
Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenterung Server Firewall

Report period

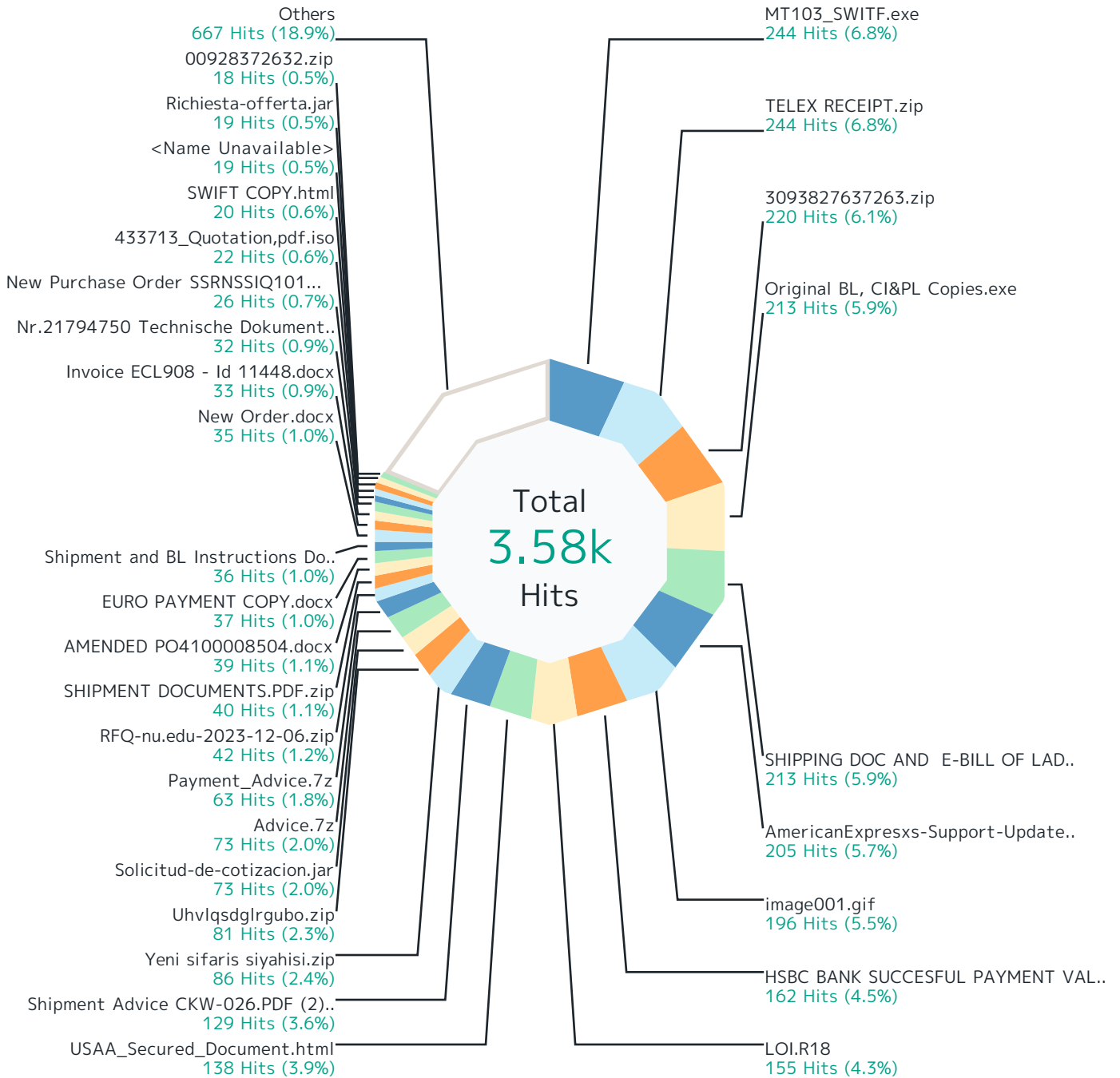
From: 2023-06-01 00:00:00+0200

To: 2023-07-01 00:00:00+0200

Table of Contents

Report run by	Virenfilterung MXe	3
SD-WAN Manager Console version	Top File Types by Scan Result	5
Update version	Top Scan Results by Responding Scanner	10
Report started	Top File Types by Responding Scanner	15
Report run time	Virenfilterung SRC IPs	17
Filters used	SMTP Virus Filtering by Time	19

