Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2023-11-01 00:00:00+0100
To: 2023-12-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.1, build 11424

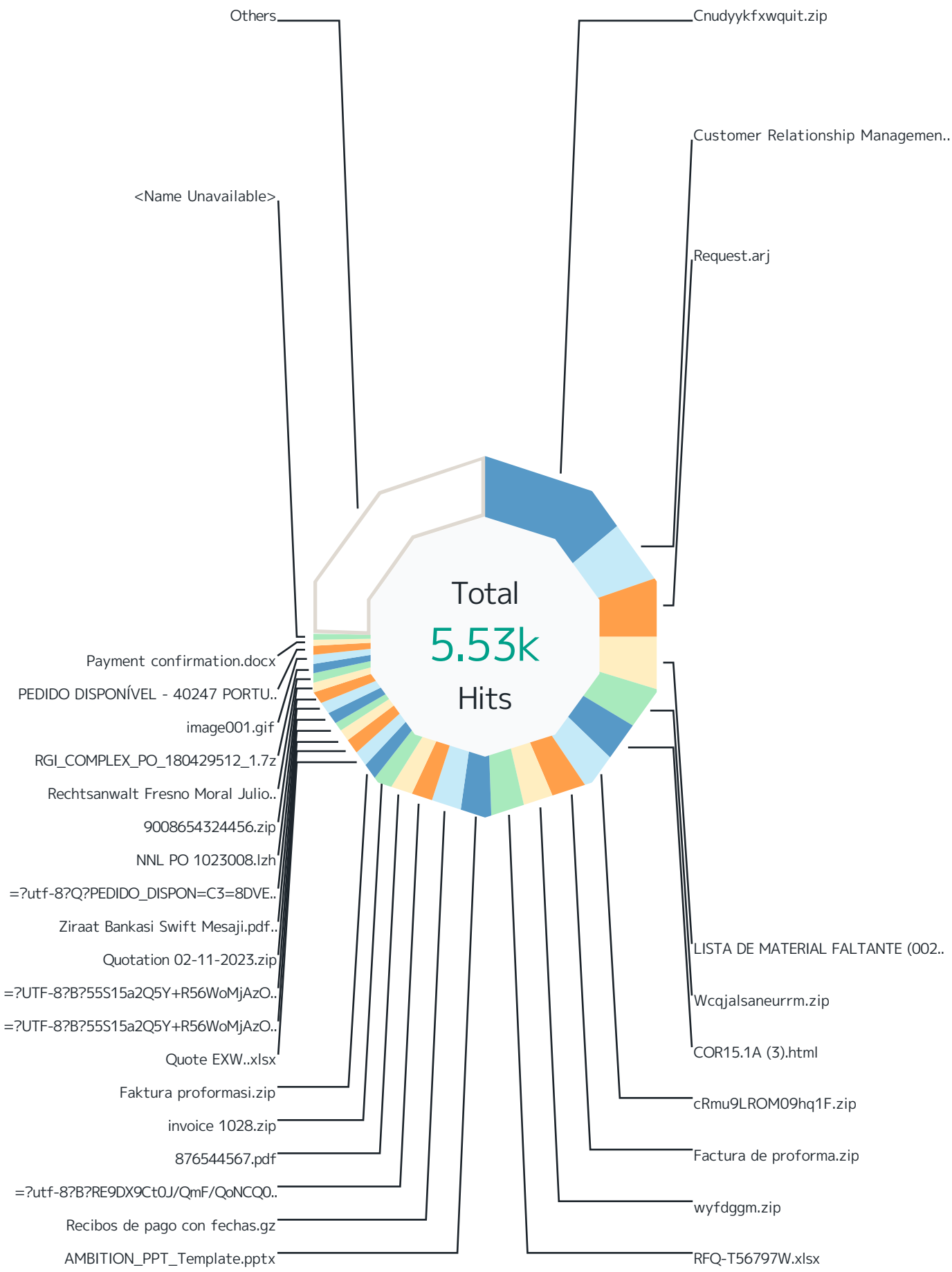
Update version
1658

Report started
2023-12-01 07:21:45+0100

Report run time
08:17:19

Filters used
Match All

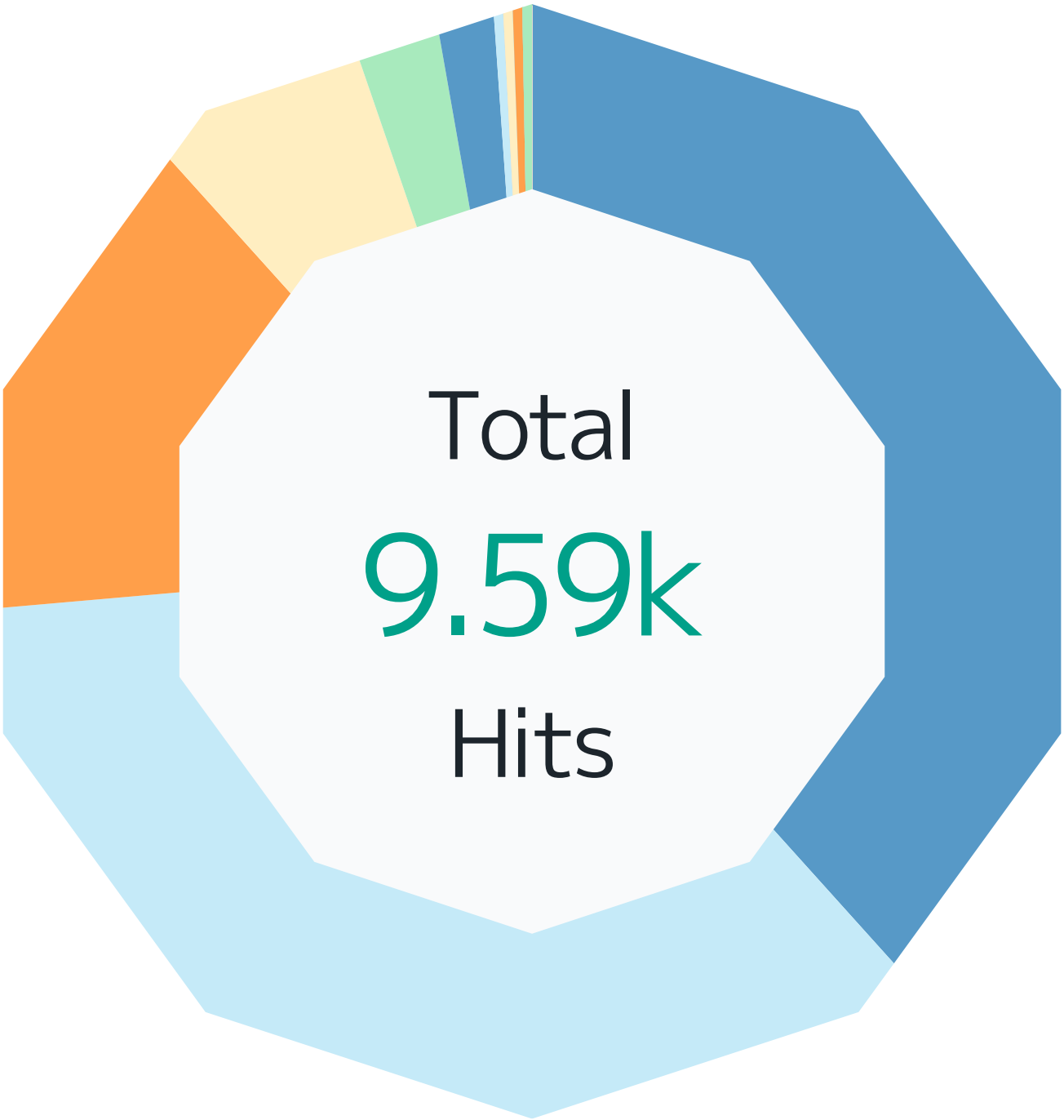
Virenfilterung MXe



Records by file name	Hits	%
Cnudyykfxwquit.zip	769	13.9 %
Customer Relationship Management.pptx	315	5.7 %
Request.arj	292	5.3 %
LISTA DE MATERIAL FALTANTE (002) (1).zip	260	4.7 %
Wcqjalsaneurrm.zip	228	4.1 %
COR15.1A (3).html	193	3.5 %
cRmu9LROM09hq1F.zip	185	3.3 %
Factura de proforma.zip	163	2.9 %
wyfdggm.zip	163	2.9 %
RFQ-T56797W.xlsx	162	2.9 %
AMBITION_PPT_Template.pptx	159	2.9 %
Recibos de pago con fechas.gz	153	2.8 %
