Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-04-01 00:00:00+0200
To: 2024-05-01 00:00:00+0200

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.3, build 11429

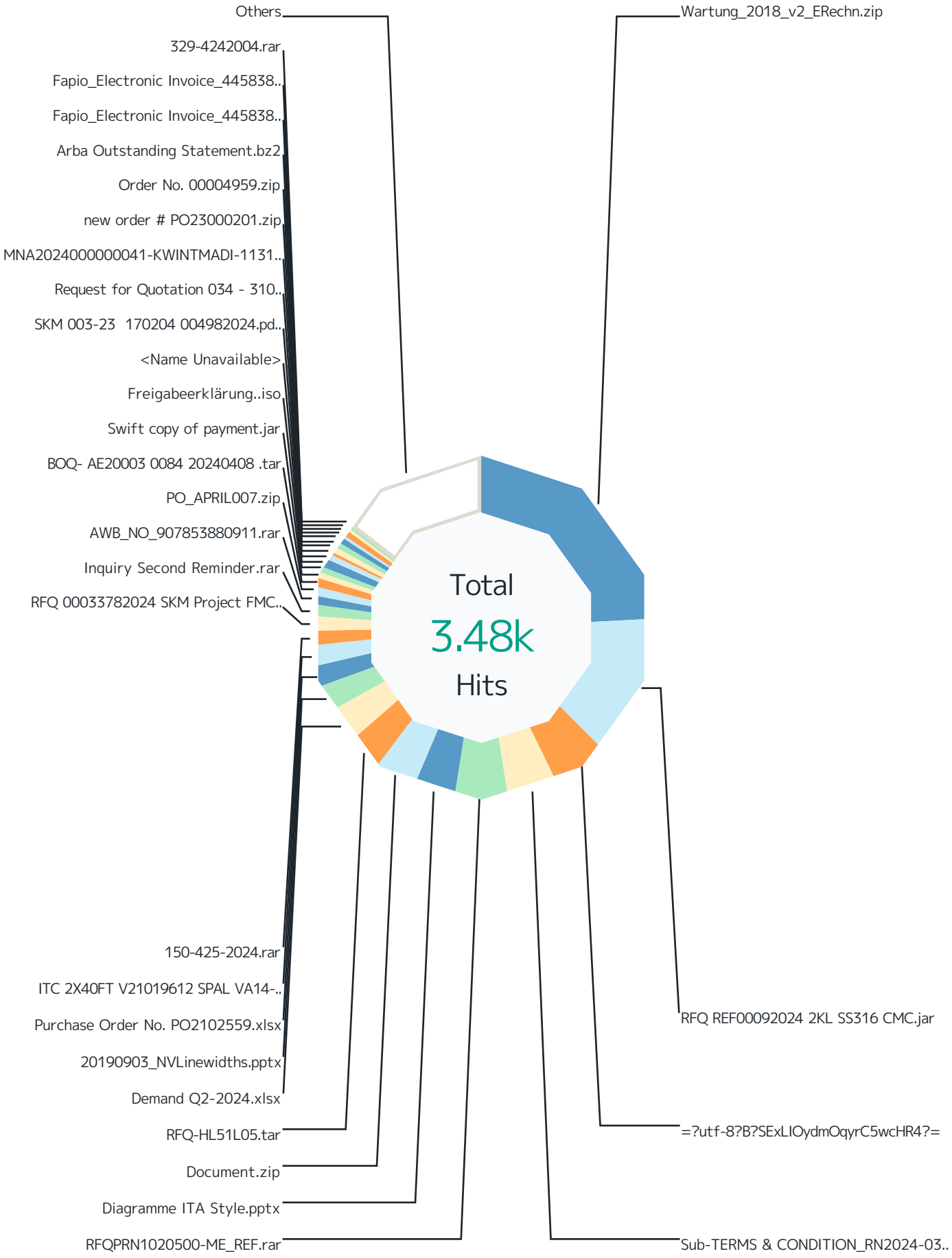
Update version
1720

Report started
2024-05-01 07:55:53+0200

Report run time
02:51:47

Filters used
Match All

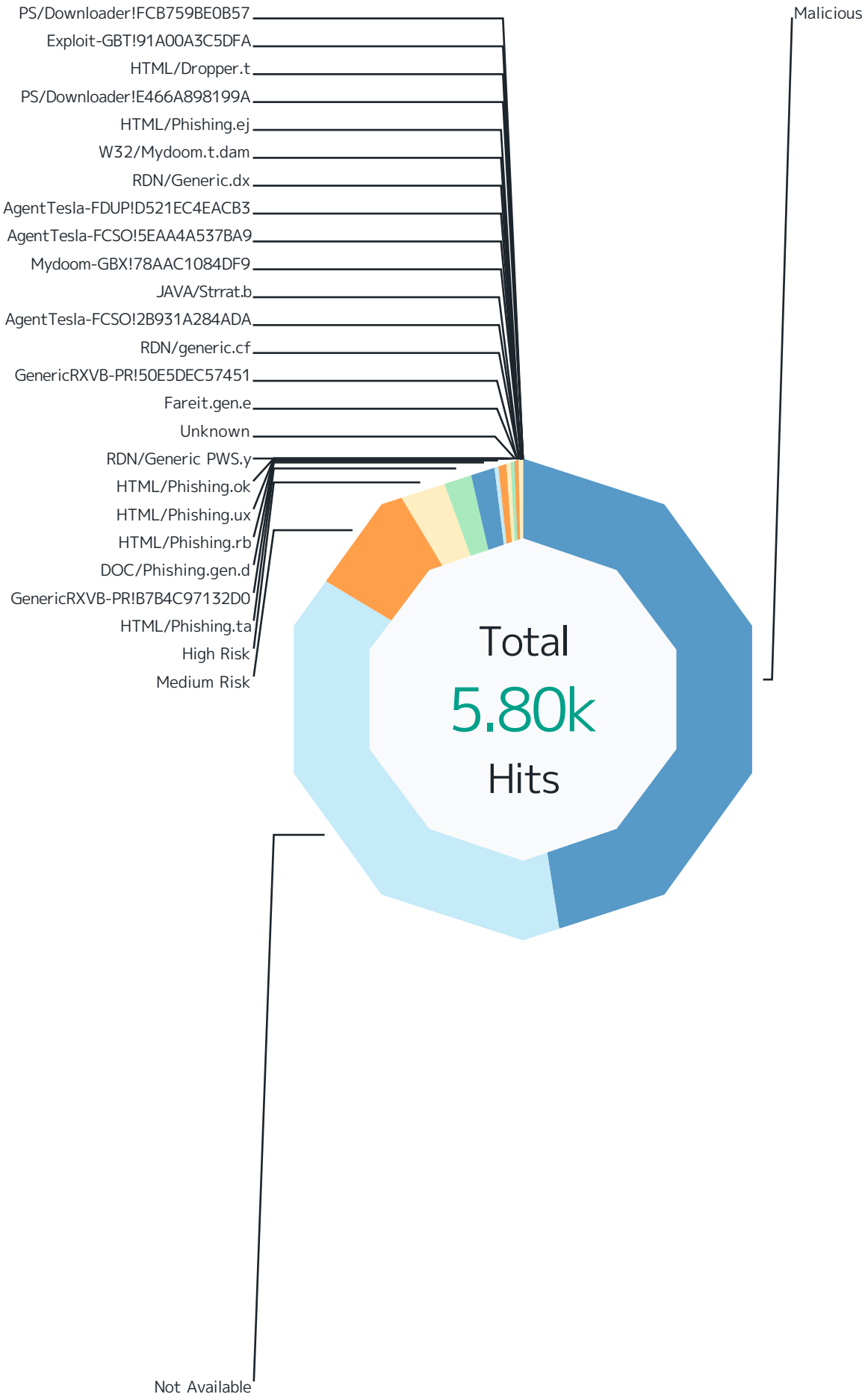
Virenfilterung MXe



Records by file name	Hits	%
Wartung_2018_v2_ERechn.zip	838	24.1 %
RFQ REF00092024 2KL SS316 CMC.jar	465	13.3 %
=?utf-8?B?SExLIOydmOqyrC5wcHR4?=	183	5.3 %
Sub-TERMS & CONDITION_RN2024-0314KP-2ACRPO 134.rar	173	5.0 %
RFQPRN1020500-ME_REF.rar	173	5.0 %
Diagramme ITA Style.pptx	136	3.9 %
Document.zip	128	3.7 %
RFQ-HL51L05.tar	124	3.6 %
