**CYBERATTACKS LABS**

**Task 1:** Perform an email header analysis. You will be given an email. The task will be to identify the various headers and body of the email and determine if the email is a genuine email or a phishing email.

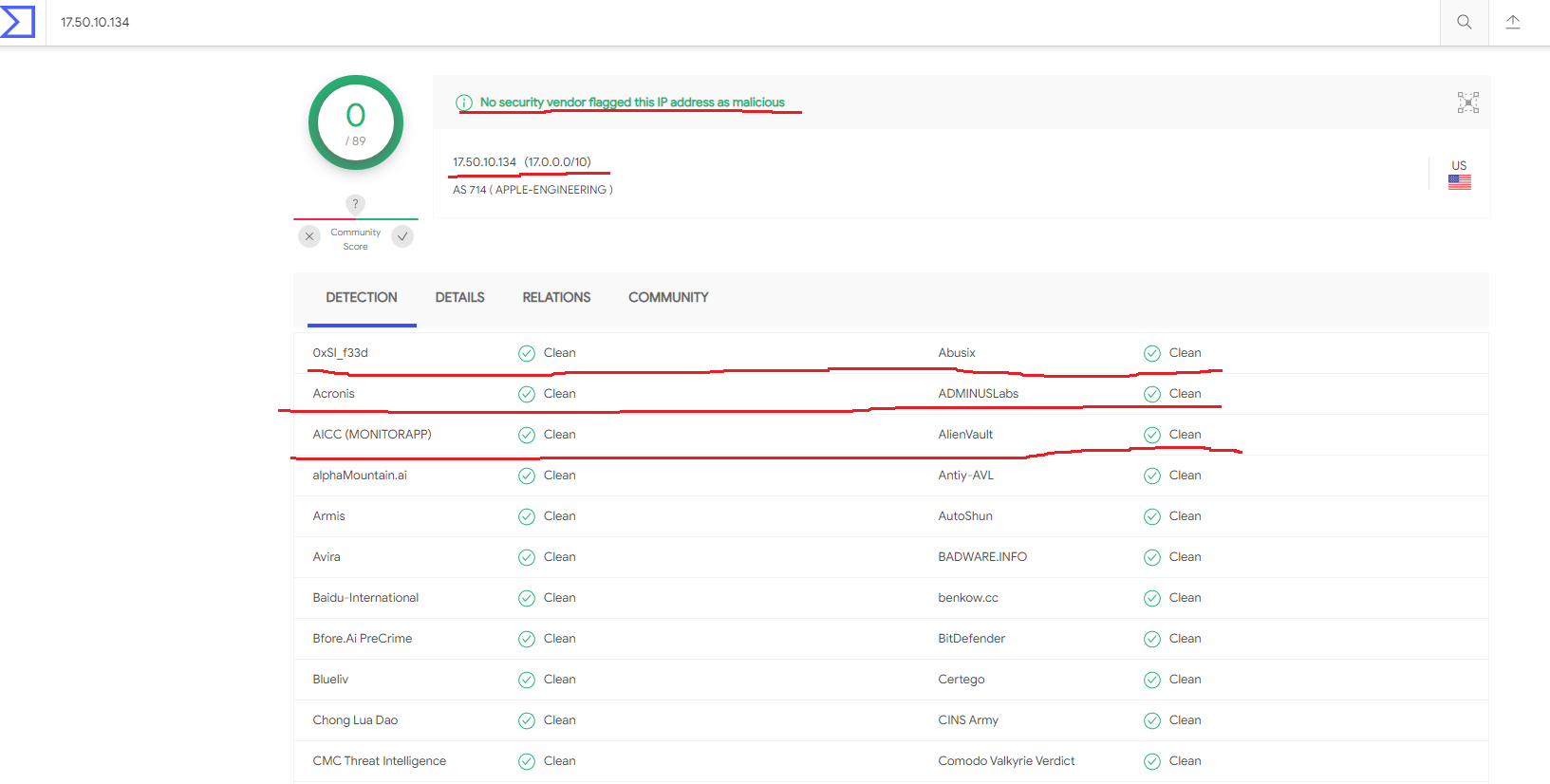
IOCs:

17.50.10.134

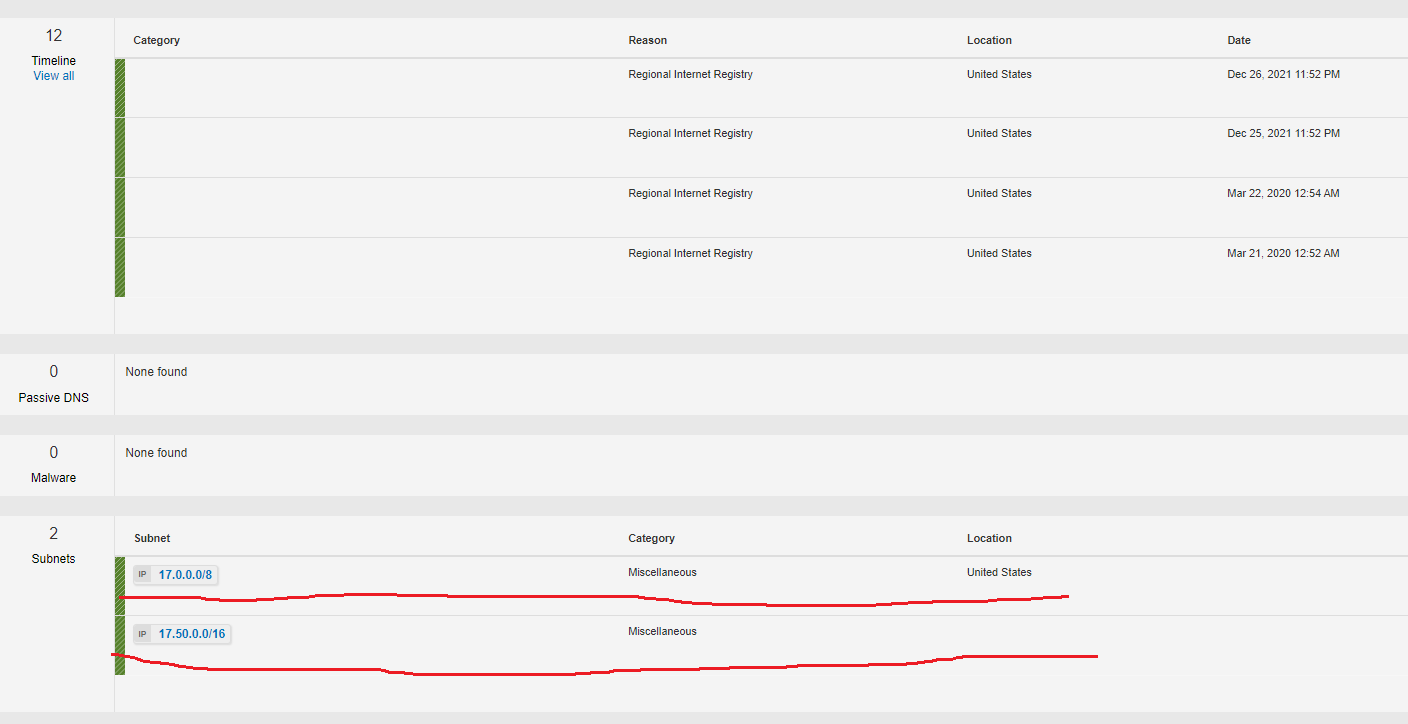
maxsgmail.top

https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net

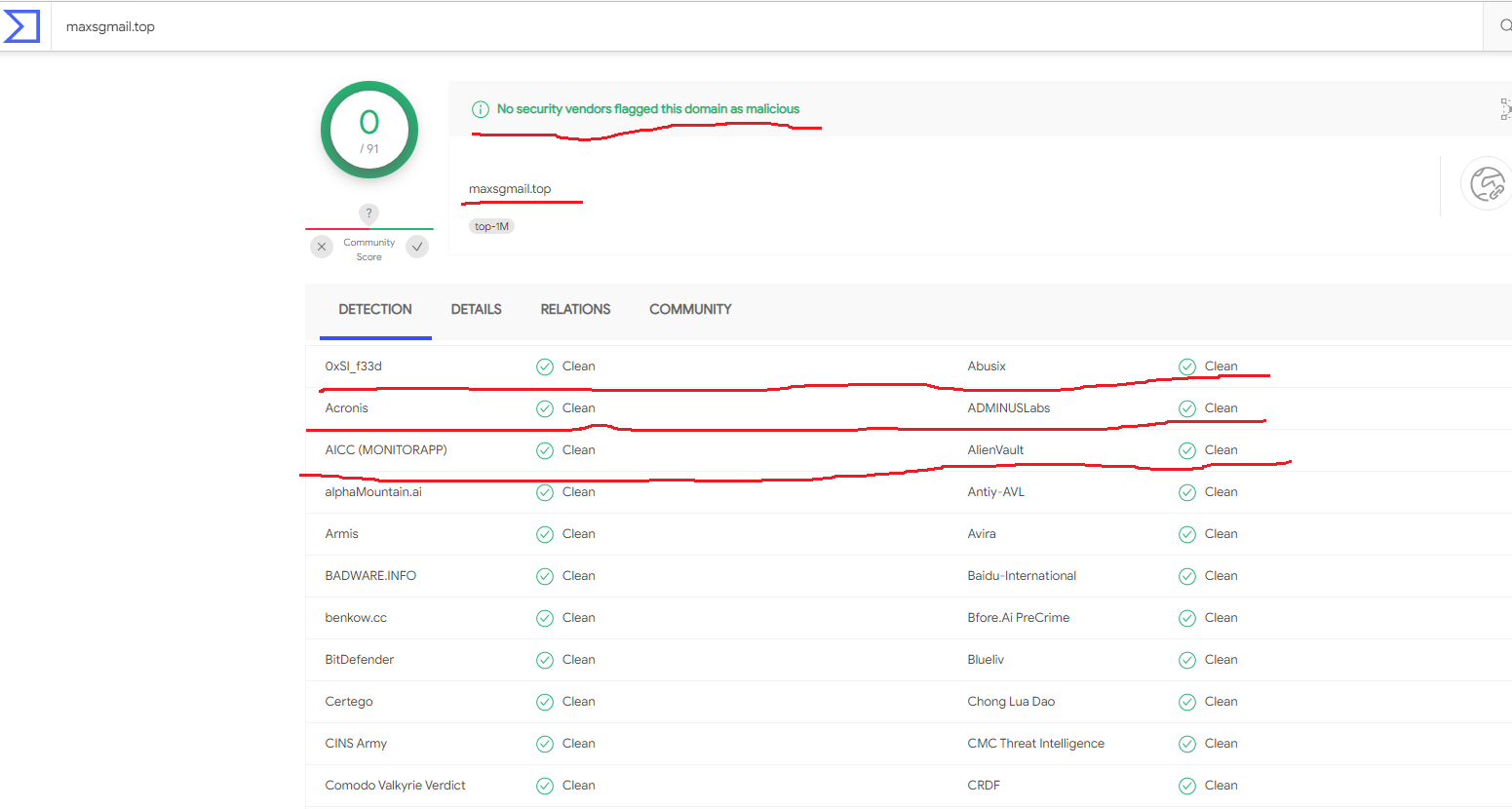
b264818bdfa95e0498fcc48734a9e40921e15d8d389294a703094e9691905de6\



Verifying IP address before blocking it. The site I have used here to verify is www.virustotal.com. Highlights show that No security vendor flagged this IP address as malicious.

