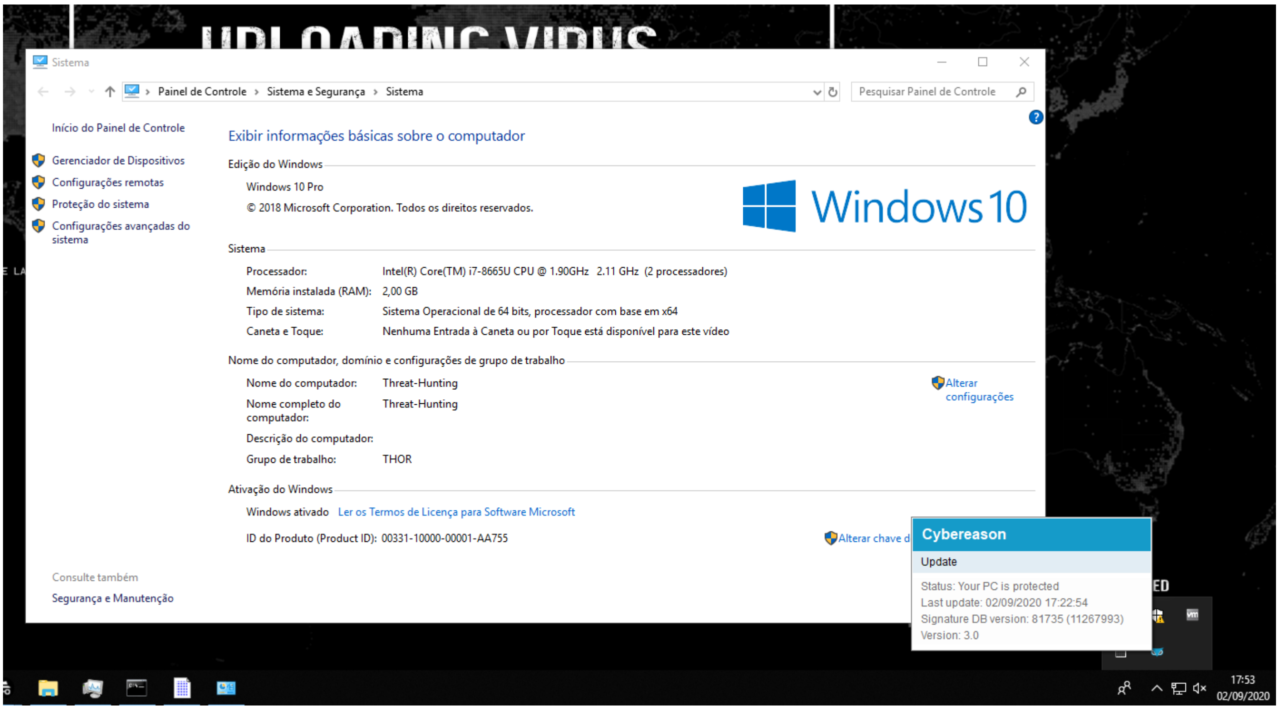
The purpose of this document, it was to execute several efficiency and detection tests in our endpoint solution, provided by Cybereason, this document brings the result of the defensive security analysis with an offensive mindset performed in the execution of 185 different Malwares in our environment.

Regarding the test performed, the first objective it was to simulate targeted attacks using known malware to obtain a panoramic view of the resilience presented by the solution, with regard to the efficiency in its detection by signatures, NGAV and Machine Learning, downloading these artifacts directly on the victim's machine. The second objective consisted of analyzing the detection of those same 185 malwares (or those not detected yet) when they were changed directories, the idea here is to work with manipulation of samples (without execution).

With the final product, the front responsible for the product will have an instrument capable of guiding a process of mitigation and / or correction, as well as optimized improvement, based on the criticality of risks.

2.0.1 Scope

The efficiency and detection analysis had as target the Cybereason Endpoint Protection application (`Cybereason Solution Cloud`) in **Version 20.1.261.0;**
Installed in the windows machine `Windows 10 Pro`;
Hostname - `Threat-Hunting`, as you can see in the picture below:


UPLOADING VIRUS
Sistema
Painel de Controle › Sistema e Segurança › Sistema
Pesquisar Painel de Controle
Início do Painel de Controle
Gerenciador de Dispositivos
Configurações remotas
Proteção do sistema
Configurações avançadas do sistema
Windows 10
Alterar configurações
Alterar chave d
Consulte também
Segurança e Manutenção
17:53
02/09/2020

Exibir informações básicas sobre o computador

Edição do Windows
Windows 10 Pro
© 2018 Microsoft Corporation. Todos os direitos reservados.

Sistema
Processador: Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz 2.11 GHz (2 processadores)
Memória instalada (RAM): 2,00 GB
Tipo de sistema: Sistema Operacional de 64 bits, processador com base em x64
Caneta e Toque: Nenhuma Entrada à Caneta ou por Toque está disponível para este vídeo

Nome do computador, domínio e configurações de grupo de trabalho
Nome do computador: Threat-Hunting
Nome completo do computador: Threat-Hunting
Descrição do computador:
Grupo de trabalho: THOR

Ativação do Windows
Windows ativado Ler os Termos de Licença para Software Microsoft
ID do Produto (Product ID): 00331-10000-00001-AA755

Cybereason
Update
Status: Your PC is protected
Last update: 02/09/2020 17:22:54
Signature DB version: 81735 (11267993)
Version: 3.0

Image 1.1: Windows 10 Education 2019 Virtual Machine

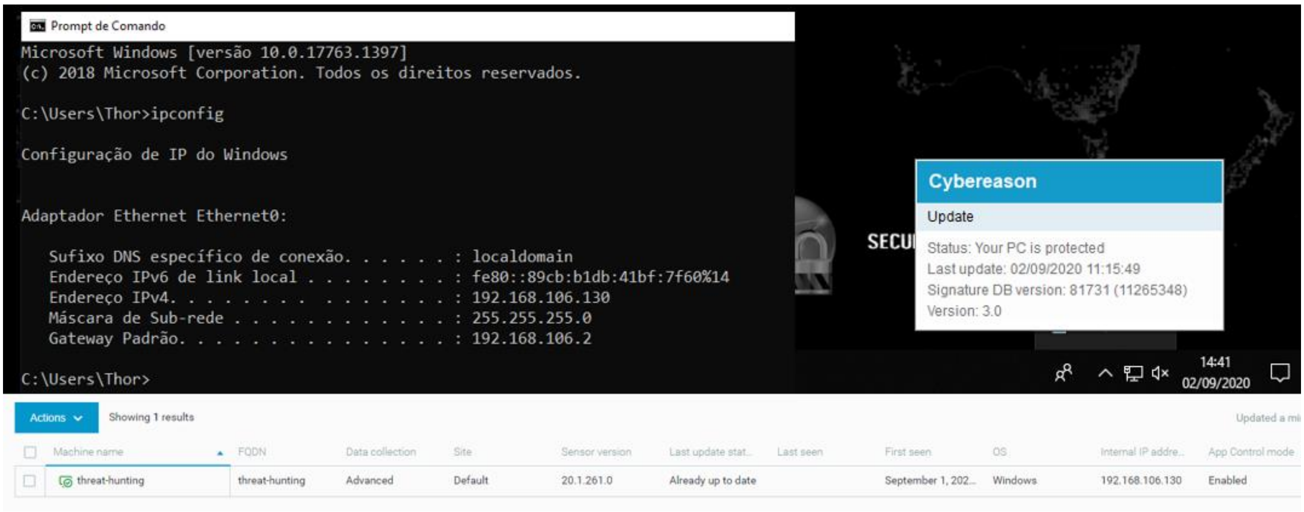
2.0.2 Project Summary

The execution of the security analysis tests of the Threat Hunting team it was carried out through the execution of 185 Malwares in a virtualized environment in a controlled way, simulating a real environment, together with their respective best practices of the security policies applied, the test occurred during **1 day**, without count the weekend, along with the making of this document. The intrusion test started on the **02nd of September** of the year 2020 and it was completed on the **03rd of September** of the same year.

1 Running the Tests

3.1 Description

A virtual machine with Windows 10 operating system it was deployed to perform the appropriate tests, as well as the creation of a security policy on the management platform (`ZUP - Threat Hunting - Policy`) e and applied to due device.



Prompt de Comando

```
Microsoft Windows [versão 10.0.17763.1397]
(c) 2018 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Thor>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet0:

   Sufixo DNS específico de conexão. . . . . . : localdomain
   Endereço IPv6 de link local . . . . . . . . : fe80::89cb:b1db:41bf:7f60%14
   Endereço IPv4. . . . . . . .  . . . . . . . : 192.168.106.130
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 192.168.106.2

C:\Users\Thor>
```

