
Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenterung Server Firewall

Report period

From: 2024-01-01 00:00:00+0100

To: 2024-02-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.2, build 11426

Update version
1684

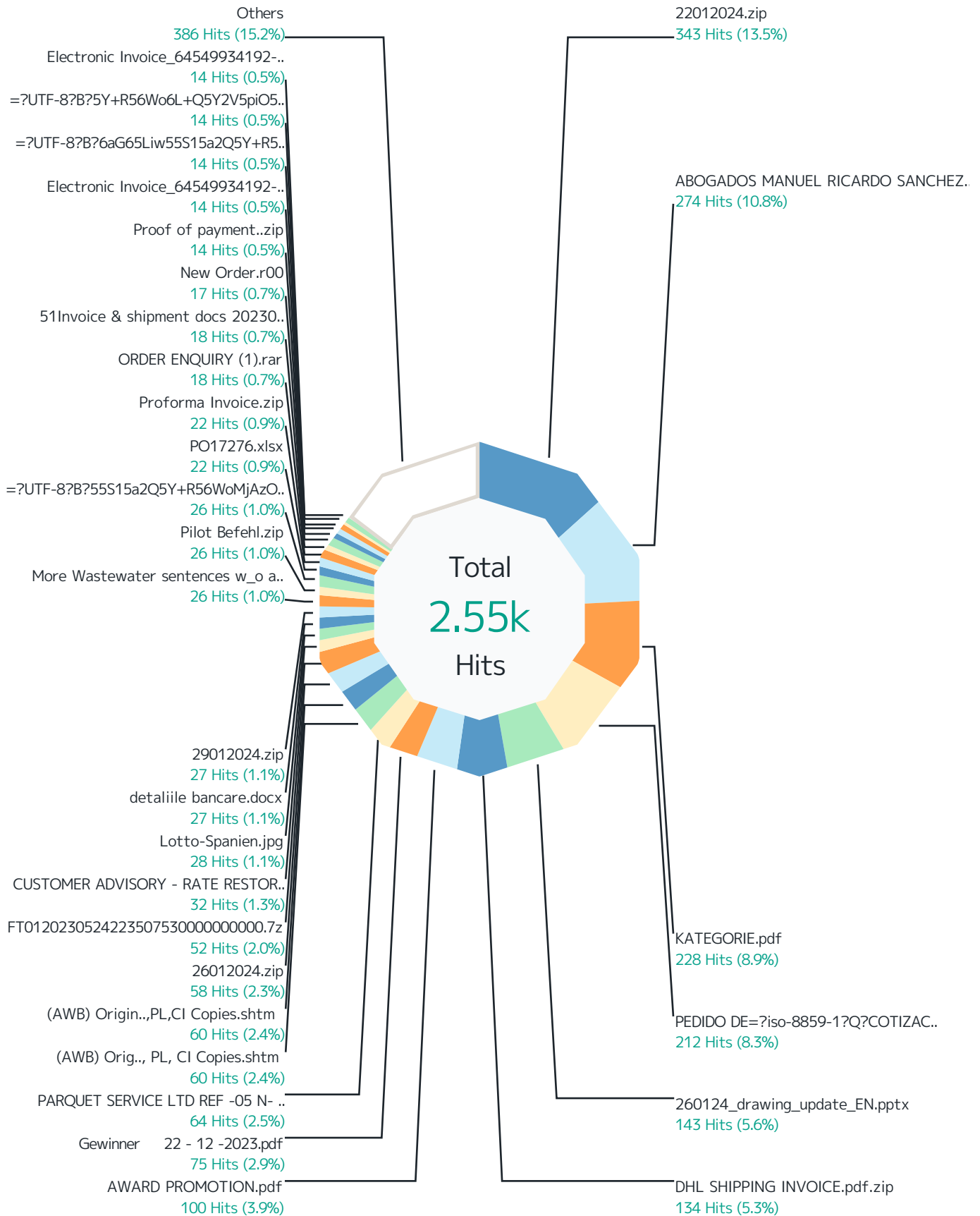
Report started
2024-02-01 08:02:47+0100

Report run time
10:01:13

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

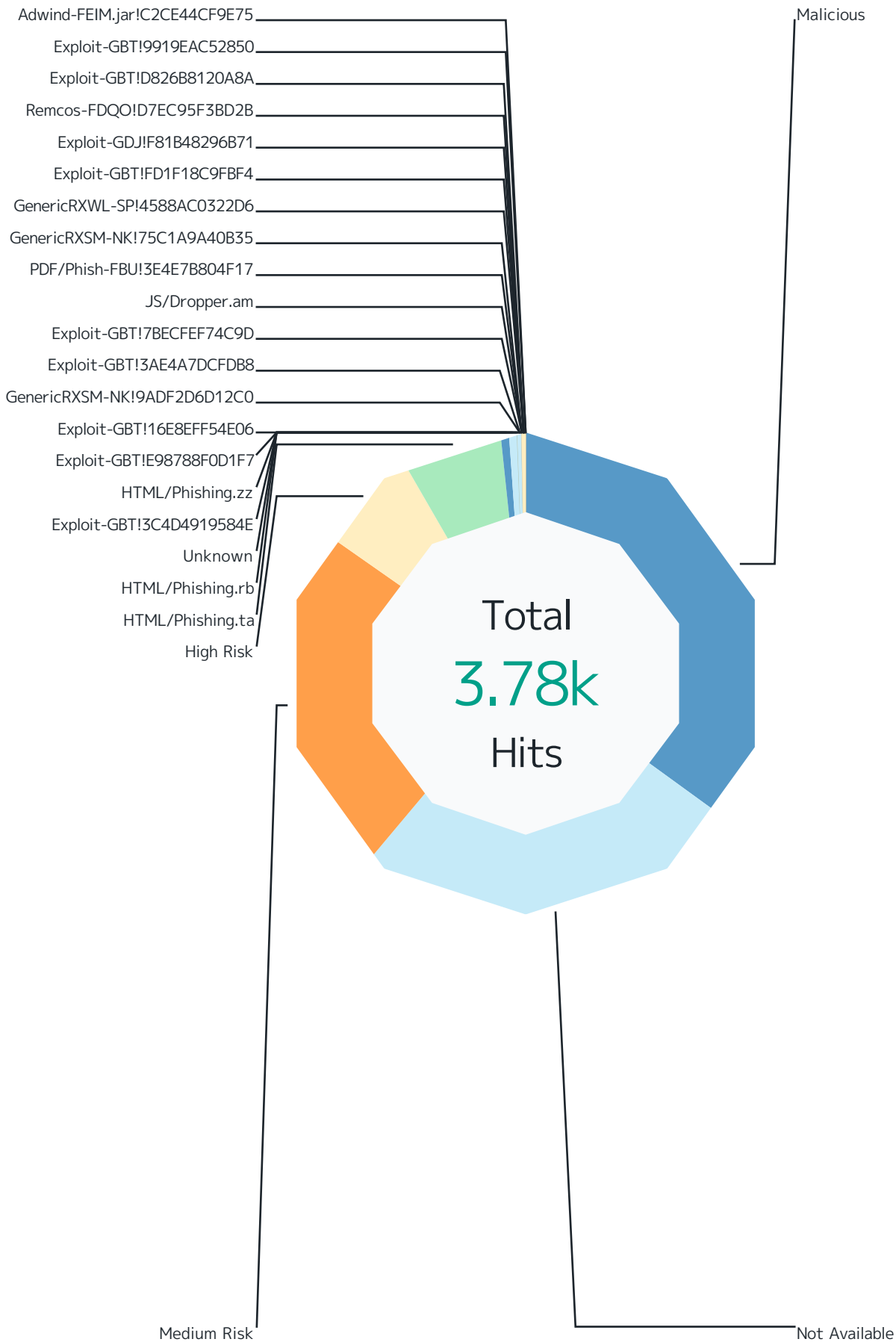
Virenfilterung MXe



Records by file name	Hits	%
22012024.zip	343	13.5 %
ABOGADOS MANUEL RICARDO SANCHEZ & CO.pdf	274	10.8 %
KATEGORIE.pdf	228	8.9 %
PEDIDO DE=?iso-8859-1?Q?COTIZACI=D3N____pdf.zip?=-	212	8.3 %
