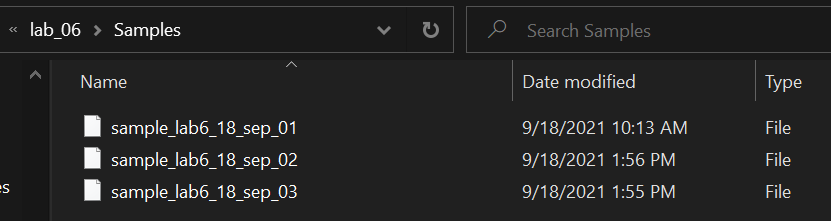
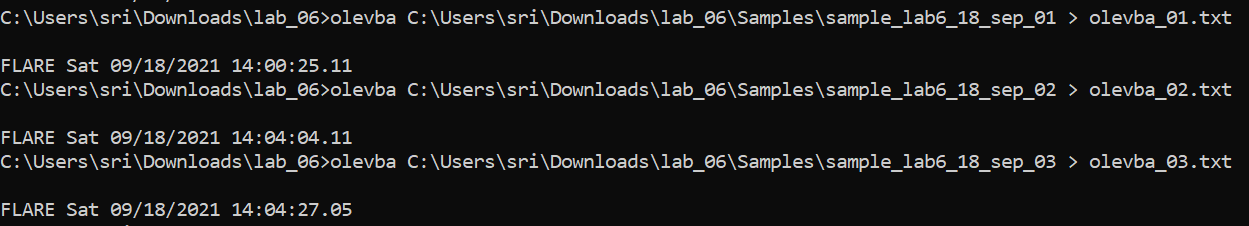
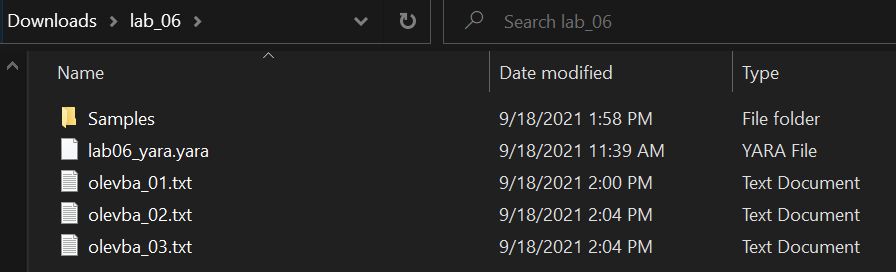
**Type of File** 🡪 Macro – VBA