Cybereason

Update

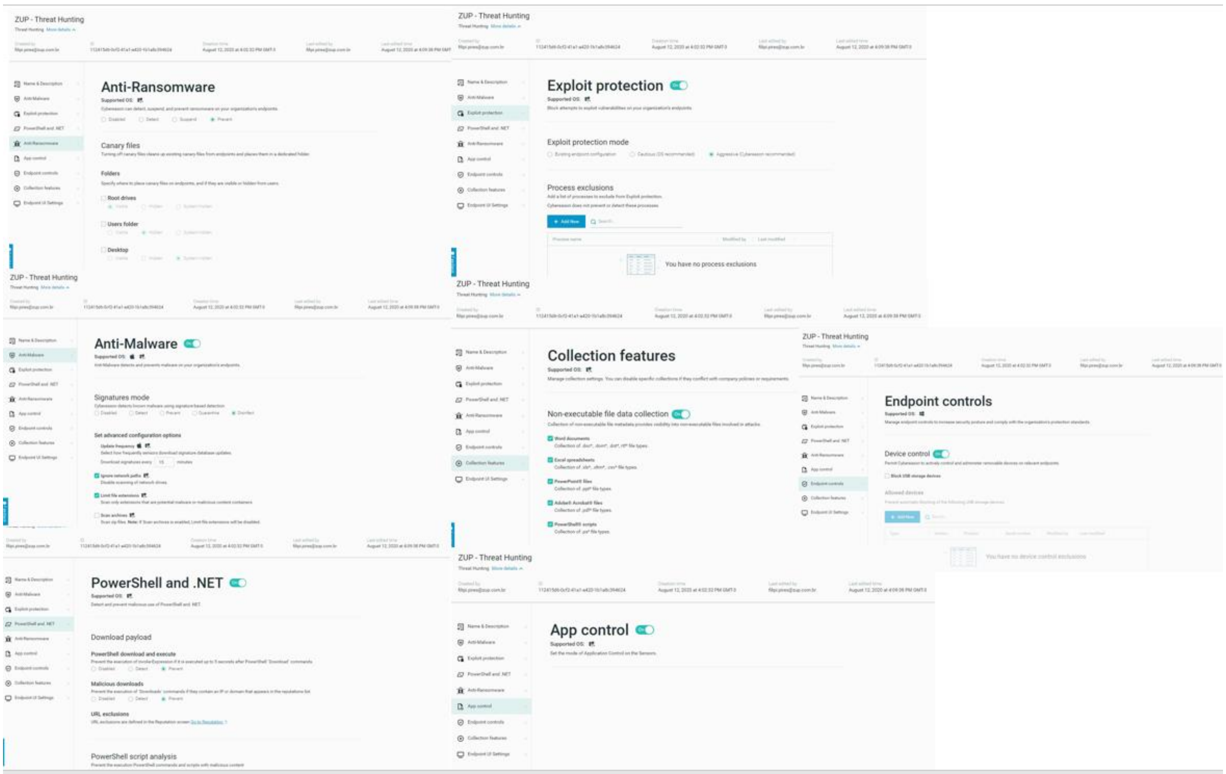
Status: Your PC is protected
Last update: 02/09/2020 11:15:49
Signature DB version: 81731 (11265348)
Version: 3.0

Showing 1 results

□	Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS	Internal IP addre...	App Control mode
□	threat-hunting	threat-hunting	Advanced	Default	20.1.261.0	Already up to date		September 1, 202...	Windows	192.168.106.130	Enabled

Image 1.2: Virtual Machine with Policy applied

The policy created was named **`ZUP - Threat Hunting`**, following the best practices recommended by the manufacturer, and, for testing purposes, all due actions were based on an aggressive detection method.



ZUP - Threat Hunting

Anti-Ransomware

Canary files

Folders

Root drives

Users folder

Desktop

Exploit protection

Exploit protection mode

Process exclusions

You have no process exclusions

Anti-Malware

Signatures mode

Set advanced configuration options

Collection features

Non-executable file data collection

Endpoint controls

Device control

PowerShell and .NET

Download payload

PowerShell download and execute

Malicious downloads

URL exclusions

PowerShell script analysis

App control

Image 1.3: Policy cretead by Cybereason Manager

3.2 First Test

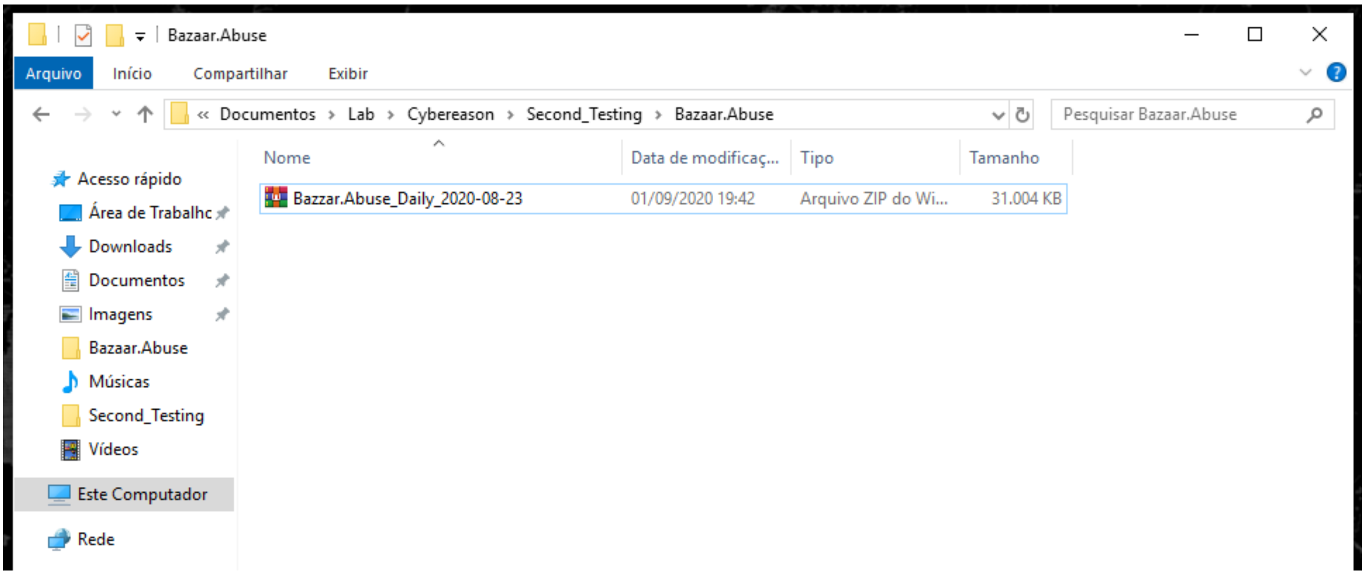
The first stage of the tests was through the download of 185 malware, that it was uploaded from public repository known and maintained by the security community called **MalwareBazzar** (`https://bazaar.abuse.ch/`);.

> *MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.*

MalwareBazaar creates daily batches of malware sample). The daily batches are created once a day at midnight (00:00 UTC). Please consider that it takes a few minutes to create the batch. So, I kindly ask you to not fetch the daily batch before 00:15 UTC.

The day choose for this test it was 2020-08-23

(`https://mb-api.abuse.ch/downloads/2020-08-23.zip`)



Nome	Data de modificaç...	Tipo	Tamanho
Bazzar.Abuse_Daily_2020-08-23	01/09/2020 19:42	Arquivo ZIP do Wi...	31.004 KB

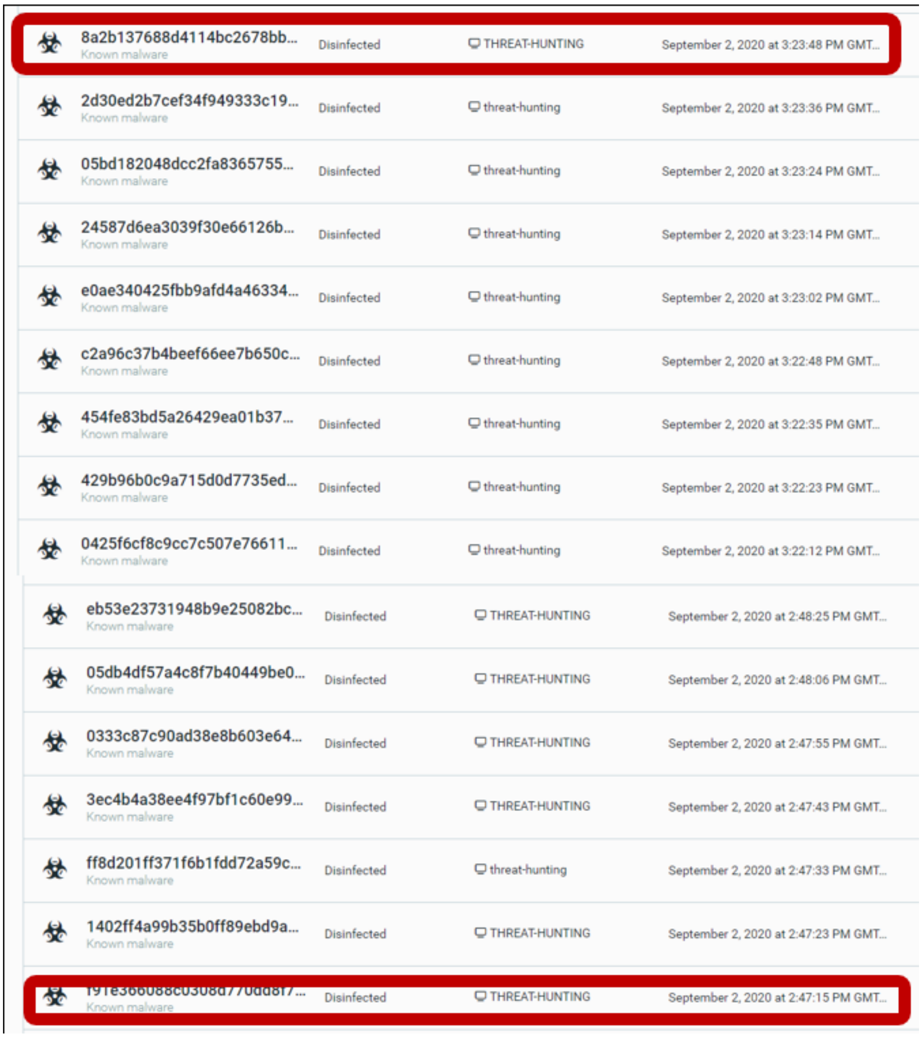
Image 1.4: Download 185 Malwares inside this Folders

The purpose of this test, it was to simulate the same process as a user receiving a zipped file (`.zip`) and performing the extraction of these artifacts in their own environment.