260124_drawing_update_EN.pptx	143	5.6 %
DHL SHIPPING INVOICE.pdf.zip	134	5.3 %
AWARD PROMOTION.pdf	100	3.9 %
Gewinner 22 - 12 -2023.pdf	75	2.9 %
PARQUET SERVICE LTD REF -05 N- JAN 19.01.2024.7z	64	2.5 %
(AWB) Original BL, PL, CI Copies.shtm	60	2.4 %
(AWB) Original BL,PL,CI Copies.shtm	60	2.4 %
26012024.zip	58	2.3 %
FT0120230524223507530000000000.7z	52	2.0 %
CUSTOMER ADVISORY - RATE RESTORATION - USEC - USGC EFFECTIVE FROM FEBRUARY 12TH 2024.pdf.gz	32	1.3 %
Lotto-Spanien.jpg	28	1.1 %
detaliile bancare.docx	27	1.1 %
29012024.zip	27	1.1 %
More Wastewater sentences w_o answers.docx	26	1.0 %
Pilot Befehl.zip	26	1.0 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTETmJyAyMy5qcGcuahrTbA==?=-	26	1.0 %
PO17276.xlsx	22	0.9 %
Proforma Invoice.zip	22	0.9 %
ORDER ENQUIRY (1).rar	18	0.7 %
51Invoice & shipment docs 2023083411.pdf.html	18	0.7 %
New Order.r00	17	0.7 %
Proof of payment..zip	14	0.5 %
Electronic Invoice_64549934192-2023_JPG.htm	14	0.5 %
=?UTF-8?B?6aG65Liw55S15a2Q5Y+R56WoX1BERi5zaHRtbA==?=-	14	0.5 %
=?UTF-8?B?5Y+R56Wo6L+Q5Y2V5piO57uGX3BkZi5odG1s?=-	14	0.5 %
Electronic Invoice_64549934192-2023 PDF.htm	14	0.5 %
Others	386	15.1 %
Total	2.55k	100 %

Top File Types by Scan Result

Top 10 file types by scan result.



