THREAT INTELLIGENCE LAB (CS-5202)

2021-2022

**YARA RULE FOR ARTRA DOWNLOADER**

**Arjun Anil (MT20ACS499)**

**Prof. Debashis Sengupta Dr. Ashu Sharma Professor and Area Director Assistant Professor**

Contents

[Artra Downloader Yara Rule 2](#_Toc80989221)

[**Artra Downloader Malware Family** 2](#_Toc80989222)

[**Details Collected from Virustotal** 2](#_Toc80989223)

[**Describing Yara Patterns** 3](#_Toc80989224)

[**Strings Explained** 4](#_Toc80989225)

# Artra Downloader Yara Rule

## **Artra Downloader Malware Family**

### **Details Collected from Virustotal**

File Type : Win32 EXE

Vhash : 034056655d15155048z18hz22z145zc2z3a1z

Authentihash : 809e1b4e7f0bcb931b25c3762fe00bb0c5427a5498ef106f1eb13f14bffba520

Imphash : 2dfea0cb99dfd178aefd42a0ebb0ea98

Threat Name : Artemis!Trojan (Trojan Downloader)

Target Machine: Intel 386 or later processors and compatible processors

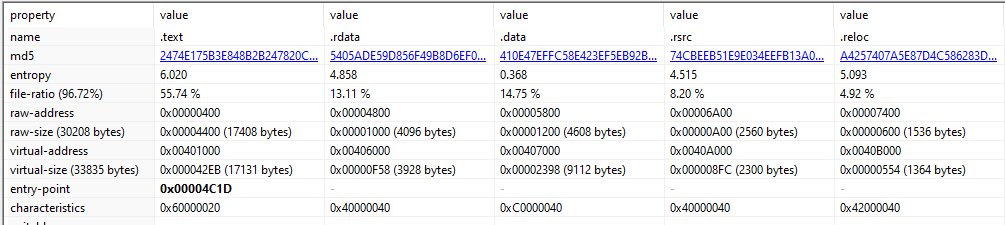
Entry Point : 19484

File Size : 30.5 kB

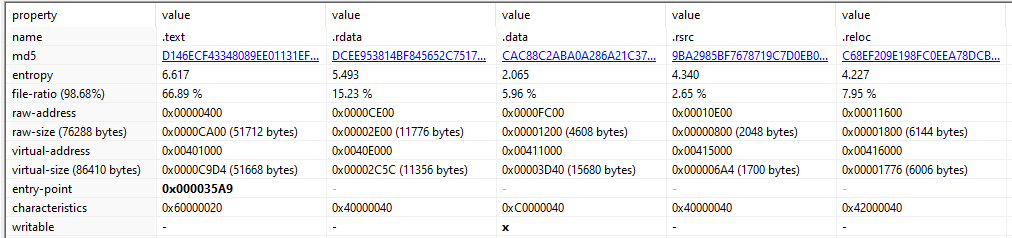
IP Traffic : 162.222.215.90:80

**From Pestudio:**

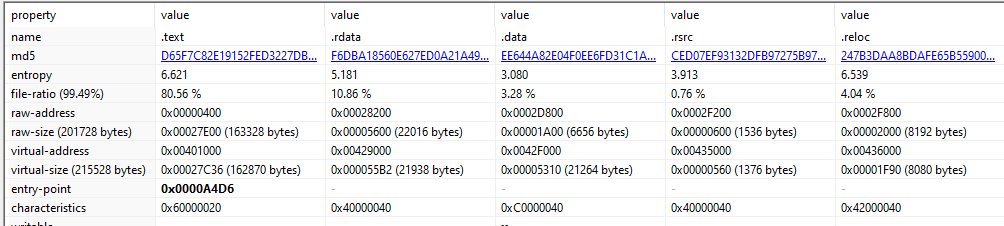
File: 0b2a794bac4bf650b6ba537137504162520b67266449be979679afbb14e8e5c0



