

# SecurityOps

## ANALYSIS

### Report Summary

User Group	Security Operations
Reference Ticket	ITE123456
Target	de2ac4e6a70f561bee933528675a5f145ddc257c575c70d75891277fe42a7b7f
Date Generated	30/06/2022 22:53:45 PST
Scanner	API-OSINT Automater (Python3)
Version	v.0.1

### Security Vendors' Analysis

[+] VirusTotal (URL, IP address, Domain and Hash)	Security vendors found it as <b>Malicious</b>
[+] AbuseIPDB (IP address and Domain)	
[+] Shodan (IP address)	
[+] URLScanIO (URL)	
[+] GreyNoise (IP address)	
[+] IBM X-Force (URL, IP address and Domain)	

### Detailed Information

VirusTotal

AbuseIPDB

Shodan

URLScanIO

GreyNoise

IBM X-Force

Others

SUMMARY

Score

14 / 58

Last Analysis Date

2022-05-26 08:22:06

Virus Total

[View Full Report](#)

SCAN

Scanner

Detected

Version

Result

Update

K7AntiVirus

True

12.14.42511

Exploit ( 04c557941 )

20220526

K7GW

True

12.14.42510

Exploit ( 04c557941 )

20220526

VirIT

True

9.5.203

JS.Agent.U

20220525

Cyren

True

6.5.1.2

JS/Phish.SX

20220526

ESET-NOD32

True

25329

HTML/Phishing.Agent.CAR

20220526

Avast	True	21.1.5827.0	<b>Other:SNH-gen [Phish]</b>	20220526
Cynet	True	4.0.0.27	<b>Malicious (score: 99)</b>	20220526
Kaspersky	True	21.0.1.45	<b>HEUR:Trojan.Script.Generic</b>	20220526
F-Secure	True	18.10.978.51	<b>Malware.HTML/Infected.WebPage.Gen2</b>	20220526
Avira	True	8.3.3.14	<b>HTML/Infected.WebPage.Gen2</b>	20220526
ZoneAlarm	True	1.0	<b>HEUR:Trojan.Script.Generic</b>	20220526
Ikarus	True	6.0.24.0	<b>Phishing.HTML.Doc</b>	20220525
Fortinet	True	6.2.142.0	<b>HTML/Phish.C1E3!tr</b>	20220526
AVG	True	21.1.5827.0	<b>Other:SNH-gen [Phish]</b>	20220526