
Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-10-01 00:00:00+0200

To: 2023-11-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.1, build 11424

Update version
1645

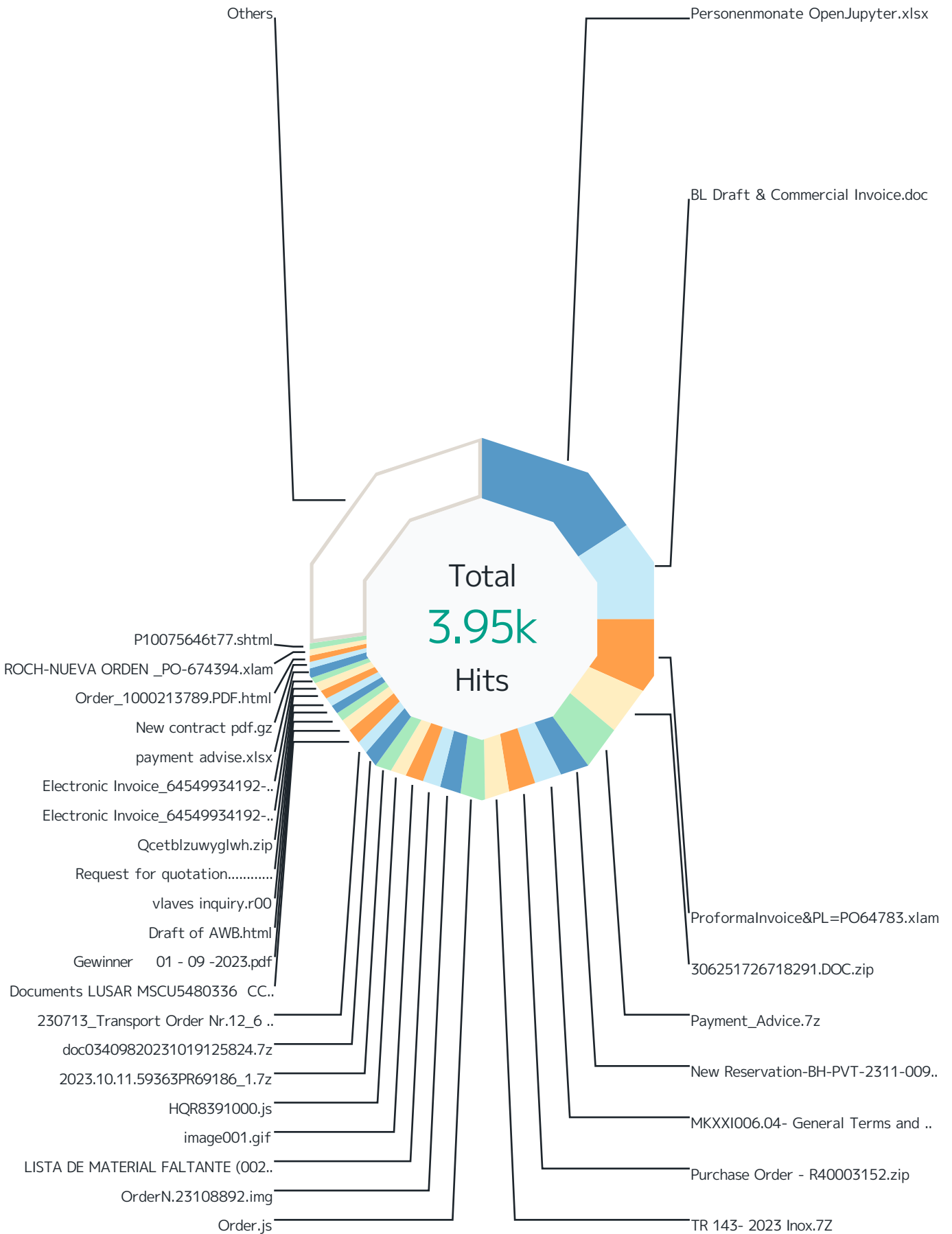
Report started
2023-11-01 09:14:56+0100

Report run time
08:14:53

Filters used
Match All

Virenfilterung MXe	3
Top File Types by Scan Result	5
Top Scan Results by Responding Scanner	10
Top File Types by Responding Scanner	15
Virenfilterung SRC IPs	17
SMTP Virus Filtering by Time	19

