Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-12-01 00:00:00+0100
To: 2025-01-01 00:00:00+0100

Forcepoint

Report run by
jens

SD-WAN Manager Console version
7.1.5, build 11435

Update version
1819

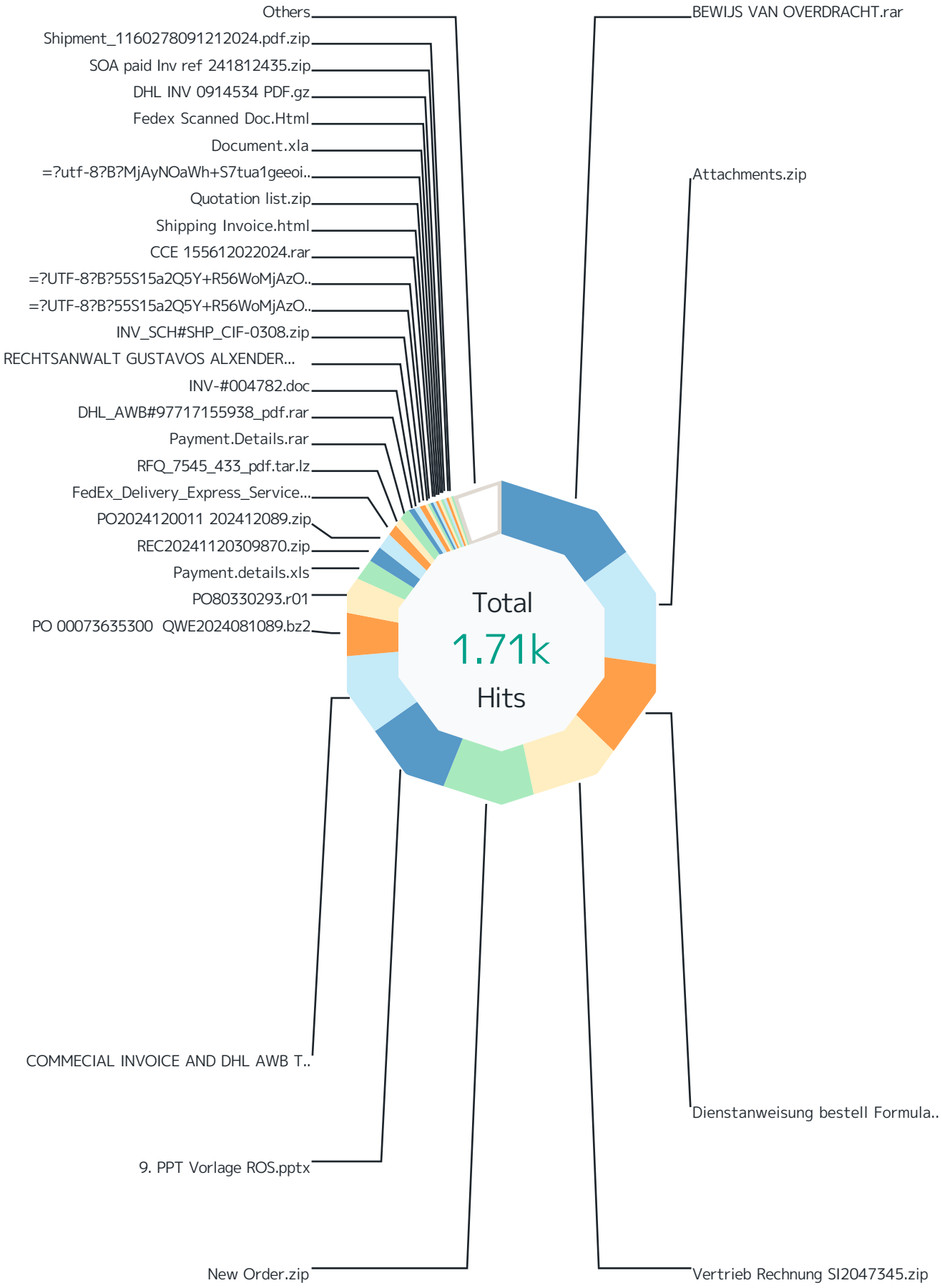
Report started
2025-01-02 11:32:38+0100

Report run time
03:39:51

Filters used
Match All

Table of Contents

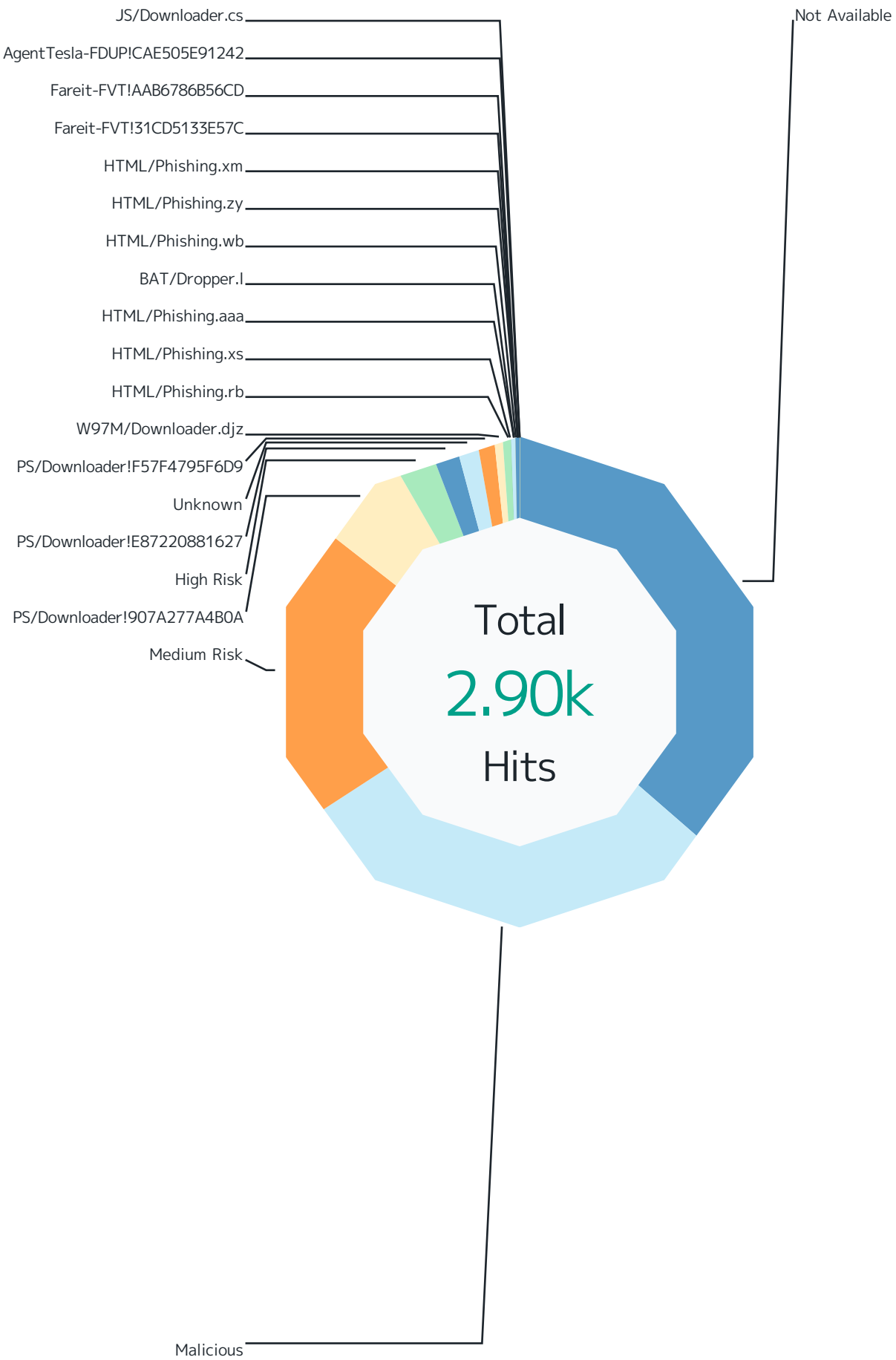
Virenfilterung MXe



Records by file name	Hits	%
BEWIJS VAN OVERDRACHT.rar	258	15.1 %
Attachments.zip	210	12.3 %
Dienstanweisung bestell Formular Kleiderkammer.docx	169	9.9 %
