Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2025-02-01 00:00:00+0100
To: 2025-03-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

Secure SD-WAN Manager Console version
7.2.3, build 11587

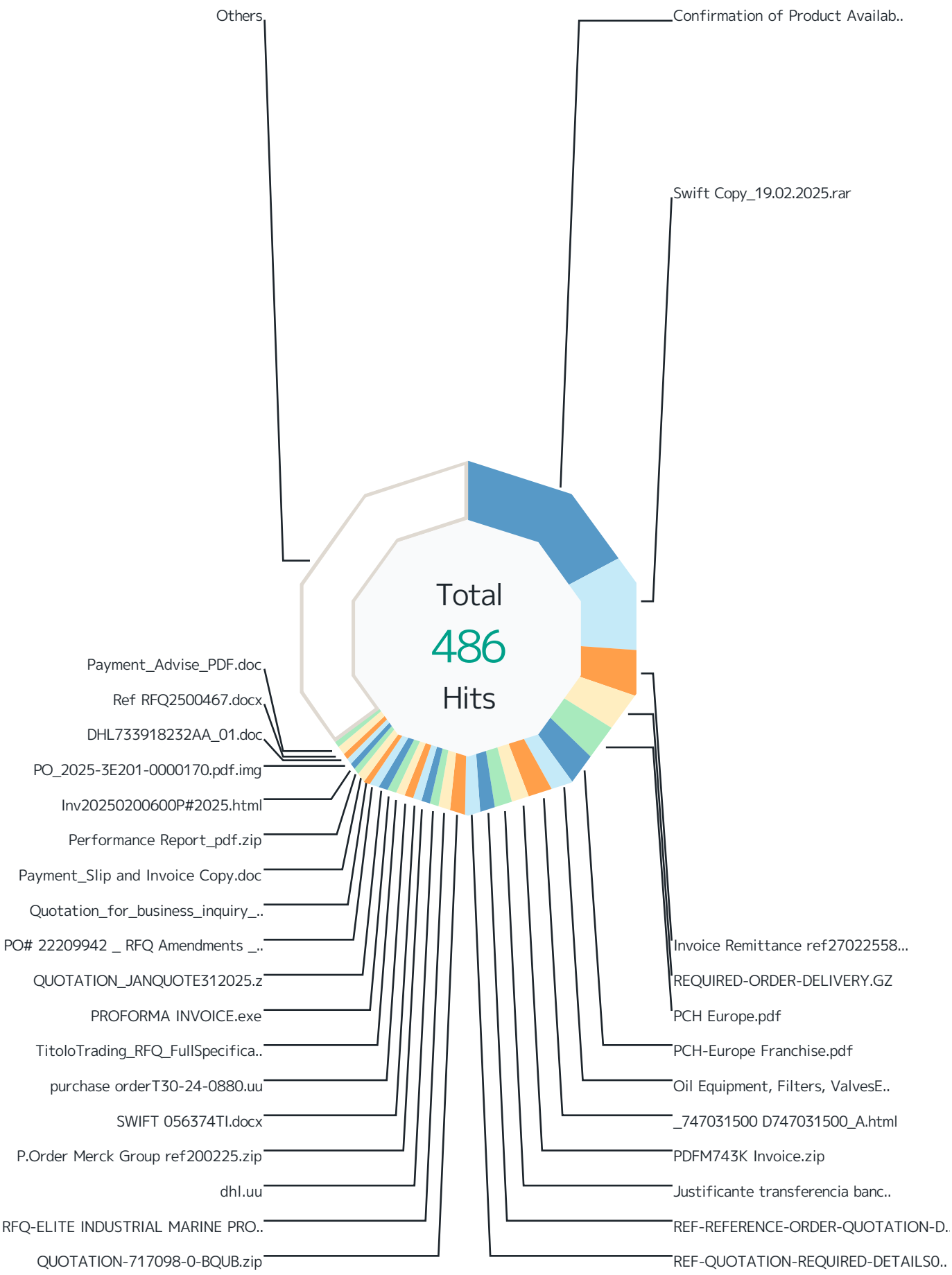
Update version
1844

Report started
2025-03-04 14:06:10+0100

Report run time
03:13:47

Filters used
Match All

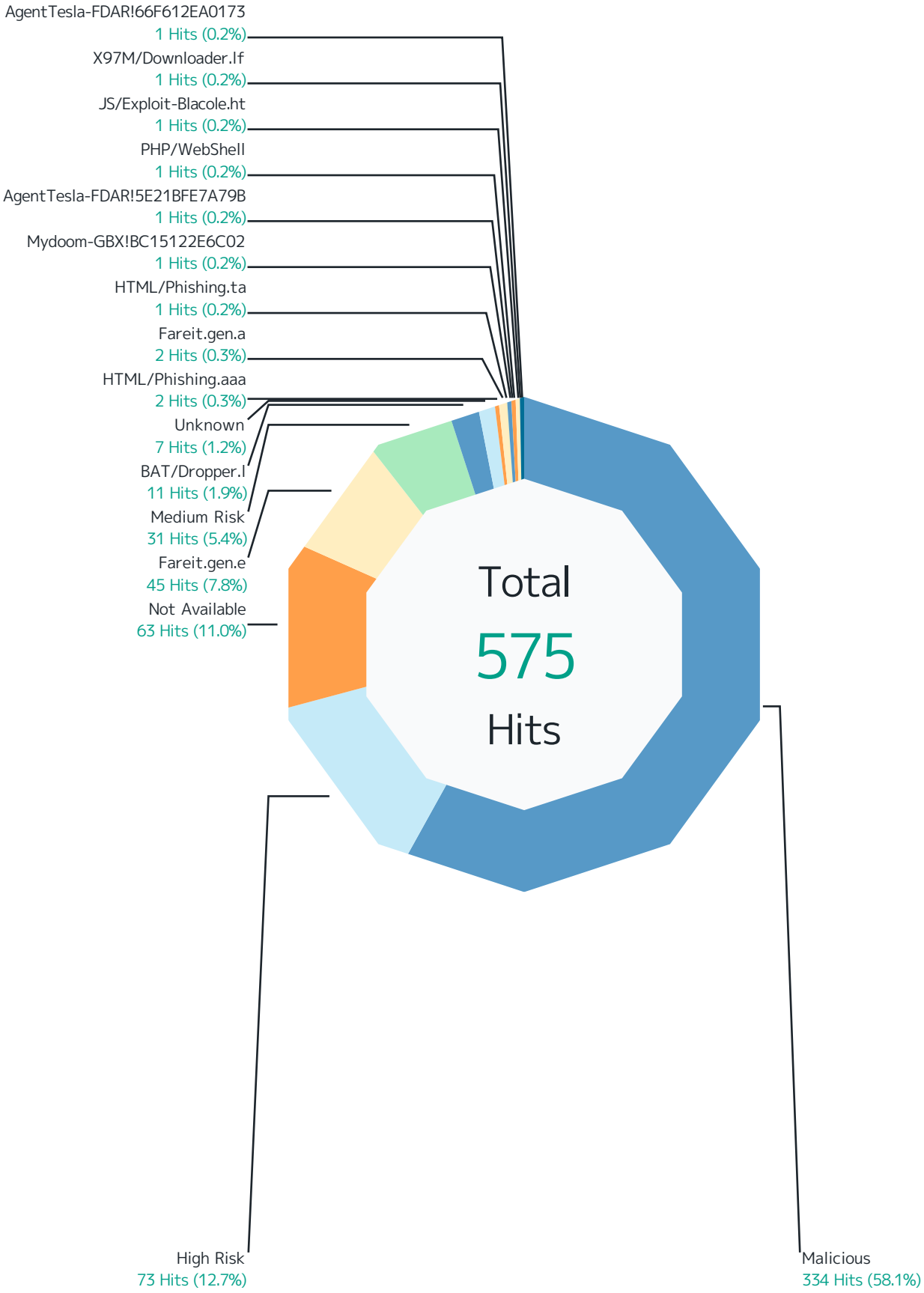
Virenfilterung MXe



Records by file name	Hits	%
Confirmation of Product Availability.ace	84	17.3 %
Swift Copy_19.02.2025.rar	43	8.8 %
Invoice Remittance ref27022558.zip	20	4.1 %
REQUIRED-ORDER-DELIVERY.GZ	18	3.7 %
PCH Europe.pdf	16	3.3 %
PCH-Europe Franchise.pdf	13	2.7 %
Oil Equipment, Filters, ValvesETC_SMT25S0907242.ace	10	2.1 %
_747031500 D747031500_A.html	10	2.1 %
PDFM743K Invoice.zip	9	1.9 %
Justificante transferencia bancaria 097185445.rar	8	1.6 %
