
Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenterung Server Firewall

Report period

From: 2024-07-01 00:00:00+0200

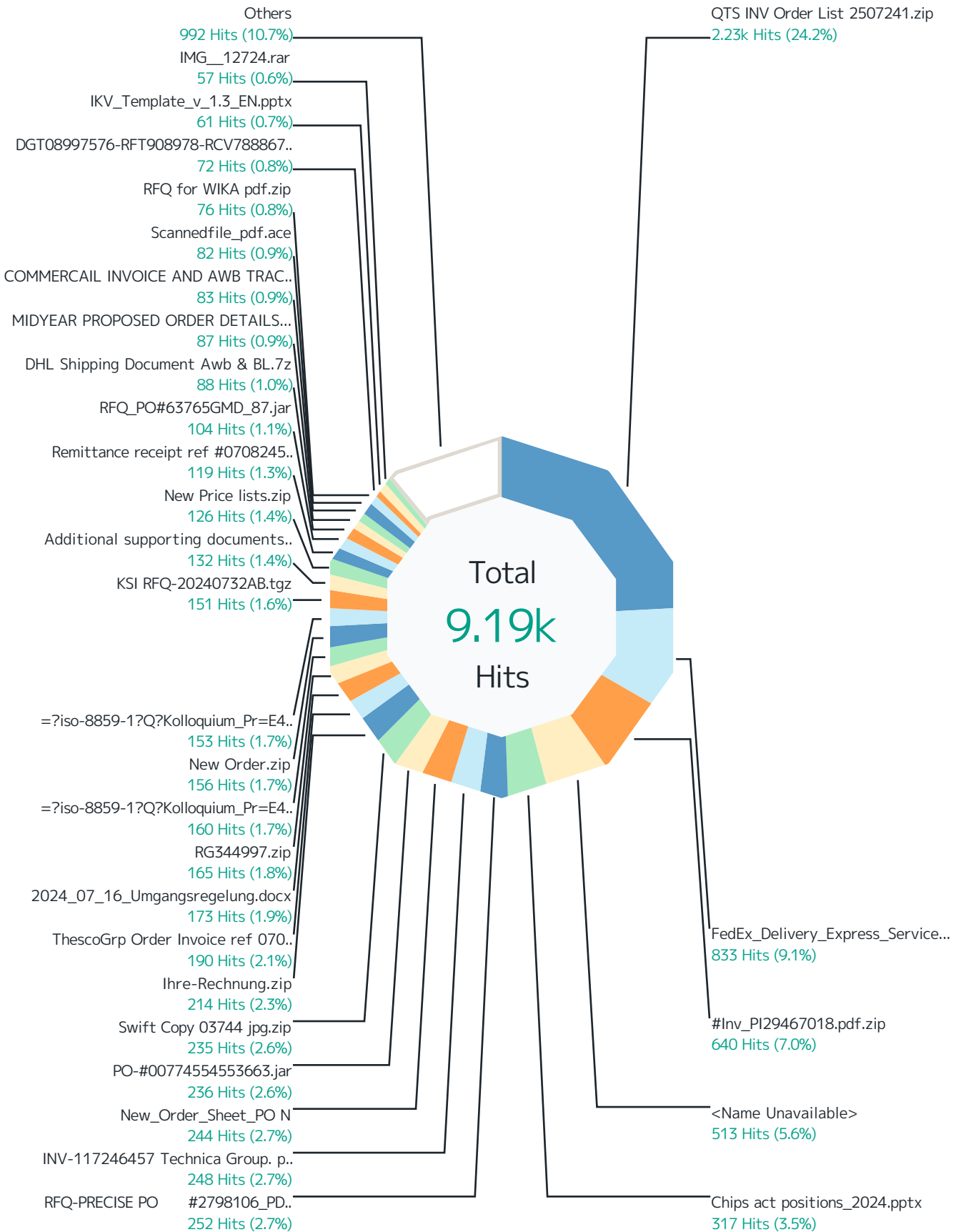
To: 2024-08-01 00:00:00+0200

Forcepoint

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

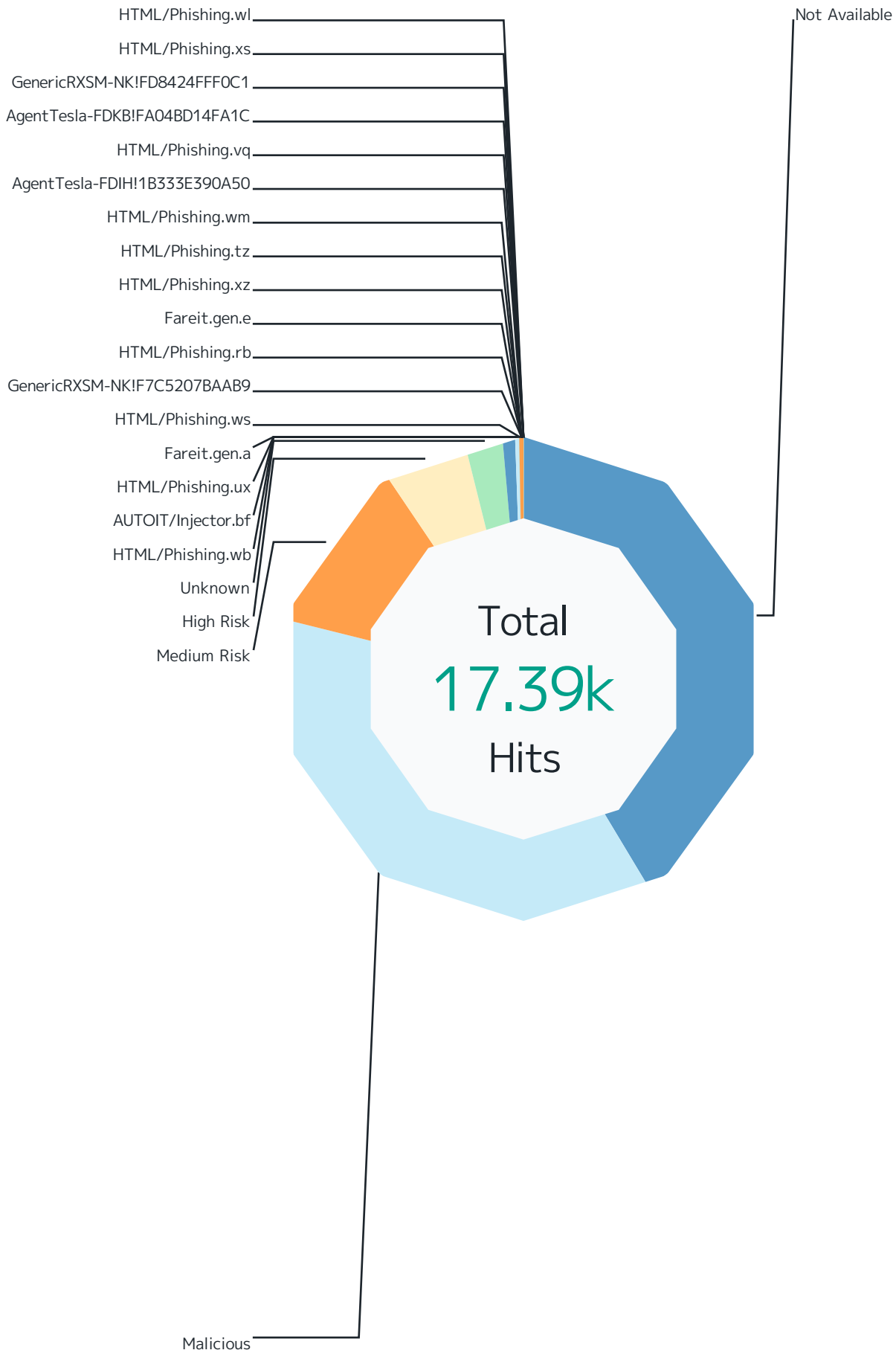
Virenfiterung MXe



Records by file name	Hits	%
QTS INV Order List 2507241.zip	2.23k	24.2 %
FedEx_Delivery_Express_Service.docx	833	9.1 %
#Inv_PI29467018.pdf.zip	640	7.0 %
<Name Unavailable>	513	5.6 %
Chips act positions_2024.pptx	317	3.5 %