Vertrieb Rechnung SI2047345.zip	163	9.5 %
New Order.zip	163	9.5 %
9. PPT Vorlage ROS.pptx	153	8.9 %
COMMECIAL INVOICE AND DHL AWB TRACKING DETAILS.PDF.GZ	146	8.5 %
PO 00073635300 QWE2024081089.bz2	76	4.4 %
PO80330293.r01	59	3.4 %
Payment.details.xls	38	2.2 %
REC20241120309870.zip	30	1.8 %
PO2024120011 202412089.zip	27	1.6 %
FedEx_Delivery_Express_Service.docx	19	1.1 %
RFQ_7545_433_pdf.tar.lz	17	1.0 %
Payment.Details.rar	17	1.0 %
DHL_AWB#97717155938_pdf.rar	13	0.8 %
INV-#004782.doc	8	0.5 %
RECHTSANWALT GUSTAVOS ALXENDER.pdf	8	0.5 %
INV_SCH#SHP_CIF-0308.zip	6	0.4 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTEtMjAyMy5qcGcuaHRtbA==?=	5	0.3 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDExLTUtMjAyMy5wZGYuc2h0bWw=?=	5	0.3 %
CCE 155612022024.rar	4	0.2 %
Shipping Invoice.html	4	0.2 %
Quotation list.zip	4	0.2 %
=?utf-8?B?MjAyNOaWh+S7tua1geeoi+mhueebruWKnueQhumAmuefpe+8gS5kb2N4?=	4	0.2 %
Document.xla	4	0.2 %
Fedex Scanned Doc.Html	4	0.2 %
DHL INV 0914534 PDF.gz	4	0.2 %
SOA paid Inv ref 241812435.zip	4	0.2 %
Shipment_1160278091212024.pdf.zip	3	0.2 %
Others	88	5.1 %
Total	**1.71k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.

