
Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-08-01 00:00:00+0200

To: 2023-09-01 00:00:00+0200

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.0, build 11407

Update version
1626

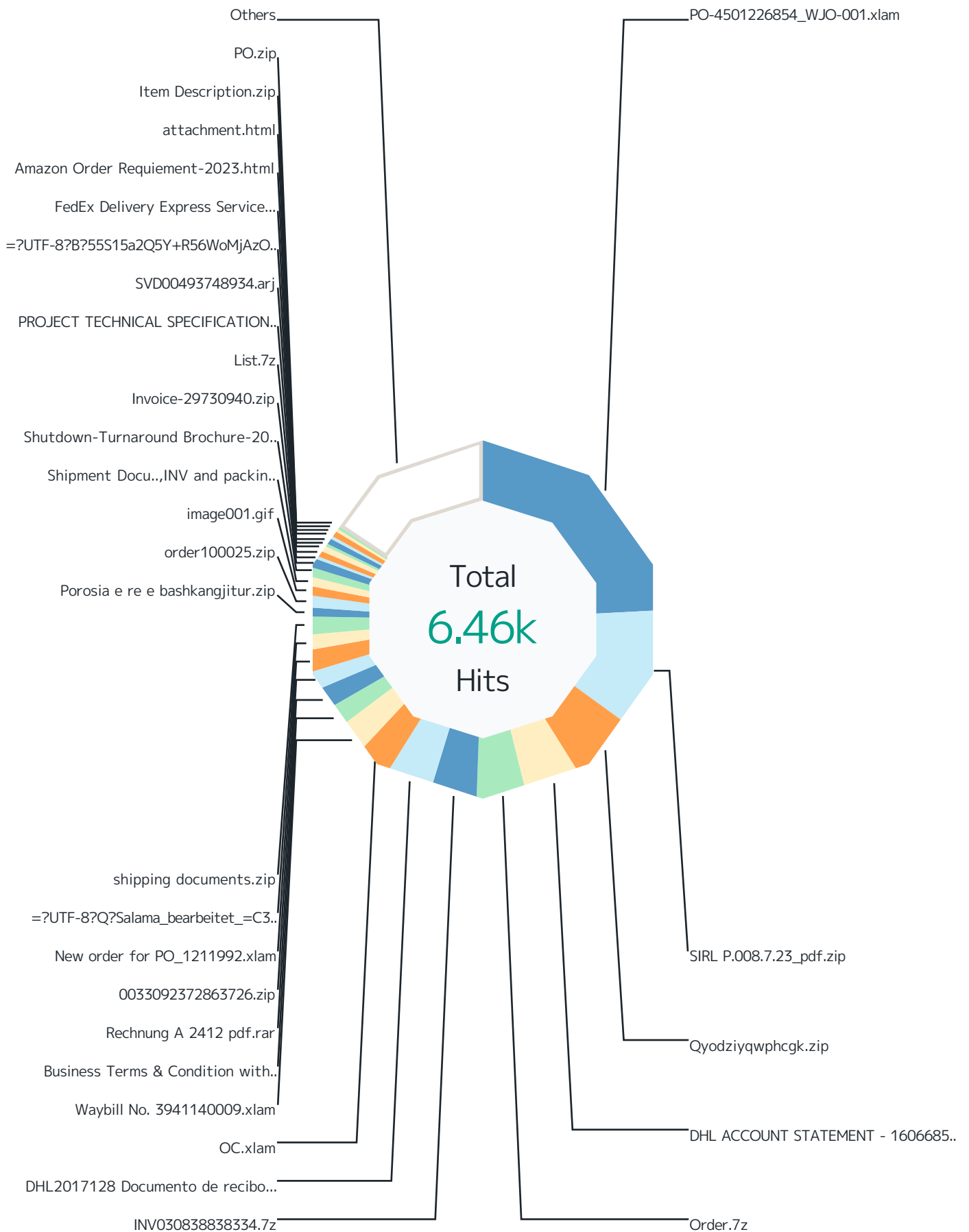
Report started
2023-09-01 08:51:41+0200

Report run time
08:58:08

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

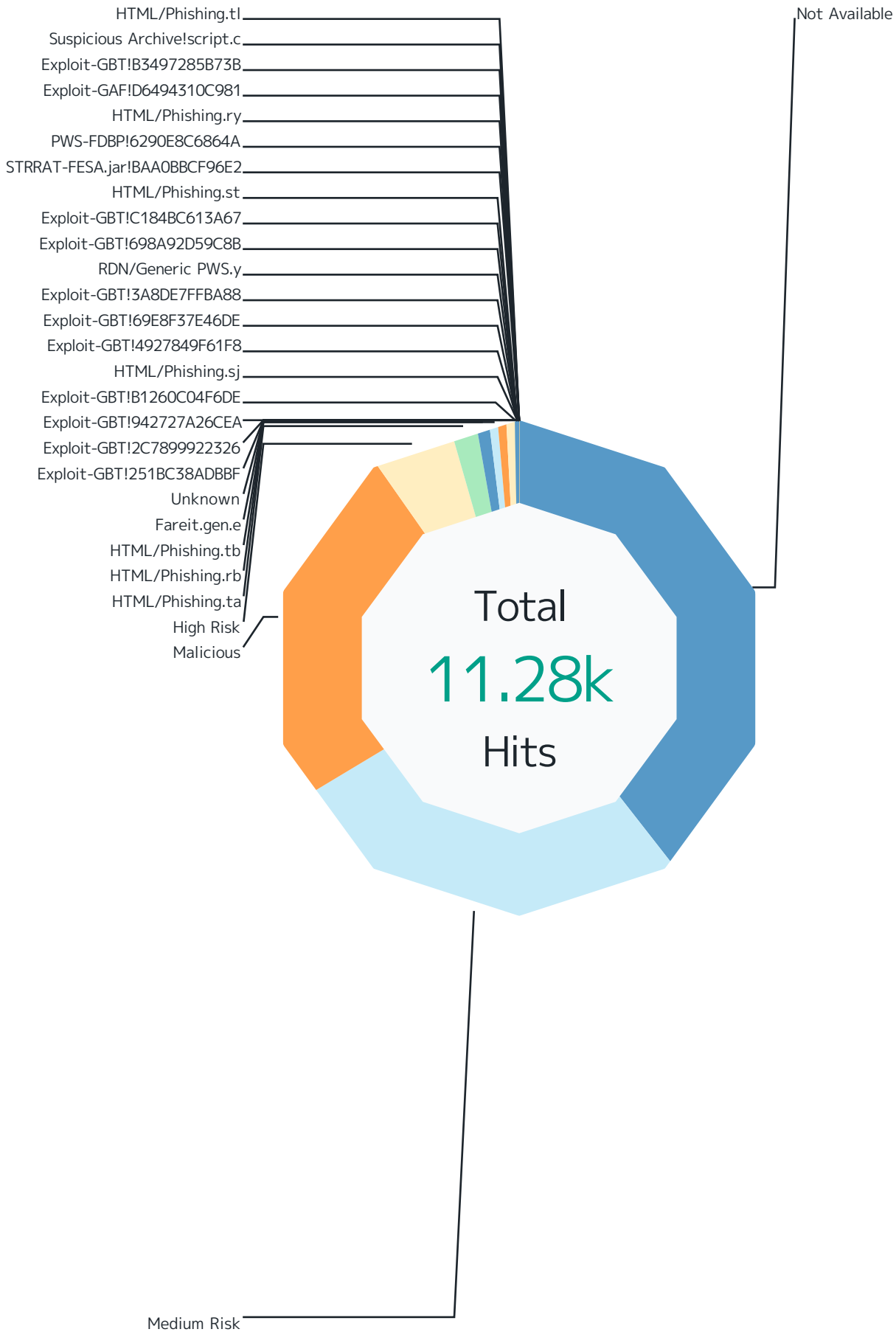
Virenterung MXe



Records by file name	Hits	%
PO-4501226854_WJO-001.xlam	1.56k	24.2 %
SIRL P.008.7.23_pdf.zip	705	10.9 %
Qyodziyqwphcgk.zip	380	5.9 %
