11/29/2023

Traffic Analysis Report

2024/2023

Oussama Binike
RAGHIP IT

DECLERATION

I declare that this is my own work, and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text

ABSTRACT

Cybercrime is becoming more common with each passing day, and criminals are coming up with new ways to destroy their targets through propagating worms and malware. In a fast – changing world technologies and innovations are released on a daily basis; it is possible to attack a system and exploit the system's vulnerabilities. Malware's impact, according to studies, is worsening. Malware is any harmful software that is designed to carry out malicious actions on a computer system. Virus, worms, backdoors, trojans, backdoors and adware are some examples for malwares.

There are various kind of malware analysis such as dynamic analysis, static analysis and behavior analysis. There are some drawbacks to static malware analysis. Dynamic malware analysis is the preferred method of malware analysis, and it can be done with a variety of tool and techniques.

INTRODUCTION

Malware is an abbreviation for malicious software, which is meant to harm a computer without the user's knowledge. There are various kind of malwares such as viruses, trojans, worms, spywares and rootkits. Malware is a key element of several vulnerabilities. Companies struggle to comprehend the malware that they come across. Understanding how to detect malware allows you to take control of the situation. The process of determining the objective and features of a given malware sample, such as a virus, worm, or Trojan horse, is known as malware analysis. The procedure is required in order to build efficient detecting tools for malicious programs. Static analysis tools attempt to analyze a binary without actually running it. After a binary has been executed, live analysis techniques will examine its behavior. Static analysis refers to the process of evaluating software without running it. There are various kind of static analysis techniques. Additionally, useful information can be retrieved by exploiting the metadata of a specific file format. It includes a number on UNIX, that may indicate the type of the file. A lot of information can be gathered like the compilation time stamp, imports and exports. Mostly malwares are in obfuscated format. It is done by using packers. When the malware is packed it is hard to recover. Major part of static analysis is the disassembly. It is done with tools like IDA Pro, that are able of reversing machine code to assembly language. Because the source code is not executed in static analysis, it is more secure than dynamic analysis. Dynamic malware analysis is the process of analyzing malware within a controlled environment. It is done in order to analyze the behavior of the malware. This is conducted with the use of a sandbox. And the sandbox is a controlled environment that is used to isolate the process of malware. The malware analysis report covers the malicious attacks that Stark Industries had to deal with. The figure below illustrates the malware analysis process that was used during the analysis.

static analysis

Static analysis of network traffic pcap (Packet Capture) files using Wireshark involves examining captured data without actively monitoring live network communication. These pcap files contain a record of the packets exchanged between devices on a network during a specific time frame. Wireshark, a popular open-source network protocol analyzer, provides a comprehensive platform for dissecting and interpreting the contents of these pcap files.

Network Incident Details for Victim Device

table provides details related to a network incident and specifying that the information pertains to a victim device

victim's ip address	victim's mac address	victim's windows host name	victim's windows user account name
10.4.19.138	**00:90:27:cd:92:90**	**DESKTOP-RETP4BU**	**irichardson**

Network Incident Report: Potentially Malicious File Download from IP 10.4.19.138

The user, identified with IP address **10.4.19.138** on **'Wed, 19 Apr 2023 17:17:11 GMT'** began downloading a potentially malicious zip file **'643d0491bcea1.zip'** from the host located at **'cotecsecuritygroup.com'**