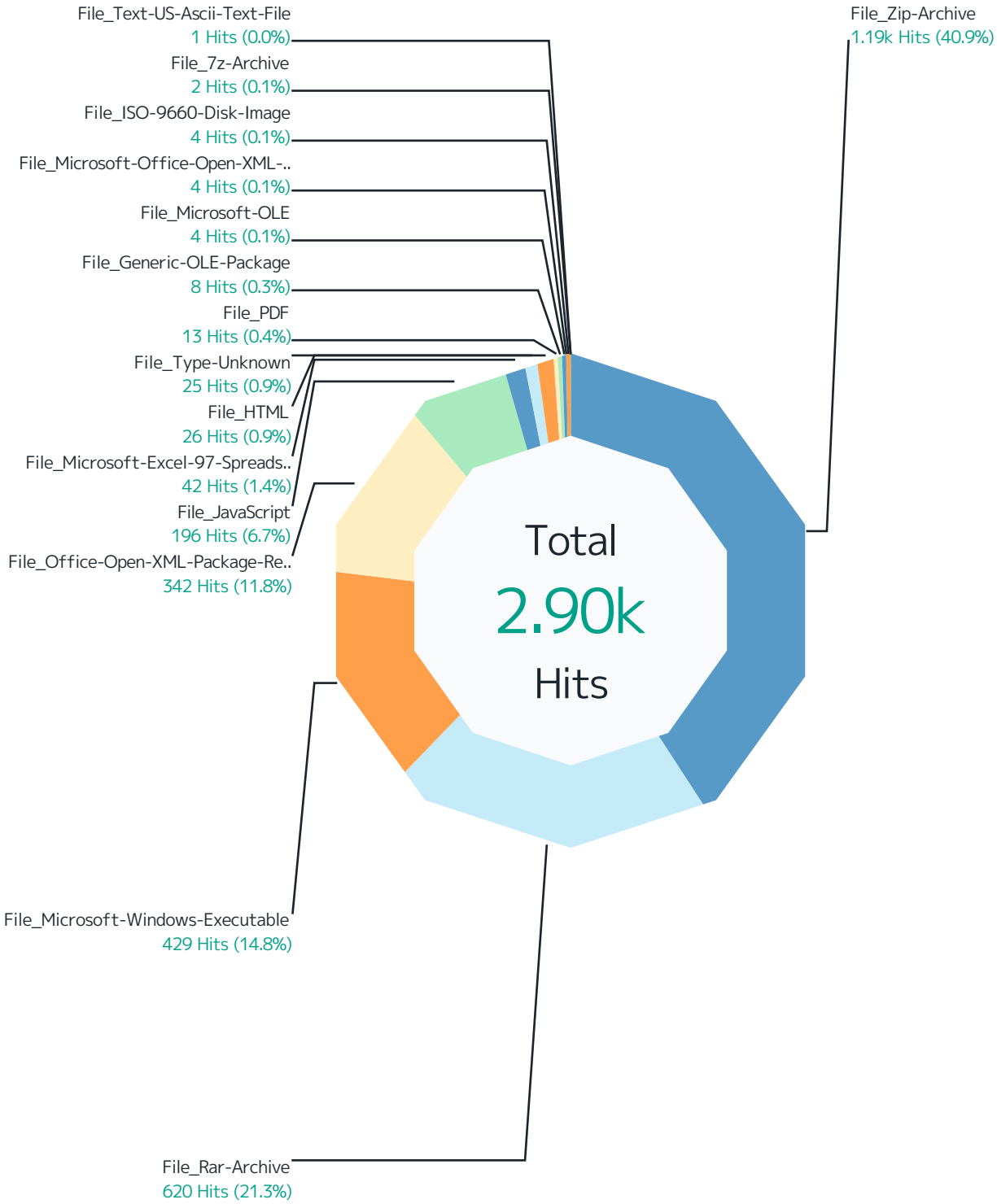

JS/Downloader.cs
AgentTesla-FDUP!CAE505E91242
Fareit-FVT!AAB6786B56CD
Fareit-FVT!31CD5133E57C
HTML/Phishing.xm
HTML/Phishing.zy
HTML/Phishing.wb
BAT/Dropper.l
HTML/Phishing.aaa
HTML/Phishing.xs
HTML/Phishing.rb
W97M/Downloader.djz
PS/Downloader!F57F4795F6D9
Unknown
PS/Downloader!E87220881627
High Risk
PS/Downloader!907A277A4B0A
Medium Risk
Not Available
Malicious
Total
2.90k
Hits

Scan Result	Hits	%
Not Available	**1.06k**	**36.4 %**
File_Zip-Archive	1.06k	36.3 %
File_Microsoft-Office-Open-XML-Document	3	0.1 %
Malicious	**857**	**29.5 %**
File_Microsoft-Windows-Executable	402	13.8 %
File_Rar-Archive	338	11.6 %
File_Zip-Archive	61	2.1 %
File_Type-Unknown	20	0.7 %
File_Microsoft-Excel-97-Spreadsheet	16	0.6 %
File_Generic-OLE-Package	8	0.3 %
File_Microsoft-OLE	4	0.1 %
File_ISO-9660-Disk-Image	3	0.1 %