**Static Analysis** 🡪 using olevba, pestudio, Microsoft strings, Virustotal, InQuest labs

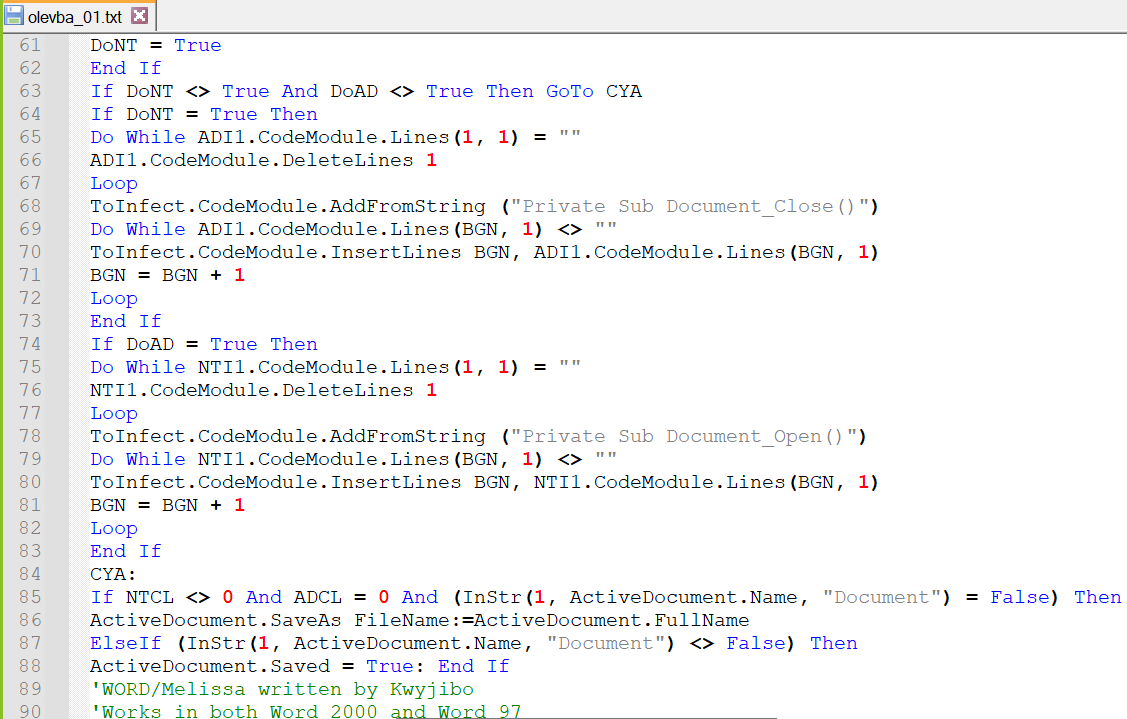


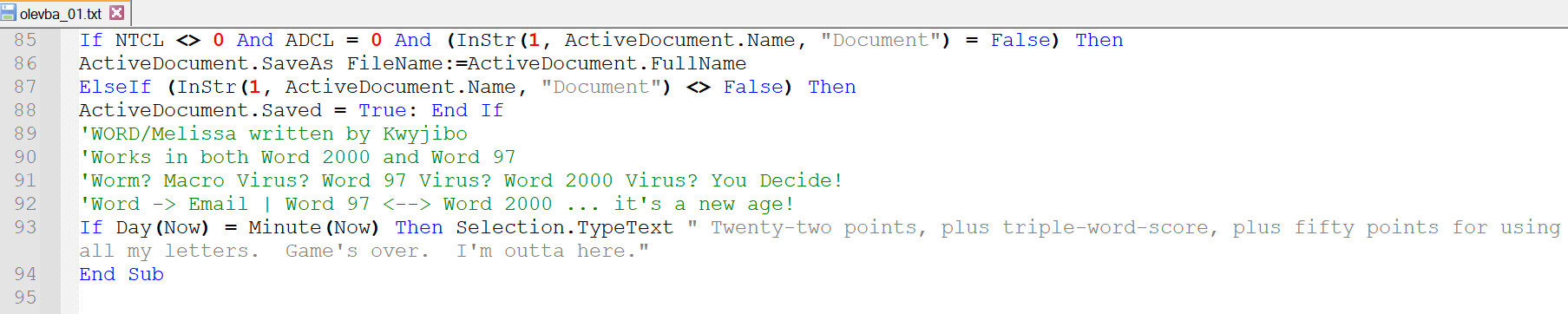


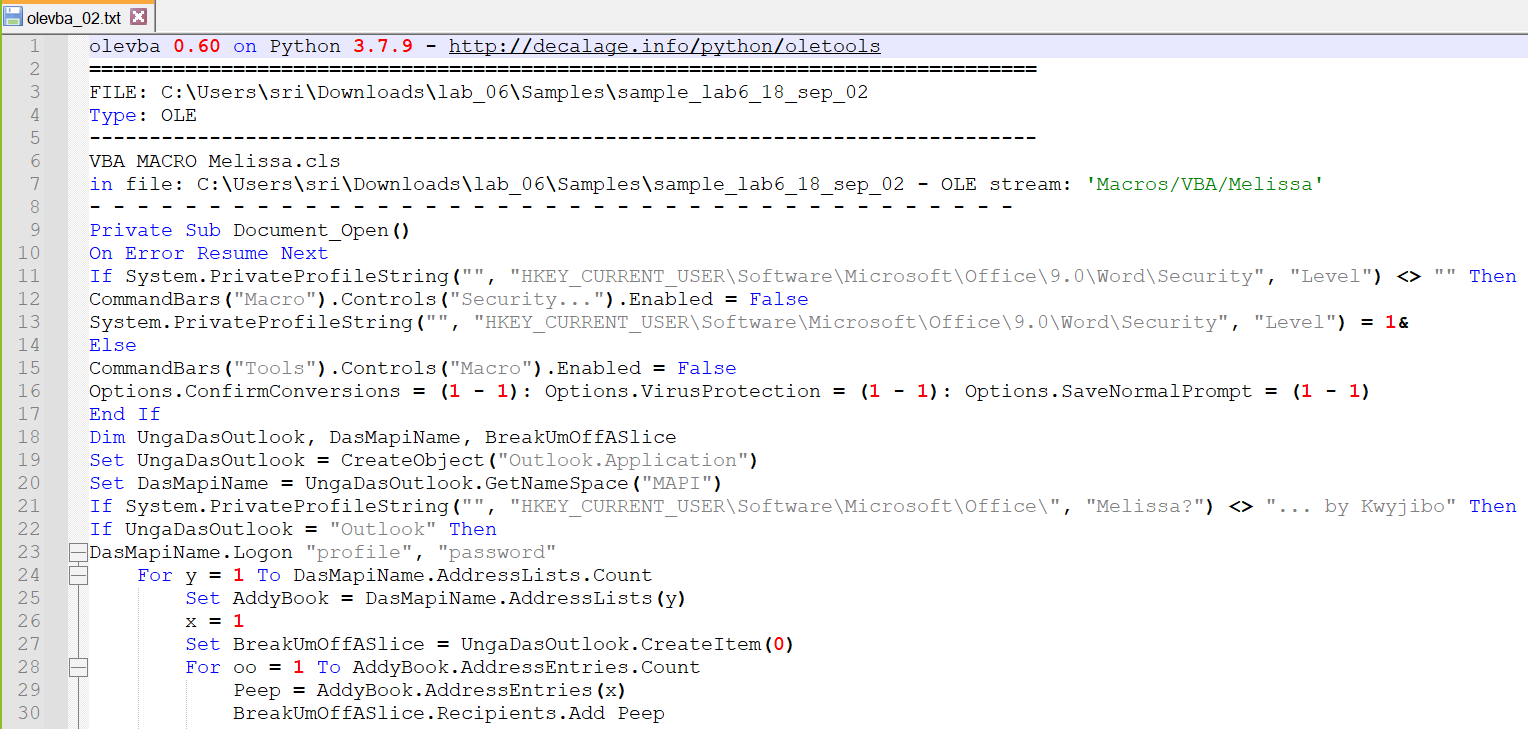


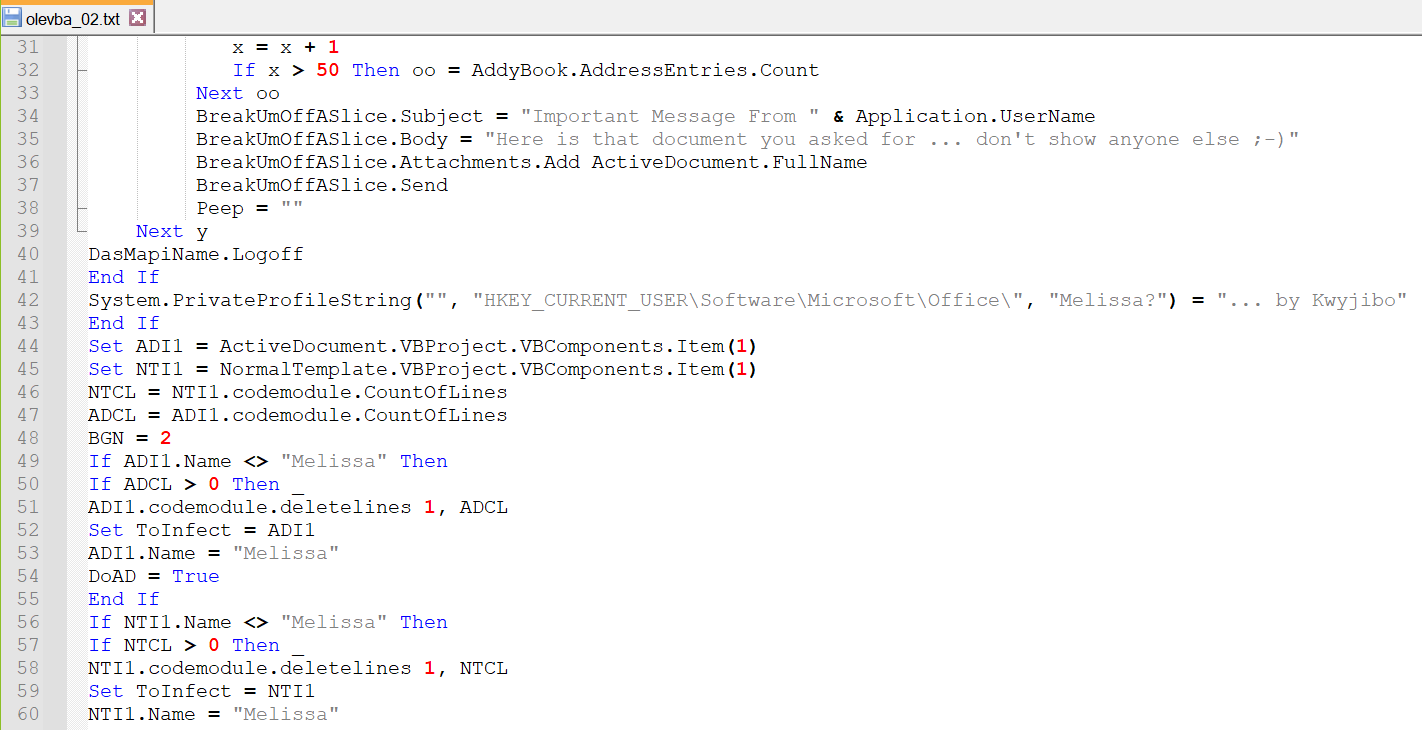