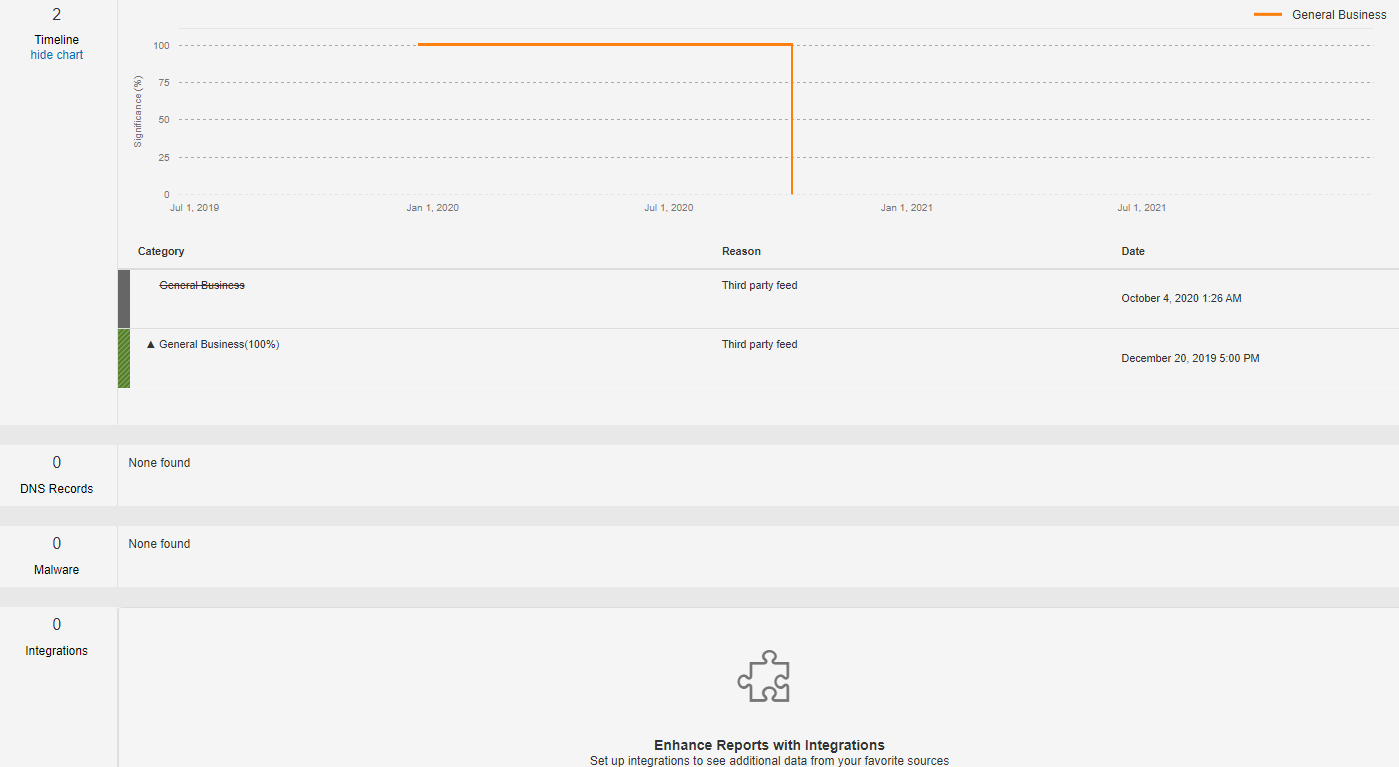


Verifying IP address in IBM X-force exchange. Highlights show that it is using two subnets which are miscellaneous.

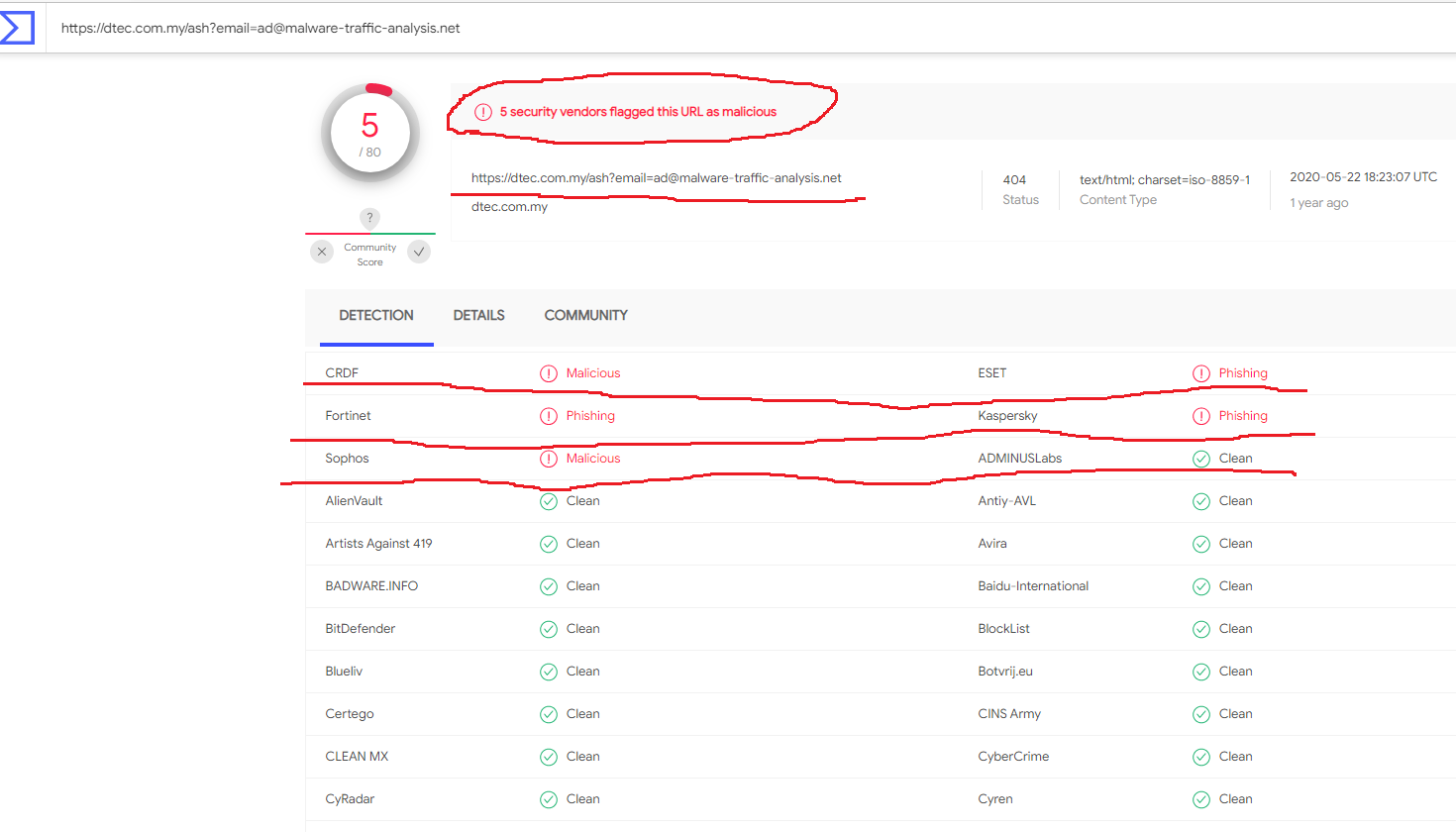


Verifying Domain before blocking it. The site I have used here to verify is [www.virustotal.com](http://www.virustotal.com).

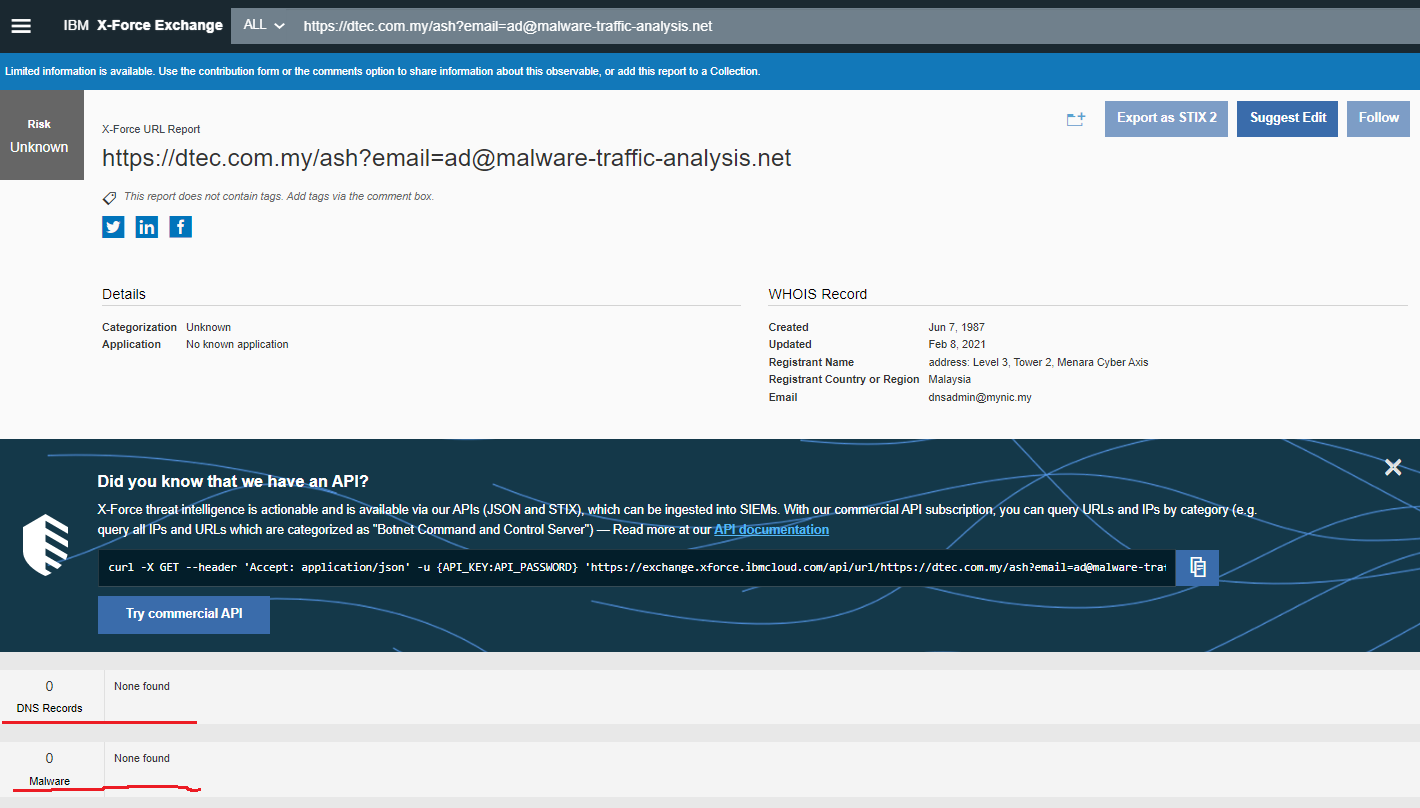
Highlights show that No security vendor flagged this domain address as malicious.