=?utf-8?B?RE9DX9Ct0J/QmF/QoNCQ0JfQkdCY0JLQmtCQX9Cf0JXQp9CQ0KLQrC5HWg==?=	112	2.0 %
876544567.pdf	110	2.0 %
invoice 1028.zip	83	1.5 %
Faktura proformasi.zip	80	1.4 %
Quote EXW..xlsx	80	1.4 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTEtMjAyMy5qcGcuaHRtbA==?=	65	1.2 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDExLTUtMjAyMy5wZGYuc2h0bWw=?=	61	1.1 %
Quotation 02-11-2023.zip	60	1.1 %
Ziraat Bankasi Swift Mesaji.pdf.rar	60	1.1 %
=?utf-8?Q?PEDIDO_DISPON=C3=8DVEL_-_40247_PORTUGAL=2E7z?=	59	1.1 %
NNL PO 1023008.lzh	52	0.9 %
9008654324456.zip	51	0.9 %
Rechtsanwalt Fresno Moral Julio.pdf	49	0.9 %
RGI_COMPLEX_PO_180429512_1.7z	49	0.9 %
image001.gif	45	0.8 %
PEDIDO DISPONÍVEL - 40247 PORTUGAL.7z	45	0.8 %
Payment confirmation.docx	33	0.6 %
<Name Unavailable>	31	0.6 %
Others	1.36k	24.6 %
Total	**5.53k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.