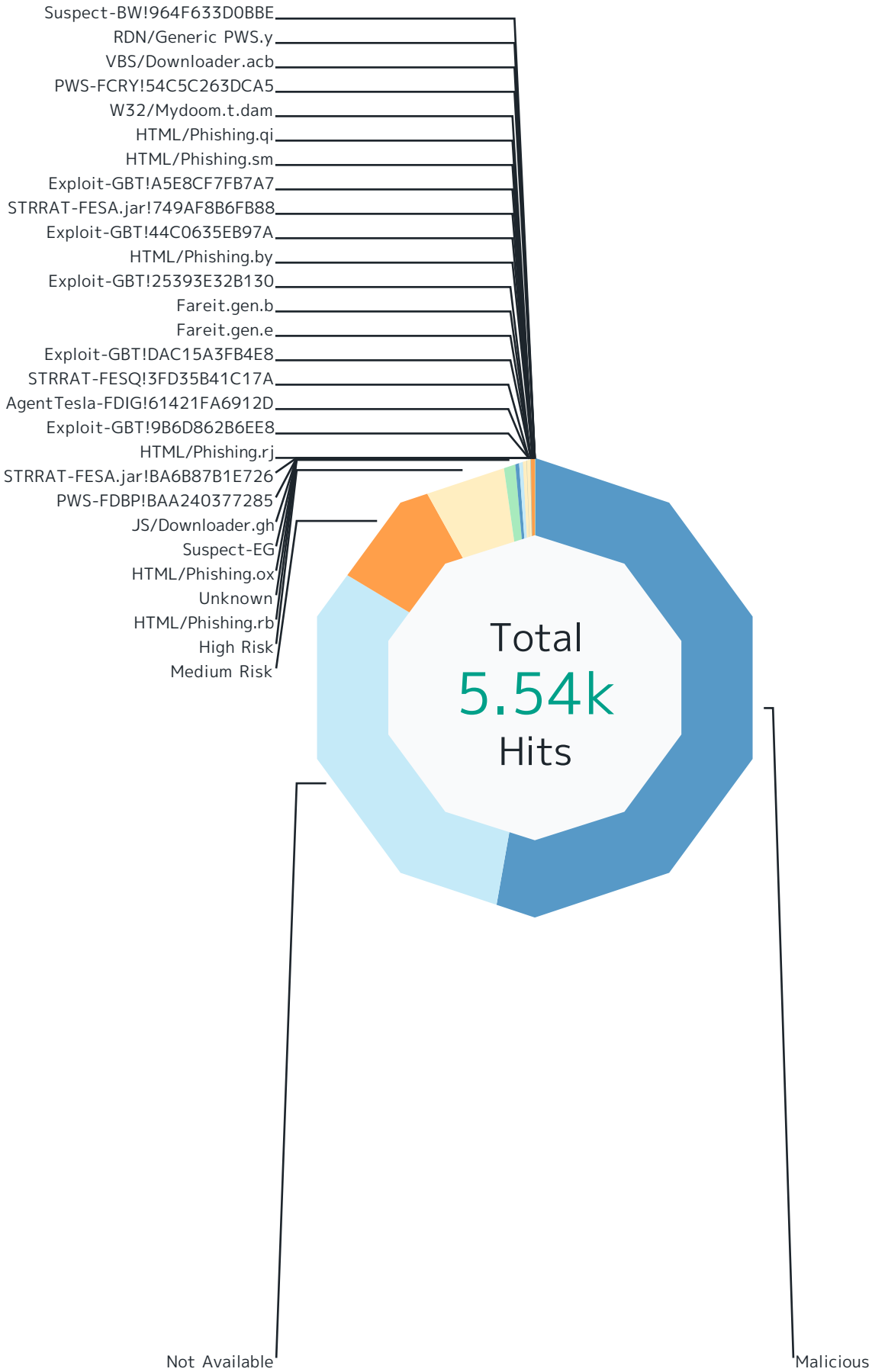
Virenfiterung MXe



Records by file name	Hits	%
MT103_SWITF.exe	244	6.8 %
TELEX RECEIPT.zip	244	6.8 %
3093827637263.zip	220	6.1 %
Original BL, CI&PL Copies.exe	213	5.9 %
SHIPPING DOC AND E-BILL OF LADING..zip	213	5.9 %
AmericanExpresxs-Support-Update.html	205	5.7 %
image001.gif	196	5.5 %
HSBC BANK SUCCESFUL PAYMENT VALUE DATE JUNE 19 2023.pdf.zip	162	4.5 %
LOI.R18	155	4.3 %
USAA_Secured_Document.html	138	3.9 %
Shipment Advice CKW-026.PDF (2).zip	129	3.6 %
Yeni sifaris siyahisi.zip	86	2.4 %
Uhlvqsdglrgubo.zip	81	2.3 %
Solicitud-de-cotizacion.jar	73	2.0 %
Advice.7z	73	2.0 %
Payment_Advice.7z	63	1.8 %
RFQ-nu.edu-2023-12-06.zip	42	1.2 %
SHIPMENT DOCUMENTS.PDF.zip	40	1.1 %
AMENDED PO410008504.docx	39	1.1 %
EURO PAYMENT COPY.docx	37	1.0 %
Shipment and BL Instructions Docs.docx	36	1.0 %
New Order.docx	35	1.0 %
Invoice ECL908 - Id 11448.docx	33	0.9 %
Nr.21794750 Technische Dokumentation.img	32	0.9 %
New Purchase Order SSRNSSIQ101.iso	26	0.7 %
433713_Quotation,pdf.iso	22	0.6 %
SWIFT COPY.html	20	0.6 %
<Name Unavailable>	19	0.5 %
Richiesta-offerta.jar	19	0.5 %
00928372632.zip	18	0.5 %
Others	667	18.6 %
Total	3.58k	100 %

Top File Types by Scan Result

Top 10 file types by scan result.



