Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-11-01 00:00:00+0100
To: 2024-12-01 00:00:00+0100

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.4, build 11432

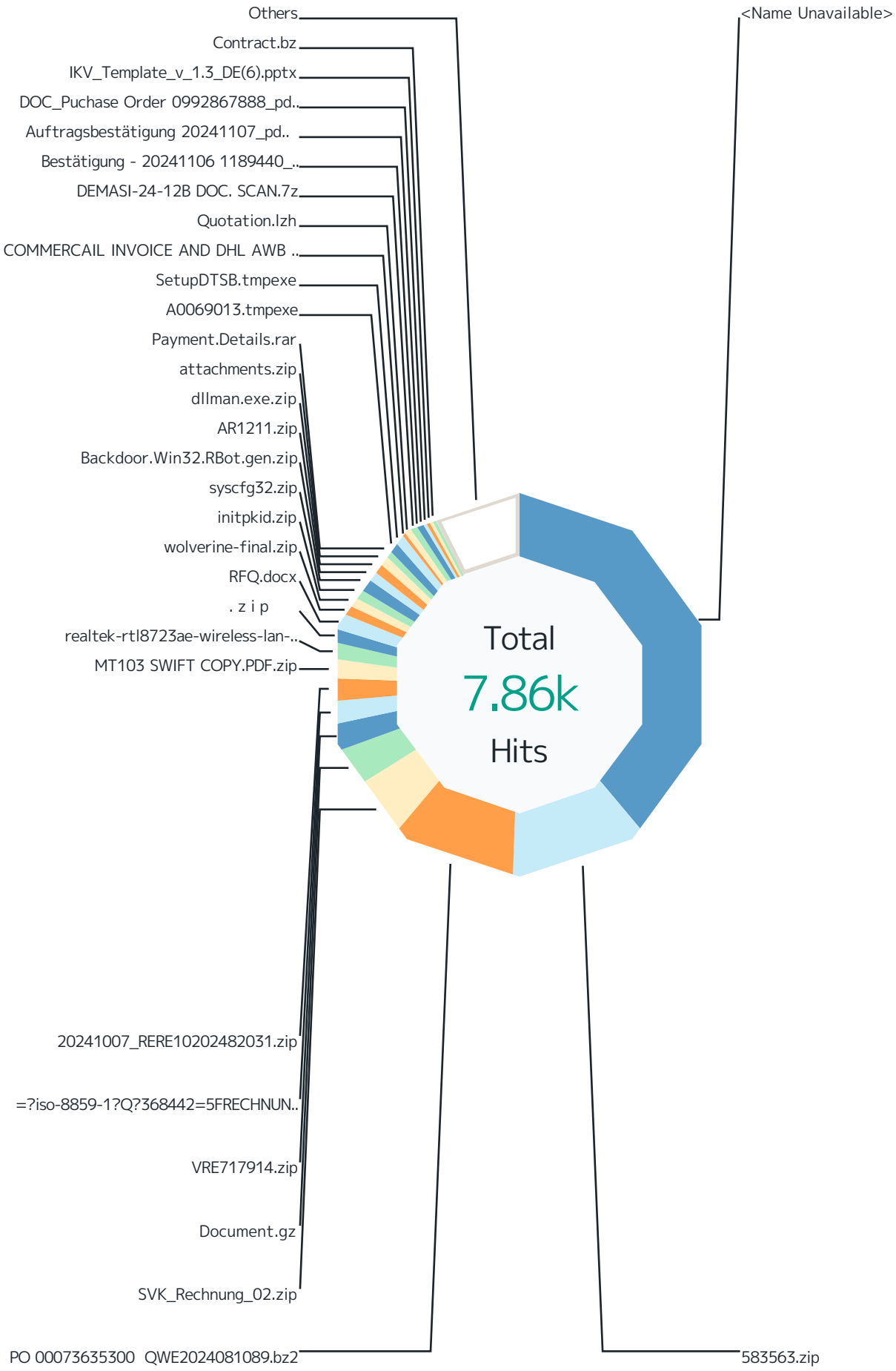
Update version
1805

Report started
2024-12-02 14:24:03+0100

Report run time
03:38:04

Filters used
Match All

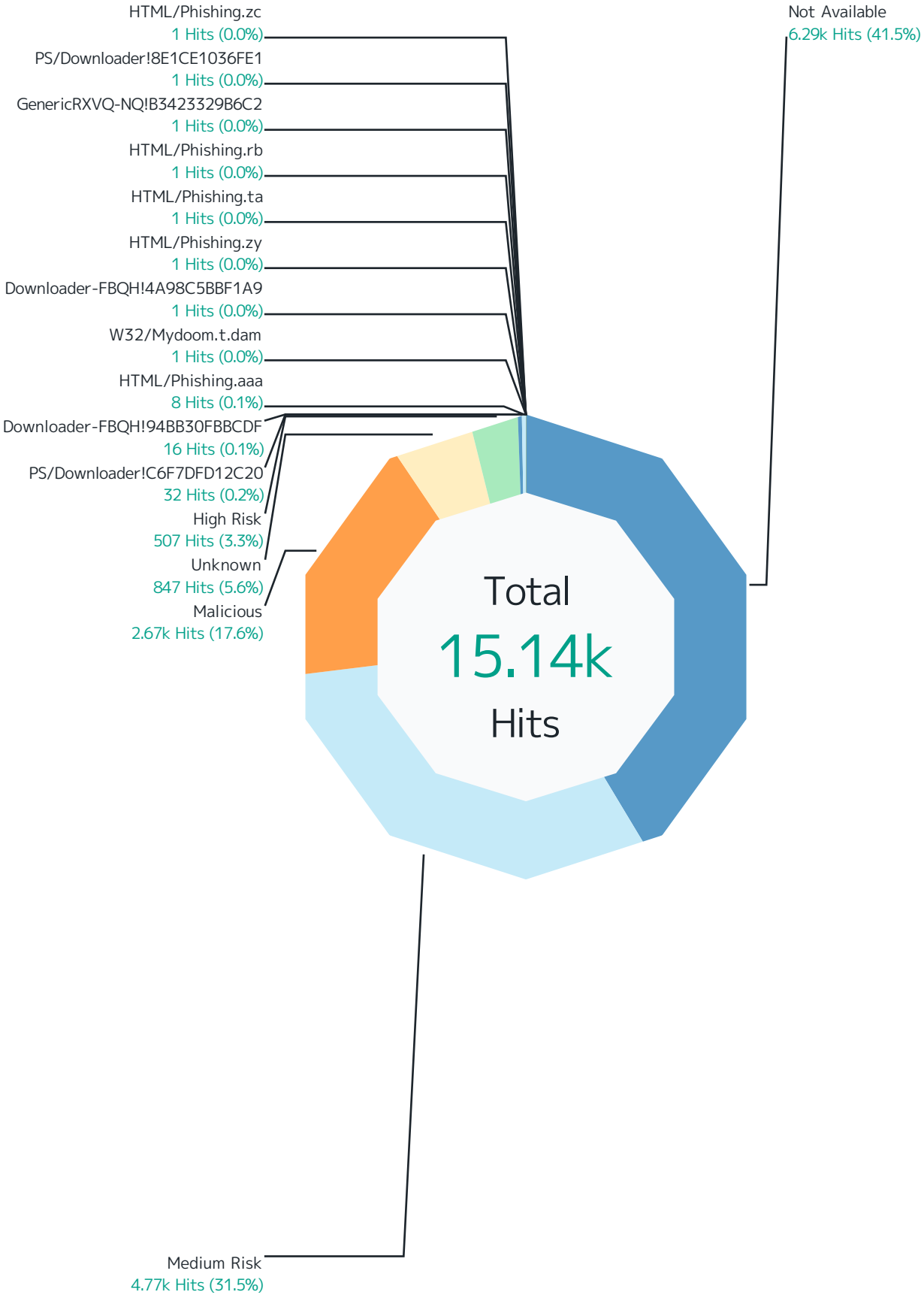
Virenfilterung MXe



Records by file name	Hits	%
<Name Unavailable>	3.05k	38.8 %
583563.zip	915	11.6 %
PO 00073635300 QWE2024081089.bz2	844	10.7 %
SVK_Rechnung_02.zip	387	4.9 %
Document.gz	269	3.4 %
VRE717914.zip	163	2.1 %
=?iso-8859-1?Q?368442=5FRECHNUNG.zip?=	156	2.0 %
20241007_RERE10202482031.zip	156	2.0 %
MT103 SWIFT COPY.PDF.zip	117	1.5 %