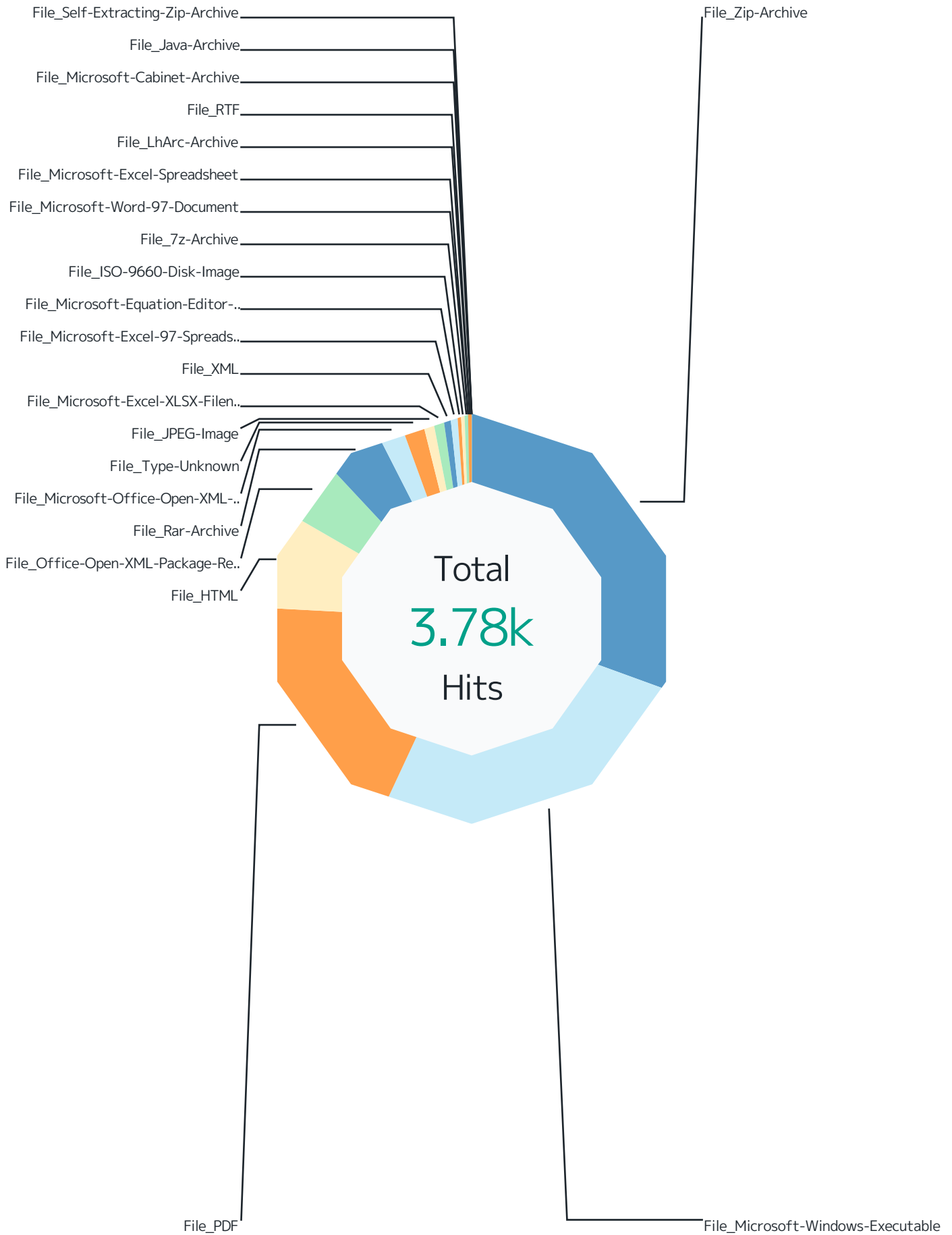
Scan Result	Hits	%
Malicious	1.32k	35.0 %
File_Microsoft-Windows-Executable	945	25.0 %
File_Zip-Archive	154	4.1 %
File_Rar-Archive	97	2.6 %
File_Type-Unknown	33	0.9 %
File_JPEG-Image	28	0.7 %
File_PDF	17	0.5 %
File_Microsoft-Excel-97-Spreadsheet	14	0.4 %
File_Microsoft-Equation-Editor-Document	13	0.3 %
File_Microsoft-Office-Open-XML-Document	7	0.2 %
File_7z-Archive	5	0.1 %
File_Microsoft-Word-97-Document	3	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
File_RTF	2	0.1 %
File_ISO-9660-Disk-Image	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Not Available	987	26.1 %
File_Zip-Archive	933	24.7 %
File_Microsoft-Office-Open-XML-Document	42	1.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	12	0.3 %
Medium Risk	890	23.6 %
File_PDF	605	16.0 %
File_Office-Open-XML-Package-Relations-Item	170	4.5 %
File_Zip-Archive	33	0.9 %
File_XML	26	0.7 %
File_Microsoft-Windows-Executable	25	0.7 %
File_HTML	11	0.3 %
File_Microsoft-Office-Open-XML-Document	7	0.2 %
File_ISO-9660-Disk-Image	5	0.1 %
File_Rar-Archive	3	0.1 %
File_LhArc-Archive	3	0.1 %
File_Type-Unknown	1	0.0 %
File_Microsoft-Word-97-Document	1	0.0 %
High Risk	264	7.0 %
File_PDF	89	2.4 %
File_Rar-Archive	66	1.7 %
File_Type-Unknown	28	0.7 %
File_Zip-Archive	26	0.7 %
File_Microsoft-Windows-Executable	24	0.6 %