Total
9.59k
Hits

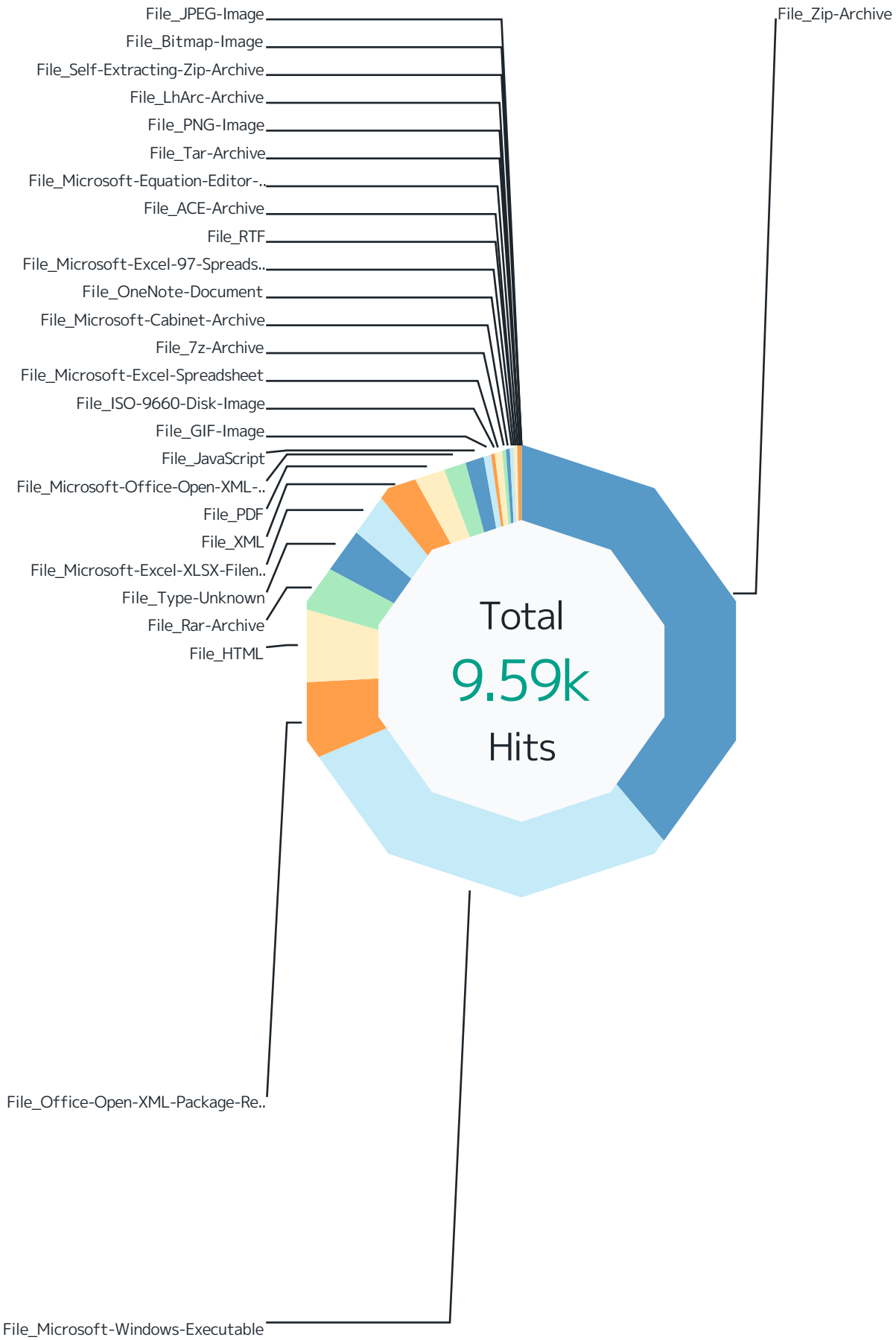
Scan Result	Hits	%
Malicious	**3.66k**	**38.2 %**
File_Microsoft-Windows-Executable	2.69k	28.0 %
File_Zip-Archive	420	4.4 %
File_Rar-Archive	179	1.9 %
File_Type-Unknown	166	1.7 %
File_Office-Open-XML-Package-Relations-Item	75	0.8 %
File_JavaScript	27	0.3 %
File_ISO-9660-Disk-Image	19	0.2 %
File_PDF	17	0.2 %
File_OneNote-Document	16	0.2 %
File_Microsoft-Office-Open-XML-Document	15	0.2 %
File_7z-Archive	11	0.1 %
File_Microsoft-Equation-Editor-Document	7	0.1 %
File_HTML	6	0.1 %
File_Microsoft-Cabinet-Archive	6	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
File_Tar-Archive	2	0.0 %
File_LhArc-Archive	2	0.0 %
File_ACE-Archive	1	0.0 %
Not Available	**3.41k**	**35.5 %**
File_Zip-Archive	3.09k	32.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	248	2.6 %
File_Microsoft-Office-Open-XML-Document	64	0.7 %
File_Microsoft-Excel-Spreadsheet	9	0.1 %
Medium Risk	**1.41k**	**14.7 %**
File_Office-Open-XML-Package-Relations-Item	474	4.9 %
File_XML	269	2.8 %
File_HTML	193	2.0 %
File_PDF	153	1.6 %
File_Type-Unknown	123	1.3 %
File_GIF-Image	56	0.6 %
File_Microsoft-Windows-Executable	52	0.5 %
File_JavaScript	49	0.5 %
File_Rar-Archive	18	0.2 %
File_7z-Archive	6	0.1 %
File_PNG-Image	6	0.1 %
File_Zip-Archive	3	0.0 %
File_Microsoft-Excel-97-Spreadsheet	3	0.0 %