realtek-rtl8723ae-wireless-lan-80211n-pci-e-nic-1721363.zip	114	1.5 %
.zip	95	1.2 %
RFQ.docx	95	1.2 %
wolverine-final.zip	72	0.9 %
initpkid.zip	72	0.9 %
syscfg32.zip	72	0.9 %
Backdoor.Win32.RBot.gen.zip	72	0.9 %
AR1211.zip	67	0.9 %
dllman.exe.zip	64	0.8 %
attachments.zip	64	0.8 %
Payment.Details.rar	59	0.8 %
A0069013.tmpexe	57	0.7 %
SetupDTSB.tmpexe	57	0.7 %
COMMERCAIL INVOICE AND DHL AWB TRACKING DETAILS.PDF.zip	41	0.5 %
Quotation.lzh	40	0.5 %
DEMASI-24-12B DOC. SCAN.7z	38	0.5 %
Bestätigung - 20241106 1189440_pdf.7z	35	0.4 %
Auftragsbestätigung 20241107_pdf.z	29	0.4 %
DOC_Puchase Order 0992867888_pdf.rar	26	0.3 %
IKV_Template_v_1.3_DE(6).pptx	26	0.3 %
Contract.bz	25	0.3 %
Others	579	7.4 %
Total	**7.86k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.