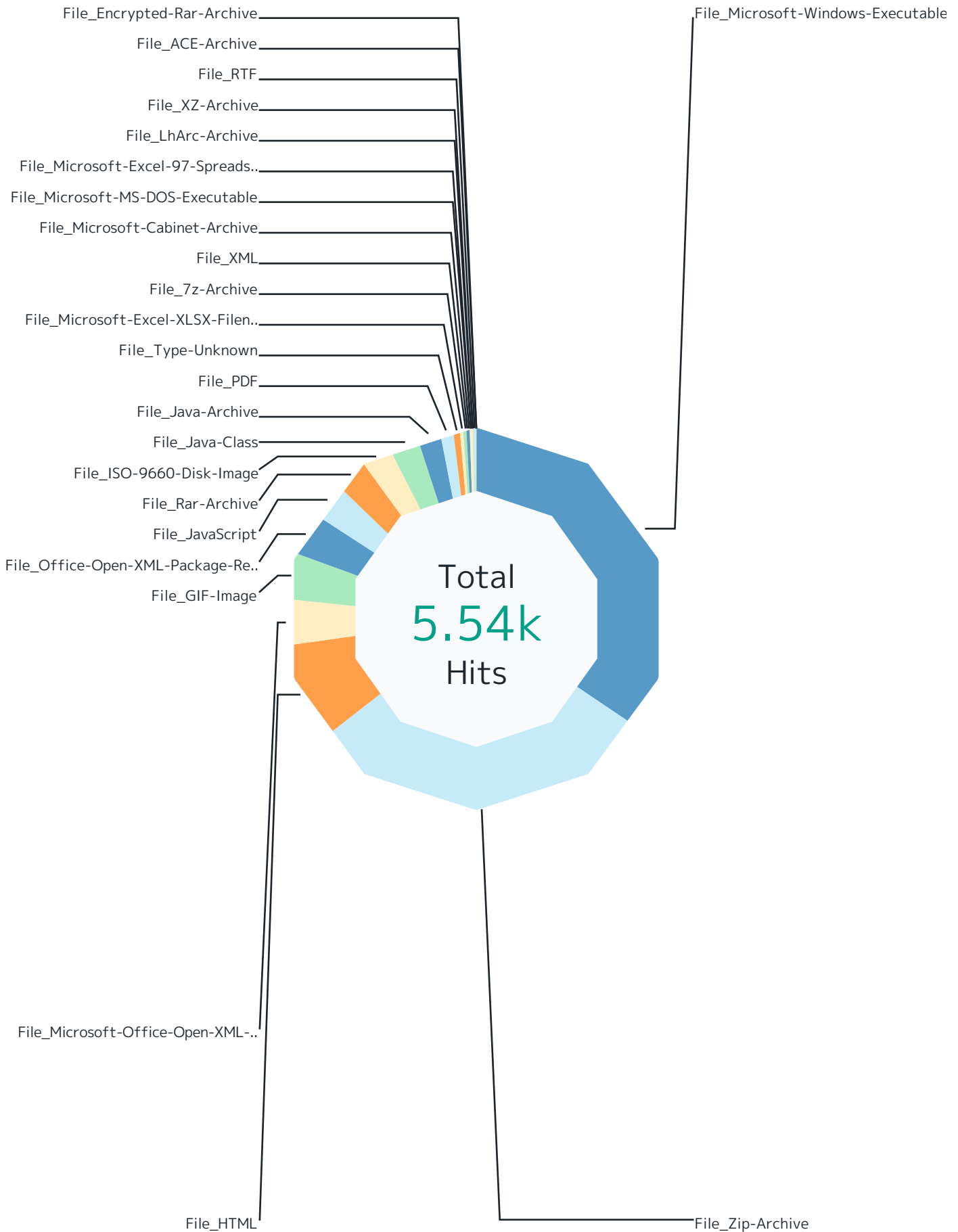
Scan Result	Hits	%
Malicious	2.92k	52.8 %
File_Microsoft-Windows-Executable	1.82k	32.9 %
File_HTML	376	6.8 %
File_Zip-Archive	206	3.7 %
File_Office-Open-XML-Package-Relations-Item	128	2.3 %
File_JavaScript	125	2.3 %
File_Java-Class	99	1.8 %
File_Rar-Archive	81	1.5 %
File_ISO-9660-Disk-Image	30	0.5 %
File_PDF	14	0.3 %
File_Microsoft-Office-Open-XML-Document	7	0.1 %
File_Type-Unknown	7	0.1 %
File_Microsoft-Cabinet-Archive	7	0.1 %
File_Microsoft-MS-DOS-Executable	5	0.1 %
File_XZ-Archive	5	0.1 %
File_Microsoft-Excel-97-Spreadsheet	4	0.1 %
File_7z-Archive	2	0.0 %
File_Encrypted-Rar-Archive	2	0.0 %
Not Available	1.72k	31.0 %
File_Zip-Archive	1.42k	25.6 %
File_Microsoft-Office-Open-XML-Document	197	3.6 %
File_Java-Archive	93	1.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.2 %
Medium Risk	459	8.3 %
File_GIF-Image	207	3.7 %
File_Microsoft-Windows-Executable	51	0.9 %
File_Java-Class	41	0.7 %
File_PDF	36	0.6 %
File_JavaScript	33	0.6 %
File_ISO-9660-Disk-Image	25	0.5 %
File_HTML	15	0.3 %
File_Microsoft-Office-Open-XML-Document	15	0.3 %
File_Rar-Archive	13	0.2 %
File_XML	9	0.2 %
File_LhArc-Archive	5	0.1 %
File_Zip-Archive	3	0.1 %
File_Type-Unknown	3	0.1 %
File_Office-Open-XML-Package-Relations-Item	1	0.0 %
File_7z-Archive	1	0.0 %