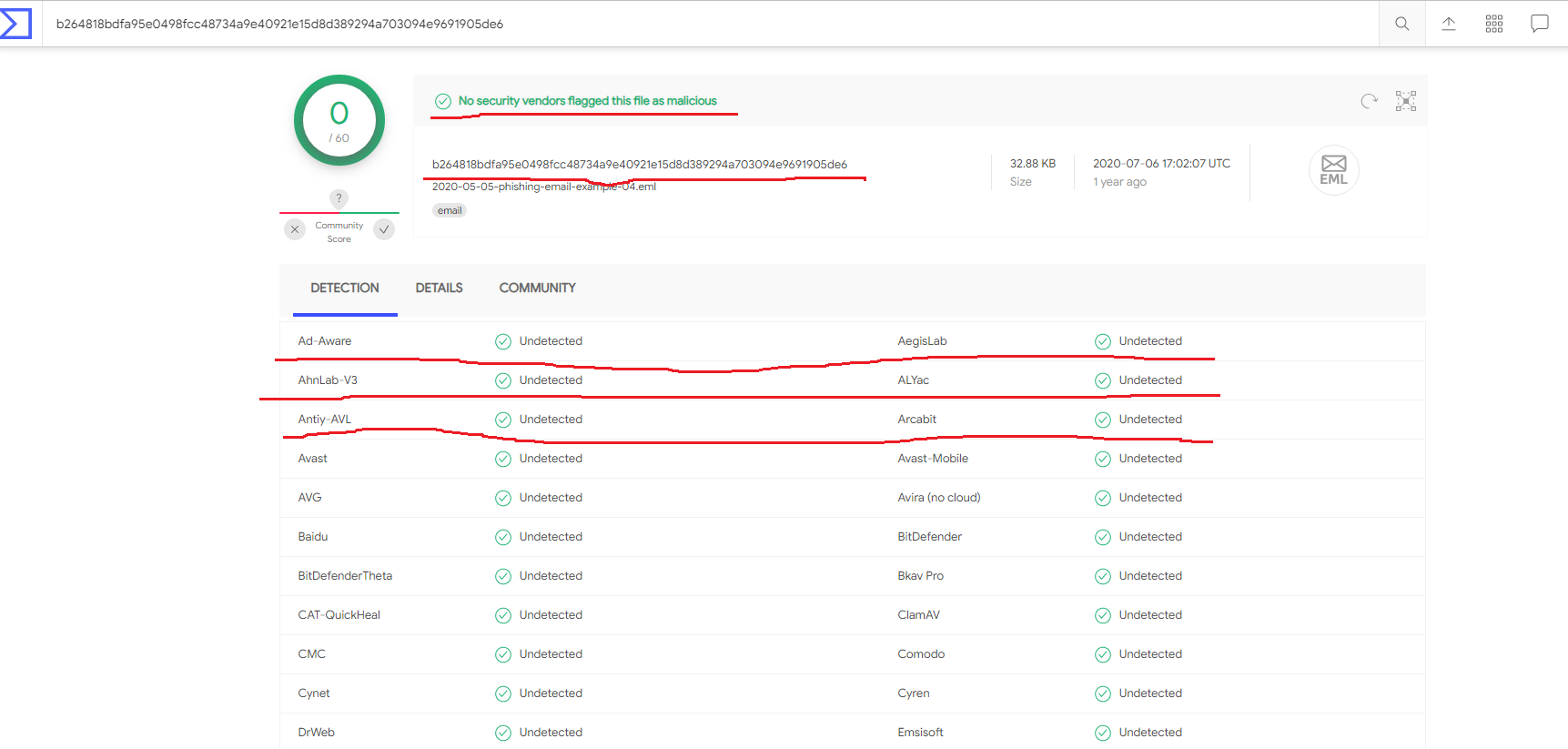
Verifying Domain in IBM X-force exchange. It shows risk is unknown. No DNS record and malware found.



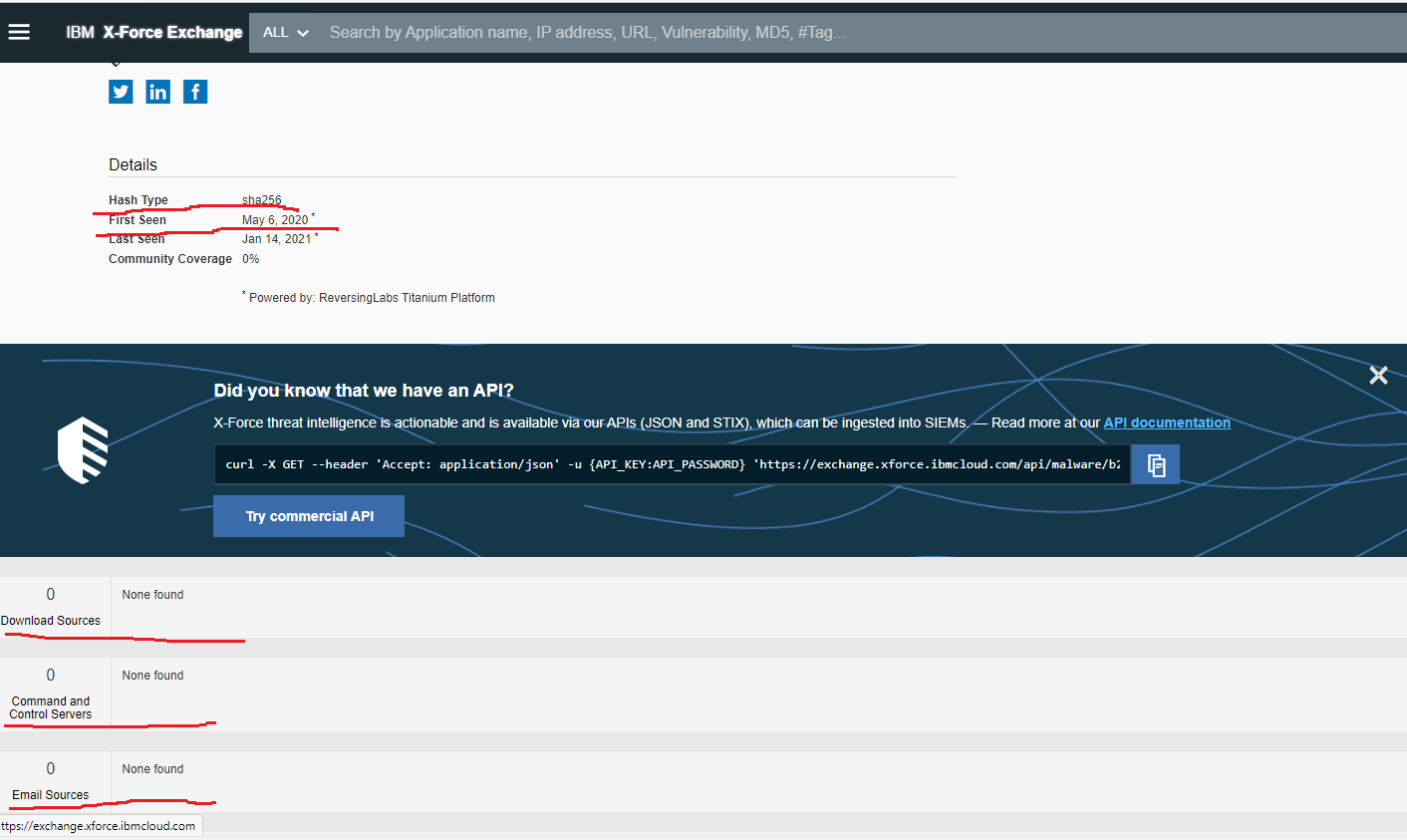
Verifying Hyperlink in virustotal. Highlights show 5 security vendors flagged this URL as malicious. 3 vendors say it is phishing and 2 vendors say its malware.



Verifying Hyperlink in IBM X-force exchange. It shows risk is unknown. No DNS record and malware found.



Verifying hash of the mail in virustotal. Highlights show that No security vendor flagged this file as malicious.



Verifying hash of the mail in IBM X-force exchange. Highlights show the type of hash is “sha256”.

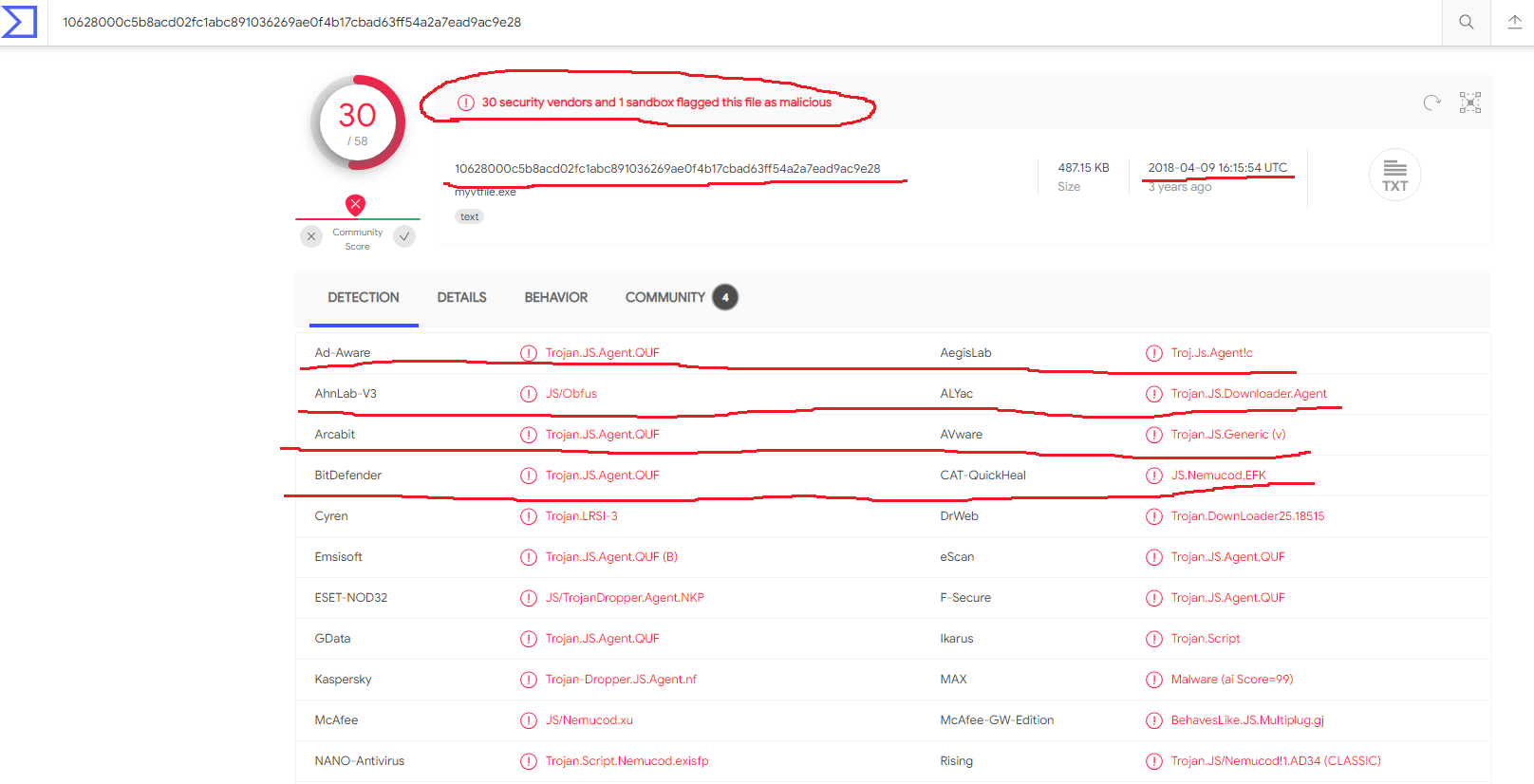
It is verified that the given email is not genuine and it is a phishing email from the hyperlink given.

**Task 2:** Perform malware analysis. You will be given a piece of malware for investigate. The task will be to analyze the piece of malware and prepare a report accordingly. Please feel free to choose any malware report template from the internet. Check for the good ones like Mandiant, Threat Intel and Kroll as few examples.