RFQ-PRECISE PO #2798106_PDF.lzh	252	2.7 %
INV-117246457 Technica Group. pdf.zip	248	2.7 %
New_Order_Sheet_PO N	244	2.7 %
PO-#00774554553663.jar	236	2.6 %
Swift Copy 03744 .jpg.zip	235	2.6 %
Ihre-Rechnung.zip	214	2.3 %
ThescoGrp Order Invoice ref 07042467.zip	190	2.1 %
2024_07_16_Umgangsregelung.docx	173	1.9 %
RG344997.zip	165	1.8 %
=?iso-8859-1?Q?Kolloquium_Pr=E4sentation_2.0.pptx?=>	160	1.7 %
New Order.zip	156	1.7 %
=?iso-8859-1?Q?Kolloquium_Pr=E4sentation_2.1.pptx?=>	153	1.7 %
KSI RFQ-20240732AB.tgz	151	1.6 %
Additional supporting documents_461489615.z	132	1.4 %
New Price lists.zip	126	1.4 %
Remittance receipt ref #0708245467654.zip	119	1.3 %
RFQ_PO#63765GMD_87.jar	104	1.1 %
DHL Shipping Document Awb & BL.7z	88	1.0 %
MIDYEAR PROPOSED ORDER DETAILS..tar.zip	87	0.9 %
COMMERCAIL INVOICE AND AWB TRACKING DETAILS.PDF.zip	83	0.9 %
Scannedfile_pdf.ace	82	0.9 %
RFQ for WIKA pdf.zip	76	0.8 %
DGT08997576-RFT908978-RCV78886777.ARJ	72	0.8 %
IKV_Template_v_1.3_EN.pptx	61	0.7 %
IMG__12724.rar	57	0.6 %
Others	992	10.8 %
Total	9.19k	100 %

Top File Types by Scan Result

Top 10 file types by scan result.



