

**CHECKING THE INTEGRITY OF DATA USING THEIR  
HASH VALUES**

**BY**

**SOMKENE RICHARD**

**24TH SEPTEMBER,2024**

## **EXECUTIVE SUMMARY**

This report examines the integrity of five provided hashes to assess the safety of the associated data for interaction. After conducting a security scan using specialized tools, three of the hashes were identified as malicious, indicating that their data is unsafe for interaction. The remaining two hashes were confirmed to be free of malicious content, making their data safe for interaction.

## **INTRODUCTION**

Integrity is a key component of the CIA Triad (Confidentiality, Integrity, and Availability), a fundamental framework for safeguarding and enhancing data security. In cybersecurity, integrity ensures that system information is protected from intentional or accidental modification. This can be achieved through mechanisms such as hash functions.

For this report, the provided file hashes includes;

7DBD0DF279062090C34F796EFC7DD239ECCD46B99B67AAC370D6048D5ADBB9EC  
002ce0d28ec990aadb9c89df457189de37d8adaadc9c084b78eb7be9a9820c81  
e4d098122d676445d7e89826b59fe891a9bb9d3c78226e402406688cae0f7a62  
04631dabeccc7d887cc5317c6de48266272f1c90920d644c08895bc956ba3b3b  
9389a00c0f655dbddcb4fa420c4690b7d0ca672e19771a0f5f2e3479f31a7232

## **TOOL**

Virustotal

## ANALYSIS

The screenshot shows the VirusTotal web interface for a file with hash `7dbd0df279062090c34f796efc7dd239eccd46b99b67aac370d6048d5adbb9ec`. The file is identified as `apisetstub` (448.00 KB, analyzed 1 minute ago). It has a Community Score of 61/70 and is flagged as malicious by 61/70 security vendors. The file is categorized as a trojan, specifically `Trojan.Agent.QakBot`. The security vendors' analysis table shows detections from AhnLab-V3, ALYac, Arcabit, Alibaba, Antiy-AVL, and Avast, all identifying it as a trojan. The file is also associated with the threat label `trojan.cgws/qakbot` and family labels `cgws`, `qakbot`, and `bldr`.

Security vendors' analysis	
AhnLab-V3	Trojan.Win32.Generic.R203206
ALYac	Trojan.Agent.QakBot
Arcabit	Trojan.Agent.CGWS
Alibaba	Trojan.Win32/Kryptik.c08f3d75
Antiy-AVL	Trojan.Win32.SGeneric
Avast	Win32:Evo-gen [Trj]

*This hash can be seen to be malicious*

The screenshot shows the VirusTotal web interface for a file with hash `002ce0d28ec990aadb9c89df457189de37d8adaadc9c084b78eb7be9a9820c81`. The file is identified as `VSPerfCmdUI.dll` (391.45 KB, analyzed 13 hours ago). It has a Community Score of 0/73 and is flagged as benign by all security vendors. The file is categorized as a known-distributor, specifically `File distributed by Microsoft`. The security vendors' analysis table shows undetections from Acronis (Static ML), Alibaba, ALYac, Arcabit, AhnLab-V3, AliCloud, Antiy-AVL, and Avast. The file is also associated with the threat label `File distributed by Microsoft` and family labels `peexe`, `64bits`, `overlay`, `idle`, `detect-debug-environment`, `assembly`, `known-distributor`, and `signed`.

Security vendors' analysis	
Acronis (Static ML)	Undetected
Alibaba	Undetected
ALYac	Undetected
Arcabit	Undetected
AhnLab-V3	Undetected
AliCloud	Undetected
Antiy-AVL	Undetected
Avast	Undetected

*This hash can be seen to be malicious free*

https://www.virustotal.com/gui/file/e4d098122d676445d7e89826b59fe891a9bb9d3c78226e402406688cae0f7a62

e4d098122d676445d7e89826b59fe891a9bb9d3c78226e402406688cae0f7a62

58 / 72  
Community Score -1

58/72 security vendors flagged this file as malicious

Reanalyze Similar More

e4d098122d676445d7e89826b59fe891a9bb9d3c78226e402406688cae0f7a62  
YLzk.exe  
Size: 590.50 KB  
Last Analysis Date: 18 hours ago  
EXE

peexe checks-user-input assembly spreader long-sleeps checks-bios checks-network-adapters detect-debug-environment calls-wmi

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/agenla Threat categories trojan Family labels msil agenla agenttesla