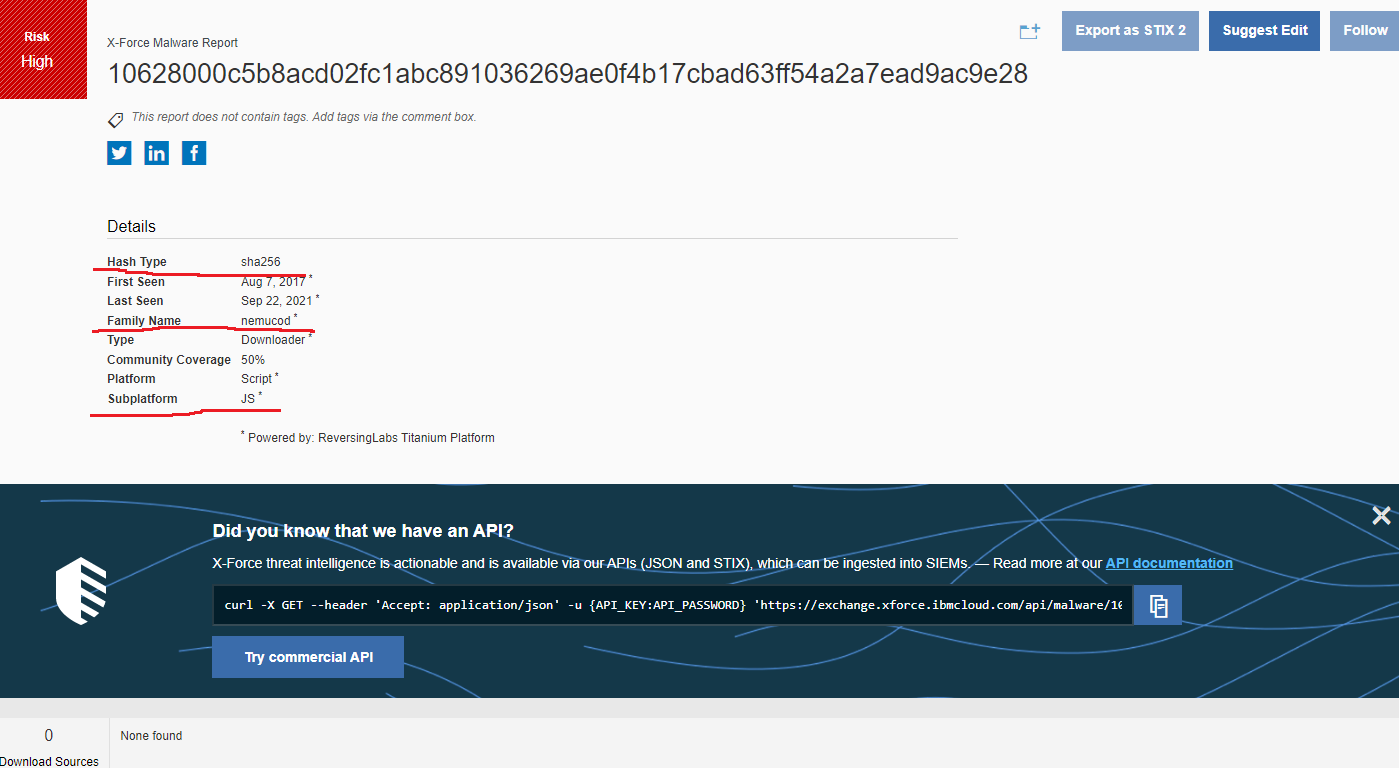
**Compliant\_29769200-352**

****

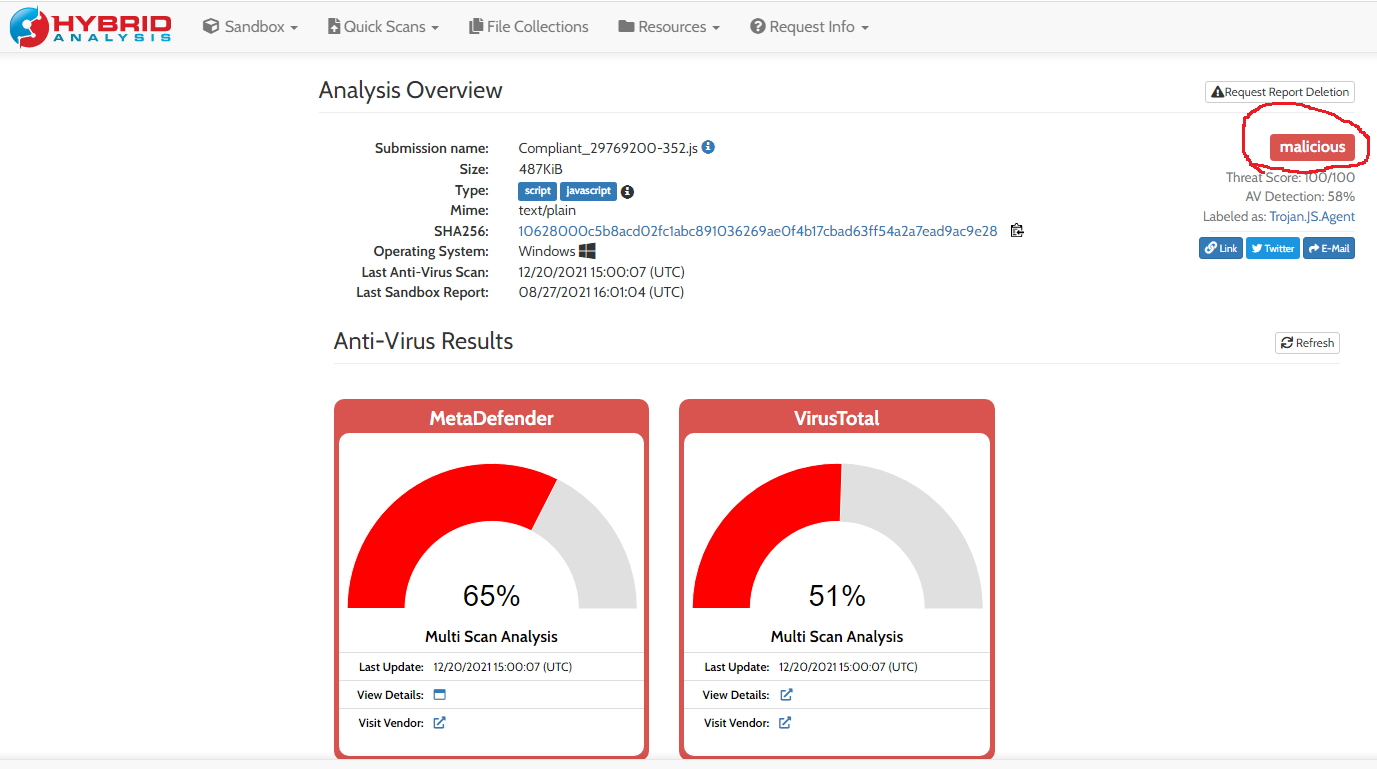
Opening the file script in sublime text. And saving it as a java file.

****

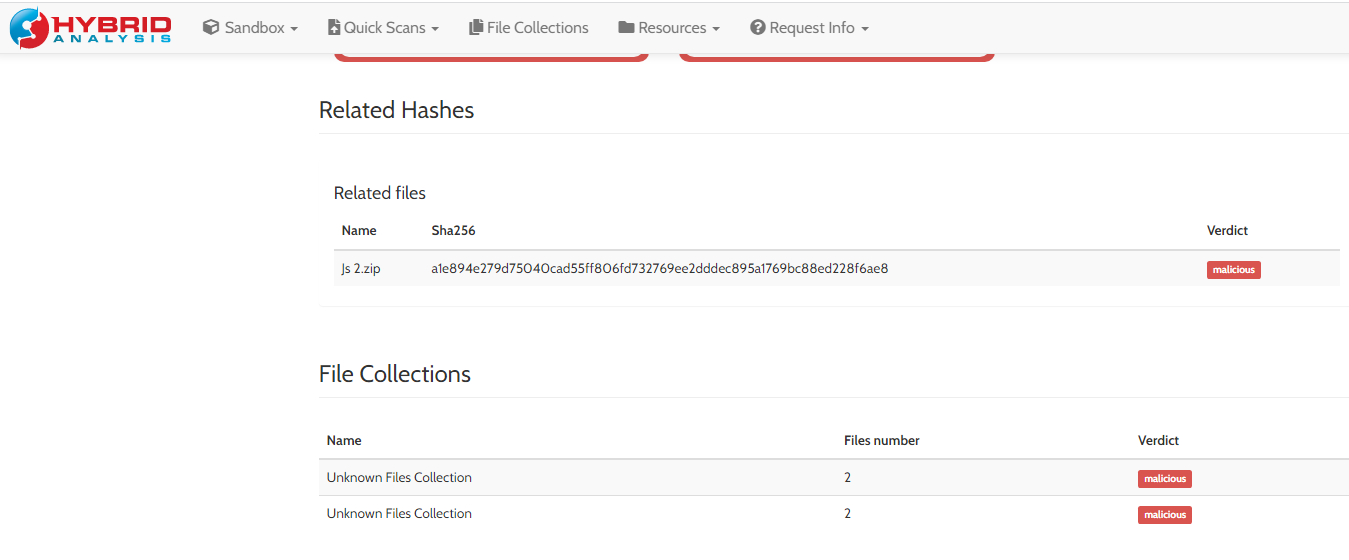
Verifying script file in virustotal. Highlights show 30 security vendors and 1 sandbox flagged this file as malicious.

****

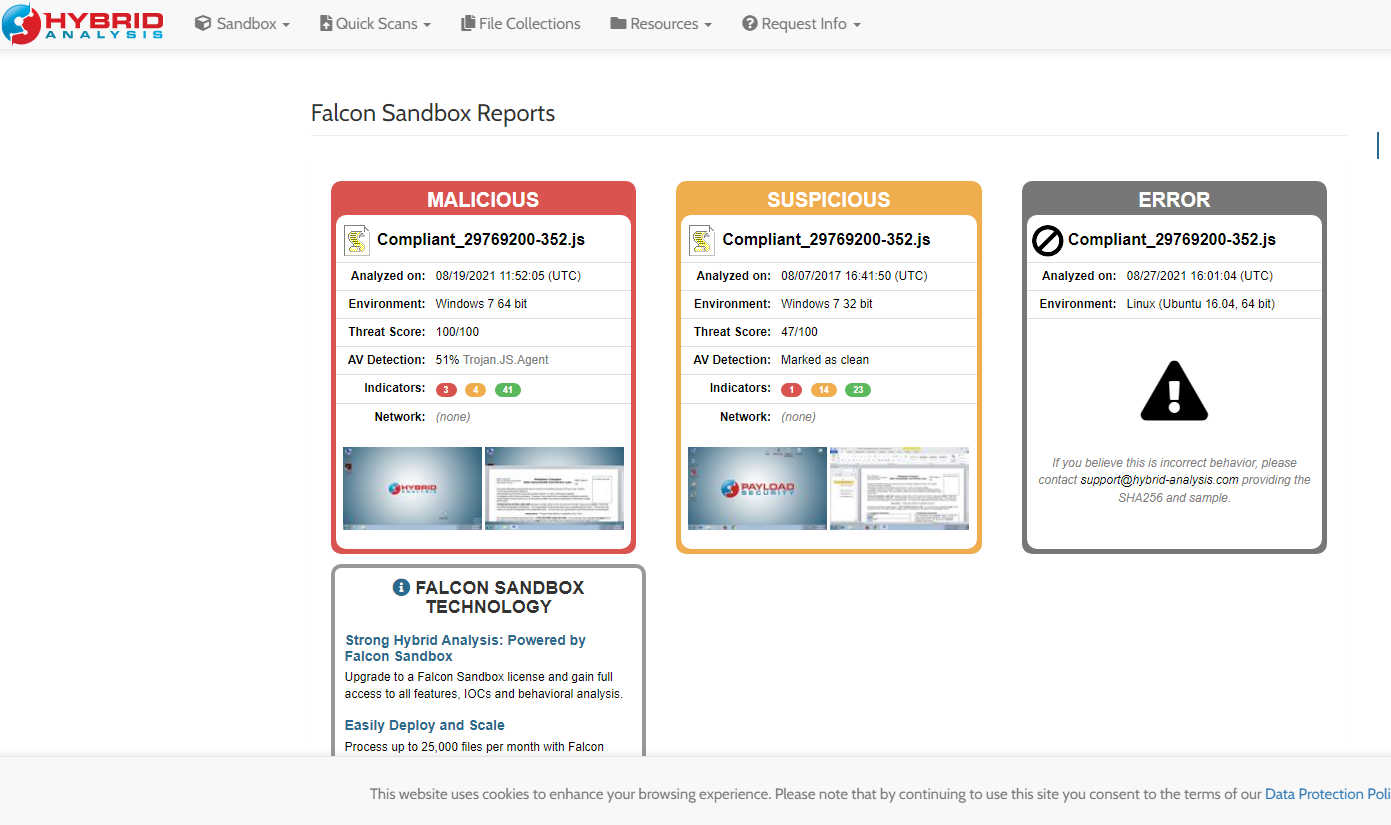
Verifying the script file in IBM X-force exchange. It marks it as a risk high file. The highlights show its hash type is sha256.