During this test, one thing called my attention:

- **First Detection** happened on **September 2, 2020 at 2:47:15 PM GMT-3**
- **Last Detection** happened on **September 2, 2020 at 3:23:48 PM GMT-3**

That is, we have a time gap with more than 30 min between the first and the last detection, that was the time it took for malwares to be detected.



8a2b137688d4114bc2678bb… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 3:23:48 PM GMT…
2d30ed2b7cef34f949333c19… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:23:36 PM GMT…
05bd182048dcc2fa8365755… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:23:24 PM GMT…
24587d6ea3039f30e66126b… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:23:14 PM GMT…
e0ae340425fbb9afd4a46334… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:23:02 PM GMT…
c2a96c37b4beef66ee7b650c… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:22:48 PM GMT…
454fe83bd5a26429ea01b37… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:22:35 PM GMT…
429b96b0c9a715d0d7735ed… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:22:23 PM GMT…
0425f6cf8c9cc7c507e76611… Known malware	Disinfected	threat-hunting	September 2, 2020 at 3:22:12 PM GMT…
eb53e23731948b9e25082bc… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:48:25 PM GMT…
05db4df57a4c8f7b40449be0… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:48:06 PM GMT…
0333c87c90ad38e8b603e64… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:47:55 PM GMT…
3ec4b4a38ee4f97bf1c60e99… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:47:43 PM GMT…
ff8d201ff371f6b1fdd72a59c… Known malware	Disinfected	threat-hunting	September 2, 2020 at 2:47:33 PM GMT…
1402ff4a99b35b0ff89ebd9a… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:47:23 PM GMT…
f91e366088c0308d770dd8f7… Known malware	Disinfected	THREAT-HUNTING	September 2, 2020 at 2:47:15 PM GMT…

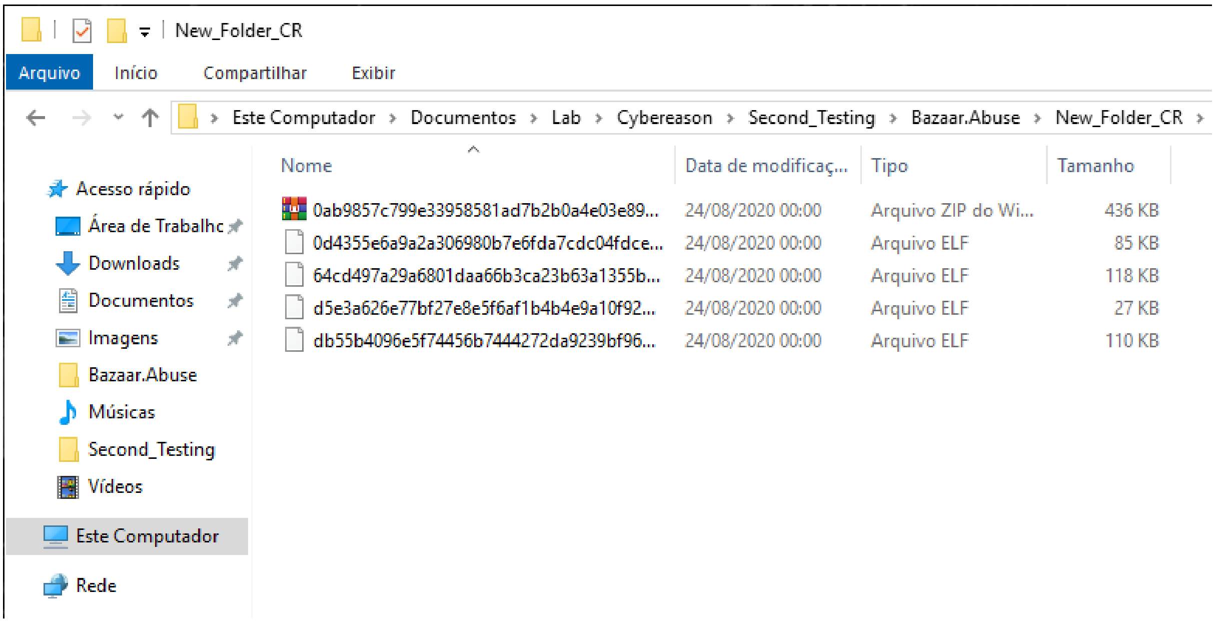
Image 1.5: Malware Alerts Detection by Cybereason

After performing the action of extracting the files, it was possible to verify in the *Cybereason* "**`Malware Alerts`**" logs that many malwares were detected, however it was possible to verify that there are currently **5 (five) Malwares** that, when executed inside the environment, could perform an infection.

All these malwares will be explored in the "Impact" tag.

3.3 Second Test

The second stage of the tests was through the transfer of folders to another directory within the same machine, the purpose of this test was to simulate a transfer of files within the same environment.

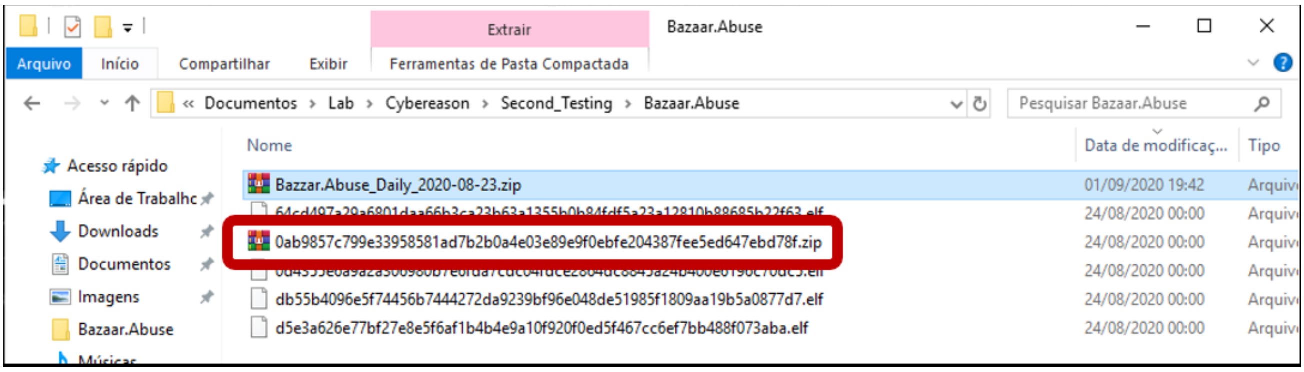


Nome	Data de modificaç...	Tipo	Tamanho
0ab9857c799e33958581ad7b2b0a4e03e89...	24/08/2020 00:00	Arquivo ZIP do Wi...	436 KB
0d4355e6a9a2a306980b7e6fda7cdc04fdce...	24/08/2020 00:00	Arquivo ELF	85 KB
64cd497a29a6801daa66b3ca23b63a1355b...	24/08/2020 00:00	Arquivo ELF	118 KB
d5e3a626e77bf27e8e5f6af1b4b4e9a10f92...	24/08/2020 00:00	Arquivo ELF	27 KB
db55b4096e5f74456b7444272da9239bf96...	24/08/2020 00:00	Arquivo ELF	110 KB

Image 1.6: New_Folder_CR – Malware manipulation

When a new file is generated on the disk, soon we should have a new entry in a block of that disk and in theory the antivirus should take some action (considering that it has the real time enabled), we could define it as a file manipulation (**still not running**) where the endpoint protection is already necessary, considering that a new directory was created, soon we would have a new repository with several new hashes inside to be examined.

One of these malwares that were within of the originally ***Bazaar.ZIP*** file, had other zip packet layer as you can see below.



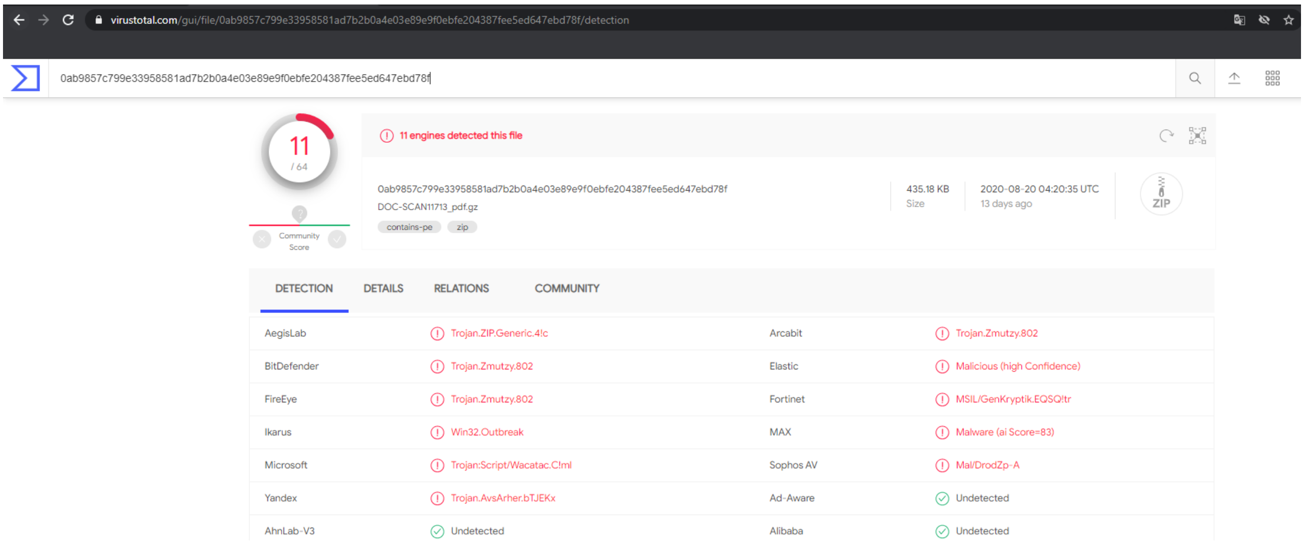
Nome	Data de modificaç...	Tipo
Bazzar.Abuse_Daily_2020-08-23.zip	01/09/2020 19:42	Arquiv
64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63.elf	24/08/2020 00:00	Arquiv
0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f.zip	24/08/2020 00:00	Arquiv
0d4355e6a9a2a306980b7e6fda7cdc04fdce2804dc8843a24b400e0190c70dc5.elf	24/08/2020 00:00	Arquiv
db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7.elf	24/08/2020 00:00	Arquiv
d5e3a626e77bf27e8e5f6af1b4b4e9a10f920f0ed5f467cc6ef7bb488f073aba.elf	24/08/2020 00:00	Arquiv

Image 1.7: New extraction malicious

When we look in this file, with some researches we can find some information's about that.

