Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-02-01 00:00:00+0100
To: 2024-03-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.2, build 11426

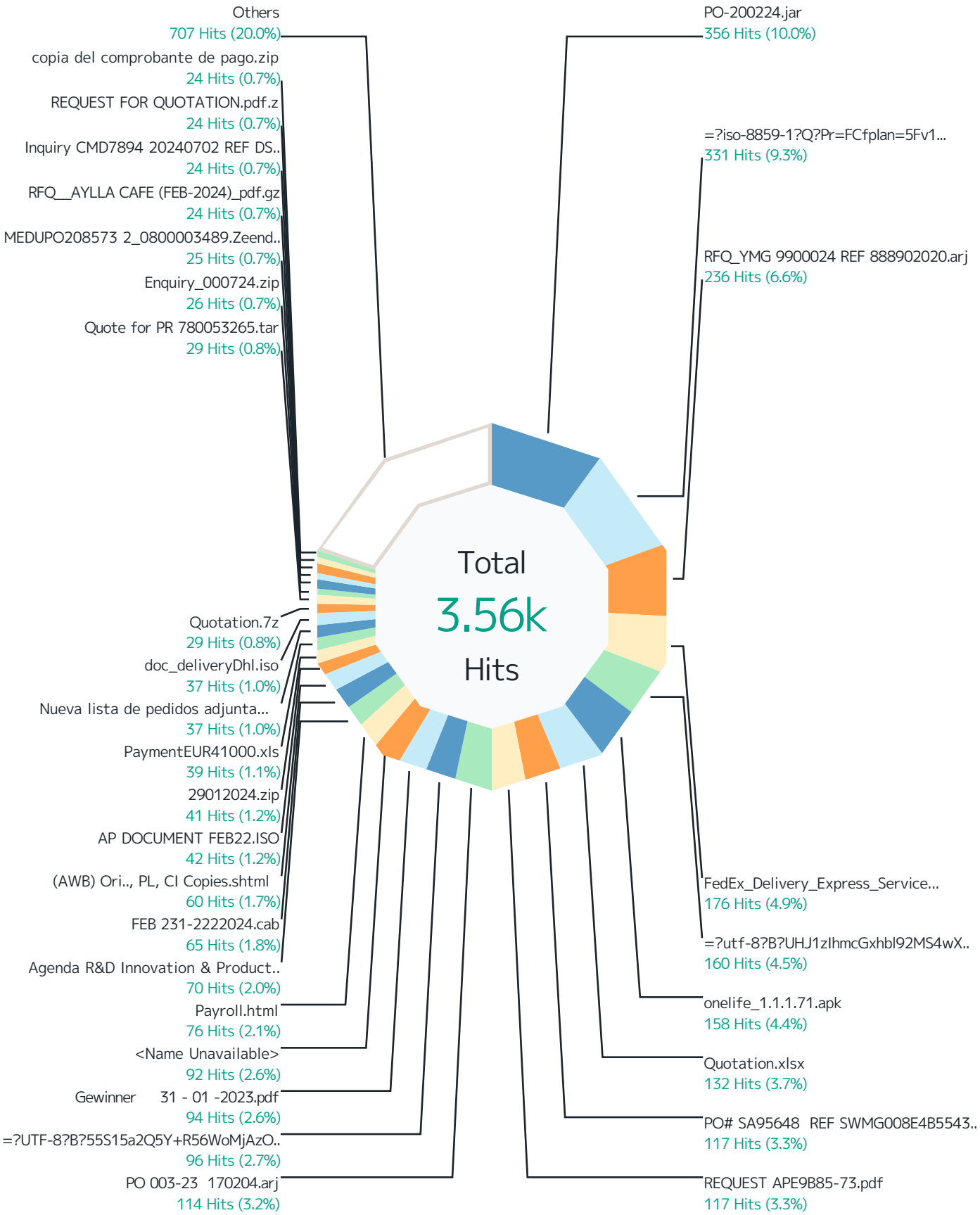
Update version
1697

Report started
2024-03-01 07:59:06+0100

Report run time
07:41:02

Filters used
Match All

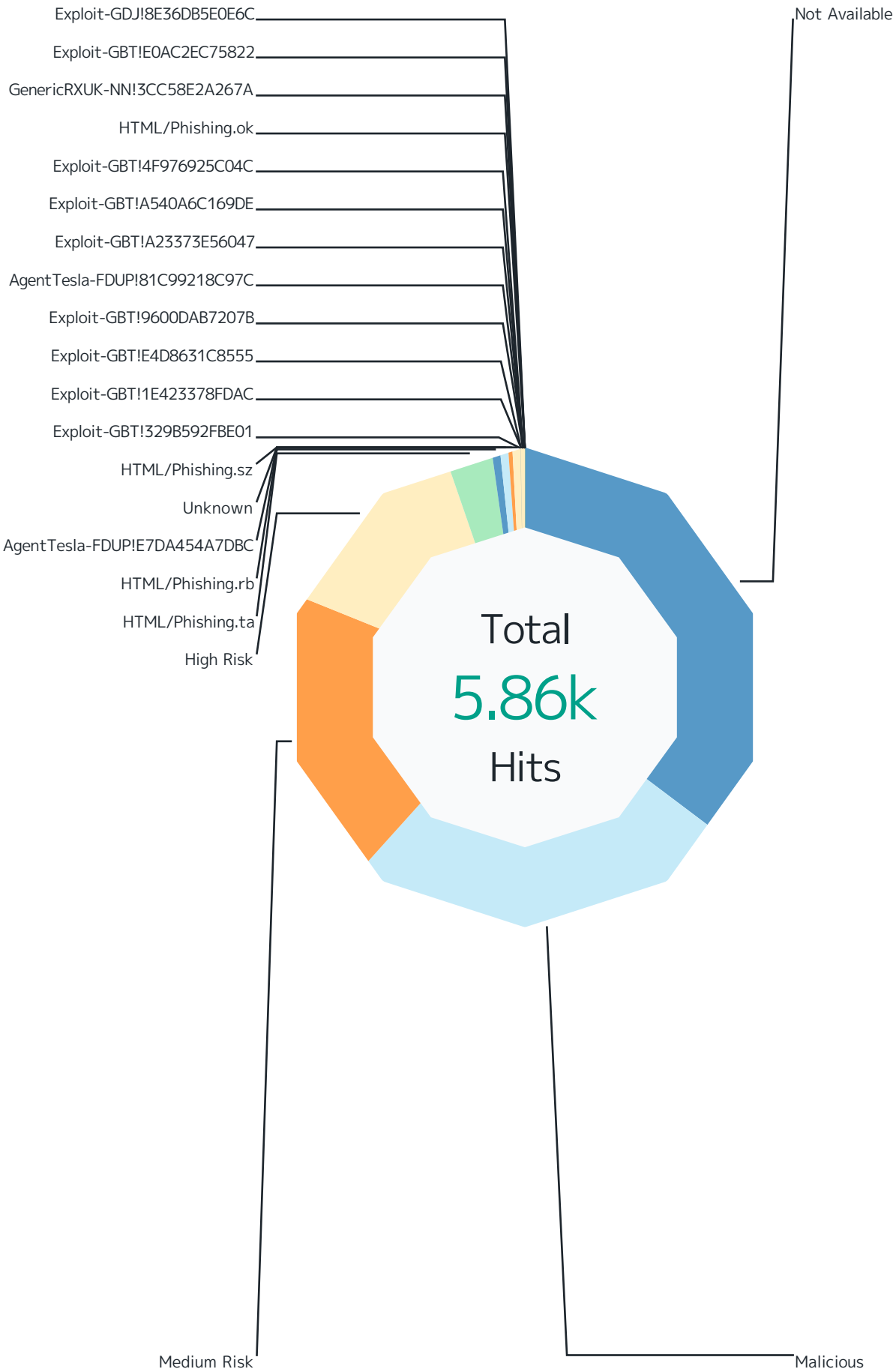
Virenfilterung MXe



Records by file name	Hits	%
PO-200224.jar	356	10.0 %
=?iso-8859-1?Q?Pr=FCfplan=5Fv1.0=5F20230426=5FFACROSS=5FHS.docx?=	331	9.3 %
RFQ_YMG 9900024 REF 888902020.arj	236	6.6 %
FedEx_Delivery_Express_Service.docx	176	4.9 %
=?utf-8?B?UHJ1zIhmcGxhbI92MS4wXzIwMjMwNDI2X0ZBQ1JPU1NfSFMuZG9jeA==?=	160	4.5 %
onelife_1.1.1.71.apk	158	4.4 %
Quotation.xlsx	132	3.7 %
PO# SA95648 REF SWMG008E4B5543 202402222.arj	117	3.3 %
REQUEST APE9B85-73.pdf	117	3.3 %