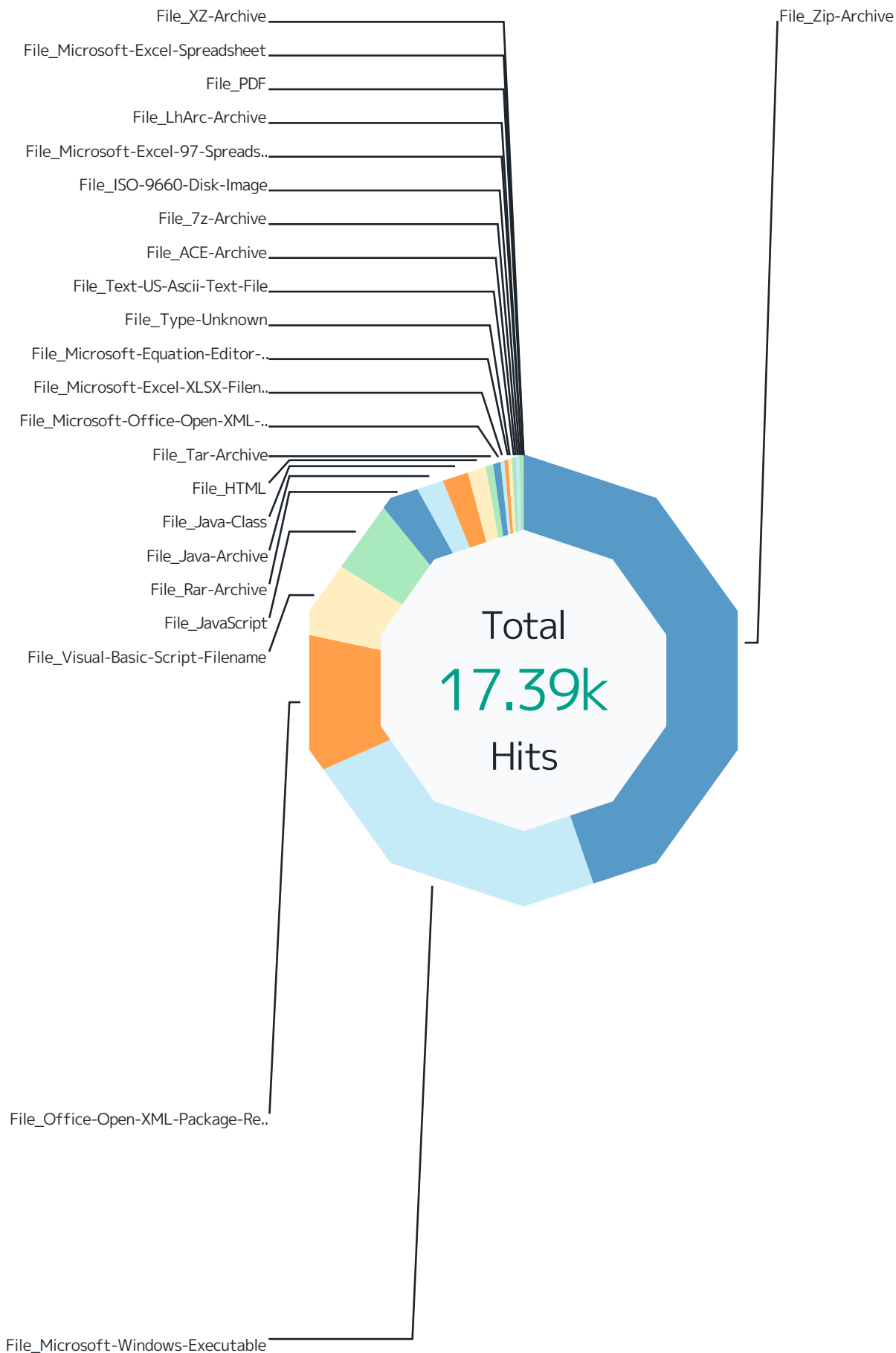
Scan Result	Hits	%
Not Available	7.21k	41.5 %
File_Zip-Archive	6.79k	39.1 %
File_Java-Archive	325	1.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	49	0.3 %
File_Microsoft-Office-Open-XML-Document	45	0.3 %
Malicious	6.49k	37.3 %
File_Microsoft-Windows-Executable	3.97k	22.8 %
File_Visual-Basic-Script-Filename	938	5.4 %
File_Zip-Archive	539	3.1 %
File_Rar-Archive	482	2.8 %
File_Java-Class	132	0.8 %
File_JavaScript	105	0.6 %
File_Tar-Archive	105	0.6 %
File_HTML	68	0.4 %
File_Type-Unknown	37	0.2 %
File_7z-Archive	19	0.1 %
File_Microsoft-Office-Open-XML-Document	17	0.1 %
File_Java-Archive	15	0.1 %
File_Microsoft-Excel-97-Spreadsheet	15	0.1 %
File_LhArc-Archive	14	0.1 %
File_ISO-9660-Disk-Image	11	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.1 %
File_ACE-Archive	7	0.0 %
File_PDF	7	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_XZ-Archive	1	0.0 %
Medium Risk	2.02k	11.6 %
File_Office-Open-XML-Package-Relations-Item	876	5.0 %
File_JavaScript	779	4.5 %
File_Microsoft-Windows-Executable	172	1.0 %
File_Java-Class	127	0.7 %
File_Visual-Basic-Script-Filename	37	0.2 %
File_Text-US-Ascii-Text-File	14	0.1 %
File_HTML	6	0.0 %
File_Zip-Archive	4	0.0 %
File_Type-Unknown	4	0.0 %
File_PDF	3	0.0 %
File_Java-Archive	1	0.0 %
High Risk	993	5.7 %