`0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f.zip`

In Virus Total reference we can see that this file is known like **Malicious file**, by eleven different antivirus engines.


virustotal.com/gui/file/0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f/detection
0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f
11
/ 64
?
Community Score
ZIP
DETECTION
DETAILS
RELATIONS
COMMUNITY

11 engines detected this file

0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f
DOC-SCAN11713_pdf.gz
contains-pe zip

435.18 KB
Size

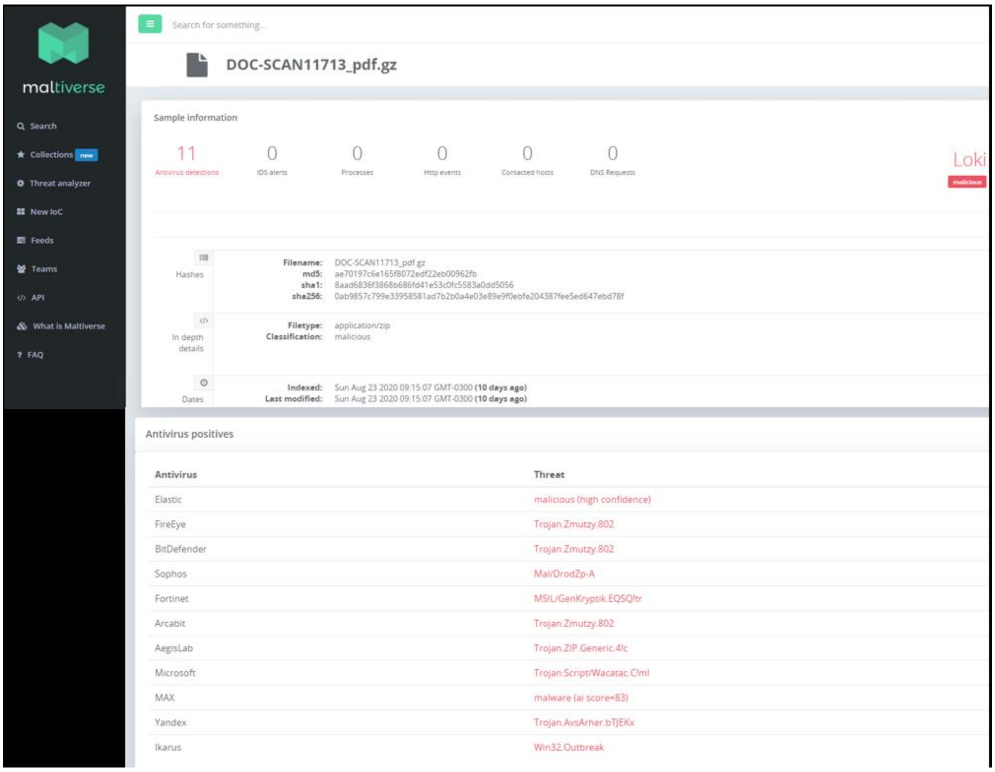
2020-08-20 04:20:35 UTC
13 days ago

AegisLab	Trojan.ZIP.Generic.4!c	Arcabit	Trojan.Zmutzy.802
BitDefender	Trojan.Zmutzy.802	Elastic	Malicious (high Confidence)
FireEye	Trojan.Zmutzy.802	Fortinet	MSIL/GenKryptik.EQSQ!tr
Ikarus	Win32.Outbreak	MAX	Malware (ai Score=83)
Microsoft	Trojan:Script/Wacatac.C!ml	Sophos AV	Mal/DrodZp-A
Yandex	Trojan.AvsArher.bTJEKx	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected

Image 1.8: VirusTotal Detection

Other perspective is to try find any information in another kind of platforms, or others databases and to try find any reputation for this domain, I made an testing in **Maltiverse** platform, It is born as a service oriented to get used by cybersecurity analysts to research on indicators of compromise (IOCs), as you can see in the *prescreen* below provide by **Maltiverse** Platform.

The result of this test, brought to us that this file is **Malicious**.



DOC-SCAN11713_pdf.gz

Sample information

11	0	0	0	0	0
Antivirus detections	IDS alerts	Processes	Http events	Contacted hosts	DNS Requests

Hashes
Filename: DOC-SCAN11713_pdf.gz
md5: ae70197c6e165f8072edf22eb00962fb
sha1: 8aad6836f3868b686fd41e53c0fc5583a0dd5056
sha256: 0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f

In depth details
Filetype: application/zip
Classification: malicious

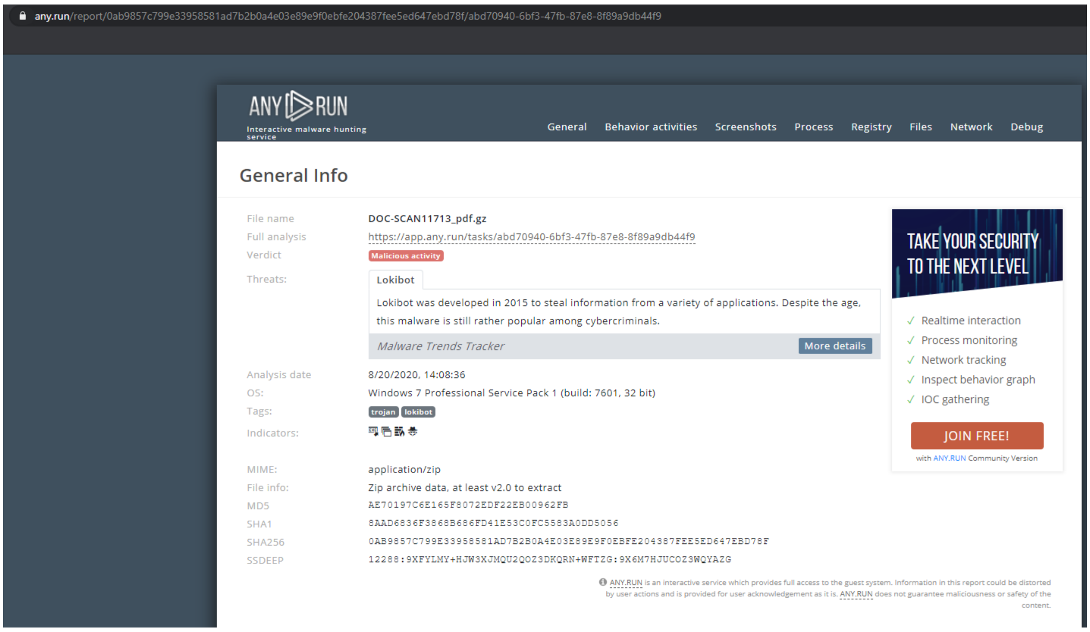
Dates
Indexed: Sun Aug 23 2020 09:15:07 GMT-0300 **(10 days ago)**
Last modified: Sun Aug 23 2020 09:15:07 GMT-0300 **(10 days ago)**

Antivirus positives

Antivirus	Threat
Elastic	malicious (high confidence)
FireEye	Trojan.Zmutzy.802
BitDefender	Trojan.Zmutzy.802
Sophos	Mal/DrodZp-A
Fortinet	MSIL/GenKryptik.EQSQ!tr
Arcabit	Trojan.Zmutzy.802
AegisLab	Trojan.ZIP.Generic.4!c
Microsoft	Trojan:Script/Wacatac.C!ml
MAX	malware (ai score=83)
Yandex	Trojan.AvsArher.bTJEKx
Ikarus	Win32.Outbreak

Image 1.9: Maltiverse Detection

After this, I made other test in **Any.Run** platform, Cloud-based malware analysis service. Take your information security to the next level. Analyze suspicious and malicious activities using some innovative tools, the result of this test, brought to us the same result **Malicious** file.


any.run/report/0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f/abd70940-6bf3-47fb-87e8-8f89a9db44f9
ANY RUN
Interactive malware hunting service
General
Behavior activities
Screenshots
Process
Registry
Files
Network
Debug
TAKE YOUR SECURITY TO THE NEXT LEVEL
✓ Realtime interaction
✓ Process monitoring
✓ Network tracking
✓ Inspect behavior graph
✓ IOC gathering
JOIN FREE!
with ANY.RUN Community Version

General Info

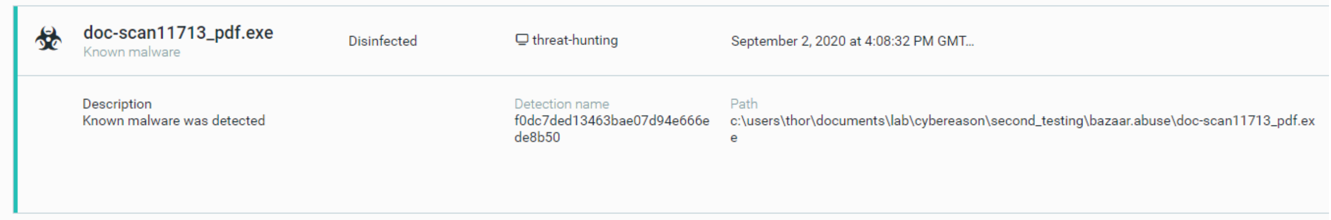
File name DOC-SCAN11713_pdf.gz
Full analysis https://app.any.run/tasks/abd70940-6bf3-47fb-87e8-8f89a9db44f9
Verdict Malicious activity
Threats: Lokibot
Lokibot was developed in 2015 to steal information from a variety of applications. Despite the age, this malware is still rather popular among cybercriminals.
Malware Trends Tracker More details
Analysis date 8/20/2020, 14:08:36
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: trojan lokibot
Indicators:

MIME: application/zip
File info: Zip archive data, at least v2.0 to extract
MD5 AE70197C6E165F8072EDF22EB00962FB
SHA1 8AAD6836F3868B686FD41E53C0FC5583A0DD5056
SHA256 0AB9857C799E33958581AD7B2B0A4E03E89E9F0EBFE204387FEE5ED647EBD78F
SSDEEP 12288:9XFYLMY+HJW3XJMQU2QOZ3DKQRN+WFTZG:9X6M7HJUCOZ3WQYAZG

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Image 1.10: Any Run - Detection

After performing this new extraction of zip file, the Cybereason solution endpoint, blocked the file inside this zip packet as you can see below in the **"Malware Alerts"** log.