Virenfilterung Mx



Records by file name	Hits	%
Personenmonate OpenJupyter.xlsx	620	15.7 %
BL Draft & Commercial Invoice.doc	367	9.3 %
ProformaInvoice&PL=PO64783.xlam	267	6.8 %
306251726718291.DOC.zip	167	4.2 %
Payment_Advice.7z	153	3.9 %
New Reservation-BH-PVT-2311-00928.xlam	107	2.7 %
MKXXI006.04- General Terms and Conditions of Procurement.7z	97	2.5 %
Purchase Order - R40003152.zip	97	2.5 %
TR 143- 2023 Inox.7Z	92	2.3 %
Order.js	88	2.2 %
OrderN.23108892.img	75	1.9 %
LISTA DE MATERIAL FALTANTE (002) (1).zip	64	1.6 %
image001.gif	61	1.5 %
HQR8391000.js	58	1.5 %
2023.10.11.59363PR69186_1.7z	54	1.4 %
doc03409820231019125824.7z	52	1.3 %
230713_Transport Order Nr.12_6 units of Kodiaoq.7z	50	1.3 %
Documents LUSAR MSCU5480336 CC 416.7z	49	1.2 %
Gewinner 01 - 09 -2023.pdf	44	1.1 %
Draft of AWB.html	40	1.0 %
vlaves inquiry.r00	34	0.9 %
Request for quotation.....123453755.zip	34	0.9 %
Qcetblzuwylwh.zip	30	0.8 %
Electronic Invoice_64549934192-2023_JPG.htm	29	0.7 %
Electronic Invoice_64549934192-2023 PDF.htm	29	0.7 %
payment advise.xlsx	27	0.7 %
New contract pdf.gz	25	0.6 %
Order_1000213789.PDF.html	23	0.6 %
ROCH-NUEVA ORDEN _PO-674394.xlam	22	0.6 %
P10075646t77.shtml	22	0.6 %
Others	1.07k	27.1 %
Total	3.95k	100 %

Top File Types by Scan Result

Top 10 file types by scan result.