DHL ACCOUNT STATEMENT - 1606685194.xlam	324	5.0 %
Order.7z	294	4.6 %
INV030838838334.7z	271	4.2 %
DHL2017128 Documento de recibo.xlam	261	4.0 %
OC.xlam	197	3.1 %
Waybill No. 3941140009.xlam	180	2.8 %
Business Terms & Condition withPurchase Order.zip	134	2.1 %
Rechnung A 2412 pdf.rar	122	1.9 %
0033092372863726.zip	116	1.8 %
New order for PO_1211992.xlam	110	1.7 %
=?UTF-8?Q?Salama_bearbeitet_=C3=BCberarbeitet_von_DS_1_August_2023=2Edo cx?= shipping documents.zip	107	1.7 %
Porosia e re e bashkangjitur.zip	91	1.4 %
order100025.zip	70	1.1 %
image001.gif	60	0.9 %
Shipment Document BL,INV and packing list.ace	58	0.9 %
Shutdown-Turnaround Brochure-2023.pdf	57	0.9 %
Invoice-29730940.zip	54	0.8 %
List.7z	42	0.7 %
PROJECT TECHNICAL SPECIFICATION AND EVALUATION.pdf	34	0.5 %
SVD00493748934.arj	31	0.5 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMi0yMDIyLnBkZi5odG0=?= FedEx Delivery Express Service.docx	27	0.4 %
Amazon Order Requiement-2023.html	27	0.4 %
attachment.html	26	0.4 %
Item Description.zip	24	0.4 %
PO.zip	24	0.4 %
Others	22	0.3 %
Total	6.46k	100 %

Top File Types by Scan Result

Top 10 file types by scan result.