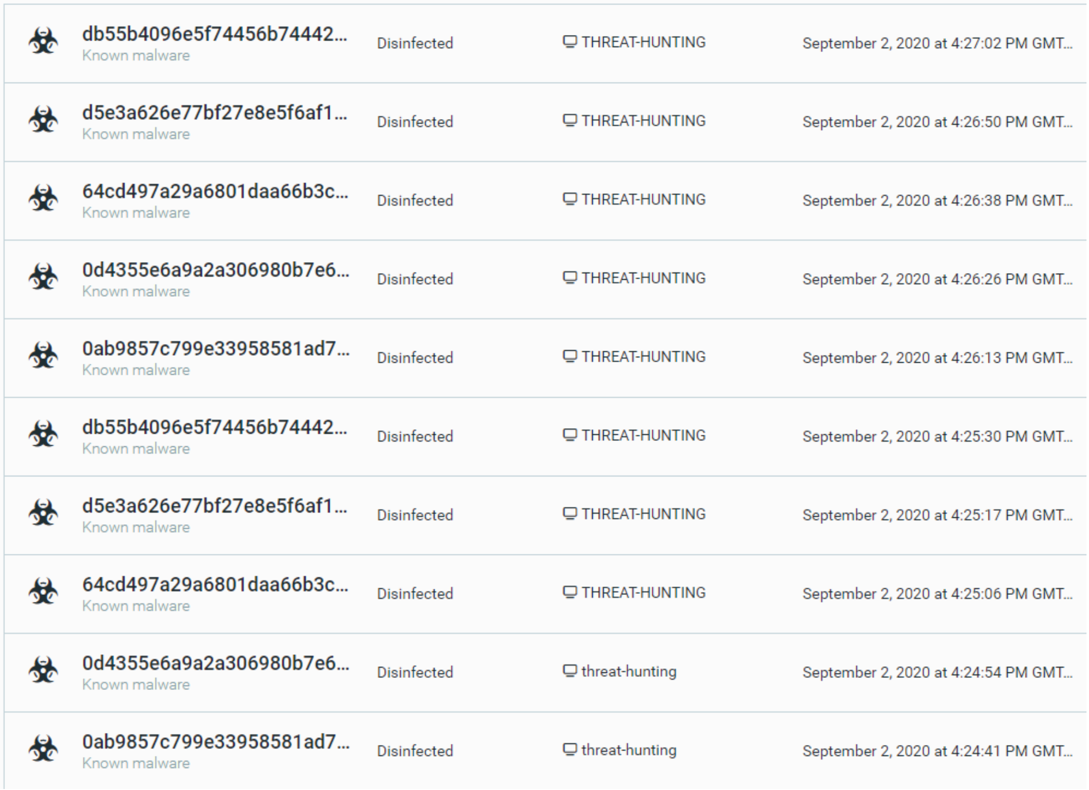


doc-scan11713_pdf.exe Known malware	Disinfected	🖵 threat-hunting	September 2, 2020 at 4:08:32 PM GMT...
Description Known malware was detected		Detection name f0dc7ded13463bae07d94e666ede8b50	Path c:\users\thor\documents\lab\cybereason\second_testing\bazaar.abuse\doc-scan11713_pdf.exe

Image 1.11: Detection logs about Manipulations files (without execution)

After the extraction, we can notice that the malware that had not previously been detected, started to be detected, the thing here in this case, is that there was the manipulation of the files (without execution) and after almost 20min he performed the ***disinfected*** action.

So, the question here is, how is it works? Detection by pattern? Signature? NGAV? ML?



db55b4096e5f74456b74442... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:27:02 PM GMT...
d5e3a626e77bf27e8e5f6af1... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:26:50 PM GMT...
64cd497a29a6801daa66b3c... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:26:38 PM GMT...
0d4355e6a9a2a306980b7e6... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:26:26 PM GMT...
0ab9857c799e33958581ad7... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:26:13 PM GMT...
db55b4096e5f74456b74442... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:25:30 PM GMT...
d5e3a626e77bf27e8e5f6af1... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:25:17 PM GMT...
64cd497a29a6801daa66b3c... Known malware	Disinfected	🖵 THREAT-HUNTING	September 2, 2020 at 4:25:06 PM GMT...
0d4355e6a9a2a306980b7e6... Known malware	Disinfected	🖵 threat-hunting	September 2, 2020 at 4:24:54 PM GMT...
0ab9857c799e33958581ad7... Known malware	Disinfected	🖵 threat-hunting	September 2, 2020 at 4:24:41 PM GMT...

Image 1.9: Malware Alerts Detection

2 Impact

At the end of this test, it was possible to verify that there were **5 known malware** that, when executed inside the environment, may perform an infection.

- **Problem during the first test - unzipping ZIP file (detection time)**
  - During this test it was possible to see that the Cybereason Endpoint Solution took almost 30 min to realize all detections in our environment test, that is, if the attack happened in the same time in the victim, this user could click in anyone of the samples and could be infected, because it's not clear how works the prevalence, maybe priority of the engine in the detection flow.
- **Malicious Zip NOT Detected**
  - As we can see the sample (`0ab9857c799e33958581ad7b2b0a4e03e89e9f0ebfe204387fee5ed647ebd78f.zip`) it's not detected like a Malicious, we used three different source to prove that is sample it's malicious.
- **File Manipulation (no execution) Problem during second test - unzipping ZIP file (detection time)**
  - During the last test it was possible to see that the Cybereason Endpoint Solution took almost 20 min to realize all detections in our environment test, that is, if the attack happened in the same time in the victim, this user could click in anyone of the samples and could be infected, because it's not clear how works the prevalence, maybe priority of the engine in the detection flow, but in this case, we are talking about just 10 malwares, that is, there was the manipulation of the files (without execution) and "just" after almost 20min he got performed the ***disinfection*** action.

MALWARE INFORMATION

- **Backdoor.Linux.BASHLITE.SMJC3 | Unix Dropper MIRAI**

`hxxps://bazaar.abuse.ch/sample/0d4355e6a9a2a306980b7e6fda7cdc04fdce2864dc8845a24b400e6196c70dc5/`

This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

Backdoor Routine

This Backdoor executes the following commands from a remote malicious user:

UDP - UDP flood or UDP flood with random strings

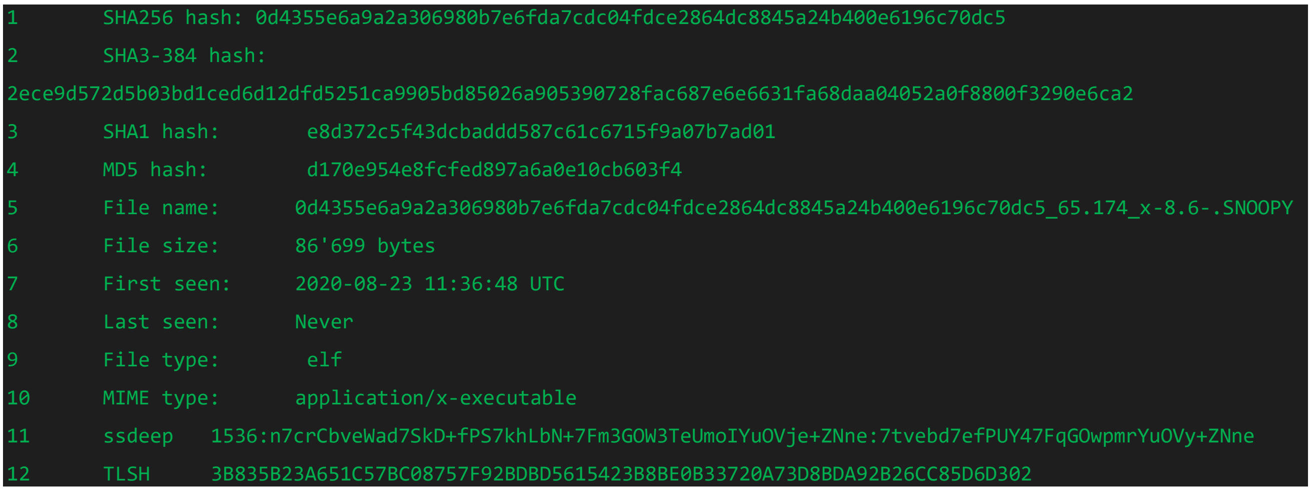
XMAS - TCP flood (flags are set to high)