File_HTML	2	0.1 %
File_7z-Archive	2	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
Medium Risk	**571**	**19.7 %**
File_Office-Open-XML-Package-Relations-Item	322	11.1 %
File_JavaScript	196	6.7 %
File_Microsoft-Windows-Executable	27	0.9 %
File_Zip-Archive	21	0.7 %
File_Rar-Archive	2	0.1 %
File_Type-Unknown	2	0.1 %
File_PDF	1	0.0 %
PS/Downloader!907A277A4B0A	**177**	**6.1 %**
File_Rar-Archive	177	6.1 %
High Risk	**71**	**2.4 %**
File_Office-Open-XML-Package-Relations-Item	20	0.7 %
File_Rar-Archive	19	0.7 %
File_Zip-Archive	13	0.4 %
File_PDF	11	0.4 %
File_Microsoft-Excel-97-Spreadsheet	4	0.1 %
File_HTML	3	0.1 %
File_ISO-9660-Disk-Image	1	0.0 %
PS/Downloader!E87220881627	**51**	**1.8 %**
File_Rar-Archive	51	1.8 %
Unknown	**38**	**1.3 %**
File_Zip-Archive	38	1.3 %
PS/Downloader!F57F4795F6D9	**30**	**1.0 %**
File_Rar-Archive	30	1.0 %