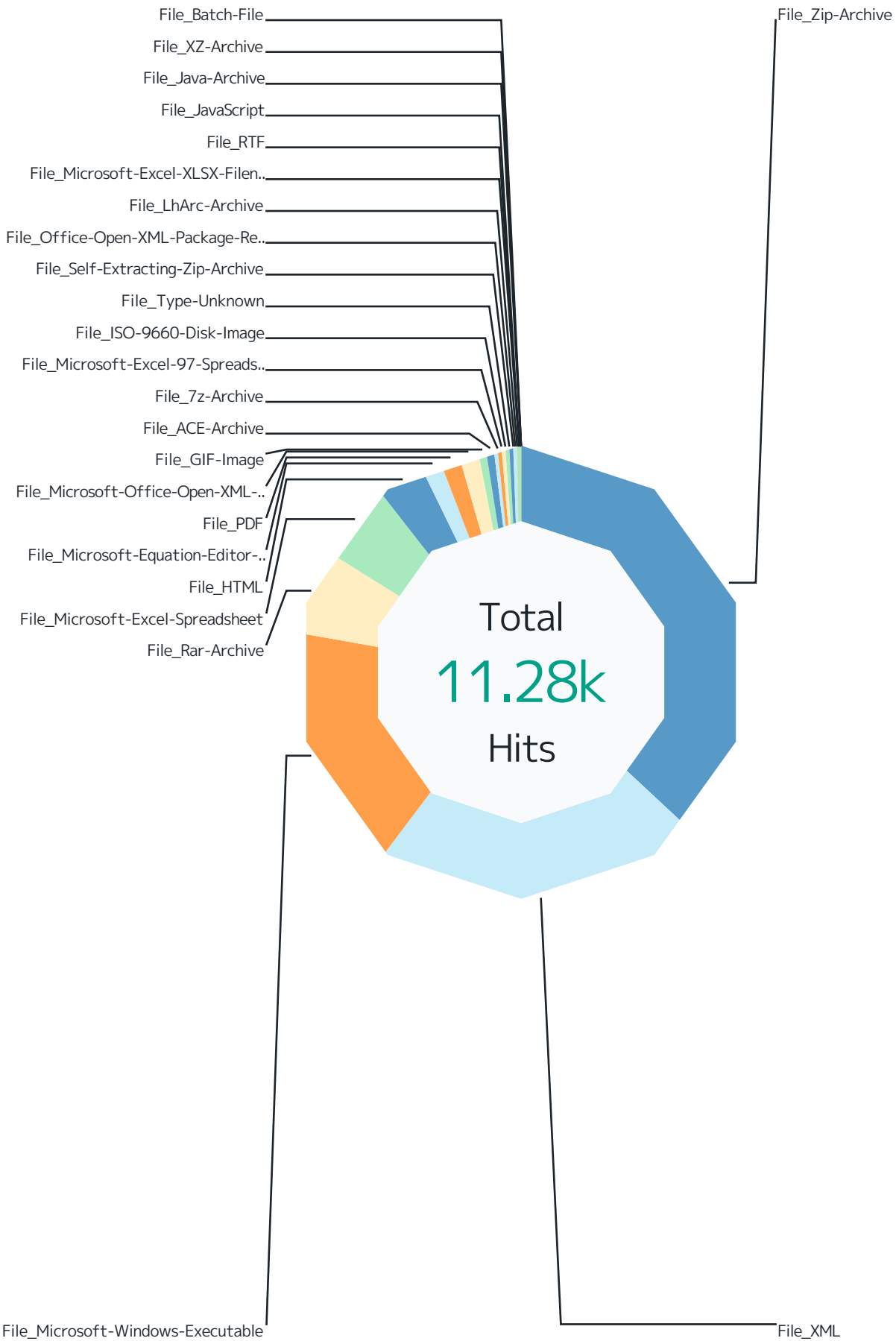
Scan Result	Hits	%
Not Available	4.45k	39.5 %
File_Zip-Archive	3.80k	33.7 %
File_Microsoft-Excel-Spreadsheet	591	5.2 %
File_Microsoft-Office-Open-XML-Document	67	0.6 %
Medium Risk	3.04k	27.0 %
File_XML	2.62k	23.2 %
File_Rar-Archive	113	1.0 %
File_PDF	103	0.9 %
File_GIF-Image	73	0.6 %
File_Microsoft-Windows-Executable	70	0.6 %
File_HTML	18	0.2 %
File_Microsoft-Excel-Spreadsheet	11	0.1 %
File_Microsoft-Office-Open-XML-Document	11	0.1 %
File_Office-Open-XML-Package-Relations-Item	7	0.1 %
File_7z-Archive	4	0.0 %
File_Type-Unknown	4	0.0 %
File_LhArc-Archive	3	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_Zip-Archive	1	0.0 %
File_JavaScript	1	0.0 %
Malicious	2.67k	23.7 %
File_Microsoft-Windows-Executable	1.73k	15.3 %
File_Rar-Archive	454	4.0 %
File_Zip-Archive	279	2.5 %
File_7z-Archive	30	0.3 %
File_Microsoft-Office-Open-XML-Document	27	0.2 %
File_ISO-9660-Disk-Image	27	0.2 %
File_Microsoft-Excel-97-Spreadsheet	25	0.2 %
File_Self-Extracting-Zip-Archive	24	0.2 %
File_HTML	22	0.2 %
File_Microsoft-Excel-Spreadsheet	15	0.1 %
File_ACE-Archive	13	0.1 %
File_Type-Unknown	7	0.1 %
File_Microsoft-Equation-Editor-Document	6	0.1 %
File_Office-Open-XML-Package-Relations-Item	5	0.0 %
File_PDF	4	0.0 %
File_LhArc-Archive	2	0.0 %
File_XZ-Archive	1	0.0 %
File_Batch-File	1	0.0 %