PO 003-23 170204.arj	114	3.2 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTEtMjAyMy5qcGcuaHRtbA==?=	96	2.7 %
Gewinner 31 - 01 -2023.pdf	94	2.6 %
<Name Unavailable>	92	2.6 %
Payroll.html	76	2.1 %
Agenda R&D Innovation & Product Development World Summit.pdf	70	2.0 %
FEB 231-2222024.cab	65	1.8 %
(AWB) Original BL, PL, CI Copies.shtml	60	1.7 %
AP DOCUMENT FEB22.ISO	42	1.2 %
29012024.zip	41	1.2 %
PaymentEUR41000.xls	39	1.1 %
Nueva lista de pedidos adjunta.zip	37	1.0 %
doc_deliveryDhl.iso	37	1.0 %
Quotation.7z	29	0.8 %
Quote for PR 780053265.tar	29	0.8 %
Enquiry_000724.zip	26	0.7 %
MEDUPO208573 2_0800003489.Zeendoc.7z	25	0.7 %
RFQ__AYLLA CAFE (FEB-2024)_pdf.gz	24	0.7 %
Inquiry CMD7894 20240702 REF DSCM66fcvfhf.arj	24	0.7 %
REQUEST FOR QUOTATION.pdf.z	24	0.7 %
copia del comprobante de pago.zip	24	0.7 %
Others	707	19.9 %
Total	**3.56k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.