Scan Result	Hits	%
File_Office-Open-XML-Package-Relations-Item	846	4.9 %
File_Java-Class	81	0.5 %
File_Microsoft-Equation-Editor-Document	46	0.3 %
File_Zip-Archive	6	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.0 %
File_Rar-Archive	4	0.0 %
File_Type-Unknown	3	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
Unknown	439	2.5 %
File_Zip-Archive	425	2.4 %
File_Microsoft-Office-Open-XML-Document	14	0.1 %
HTML/Phishing.wb	133	0.8 %
File_HTML	133	0.8 %
AUTOIT/Injector.bf	30	0.2 %
File_Rar-Archive	30	0.2 %
HTML/Phishing.ux	17	0.1 %
File_Text-US-Ascii-Text-File	17	0.1 %
Fareit.gen.a	10	0.1 %
File_ACE-Archive	10	0.1 %
HTML/Phishing.ws	7	0.0 %
File_HTML	7	0.0 %
GenericRXSM-NK!F7C5207BAAB9	6	0.0 %
File_ISO-9660-Disk-Image	6	0.0 %
HTML/Phishing.rb	5	0.0 %
File_Text-US-Ascii-Text-File	3	0.0 %
File_HTML	2	0.0 %
Fareit.gen.e	5	0.0 %
File_ACE-Archive	5	0.0 %
HTML/Phishing.xz	4	0.0 %
File_HTML	4	0.0 %
HTML/Phishing.tz	3	0.0 %
File_HTML	3	0.0 %
HTML/Phishing.wm	3	0.0 %
File_HTML	3	0.0 %
AgentTesla-FDIH!1B333E390A50	3	0.0 %
File_Rar-Archive	3	0.0 %
HTML/Phishing.vq	2	0.0 %
File_HTML	2	0.0 %

Scan Result	Hits	%
AgentTesla-FDKB!FA04BD14FA1C	2	0.0%
File_ISO-9660-Disk-Image	2	0.0%
GenericRXSM-NK!FD8424FFF0C1	1	0.0%
File_Rar-Archive	1	0.0%
HTML/Phishing.xs	1	0.0%
File_HTML	1	0.0%
HTML/Phishing.wl	1	0.0%
File_HTML	1	0.0%
Total	17.39k	100%

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



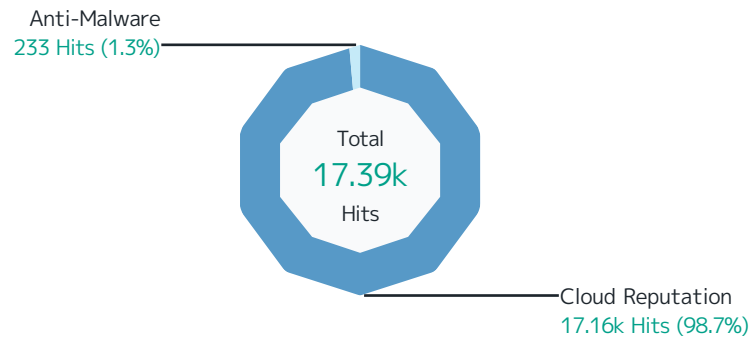
Responding Scanner	Hits	%
File_Zip-Archive	7.77k	44.7 %
Not Available	6.79k	39.1 %
Malicious	539	3.1 %
Unknown	425	2.4 %
High Risk	6	0.0 %
Medium Risk	4	0.0 %
File_Microsoft-Windows-Executable	4.14k	23.8 %
Malicious	3.97k	22.8 %
Medium Risk	172	1.0 %
High Risk	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	1.72k	9.9 %
Medium Risk	876	5.0 %
High Risk	846	4.9 %
File_Visual-Basic-Script-Filename	975	5.6 %
Malicious	938	5.4 %
Medium Risk	37	0.2 %
File_JavaScript	884	5.1 %
Medium Risk	779	4.5 %
Malicious	105	0.6 %
File_Rar-Archive	520	3.0 %
Malicious	482	2.8 %
AUTOIT/Injector.bf	30	0.2 %
High Risk	4	0.0 %
AgentTesla-FDIH!1B333E390A50	3	0.0 %
GenericRXSM-NK!FD8424FFFOC1	1	0.0 %
File_Java-Archive	341	2.0 %
Not Available	325	1.9 %
Malicious	15	0.1 %
Medium Risk	1	0.0 %
File_Java-Class	340	2.0 %
Malicious	132	0.8 %
Medium Risk	127	0.7 %
High Risk	81	0.5 %
File_HTML	230	1.3 %
HTML/Phishing.wb	133	0.8 %
Malicious	68	0.4 %
HTML/Phishing.ws	7	0.0 %
Medium Risk	6	0.0 %
HTML/Phishing.xz	4	0.0 %