Scan Result	Hits	%
File_ISO-9660-Disk-Image	1	0.0 %
High Risk	**614**	**6.4 %**
File_Rar-Archive	134	1.4 %
File_Microsoft-Windows-Executable	105	1.1 %
File_Microsoft-Office-Open-XML-Document	82	0.9 %
File_Zip-Archive	76	0.8 %
File_PDF	57	0.6 %
File_JavaScript	37	0.4 %
File_Type-Unknown	33	0.3 %
File_Microsoft-Cabinet-Archive	23	0.2 %
File_7z-Archive	15	0.2 %
File_ISO-9660-Disk-Image	14	0.1 %
File_RTF	12	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	7	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_Tar-Archive	4	0.0 %
File_Self-Extracting-Zip-Archive	3	0.0 %
File_HTML	2	0.0 %
File_Bitmap-Image	2	0.0 %
File_JPEG-Image	2	0.0 %
File_LhArc-Archive	1	0.0 %
HTML/Phishing.ta	**247**	**2.6 %**
File_HTML	241	2.5 %
File_Type-Unknown	6	0.1 %
Unknown	**140**	**1.5 %**
File_Zip-Archive	138	1.4 %
File_Microsoft-Office-Open-XML-Document	2	0.0 %
HTML/Phishing.rb	**33**	**0.3 %**
File_HTML	32	0.3 %
File_Type-Unknown	1	0.0 %
Exploit-GBT!924C87CF98F9	**11**	**0.1 %**
File_Microsoft-Excel-Spreadsheet	11	0.1 %
HTML/Phishing.rj	**11**	**0.1 %**
File_JavaScript	11	0.1 %
HTML/Phishing.tb	**9**	**0.1 %**
File_HTML	9	0.1 %
Fareit.gen.e	**5**	**0.1 %**
File_ACE-Archive	5	0.1 %
Exploit-GBT!F96CC4346B93	**3**	**0.0 %**

Scan Result	Hits	%
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Exploit-GBT!41EDBC4C6C34	**3**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	3	0.0 %
Fareit.gen.a	**3**	**0.0 %**
File_ACE-Archive	3	0.0 %
HTML/Phishing.ec	**3**	**0.0 %**
File_HTML	3	0.0 %
Exploit-GBT!3C96AA8F5424	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Exploit-GBT!42D46DE30628	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!02B686025FFF	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!4E19C4445C61	**2**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	2	0.0 %
HTML/Phishing.qi	**2**	**0.0 %**
File_HTML	2	0.0 %
Exploit-GBT!03939A81BA4A	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
HTML/Phishing.ok	**2**	**0.0 %**
File_HTML	2	0.0 %
Exploit-GBT!7B6618D52EB2	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!5DC9536934C3	**2**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	2	0.0 %
Exploit-GBT!559E42FE1C7B	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Exploit-GBT!8EB548417CFD	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!F27F8F6C4B8C	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
AgentTesla-FCSO!78BA688489C8	**1**	**0.0 %**
File_ISO-9660-Disk-Image	1	0.0 %
Exploit-GBT!33D6153DC354	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Exploit-GBT!67BE56A35BD4	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Others	**8**	**0.1 %**
Total	**9.59k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.