Scan Result	Hits	%
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
High Risk	318	5.7 %
File_ISO-9660-Disk-Image	88	1.6 %
File_Office-Open-XML-Package-Relations-Item	76	1.4 %
File_Rar-Archive	44	0.8 %
File_Microsoft-Windows-Executable	36	0.6 %
File_PDF	19	0.3 %
File_HTML	18	0.3 %
File_Zip-Archive	8	0.1 %
File_Microsoft-Office-Open-XML-Document	7	0.1 %
File_JavaScript	7	0.1 %
File_7z-Archive	6	0.1 %
File_RTF	5	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
HTML/Phishing.rb	45	0.8 %
File_HTML	29	0.5 %
File_Type-Unknown	16	0.3 %
Unknown	22	0.4 %
File_Zip-Archive	21	0.4 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
HTML/Phishing.ox	12	0.2 %
File_HTML	12	0.2 %
Suspect-EG	6	0.1 %
File_Zip-Archive	6	0.1 %
JS/Downloader.gh	4	0.1 %
File_JavaScript	4	0.1 %
PWS-FDBP!BAA240377285	4	0.1 %
File_Rar-Archive	4	0.1 %
STRRAT-FESA.jar!BA6B87B1E726	3	0.1 %
File_Java-Archive	3	0.1 %
HTML/Phishing.rj	3	0.1 %
File_JavaScript	3	0.1 %
Exploit-GBT!9B6D862B6EE8	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
AgentTesla-FDIG!61421FA6912D	2	0.0 %
File_7z-Archive	2	0.0 %
STRRAT-FESQ!3FD35B41C17A	2	0.0 %
File_Java-Archive	2	0.0 %
Exploit-GBT!DAC15A3FB4E8	2	0.0 %

Scan Result	Hits	%
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Fareit.gen.e	2	0.0 %
File_ACE-Archive	2	0.0 %
Fareit.gen.b	2	0.0 %
File_ACE-Archive	2	0.0 %
Exploit-GBT!25393E32B130	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
HTML/Phishing.by	2	0.0 %
File_Type-Unknown	2	0.0 %
Exploit-GBT!44C0635EB97A	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
STRRAT-FESA.jar!749AF8B6FB88	1	0.0 %
File_Java-Archive	1	0.0 %
Exploit-GBT!A5E8CF7FB7A7	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
HTML/Phishing.sm	1	0.0 %
File_HTML	1	0.0 %
HTML/Phishing.qi	1	0.0 %
File_HTML	1	0.0 %
W32/Mydoom.t.dam	1	0.0 %
File_Zip-Archive	1	0.0 %
PWS-FCRY!54C5C263DCA5	1	0.0 %
File_Rar-Archive	1	0.0 %
VBS/Downloader.acb	1	0.0 %
File_Rar-Archive	1	0.0 %
RDN/Generic PWS.y	1	0.0 %
File_Rar-Archive	1	0.0 %
Suspect-BW!964F633D0BBE	1	0.0 %
File_Zip-Archive	1	0.0 %
Total	5.54k	100 %