Demand Q2-2024.xlsx	108	3.1 %
20190903_NVLinewidths.pptx	93	2.7 %
Purchase Order No. PO2102559.xlsx	67	1.9 %
ITC 2X40FT V21019612 SPAL VA14-BP7C-34GGH.tar	63	1.8 %
150-425-2024.rar	51	1.5 %
RFQ 00033782024 SKM Project FMC.arj	48	1.4 %
Inquiry Second Reminder.rar	38	1.1 %
AWB_NO_907853880911.rar	35	1.0 %
PO_APRIL007.zip	28	0.8 %
BOQ- AE20003 0084 20240408 .tar	28	0.8 %
Swift copy of payment.jar	21	0.6 %
Freigabeerklärung..iso	21	0.6 %
<Name Unavailable>	21	0.6 %
SKM 003-23 170204 004982024.pdf.arj	19	0.5 %
Request for Quotation 034 - 3105.arj	18	0.5 %
MNA2024000000041-KWINTMADI-11310 YÜK.7z	18	0.5 %
new order # PO23000201.zip	16	0.5 %
Order No. 00004959.zip	16	0.5 %
Arba Outstanding Statement.bz2	15	0.4 %
Fapio_Electronic Invoice_44583809_PDF2.shtm	14	0.4 %
Fapio_Electronic Invoice_44583809_PDF.shtm	14	0.4 %
329-4242004.rar	13	0.4 %
Others	499	14.3 %
Total	**3.48k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.


PS/Downloader!FCB759BE0B57
Exploit-GBT!91A00A3C5DFA
HTML/Dropper.t
PS/Downloader!E466A898199A
HTML/Phishing.ej
W32/Mydoom.t.dam
RDN/Generic.dx
AgentTesla-FDUP!D521EC4EACB3
AgentTesla-FCSO!5EAA4A537BA9
Mydoom-GBX!78AAC1084DF9
JAVA/Strrat.b
AgentTesla-FCSO!2B931A284ADA
RDN/generic.cf
GenericRXVB-PR!50E5DEC57451
Fareit.gen.e
Unknown
RDN/Generic PWS.y
HTML/Phishing.ok
HTML/Phishing.ux
HTML/Phishing.rb
DOC/Phishing.gen.d
GenericRXVB-PR!B7B4C97132D0
HTML/Phishing.ta
High Risk
Medium Risk
Malicious
Total
5.80k
Hits
Not Available