File: ef0cb0a1a29bcdf2b36622f72734aec8d38326fc8f7270f78bd956e706a5fd57

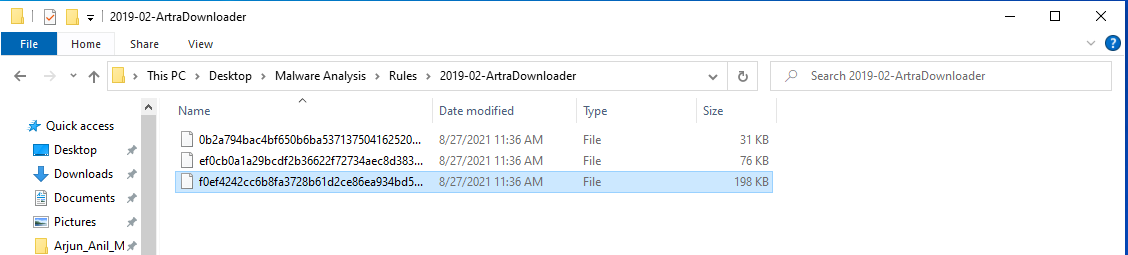


File: f0ef4242cc6b8fa3728b61d2ce86ea934bd59f550de9167afbca0b0aaa3b2c22

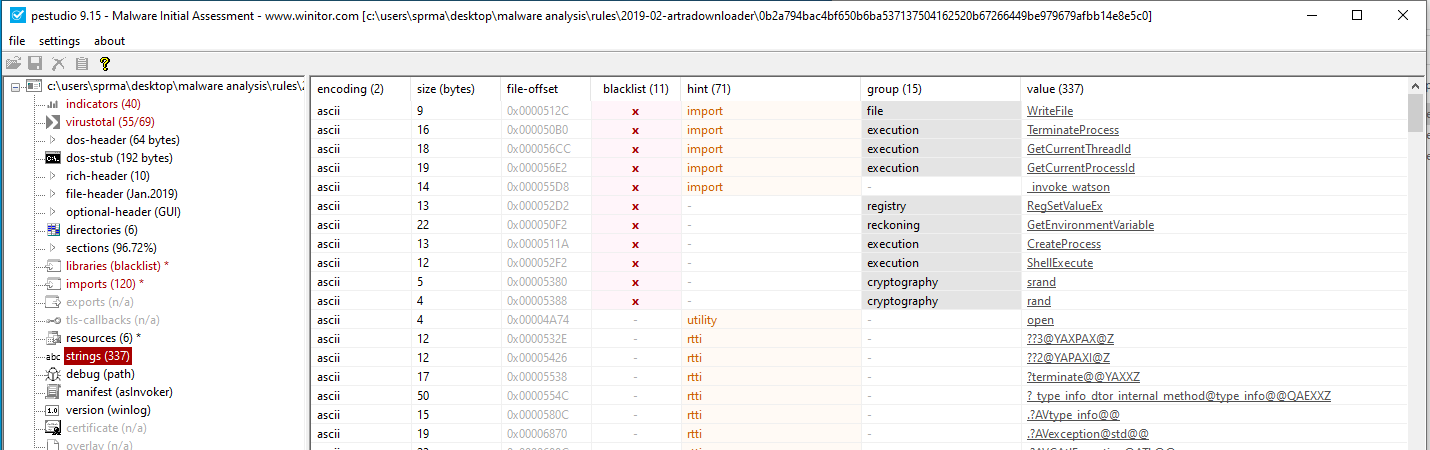


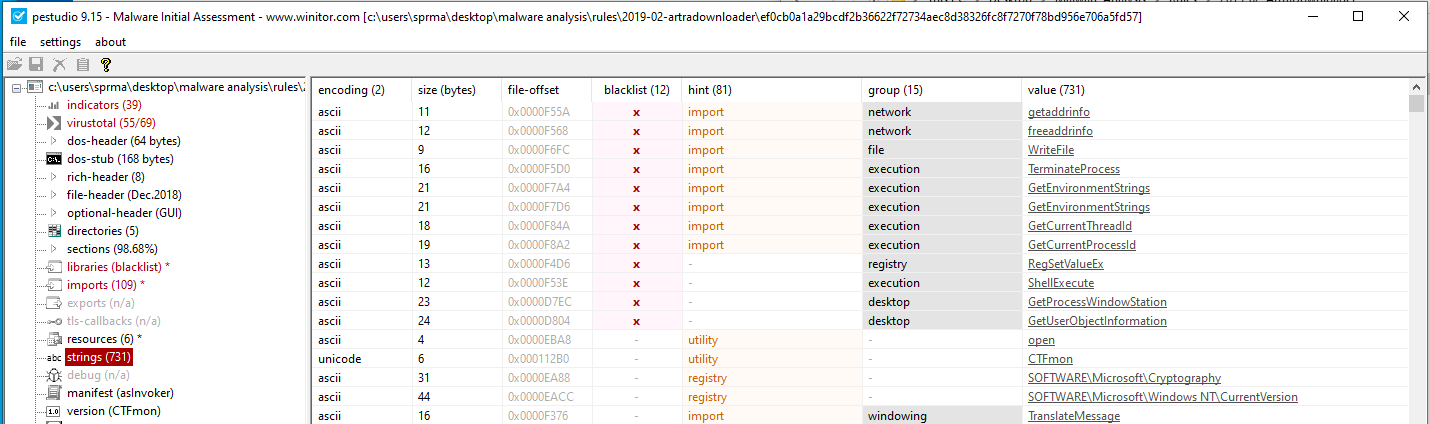
## **Describing Yara Patterns**

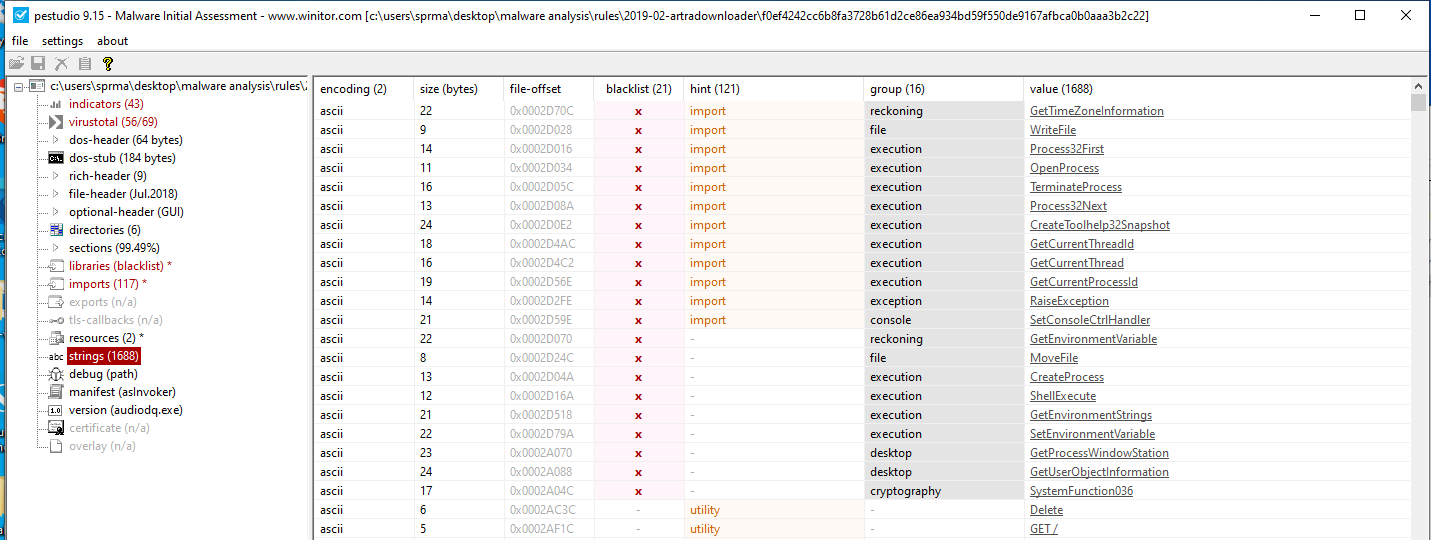
In the Artra Downloader malware family, below were the list of files for analysis.



Opened the files in pestudio and below are the list of strings on each file. Sorted the strings and selected the blacklisted strings from each malware file.







From these blacklisted strings, identified the list of strings which are appearing on all the malware files, they are : TerminateProcess, WriteFile, GetCurrentThreadId, GetCurrentProcessId and ShellExecute.

With the common strings identified, created a yara rule with condition satisfying all these strings present. The yara rule is as below:

rule search\_exe

{

meta:

author = "Arjun Anil"

date = "2021-08-26"

description = "To find malwares coming under Artra Downloader"

strings:

$a = "TerminateProcess"

$b = "WriteFile"

$c = "GetCurrentThreadId"

$d = "GetCurrentProcessId"

$e = "ShellExecute"

condition:

$a and $b and $c and $d and $e

}

### **Strings Explained**

* "TerminateProcess" : Not meant to be used in 'Release' applications. They are reserved for debugging tools and exceptional applications such as process managers. Clearly, they cause great damage to a system.
* "WriteFile"
* "GetCurrentThreadId" : Retrieves the thread identifier of the calling thread.
* "GetCurrentProcessId" : Retrieves the process identifier of the calling process.
* "ShellExecute" : Performs an operation on a specified file.