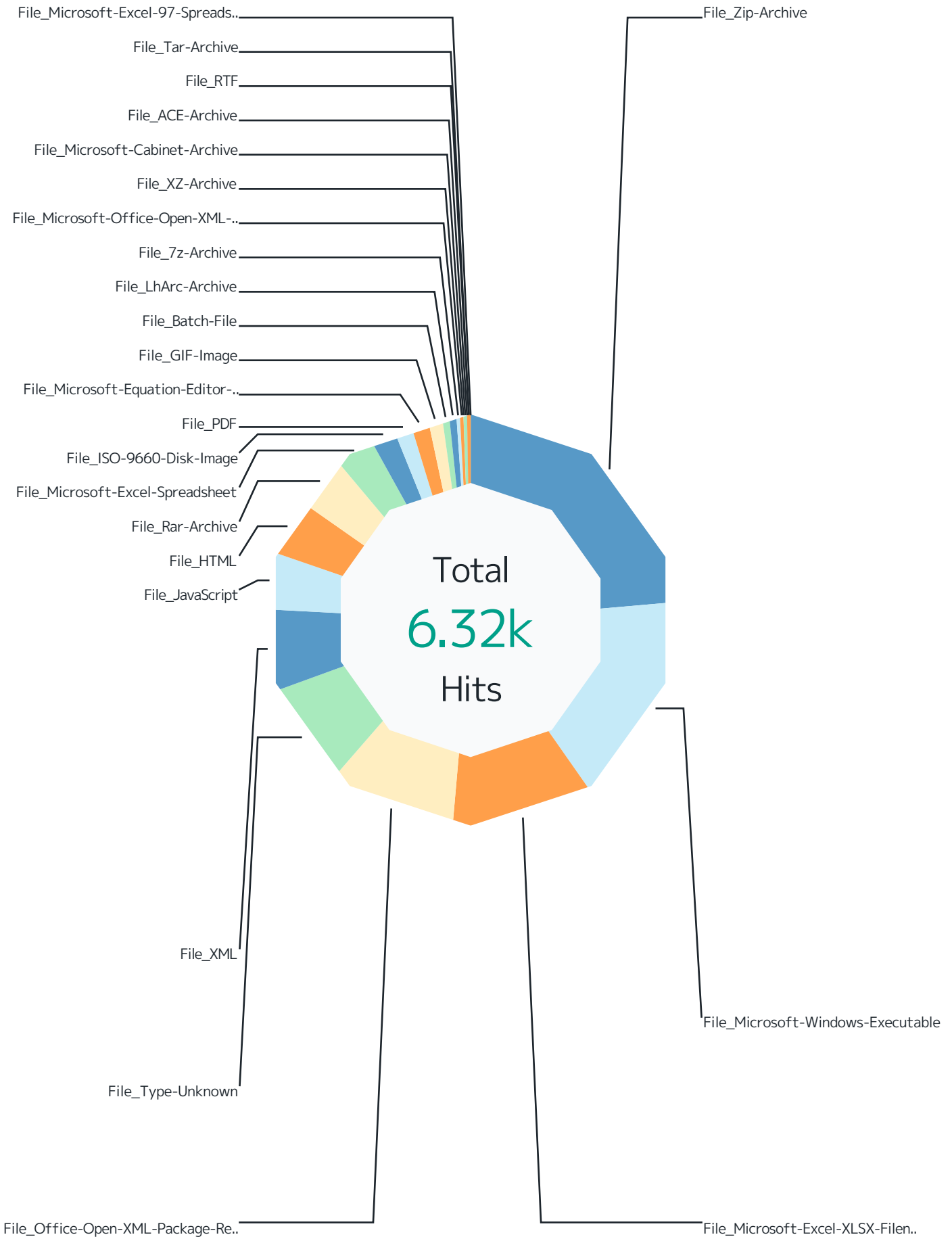
Scan Result	Hits	%
Not Available	2.04k	32.3 %
File_Zip-Archive	1.20k	19.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	667	10.6 %
File_Microsoft-Excel-Spreadsheet	168	2.7 %
File_Microsoft-Office-Open-XML-Document	7	0.1 %
Malicious	1.64k	26.0 %
File_Microsoft-Windows-Executable	955	15.1 %
File_Zip-Archive	202	3.2 %
File_Rar-Archive	148	2.3 %
File_Microsoft-Equation-Editor-Document	81	1.3 %
File_ISO-9660-Disk-Image	62	1.0 %
File_HTML	39	0.6 %
File_JavaScript	33	0.5 %
File_Type-Unknown	29	0.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	20	0.3 %
File_PDF	17	0.3 %
File_Microsoft-Excel-Spreadsheet	9	0.1 %
File_Microsoft-Cabinet-Archive	7	0.1 %
File_XZ-Archive	6	0.1 %
File_LhArc-Archive	5	0.1 %
File_ACE-Archive	5	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_Office-Open-XML-Package-Relations-Item	4	0.1 %
File_7z-Archive	4	0.1 %
File_RTF	4	0.1 %
File_Tar-Archive	4	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
Medium Risk	1.44k	22.8 %
File_Office-Open-XML-Package-Relations-Item	620	9.8 %
File_XML	412	6.5 %
File_GIF-Image	74	1.2 %
File_JavaScript	69	1.1 %
File_Type-Unknown	67	1.1 %
File_HTML	43	0.7 %
File_Batch-File	34	0.5 %
File_Rar-Archive	29	0.5 %
File_PDF	27	0.4 %
File_Microsoft-Windows-Executable	25	0.4 %
File_LhArc-Archive	22	0.3 %