Exploit-GDJ!8E36DB5E0E6C
Exploit-GBT!E0AC2EC75822
GenericRXUK-NN!3CC58E2A267A
HTML/Phishing.ok
Exploit-GBT!4F976925C04C
Exploit-GBT!A540A6C169DE
Exploit-GBT!A23373E56047
AgentTesla-FDUP!81C99218C97C
Exploit-GBT!9600DAB7207B
Exploit-GBT!E4D8631C8555
Exploit-GBT!1E423378FDAC
Exploit-GBT!329B592FBE01
HTML/Phishing.sz
Unknown
AgentTesla-FDUP!E7DA454A7DBC
HTML/Phishing.rb
HTML/Phishing.ta
High Risk
Not Available
Total
5.86k
Hits
Medium Risk
Malicious

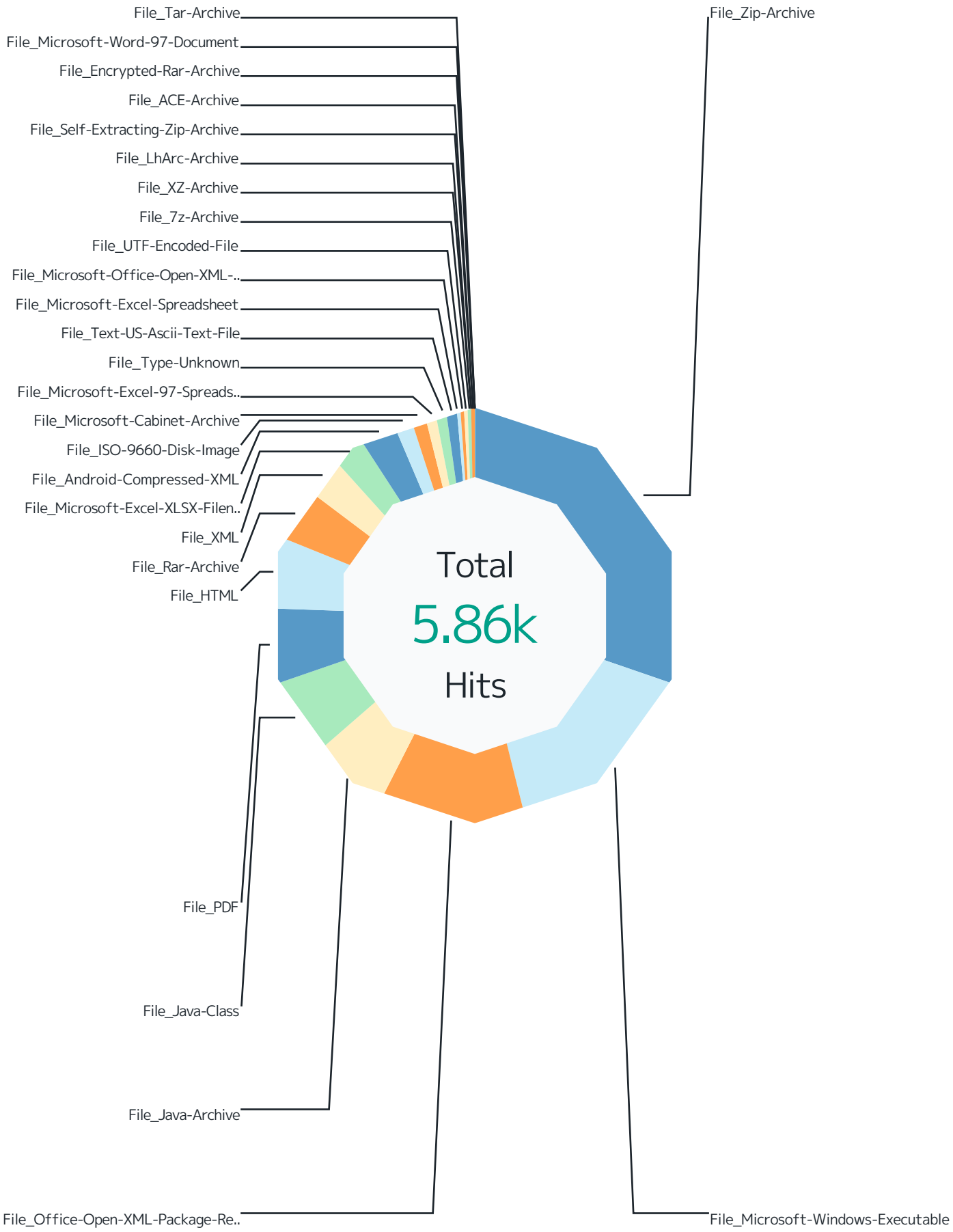
Scan Result	Hits	%
Not Available	**2.07k**	**35.4 %**
File_Zip-Archive	1.55k	26.4 %
File_Java-Archive	365	6.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	141	2.4 %
File_Microsoft-Excel-Spreadsheet	20	0.3 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
Malicious	**1.54k**	**26.4 %**
File_Microsoft-Windows-Executable	760	13.0 %
File_Office-Open-XML-Package-Relations-Item	176	3.0 %
File_Android-Compressed-XML	158	2.7 %
File_Zip-Archive	117	2.0 %
File_Rar-Archive	98	1.7 %
File_PDF	93	1.6 %
File_Microsoft-Cabinet-Archive	43	0.7 %
File_Microsoft-Excel-97-Spreadsheet	31	0.5 %
File_Type-Unknown	28	0.5 %
File_ISO-9660-Disk-Image	14	0.2 %
File_Text-US-Ascii-Text-File	8	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
File_HTML	3	0.1 %
File_LhArc-Archive	3	0.1 %
File_Self-Extracting-Zip-Archive	3	0.1 %
File_Java-Archive	2	0.0 %
File_7z-Archive	2	0.0 %
File_XZ-Archive	1	0.0 %
Medium Risk	**1.13k**	**19.3 %**
File_Office-Open-XML-Package-Relations-Item	491	8.4 %
File_PDF	243	4.1 %
File_XML	165	2.8 %
File_Microsoft-Windows-Executable	110	1.9 %
File_Rar-Archive	53	0.9 %
File_Microsoft-Cabinet-Archive	22	0.4 %
File_Microsoft-Office-Open-XML-Document	16	0.3 %
File_Zip-Archive	9	0.2 %
File_HTML	6	0.1 %
File_ISO-9660-Disk-Image	6	0.1 %
File_XZ-Archive	5	0.1 %
File_7z-Archive	2	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %

Scan Result	Hits	%
File_Type-Unknown	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_Microsoft-Word-97-Document	1	0.0 %
High Risk	**802**	**13.7 %**
File_Java-Class	356	6.1 %
File_HTML	101	1.7 %
File_Rar-Archive	98	1.7 %
File_Zip-Archive	78	1.3 %
File_Microsoft-Windows-Executable	55	0.9 %
File_Microsoft-Excel-97-Spreadsheet	24	0.4 %
File_ISO-9660-Disk-Image	23	0.4 %
File_Type-Unknown	21	0.4 %
File_UTF-Encoded-File	18	0.3 %
File_PDF	8	0.1 %
File_7z-Archive	4	0.1 %
File_Text-US-Ascii-Text-File	3	0.1 %
File_ACE-Archive	3	0.1 %
File_Encrypted-Rar-Archive	3	0.1 %
File_Office-Open-XML-Package-Relations-Item	2	0.0 %
File_Microsoft-Office-Open-XML-Document	2	0.0 %
File_XZ-Archive	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %
HTML/Phishing.ta	**169**	**2.9 %**
File_HTML	169	2.9 %
HTML/Phishing.rb	**40**	**0.7 %**
File_HTML	37	0.6 %
File_Text-US-Ascii-Text-File	3	0.1 %
AgentTesla-FDUP!E7DA454A7DBC	**34**	**0.6 %**
File_ISO-9660-Disk-Image	34	0.6 %
Unknown	**22**	**0.4 %**
File_Zip-Archive	22	0.4 %
HTML/Phishing.sz	**20**	**0.3 %**
File_Text-US-Ascii-Text-File	20	0.3 %
Exploit-GBT!329B592FBE01	**5**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.1 %
Exploit-GBT!1E423378FDAC	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
Exploit-GBT!E4D8631C8555	**3**	**0.1 %**

Scan Result	Hits	%
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
Exploit-GBT!9600DAB7207B	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
AgentTesla-FDUP!81C99218C97C	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
Exploit-GBT!A23373E56047	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Exploit-GBT!A540A6C169DE	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!4F976925C04C	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
HTML/Phishing.ok	**1**	**0.0 %**
File_HTML	1	0.0 %
GenericRXUK-NN!3CC58E2A267A	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Exploit-GBT!E0AC2EC75822	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GDJ!8E36DB5E0E6C	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Total	**5.86k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.