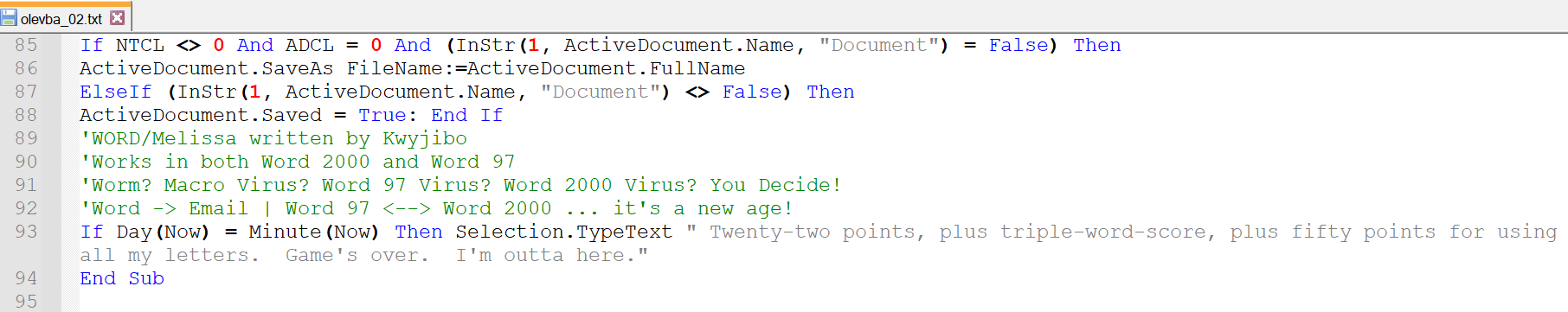


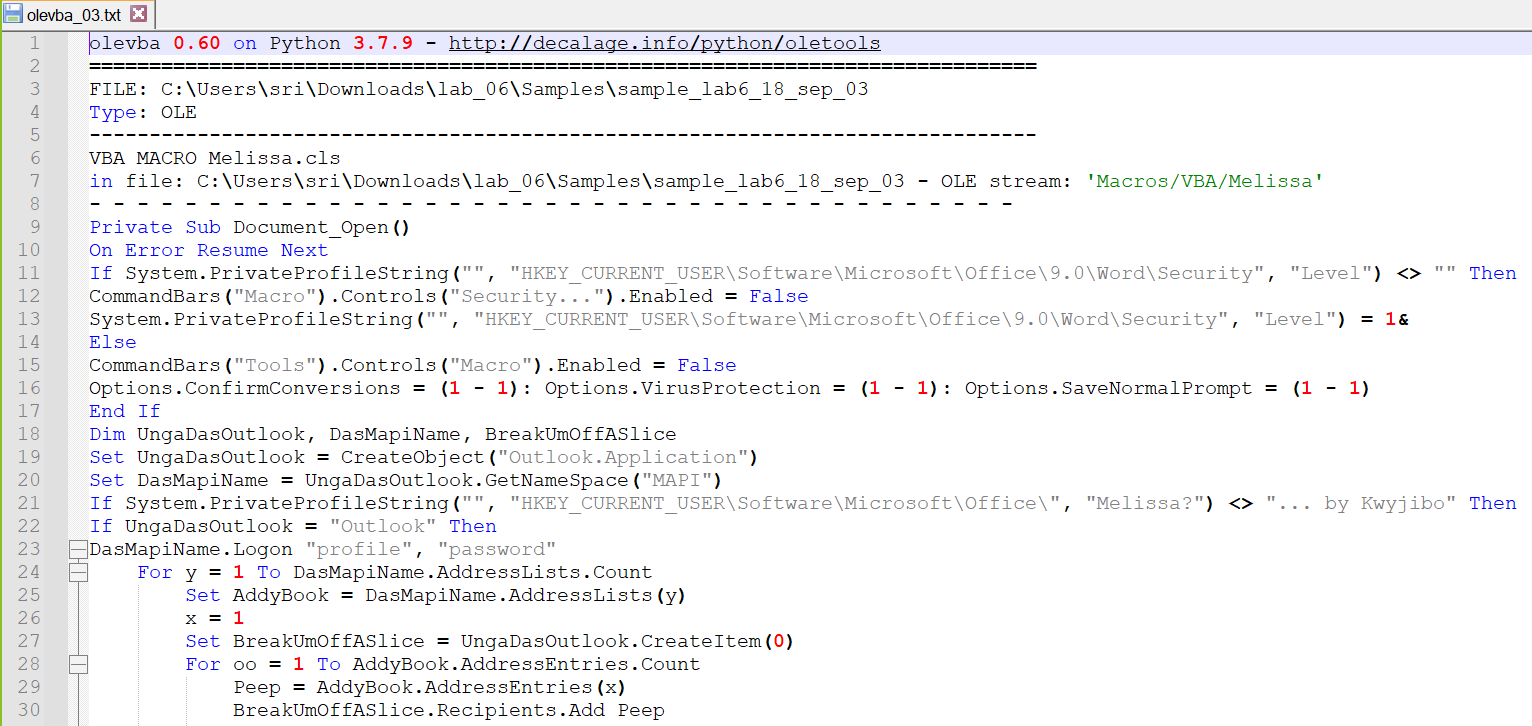


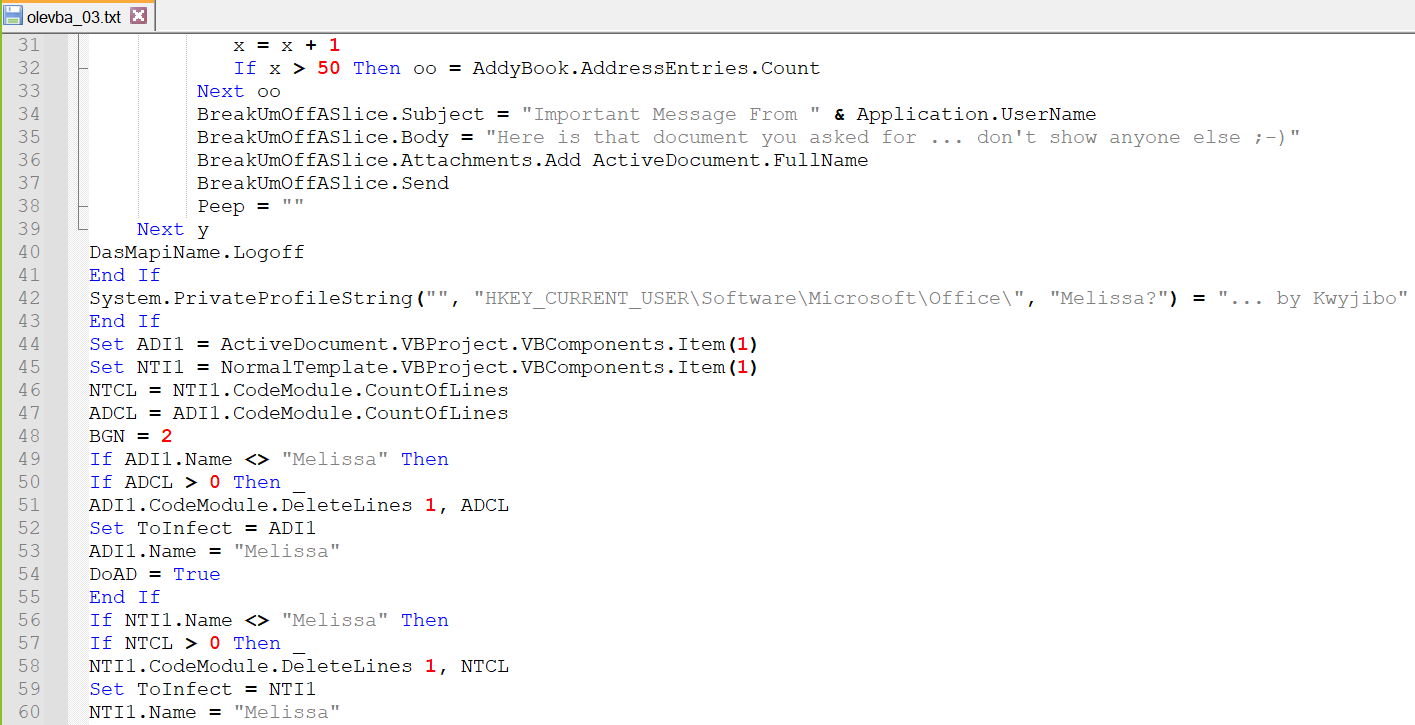


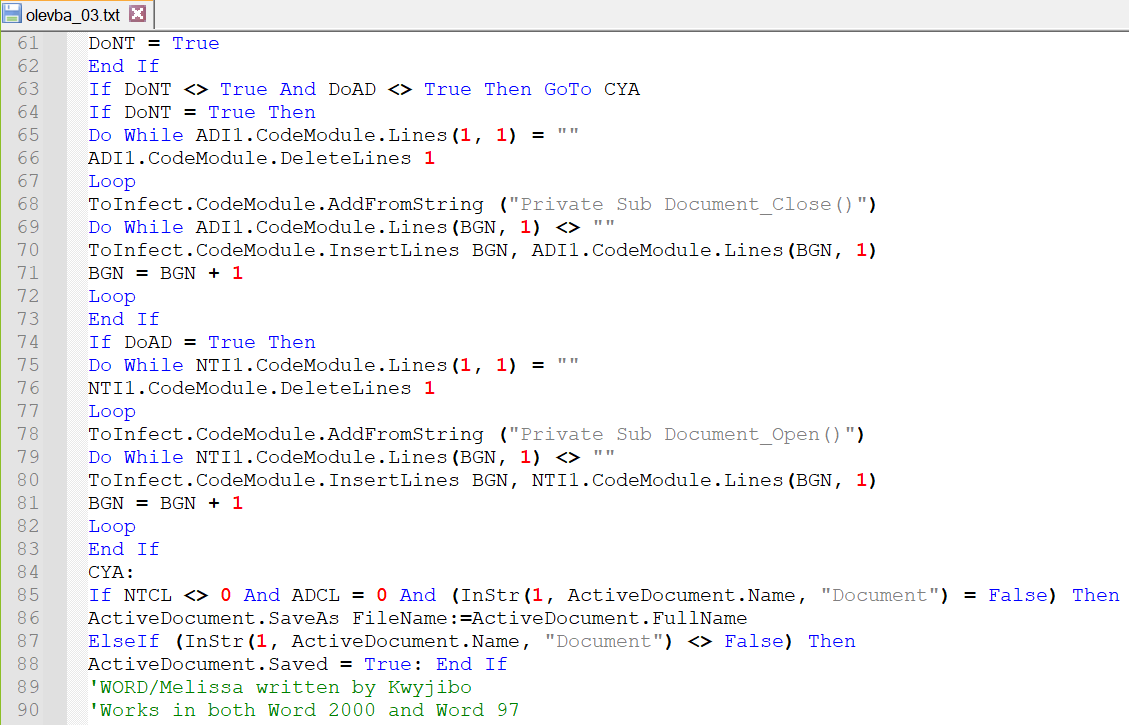


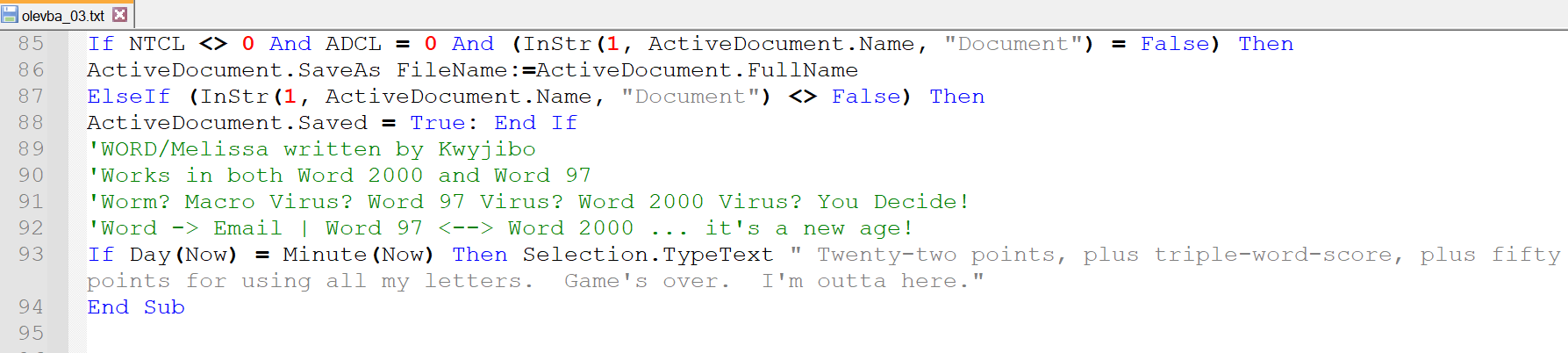


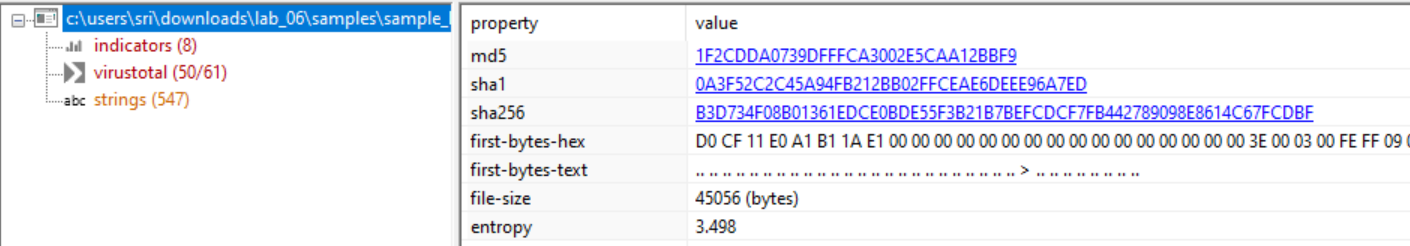


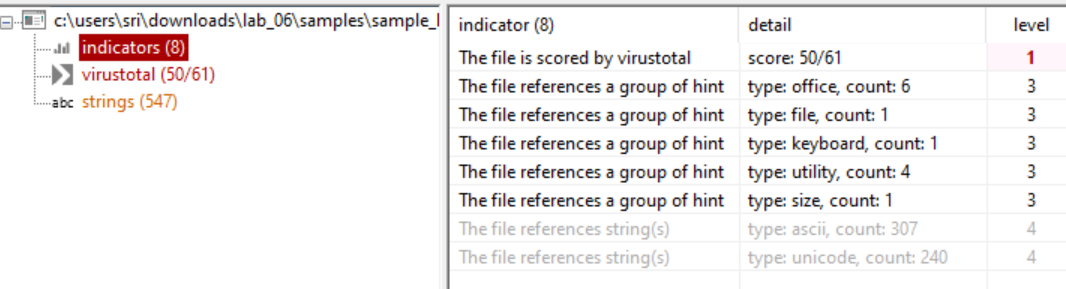