VSE - VSE flood or VSE flood with random strings

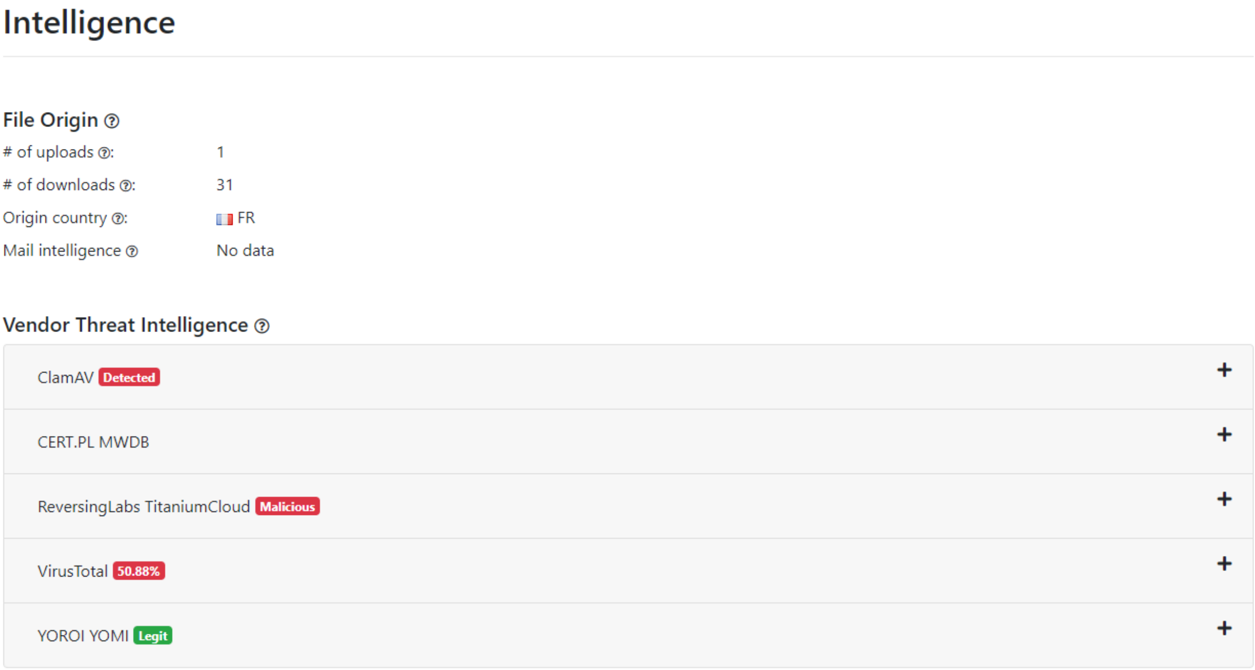
TCP - TCP flood with a flag set to high or all flags set to high (XMAS)

STD - UDP flood with specific strings.

HEX STOP - stop bot operation



```
        SHA256 hash: 0d4355e6a9a2a306980b7e6fda7cdc04fdce2864dc8845a24b400e6196c70dc5
        SHA3-384 hash:
2ece9d572d5b03bd1ced6d12dfd5251ca9905bd85026a905390728fac687e6e6631fa68daa04052a0f8800f3290e6ca2
        SHA1 hash:       e8d372c5f43dcbaddd587c61c6715f9a07b7ad01
        MD5 hash:        d170e954e8fcfed897a6a0e10cb603f4
        File name:      0d4355e6a9a2a306980b7e6fda7cdc04fdce2864dc8845a24b400e6196c70dc5_65.174_x-8.6-.SNOOPY
        File size:      86'699 bytes
        First seen:     2020-08-23 11:36:48 UTC
        Last seen:      Never
        File type:       elf
        MIME type:      application/x-executable
        ssdeep   1536:n7crCbveWad7SkD+fPS7khLbN+7Fm3GOW3TeUmoIYuOVje+ZNne:7tvebd7efPUY47FqGOwpmrYuOVy+ZNne
        TLSH     3B835B23A651C57BC08757F92BDBD5615423B8BE0B33720A73D8BDA92B26CC85D6D302
```



Intelligence

File Origin ⓘ

# of uploads ⓘ:	1
# of downloads ⓘ:	31
Origin country ⓘ:	FR
Mail intelligence ⓘ	No data

Vendor Threat Intelligence ⓘ

ClamAV Detected +

CERT.PL MWDB +

ReversingLabs TitaniumCloud Malicious +

VirusTotal 50.88% +

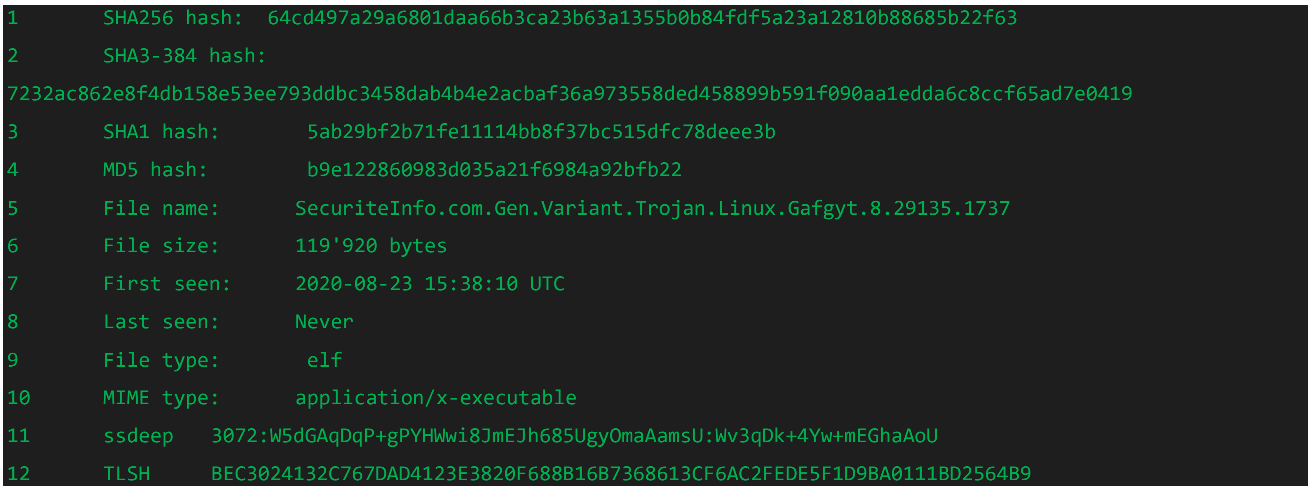
YOROI YOMI Legit +

Image 1.11: Backdoor.Linux.BASHLITE – MalwareBazaar

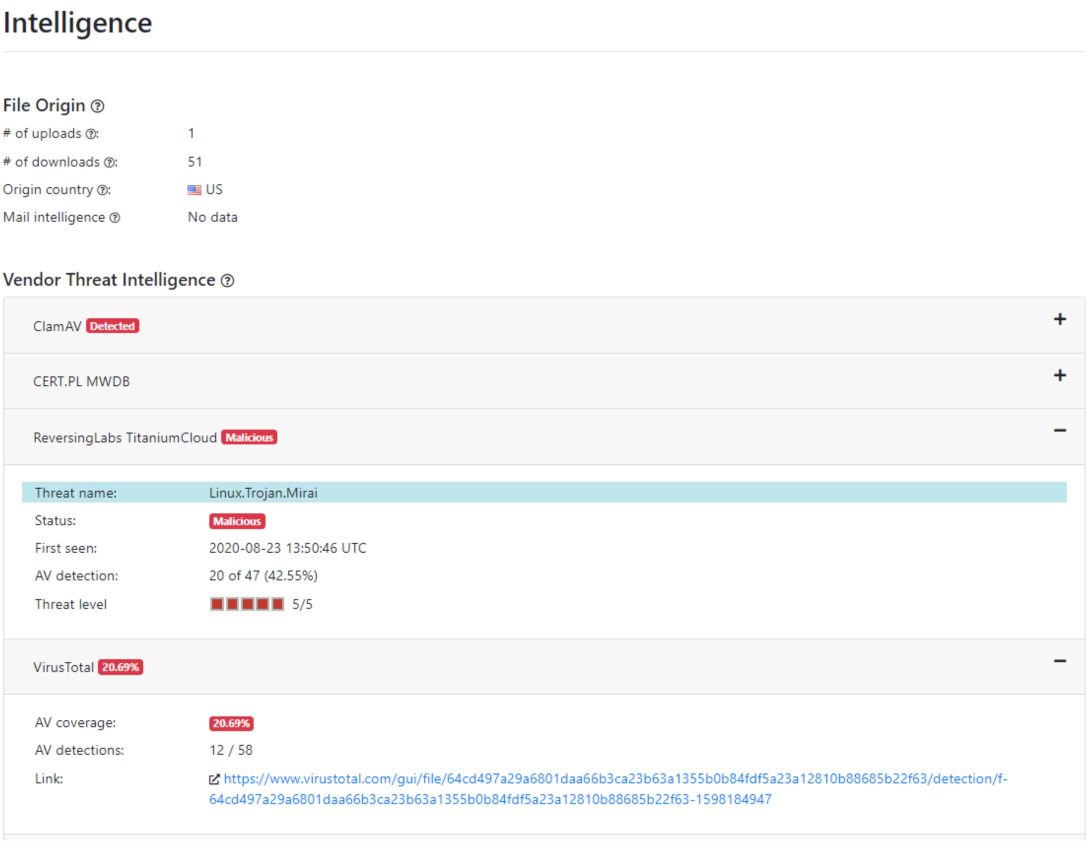
- **Gen.Variant.Trojan Linux.GAFGYT | Linux Trojan MIRAI**

hxxps://bazaar.abuse.ch/sample/64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63/