File_Tar-Archive
File_Microsoft-Word-97-Document
File_Encrypted-Rar-Archive
File_ACE-Archive
File_Self-Extracting-Zip-Archive
File_LhArc-Archive
File_XZ-Archive
File_7z-Archive
File_UTF-Encoded-File
File_Microsoft-Office-Open-XML-..
File_Microsoft-Excel-Spreadsheet
File_Text-US-Ascii-Text-File
File_Type-Unknown
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Cabinet-Archive
File_ISO-9660-Disk-Image
File_Android-Compressed-XML
File_Microsoft-Excel-XLSX-Filen..
File_XML
File_Rar-Archive
File_HTML
File_Zip-Archive
Total
5.86k
Hits
File_PDF
File_Java-Class
File_Java-Archive
File_Office-Open-XML-Package-Re..
File_Microsoft-Windows-Executable

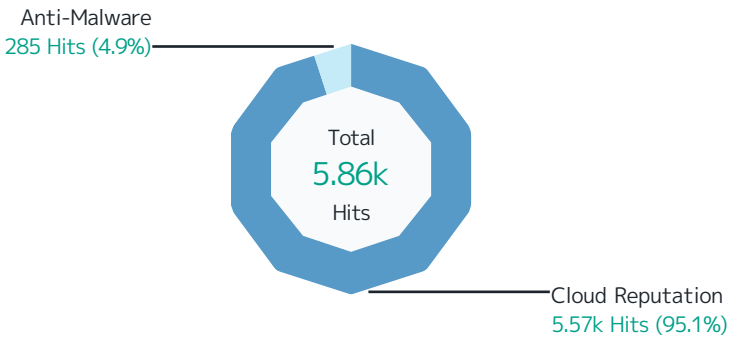
Responding Scanner	Hits	%
File_Zip-Archive	**1.77k**	**30.2 %**
Not Available	1.55k	26.4 %
Malicious	117	2.0 %
High Risk	78	1.3 %
Unknown	22	0.4 %
Medium Risk	9	0.2 %
File_Microsoft-Windows-Executable	**925**	**15.8 %**
Malicious	760	13.0 %
Medium Risk	110	1.9 %
High Risk	55	0.9 %
File_Office-Open-XML-Package-Relations-Item	**669**	**11.4 %**
Medium Risk	491	8.4 %
Malicious	176	3.0 %
High Risk	2	0.0 %
File_Java-Archive	**367**	**6.3 %**
Not Available	365	6.2 %
Malicious	2	0.0 %
File_Java-Class	**356**	**6.1 %**
High Risk	356	6.1 %
File_PDF	**344**	**5.9 %**
Medium Risk	243	4.1 %
Malicious	93	1.6 %
High Risk	8	0.1 %
File_HTML	**317**	**5.4 %**
HTML/Phishing.ta	169	2.9 %
High Risk	101	1.7 %
HTML/Phishing.rb	37	0.6 %
Medium Risk	6	0.1 %
Malicious	3	0.1 %
HTML/Phishing.ok	1	0.0 %
File_Rar-Archive	**252**	**4.3 %**
Malicious	98	1.7 %
High Risk	98	1.7 %
Medium Risk	53	0.9 %
AgentTesla-FDUP!81C99218C97C	2	0.0 %
GenericRXUK-NN!3CC58E2A267A	1	0.0 %
File_XML	**165**	**2.8 %**
Medium Risk	165	2.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	**162**	**2.8 %**