Scan Result	Hits	%
File_Zip-Archive	15	0.2 %
File_XZ-Archive	4	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
High Risk	809	12.8 %
File_Type-Unknown	414	6.6 %
File_Rar-Archive	84	1.3 %
File_Microsoft-Windows-Executable	70	1.1 %
File_Zip-Archive	67	1.1 %
File_ISO-9660-Disk-Image	59	0.9 %
File_PDF	47	0.7 %
File_JavaScript	28	0.4 %
File_7z-Archive	16	0.3 %
File_Batch-File	7	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
File_Office-Open-XML-Package-Relations-Item	3	0.0 %
File_HTML	3	0.0 %
File_RTF	2	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
File_XZ-Archive	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %
JS/Downloader.fp	137	2.2 %
File_JavaScript	137	2.2 %
HTML/Phishing.ta	105	1.7 %
File_HTML	104	1.6 %
File_Type-Unknown	1	0.0 %
HTML/Phishing.tb	38	0.6 %
File_HTML	38	0.6 %
Unknown	15	0.2 %
File_Zip-Archive	14	0.2 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.rb	14	0.2 %
File_HTML	11	0.2 %
File_JavaScript	2	0.0 %
File_Type-Unknown	1	0.0 %
HTML/Phishing.qj	12	0.2 %
File_HTML	12	0.2 %

Scan Result	Hits	%
HTML/Phishing.ry	8	0.1 %
File_HTML	8	0.1 %
Exploit-GBT!C60E496535DB	6	0.1 %
File_Microsoft-Excel-Spreadsheet	6	0.1 %
HTML/Phishing.st	5	0.1 %
File_Type-Unknown	5	0.1 %
HTML/Phishing.ok	5	0.1 %
File_HTML	5	0.1 %
Exploit-GBT!DA70FF97FA6E	4	0.1 %
File_Microsoft-Excel-Spreadsheet	4	0.1 %
HTML/Phishing.ol	4	0.1 %
File_HTML	4	0.1 %
JS/Wonka	3	0.0 %
File_JavaScript	3	0.0 %
Exploit-GBT!C8ECCA73A3EE	3	0.0 %
File_Microsoft-Excel-Spreadsheet	3	0.0 %
AgentTesla-FDKB!017997B8DFE4	3	0.0 %
File_ISO-9660-Disk-Image	3	0.0 %
HTML/Phishing.rj	3	0.0 %
File_JavaScript	3	0.0 %
Exploit-GBT!0B6EA1A06FB0	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
Exploit-GBT!695CD9B6D11C	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
HTML/Phishing.sc	2	0.0 %
File_HTML	2	0.0 %
HTML/Phishing.rl	2	0.0 %
File_JavaScript	2	0.0 %
Exploit-CVE2017-11882.yx	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
Fareit.gen.e	1	0.0 %
File_ACE-Archive	1	0.0 %
Exploit-CVE2017-11882.av	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!B2BFDD558C8A	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Total	6.31k	100 %