File_JPEG-Image
File_Bitmap-Image
File_Self-Extracting-Zip-Archive
File_LhArc-Archive
File_PNG-Image
File_Tar-Archive
File_Microsoft-Equation-Editor-..
File_ACE-Archive
File_RTF
File_Microsoft-Excel-97-Spreads..
File_OneNote-Document
File_Microsoft-Cabinet-Archive
File_7z-Archive
File_Microsoft-Excel-Spreadsheet
File_ISO-9660-Disk-Image
File_GIF-Image
File_JavaScript
File_Microsoft-Office-Open-XML-..
File_PDF
File_XML
File_Microsoft-Excel-XLSX-Filen..
File_Type-Unknown
File_Rar-Archive
File_HTML
File_Office-Open-XML-Package-Re..
File_Microsoft-Windows-Executable
File_Zip-Archive
Total
9.59k
Hits

Responding Scanner	Hits	%
File_Zip-Archive	**3.72k**	**38.8 %**
Not Available	3.09k	32.2 %
Malicious	420	4.4 %
Unknown	138	1.4 %
High Risk	76	0.8 %
Medium Risk	3	0.0 %
JS/Dropper.am	1	0.0 %
DOC/Phishing.gen.d	1	0.0 %
File_Microsoft-Windows-Executable	**2.85k**	**29.7 %**
Malicious	2.69k	28.0 %
High Risk	105	1.1 %
Medium Risk	52	0.5 %
File_Office-Open-XML-Package-Relations-Item	**549**	**5.7 %**
Medium Risk	474	4.9 %
Malicious	75	0.8 %
File_HTML	**492**	**5.1 %**
HTML/Phishing.ta	241	2.5 %
Medium Risk	193	2.0 %
HTML/Phishing.rb	32	0.3 %
HTML/Phishing.tb	9	0.1 %
Malicious	6	0.1 %
HTML/Phishing.ec	3	0.0 %
High Risk	2	0.0 %
HTML/Phishing.qi	2	0.0 %
HTML/Phishing.ok	2	0.0 %
HTML/Phishing.sc	1	0.0 %
HTML/Phishing.ol	1	0.0 %
File_Rar-Archive	**331**	**3.5 %**
Malicious	179	1.9 %
High Risk	134	1.4 %
Medium Risk	18	0.2 %
File_Type-Unknown	**329**	**3.4 %**
Malicious	166	1.7 %
Medium Risk	123	1.3 %
High Risk	33	0.3 %
HTML/Phishing.ta	6	0.1 %
HTML/Phishing.rb	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**271**	**2.8 %**
Not Available	248	2.6 %

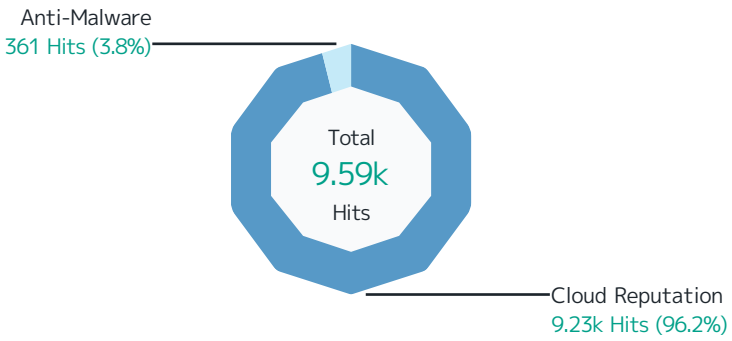
Responding Scanner	Hits	%
High Risk	7	0.1 %
Exploit-GBT!F96CC4346B93	3	0.0 %
Exploit-GBT!3C96AA8F5424	3	0.0 %
Exploit-GBT!42D46DE30628	2	0.0 %
Exploit-GBT!02B686025FFF	2	0.0 %
Exploit-GBT!03939A81BA4A	2	0.0 %
Exploit-GBT!7B6618D52EB2	2	0.0 %
Exploit-GBT!8EB548417CFD	1	0.0 %
Exploit-GBT!67BE56A35BD4	1	0.0 %
File_XML	**269**	**2.8 %**
Medium Risk	269	2.8 %
File_PDF	**228**	**2.4 %**
Medium Risk	153	1.6 %
High Risk	57	0.6 %
Malicious	17	0.2 %
PDF/Phish-FBU!3463198451B8	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**163**	**1.7 %**
High Risk	82	0.9 %
Not Available	64	0.7 %
Malicious	15	0.2 %
Unknown	2	0.0 %
File_JavaScript	**125**	**1.3 %**
Medium Risk	49	0.5 %
High Risk	37	0.4 %
Malicious	27	0.3 %
HTML/Phishing.rj	11	0.1 %
HTML/Phishing.rl	1	0.0 %
File_GIF-Image	**56**	**0.6 %**
Medium Risk	56	0.6 %
File_ISO-9660-Disk-Image	**35**	**0.4 %**
Malicious	19	0.2 %
High Risk	14	0.1 %
Medium Risk	1	0.0 %
AgentTesla-FCSO!78BA688489C8	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**34**	**0.4 %**
Exploit-GBT!924C87CF98F9	11	0.1 %
Not Available	9	0.1 %
Exploit-GBT!41EDBC4C6C34	3	0.0 %
Malicious	2	0.0 %