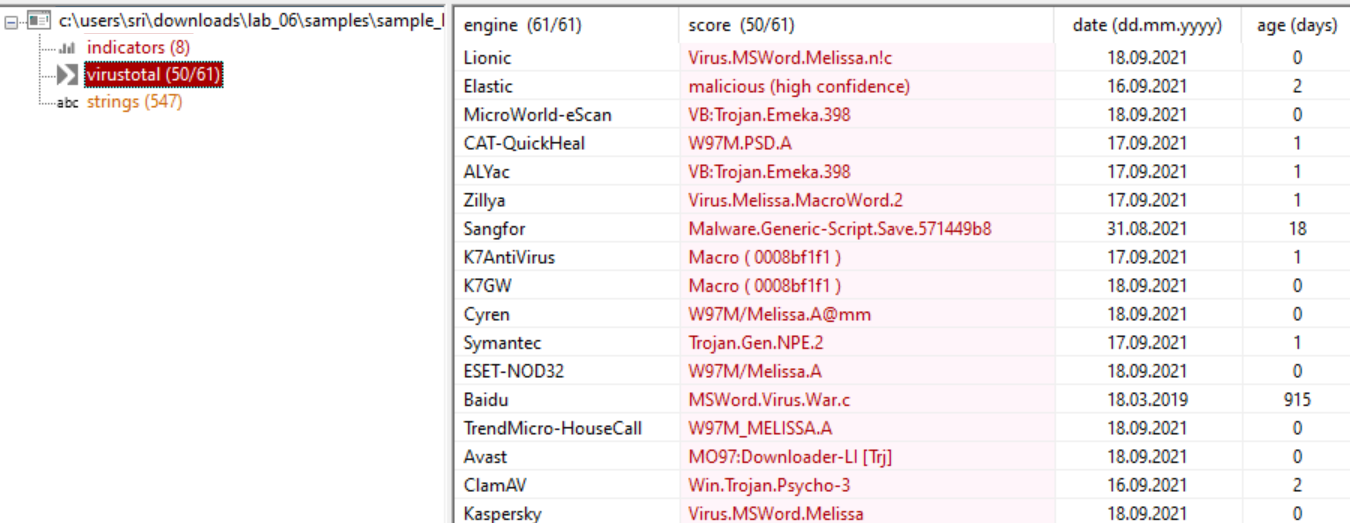




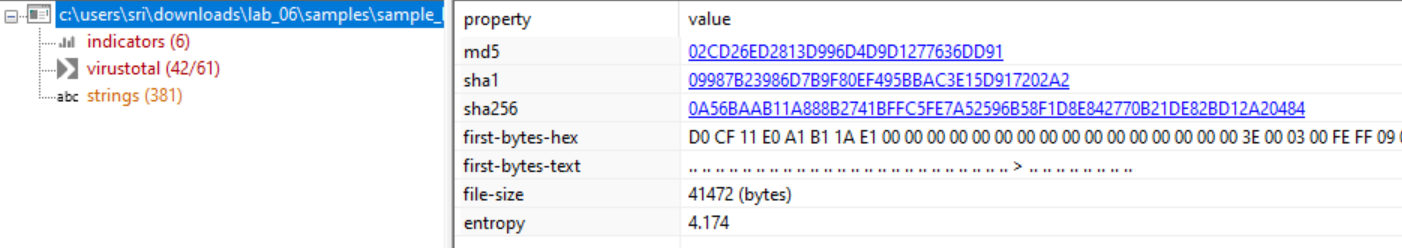


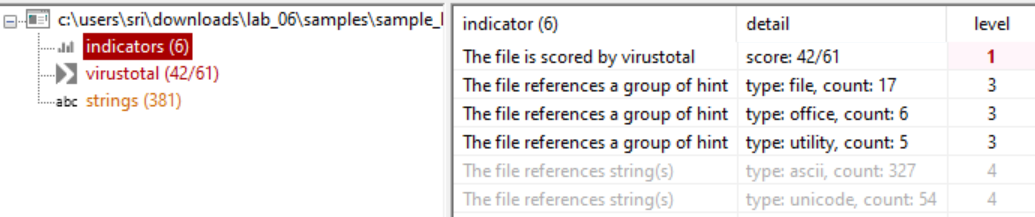


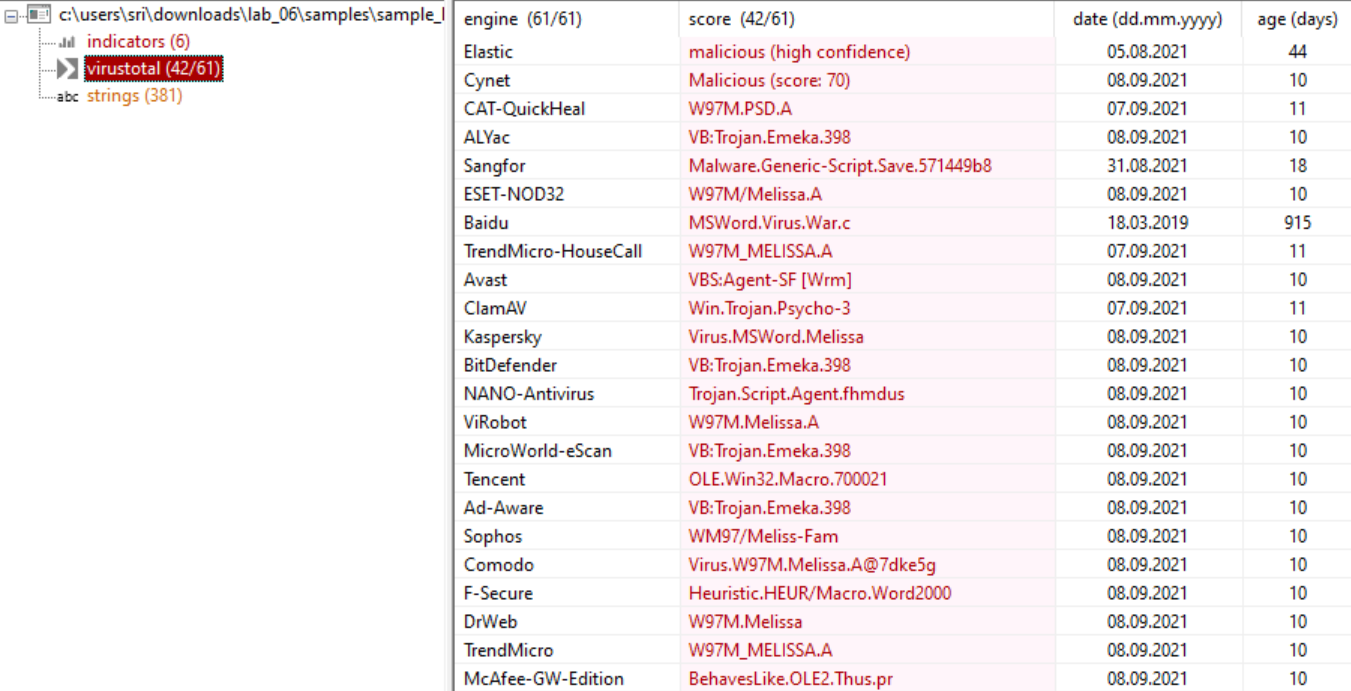


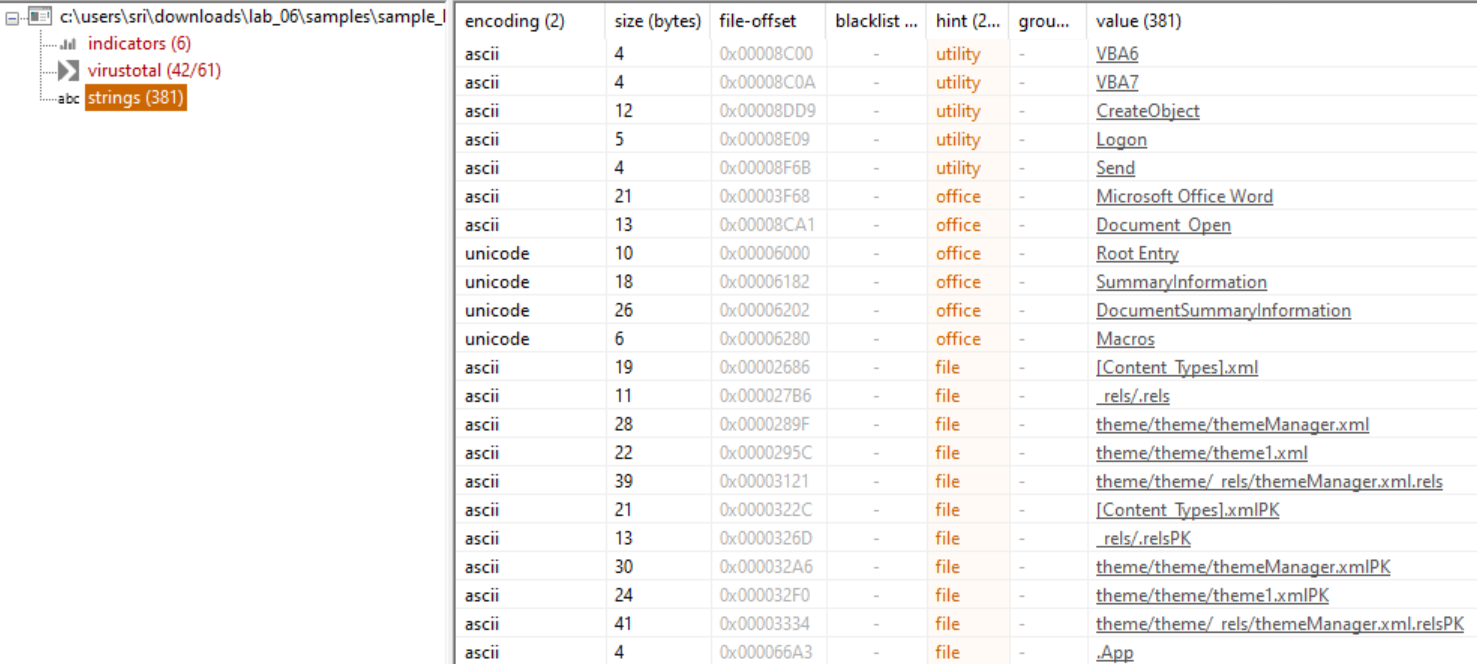


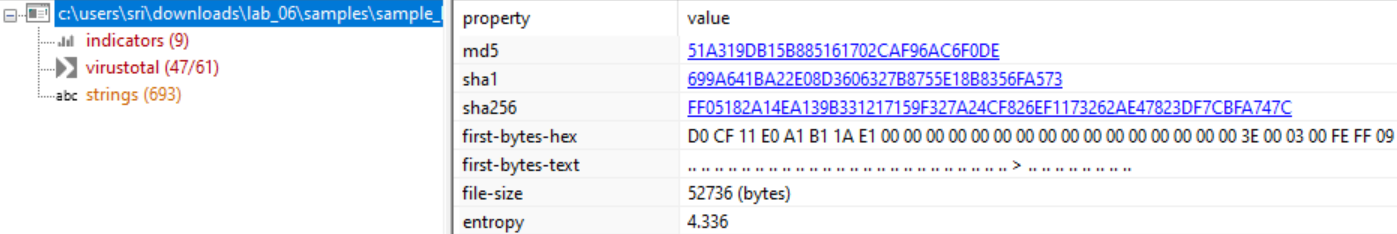