Scan Result	Hits	%
File_Microsoft-Office-Open-XML-Document	11	0.3 %
File_Office-Open-XML-Package-Relations-Item	10	0.3 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_ISO-9660-Disk-Image	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
File_Microsoft-Equation-Editor-Document	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
HTML/Phishing.ta	250	6.6 %
File_HTML	250	6.6 %
HTML/Phishing.rb	25	0.7 %
File_HTML	24	0.6 %
File_Type-Unknown	1	0.0 %
Unknown	13	0.3 %
File_Microsoft-Office-Open-XML-Document	7	0.2 %
File_Zip-Archive	6	0.2 %
Exploit-GBT!3C4D4919584E	4	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
HTML/Phishing.zz	2	0.1 %
File_HTML	2	0.1 %
Exploit-GBT!E98788F0D1F7	2	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.1 %
Exploit-GBT!16E8EFF54E06	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
GenericRXSM-NK!9ADF2D6D12C0	2	0.1 %
File_Zip-Archive	2	0.1 %
Exploit-GBT!3AE4A7DCFDB8	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
Exploit-GBT!7BECFEF74C9D	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
JS/Dropper.am	1	0.0 %
File_Zip-Archive	1	0.0 %
PDF/Phish-FBU!3E4E7B804F17	1	0.0 %
File_PDF	1	0.0 %
GenericRXSM-NK!75C1A9A40B35	1	0.0 %
File_Zip-Archive	1	0.0 %
GenericRXWL-SPI!4588AC0322D6	1	0.0 %
File_Zip-Archive	1	0.0 %
Exploit-GBT!FD1F18C9FBF4	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %

Scan Result	Hits	%
Exploit-GDJ!F81B48296B71	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Remcos-FDQO!D7EC95F3BD2B	1	0.0 %
File_Zip-Archive	1	0.0 %
Exploit-GBT!D826B8120A8A	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!9919EAC52850	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Adwind-FEIM.jar!C2CE44CF9E75	1	0.0 %
File_Java-Archive	1	0.0 %
Total	3.78k	100 %

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



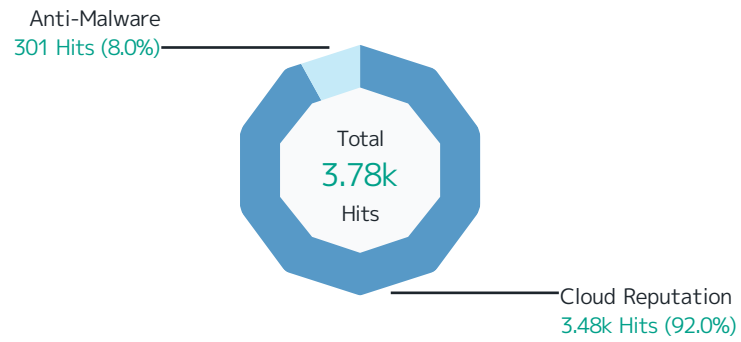
Responding Scanner	Hits	%
File_Zip-Archive	1.16k	30.7 %
Not Available	933	24.7 %
Malicious	154	4.1 %
Medium Risk	33	0.9 %
High Risk	26	0.7 %
Unknown	6	0.2 %
GenericRXSM-NK!9ADF2D6D12C0	2	0.1 %
JS/Dropper.am	1	0.0 %
GenericRXSM-NK!75C1A9A40B35	1	0.0 %
GenericRXWL-SPI4588AC0322D6	1	0.0 %
Remcos-FDQO!D7EC95F3BD2B	1	0.0 %
File_Microsoft-Windows-Executable	994	26.3 %
Malicious	945	25.0 %
Medium Risk	25	0.7 %
High Risk	24	0.6 %
File_PDF	712	18.9 %
Medium Risk	605	16.0 %
High Risk	89	2.4 %
Malicious	17	0.5 %
PDF/Phish-FBU!3E4E7B804F17	1	0.0 %
File_HTML	287	7.6 %
HTML/Phishing.ta	250	6.6 %
HTML/Phishing.rb	24	0.6 %
Medium Risk	11	0.3 %
HTML/Phishing.zz	2	0.1 %
File_Office-Open-XML-Package-Relations-Item	180	4.8 %
Medium Risk	170	4.5 %
High Risk	10	0.3 %
File_Rar-Archive	166	4.4 %
Malicious	97	2.6 %
High Risk	66	1.7 %
Medium Risk	3	0.1 %
File_Microsoft-Office-Open-XML-Document	74	2.0 %
Not Available	42	1.1 %
High Risk	11	0.3 %
Malicious	7	0.2 %
Medium Risk	7	0.2 %
Unknown	7	0.2 %
File_Type-Unknown	63	1.7 %