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



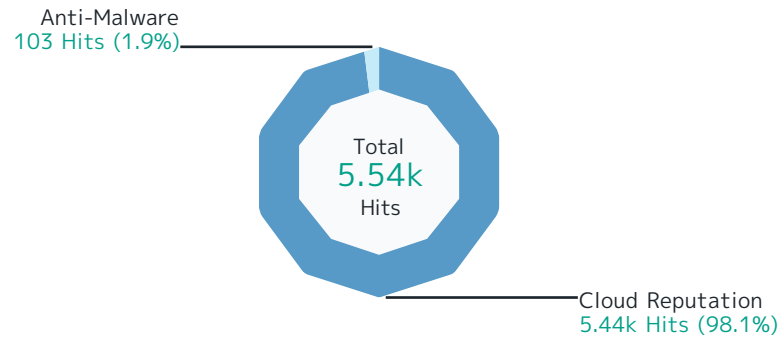
Responding Scanner	Hits	%
File_Microsoft-Windows-Executable	1.91k	34.5 %
Malicious	1.82k	32.9 %
Medium Risk	51	0.9 %
High Risk	36	0.6 %
File_Zip-Archive	1.66k	30.0 %
Not Available	1.42k	25.6 %
Malicious	206	3.7 %
Unknown	21	0.4 %
High Risk	8	0.1 %
Suspect-EG	6	0.1 %
Medium Risk	3	0.1 %
W32/Mydoom.t.dam	1	0.0 %
Suspect-BW!964F633DOBBE	1	0.0 %
File_HTML	452	8.2 %
Malicious	376	6.8 %
HTML/Phishing.rb	29	0.5 %
High Risk	18	0.3 %
Medium Risk	15	0.3 %
HTML/Phishing.ox	12	0.2 %
HTML/Phishing.sm	1	0.0 %
HTML/Phishing.qi	1	0.0 %
File_Microsoft-Office-Open-XML-Document	227	4.1 %
Not Available	197	3.6 %
Medium Risk	15	0.3 %
Malicious	7	0.1 %
High Risk	7	0.1 %
Unknown	1	0.0 %
File_GIF-Image	207	3.7 %
Medium Risk	207	3.7 %
File_Office-Open-XML-Package-Relations-Item	205	3.7 %
Malicious	128	2.3 %
High Risk	76	1.4 %
Medium Risk	1	0.0 %
File_JavaScript	172	3.1 %
Malicious	125	2.3 %
Medium Risk	33	0.6 %
High Risk	7	0.1 %
JS/Downloader.gh	4	0.1 %
HTML/Phishing.rj	3	0.1 %

Responding Scanner	Hits	%
File_Rar-Archive	145	2.6 %
Malicious	81	1.5 %
High Risk	44	0.8 %
Medium Risk	13	0.2 %
PWS-FDBP!BAA240377285	4	0.1 %
PWS-FCRY!54C5C263DCA5	1	0.0 %
VBS/Downloader.acb	1	0.0 %
RDN/Generic PWS.y	1	0.0 %
File_ISO-9660-Disk-Image	143	2.6 %
High Risk	88	1.6 %
Malicious	30	0.5 %
Medium Risk	25	0.5 %
File_Java-Class	140	2.5 %
Malicious	99	1.8 %
Medium Risk	41	0.7 %
File_Java-Archive	99	1.8 %
Not Available	93	1.7 %
STRRAT-FESA.jar!BA6B87B1E726	3	0.1 %
STRRAT-FESQ!3FD35B41C17A	2	0.0 %
STRRAT-FESA.jar!749AF8B6FB88	1	0.0 %
File_PDF	69	1.2 %
Medium Risk	36	0.6 %
High Risk	19	0.3 %
Malicious	14	0.3 %
File_Type-Unknown	28	0.5 %
HTML/Phishing.rb	16	0.3 %
Malicious	7	0.1 %
Medium Risk	3	0.1 %
HTML/Phishing.by	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	21	0.4 %
Not Available	9	0.2 %
High Risk	4	0.1 %
Exploit-GBT!9B6D862B6EE8	2	0.0 %
Exploit-GBT!DAC15A3FB4E8	2	0.0 %
Exploit-GBT!25393E32B130	2	0.0 %
Exploit-GBT!44C0635EB97A	1	0.0 %
Exploit-GBT!A5E8CF7FB7A7	1	0.0 %
File_7z-Archive	11	0.2 %
High Risk	6	0.1 %