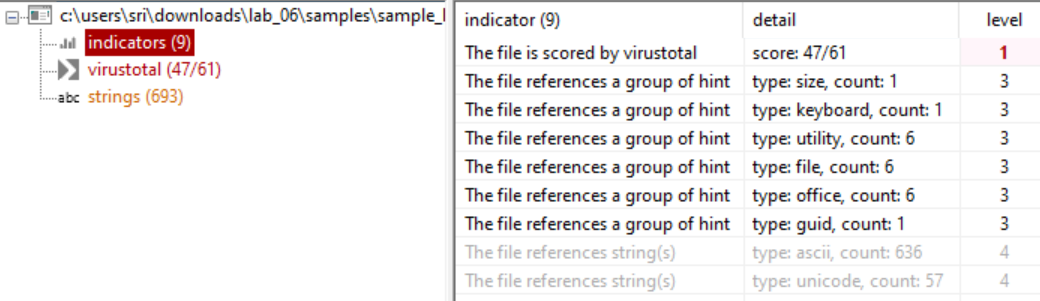


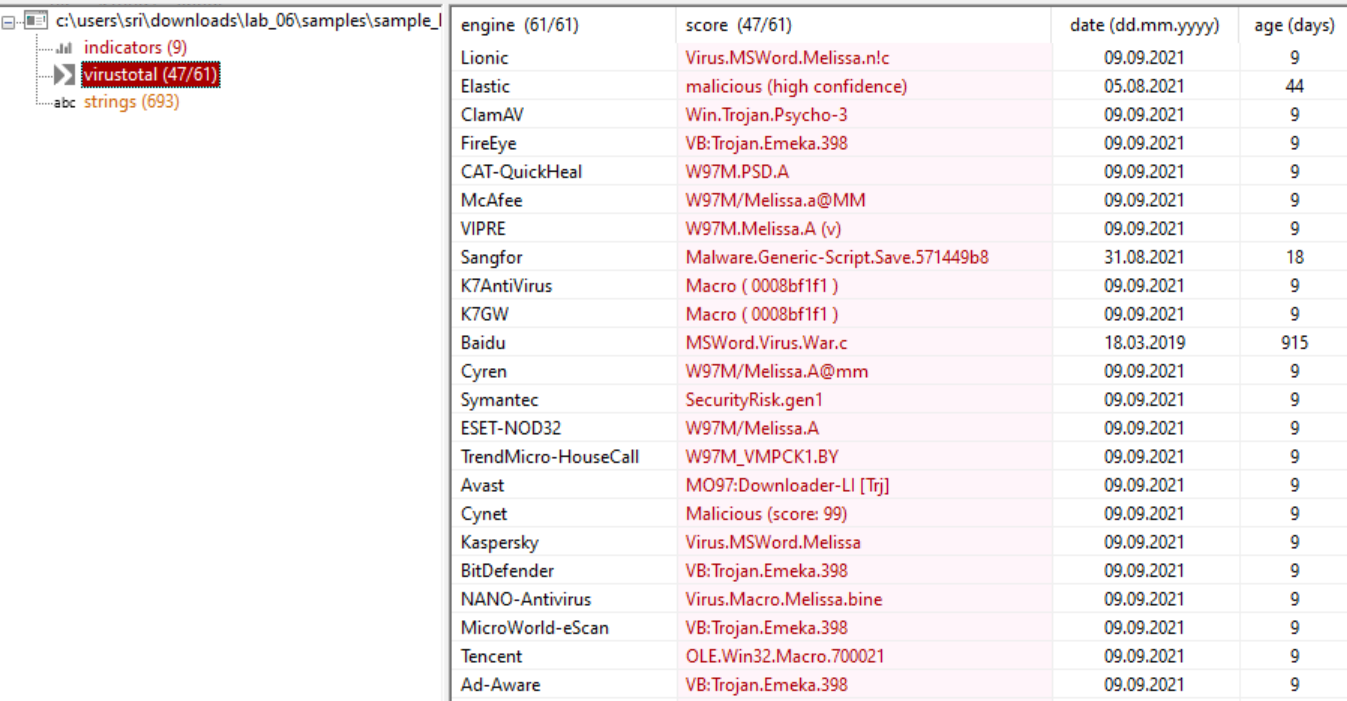


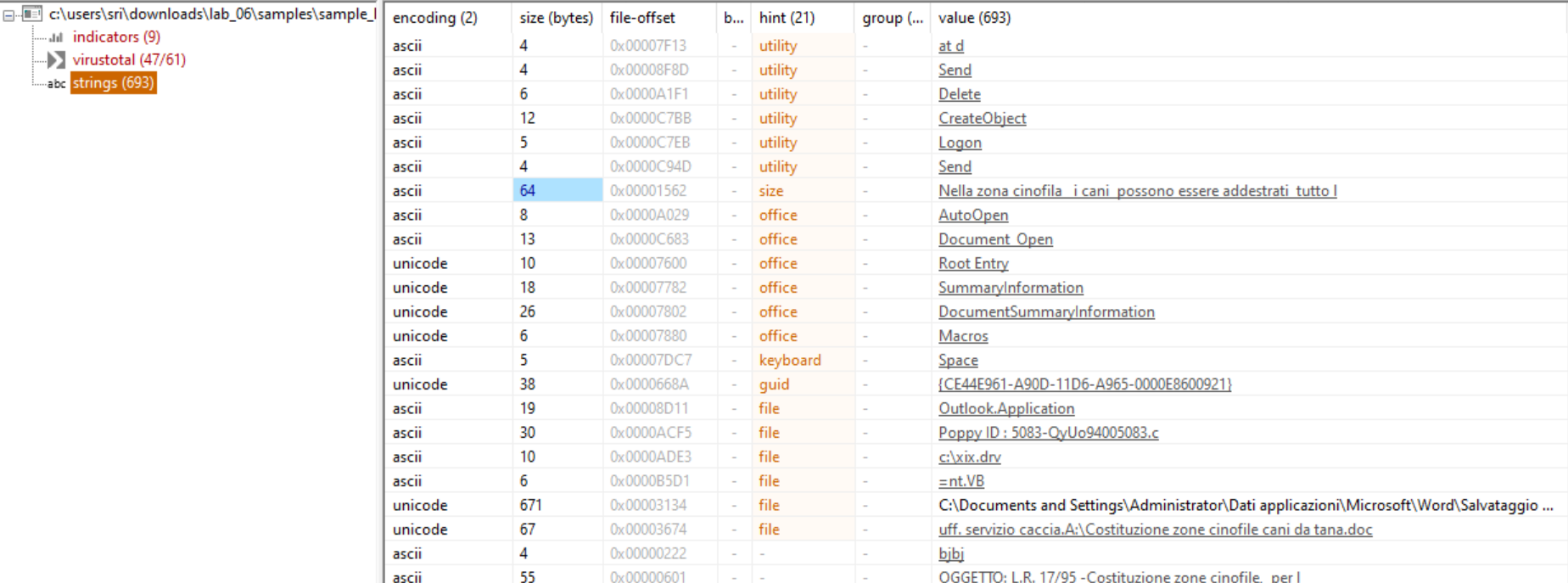


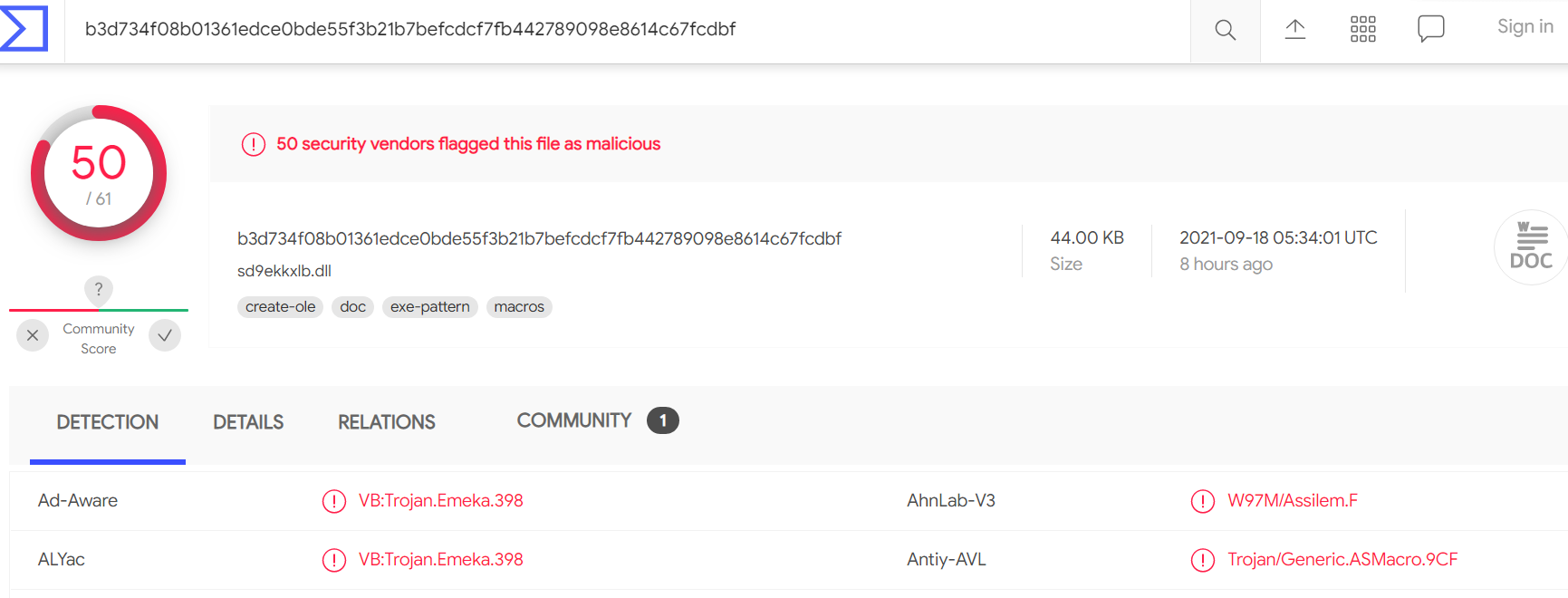


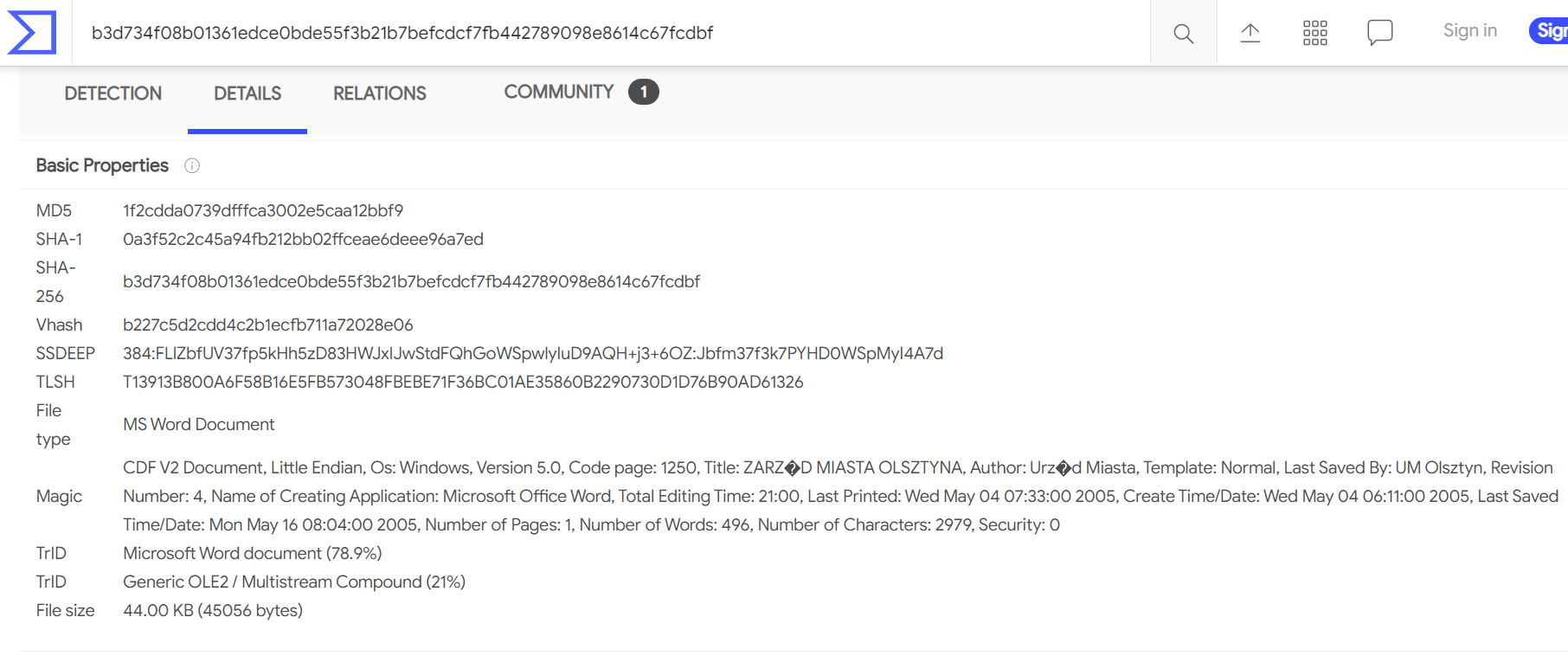


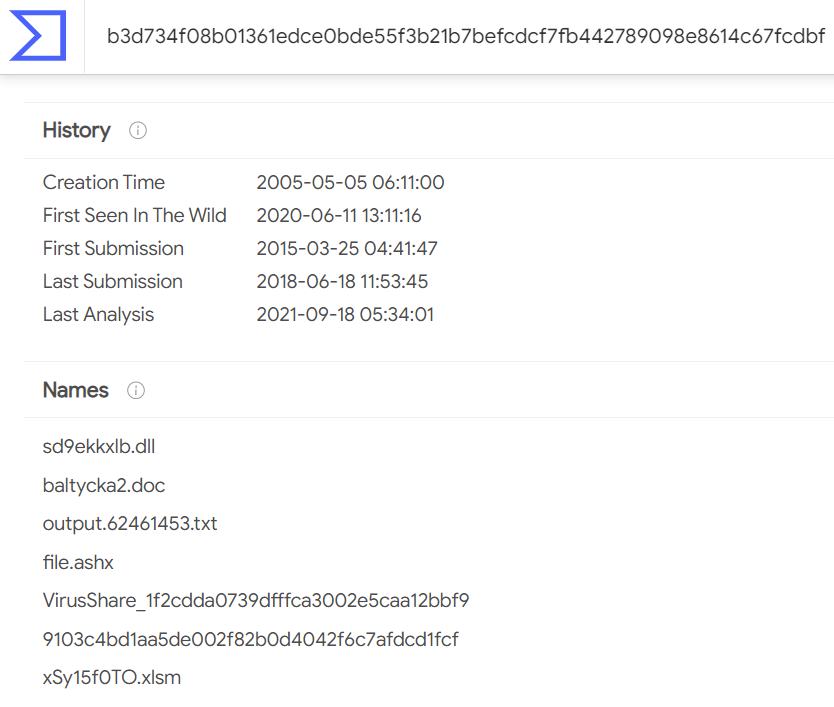


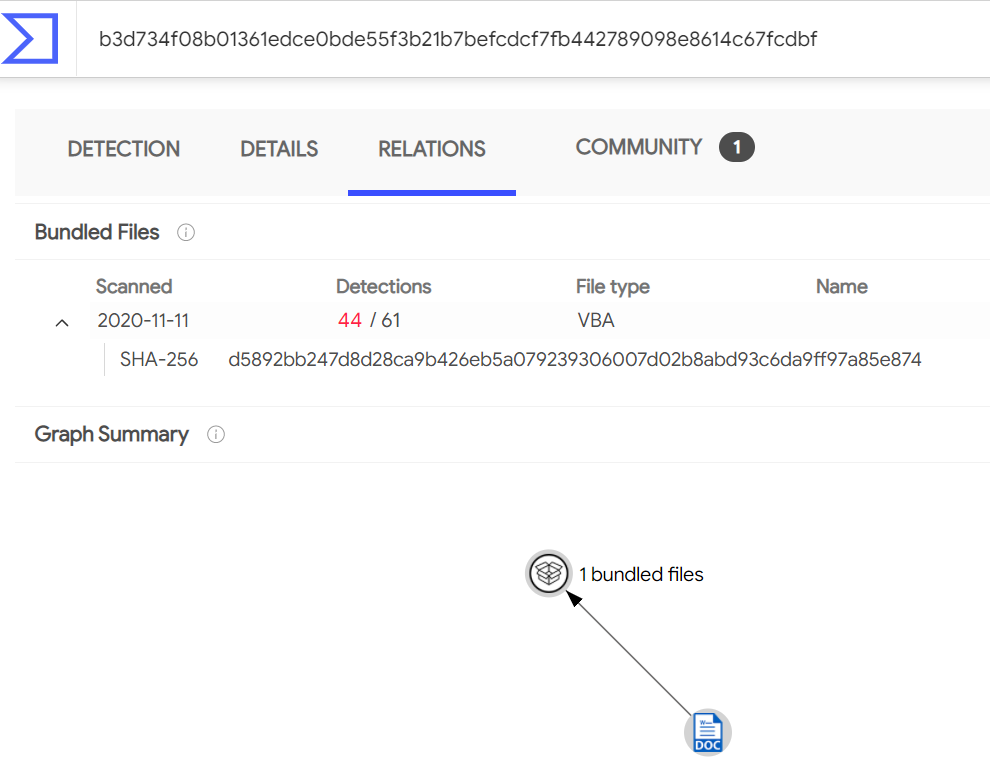