****

Scanning above file in Hybrid analysis. It also marks it as malicious.

****

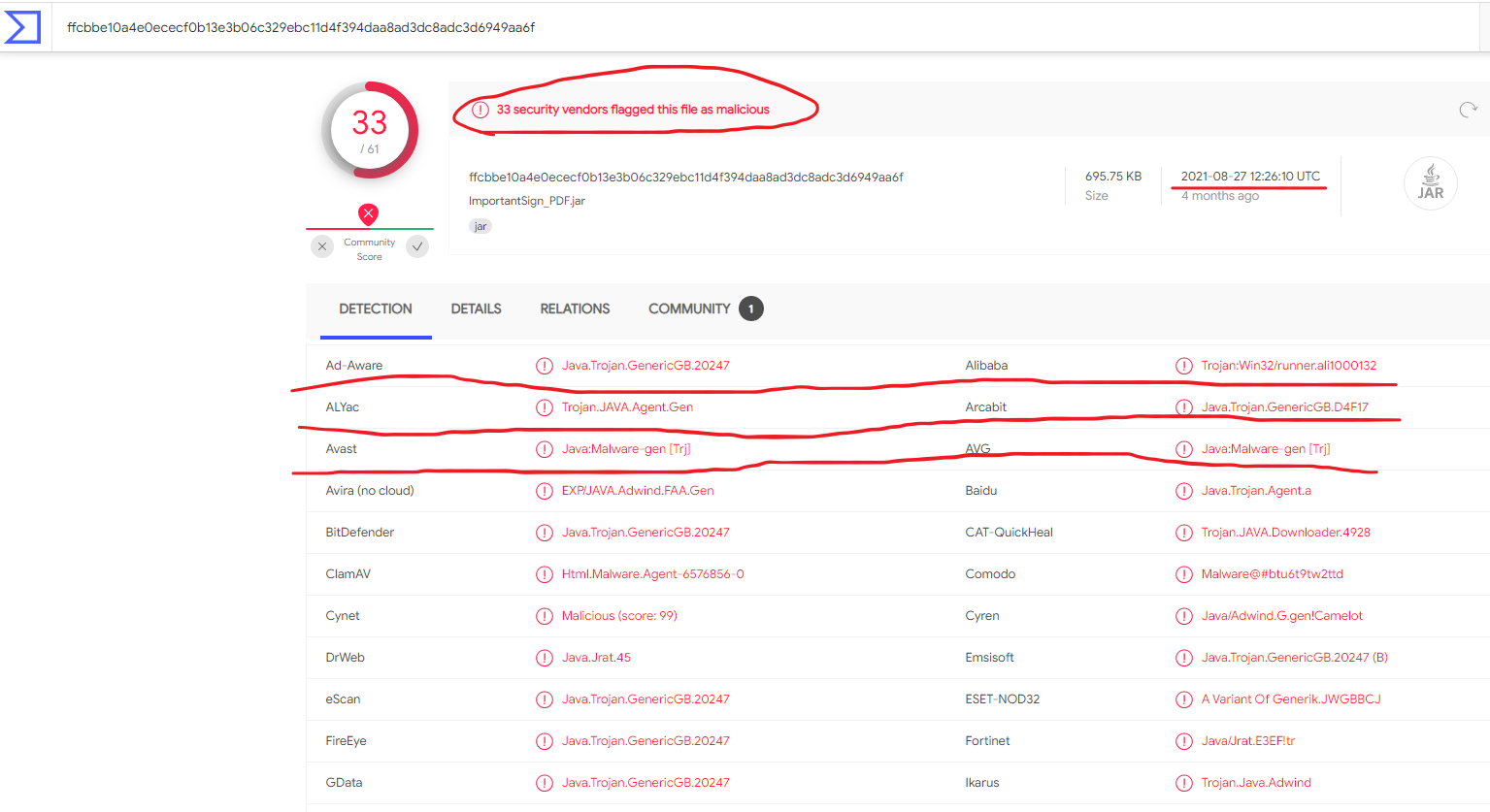
It shows its related files and file collections which are also malicious.

****

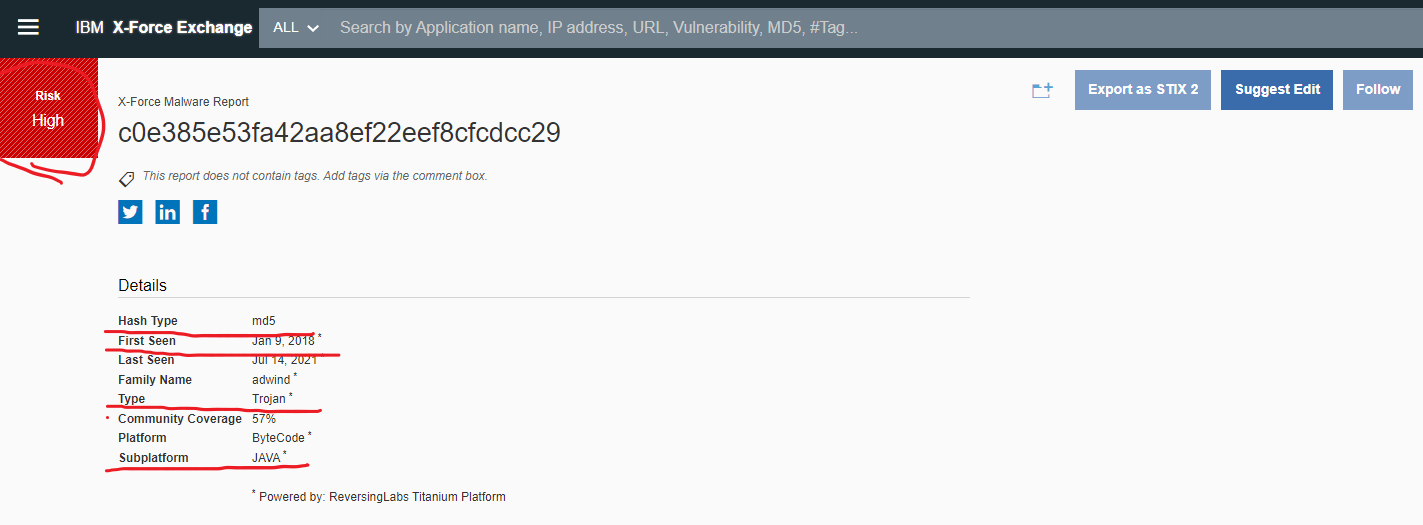
Falcon Sandbox reports are shown above.

From the above verification it is verified that the script of the file is malicious.

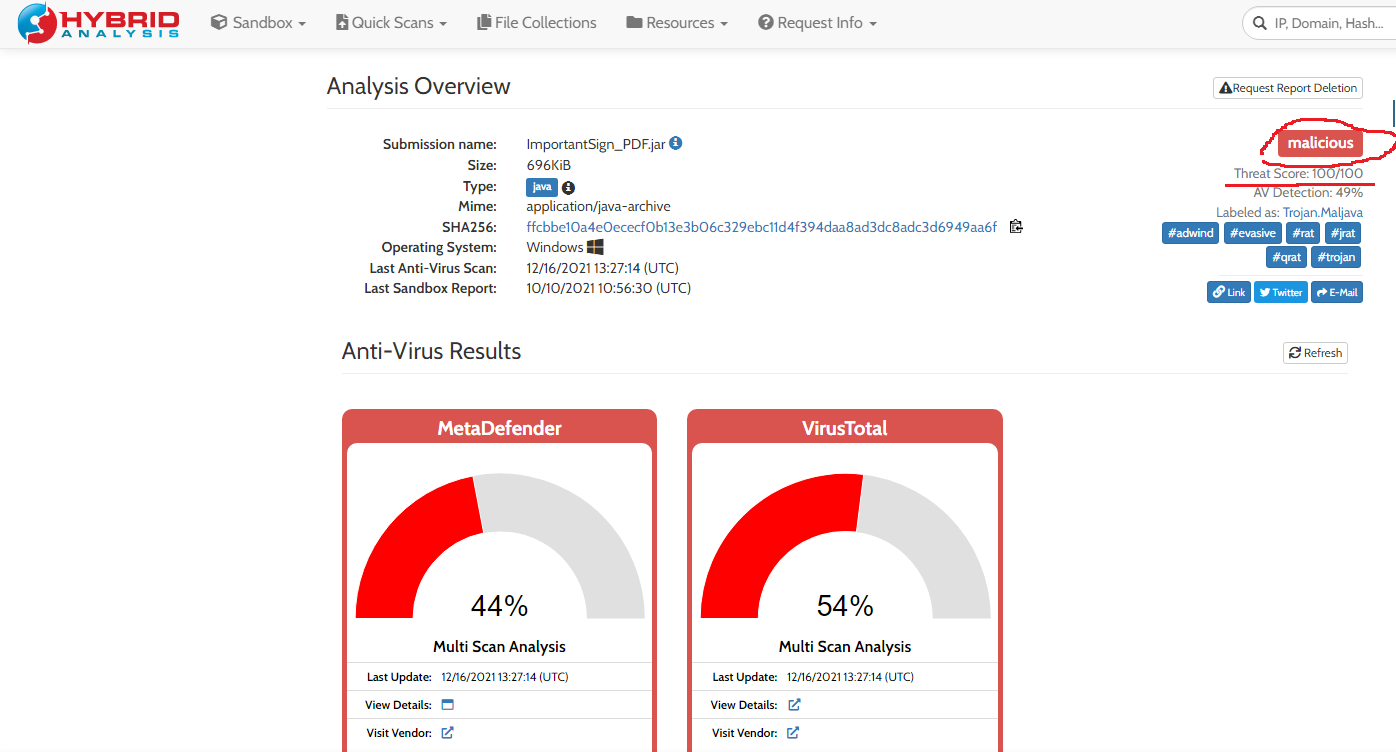
**ImportantSign\_PDF**

****

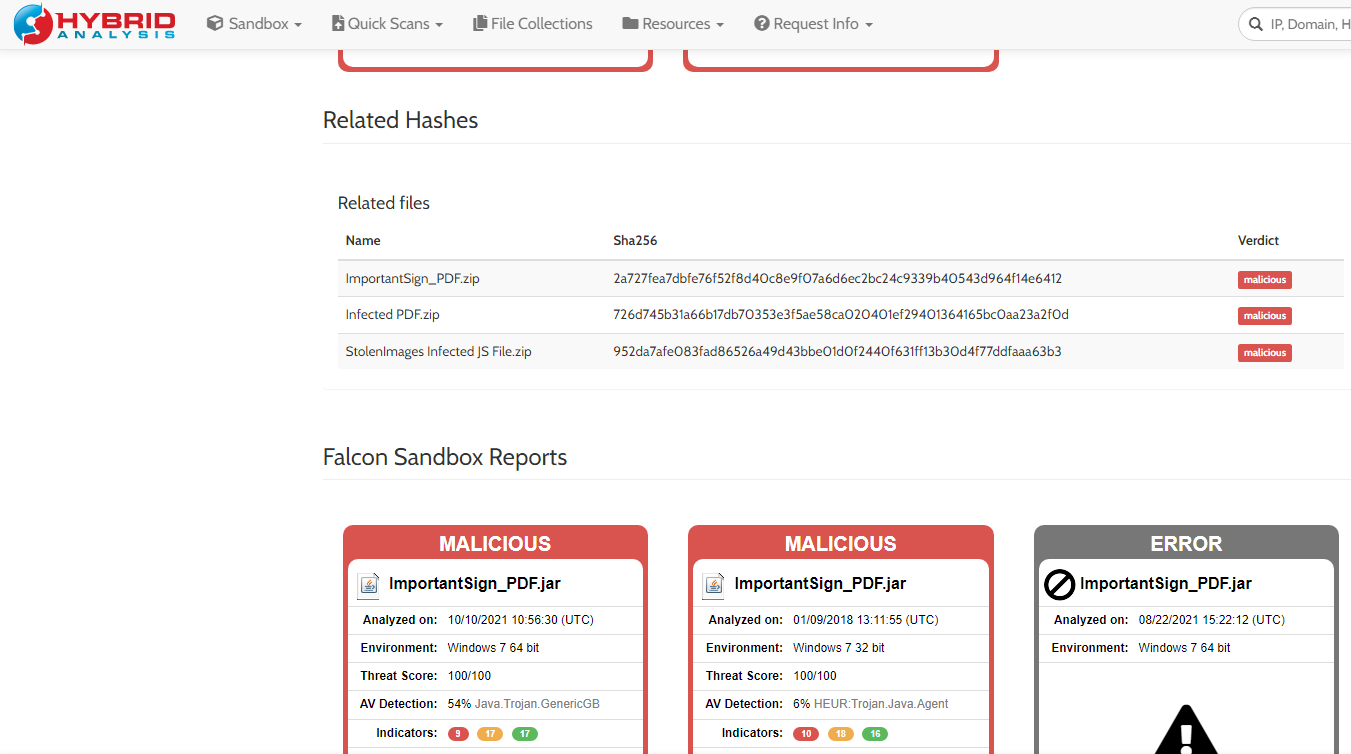
Verifying file in virustotal. Highlights show 33 security vendors flagged this file as malicious.