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



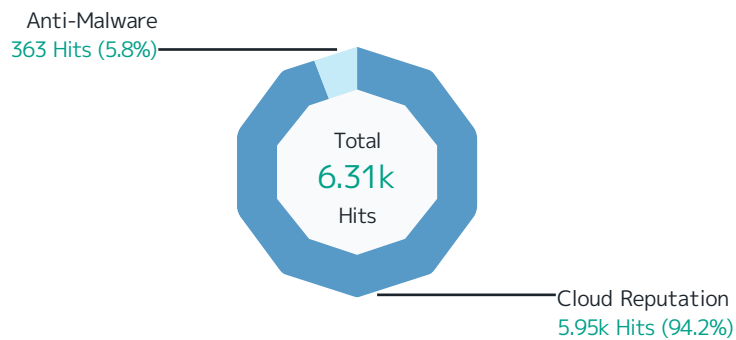
Responding Scanner	Hits	%
File_Zip-Archive	1.50k	23.7 %
Not Available	1.20k	19.0 %
Malicious	202	3.2 %
High Risk	67	1.1 %
Medium Risk	15	0.2 %
Unknown	14	0.2 %
File_Microsoft-Windows-Executable	1.05k	16.6 %
Malicious	955	15.1 %
High Risk	70	1.1 %
Medium Risk	25	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	694	11.0 %
Not Available	667	10.6 %
Malicious	20	0.3 %
High Risk	3	0.0 %
Exploit-GBT!695CD9B6D11C	2	0.0 %
Medium Risk	1	0.0 %
Exploit-CVE2017-11882.av	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	627	9.9 %
Medium Risk	620	9.8 %
Malicious	4	0.1 %
High Risk	3	0.0 %
File_Type-Unknown	517	8.2 %
High Risk	414	6.6 %
Medium Risk	67	1.1 %
Malicious	29	0.5 %
HTML/Phishing.st	5	0.1 %
HTML/Phishing.ta	1	0.0 %
HTML/Phishing.rb	1	0.0 %
File_XML	412	6.5 %
Medium Risk	412	6.5 %
File_JavaScript	277	4.4 %
JS/Downloader.fp	137	2.2 %
Medium Risk	69	1.1 %
Malicious	33	0.5 %
High Risk	28	0.4 %
JS/Wonka	3	0.0 %
HTML/Phishing.rj	3	0.0 %
HTML/Phishing.rb	2	0.0 %
HTML/Phishing.rl	2	0.0 %

Responding Scanner	Hits	%
File_HTML	272	4.3 %
HTML/Phishing.ta	104	1.6 %
Medium Risk	43	0.7 %
Malicious	39	0.6 %
HTML/Phishing.tb	38	0.6 %
HTML/Phishing.qi	12	0.2 %
HTML/Phishing.rb	11	0.2 %
HTML/Phishing.ry	8	0.1 %
HTML/Phishing.ok	5	0.1 %
HTML/Phishing.ol	4	0.1 %
High Risk	3	0.0 %
HTML/Phishing.sc	2	0.0 %
File_Rar-Archive	261	4.1 %
Malicious	148	2.3 %
High Risk	84	1.3 %
Medium Risk	29	0.5 %
File_Microsoft-Excel-Spreadsheet	197	3.1 %
Not Available	168	2.7 %
Malicious	9	0.1 %
Exploit-GBT!C60E496535DB	6	0.1 %
Exploit-GBT!DA70FF97FA6E	4	0.1 %
Exploit-GBT!C8ECCA73A3EE	3	0.0 %
Exploit-GBT!0B6EA1A06FBO	2	0.0 %
Exploit-CVE2017-11882.yx	2	0.0 %
High Risk	1	0.0 %
Unknown	1	0.0 %
Exploit-GBT!B2BFDD558C8A	1	0.0 %
File_ISO-9660-Disk-Image	124	2.0 %
Malicious	62	1.0 %
High Risk	59	0.9 %
Agent Tesla-FDKB!017997B8DFE4	3	0.0 %
File_PDF	91	1.4 %
High Risk	47	0.7 %
Medium Risk	27	0.4 %
Malicious	17	0.3 %
File_Microsoft-Equation-Editor-Document	81	1.3 %
Malicious	81	1.3 %
File_GIF-Image	74	1.2 %
Medium Risk	74	1.2 %