Scan Result	Hits	%
W97M/Downloader.djz	**22**	**0.8 %**
File_Microsoft-Excel-97-Spreadsheet	22	0.8 %
HTML/Phishing.rb	**10**	**0.3 %**
File_HTML	10	0.3 %
HTML/Phishing.xs	**4**	**0.1 %**
File_HTML	4	0.1 %
HTML/Phishing.aaa	**4**	**0.1 %**
File_HTML	4	0.1 %
BAT/Dropper.l	**3**	**0.1 %**
File_Type-Unknown	3	0.1 %
HTML/Phishing.wb	**2**	**0.1 %**
File_HTML	2	0.1 %
HTML/Phishing.zy	**1**	**0.0 %**
File_Text-US-Ascii-Text-File	1	0.0 %
HTML/Phishing.xm	**1**	**0.0 %**
File_HTML	1	0.0 %
Fareit-FVT!31CD5133E57C	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Fareit-FVT!AAB6786B56CD	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
AgentTesla-FDUP!CAE505E91242	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
JS/Downloader.cs	**1**	**0.0 %**
File_PDF	1	0.0 %
Total	**2.90k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

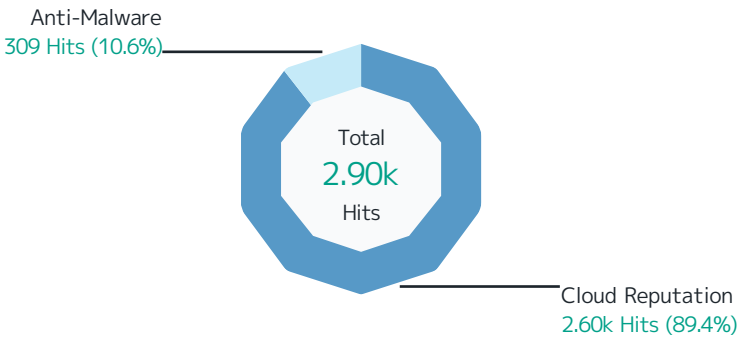


Responding Scanner	Hits	%
File_Zip-Archive	**1.19k**	**40.9 %**
Not Available	1.06k	36.3 %
Malicious	61	2.1 %
Unknown	38	1.3 %
Medium Risk	21	0.7 %
High Risk	13	0.4 %
File_Rar-Archive	**620**	**21.3 %**
Malicious	338	11.6 %
PS/Downloader!907A277A4B0A	177	6.1 %
PS/Downloader!E87220881627	51	1.8 %
PS/Downloader!F57F4795F6D9	30	1.0 %
High Risk	19	0.7 %
Medium Risk	2	0.1 %
Fareit-FVT!31CD5133E57C	1	0.0 %
Fareit-FVT!AAB6786B56CD	1	0.0 %
AgentTesla-FDUP!CAE505E91242	1	0.0 %
File_Microsoft-Windows-Executable	**429**	**14.8 %**
Malicious	402	13.8 %
Medium Risk	27	0.9 %
File_Office-Open-XML-Package-Relations-Item	**342**	**11.8 %**
Medium Risk	322	11.1 %
High Risk	20	0.7 %
File_JavaScript	**196**	**6.7 %**
Medium Risk	196	6.7 %
File_Microsoft-Excel-97-Spreadsheet	**42**	**1.4 %**
W97M/Downloader.djz	22	0.8 %
Malicious	16	0.6 %
High Risk	4	0.1 %
File_HTML	**26**	**0.9 %**
HTML/Phishing.rb	10	0.3 %
HTML/Phishing.xs	4	0.1 %
HTML/Phishing.aaa	4	0.1 %
High Risk	3	0.1 %
Malicious	2	0.1 %
HTML/Phishing.wb	2	0.1 %
HTML/Phishing.xm	1	0.0 %
File_Type-Unknown	**25**	**0.9 %**
Malicious	20	0.7 %
BAT/Dropper.I	3	0.1 %