REF-REFERENCE-ORDER-QUOTATION-DETAILS.rar	7	1.4 %
REF-QUOTATION-REQUIRED-DETAILS00028837849.GZ	7	1.4 %
QUOTATION-717098-0-BQUB.zip	6	1.2 %
RFQ-ELITE INDUSTRIAL MARINE PROJECT.7z	5	1.0 %
dhl.uu	5	1.0 %
P.Order Merck Group ref200225.zip	4	0.8 %
SWIFT 056374TI.docx	4	0.8 %
purchase orderT30-24-0880.uu	4	0.8 %
TitoloTrading_RFQ_FullSpecifications_20250502.z	4	0.8 %
PROFORMA INVOICE.exe	4	0.8 %
QUOTATION_JANQUOTE312025.z	4	0.8 %
PO# 22209942 _ RFQ Amendments _Shipping Doc_FEDEX.....Pdf.TAR	4	0.8 %
Quotation_for_business_inquiry_list.UUE	3	0.6 %
Payment_Slip and Invoice Copy.doc	3	0.6 %
Performance Report_pdf.zip	3	0.6 %
Inv20250200600P#2025.html	3	0.6 %
PO_2025-3E201-0000170.pdf.img	3	0.6 %
DHL733918232AA_01.doc	3	0.6 %
Ref RFQ2500467.docx	3	0.6 %
Payment_Advise_PDF.doc	3	0.6 %
Others	173	35.6 %
Total	**486**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.