Responding Scanner	Hits	%
File_Batch-File	41	0.6 %
Medium Risk	34	0.5 %
High Risk	7	0.1 %
File_LhArc-Archive	28	0.4 %
Medium Risk	22	0.3 %
Malicious	5	0.1 %
High Risk	1	0.0 %
File_7z-Archive	20	0.3 %
High Risk	16	0.3 %
Malicious	4	0.1 %
File_Microsoft-Office-Open-XML-Document	11	0.2 %
Not Available	7	0.1 %
Malicious	3	0.0 %
High Risk	1	0.0 %
File_XZ-Archive	11	0.2 %
Malicious	6	0.1 %
Medium Risk	4	0.1 %
High Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	8	0.1 %
Malicious	7	0.1 %
High Risk	1	0.0 %
File_ACE-Archive	6	0.1 %
Malicious	5	0.1 %
Fareit.gen.e	1	0.0 %
File_RTF	6	0.1 %
Malicious	4	0.1 %
High Risk	2	0.0 %
File_Tar-Archive	5	0.1 %
Malicious	4	0.1 %
High Risk	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
Malicious	5	0.1 %
Total	6.32k	100 %

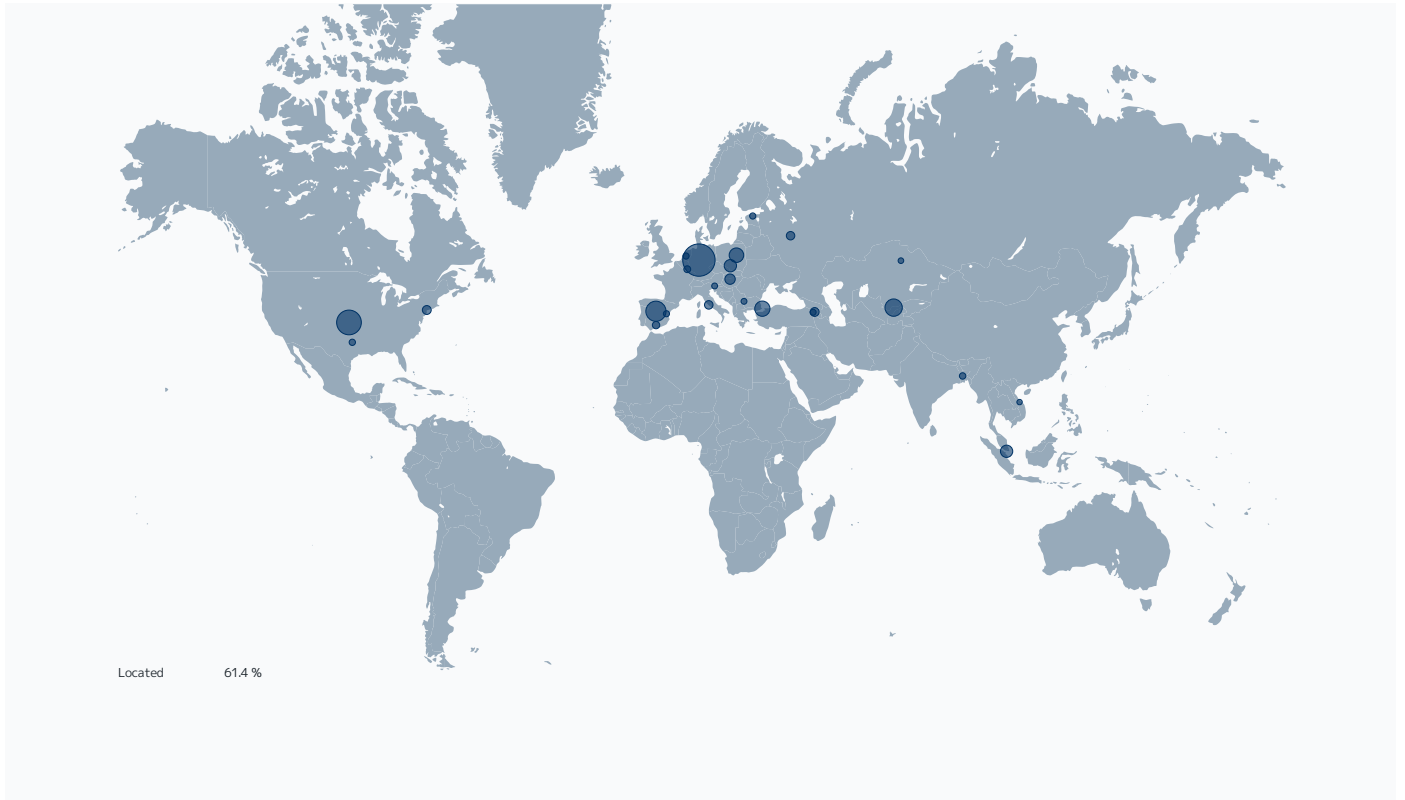
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	5.95k	94.2 %
File_Zip-Archive	1.50k	23.7 %
File_Microsoft-Windows-Executable	1.05k	16.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	691	10.9 %