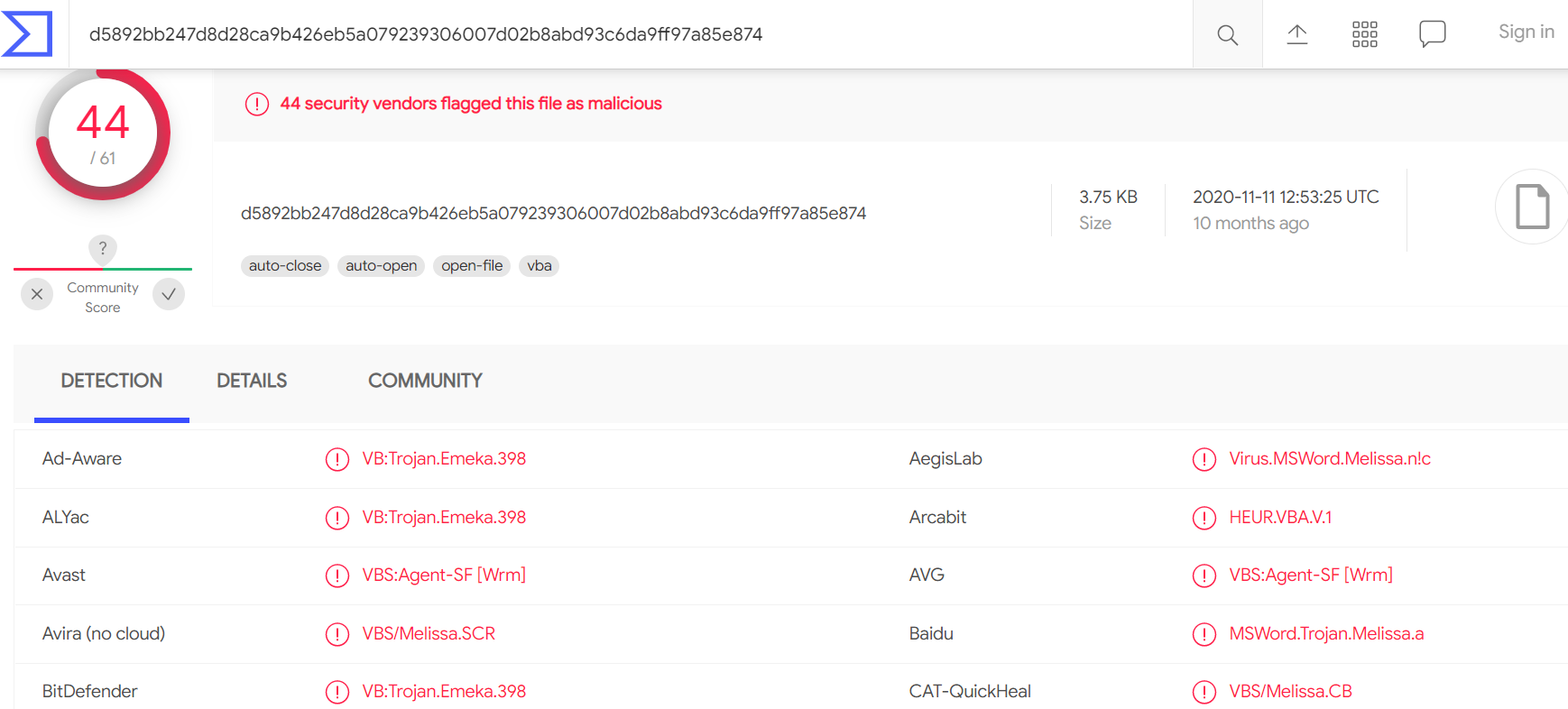


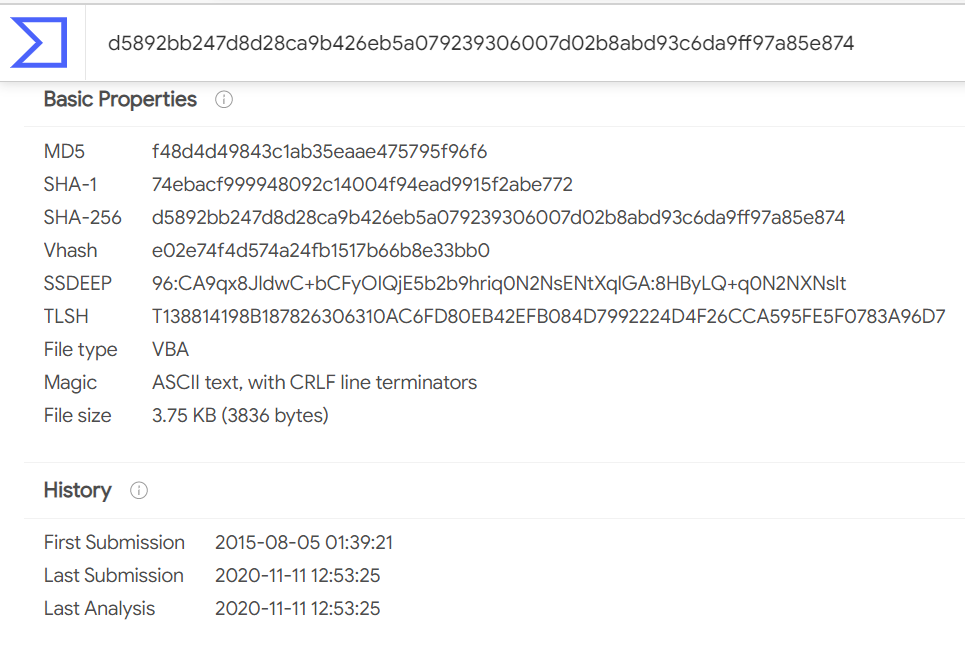


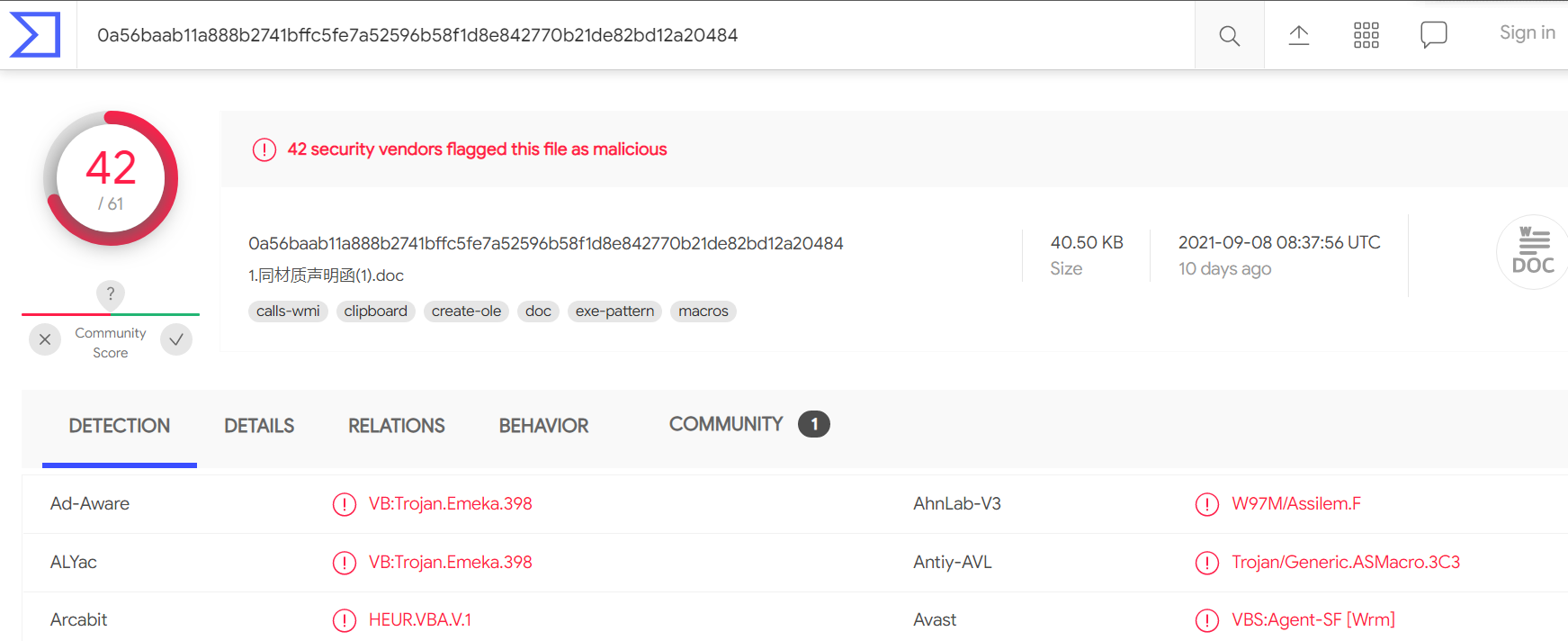


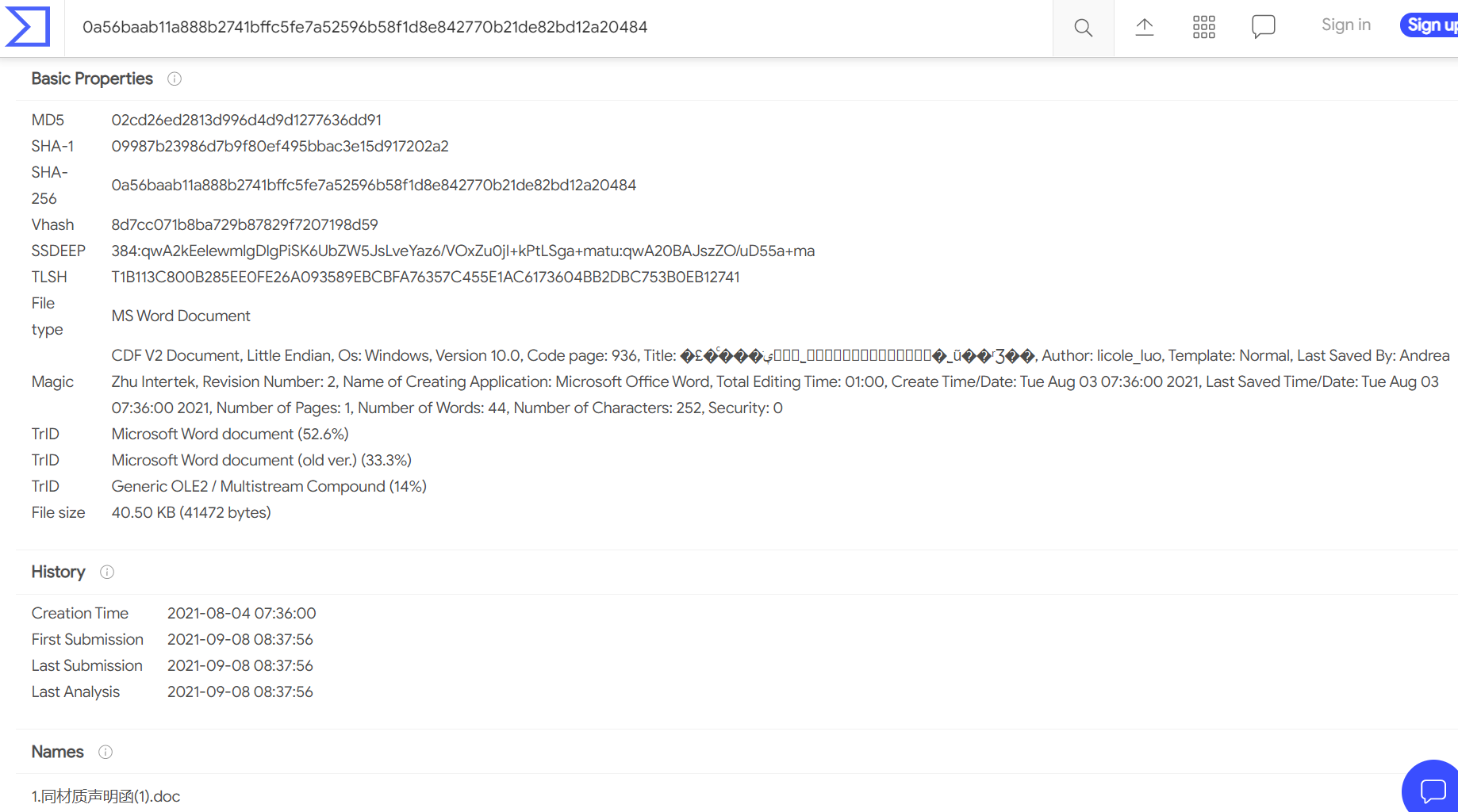


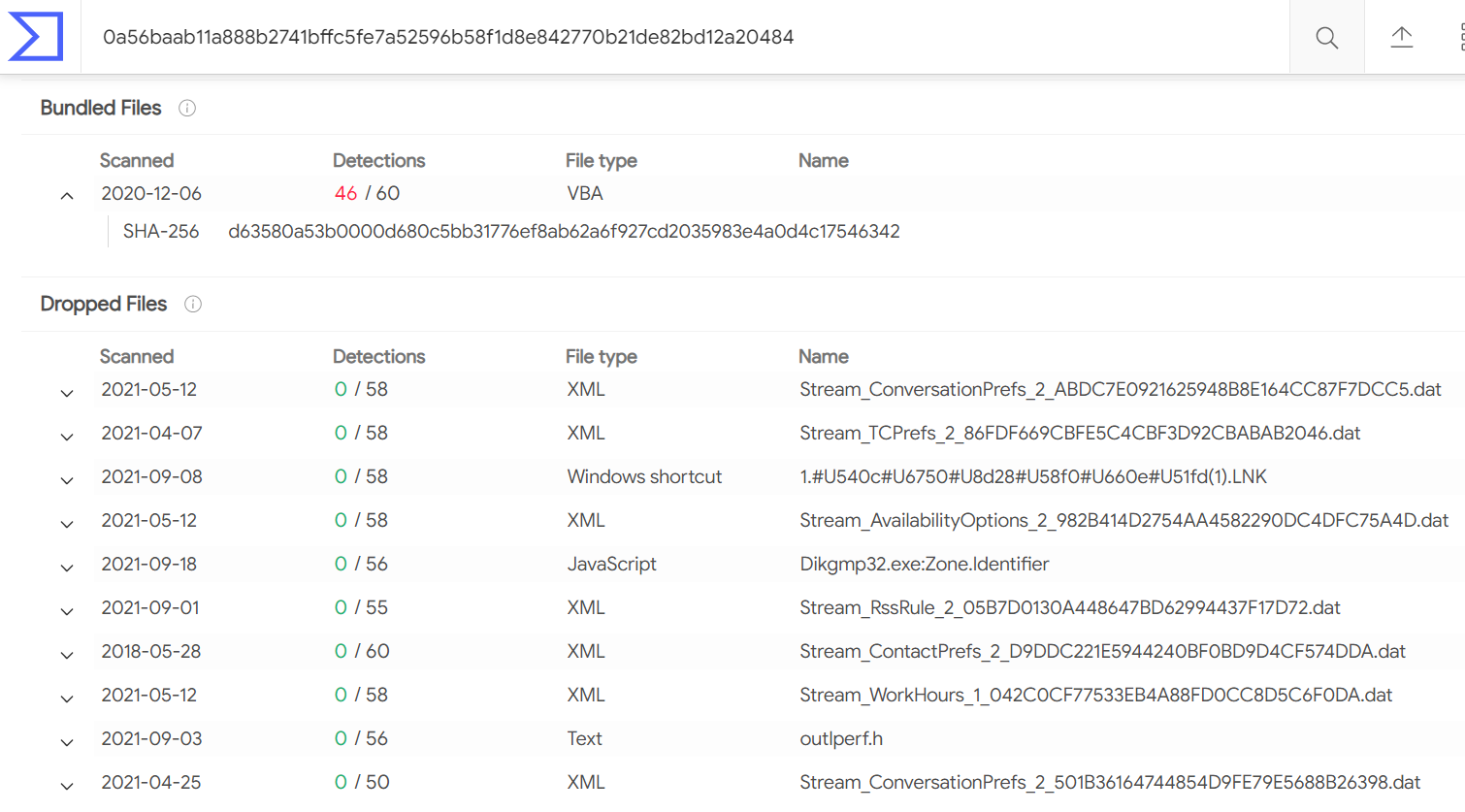


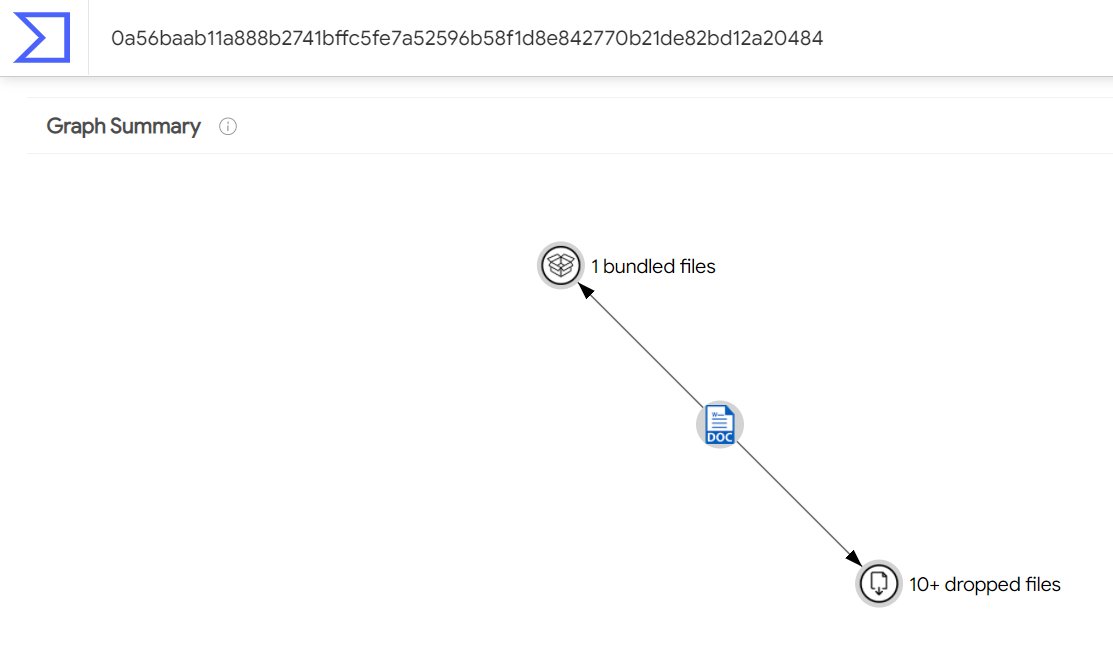