Responding Scanner	Hits	%
Not Available	141	2.4 %
Exploit-GBT!329B592FBE01	5	0.1 %
Malicious	4	0.1 %
Exploit-GBT!1E423378FDAC	3	0.1 %
Exploit-GBT!E4D8631C8555	3	0.1 %
Exploit-GBT!9600DAB7207B	2	0.0 %
Exploit-GBT!A540A6C169DE	1	0.0 %
Exploit-GBT!4F976925C04C	1	0.0 %
Exploit-GBT!E0AC2EC75822	1	0.0 %
Exploit-GDJ!8E36DB5E0E6C	1	0.0 %
File_Android-Compressed-XML	**158**	**2.7 %**
Malicious	158	2.7 %
File_ISO-9660-Disk-Image	**77**	**1.3 %**
AgentTesla-FDUP!E7DA454A7DBC	34	0.6 %
High Risk	23	0.4 %
Malicious	14	0.2 %
Medium Risk	6	0.1 %
File_Microsoft-Cabinet-Archive	**65**	**1.1 %**
Malicious	43	0.7 %
Medium Risk	22	0.4 %
File_Microsoft-Excel-97-Spreadsheet	**56**	**1.0 %**
Malicious	31	0.5 %
High Risk	24	0.4 %
Medium Risk	1	0.0 %
File_Type-Unknown	**50**	**0.9 %**
Malicious	28	0.5 %
High Risk	21	0.4 %
Medium Risk	1	0.0 %
File_Text-US-Ascii-Text-File	**34**	**0.6 %**
HTML/Phishing.sz	20	0.3 %
Malicious	8	0.1 %
High Risk	3	0.1 %
HTML/Phishing.rb	3	0.1 %
File_Microsoft-Excel-Spreadsheet	**21**	**0.4 %**
Not Available	20	0.3 %
Exploit-GBT!A23373E56047	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**19**	**0.3 %**
Medium Risk	16	0.3 %
High Risk	2	0.0 %

Responding Scanner	Hits	%
Not Available	1	0.0 %
File_UTF-Encoded-File	**18**	**0.3 %**
High Risk	18	0.3 %
File_7z-Archive	**8**	**0.1 %**
High Risk	4	0.1 %
Malicious	2	0.0 %
Medium Risk	2	0.0 %
File_XZ-Archive	**7**	**0.1 %**
Medium Risk	5	0.1 %
Malicious	1	0.0 %
High Risk	1	0.0 %
File_LhArc-Archive	**5**	**0.1 %**
Malicious	3	0.1 %
Medium Risk	1	0.0 %
High Risk	1	0.0 %
File_Self-Extracting-Zip-Archive	**3**	**0.1 %**
Malicious	3	0.1 %
File_ACE-Archive	**3**	**0.1 %**
High Risk	3	0.1 %
File_Encrypted-Rar-Archive	**3**	**0.1 %**
High Risk	3	0.1 %
File_Microsoft-Word-97-Document	**1**	**0.0 %**
Medium Risk	1	0.0 %
File_Tar-Archive	**1**	**0.0 %**
High Risk	1	0.0 %
Total	**5.86k**	**100 %**