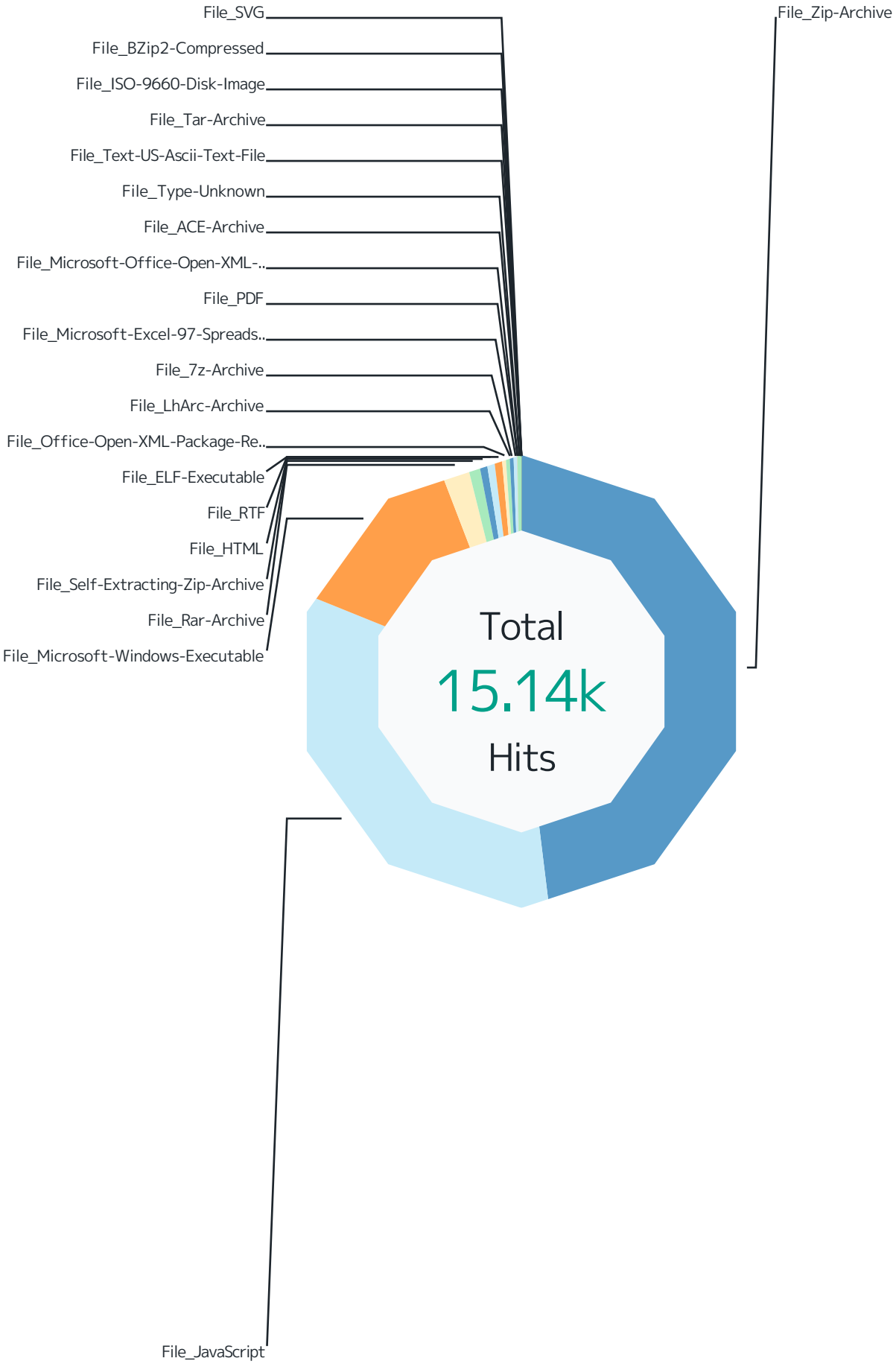

HTML/Phishing.zc
1 Hits (0.0%)
PS/Downloader!8E1CE1036FE1
1 Hits (0.0%)
GenericRXVQ-NQ!B3423329B6C2
1 Hits (0.0%)
HTML/Phishing.rb
1 Hits (0.0%)
HTML/Phishing.ta
1 Hits (0.0%)
HTML/Phishing.zy
1 Hits (0.0%)
Downloader-FBQH!4A98C5BBF1A9
1 Hits (0.0%)
W32/Mydoom.t.dam
1 Hits (0.0%)
HTML/Phishing.aaa
8 Hits (0.1%)
Downloader-FBQH!94BB30FBBCDF
16 Hits (0.1%)
PS/Downloader!C6F7DFD12C20
32 Hits (0.2%)
High Risk
507 Hits (3.3%)
Unknown
847 Hits (5.6%)
Malicious
2.67k Hits (17.6%)
Not Available
6.29k Hits (41.5%)
Total
15.14k
Hits
Medium Risk
4.77k Hits (31.5%)

Scan Result	Hits	%
Not Available	**6.29k**	**41.5 %**
File_Zip-Archive	6.28k	41.5 %
File_Microsoft-Office-Open-XML-Document	11	0.1 %
Medium Risk	**4.77k**	**31.5 %**
File_JavaScript	4.67k	30.8 %
File_Office-Open-XML-Package-Relations-Item	49	0.3 %
File_Microsoft-Windows-Executable	27	0.2 %
File_HTML	16	0.1 %
File_PDF	6	0.0 %
File_Zip-Archive	4	0.0 %
File_Rar-Archive	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
Malicious	**2.67k**	**17.6 %**
File_Microsoft-Windows-Executable	1.95k	12.9 %
File_Rar-Archive	206	1.4 %
File_Zip-Archive	154	1.0 %
File_RTF	86	0.6 %
File_HTML	74	0.5 %
File_ELF-Executable	72	0.5 %
File_LhArc-Archive	33	0.2 %
File_7z-Archive	32	0.2 %
File_Microsoft-Excel-97-Spreadsheet	25	0.2 %
File_ACE-Archive	8	0.1 %
File_Type-Unknown	8	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