Responding Scanner	Hits	%
HTML/Phishing.tz	3	0.0 %
HTML/Phishing.wm	3	0.0 %
HTML/Phishing.rb	2	0.0 %
HTML/Phishing.vq	2	0.0 %
HTML/Phishing.xs	1	0.0 %
HTML/Phishing.wl	1	0.0 %
File_Tar-Archive	105	0.6 %
Malicious	105	0.6 %
File_Microsoft-Office-Open-XML-Document	76	0.4 %
Not Available	45	0.3 %
Malicious	17	0.1 %
Unknown	14	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	64	0.4 %
Not Available	49	0.3 %
Malicious	10	0.1 %
High Risk	5	0.0 %
File_Microsoft-Equation-Editor-Document	46	0.3 %
High Risk	46	0.3 %
File_Type-Unknown	44	0.3 %
Malicious	37	0.2 %
Medium Risk	4	0.0 %
High Risk	3	0.0 %
File_Text-US-Ascii-Text-File	34	0.2 %
HTML/Phishing.ux	17	0.1 %
Medium Risk	14	0.1 %
HTML/Phishing.rb	3	0.0 %
File_ACE-Archive	22	0.1 %
Fareit.gen.a	10	0.1 %
Malicious	7	0.0 %
Fareit.gen.e	5	0.0 %
File_7z-Archive	19	0.1 %
Malicious	19	0.1 %
File_ISO-9660-Disk-Image	19	0.1 %
Malicious	11	0.1 %
GenericRXSM-NK!F7C5207BAAB9	6	0.0 %
AgentTesla-FDKB!FA04BD14FA1C	2	0.0 %
File_Microsoft-Excel-97-Spreadsheet	16	0.1 %
Malicious	15	0.1 %
High Risk	1	0.0 %

Responding Scanner	Hits	%
File_LhArc-Archive	14	0.1 %
Malicious	14	0.1 %
File_PDF	10	0.1 %
Malicious	7	0.0 %
Medium Risk	3	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Malicious	1	0.0 %
File_XZ-Archive	1	0.0 %
Malicious	1	0.0 %
Total	17.39k	100 %