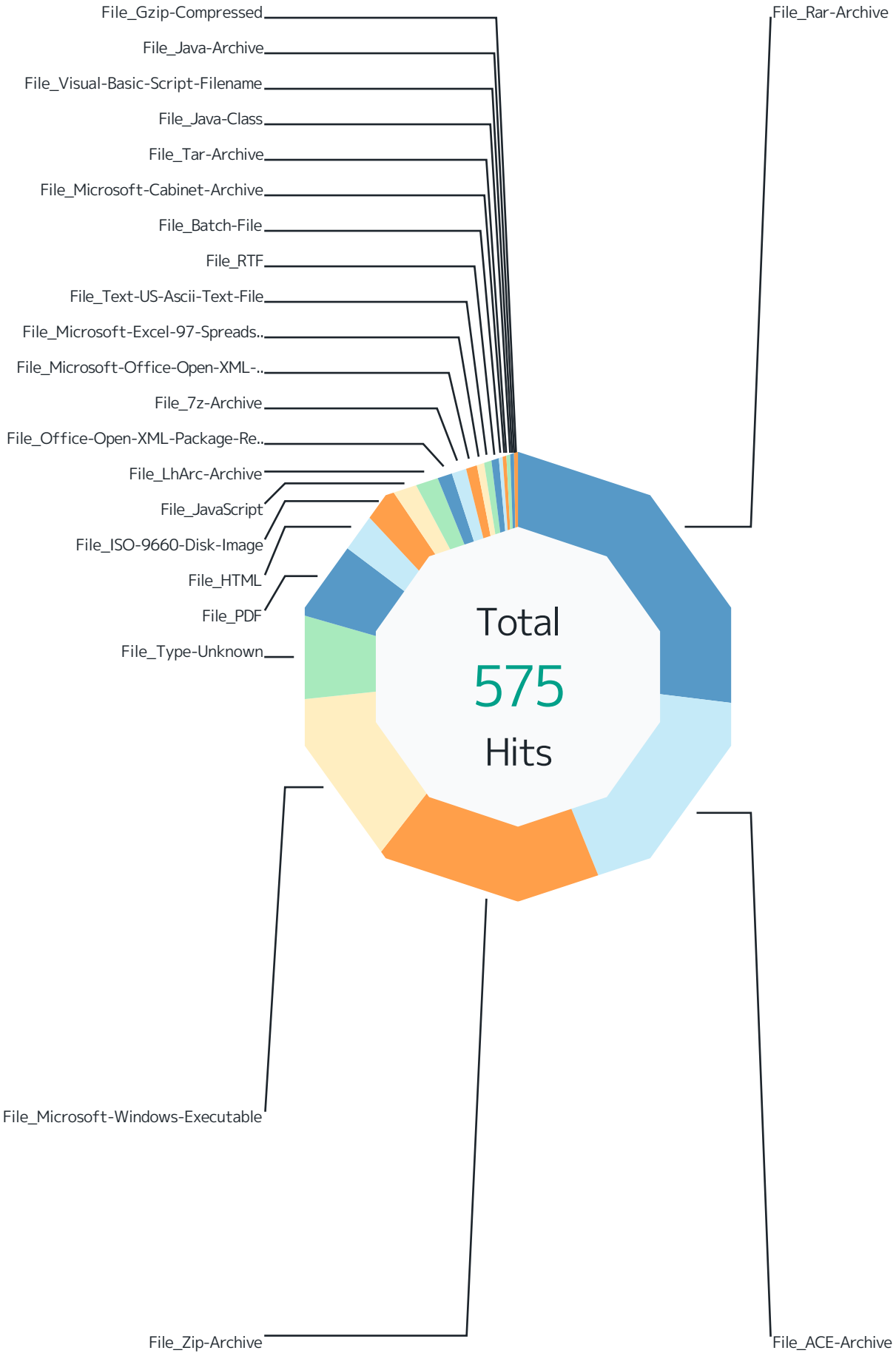

AgentTesla-FDAR!66F612EA0173
1 Hits (0.2%)
X97M/Downloader.lf
1 Hits (0.2%)
JS/Exploit-Blacole.ht
1 Hits (0.2%)
PHP/WebShell
1 Hits (0.2%)
AgentTesla-FDAR!5E21BFE7A79B
1 Hits (0.2%)
Mydoom-GBX!BC15122E6C02
1 Hits (0.2%)
HTML/Phishing.ta
1 Hits (0.2%)
Fareit.gen.a
2 Hits (0.3%)
HTML/Phishing.aaa
2 Hits (0.3%)
Unknown
7 Hits (1.2%)
BAT/Dropper.l
11 Hits (1.9%)
Medium Risk
31 Hits (5.4%)
Fareit.gen.e
45 Hits (7.8%)
Not Available
63 Hits (11.0%)
Total
575
Hits
High Risk
73 Hits (12.7%)
Malicious
334 Hits (58.1%)

Scan Result	Hits	%
Malicious	**334**	**58.1 %**
File_Rar-Archive	142	24.7 %
File_Microsoft-Windows-Executable	65	11.3 %
File_ACE-Archive	50	8.7 %
File_Zip-Archive	25	4.3 %
File_ISO-9660-Disk-Image	13	2.3 %
File_Type-Unknown	11	1.9 %
File_HTML	7	1.2 %
File_LhArc-Archive	4	0.7 %
File_7z-Archive	3	0.5 %