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan.Win.Injection.C5456949	Alibaba	Trojan.PSW:MSIL/Agensla.10009756
ALYac	Trojan.GenericKDZ.101967	Antiy-AVL	Trojan/MSIL.GenKryptik
Arcabit	Trojan.Generic.D18E4F	Avast	Win32:CrypterX-gen [Trj]

*This hash can be seen to be malicious*

https://www.virustotal.com/gui/file/04631dabeccc7d887cc5317c6de48266272f1c90920d644c08895bc956ba3b3b

04631dabeccc7d887cc5317c6de48266272f1c90920d644c08895bc956ba3b3b

0 / 74  
Community Score

File distributed by Microsoft

Reanalyze Similar More

04631dabeccc7d887cc5317c6de48266272f1c90920d644c08895bc956ba3b3b  
VCPkgSrv.exe  
Size: 122.95 KB  
Last Analysis Date: 3 months ago  
EXE

peexe detect-debug-environment overlay known-distributor signed idle trusted

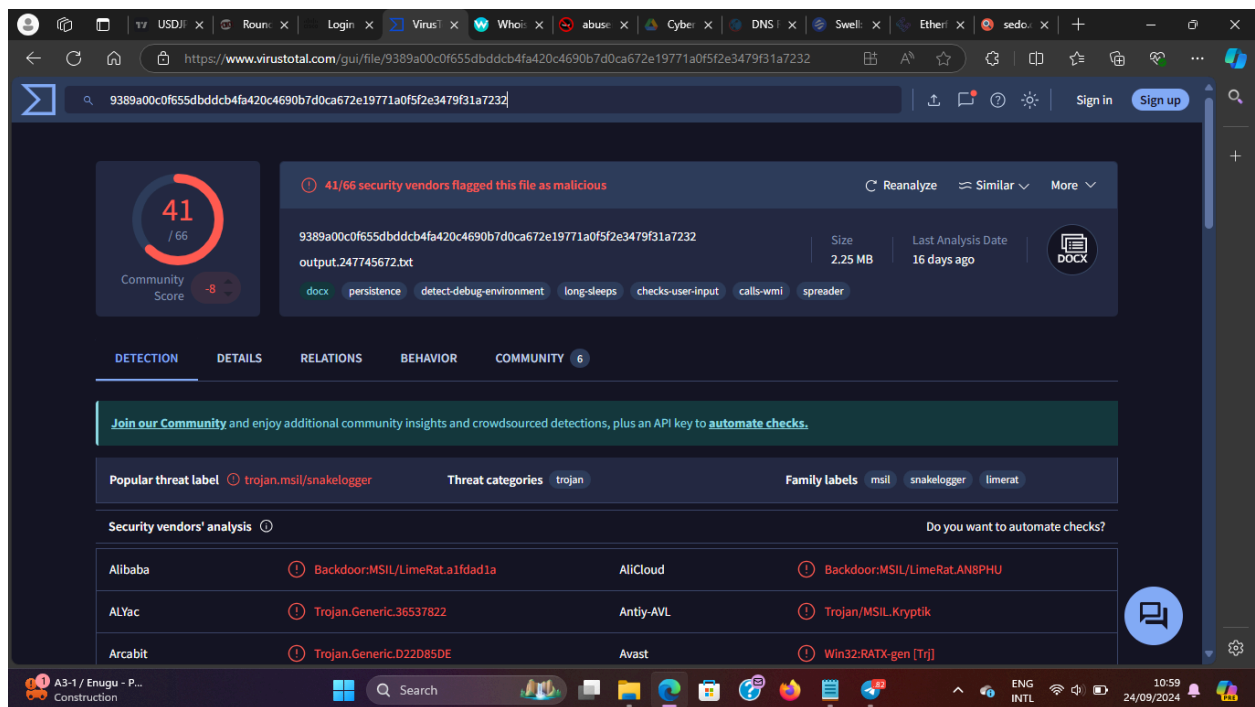
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected

*This hash can be seen to be malicious free*



*This hash can be seen to be malicious*

## RECOMMENDATIONS

1. Monitor for hash anomalies: doing this will help ascertain when a file has been altered or compromised.
2. Educating employees and individuals on the importance of data integrity and proper use of hashing.
3. Conduct regular hash verification to help detect any unauthorized modifications.
4. Regularly conduct security audits and assessments of your data integrity processes to identify weaknesses and areas for improvement.

## CONCLUSION

Using a secure and widely accepted hashing algorithm such as SHA-256 or SHA-3 for data integrity checks in cybersecurity is advisable as outdated or weak algorithms like MD5 or SHA-1 are susceptible to vulnerabilities.