Responding Scanner	Hits	%
Malicious	33	0.9 %
High Risk	28	0.7 %
Medium Risk	1	0.0 %
HTML/Phishing.rb	1	0.0 %
File_JPEG-Image	28	0.7 %
Malicious	28	0.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	28	0.7 %
Not Available	12	0.3 %
Exploit-GBT!3C4D4919584E	4	0.1 %
Malicious	2	0.1 %
Exploit-GBT!16E8EFF54E06	2	0.1 %
Exploit-GBT!3AE4A7DCFDB8	2	0.1 %
Exploit-GBT!7BECFEF74C9D	2	0.1 %
High Risk	1	0.0 %
Exploit-GBT!FD1F18C9FBF4	1	0.0 %
Exploit-GDJ!F81B48296B71	1	0.0 %
Exploit-GBT!D826B8120A8A	1	0.0 %
File_XML	26	0.7 %
Medium Risk	26	0.7 %
File_Microsoft-Excel-97-Spreadsheet	19	0.5 %
Malicious	14	0.4 %
High Risk	5	0.1 %
File_Microsoft-Equation-Editor-Document	14	0.4 %
Malicious	13	0.3 %
High Risk	1	0.0 %
File_ISO-9660-Disk-Image	8	0.2 %
Medium Risk	5	0.1 %
High Risk	2	0.1 %
Malicious	1	0.0 %
File_7z-Archive	5	0.1 %
Malicious	5	0.1 %
File_Microsoft-Word-97-Document	4	0.1 %
Malicious	3	0.1 %
Medium Risk	1	0.0 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
Exploit-GBT!E98788F0D1F7	2	0.1 %
Exploit-GBT!9919EAC52850	1	0.0 %
File_LhArc-Archive	3	0.1 %
Medium Risk	3	0.1 %

Responding Scanner	Hits	%
File_RTF	2	0.1 %
Malicious	2	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
High Risk	1	0.0 %
File_Java-Archive	1	0.0 %
Adwind-FEIM.jar!C2CE44CF9E75	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Malicious	1	0.0 %
Total	3.78k	100 %