File_Microsoft-Office-Open-XML-Document	2	0.3 %
File_Microsoft-Excel-97-Spreadsheet	2	0.3 %
File_Text-US-Ascii-Text-File	2	0.3 %
File_RTF	2	0.3 %
File_Batch-File	2	0.3 %
File_PDF	1	0.2 %
File_Microsoft-Cabinet-Archive	1	0.2 %
File_Tar-Archive	1	0.2 %
File_Visual-Basic-Script-Filename	1	0.2 %
High Risk	**73**	**12.7 %**
File_PDF	32	5.6 %
File_Type-Unknown	19	3.3 %
File_Rar-Archive	6	1.0 %
File_LhArc-Archive	5	0.9 %
File_Zip-Archive	3	0.5 %
File_7z-Archive	2	0.3 %
File_Microsoft-Excel-97-Spreadsheet	2	0.3 %
File_HTML	1	0.2 %
File_ISO-9660-Disk-Image	1	0.2 %
File_RTF	1	0.2 %
File_Java-Class	1	0.2 %
Not Available	**63**	**11.0 %**
File_Zip-Archive	60	10.4 %
File_Microsoft-Office-Open-XML-Document	2	0.3 %
File_Java-Archive	1	0.2 %
Fareit.gen.e	**45**	**7.8 %**
File_ACE-Archive	45	7.8 %
Medium Risk	**31**	**5.4 %**
File_JavaScript	9	1.6 %