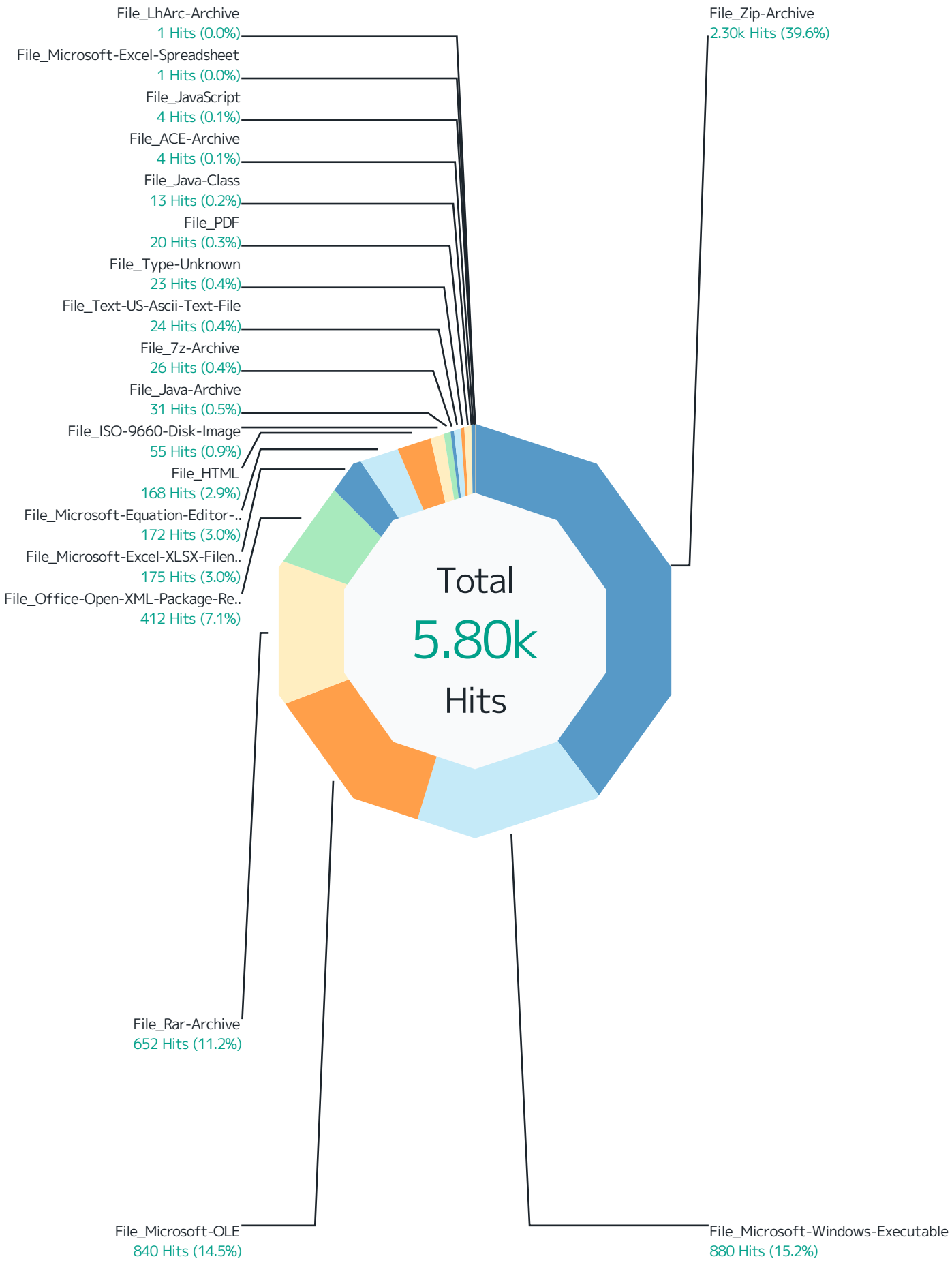
Scan Result	Hits	%
Malicious	**2.75k**	**47.4 %**
File_Microsoft-Windows-Executable	875	15.1 %
File_Microsoft-OLE	840	14.5 %
File_Rar-Archive	638	11.0 %
File_Zip-Archive	241	4.2 %
File_ISO-9660-Disk-Image	54	0.9 %
File_HTML	31	0.5 %
File_7z-Archive	23	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	15	0.3 %
File_Type-Unknown	15	0.3 %
File_PDF	10	0.2 %
File_Java-Archive	7	0.1 %
File_JavaScript	1	0.0 %
File_LhArc-Archive	1	0.0 %
Not Available	**2.10k**	**36.2 %**
File_Zip-Archive	1.93k	33.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	157	2.7 %
File_Java-Archive	13	0.2 %
Medium Risk	**446**	**7.7 %**
File_Office-Open-XML-Package-Relations-Item	412	7.1 %
File_Java-Class	13	0.2 %
File_PDF	6	0.1 %
File_Microsoft-Windows-Executable	4	0.1 %
File_JavaScript	3	0.1 %
File_Zip-Archive	2	0.0 %
File_Rar-Archive	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
File_Java-Archive	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
High Risk	**189**	**3.3 %**
File_Microsoft-Equation-Editor-Document	172	3.0 %
File_Rar-Archive	7	0.1 %
File_Type-Unknown	6	0.1 %
File_7z-Archive	3	0.1 %
File_ISO-9660-Disk-Image	1	0.0 %
HTML/Phishing.ta	**112**	**1.9 %**
File_HTML	110	1.9 %
File_Zip-Archive	2	0.0 %
GenericRXVB-PR!B7B4C97132D0	**92**	**1.6 %**