Scan Result	Hits	%
High Risk	609	5.4 %
File_Microsoft-Windows-Executable	198	1.8 %
File_Microsoft-Equation-Editor-Document	170	1.5 %
File_Rar-Archive	107	0.9 %
File_PDF	42	0.4 %
File_Zip-Archive	27	0.2 %
File_HTML	12	0.1 %
File_Office-Open-XML-Package-Relations-Item	8	0.1 %
File_Microsoft-Excel-97-Spreadsheet	7	0.1 %
File_Type-Unknown	6	0.1 %
File_LhArc-Archive	6	0.1 %
File_RTF	6	0.1 %
File_Microsoft-Office-Open-XML-Document	4	0.0 %
File_7z-Archive	3	0.0 %
File_JavaScript	3	0.0 %
File_Java-Archive	3	0.0 %
File_ACE-Archive	2	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_XZ-Archive	2	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.ta	176	1.6 %
File_HTML	134	1.2 %
File_Zip-Archive	42	0.4 %
HTML/Phishing.rb	111	1.0 %
File_HTML	101	0.9 %
File_Type-Unknown	10	0.1 %
HTML/Phishing.tb	63	0.6 %
File_HTML	63	0.6 %
Fareit.gen.e	57	0.5 %
File_ACE-Archive	57	0.5 %
Unknown	54	0.5 %
File_Microsoft-Office-Open-XML-Document	32	0.3 %
File_Zip-Archive	22	0.2 %
Exploit-GBT!251BC38ADBBF	8	0.1 %
File_Microsoft-Excel-Spreadsheet	8	0.1 %
Exploit-GBT!2C7899922326	5	0.0 %
File_Microsoft-Excel-Spreadsheet	5	0.0 %
Exploit-GBT!942727A26CEA	3	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %

Scan Result	Hits	%
Exploit-GBT!B1260C04F6DE	3	0.0 %
File_Microsoft-Excel-Spreadsheet	3	0.0 %
HTML/Phishing.sj	2	0.0 %
File_Type-Unknown	2	0.0 %
Exploit-GBT!4927849F61F8	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!69E8F37E46DE	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
Exploit-GBT!3A8DE7FFBA88	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
RDN/Generic PWS.y	2	0.0 %
File_Rar-Archive	2	0.0 %
Exploit-GBT!698A92D59C8B	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!C184BC613A67	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.st	1	0.0 %
File_Type-Unknown	1	0.0 %
STRRAT-FESA.jar!BAA0BBCF96E2	1	0.0 %
File_Java-Archive	1	0.0 %
PWS-FDBP!6290E8C6864A	1	0.0 %
File_Rar-Archive	1	0.0 %
HTML/Phishing.ry	1	0.0 %
File_HTML	1	0.0 %
Exploit-GAF!D6494310C981	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!B3497285B73B	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Suspicious Archive!script.c	1	0.0 %
File_7z-Archive	1	0.0 %
HTML/Phishing.tl	1	0.0 %
File_HTML	1	0.0 %
Total	11.28k	100 %