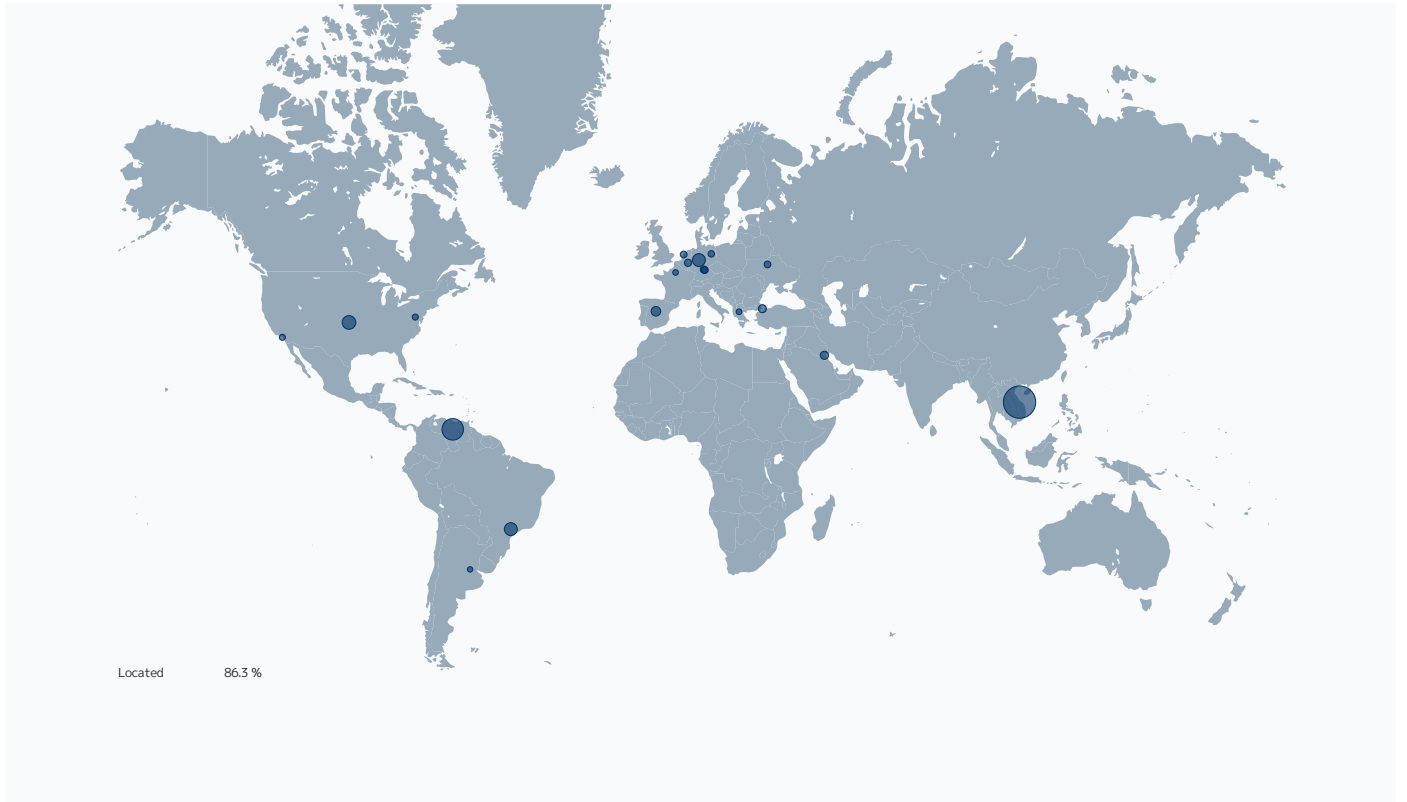
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	17.16k	98.7 %
File_Zip-Archive	7.77k	44.7 %
File_Microsoft-Windows-Executable	4.14k	23.8 %
File_Office-Open-XML-Package-Relations-Item	1.72k	9.9 %
File_Visual-Basic-Script-Filename	975	5.6 %
File_JavaScript	884	5.1 %
File_Rar-Archive	486	2.8 %
File_Java-Archive	341	2.0 %
File_Java-Class	340	2.0 %
File_Tar-Archive	105	0.6 %
File_Microsoft-Office-Open-XML-Document	76	0.4 %
File_HTML	74	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	64	0.4 %
File_Microsoft-Equation-Editor-Document	46	0.3 %
File_Type-Unknown	44	0.3 %
File_7z-Archive	19	0.1 %
File_Microsoft-Excel-97-Spreadsheet	16	0.1 %
File_Text-US-Ascii-Text-File	14	0.1 %
File_LhArc-Archive	14	0.1 %
File_ISO-9660-Disk-Image	11	0.1 %
File_PDF	10	0.1 %
File_ACE-Archive	7	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_XZ-Archive	1	0.0 %
Anti-Malware	233	1.3 %
File_HTML	156	0.9 %
File_Rar-Archive	34	0.2 %
File_Text-US-Ascii-Text-File	20	0.1 %
File_ACE-Archive	15	0.1 %
File_ISO-9660-Disk-Image	8	0.0 %
Total	17.39k	100 %