Scan Result	Hits	%
File_Zip-Archive	92	1.6 %
DOC/Phishing.gen.d	**22**	**0.4 %**
File_Zip-Archive	22	0.4 %
HTML/Phishing.rb	**21**	**0.4 %**
File_HTML	11	0.2 %
File_Text-US-Ascii-Text-File	10	0.2 %
HTML/Phishing.ux	**14**	**0.2 %**
File_Text-US-Ascii-Text-File	14	0.2 %
HTML/Phishing.ok	**14**	**0.2 %**
File_HTML	14	0.2 %
RDN/Generic PWS.y	**8**	**0.1 %**
File_Java-Archive	8	0.1 %
Unknown	**5**	**0.1 %**
File_Zip-Archive	5	0.1 %
Fareit.gen.e	**4**	**0.1 %**
File_ACE-Archive	4	0.1 %
GenericRXVB-PR!50E5DEC57451	**4**	**0.1 %**
File_Zip-Archive	4	0.1 %
RDN/generic.cf	**3**	**0.1 %**
File_PDF	3	0.1 %
AgentTesla-FCSO!2B931A284ADA	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
JAVA/Strrat.b	**2**	**0.0 %**
File_Java-Archive	2	0.0 %
Mydoom-GBX!78AAC1084DF9	**2**	**0.0 %**
File_Zip-Archive	1	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
AgentTesla-FCSO!5EAA4A537BA9	**2**	**0.0 %**
File_Type-Unknown	2	0.0 %
AgentTesla-FDUP!D521EC4EACB3	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
RDN/Generic.dx	**1**	**0.0 %**
File_PDF	1	0.0 %
W32/Mydoom.t.dam	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
HTML/Phishing.ej	**1**	**0.0 %**
File_HTML	1	0.0 %
PS/Downloader!E466A898199A	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %

Scan Result	Hits	%
HTML/Dropper.t	**1**	**0.0 %**
File_HTML	1	0.0 %
Exploit-GBT!91A00A3C5DFA	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
PS/Downloader!FCB759BE0B57	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Total	**5.80k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

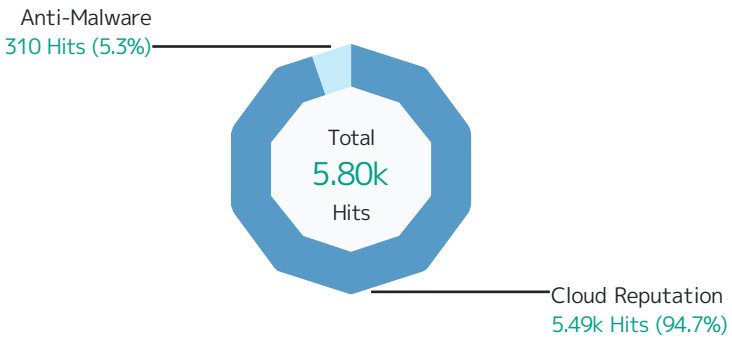

File_LhArc-Archive
1 Hits (0.0%)
File_Microsoft-Excel-Spreadsheet
1 Hits (0.0%)
File_JavaScript
4 Hits (0.1%)
File_ACE-Archive
4 Hits (0.1%)
File_Java-Class
13 Hits (0.2%)
File_PDF
20 Hits (0.3%)
File_Type-Unknown
23 Hits (0.4%)
File_Text-US-Ascii-Text-File
24 Hits (0.4%)
File_7z-Archive
26 Hits (0.4%)
File_Java-Archive
31 Hits (0.5%)
File_ISO-9660-Disk-Image
55 Hits (0.9%)
File_HTML
168 Hits (2.9%)
File_Microsoft-Equation-Editor-..
172 Hits (3.0%)
File_Microsoft-Excel-XLSX-Filen..
175 Hits (3.0%)
File_Office-Open-XML-Package-Re..
412 Hits (7.1%)
Total
5.80k
Hits
File_Zip-Archive
2.30k Hits (39.6%)
File_Rar-Archive
652 Hits (11.2%)
File_Microsoft-OLE
840 Hits (14.5%)
File_Microsoft-Windows-Executable
880 Hits (15.2%)