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



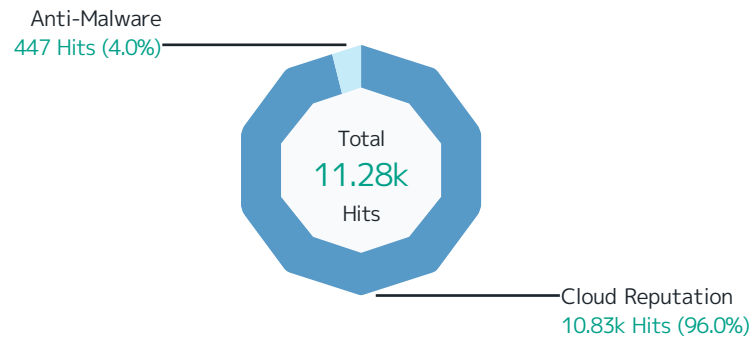
Responding Scanner	Hits	%
File_Zip-Archive	4.17k	36.9 %
Not Available	3.80k	33.7 %
Malicious	279	2.5 %
HTML/Phishing.ta	42	0.4 %
High Risk	27	0.2 %
Unknown	22	0.2 %
Medium Risk	1	0.0 %
File_XML	2.62k	23.2 %
Medium Risk	2.62k	23.2 %
File_Microsoft-Windows-Executable	2.00k	17.7 %
Malicious	1.73k	15.3 %
High Risk	198	1.8 %
Medium Risk	70	0.6 %
File_Rar-Archive	677	6.0 %
Malicious	454	4.0 %
Medium Risk	113	1.0 %
High Risk	107	0.9 %
RDN/Generic PWS.y	2	0.0 %
PWS-FDBP!6290E8C6864A	1	0.0 %
File_Microsoft-Excel-Spreadsheet	640	5.7 %
Not Available	591	5.2 %
Malicious	15	0.1 %
Medium Risk	11	0.1 %
Exploit-GBT!251BC38ADBBF	8	0.1 %
Exploit-GBT!2C7899922326	5	0.0 %
Exploit-GBT!B1260C04F6DE	3	0.0 %
Exploit-GBT!69E8F37E46DE	2	0.0 %
Exploit-GBT!3A8DE7FFBA88	2	0.0 %
High Risk	1	0.0 %
Exploit-GBT!C184BC613A67	1	0.0 %
Exploit-GBT!B3497285B73B	1	0.0 %
File_HTML	352	3.1 %
HTML/Phishing.ta	134	1.2 %
HTML/Phishing.rb	101	0.9 %
HTML/Phishing.tb	63	0.6 %
Malicious	22	0.2 %
Medium Risk	18	0.2 %
High Risk	12	0.1 %
HTML/Phishing.ry	1	0.0 %

Responding Scanner	Hits	%
HTML/Phishing.tl	1	0.0 %
File_Microsoft-Equation-Editor-Document	176	1.6 %
High Risk	170	1.5 %
Malicious	6	0.1 %
File_PDF	149	1.3 %
Medium Risk	103	0.9 %
High Risk	42	0.4 %
Malicious	4	0.0 %
File_Microsoft-Office-Open-XML-Document	141	1.3 %
Not Available	67	0.6 %
Unknown	32	0.3 %
Malicious	27	0.2 %
Medium Risk	11	0.1 %
High Risk	4	0.0 %
File_GIF-Image	73	0.6 %
Medium Risk	73	0.6 %
File_ACE-Archive	72	0.6 %
Fareit.gen.e	57	0.5 %
Malicious	13	0.1 %
High Risk	2	0.0 %
File_7z-Archive	38	0.3 %
Malicious	30	0.3 %
Medium Risk	4	0.0 %
High Risk	3	0.0 %
Suspicious Archive!script.c	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	32	0.3 %
Malicious	25	0.2 %
High Risk	7	0.1 %
File_ISO-9660-Disk-Image	31	0.3 %
Malicious	27	0.2 %
Medium Risk	2	0.0 %
High Risk	2	0.0 %
File_Type-Unknown	30	0.3 %
HTML/Phishing.rb	10	0.1 %
Malicious	7	0.1 %
High Risk	6	0.1 %
Medium Risk	4	0.0 %
HTML/Phishing.sj	2	0.0 %
HTML/Phishing.st	1	0.0 %

Responding Scanner	Hits	%
File_Self-Extracting-Zip-Archive	24	0.2 %
Malicious	24	0.2 %
File_Office-Open-XML-Package-Relations-Item	20	0.2 %
High Risk	8	0.1 %
Medium Risk	7	0.1 %
Malicious	5	0.0 %
File_LhArc-Archive	11	0.1 %
High Risk	6	0.1 %
Medium Risk	3	0.0 %
Malicious	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.1 %
Exploit-GBT!942727A26CEA	3	0.0 %
Exploit-GBT!4927849F61F8	2	0.0 %
Exploit-GBT!698A92D59C8B	2	0.0 %
Exploit-GAF!D6494310C981	1	0.0 %
File_RTF	6	0.1 %
High Risk	6	0.1 %
File_JavaScript	4	0.0 %
High Risk	3	0.0 %
Medium Risk	1	0.0 %
File_Java-Archive	4	0.0 %
High Risk	3	0.0 %
STRRAT-FESA.jar!BAA0BBCF96E2	1	0.0 %
File_XZ-Archive	3	0.0 %
High Risk	2	0.0 %
Malicious	1	0.0 %
File_Batch-File	1	0.0 %
Malicious	1	0.0 %
Total	11.28k	100 %