File_Office-Open-XML-Package-Relations-Item	627	9.9 %
File_Type-Unknown	510	8.1 %
File_XML	412	6.5 %
File_Rar-Archive	261	4.1 %
File_Microsoft-Excel-Spreadsheet	179	2.8 %
File_JavaScript	130	2.1 %
File_ISO-9660-Disk-Image	121	1.9 %
File_PDF	91	1.4 %
File_HTML	85	1.3 %
File_Microsoft-Equation-Editor-Document	81	1.3 %
File_GIF-Image	74	1.2 %
File_Batch-File	41	0.6 %
File_LhArc-Archive	28	0.4 %
File_7z-Archive	20	0.3 %
File_Microsoft-Office-Open-XML-Document	11	0.2 %
File_XZ-Archive	11	0.2 %
File_Microsoft-Cabinet-Archive	8	0.1 %
File_RTF	6	0.1 %
File_ACE-Archive	5	0.1 %
File_Tar-Archive	5	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
Anti-Malware	363	5.8 %
File_HTML	184	2.9 %
File_JavaScript	147	2.3 %
File_Microsoft-Excel-Spreadsheet	18	0.3 %
File_Type-Unknown	7	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
File_ISO-9660-Disk-Image	3	0.0 %
File_ACE-Archive	1	0.0 %
Total	6.31k	100 %