Responding Scanner	Hits	%
File_Zip-Archive	**2.30k**	**39.6 %**
Not Available	1.93k	33.3 %
Malicious	241	4.2 %
GenericRXVB-PR!B7B4C97132D0	92	1.6 %
DOC/Phishing.gen.d	22	0.4 %
Unknown	5	0.1 %
GenericRXVB-PR!50E5DEC57451	4	0.1 %
Medium Risk	2	0.0 %
HTML/Phishing.ta	2	0.0 %
Mydoom-GBX!78AAC1084DF9	1	0.0 %
W32/Mydoom.t.dam	1	0.0 %
File_Microsoft-Windows-Executable	**880**	**15.2 %**
Malicious	875	15.1 %
Medium Risk	4	0.1 %
Mydoom-GBX!78AAC1084DF9	1	0.0 %
File_Microsoft-OLE	**840**	**14.5 %**
Malicious	840	14.5 %
File_Rar-Archive	**652**	**11.2 %**
Malicious	638	11.0 %
High Risk	7	0.1 %
Medium Risk	2	0.0 %
AgentTesla-FCSO!2B931A284ADA	2	0.0 %
AgentTesla-FDUP!D521EC4EACB3	1	0.0 %
PS/Downloader!E466A898199A	1	0.0 %
PS/Downloader!FCB759BE0B57	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**412**	**7.1 %**
Medium Risk	412	7.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**175**	**3.0 %**
Not Available	157	2.7 %
Malicious	15	0.3 %
Medium Risk	2	0.0 %
Exploit-GBT!91A00A3C5DFA	1	0.0 %
File_Microsoft-Equation-Editor-Document	**172**	**3.0 %**
High Risk	172	3.0 %
File_HTML	**168**	**2.9 %**
HTML/Phishing.ta	110	1.9 %
Malicious	31	0.5 %
HTML/Phishing.ok	14	0.2 %
HTML/Phishing.rb	11	0.2 %

Responding Scanner	Hits	%
HTML/Phishing.ej	1	0.0 %
HTML/Dropper.t	1	0.0 %
File_ISO-9660-Disk-Image	**55**	**0.9 %**
Malicious	54	0.9 %
High Risk	1	0.0 %
File_Java-Archive	**31**	**0.5 %**
Not Available	13	0.2 %
RDN/Generic PWS.y	8	0.1 %
Malicious	7	0.1 %
JAVA/Strrat.b	2	0.0 %
Medium Risk	1	0.0 %
File_7z-Archive	**26**	**0.4 %**
Malicious	23	0.4 %
High Risk	3	0.1 %
File_Text-US-Ascii-Text-File	**24**	**0.4 %**
HTML/Phishing.ux	14	0.2 %
HTML/Phishing.rb	10	0.2 %
File_Type-Unknown	**23**	**0.4 %**
Malicious	15	0.3 %
High Risk	6	0.1 %
AgentTesla-FCSO!5EAA4A537BA9	2	0.0 %
File_PDF	**20**	**0.3 %**
Malicious	10	0.2 %
Medium Risk	6	0.1 %
RDN/generic.cf	3	0.1 %
RDN/Generic.dx	1	0.0 %
File_Java-Class	**13**	**0.2 %**
Medium Risk	13	0.2 %
File_ACE-Archive	**4**	**0.1 %**
Fareit.gen.e	4	0.1 %
File_JavaScript	**4**	**0.1 %**
Medium Risk	3	0.1 %
Malicious	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.0 %**
Medium Risk	1	0.0 %
File_LhArc-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**5.80k**	**100 %**

