Uploaded File Report

File Type: Rich Text Format

**SHA256 Hash of File:
0af43e1d9e43069d04daed4d281f043c90deb59535c00bc1fae87c0058decfac**

Antivirus Scanners that fond uploded file Malicious:

MicroWorld-eScan

- **method:** blacklist

- **engine_name:** MicroWorld-eScan

- **engine_version:** 14.0.409.0

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

CTX

- **method:** blacklist

- **engine_name:** CTX

- **engine_version:** 2024.8.29.1

- **engine_update:** 20240929

- **category:** malicious

- **result:** rtf.exploit-kit.obfsobjdat

ALYac

- **method:** blacklist

- **engine_name:** ALYac

- **engine_version:** 2.0.0.10

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

Sangfor

- **method:** blacklist
- **engine_name:** Sangfor
- **engine_version:** 2.25.10.0
- **engine_update:** 20240926
- **category:** malicious
- **result:** Malware.Generic-RTF.Save.6dc7af2a

Arcabit

- **method:** blacklist
- **engine_name:** Arcabit
- **engine_version:** 2022.0.0.18
- **engine_update:** 20240929
- **category:** malicious
- **result:** Exploit.RTF-ObfsObjDat.Gen

Avast

- **method:** blacklist
- **engine_name:** Avast
- **engine_version:** 23.9.8494.0
- **engine_update:** 20240929
- **category:** malicious
- **result:** OLE:CVE-2018-0798 [Expl]

BitDefender

- **method:** blacklist
- **engine_name:** BitDefender

- **engine_version:** 7.2

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

Emsisoft

- **method:** blacklist

- **engine_name:** Emsisoft

- **engine_version:** 2024.1.0.53752

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen (B)

VIPRE

- **method:** blacklist

- **engine_name:** VIPRE

- **engine_version:** 6.0.0.35

- **engine_update:** 20240928

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

Ikarus

- **method:** blacklist

- **engine_name:** Ikarus

- **engine_version:** 6.3.23.0

- **engine_update:** 20240928

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat

FireEye

- **method:** blacklist

- **engine_name:** FireEye

- **engine_version:** 35.47.0.0

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

GData

- **method:** blacklist

- **engine_name:** GData

- **engine_version:** A:25.38968B:27.37628

- **engine_update:** 20240929

- **category:** malicious

- **result:** Exploit.RTF-ObfsObjDat.Gen

Google

- **method:** blacklist

- **engine_name:** Google

- **engine_version:** 1727587844

- **engine_update:** 20240929

- **category:** malicious

- **result:** Detected

AVG

- **method:** blacklist

- **engine_name:** AVG

- **engine_version:** 23.9.8494.0

- **engine_update:** 20240929

- **category:** malicious

- **result:** OLE:CVE-2018-0798 [Expl]

Category wise Antivirus Scanners:

undetected

- Bkav

- Lionic

- tehtris

- ClamAV

- CAT-QuickHeal

- Skyhigh

- Malwarebytes

- Zillya

- K7AntiVirus

- K7GW

- CrowdStrike

- Baidu

- VirIT

- Symantec

- ESET-NOD32

- TrendMicro-HouseCall

- Cynet

- Kaspersky

- NANO-Antivirus

- SUPERAntiSpyware

- Tencent

- F-Secure

- DrWeb

- TrendMicro

- CMC

- Sophos

- Jiangmin

- Varist

- Avira

- Antiy-AVL

- Kingsoft

- Gridinsoft

- Xcitium

- Microsoft

- ViRobot

- ZoneAlarm

- AhnLab-V3

- Acronis

- McAfee

- TACHYON

- VBA32

- Zoner

- Rising

- Yandex

- huorong

- MaxSecure

- Fortinet

- Panda

- alibabacloud

type-unsupported

- Avast-Mobile

- SymantecMobileInsight

- BitDefenderFalx

- McAfeeD

- DeepInstinct

- APEX

- Paloalto

- Trapmine

- Alibaba

- Webroot

- Cylance

- SentinelOne

- Trustlook

- Elastic

Made with ❤ by Neel Thakor