File_Text-US-Ascii-Text-File	3	0.0 %
File_JavaScript	2	0.0 %
File_PDF	2	0.0 %
File_Tar-Archive	2	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_BZip2-Compressed	2	0.0 %
Unknown	**847**	**5.6 %**
File_Zip-Archive	847	5.6 %
High Risk	**507**	**3.3 %**
File_JavaScript	338	2.2 %
File_Self-Extracting-Zip-Archive	114	0.8 %
File_Rar-Archive	24	0.2 %
File_Office-Open-XML-Package-Relations-Item	15	0.1 %
File_PDF	7	0.0 %

Scan Result	Hits	%
File_Microsoft-Excel-97-Spreadsheet	3	0.0 %
File_Zip-Archive	1	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
File_Text-US-Ascii-Text-File	1	0.0 %
File_SVG	1	0.0 %
PS/Downloader!C6F7DFD12C20	**32**	**0.2 %**
File_Rar-Archive	32	0.2 %
Downloader-FBQH!94BB30FBBCDF	**16**	**0.1 %**
File_Rar-Archive	16	0.1 %
HTML/Phishing.aaa	**8**	**0.1 %**
File_HTML	8	0.1 %
W32/Mydoom.t.dam	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
Downloader-FBQH!4A98C5BBF1A9	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
HTML/Phishing.zy	**1**	**0.0 %**
File_Text-US-Ascii-Text-File	1	0.0 %
HTML/Phishing.ta	**1**	**0.0 %**
File_HTML	1	0.0 %
HTML/Phishing.rb	**1**	**0.0 %**
File_Text-US-Ascii-Text-File	1	0.0 %
GenericRXVQ-NQ!B3423329B6C2	**1**	**0.0 %**
File_Microsoft-Windows-Executable	1	0.0 %
PS/Downloader!8E1CE1036FE1	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
HTML/Phishing.zc	**1**	**0.0 %**
File_HTML	1	0.0 %
Total	**15.14k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