Responding Scanner	Hits	%
Exploit-GBT!4E19C4445C61	2	0.0 %
Exploit-GBT!5DC9536934C3	2	0.0 %
Exploit-GBT!559E42FE1C7B	1	0.0 %
Exploit-GBT!F27F8F6C4B8C	1	0.0 %
Exploit-GBT!33D6153DC354	1	0.0 %
Exploit-GBT!39CA24F852E2	1	0.0 %
Exploit-GBT!227D2AC8C1FB	1	0.0 %
File_7z-Archive	**32**	**0.3 %**
High Risk	15	0.2 %
Malicious	11	0.1 %
Medium Risk	6	0.1 %
File_Microsoft-Cabinet-Archive	**29**	**0.3 %**
High Risk	23	0.2 %
Malicious	6	0.1 %
File_OneNote-Document	**16**	**0.2 %**
Malicious	16	0.2 %
File_Microsoft-Excel-97-Spreadsheet	**13**	**0.1 %**
Malicious	5	0.1 %
High Risk	5	0.1 %
Medium Risk	3	0.0 %
File_RTF	**12**	**0.1 %**
High Risk	12	0.1 %
File_ACE-Archive	**9**	**0.1 %**
Fareit.gen.e	5	0.1 %
Fareit.gen.a	3	0.0 %
Malicious	1	0.0 %
File_Microsoft-Equation-Editor-Document	**7**	**0.1 %**
Malicious	7	0.1 %
File_Tar-Archive	**6**	**0.1 %**
High Risk	4	0.0 %
Malicious	2	0.0 %
File_PNG-Image	**6**	**0.1 %**
Medium Risk	6	0.1 %
File_LhArc-Archive	**3**	**0.0 %**
Malicious	2	0.0 %
High Risk	1	0.0 %
File_Self-Extracting-Zip-Archive	**3**	**0.0 %**
High Risk	3	0.0 %
File_Bitmap-Image	**2**	**0.0 %**

Responding Scanner	Hits	%
High Risk	2	0.0 %
File_JPEG-Image	**2**	**0.0 %**
High Risk	2	0.0 %
Total	**9.59k**	**100 %**