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	10.83k	96.0 %
File_Zip-Archive	4.13k	36.6 %
File_XML	2.62k	23.2 %
File_Microsoft-Windows-Executable	2.00k	17.7 %
File_Rar-Archive	674	6.0 %
File_Microsoft-Excel-Spreadsheet	618	5.5 %
File_Microsoft-Equation-Editor-Document	176	1.6 %
File_PDF	149	1.3 %
File_Microsoft-Office-Open-XML-Document	141	1.3 %
File_GIF-Image	73	0.6 %
File_HTML	52	0.5 %
File_7z-Archive	37	0.3 %
File_Microsoft-Excel-97-Spreadsheet	32	0.3 %
File_ISO-9660-Disk-Image	31	0.3 %
File_Self-Extracting-Zip-Archive	24	0.2 %
File_Office-Open-XML-Package-Relations-Item	20	0.2 %
File_Type-Unknown	17	0.2 %
File_ACE-Archive	15	0.1 %
File_LhArc-Archive	11	0.1 %
File_RTF	6	0.1 %
File_JavaScript	4	0.0 %
File_Java-Archive	3	0.0 %
File_XZ-Archive	3	0.0 %
File_Batch-File	1	0.0 %
Anti-Malware	447	4.0 %
File_HTML	300	2.7 %
File_ACE-Archive	57	0.5 %
File_Zip-Archive	42	0.4 %
File_Microsoft-Excel-Spreadsheet	22	0.2 %
File_Type-Unknown	13	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.1 %
File_Rar-Archive	3	0.0 %
File_7z-Archive	1	0.0 %
File_Java-Archive	1	0.0 %
Total	11.28k	100 %