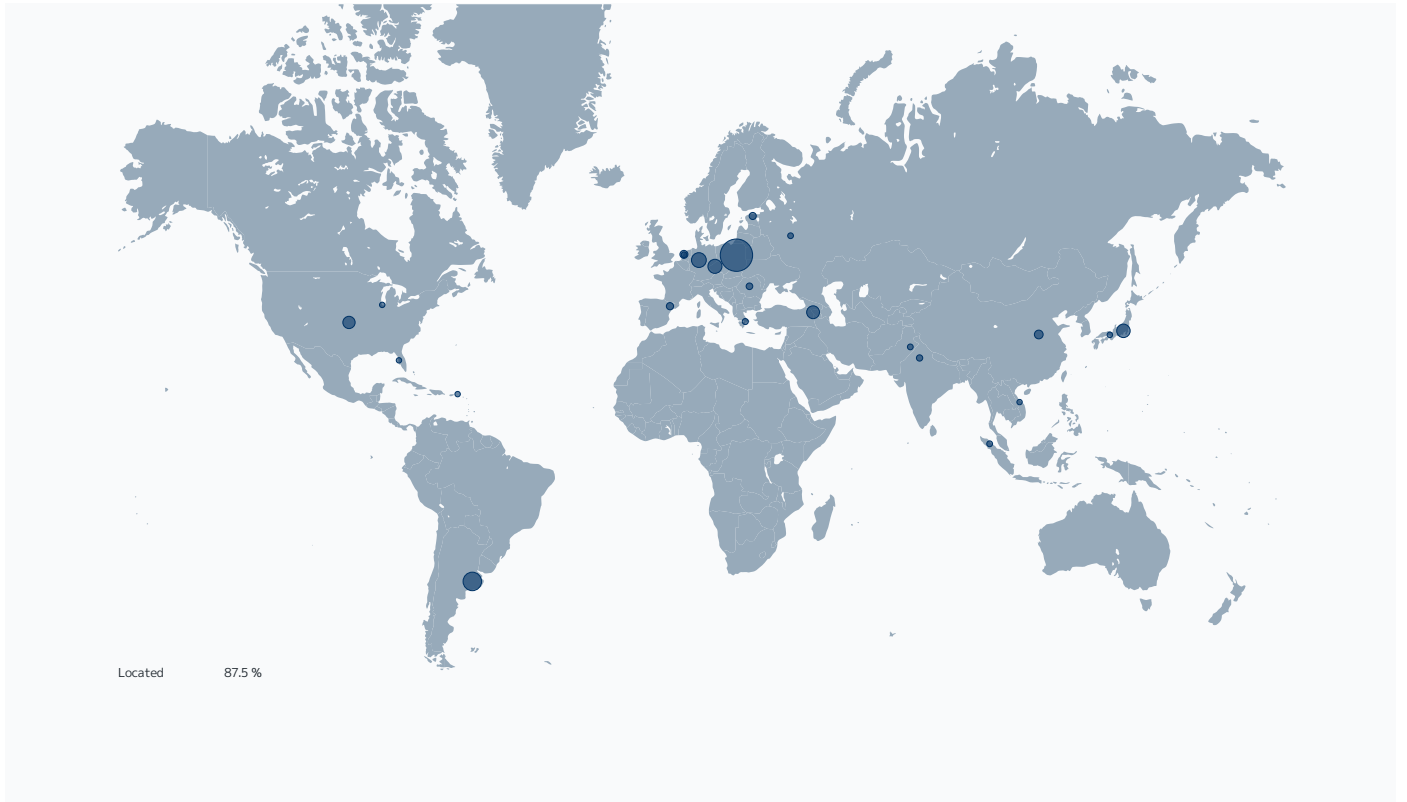
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	3.48k	92.0 %
File_Zip-Archive	1.15k	30.5 %
File_Microsoft-Windows-Executable	994	26.3 %
File_PDF	711	18.8 %
File_Office-Open-XML-Package-Relations-Item	180	4.8 %
File_Rar-Archive	166	4.4 %
File_Microsoft-Office-Open-XML-Document	74	2.0 %
File_Type-Unknown	62	1.6 %
File_JPEG-Image	28	0.7 %
File_XML	26	0.7 %
File_Microsoft-Excel-97-Spreadsheet	19	0.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	15	0.4 %
File_Microsoft-Equation-Editor-Document	14	0.4 %
File_HTML	11	0.3 %
File_ISO-9660-Disk-Image	8	0.2 %
File_7z-Archive	5	0.1 %
File_Microsoft-Word-97-Document	4	0.1 %
File_LhArc-Archive	3	0.1 %
File_RTF	2	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Anti-Malware	301	8.0 %
File_HTML	276	7.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.3 %
File_Zip-Archive	6	0.2 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
File_PDF	1	0.0 %
File_Type-Unknown	1	0.0 %
File_Java-Archive	1	0.0 %
Total	3.78k	100 %