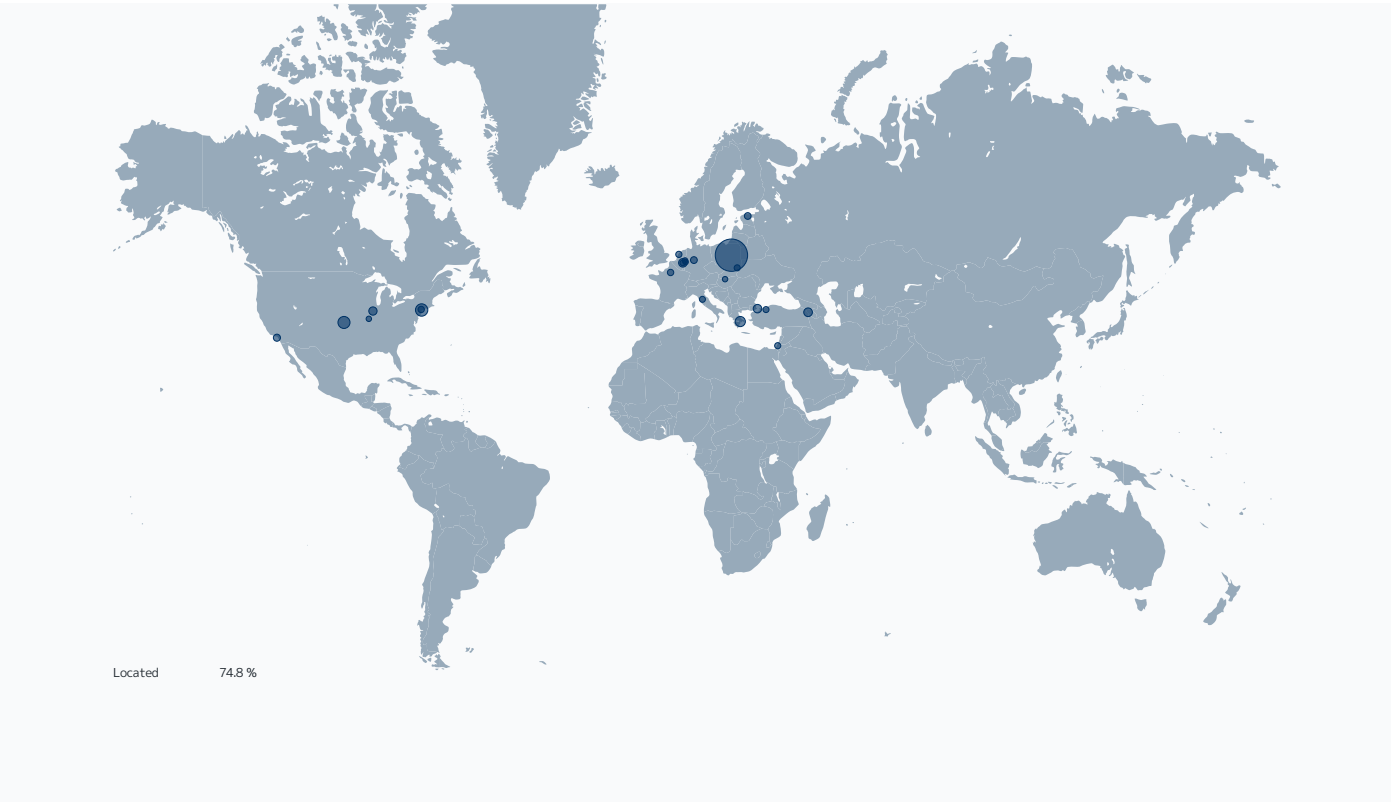
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**9.23k**	**96.2 %**
File_Zip-Archive	3.72k	38.8 %
File_Microsoft-Windows-Executable	2.85k	29.7 %
File_Office-Open-XML-Package-Relations-Item	549	5.7 %
File_Rar-Archive	331	3.5 %
File_Type-Unknown	322	3.4 %
File_XML	269	2.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	255	2.7 %
File_PDF	227	2.4 %
File_HTML	201	2.1 %
File_Microsoft-Office-Open-XML-Document	163	1.7 %
File_JavaScript	113	1.2 %
File_GIF-Image	56	0.6 %
File_ISO-9660-Disk-Image	34	0.4 %
File_7z-Archive	32	0.3 %
File_Microsoft-Cabinet-Archive	29	0.3 %
File_OneNote-Document	16	0.2 %
File_Microsoft-Excel-97-Spreadsheet	13	0.1 %
File_RTF	12	0.1 %
File_Microsoft-Excel-Spreadsheet	11	0.1 %
File_Microsoft-Equation-Editor-Document	7	0.1 %
File_Tar-Archive	6	0.1 %
File_PNG-Image	6	0.1 %
File_LhArc-Archive	3	0.0 %
File_Self-Extracting-Zip-Archive	3	0.0 %
File_Bitmap-Image	2	0.0 %
File_JPEG-Image	2	0.0 %
File_ACE-Archive	1	0.0 %
Anti-Malware	**361**	**3.8 %**
File_HTML	291	3.0 %
File_Microsoft-Excel-Spreadsheet	23	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	16	0.2 %
File_JavaScript	12	0.1 %
File_ACE-Archive	8	0.1 %
File_Type-Unknown	7	0.1 %
File_Zip-Archive	2	0.0 %
File_PDF	1	0.0 %
File_ISO-9660-Disk-Image	1	0.0 %
Total	**9.59k**	**100 %**