****

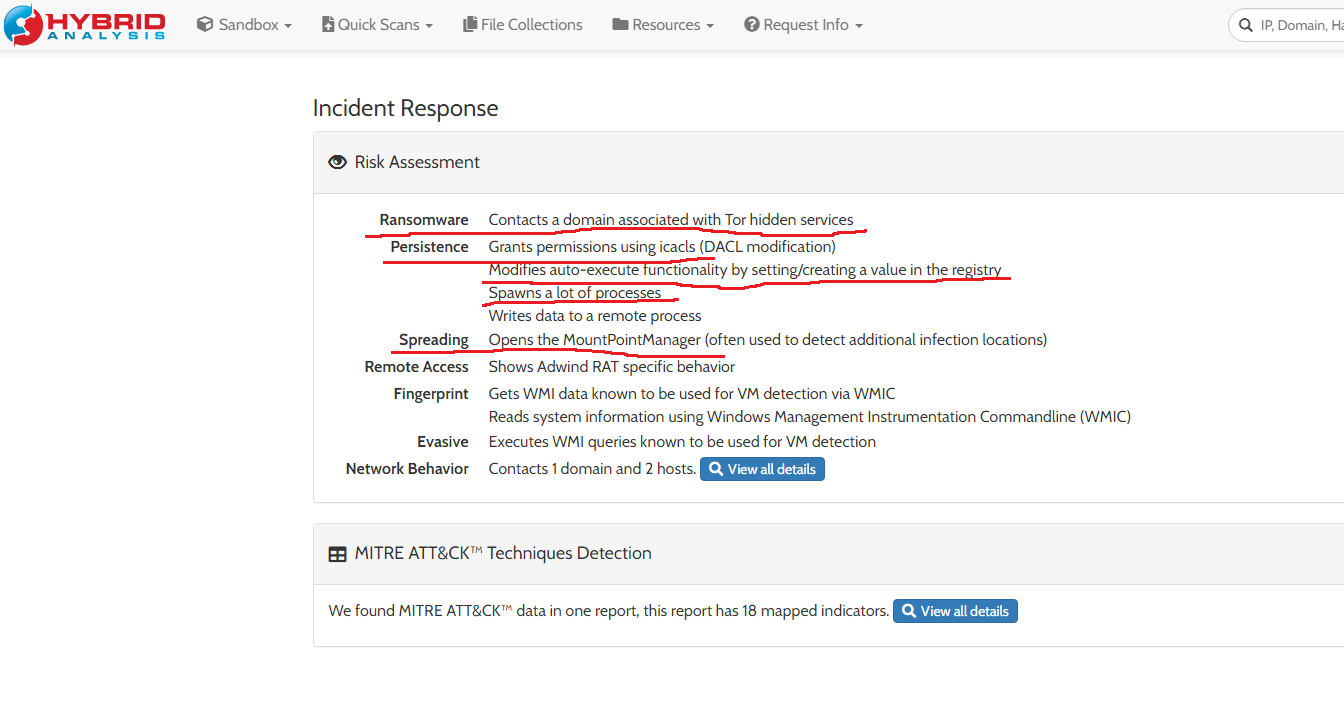
Verifying the file in IBM X-force exchange. It marks it as a risk high file. The highlights show its hash type is md5. It classified it as a trojan file.

****

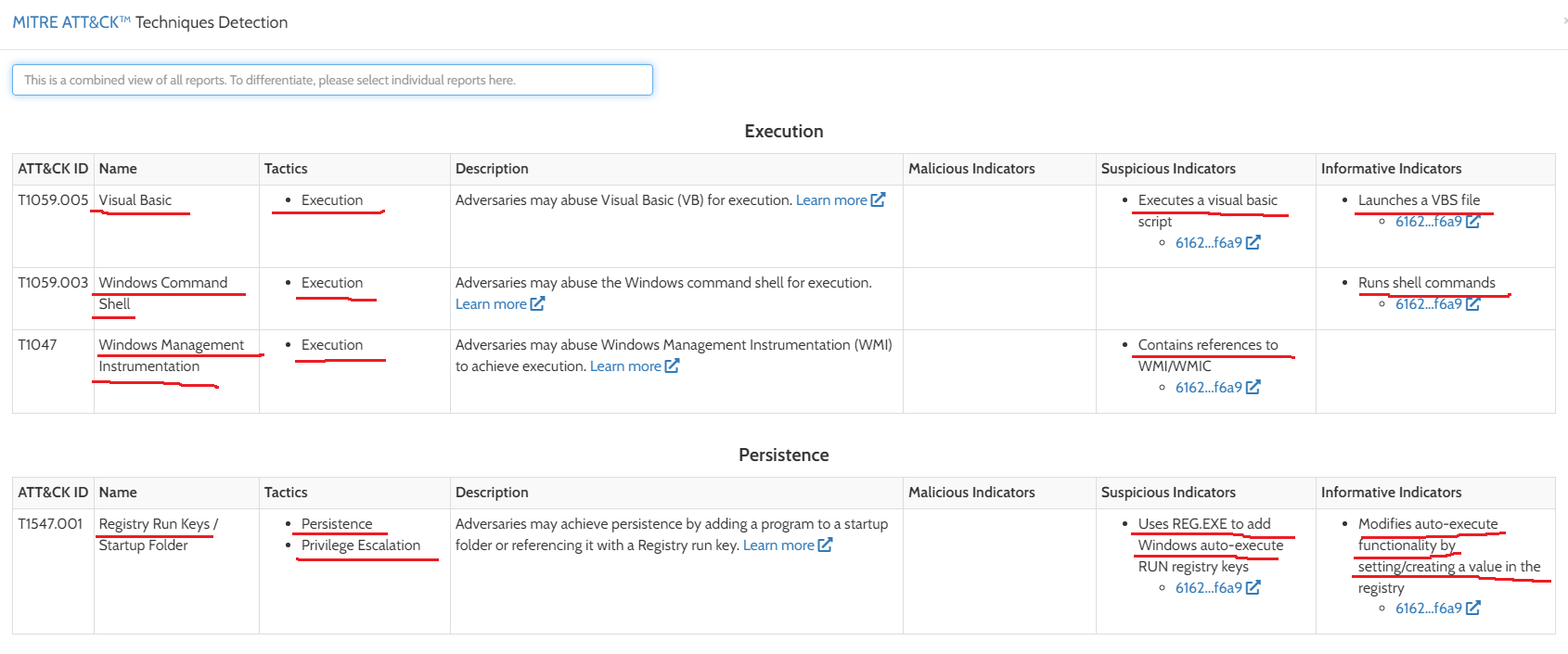
Scanning above file in Hybrid analysis. It also marks it as malicious.

****

It provides its related files and hashes which are also malicious. Falcon Sandbox reports showing threat score, environment in which the file got detected, analyzed date and time.

****

It shows risk assessment associated with the file which are ransomware, persistence, spreading, remote access and others highlighted above.

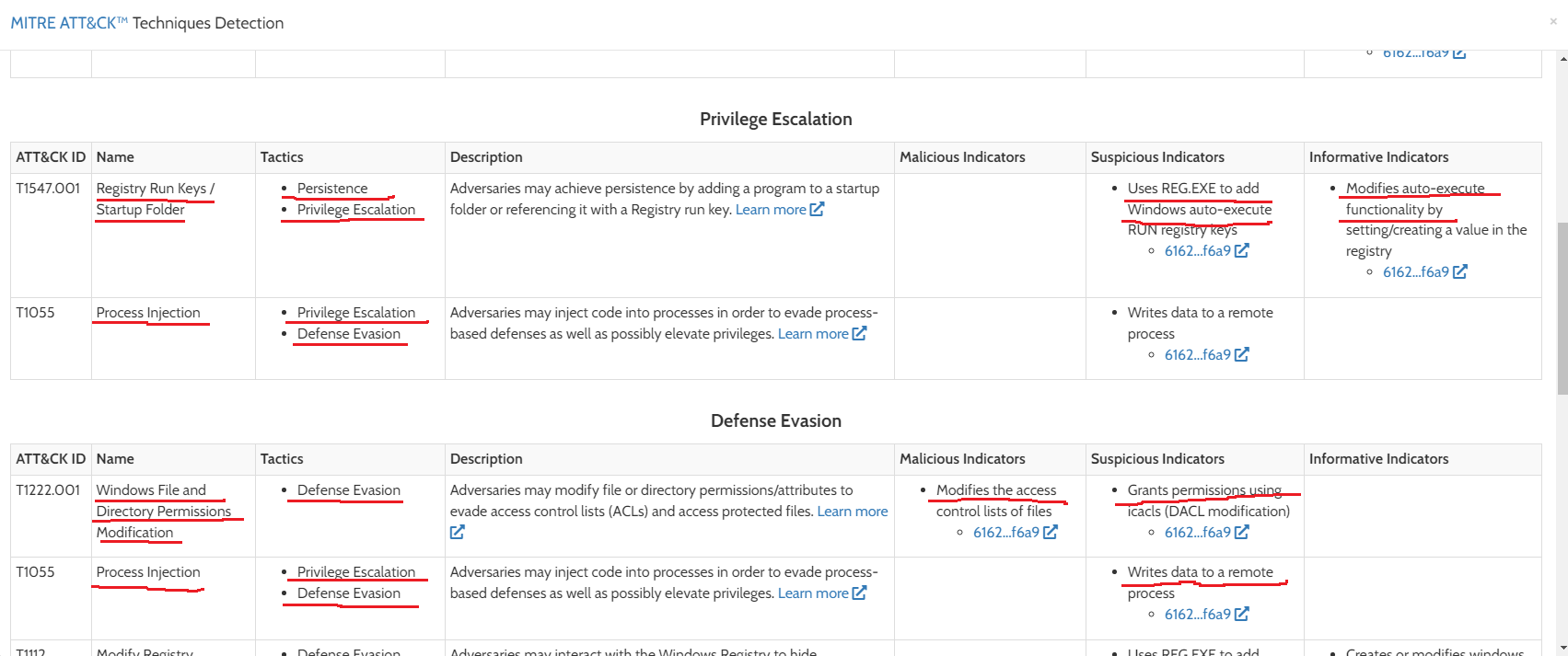
****

Found MITRE ATT&C data in one report, this report has 18 mapped indicators. These are the pre-indicators from an Attackers perspective telling how the trojan is proceeding.

It is using Visual Basic technique using tactic Execution whose suspicious and informative indicators are given.

It is using Windows Command Shell technique using tactic Execution whose informative indicators are given.

It is using Windows Management Instrumentation technique using tactic as Execution whose informative and suspicious indicators are given.