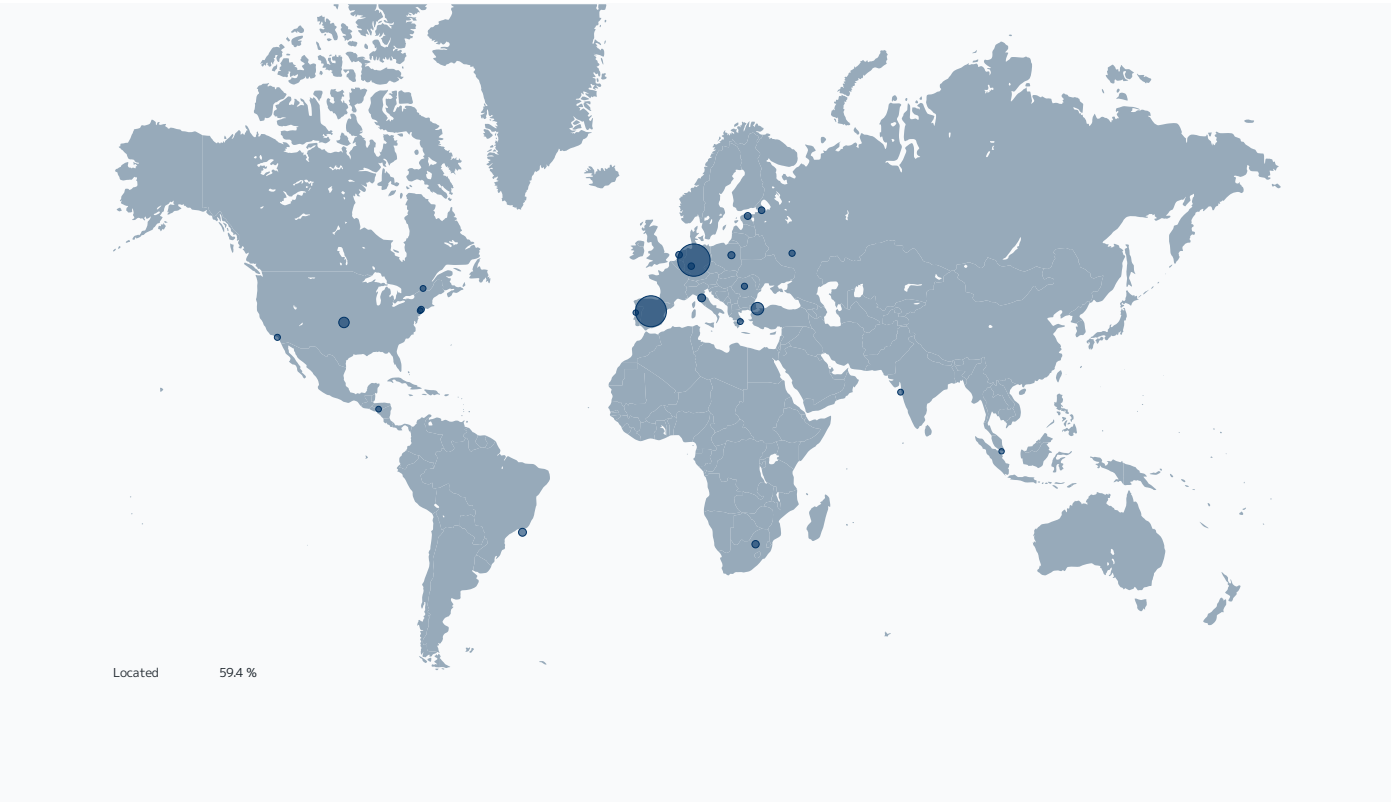
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**5.57k**	**95.1 %**
File_Zip-Archive	1.77k	30.2 %
File_Microsoft-Windows-Executable	925	15.8 %
File_Office-Open-XML-Package-Relations-Item	669	11.4 %
File_Java-Archive	367	6.3 %
File_Java-Class	356	6.1 %
File_PDF	344	5.9 %
File_Rar-Archive	249	4.3 %
File_XML	165	2.8 %
File_Android-Compressed-XML	158	2.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	145	2.5 %
File_HTML	110	1.9 %
File_Microsoft-Cabinet-Archive	65	1.1 %
File_Microsoft-Excel-97-Spreadsheet	56	1.0 %
File_Type-Unknown	50	0.9 %
File_ISO-9660-Disk-Image	43	0.7 %
File_Microsoft-Excel-Spreadsheet	20	0.3 %
File_Microsoft-Office-Open-XML-Document	19	0.3 %
File_UTF-Encoded-File	18	0.3 %
File_Text-US-Ascii-Text-File	11	0.2 %
File_7z-Archive	8	0.1 %
File_XZ-Archive	7	0.1 %
File_LhArc-Archive	5	0.1 %
File_Self-Extracting-Zip-Archive	3	0.1 %
File_ACE-Archive	3	0.1 %
File_Encrypted-Rar-Archive	3	0.1 %
File_Microsoft-Word-97-Document	1	0.0 %
File_Tar-Archive	1	0.0 %
Anti-Malware	**285**	**4.9 %**
File_HTML	207	3.5 %
File_ISO-9660-Disk-Image	34	0.6 %
File_Text-US-Ascii-Text-File	23	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	17	0.3 %
File_Rar-Archive	3	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Total	**5.86k**	**100 %**