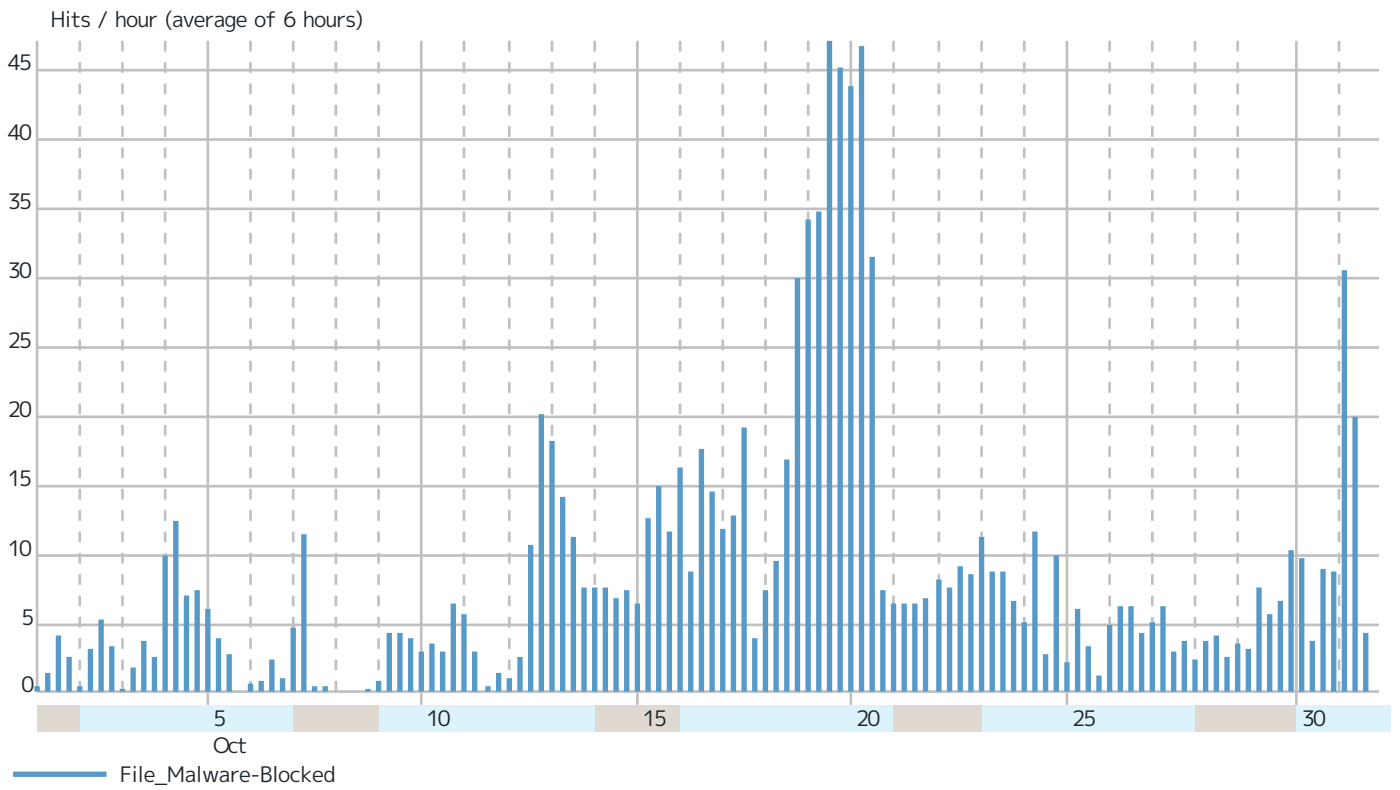
Virenfiterung SRC IPs



Records by src IP		Hits	%
91.142.209.125	 Spain	391	6.2 %
192.232.236.18	 United States	354	5.6 %
139.28.44.18	 Tashkent, Uzbekistan	320	5.1 %
37.120.175.171	 Germany	314	5.0 %
51.77.61.156	 Warsaw, Poland	250	4.0 %
89.252.134.111	 Istanbul, Turkey	218	3.5 %
85.13.136.47	 Germany	214	3.4 %
178.217.221.187	 Myslowice, Poland	195	3.1 %
31.192.238.25	 Singapore	194	3.1 %
62.146.106.21	 Germany	166	2.6 %
194.41.47.212	 Hungary	146	2.3 %
206.225.84.59	 United States	128	2.0 %
198.46.226.138	 Brooklyn, New York 11211, United States	109	1.7 %
217.113.0.244	 Armenia	108	1.7 %
77.43.14.247	 Rome, Italy	100	1.6 %
31.31.198.204	 Russia	98	1.6 %
217.18.165.50	 Alhendin, Spain	71	1.1 %
80.92.66.174	 Belvaux, Luxembourg	58	0.9 %
185.86.12.7	 Istanbul, Turkey	50	0.8 %
122.102.32.230	 Bangladesh	48	0.8 %
169.48.73.54	 Texas, United States	45	0.7 %
81.171.8.199	 Renswoude, Netherlands	42	0.7 %
188.127.235.18	 Estonia	41	0.6 %
185.31.238.131	 Geldo, Spain	40	0.6 %
5.63.162.163	 Yerevan, Armenia	38	0.6 %
82.115.209.247	 Bulgaria	34	0.5 %
93.103.218.6	 Polhov Gradec, Slovenia	34	0.5 %
185.113.132.33	 Astana, Kazakhstan	28	0.4 %
185.145.13.119	 United States	22	0.3 %
103.170.121.194	 Vietnam	22	0.3 %
Others		2.44k	38.6 %
Total		6.31k	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.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](#).

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.