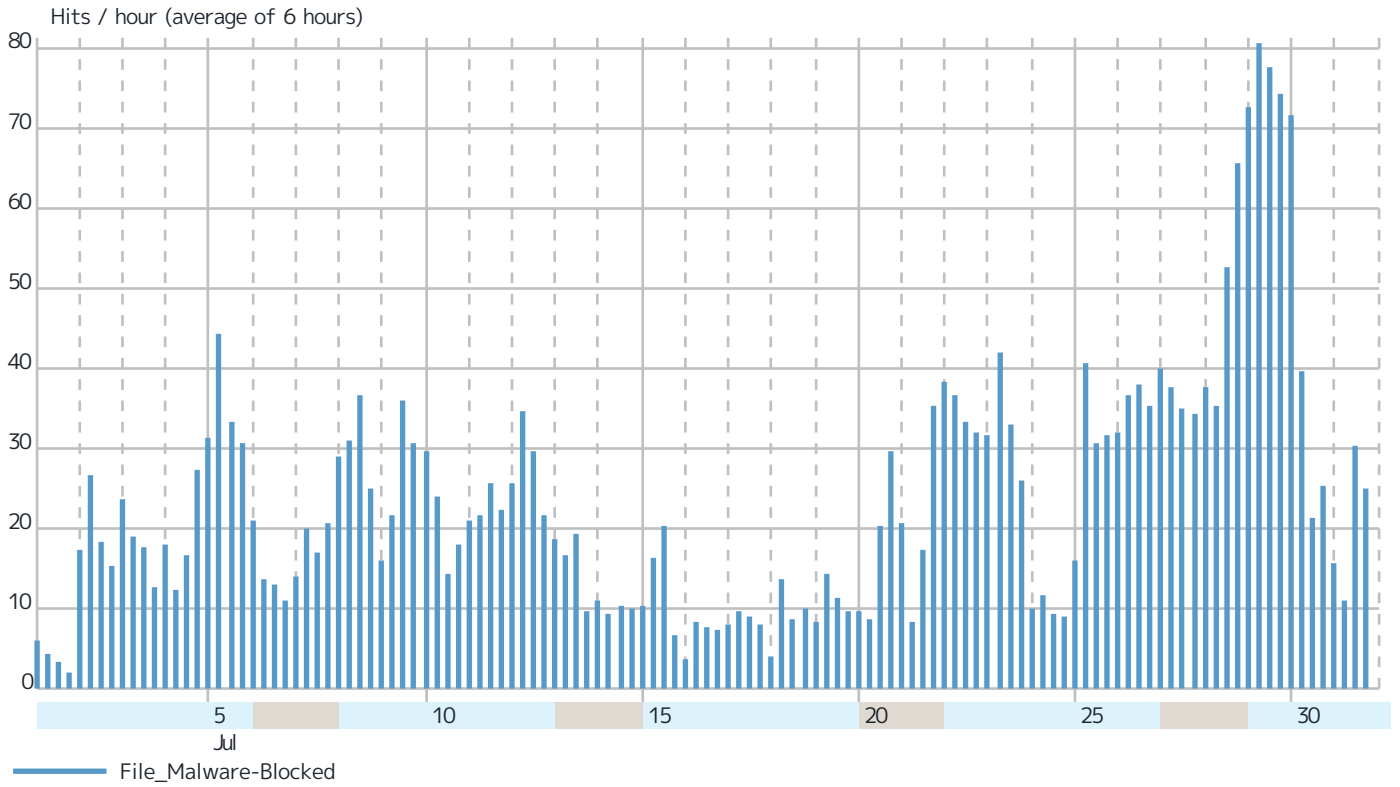
Virenfiterung SRC IPs



Records by src IP		Hits	%
45.117.79.99	Vietnam	4.45k	25.6 %
201.249.199.174	Venezuela	1.48k	8.5 %
170.233.83.8	Ribeirao Bonito, Brazil	1.28k	7.4 %
190.202.40.82	Venezuela	1.19k	6.9 %
82.165.122.100	Germany	606	3.5 %
212.227.162.72	Spain	564	3.2 %
168.187.5.210	Kuwait City, Kuwait	504	2.9 %
104.168.132.254	United States	488	2.8 %
81.169.162.214	Germany	482	2.8 %
77.92.100.50	Istanbul, Türkiye	472	2.7 %
192.236.192.226	United States	470	2.7 %
91.102.136.170	Aachen, Germany	346	2.0 %
185.244.194.184	Nuremberg, Germany	326	1.9 %
23.254.203.241	United States	264	1.5 %
168.119.146.79	Berlin, Germany	213	1.2 %
185.253.218.55	Ukraine	208	1.2 %
95.97.77.154	Amsterdam, The Netherlands	206	1.2 %
142.11.196.133	United States	176	1.0 %
81.25.126.158	Spain	166	1.0 %
74.48.81.74	Los Angeles, California 90060, United States	151	0.9 %
62.146.106.23	Burgthann, Germany	150	0.9 %
23.21.224.96	Ashburn, Virginia 20149, United States	145	0.8 %
62.146.106.26	Burgthann, Germany	136	0.8 %
194.97.9.200	Germany	92	0.5 %
46.227.62.50	Kozani, Greece	92	0.5 %
194.97.9.201	Germany	90	0.5 %
51.38.176.216	France	82	0.5 %
195.191.169.226	Ukraine	58	0.3 %
64.188.22.67	Amsterdam, The Netherlands	56	0.3 %
179.43.122.78	Rosario, Argentina	45	0.3 %
Others		2.39k	13.7 %
Total		17.39k	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.