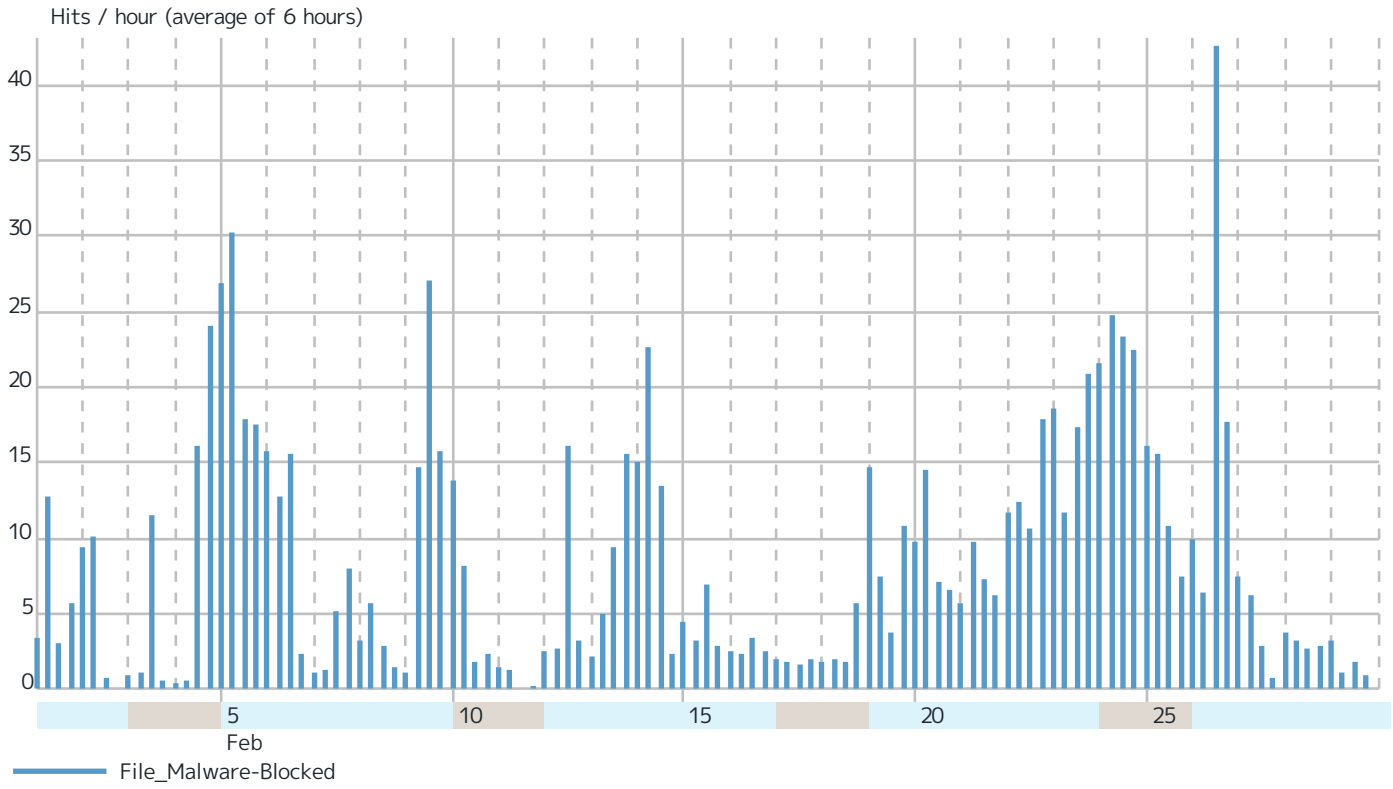
Virenfilterung SRC IPs



Records by src IP		Hits	%
94.127.187.68	Spain	935	16.0 %
88.99.92.45	Germany	712	12.2 %
217.160.246.10	Germany	248	4.2 %
91.151.82.23	Turkey	176	3.0 %
152.92.1.8	Rio de Janeiro, Brazil	112	1.9 %
195.225.169.202	Arezzo, Italy	107	1.8 %
185.48.180.104	Turkey	100	1.7 %
51.77.61.156	Warsaw, Poland	82	1.4 %
198.12.70.114	United States	78	1.3 %
64.78.49.138	United States	76	1.3 %
188.127.225.37	Estonia	72	1.2 %
92.53.107.165	St Petersburg, Russia	68	1.2 %
185.78.76.115	Frankfurt am Main, Germany	60	1.0 %
45.55.199.74	Clifton, New Jersey 07014, United States	52	0.9 %
109.195.11.226	Lipetsk, Russia	50	0.9 %
173.249.144.196	United States	48	0.8 %
89.45.194.41	Romania	48	0.8 %
41.0.3.229	Springs, South Africa	47	0.8 %
195.123.240.92	Los Angeles, California 90060, United States	46	0.8 %
41.0.3.228	Springs, South Africa	44	0.8 %
46.227.62.50	Greece	40	0.7 %
103.172.92.181	Mumbai, India	39	0.7 %
192.99.98.252	Montreal, Quebec H2K , Canada	37	0.6 %
161.129.65.88	Amsterdam, The Netherlands	36	0.6 %
209.127.121.82	Piscataway, New Jersey 08854, United States	34	0.6 %
104.223.34.164	Amsterdam, The Netherlands	32	0.5 %
181.210.30.114	Tegucigalpa, Honduras	32	0.5 %
5.206.224.146	Miranda do Corvo, Portugal	24	0.4 %
178.162.224.160	Germany	24	0.4 %
31.192.238.58	Singapore, 17 Singapore	22	0.4 %
Others		2.38k	40.6 %
Total		**5.86k**	**100 %**

SMTP Virus Filtering by Time

Top 10 file filtering situations on a timeline.



About the FlexEdge Secure SD-WAN

Forcepoint FlexEdge Secure SD-WAN enables distributed organizations to improve application performance, simplify network management, and increase security— ensuring users can safely access any application from anywhere. By combining multi-link networking and intrusion prevention with zero-touch deployment and updating, it provides centralized visibility and control with high performance that scales to thousands of sites. When used with the Forcepoint ONE SSE platform, FlexEdge Secure SD-WAN delivers true SASE and secure branch solutions that boost productivity, cut costs, reduce risk, and streamline compliance.

For further information visit forcepoint.com/product/secure-sd-wan.

Forcepoint

forcepoint.com

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.