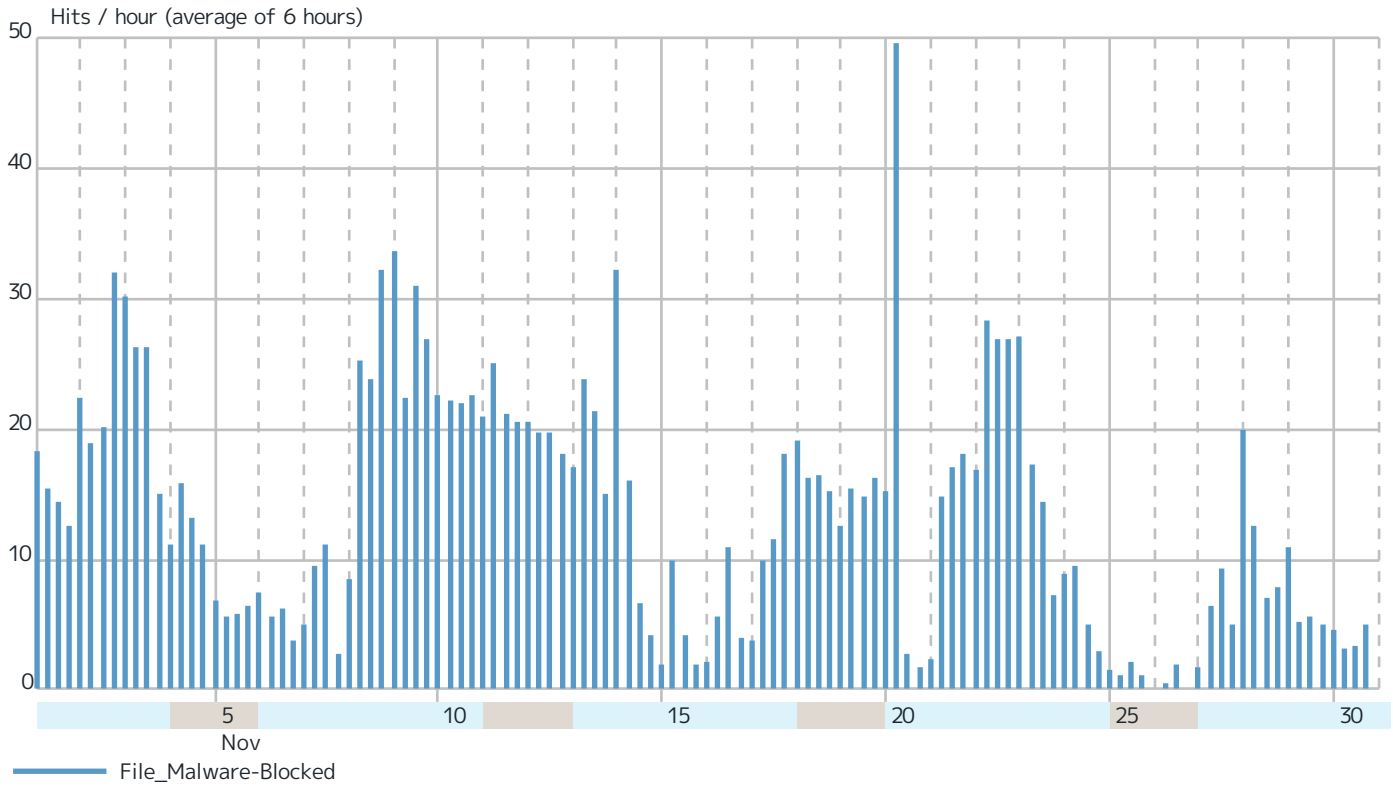
Virenfilterung SRC IPs



Records by src IP		Hits	%
51.77.61.156	Warsaw, Poland	2.56k	26.7 %
89.117.120.225	New York, New York 10118, United States	585	6.1 %
206.225.84.59	United States	520	5.4 %
46.227.62.50	Greece	482	5.0 %
5.63.162.163	Yerevan, Armenia	342	3.6 %
85.197.33.28	NOC dsl	330	3.4 %
185.59.44.224	Turkey	326	3.4 %
173.165.125.149	Bloomington, Illinois 61704, United States	306	3.2 %
172.93.160.112	Los Angeles, California 90045, United States	193	2.0 %
62.146.106.24	Germany	166	1.7 %
167.71.188.163	Clifton, New Jersey 07014, United States	120	1.3 %
185.222.57.94	Amsterdam, Netherlands	110	1.1 %
188.127.231.31	Estonia	110	1.1 %
89.116.243.40	New York, New York 10118, United States	104	1.1 %
91.240.223.143	Przemysl, Poland	98	1.0 %
45.81.241.32	Bolu, Turkey	90	0.9 %
79.98.45.57	Italy	90	0.9 %
2a00:8a60:1:11:2::10	RWTH Aachen	71	0.7 %
51.15.145.18	France	66	0.7 %
192.232.236.18	United States	58	0.6 %
62.210.28.42	France	58	0.6 %
217.66.226.249	Ramallah, Palestine	52	0.5 %
217.66.226.177	Ramallah, Palestine	50	0.5 %
192.64.82.211	United States	48	0.5 %
185.9.147.247	Estonia	46	0.5 %
2.58.95.82	Düsseldorf, Germany	44	0.5 %
80.237.138.229	Cologne, Germany	42	0.4 %
92.52.217.193	Hungary	37	0.4 %
148.72.176.68	St Louis, Missouri 63169, United States	34	0.4 %
174.136.29.202	United States	32	0.3 %
Others		2.42k	25.2 %
Total		**9.59k**	**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.