Responding Scanner	Hits	%
Malicious	2	0.0 %
AgentTesla-FDIG!61421FA6912D	2	0.0 %
Medium Risk	1	0.0 %
File_XML	9	0.2 %
Medium Risk	9	0.2 %
File_Microsoft-Cabinet-Archive	7	0.1 %
Malicious	7	0.1 %
File_Microsoft-MS-DOS-Executable	5	0.1 %
Malicious	5	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
Malicious	4	0.1 %
Medium Risk	1	0.0 %
File_LhArc-Archive	5	0.1 %
Medium Risk	5	0.1 %
File_XZ-Archive	5	0.1 %
Malicious	5	0.1 %
File_RTF	5	0.1 %
High Risk	5	0.1 %
File_ACE-Archive	4	0.1 %
Fareit.gen.e	2	0.0 %
Fareit.gen.b	2	0.0 %
File_Encrypted-Rar-Archive	2	0.0 %
Malicious	2	0.0 %
Total	5.54k	100 %

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	5.44k	98.1 %
File_Microsoft-Windows-Executable	1.91k	34.5 %
File_Zip-Archive	1.65k	29.9 %
File_HTML	409	7.4 %
File_Microsoft-Office-Open-XML-Document	227	4.1 %
File_GIF-Image	207	3.7 %
File_Office-Open-XML-Package-Relations-Item	205	3.7 %
File_JavaScript	165	3.0 %
File_ISO-9660-Disk-Image	143	2.6 %
File_Java-Class	140	2.5 %
File_Rar-Archive	138	2.5 %
File_Java-Archive	93	1.7 %
File_PDF	69	1.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.2 %
File_Type-Unknown	10	0.2 %
File_7z-Archive	9	0.2 %
File_XML	9	0.2 %
File_Microsoft-Cabinet-Archive	7	0.1 %
File_Microsoft-MS-DOS-Executable	5	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_LhArc-Archive	5	0.1 %
File_XZ-Archive	5	0.1 %
File_RTF	5	0.1 %
File_Encrypted-Rar-Archive	2	0.0 %
Anti-Malware	103	1.9 %
File_HTML	43	0.8 %
File_Type-Unknown	18	0.3 %
File_Zip-Archive	8	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.1 %
File_JavaScript	7	0.1 %
File_Rar-Archive	7	0.1 %
File_Java-Archive	6	0.1 %
File_ACE-Archive	4	0.1 %
File_7z-Archive	2	0.0 %
Total	5.54k	100 %