This Backdoor arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.



```
SHA256 hash:   64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63
SHA3-384 hash:
7232ac862e8f4db158e53ee793ddbc3458dab4b4e2acbaf36a973558ded458899b591f090aa1edda6c8ccf65ad7e0419
SHA1 hash:        5ab29bf2b71fe11114bb8f37bc515dfc78deee3b
MD5 hash:         b9e122860983d035a21f6984a92bfb22
File name:       SecuriteInfo.com.Gen.Variant.Trojan.Linux.Gafgyt.8.29135.1737
File size:       119'920 bytes
First seen:      2020-08-23 15:38:10 UTC
Last seen:       Never
File type:        elf
MIME type:       application/x-executable
ssdeep    3072:W5dGAqDqP+gPYHWwi8JmEJh685UgyOmaAamsU:Wv3qDk+4Yw+mEGhaAoU
TLSH      BEC3024132C767DAD4123E3820F688B16B7368613CF6AC2FEDE5F1D9BA0111BD2564B9
```



Intelligence

File Origin ⓘ

# of uploads ⓘ:	1
# of downloads ⓘ:	51
Origin country ⓘ:	US
Mail intelligence ⓘ	No data

Vendor Threat Intelligence ⓘ

ClamAV Detected +

CERT.PL MWDB +

ReversingLabs TitaniumCloud Malicious −

Threat name:	Linux.Trojan.Mirai
Status:	Malicious
First seen:	2020-08-23 13:50:46 UTC
AV detection:	20 of 47 (42.55%)
Threat level	🟥🟥🟥🟥🟥 5/5

VirusTotal 20.69% −

AV coverage:	20.69%
AV detections:	12 / 58
Link:	https://www.virustotal.com/gui/file/64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63/detection/f-64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63-1598184947

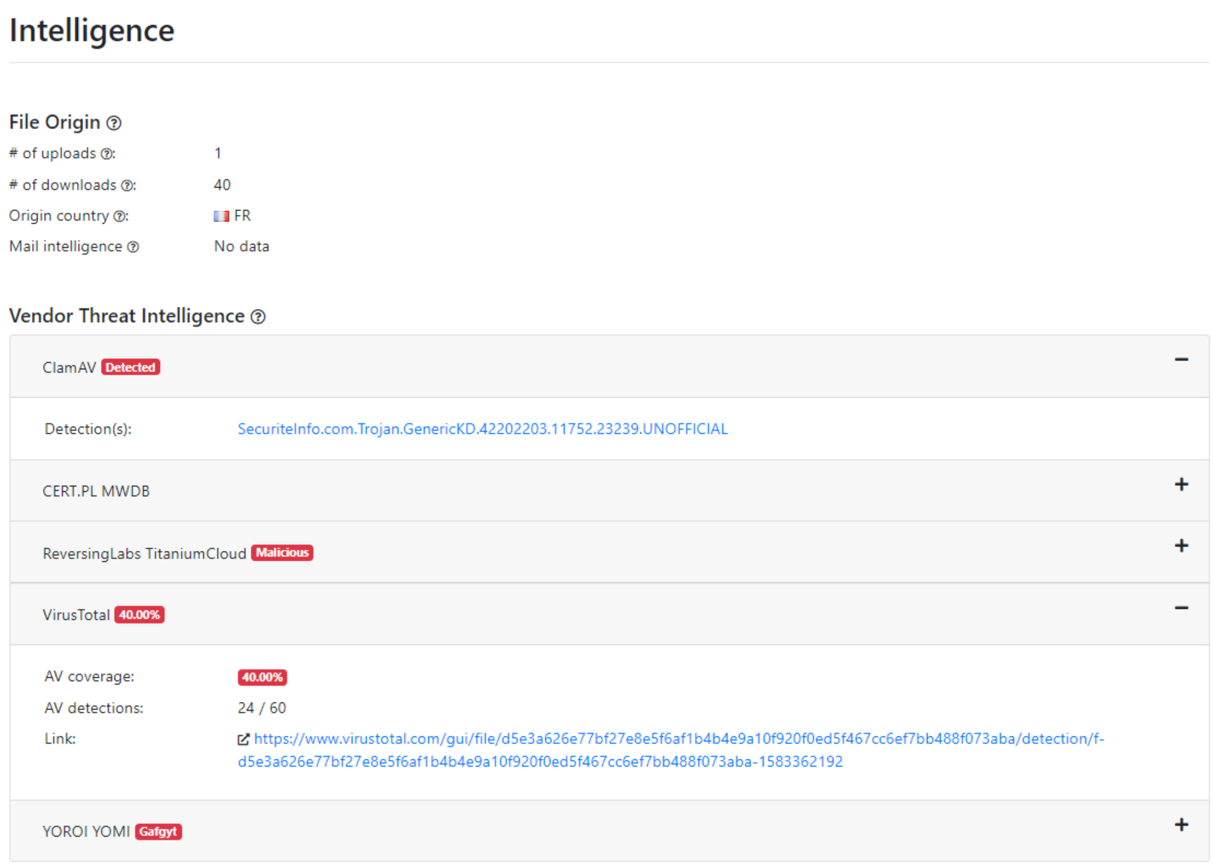
Image 1.12: Gen.Variant.Trojan Linux.GAFGYT – MalwareBazaar

- **Trojan.Linux.ZYX.USELVF319 | Trojan GenericKD**

hxxps://bazaar.abuse.ch/sample/d5e3a626e77bf27e8e5f6af1b4b4e9a10f920f0ed5f467cc6ef7bb488f073aba/

This Trojan arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. However, as of this writing, the said sites are inaccessible.

```
SHA256 hash: d5e3a626e77bf27e8e5f6af1b4b4e9a10f920f0ed5f467cc6ef7bb488f073aba
SHA3-384 hash:
0a58288993aaa631df3da8a33885d673a559ac449db90c89e0870512414d0e440fc277d11f37bc758f3dbd8944f2a0dc
SHA1 hash:       e767febe03335bf48f880edc9339892111cca672
MD5 hash:        1bbb0d45ba10d03b10b2ee581b738394
File name:      Trojan.GenericKD.42202203.11752.23239
File size:      27'512 bytes
First seen:     2020-08-23 07:39:13 UTC
Last seen:      Never
File type:       elf
MIME type:      application/x-executable
ssdeep   768:pymLLG2ABgyO4FFrkHZWlh77Ij0wkEC6rhwSy7:pymLLU1F5kHIrIj0D6rhQ
TLSH     95C2F222069B06C2CB5372B1B35075947E39829FF53F2AA9072D9719328B57C50EB3B9
```



Intelligence

File Origin

# of uploads:	1
# of downloads:	40
Origin country:	FR
Mail intelligence	No data

Vendor Threat Intelligence

ClamAV Detected

Detection(s): SecuriteInfo.com.Trojan.GenericKD.42202203.11752.23239.UNOFFICIAL

CERT.PL MWDB

ReversingLabs TitaniumCloud Malicious

VirusTotal 40.00%

AV coverage:	40.00%
AV detections:	24 / 60
Link:	https://www.virustotal.com/gui/file/d5e3a626e77bf27e8e5f6af1b4b4e9a10f920f0ed5f467cc6ef7bb488f073aba/detection/f-d5e3a626e77bf27e8e5f6af1b4b4e9a10f920f0ed5f467cc6ef7bb488f073aba-1583362192