Scan Result	Hits	%
File_Microsoft-Windows-Executable	7	1.2 %
File_Office-Open-XML-Package-Relations-Item	7	1.2 %
File_HTML	4	0.7 %
File_Zip-Archive	1	0.2 %
File_PDF	1	0.2 %
File_ISO-9660-Disk-Image	1	0.2 %
File_Text-US-Ascii-Text-File	1	0.2 %
BAT/Dropper.l	**11**	**1.9 %**
File_Type-Unknown	6	1.0 %
File_Rar-Archive	5	0.9 %
Unknown	**7**	**1.2 %**
File_Zip-Archive	7	1.2 %
HTML/Phishing.aaa	**2**	**0.3 %**
File_HTML	2	0.3 %
Fareit.gen.a	**2**	**0.3 %**
File_ACE-Archive	2	0.3 %
HTML/Phishing.ta	**1**	**0.2 %**
File_HTML	1	0.2 %
Mydoom-GBX!BC15122E6C02	**1**	**0.2 %**
File_Microsoft-Windows-Executable	1	0.2 %
AgentTesla-FDAR!5E21BFE7A79B	**1**	**0.2 %**
File_Rar-Archive	1	0.2 %
PHP/WebShell	**1**	**0.2 %**
File_Gzip-Compressed	1	0.2 %
JS/Exploit-Blacole.ht	**1**	**0.2 %**
File_JavaScript	1	0.2 %
X97M/Downloader.lf	**1**	**0.2 %**
File_Microsoft-Office-Open-XML-Document	1	0.2 %
AgentTesla-FDAR!66F612EA0173	**1**	**0.2 %**
File_Rar-Archive	1	0.2 %
Total	**575**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

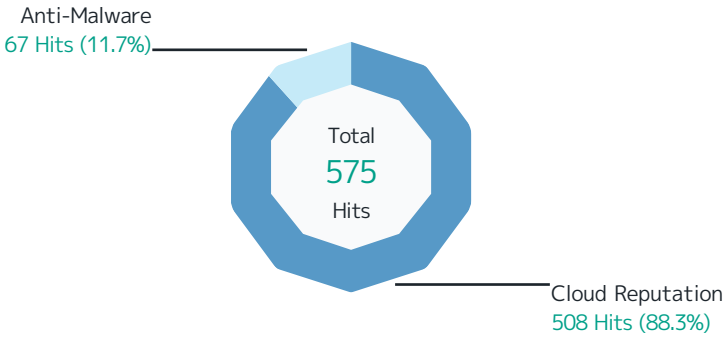

File_Gzip-Compressed
File_Java-Archive
File_Visual-Basic-Script-Filename
File_Java-Class
File_Tar-Archive
File_Microsoft-Cabinet-Archive
File_Batch-File
File_RTF
File_Text-US-Ascii-Text-File
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Office-Open-XML-..
File_7z-Archive
File_Office-Open-XML-Package-Re..
File_LhArc-Archive
File_JavaScript
File_ISO-9660-Disk-Image
File_HTML
File_PDF
File_Type-Unknown
File_Rar-Archive
Total
575
Hits
File_Microsoft-Windows-Executable
File_Zip-Archive
File_ACE-Archive

Responding Scanner	Hits	%
File_Rar-Archive	**155**	**27.0 %**
Malicious	142	24.7 %
High Risk	6	1.0 %
BAT/Dropper.I	5	0.9 %
AgentTesla-FDAR!5E21BFE7A79B	1	0.2 %
AgentTesla-FDAR!66F612EA0173	1	0.2 %
File_ACE-Archive	**97**	**16.9 %**
Malicious	50	8.7 %
Fareit.gen.e	45	7.8 %
Fareit.gen.a	2	0.3 %
File_Zip-Archive	**96**	**16.7 %**
Not Available	60	10.4 %
Malicious	25	4.3 %
Unknown	7	1.2 %
High Risk	3	0.5 %
Medium Risk	1	0.2 %
File_Microsoft-Windows-Executable	**73**	**12.7 %**
Malicious	65	11.3 %
Medium Risk	7	1.2 %
Mydoom-GBX!BC15122E6C02	1	0.2 %
File_Type-Unknown	**36**	**6.3 %**
High Risk	19	3.3 %
Malicious	11	1.9 %
BAT/Dropper.I	6	1.0 %
File_PDF	**34**	**5.9 %**
High Risk	32	5.6 %
Malicious	1	0.2 %
Medium Risk	1	0.2 %
File_HTML	**15**	**2.6 %**
Malicious	7	1.2 %
Medium Risk	4	0.7 %
HTML/Phishing.aaa	2	0.3 %
High Risk	1	0.2 %
HTML/Phishing.ta	1	0.2 %
File_ISO-9660-Disk-Image	**15**	**2.6 %**
Malicious	13	2.3 %
High Risk	1	0.2 %
Medium Risk	1	0.2 %
File_JavaScript	**10**	**1.7 %**