Responding Scanner	Hits	%
Medium Risk	2	0.1 %
File_PDF	**13**	**0.4 %**
High Risk	11	0.4 %
Medium Risk	1	0.0 %
JS/Downloader.cs	1	0.0 %
File_Generic-OLE-Package	**8**	**0.3 %**
Malicious	8	0.3 %
File_Microsoft-OLE	**4**	**0.1 %**
Malicious	4	0.1 %
File_Microsoft-Office-Open-XML-Document	**4**	**0.1 %**
Not Available	3	0.1 %
Malicious	1	0.0 %
File_ISO-9660-Disk-Image	**4**	**0.1 %**
Malicious	3	0.1 %
High Risk	1	0.0 %
File_7z-Archive	**2**	**0.1 %**
Malicious	2	0.1 %
File_Text-US-Ascii-Text-File	**1**	**0.0 %**
HTML/Phishing.zy	1	0.0 %
Total	**2.90k**	**100 %**

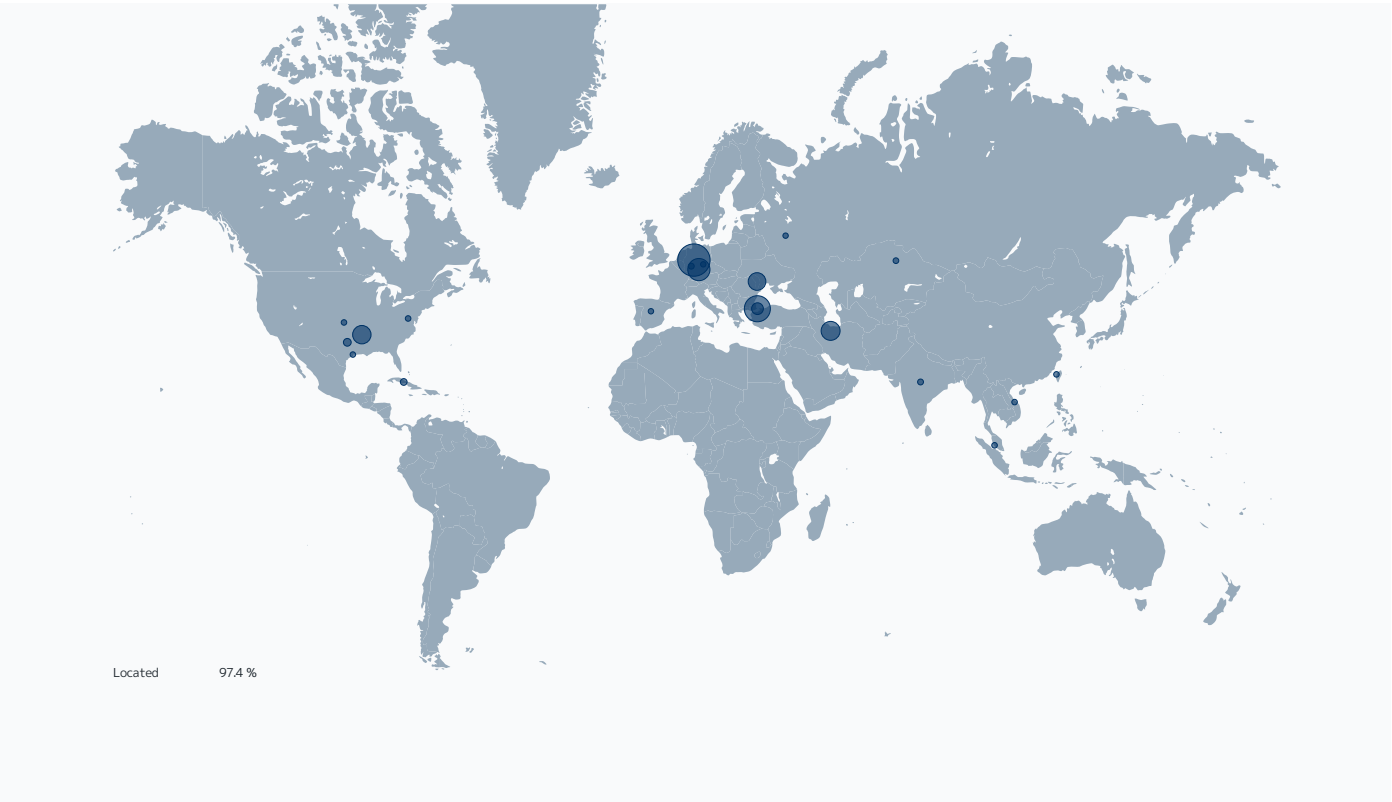
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**2.60k**	**89.4 %**
File_Zip-Archive	1.19k	40.9 %
File_Microsoft-Windows-Executable	429	14.8 %
File_Rar-Archive	359	12.4 %
File_Office-Open-XML-Package-Relations-Item	342	11.8 %
File_JavaScript	196	6.7 %
File_Type-Unknown	22	0.8 %
File_Microsoft-Excel-97-Spreadsheet	20	0.7 %
File_PDF	12	0.4 %
File_Generic-OLE-Package	8	0.3 %
File_HTML	5	0.2 %
File_Microsoft-OLE	4	0.1 %
File_Microsoft-Office-Open-XML-Document	4	0.1 %
File_ISO-9660-Disk-Image	4	0.1 %
File_7z-Archive	2	0.1 %
Anti-Malware	**309**	**10.6 %**
File_Rar-Archive	261	9.0 %
File_Microsoft-Excel-97-Spreadsheet	22	0.8 %
File_HTML	21	0.7 %
File_Type-Unknown	3	0.1 %
File_PDF	1	0.0 %
File_Text-US-Ascii-Text-File	1	0.0 %
Total	**2.90k**	**100 %**