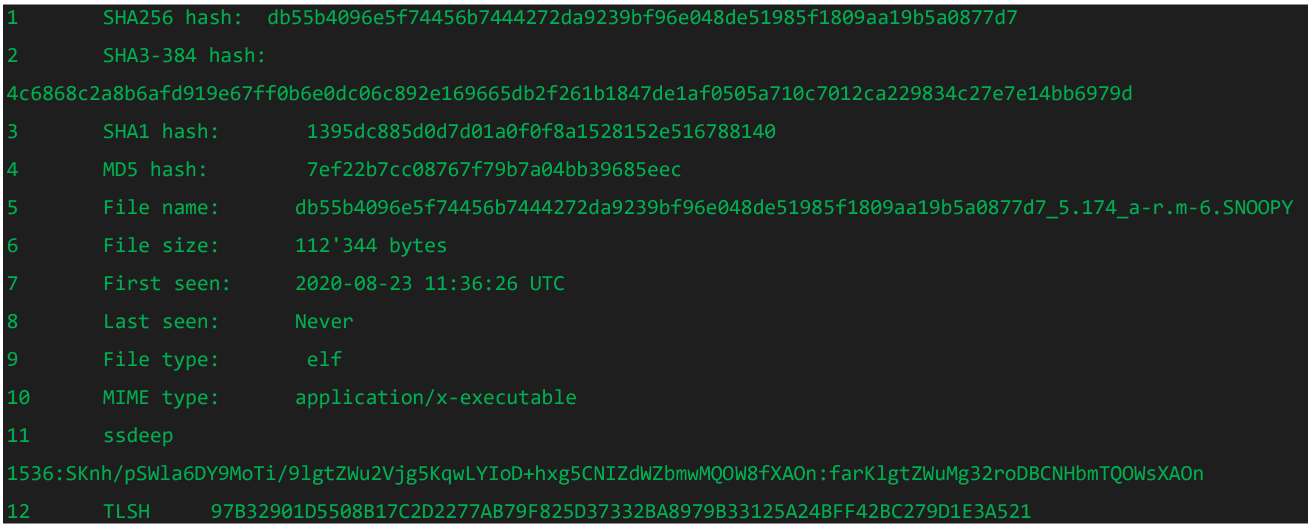
YOROI YOMI Gafgyt

Image 1.13: Trojan.Linux.ZYX.USELVF319 – Malware Bazaar

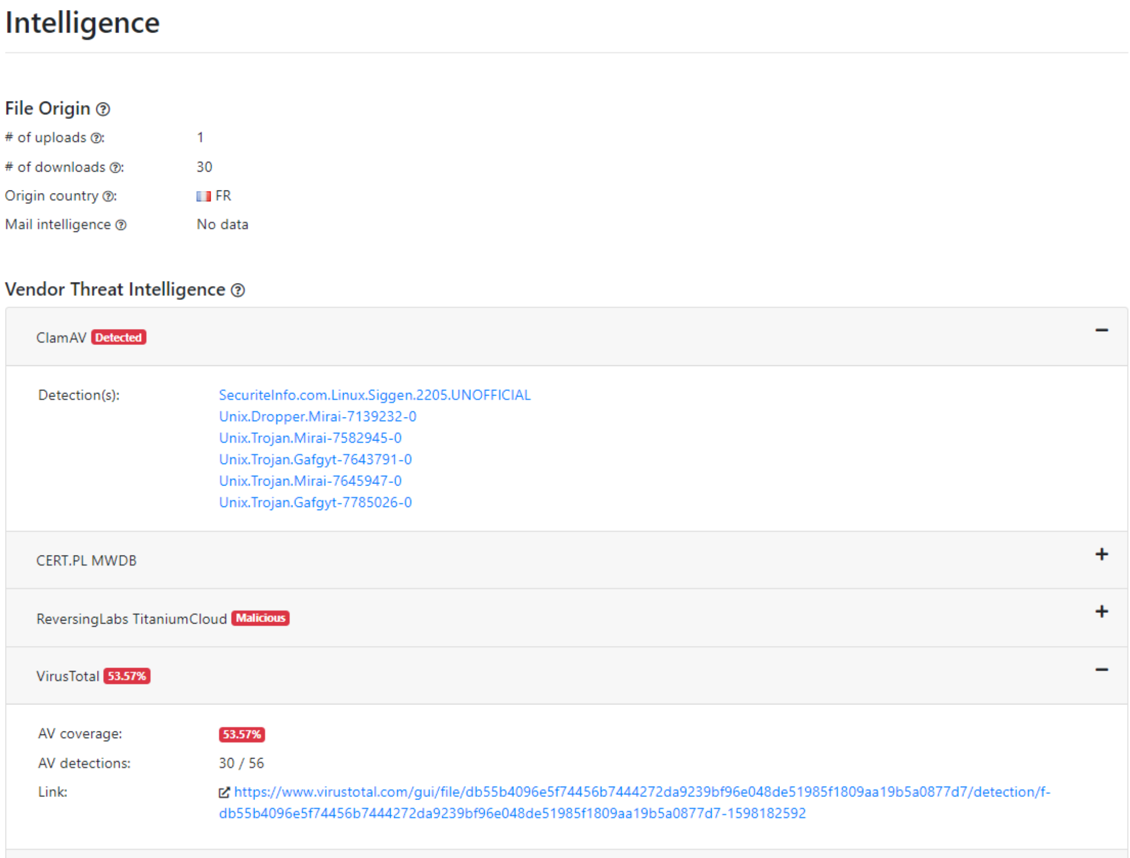
- **Backdoor.Linux.BASHLITE.SMJC2 | Unix Dropper Mirai**

hxxps://bazaar.abuse.ch/sample/db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7/

It arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. Execute commands from a malicious remote user that endangers the affected system.



```
        SHA256 hash:  db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7
        SHA3-384 hash:
4c6868c2a8b6afd919e67ff0b6e0dc06c892e169665db2f261b1847de1af0505a710c7012ca229834c27e7e14bb6979d
        SHA1 hash:       1395dc885d0d7d01a0f0f8a1528152e516788140
        MD5 hash:        7ef22b7cc08767f79b7a04bb39685eec
        File name:      db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7_5.174_a-r.m-6.SNOOPY
        File size:      112'344 bytes
        First seen:     2020-08-23 11:36:26 UTC
        Last seen:      Never
        File type:       elf
        MIME type:      application/x-executable
        ssdeep
1536:SKnh/pSWla6DY9MoTi/9lgtZWu2Vjg5KqwLYIoD+hxg5CNIZdWZbmwMQOW8fXAOn:farKlgtZWuMg32roDBCNHbmTQOWsXAOn
        TLSH     97B32901D5508B17C2D2277AB79F825D37332BA8979B33125A24BFF42BC279D1E3A521
```



Intelligence

File Origin ⓘ

# of uploads ⓘ:	1
# of downloads ⓘ:	30
Origin country ⓘ:	FR
Mail intelligence ⓘ	No data

Vendor Threat Intelligence ⓘ

ClamAV Detected −

Detection(s): SecuriteInfo.com.Linux.Siggen.2205.UNOFFICIAL
Unix.Dropper.Mirai-7139232-0
Unix.Trojan.Mirai-7582945-0
Unix.Trojan.Gafgyt-7643791-0
Unix.Trojan.Mirai-7645947-0
Unix.Trojan.Gafgyt-7785026-0

CERT.PL MWDB +

ReversingLabs TitaniumCloud Malicious +

VirusTotal 53.57% −

AV coverage:	53.57%
AV detections:	30 / 56
Link:	https://www.virustotal.com/gui/file/db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7/detection/f-db55b4096e5f74456b7444272da9239bf96e048de51985f1809aa19b5a0877d7-1598182592

Image 1.13: Backdoor.Linux.BASHLITE.SMJC2 – Malware Bazaar

3 Recommendation Actions

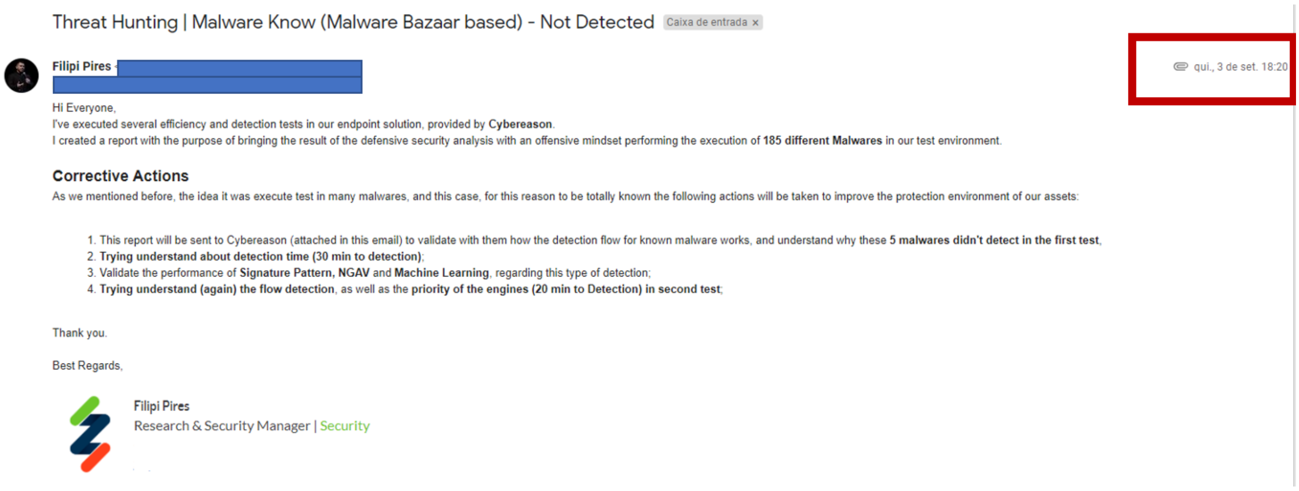
As we mentioned before, the idea it was execute test in many malwares, and this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

- This report it was sent to Cybereason to validate with them how the detection flow for known malware works, and understand why these 5 malwares didn't detect in the first test, and to try understand the detection time;
- Validate the performance of NGAV and Machine Learning, regarding this type of detection;
- The best practices of the configurations should be revalidated with the Cybereason team;
- Double checking with all policies implemented at the customer that bought the solution;

4 Answers from Cybereason Company

As we mentioned before, the idea it was execute test in many malwares, and this case to bring the result of the defensive security analysis with an offensive mindset performed in the execution of 185 different Malwares in our environment.

We opened a support case with the Cybereason support team on **September 03th** as you can see below



Threat Hunting | Malware Know (Malware Bazaar based) - Not Detected

Filipi Pires [redacted]

Hi Everyone,
I've executed several efficiency and detection tests in our endpoint solution, provided by **Cybereason**.
I created a report with the purpose of bringing the result of the defensive security analysis with an offensive mindset performing the execution of **185 different Malwares** in our test environment.

Corrective Actions

As we mentioned before, the idea it was execute test in many malwares, and this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

1. This report will be sent to Cybereason (attached in this email) to validate with them how the detection flow for known malware works, and understand why these **5 malwares didn't detect in the first test**,
2. **Trying understand about detection time (30 min to detection)**;
3. Validate the performance of **Signature Pattern, NGAV** and **Machine Learning**, regarding this type of detection;
4. **Trying understand (again) the flow detection**, as well as the **priority of the engines (20 min to Detection) in second test**;

Thank you.

Best Regards,

Filipi Pires
Research & Security Manager | Security

Image 1.15: Report to manufacturer

As this is a **Very Critical** problem, the answer should happen in 3 hours, but in some conversation with Customer Success Managers, Support Managers, Director Customers and VP from Cybereason, it was requested to wait 72 hours to us receive any answer, but it's not happened.

After 5 days (125 hours) I needed to send another email requesting some answer, and I receive another generic answer:

Apologies for the delay in response but this email will have to be escalated to our detections and product teams who will be able to answer the questions in the document with a deeper understanding. "@CustomerSucessManager" Can this email be escalated over to the support/detections team who will be able to give a better explanation on why or why not certain types of malware was detected or not.

And until now **(18/09/2020)** we didn't receive any answer provide by manufacturer.

By the end, a simple question that we need to do in those cases is:

Why didn't Cybereason detect them? ...What engine didn't work well? Or maybe, Which flow failed? Detection by pattern? Signature? NGAV? ML? We need to have (If possible) answers for these questions.