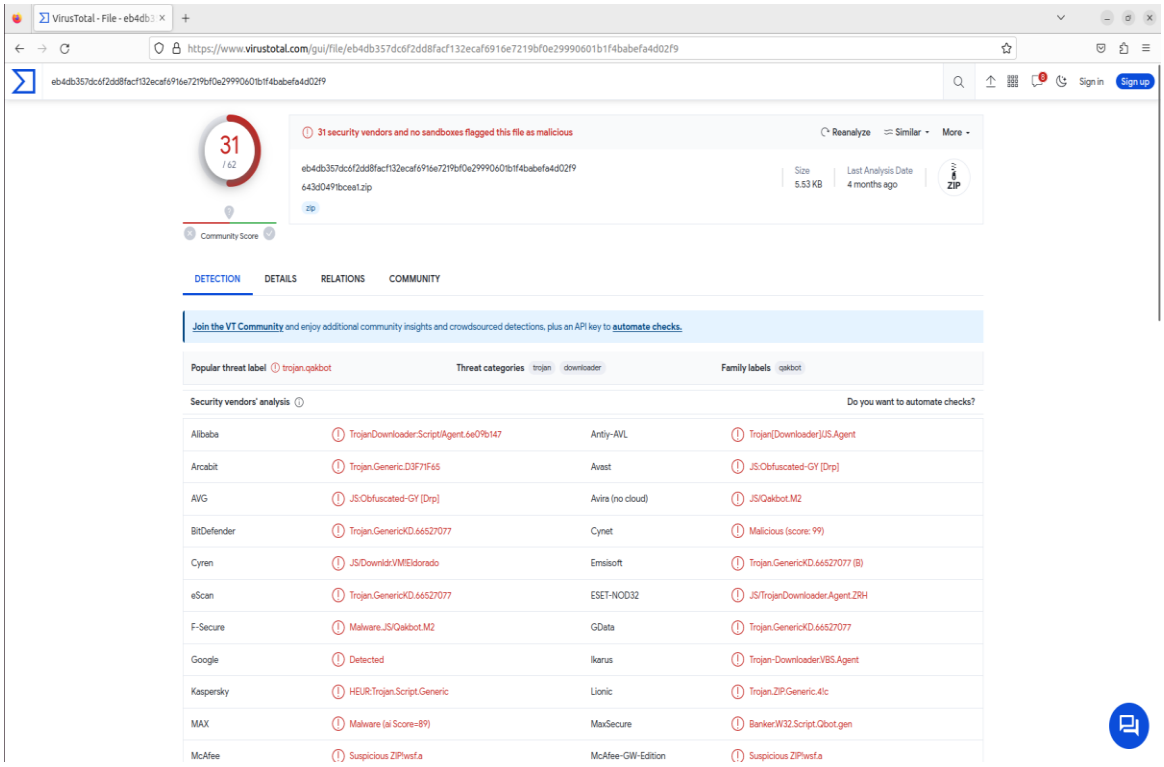
Malicious file hashes:

MD5 b054104df97949cbeb3da2290da0cf40

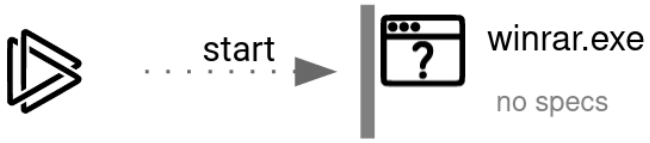
SHA-1 4e72f94fe91d16bb46707bd8a2750b6357dc0648

SHA-256 eb4db357dc6f2dd8facf132ecaf6916e7219bf0e29990601b1f4babefa4d02f9

The compressed file is infected with malware



Behavior graph



Urls in the same IP

	Blacklist	Reason	TTL	ResponseTime
LISTED	UCEPROTECTL3	66.29.147.117 was listed Detail	2100	10

Variants and Related Files

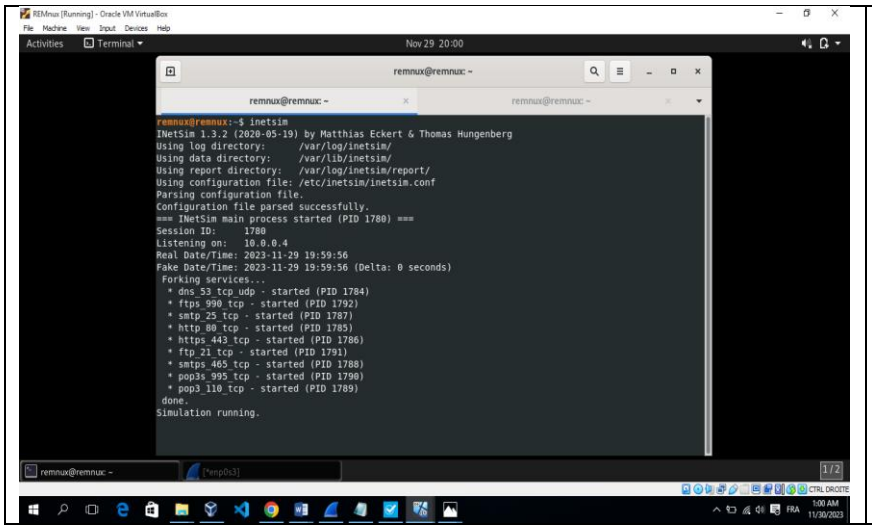
Malwere / Variants	**Client.zip**
File info	Zip archive data, at least v2.0 to extract
Malware Analyst Date	May 27, 2023 at 22:46:52
Last Analysis	2023-07-14 17:21:28
malwer's name	643d0491bcea1.zip, 054104df97949cbeb3da2290da0cf40.virus
straings and flous output	Complaint_Copy_634917.wsf Complaint_Copy_634917.wsf
MIME	application/zipFile