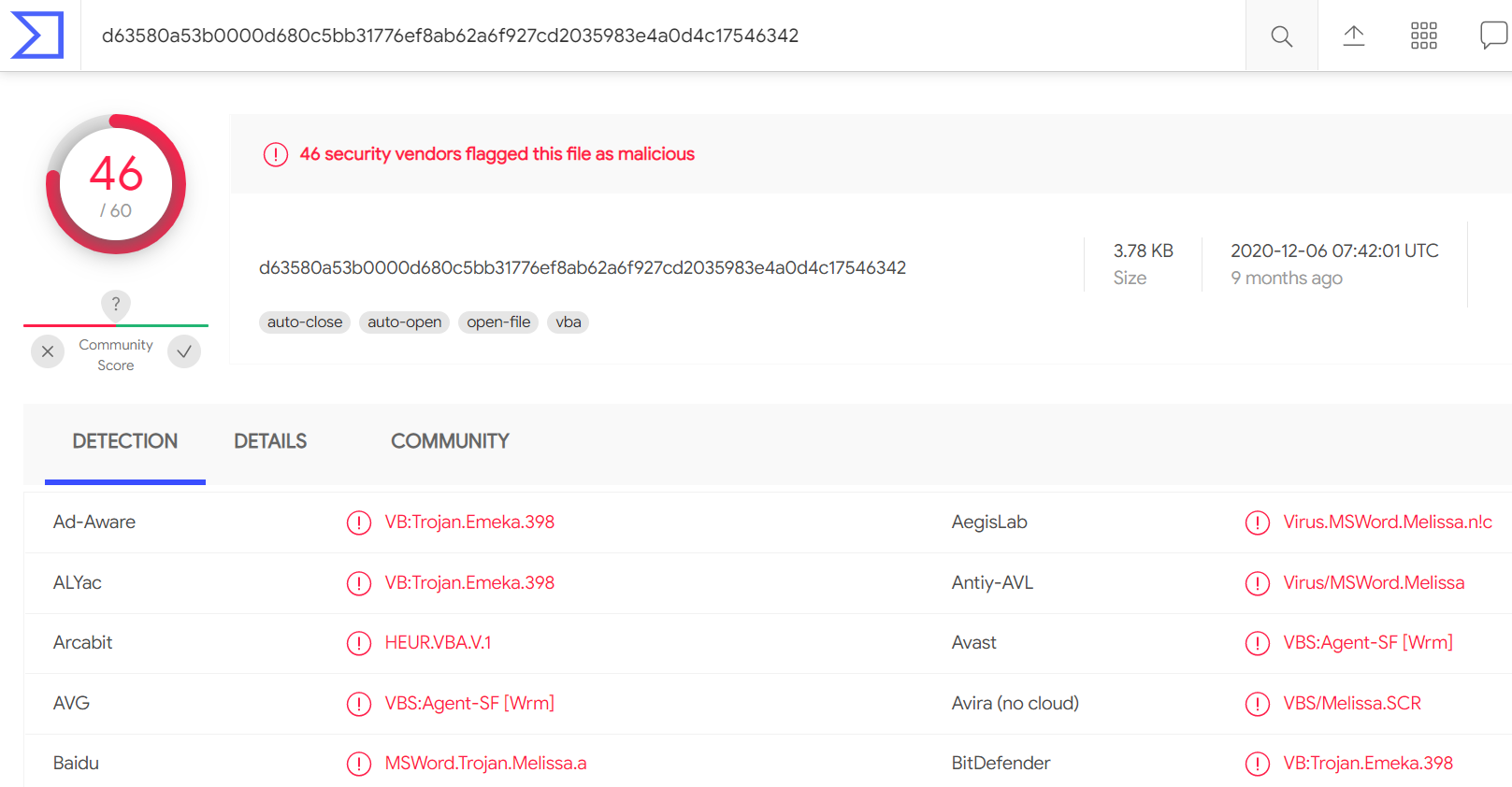


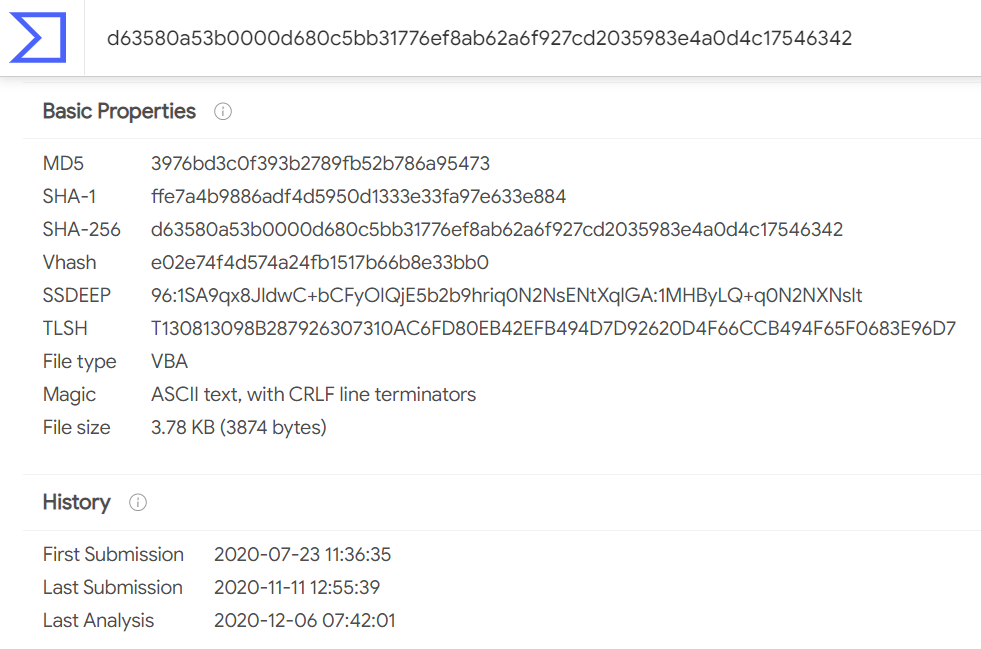


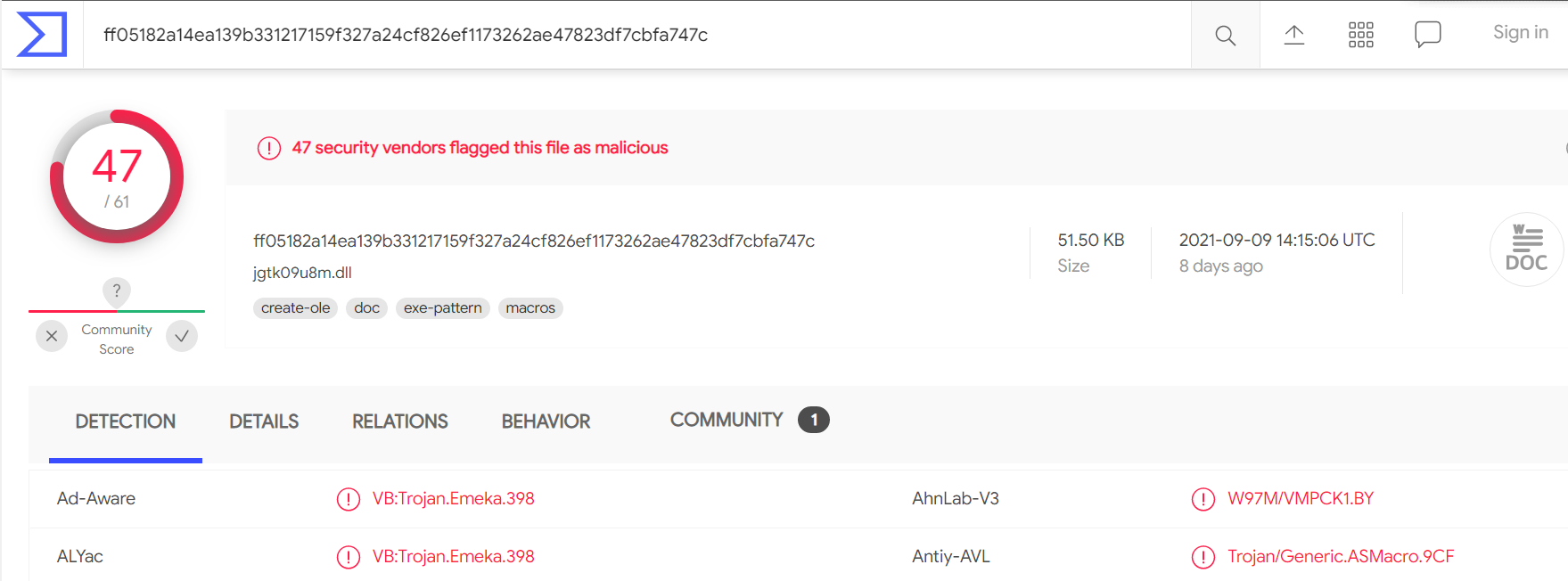




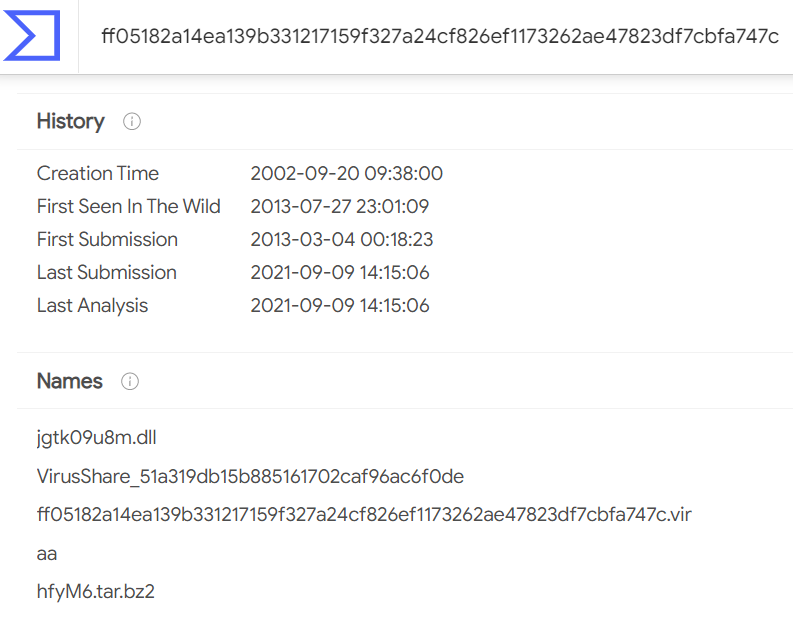


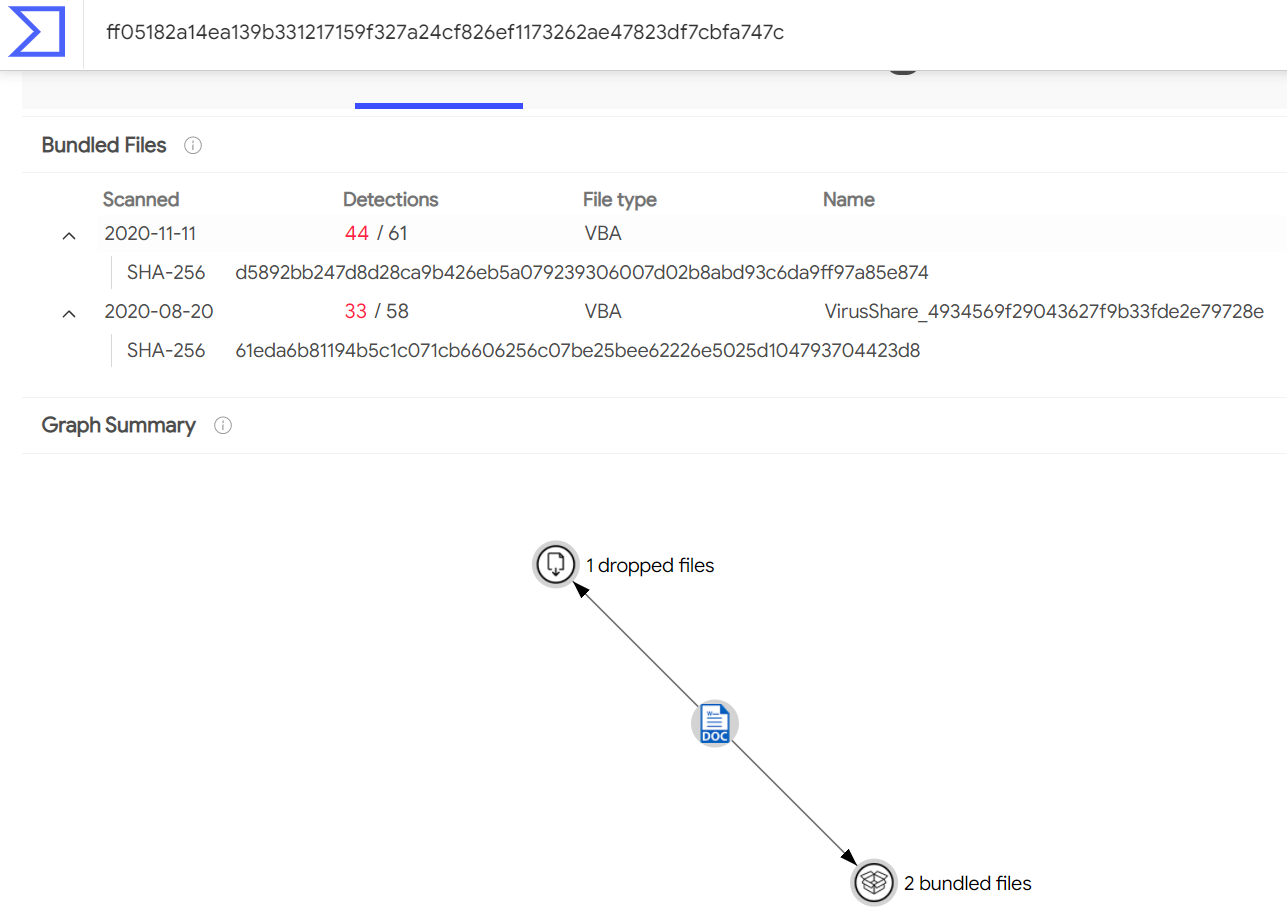


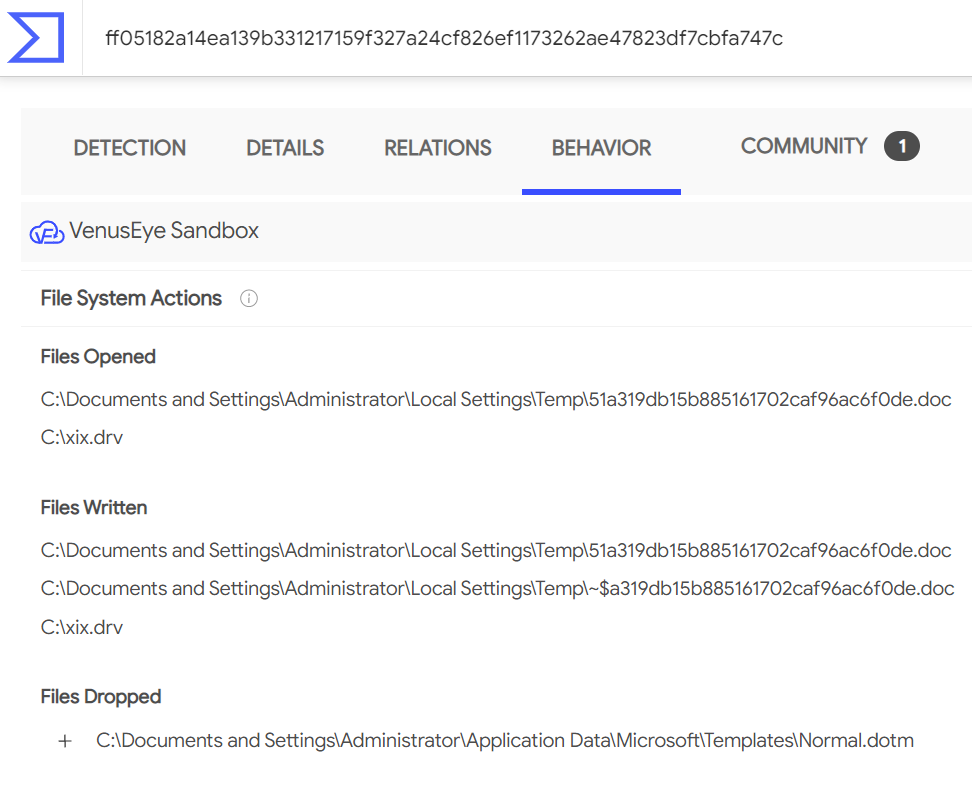
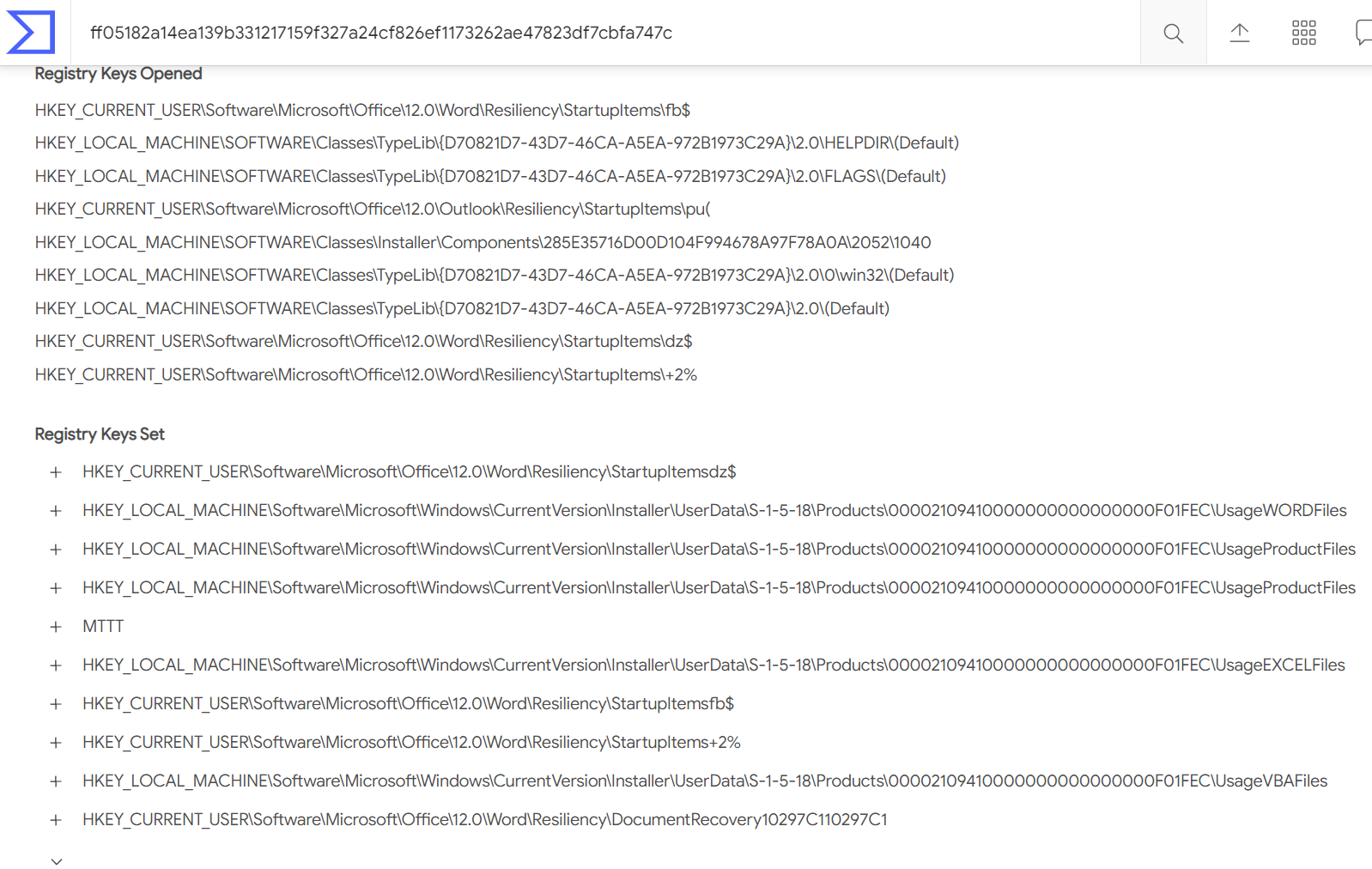