Responding Scanner	Hits	%
Medium Risk	9	1.6 %
JS/Exploit-Blacole.ht	1	0.2 %
File_LhArc-Archive	**9**	**1.6 %**
High Risk	5	0.9 %
Malicious	4	0.7 %
File_Office-Open-XML-Package-Relations-Item	**7**	**1.2 %**
Medium Risk	7	1.2 %
File_7z-Archive	**5**	**0.9 %**
Malicious	3	0.5 %
High Risk	2	0.3 %
File_Microsoft-Office-Open-XML-Document	**5**	**0.9 %**
Malicious	2	0.3 %
Not Available	2	0.3 %
X97M/Downloader.If	1	0.2 %
File_Microsoft-Excel-97-Spreadsheet	**4**	**0.7 %**
Malicious	2	0.3 %
High Risk	2	0.3 %
File_Text-US-Ascii-Text-File	**3**	**0.5 %**
Malicious	2	0.3 %
Medium Risk	1	0.2 %
File_RTF	**3**	**0.5 %**
Malicious	2	0.3 %
High Risk	1	0.2 %
File_Batch-File	**2**	**0.3 %**
Malicious	2	0.3 %
File_Microsoft-Cabinet-Archive	**1**	**0.2 %**
Malicious	1	0.2 %
File_Tar-Archive	**1**	**0.2 %**
Malicious	1	0.2 %
File_Java-Class	**1**	**0.2 %**
High Risk	1	0.2 %
File_Visual-Basic-Script-Filename	**1**	**0.2 %**
Malicious	1	0.2 %
File_Java-Archive	**1**	**0.2 %**
Not Available	1	0.2 %
File_Gzip-Compressed	**1**	**0.2 %**
PHP/WebShell	1	0.2 %
Total	**575**	**100 %**