Running Malware in a Sandbox

Sandboxes provide a secure and isolated space for the execution of malware. By confining the malware within a controlled environment, researchers can prevent it from causing harm to the primary system or network

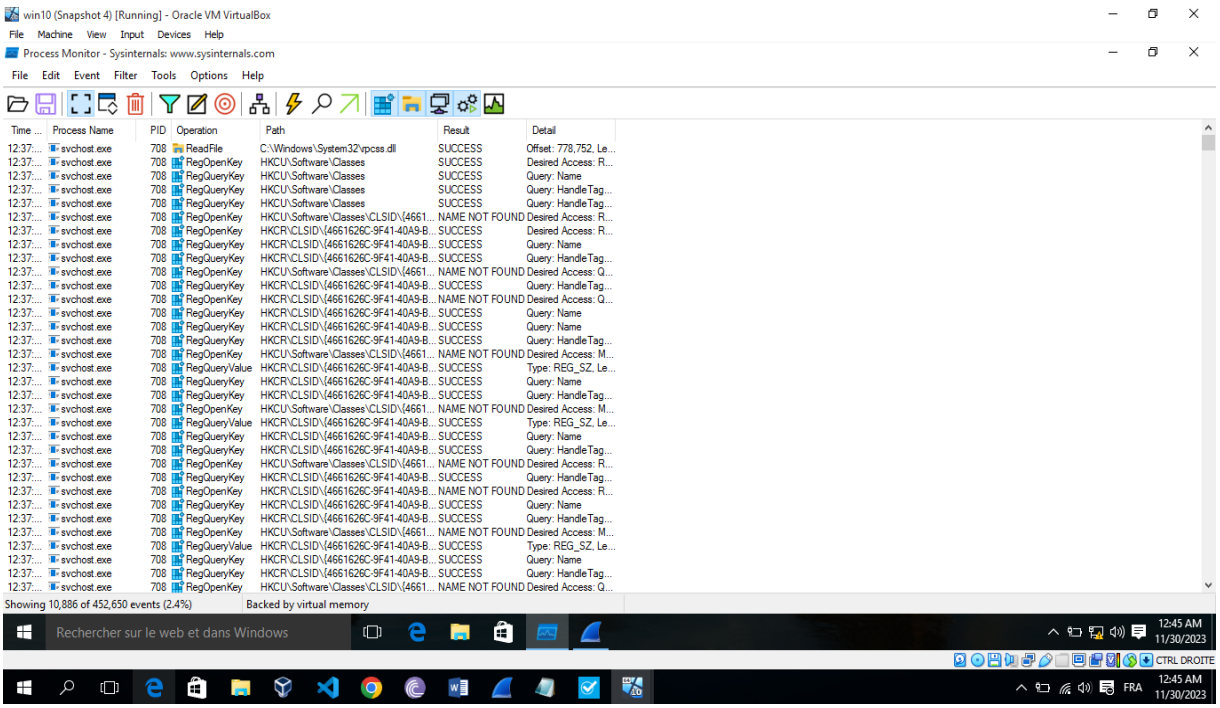
Sandbox

For the purpose of sandbox analysis, we will utilize both Romnux and Windows environments



Process name

svchost.exe	system



Connection

Protocol	PID	Process name	IP	Port
UDP	708	svchost.exe	239.255.255.250	1900
UDP	708	svchost.exe	224.0.0.252	5355