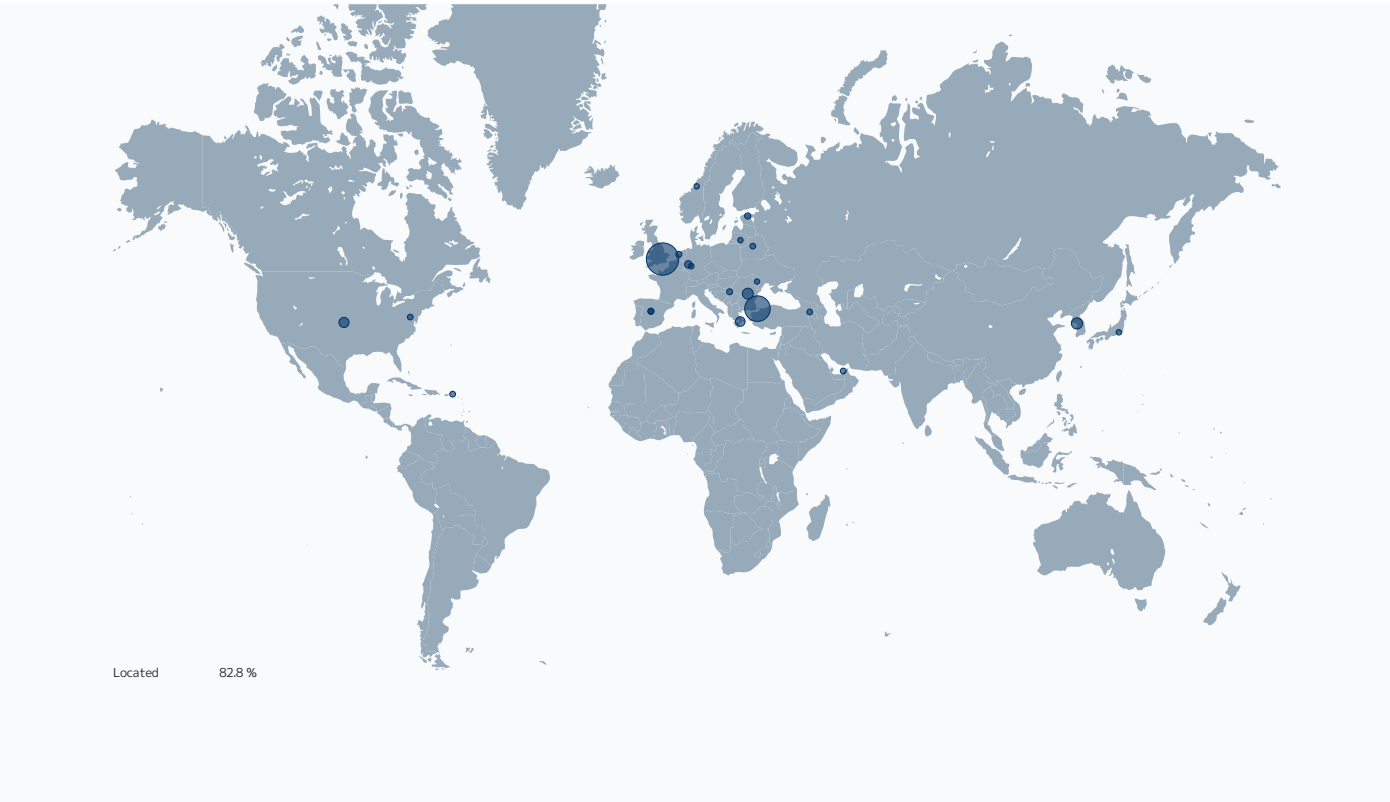
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**5.49k**	**94.7 %**
File_Zip-Archive	2.18k	37.5 %
File_Microsoft-Windows-Executable	879	15.2 %
File_Microsoft-OLE	840	14.5 %
File_Rar-Archive	647	11.2 %
File_Office-Open-XML-Package-Relations-Item	412	7.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	174	3.0 %
File_Microsoft-Equation-Editor-Document	172	3.0 %
File_ISO-9660-Disk-Image	55	0.9 %
File_HTML	31	0.5 %
File_7z-Archive	26	0.4 %
File_Java-Archive	21	0.4 %
File_Type-Unknown	21	0.4 %
File_PDF	16	0.3 %
File_Java-Class	13	0.2 %
File_JavaScript	4	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_LhArc-Archive	1	0.0 %
Anti-Malware	**310**	**5.3 %**
File_HTML	137	2.4 %
File_Zip-Archive	122	2.1 %
File_Text-US-Ascii-Text-File	24	0.4 %
File_Java-Archive	10	0.2 %
File_Rar-Archive	5	0.1 %
File_PDF	4	0.1 %
File_ACE-Archive	4	0.1 %
File_Type-Unknown	2	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Total	**5.80k**	**100 %**