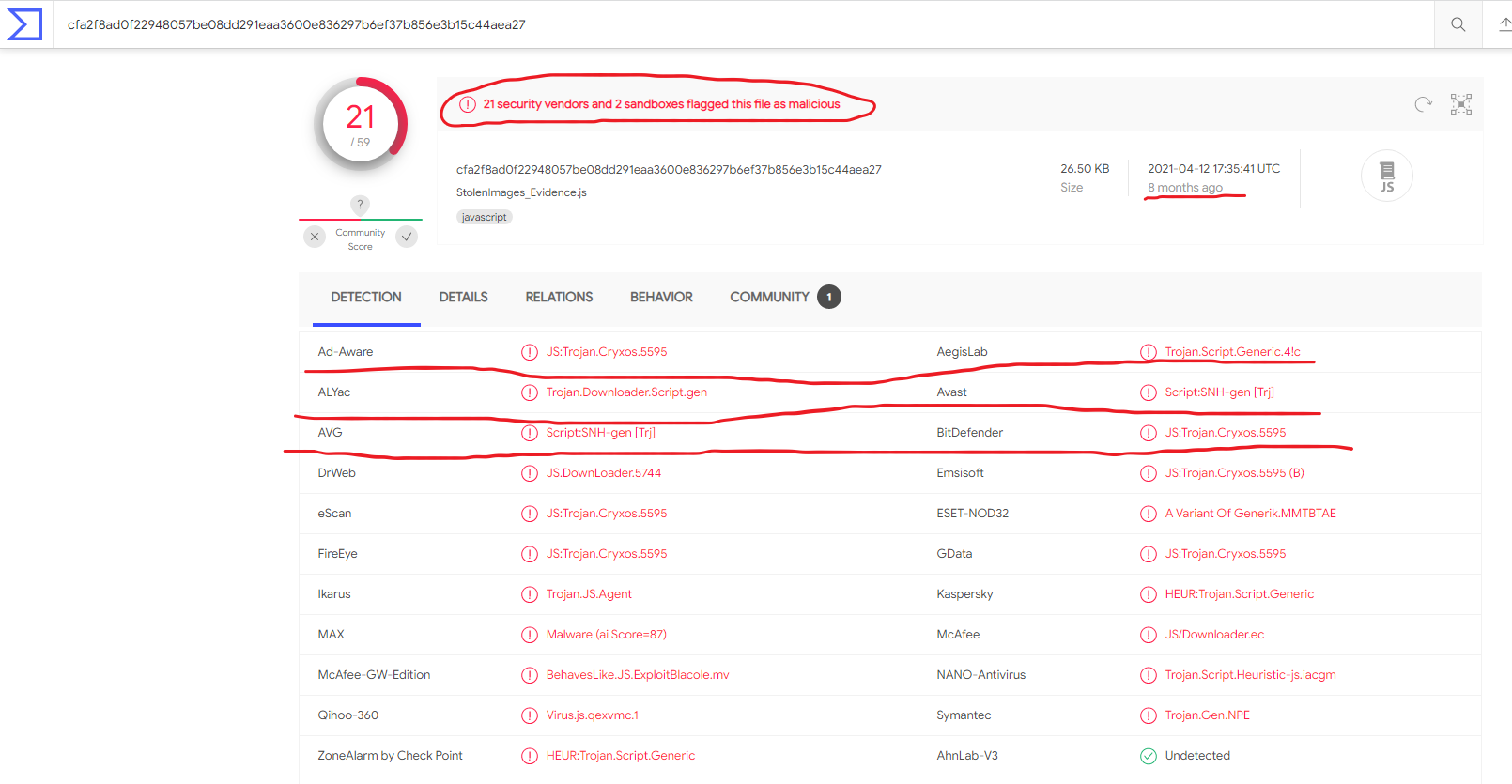
****

It is using Registry Run Keys / Startup Folder technique which is using tactics – Persistence and Privilege Escalation whose suspicious and informative indicators are given.

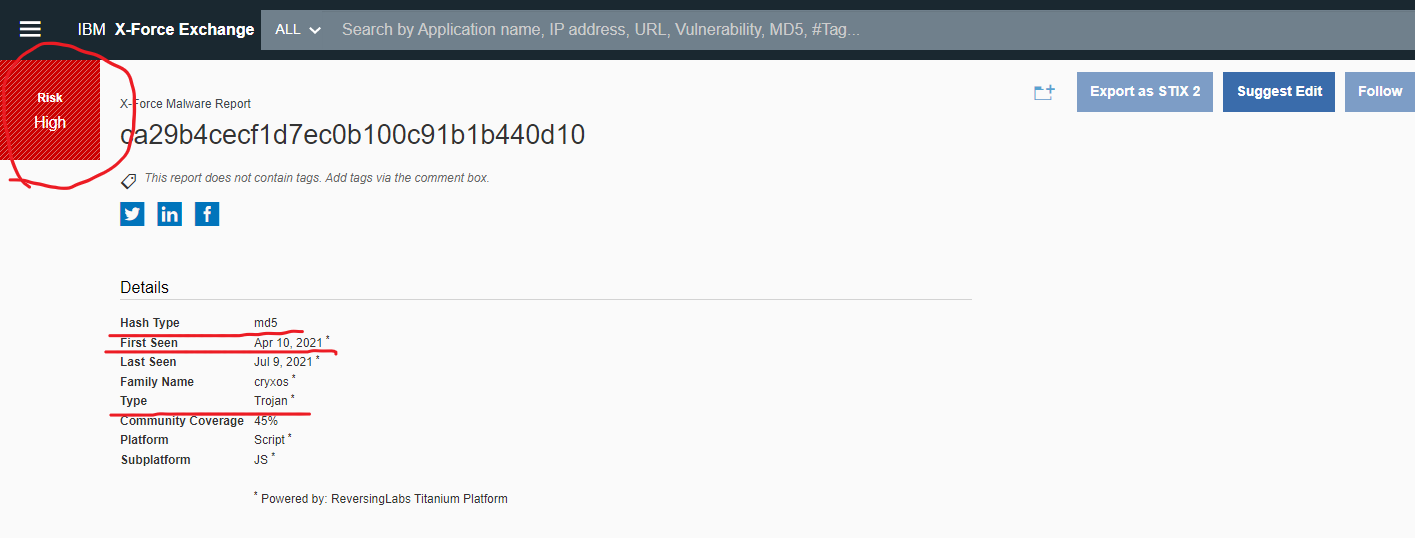
It is using Process Injection technique using tactics - Privilege Escalation and Defense Evasion whose malicious and suspicious indicators are given.

From the above verification we conclude that the file is malicious.

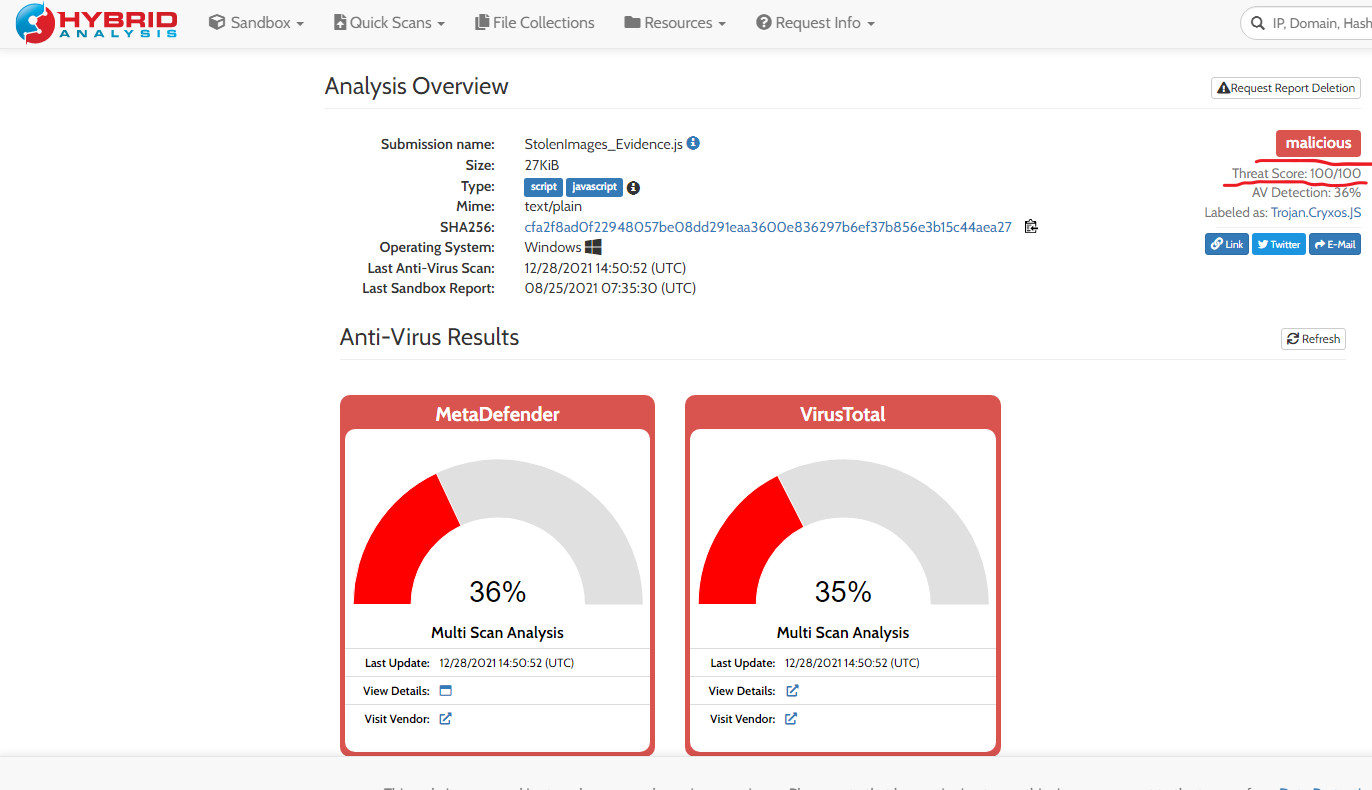
**StolenImages Infected JS File**

****

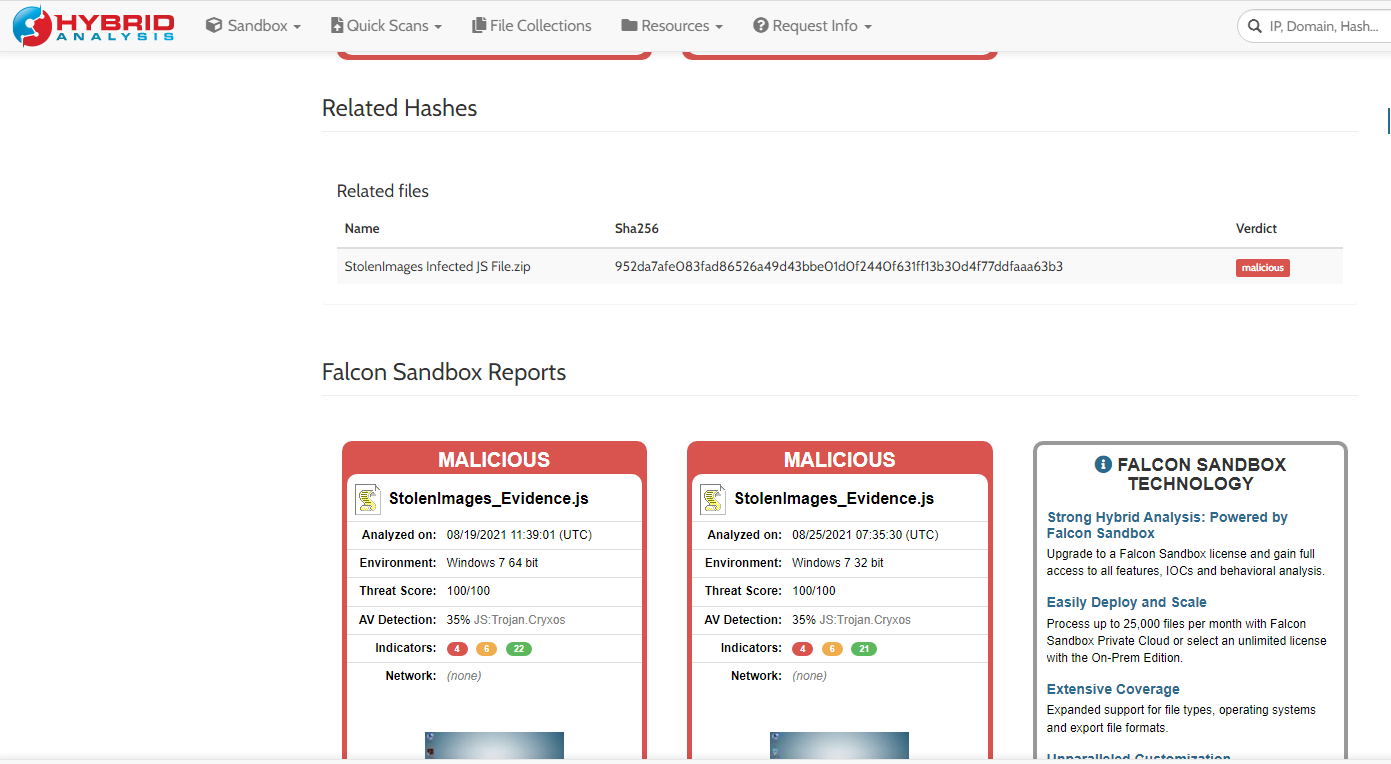
The site I have used here to verify is www.virustotal.com. Highlights show 21 security vendors and 2 sandboxes flagged this file as malicious. Ad-ware and Bitdefender shows it as a trojan.