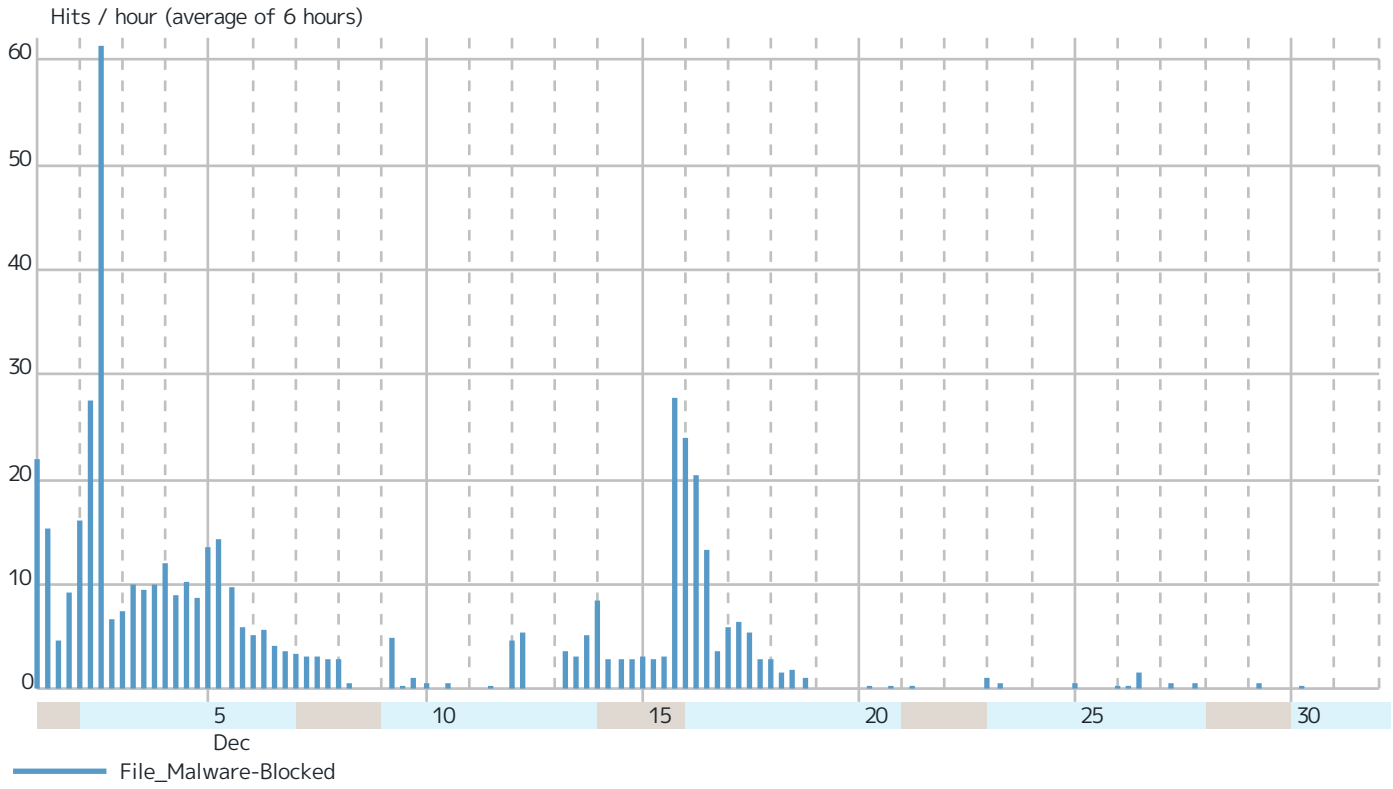
Virenfilterung SRC IPs



Records by src IP		Hits	%
45.90.89.226	Istanbul, Türkiye	429	14.8 %
91.198.228.73	Germany	338	11.6 %
188.68.63.98	Nuremberg, Germany	326	11.2 %
164.138.16.130	Tehran, Iran	326	11.2 %
12.132.7.160	Little Rock, Arkansas 72204, United States	313	10.8 %
37.221.66.134	Chisinau, Moldova	292	10.1 %
212.18.21.88	Germany	154	5.3 %
94.138.192.121	Türkiye	152	5.2 %
212.18.1.56	Germany	152	5.2 %
37.120.175.171	Nuremberg, Germany	60	2.1 %
98.142.240.248	Dallas, Texas 75270, United States	60	2.1 %
216.9.225.138	Istanbul, Türkiye	54	1.9 %
200.14.55.196	Cuba	36	1.2 %
173.249.58.67	Nuremberg, Germany	17	0.6 %
103.231.214.53	India	16	0.6 %
194.87.189.123	Frankfurt am Main, Germany	16	0.6 %
216.9.224.248	Istanbul, Türkiye	12	0.4 %
185.100.65.246	Astana, Kazakhstan	11	0.4 %
103.75.190.132	Kuala Lumpur, Malaysia	9	0.3 %
20.42.40.29	Washington, Virginia 22747, United States	8	0.3 %
61.216.161.38	Taichung, Taiwan	8	0.3 %
160.30.50.188	Vietnam	8	0.3 %
23.165.104.189	Houston, Texas 77058, United States	6	0.2 %
217.160.101.65	Spain	5	0.2 %
188.127.249.114	Moscow, Russia	4	0.1 %
23.254.165.224	United States	4	0.1 %
88.99.250.184	Falkenstein, Germany	4	0.1 %
104.168.147.70	United States	3	0.1 %
176.123.5.143	Chisinau, Moldova	3	0.1 %
194.31.79.251	Türkiye	3	0.1 %
Others		75	2.6 %
Total		**2.90k**	**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.