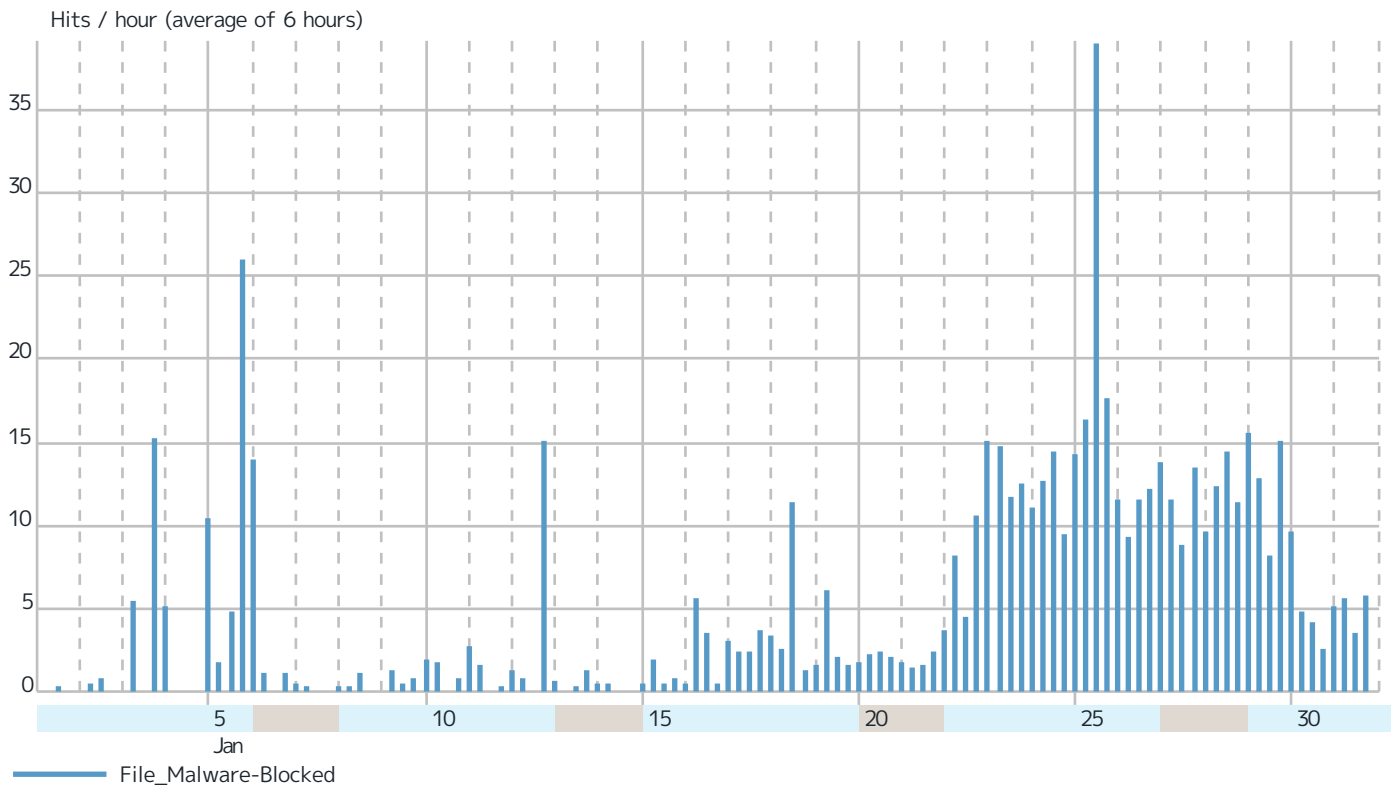
Virenfiterung SRC IPs



Records by src IP		Hits	%
51.77.61.156	 Warsaw, Poland	854	22.6 %
190.18.95.108	 Buenos Aires, Argentina	424	11.2 %
217.160.246.10	 Germany	271	7.2 %
5.63.162.163	 Yerevan, Armenia	248	6.6 %
77.75.78.212	 Czechia	198	5.2 %
203.161.44.102	 United States	153	4.1 %
210.154.211.2	 Japan	150	4.0 %
194.156.99.6	 China	120	3.2 %
210.154.211.4	 Japan	117	3.1 %
185.107.57.12	 The Netherlands	97	2.6 %
77.75.76.212	 Czechia	88	2.3 %
95.130.52.45	 Lleida, Spain	72	1.9 %
194.6.201.66	 Romania	54	1.4 %
8.39.147.105	 United States	52	1.4 %
103.13.242.147	 New Delhi, India	44	1.2 %
176.9.75.164	 Germany	38	1.0 %
46.227.62.50	 Greece	37	1.0 %
202.162.192.29	 Medan, Indonesia	30	0.8 %
202.142.147.195	 Lahore, Pakistan	28	0.7 %
188.127.227.203	 Estonia	28	0.7 %
89.253.237.7	 Russia	27	0.7 %
161.129.65.137	 Amsterdam, The Netherlands	25	0.7 %
162.0.231.123	 United States	25	0.7 %
188.127.235.228	 Estonia	20	0.5 %
188.127.225.221	 Estonia	20	0.5 %
157.7.106.90	 Ōtemae, Japan	19	0.5 %
77.83.199.117	 Chicago, Illinois 60602, United States	17	0.5 %
209.133.200.122	 Tampa, Florida 33614, United States	16	0.4 %
195.242.111.91	 British Virgin Islands	16	0.4 %
103.72.56.23	 Vietnam	16	0.4 %
Others		473	12.5 %
Total		3.78k	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](#).

© 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.