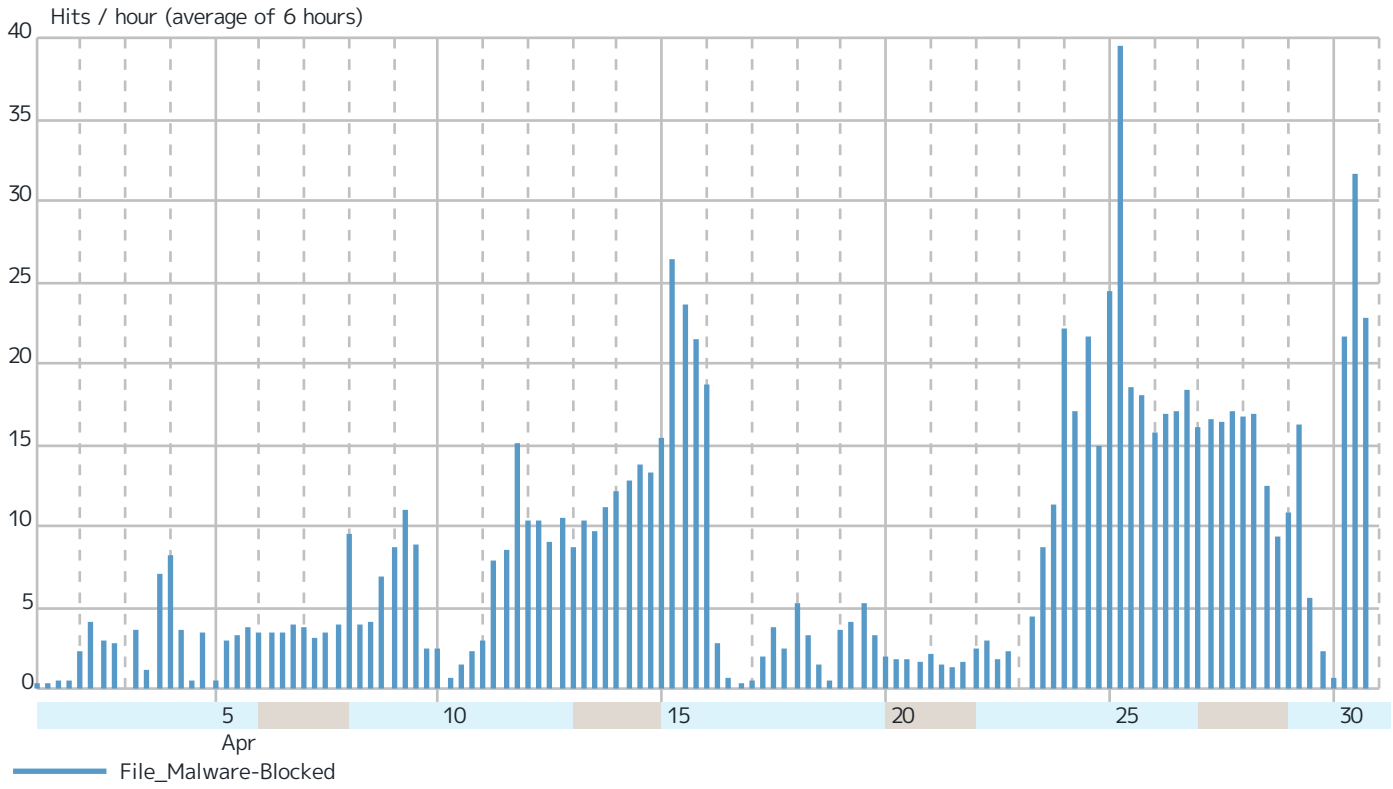
Virenfilterung SRC IPs



Records by src IP		Hits	%
185.132.180.221	United Kingdom	1.68k	28.9 %
217.116.200.14	Türkiye	1.21k	20.9 %
175.207.74.105	South Korea	366	6.3 %
82.117.255.103	Bucharest, Romania	346	6.0 %
46.227.62.50	Greece	267	4.6 %
173.249.147.74	United States	213	3.7 %
62.146.106.25	Dernbach, Germany	134	2.3 %
188.127.230.246	Estonia	58	1.0 %
85.95.240.145	Türkiye	46	0.8 %
109.111.252.76	Serbia	43	0.7 %
31.192.236.45	Madrid, Spain	38	0.7 %
217.113.3.238	Armenia	36	0.6 %
162.240.17.229	United States	35	0.6 %
5.44.42.145	Dubai, United Arab Emirates	35	0.6 %
51.81.91.105	United States	34	0.6 %
185.222.57.134	Amsterdam, The Netherlands	32	0.6 %
79.141.163.159	Ashburn, Virginia 20149, United States	32	0.6 %
194.158.218.217	Minsk, Belarus	30	0.5 %
195.242.110.21	British Virgin Islands	30	0.5 %
5.175.40.29	Spain	21	0.4 %
95.181.161.26	Frankfurt am Main, Germany	18	0.3 %
72.11.157.136	Amsterdam, The Netherlands	18	0.3 %
31.24.158.28	Spain	14	0.2 %
209.85.210.176	United States	12	0.2 %
109.70.35.10	Spain	12	0.2 %
213.226.176.101	Raudondvaris, Lithuania	12	0.2 %
129.241.56.178	Trondheim, Norway	10	0.2 %
61.199.234.210	Higashichuo, Japan	10	0.2 %
209.85.210.170	United States	8	0.1 %
176.123.3.155	Chisinau, Moldova	8	0.1 %
Others		996	17.2 %
Total		**5.80k**	**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.