silverhack

In this report is documented a large variety of public information of Malware related

Threat Intelligent Analysis

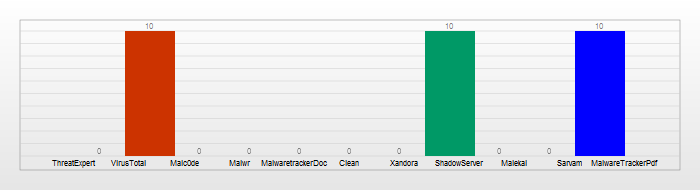
Analysis for MD5 fc67c763fc57a1a47210559613dfc5d5

# File Information

General information about the threat that is shared between websites.
Use this to match your suspicious sample and determine if the information
provided by this report is or is not accurate.

|  |  |
| --- | --- |
| MD5 | fc67c763fc57a1a47210559613dfc5d5 |
| SHA1 | 41dfa78fb7479be33de043ac6a647e71d18aea2f |
| First\_seen | Unknow |
| last\_seen | Unknow |
| Filetype | pdf |
| Size | Unknow |
| Ssdeep | Unknow |

# Graph With data founded

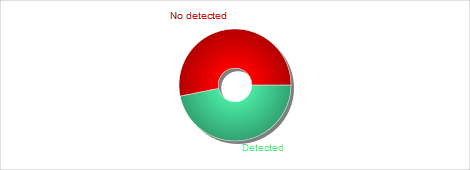


# Analysys Information

The following section presents antivirus detection of the sample being analysed.

## Antivirus detection at Virustotal

VirusTotal scans files using a large number of antiviruses;
this is the breakdown of the results. Go to Annex for VirusTotal complete information.



# Annex VirusTotal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Antivirus\_Name | Detection | Version | Result | Update |
| Bkav | False | 1.3.0.4613 |  | 20131230 |
| MicroWorld-eScan | True | 12.0.250.0 | Exploit.PDF-JS.Gen | 20131230 |
| nProtect | True | 2013-12-30.01 | Exploit.PDF-JS.Gen | 20131230 |
| CAT-QuickHeal | False | 12.00 |  | 20131230 |
| McAfee | False | 5.600.0.1067 |  | 20131230 |
| Malwarebytes | False | 1.75.0.1 |  | 20131230 |
| K7AntiVirus | False | 9.174.10656 |  | 20131227 |
| K7GW | False | 9.174.10661 |  | 20131228 |
| TheHacker | False | 6.8.0.5.385 |  | 20131229 |
| NANO-Antivirus | True | 0.28.0.57029 | Exploit.Script.Pdfka.zzoax | 20131230 |
| F-Prot | True | 4.7.1.166 | JS/ShellCode.DF.gen | 20131230 |
| Symantec | True | 20131.1.5.61 | Bloodhound.Exploit.357 | 20131230 |
| Norman | True | 7.03.02 | Exploit.US | 20131230 |
| TotalDefense | False | 37.0.10498 |  | 20131230 |
| TrendMicro-HouseCall | False | 9.700.0.1001 |  | 20131230 |
| Avast | False | 8.0.1489.320 |  | 20131230 |
| ClamAV | False | 0.97.3.0 |  | 20131230 |
| Kaspersky | True | 12.0.0.1221 | Exploit.Win32.CVE-2010-2883.a | 20131229 |
| BitDefender | True | 7.2.5028.0 | Exploit.PDF-JS.Gen | 20131230 |
| Agnitum | True | 5.5.1.3 | Exploit.CVE-2010-2883 | 20131228 |
| ViRobot | False | 2011.4.7.4223 |  | 20131230 |
| Ad-Aware | True | 12.0.163.0 | Exploit.PDF-JS.Gen | 20131230 |
| Emsisoft | True | 3.0.0.596 | Exploit.PDF-JS.Gen (B) | 20131230 |
| Comodo | False | 17523 |  | 20131230 |
| DrWeb | True |  | Exploit.PDF.2197 | 20131230 |
| VIPRE | True | 24908 | Exploit.PDF.CVE-2010-2883 (v) | 20131230 |
| AntiVir | True | 7.11.122.186 | EXP/Pidief.ZM | 20131230 |
| TrendMicro | False | 9.740.0.1012 |  | 20131230 |
| McAfee-GW-Edition | False | 2013 |  | 20131230 |
| Sophos | True | 4.96.0 | Troj/PDFJs-NA | 20131230 |
| Jiangmin | False | 16.0.100 |  | 20131230 |
| Antiy-AVL | False | 2.0.3.7 |  | 20131230 |
| Kingsoft | False | 2013.4.9.267 |  | 20130829 |
| Microsoft | True | 1.10201 | Exploit:Win32/CVE-2010-2883.C | 20131230 |
| SUPERAntiSpyware | False | 5.6.0.1032 |  | 20131229 |
| AhnLab-V3 | True | 2013.12.31.00 | PDF/Cve-2010-2883 | 20131230 |
| GData | True | 22 | Exploit.PDF-JS.Gen | 20131230 |
| Commtouch | True | 5.4.1.7 | JS/ShellCode.DF.gen | 20131230 |
| ByteHero | False | 1.0.0.1 |  | 20131226 |
| VBA32 | False | 3.12.24.3 |  | 20131230 |
| Panda | False | 10.0.3.5 |  | 20131230 |
| ESET-NOD32 | False | 9190 |  | 20131230 |
| Rising | True | 25.0.0.11 | PDF:Attention.APT-Bait.OddDocument/RDM!5.38 | 20131230 |
| Ikarus | False | T3.1.5.6.0 |  | 20131230 |
| Fortinet | True | 5.1.147.0 | PDF/CoolType!exploit.CVE20102883 | 20131230 |
| AVG | True | 13.0.0.3169 | Exploit.PDF | 20131230 |
| Baidu-International | False | 3.5.1.41473 |  | 20131213 |

# Annex Malwaretracker

## Basic information for PDF found

**Filename: 138e6d4673cc3ebc1aa423feba9d8f53c8cb9f017e15da2f798bd987c7abaf8c**

**Submitted: 2014-01-10 16**

**Size: 313920**

**MD5: fc67c763fc57a1a47210559613dfc5d5**

**Sha1: 41dfa78fb7479be33de043ac6a647e71d18aea2f**

**Sha256: 138e6d4673cc3ebc1aa423feba9d8f53c8cb9f017e15da2f798bd987c7abaf8c**

**ssdeep: 6144:eEC5dOjLExJskZ+87T/4+4dAaYWu2STBwFG/Lie/+lbHLBSz:epPsyJskZ+87T/4+4dAaYW0D/x/+lbHe**

**Severity: 100**

The PDF file is not encryptedb

## Exploits used in PDF file

* **pdf.exploit fontfile SING table overflow CVE-2010-2883 A**
* **pdf.exploit fontfile SING table overflow CVE-2010-2883 generic**
* **suspicious.flash Embedded Flash define obj**
* **suspicious.obfuscation using substring**

## Online information for PDF file

**URL: https://www.malwaretracker.com/pdfdata.php?md5=fc67c763fc57a1a47210559613dfc5d5&type=document**