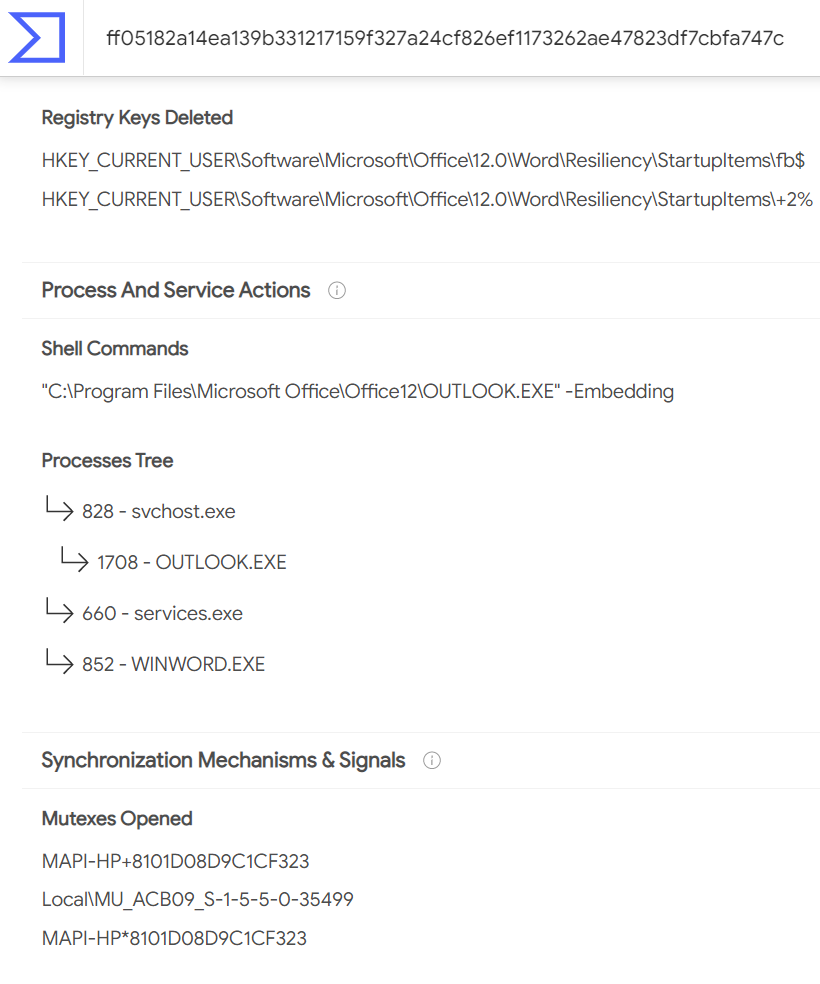


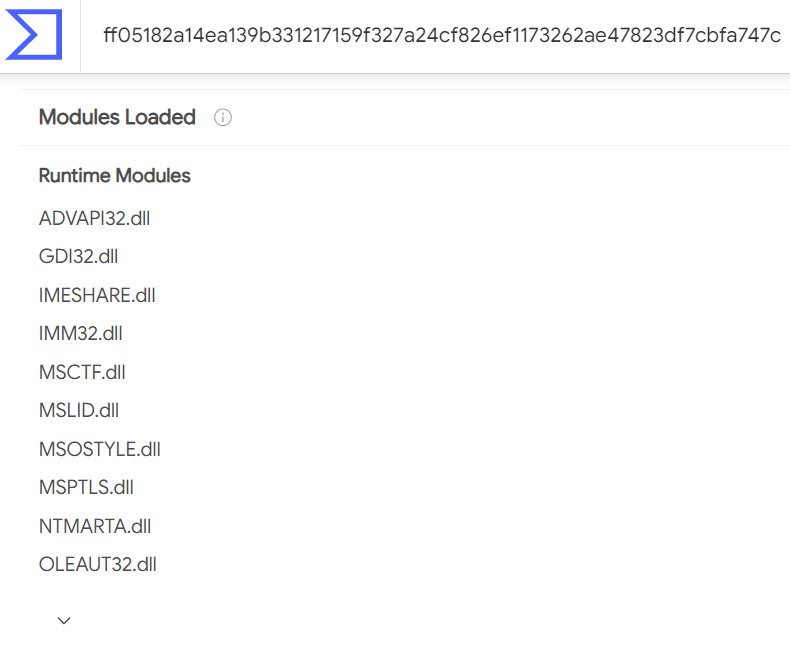


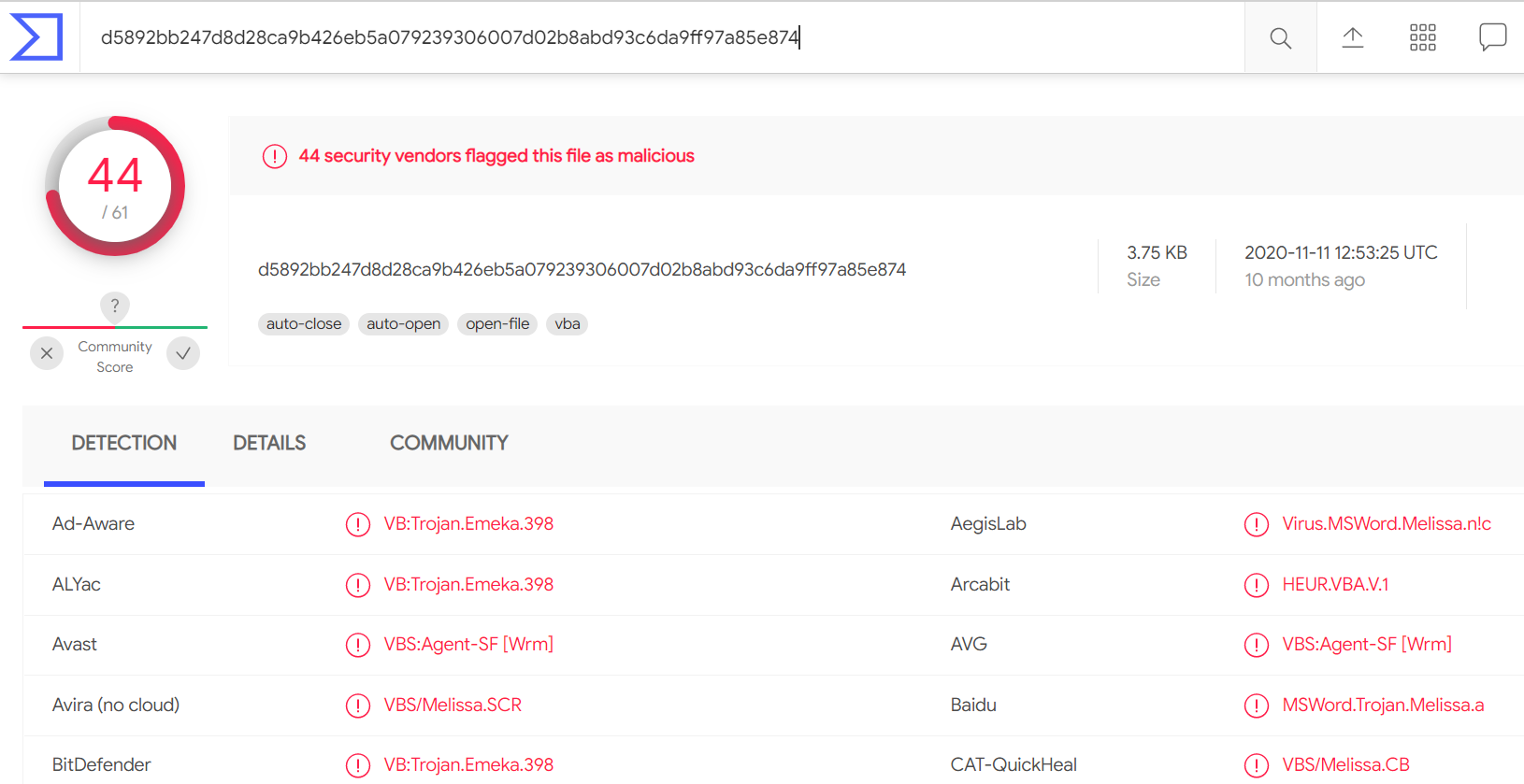


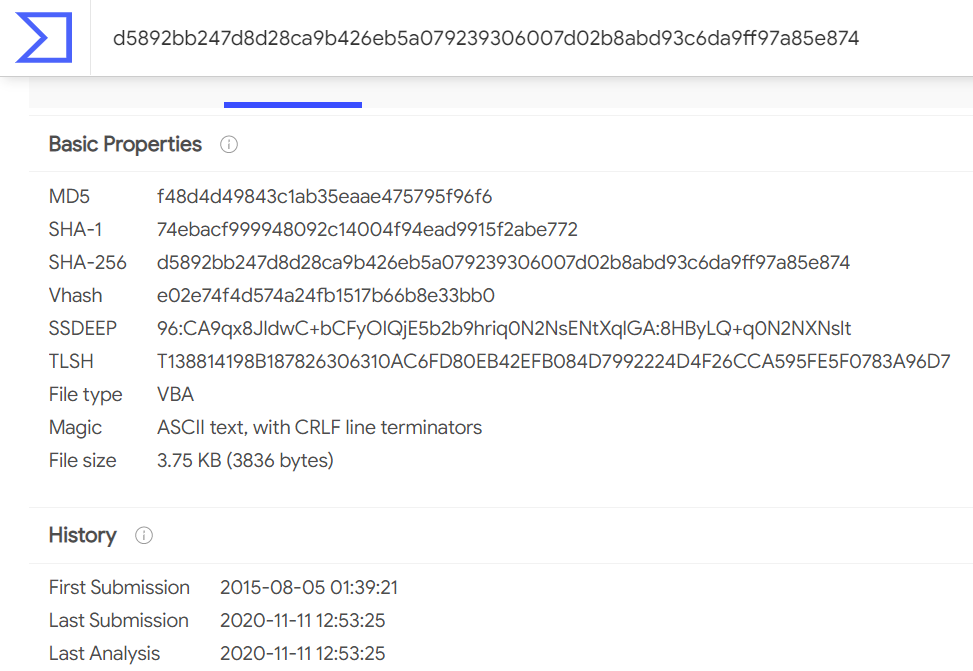


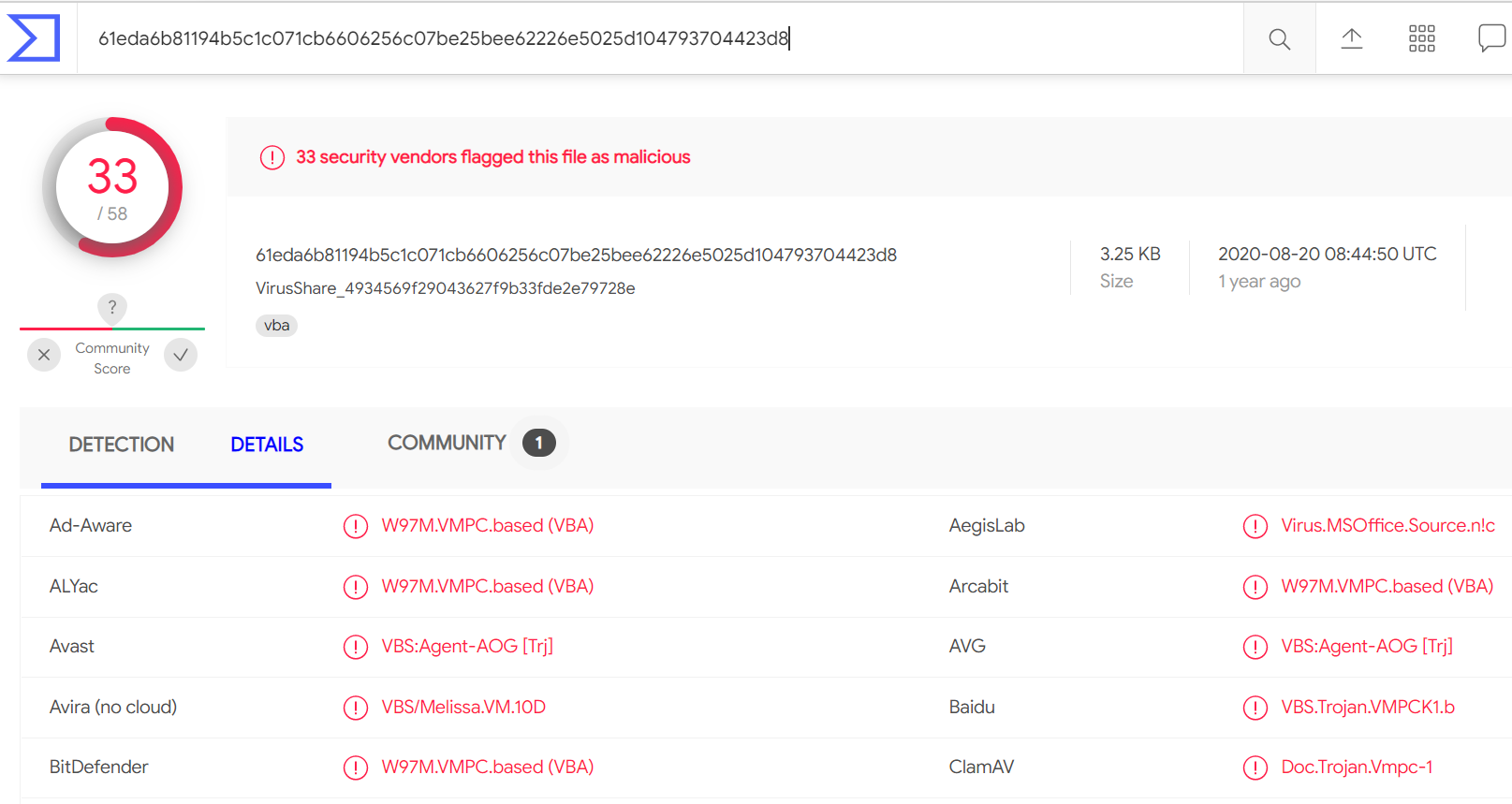
 

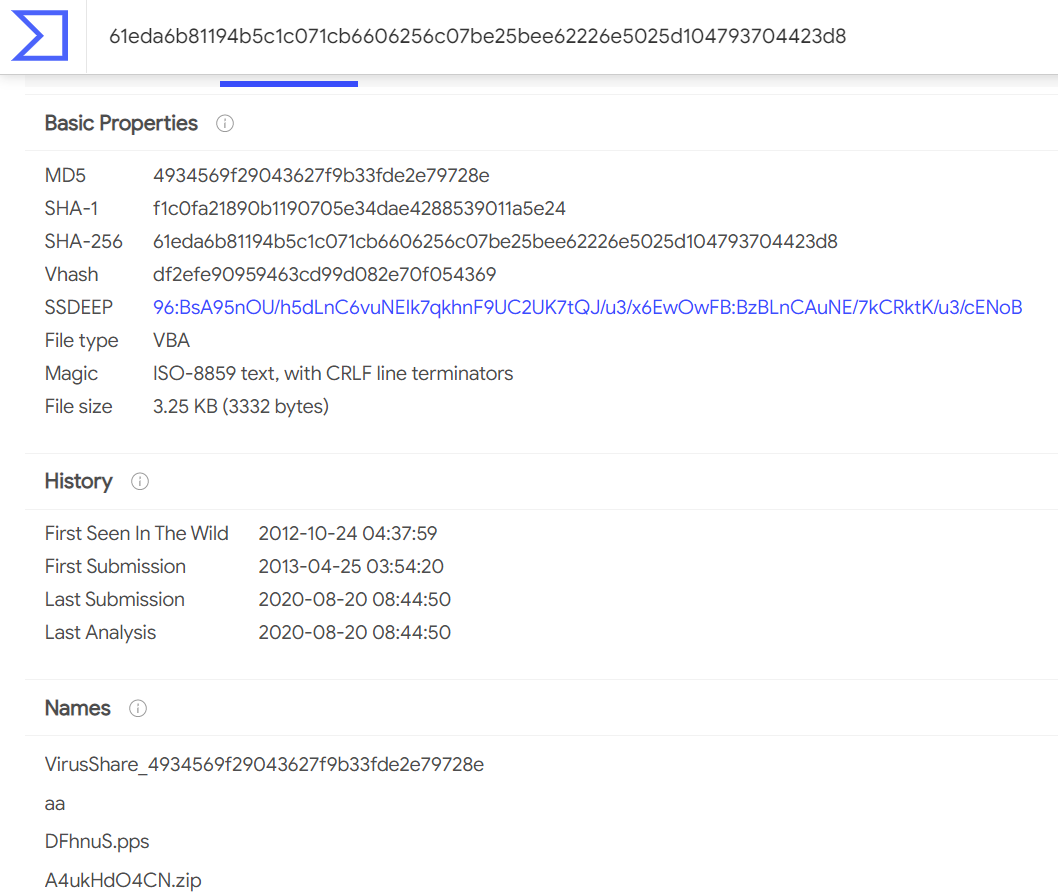












**What file do 🡪**

* Melissa's code is simple, but it does a lot of damage.
* First, it performs a query to find all the address lists available to the client.
* Then, it queries each address list and creates a message for the first 50 names that it retrieves.
* The message subject is Important Message From xxx (where xxx is the display name of the name the code has taken from the address list), and the message body contains one line of text and the infected Word document that contains the payload.
* Viruses might specifically target DLs or search for mailboxes belonging to people with titles such as president, CEO, or vice president.
* Users who know about these viruses can delete suspect messages as soon as they appear in their inbox—the viruses can't infect systems unless Word launches the payload attachment.
* Because VBA is the virus' key component, the code is useless if your PC doesn't have a program that supports VBA (e.g., Office 95).

**Yara Rule 🡪**

rule Melissa\_Virus

{

meta:

description = "Melissa virus"

file\_type = "VBA"

malware\_type = "Virus"

strings:

$a = "WORD/Melissa written by Kwyjibo"

$b = "Works in both Word 2000 and Word 97"

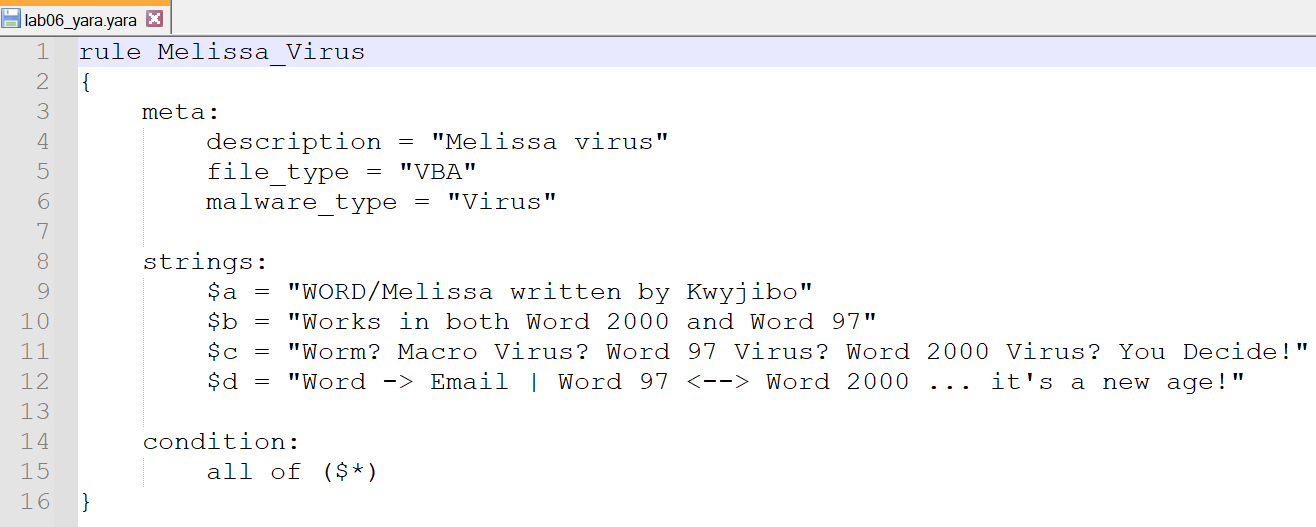
$c = "Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!"

$d = "Word -> Email | Word 97 <--> Word 2000 ... it's a new age!"

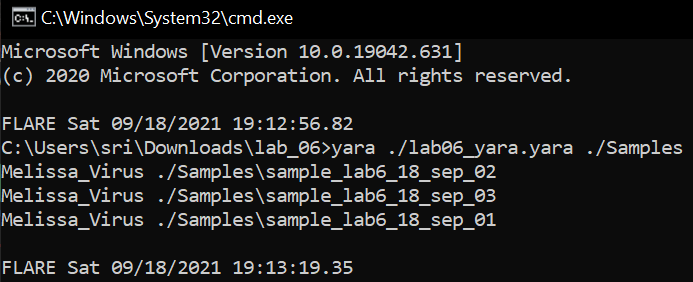
condition:

all of ($\*)

}



**OUTPUT:**



**Reference:**

* [VirusTotal - File - b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf](https://www.virustotal.com/gui/file/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf/)
* [VirusTotal - File - d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874](https://www.virustotal.com/gui/file/d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874)
* [VirusTotal - File - 0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484](https://www.virustotal.com/gui/file/0a56baab11a888b2741bffc5fe7a52596b58f1d8e842770b21de82bd12a20484)
* [VirusTotal - File - d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342](https://www.virustotal.com/gui/file/d63580a53b0000d680c5bb31776ef8ab62a6f927cd2035983e4a0d4c17546342)
* [VirusTotal - File - ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c](https://www.virustotal.com/gui/file/ff05182a14ea139b331217159f327a24cf826ef1173262ae47823df7cbfa747c)
* [VirusTotal - File - d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874](https://www.virustotal.com/gui/file/d5892bb247d8d28ca9b426eb5a079239306007d02b8abd93c6da9ff97a85e874)
* [VirusTotal - File - 61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8](https://www.virustotal.com/gui/file/61eda6b81194b5c1c071cb6606256c07be25bee62226e5025d104793704423d8)
* [InQuest Labs - InQuest.net](https://labs.inquest.net/dfi/hash/b3d734f08b01361edce0bde55f3b21b7befcdcf7fb442789098e8614c67fcdbf)
* [What is the Melissa Virus? (with pictures) (easytechjunkie.com)](https://www.easytechjunkie.com/what-is-the-melissa-virus.htm)
* [Melissa Virus — FBI](https://www.fbi.gov/history/famous-cases/melissa-virus)
* [F-Secure Warns -- Melissa is Back (responsesource.com)](https://pressreleases.responsesource.com/news/10312/f-secure-warns-melissa-is-back/)
* [Virus:W32/Melissa Description | F-Secure Labs](https://www.f-secure.com/v-descs/melissa.shtml)
* [What is Melissa virus? - Definition from WhatIs.com (techtarget.com)](https://searchsecurity.techtarget.com/definition/Melissa-virus)
* [Lessons from the Melissa Virus | IT Pro (itprotoday.com)](https://www.itprotoday.com/email-and-calendaring/lessons-melissa-virus)
* [Melissa Virus (slideshare.net)](https://www.slideshare.net/MinhNguyen92/melissa-virus)