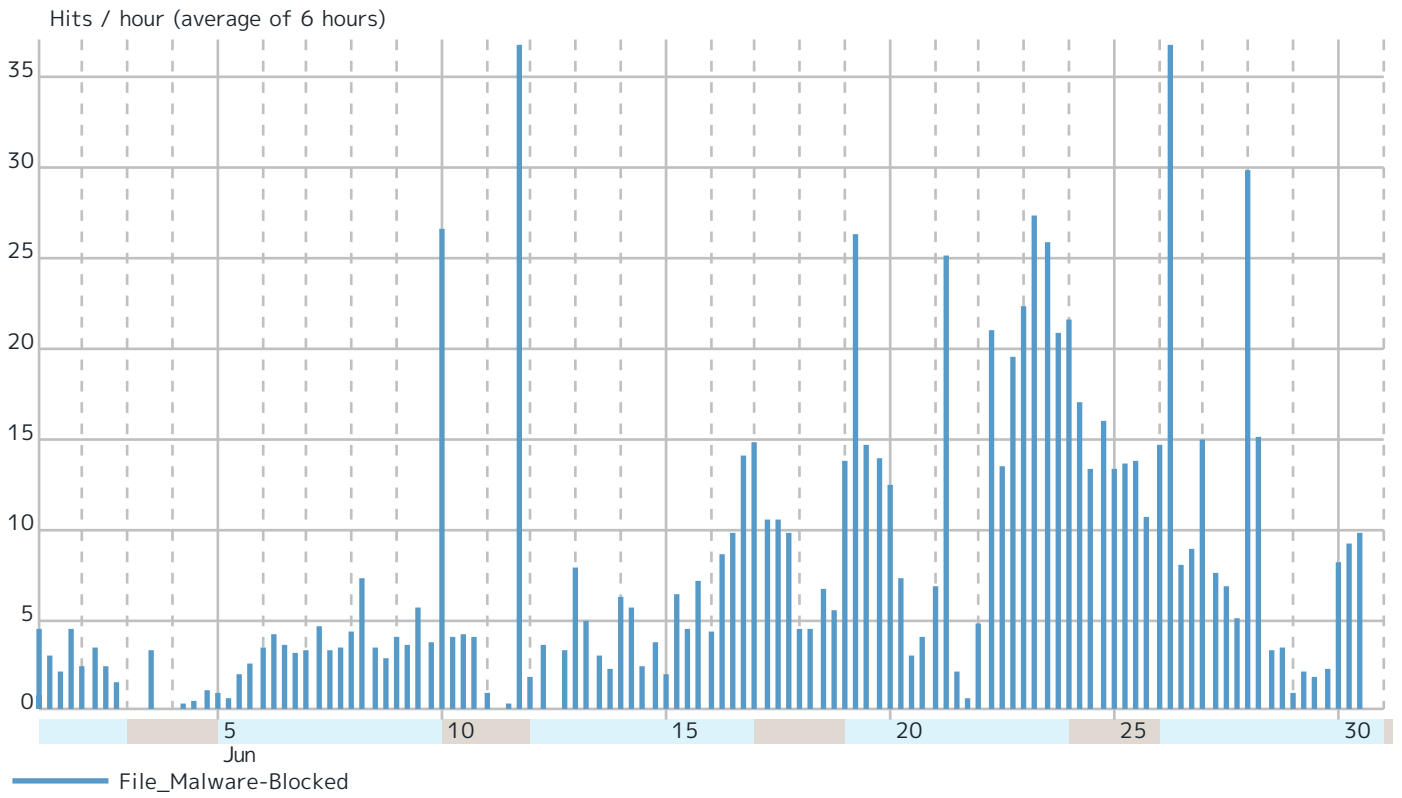
Virenfilterung SRC IPs



Records by src IP		Hits	%
142.11.217.227	 United States	1.39k	25.1 %
185.78.220.84	 Greece	612	11.0 %
46.43.1.242	 United Kingdom	310	5.6 %
95.164.38.102	 Oslo, Norway	272	4.9 %
103.241.147.51	 India	272	4.9 %
135.148.72.234	 Waco, Texas 76708, United States	205	3.7 %
46.27.49.174	 Málaga, Spain	186	3.4 %
185.59.44.224	 Turkey	162	2.9 %
185.101.23.156	 Germany	136	2.5 %
66.175.222.108	 Fremont, California 94536, United States	123	2.2 %
178.63.198.253	 Germany	84	1.5 %
77.75.230.50	 České Budějovice, Czechia	80	1.4 %
51.15.152.247	 Amsterdam, Netherlands	78	1.4 %
89.105.220.85	 New Jersey, United States	74	1.3 %
51.158.41.132	 Paris, France	72	1.3 %
212.129.41.78	 France	70	1.3 %
51.158.27.58	 Paris, France	66	1.2 %
209.160.40.54	 Seattle, Washington 98160, United States	60	1.1 %
80.67.18.53	 Germany	40	0.7 %
80.67.29.31	 Strasbourg, France	38	0.7 %
80.67.18.10	 Germany	36	0.6 %
80.67.29.50	 Strasbourg, France	36	0.6 %
80.67.18.6	 Germany	32	0.6 %
80.67.29.18	 Strasbourg, France	28	0.5 %
103.169.34.151	 Vietnam	26	0.5 %
80.67.18.52	 Germany	26	0.5 %
185.250.237.41	 United Kingdom	24	0.4 %
80.67.18.37	 Germany	24	0.4 %
80.67.18.9	 Germany	24	0.4 %
185.189.236.20	 France	24	0.4 %
Others		926	16.7 %
Total		5.54k	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.