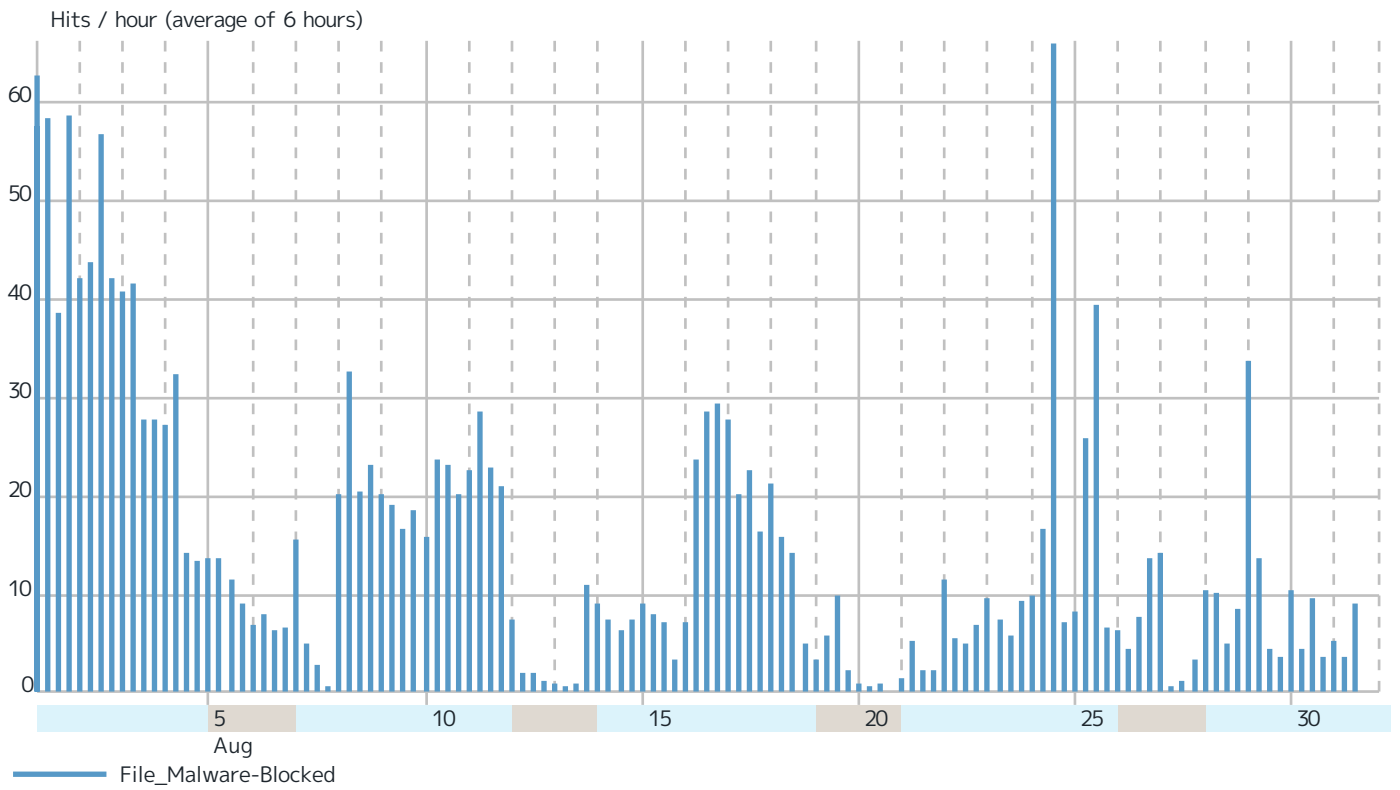
Virenfilterung SRC IPs



Records by src IP		Hits	%
209.87.159.147	 United States	3.65k	32.4 %
82.194.72.48	 Spain	1.41k	12.5 %
77.68.10.89	 United Kingdom	905	8.0 %
185.59.44.224	 Turkey	778	6.9 %
92.204.129.53	 Warrenton, Virginia 20186, United States	588	5.2 %
85.13.149.240	 Germany	518	4.6 %
213.142.149.195	 Turkey	277	2.5 %
207.244.241.153	 St Louis, Missouri 63101, United States	268	2.4 %
77.92.99.71	 Skutari, Turkey	242	2.1 %
106.75.67.156	 China	220	2.0 %
94.198.54.49	 Estonia	182	1.6 %
109.228.57.79	 United Kingdom	156	1.4 %
51.77.61.156	 Warsaw, Poland	140	1.2 %
84.54.51.224	 Ashburn, Virginia 20104, United States	113	1.0 %
192.232.236.18	 United States	68	0.6 %
168.119.36.181	 Germany	64	0.6 %
74.208.244.91	 United States	63	0.6 %
193.42.36.223	 Warsaw, Poland	48	0.4 %
103.180.136.9	 Vietnam	48	0.4 %
196.29.32.34	 Harare, Zimbabwe	45	0.4 %
45.148.122.66	 Netherlands	42	0.4 %
46.231.3.30	 Spain	42	0.4 %
94.237.102.47	 Finland	34	0.3 %
94.156.102.252	 Bulgaria	32	0.3 %
210.122.9.54	 South Korea	30	0.3 %
185.9.147.136	 Estonia	30	0.3 %
152.89.218.193	 Moscow, Russia	28	0.2 %
210.122.9.53	 South Korea	27	0.2 %
181.210.30.114	 Tegucigalpa, Honduras	27	0.2 %
172.104.10.114	 Cedar Knolls, New Jersey 07927, United States	27	0.2 %
Others		1.18k	10.4 %
Total		11.28k	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.