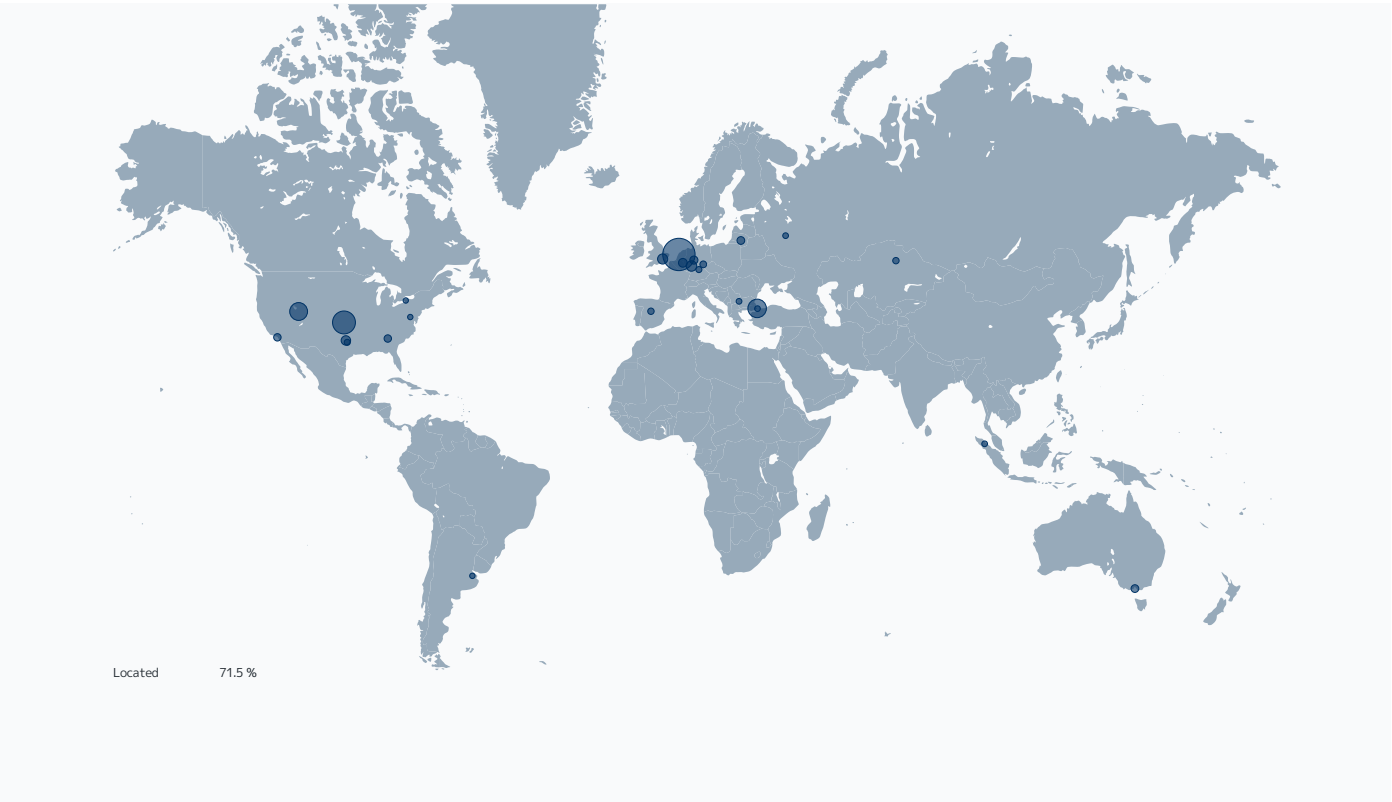
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**508**	**88.3 %**
File_Rar-Archive	148	25.7 %
File_Zip-Archive	96	16.7 %
File_Microsoft-Windows-Executable	72	12.5 %
File_ACE-Archive	50	8.7 %
File_PDF	34	5.9 %
File_Type-Unknown	30	5.2 %
File_ISO-9660-Disk-Image	15	2.6 %
File_HTML	12	2.1 %
File_JavaScript	9	1.6 %
File_LhArc-Archive	9	1.6 %
File_Office-Open-XML-Package-Relations-Item	7	1.2 %
File_7z-Archive	5	0.9 %
File_Microsoft-Office-Open-XML-Document	4	0.7 %
File_Microsoft-Excel-97-Spreadsheet	4	0.7 %
File_Text-US-Ascii-Text-File	3	0.5 %
File_RTF	3	0.5 %
File_Batch-File	2	0.3 %
File_Microsoft-Cabinet-Archive	1	0.2 %
File_Tar-Archive	1	0.2 %
File_Java-Class	1	0.2 %
File_Visual-Basic-Script-Filename	1	0.2 %
File_Java-Archive	1	0.2 %
Anti-Malware	**67**	**11.7 %**
File_ACE-Archive	47	8.2 %
File_Rar-Archive	7	1.2 %
File_Type-Unknown	6	1.0 %
File_HTML	3	0.5 %
File_Microsoft-Windows-Executable	1	0.2 %
File_JavaScript	1	0.2 %
File_Microsoft-Office-Open-XML-Document	1	0.2 %
File_Gzip-Compressed	1	0.2 %
Total	**575**	**100 %**