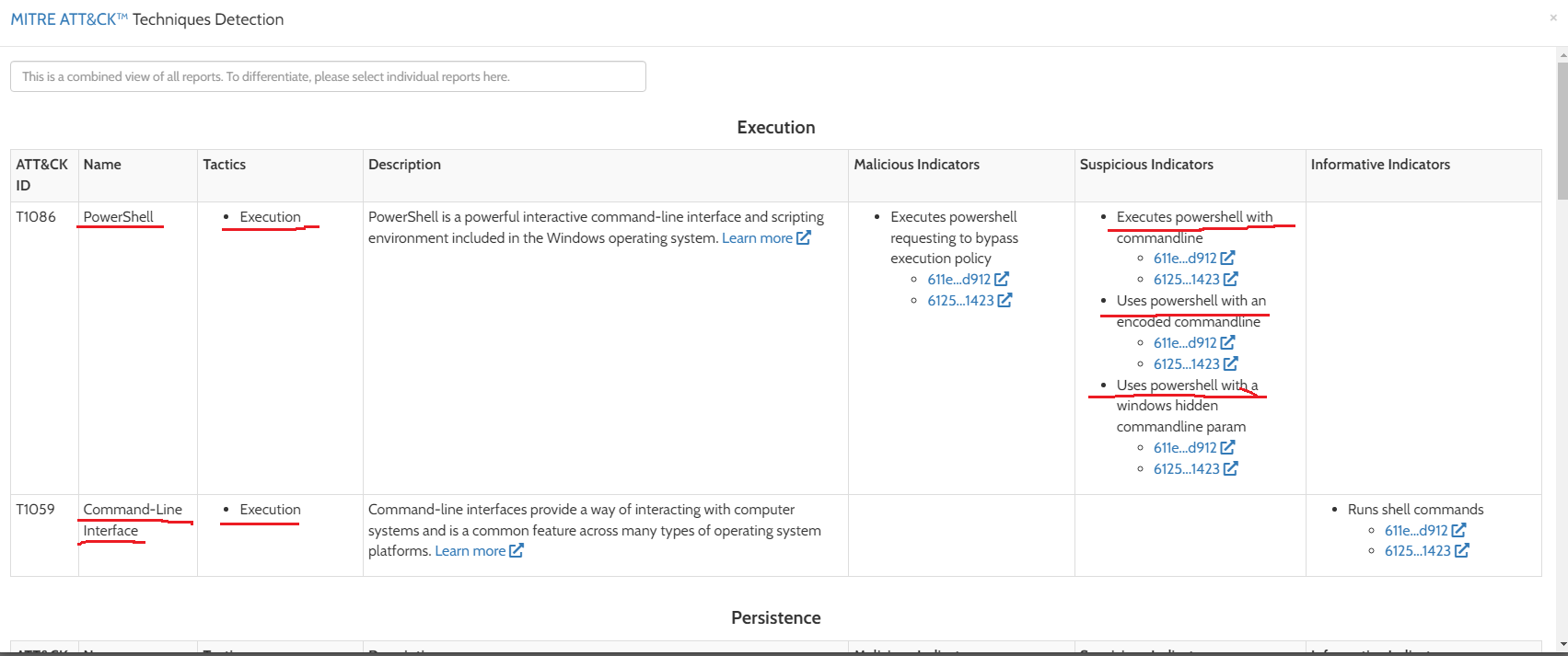
Verifying file in IBM X-force exchange. It marks it as a risk high file. Highlights show it as a trojan type.



Scanning file in hybrid analysis. Highlights show its threat score is 100/100.



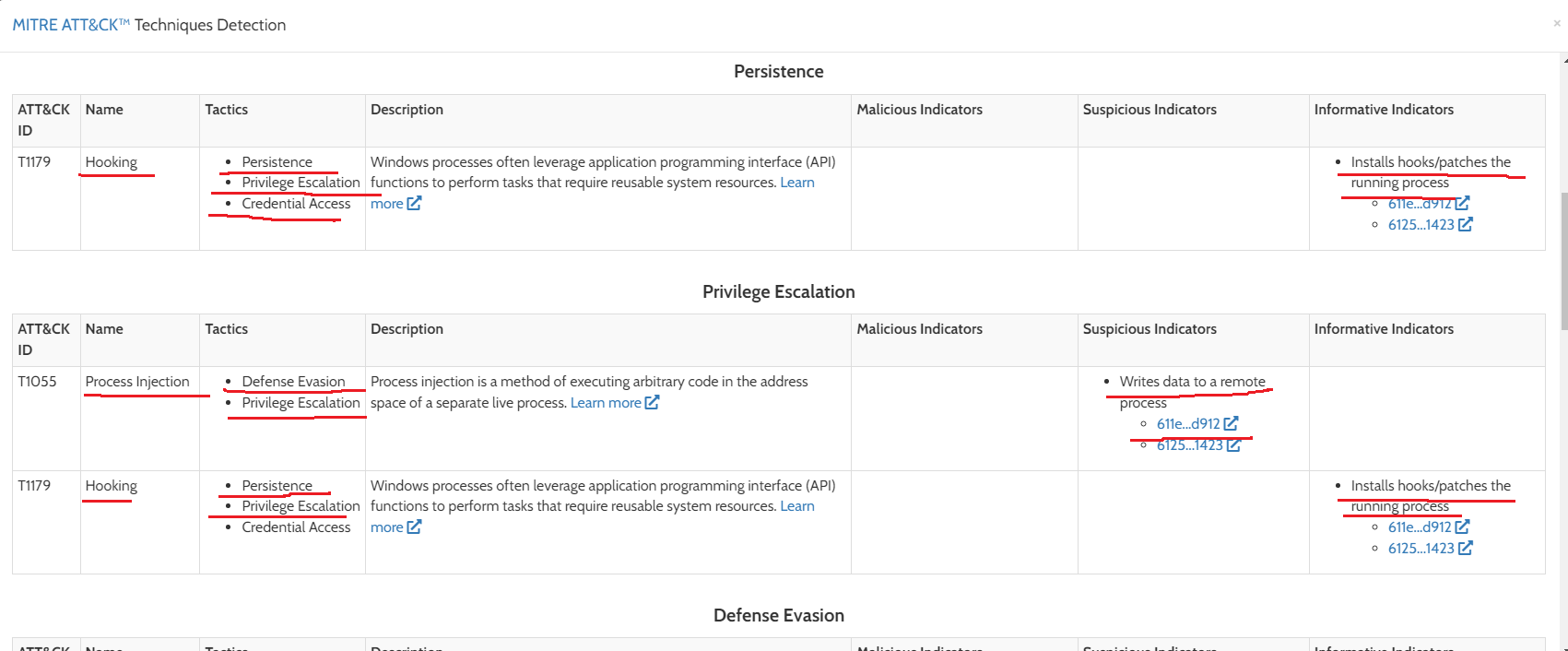
It displays its related hashes and files. Which are also malicious.



Found MITRE ATT&CK data in 2 reports, on average each report has 17 mapped indicators. These are the pre-indicators from an Attackers perspective telling how the trojan is proceeding.

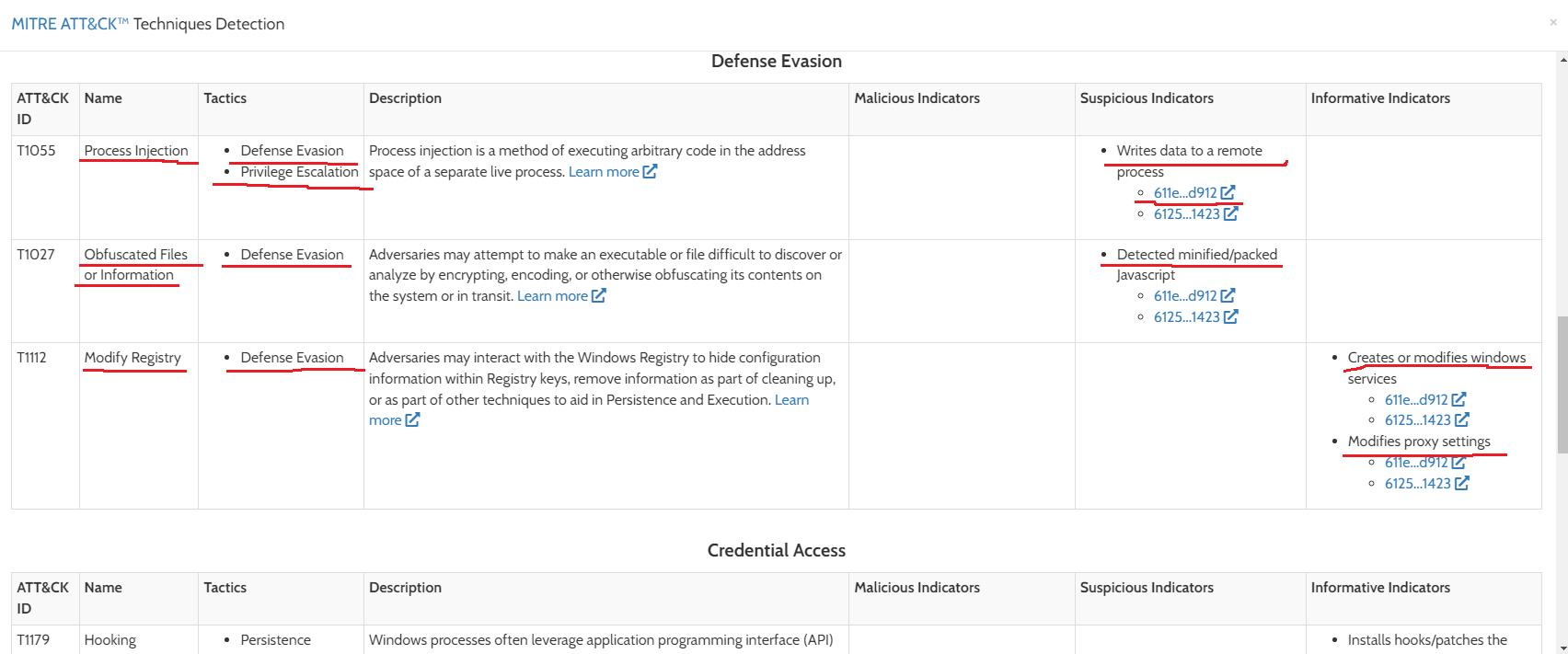
It is using PowerShell technique which is using tactic execution and indicators are given.

It is using Command-Line Interface technique which is using tactic execution and its indicators are given



It is using Hooking technique which is using tactics - persistence, privilege escalation, credential access and its indicators are given.

It is using Process Injection which is using tactics – Defense Evasion, privilege escalation and its indicators are given.



It is using Process Injection which is using tactics - Defense Evasion and Privilege Escalation and its indicators are given.

From the above verification we can conclude that the given file is malicious.