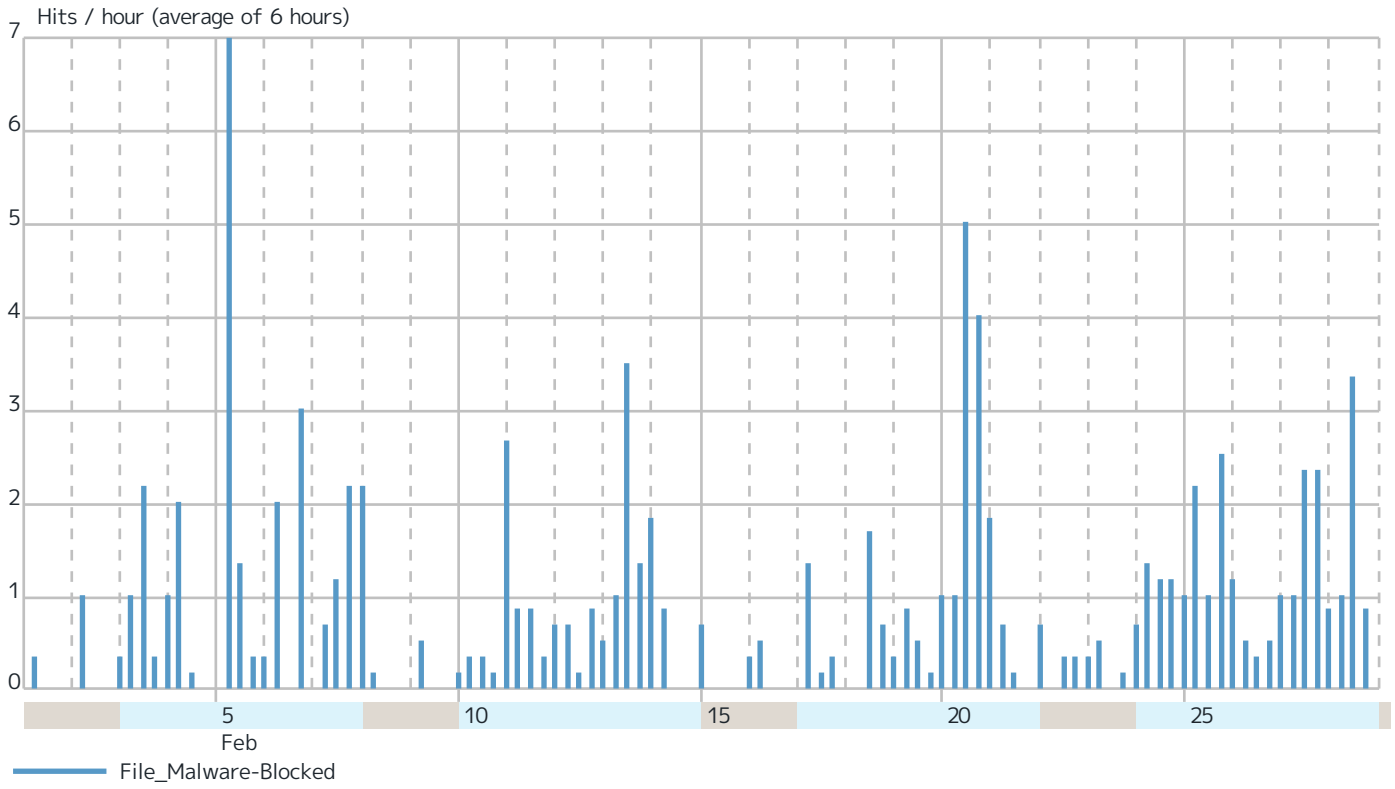
Virenfilterung SRC IPs



Records by src IP		Hits	%
185.126.34.191	Amsterdam, The Netherlands	84	14.6 %
104.168.135.205	United States	50	8.7 %
166.70.101.161	Pleasant Grove, Utah 84062, United States	41	7.1 %
45.138.183.159	Istanbul, Türkiye	32	5.6 %
151.236.19.252	London, United Kingdom	18	3.1 %
12.154.249.130	Krum, Texas 76249, United States	16	2.8 %
2a00:8a60:1:11::1006	RWTH Aachen	14	2.4 %
195.238.122.70	Frankfurt am Main, Germany	13	2.3 %
168.138.25.171	Melbourne, Australia	11	1.9 %
45.81.254.188	Lithuania	11	1.9 %
95.0.0.200	Istanbul, Türkiye	11	1.9 %
74.48.78.164	Los Angeles, California 90060, United States	10	1.7 %
45.61.59.184	Atlanta, Georgia 30303, United States	10	1.7 %
85.214.110.238	Germany	8	1.4 %
185.100.65.246	Astana, Kazakhstan	7	1.2 %
176.28.101.99	Spain	7	1.2 %
159.183.2.162	United States	6	1.0 %
37.120.175.171	Nuremberg, Germany	6	1.0 %
185.47.174.75	Frankfurt am Main, Germany	6	1.0 %
23.95.92.76	Dallas, Texas 75270, United States	6	1.0 %
188.127.249.230	Moscow, Russia	5	0.9 %
103.83.87.145	Türkiye	5	0.9 %
185.253.117.22	Bulgaria	5	0.9 %
202.162.192.27	Medan, Indonesia	5	0.9 %
78.111.75.144	Germany	4	0.7 %
190.210.9.35	Buenos Aires, Argentina	4	0.7 %
79.141.163.11	Ashburn, Virginia 20149, United States	4	0.7 %
172.245.12.77	Buffalo, New York 14205, United States	4	0.7 %
148.251.12.5	Falkenstein, Germany	4	0.7 %
5.9.85.99	Falkenstein, Germany	4	0.7 %
Others		164	28.5 %
Total		**575**	**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.