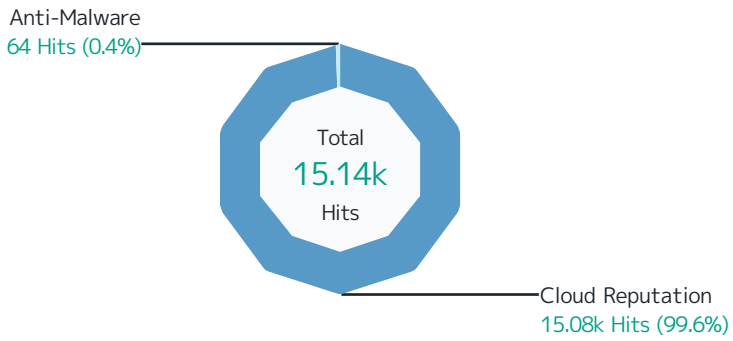

File_SVG
File_BZip2-Compressed
File_ISO-9660-Disk-Image
File_Tar-Archive
File_Text-US-Ascii-Text-File
File_Type-Unknown
File_ACE-Archive
File_Microsoft-Office-Open-XML-...
File_PDF
File_Microsoft-Excel-97-Spreads...
File_7z-Archive
File_LhArc-Archive
File_Office-Open-XML-Package-Re...
File_ELF-Executable
File_RTF
File_HTML
File_Self-Extracting-Zip-Archive
File_Rar-Archive
File_Microsoft-Windows-Executable
File_JavaScript
File_Zip-Archive
Total
15.14k
Hits

Responding Scanner	Hits	%
File_Zip-Archive	**7.28k**	**48.1 %**
Not Available	6.28k	41.5 %
Unknown	847	5.6 %
Malicious	154	1.0 %
Medium Risk	4	0.0 %
High Risk	1	0.0 %
W32/Mydoom.t.dam	1	0.0 %
File_JavaScript	**5.01k**	**33.1 %**
Medium Risk	4.67k	30.8 %
High Risk	338	2.2 %
Malicious	2	0.0 %
File_Microsoft-Windows-Executable	**1.98k**	**13.1 %**
Malicious	1.95k	12.9 %
Medium Risk	27	0.2 %
High Risk	1	0.0 %
GenericRXVQ-NQ!B3423329B6C2	1	0.0 %
File_Rar-Archive	**281**	**1.9 %**
Malicious	206	1.4 %
PS/Downloader!C6F7DFD12C20	32	0.2 %
High Risk	24	0.2 %
Downloader-FBQH!94BB30FBBCDF	16	0.1 %
Medium Risk	1	0.0 %
Downloader-FBQH!4A98C5BBF1A9	1	0.0 %
PS/Downloader!8E1CE1036FE1	1	0.0 %
File_Self-Extracting-Zip-Archive	**114**	**0.8 %**
High Risk	114	0.8 %
File_HTML	**100**	**0.7 %**
Malicious	74	0.5 %
Medium Risk	16	0.1 %
HTML/Phishing.aaa	8	0.1 %
HTML/Phishing.ta	1	0.0 %
HTML/Phishing.zc	1	0.0 %
File_RTF	**86**	**0.6 %**
Malicious	86	0.6 %
File_ELF-Executable	**72**	**0.5 %**
Malicious	72	0.5 %
File_Office-Open-XML-Package-Relations-Item	**64**	**0.4 %**
Medium Risk	49	0.3 %
High Risk	15	0.1 %

Responding Scanner	Hits	%
File_LhArc-Archive	**34**	**0.2 %**
Malicious	33	0.2 %
High Risk	1	0.0 %
File_7z-Archive	**32**	**0.2 %**
Malicious	32	0.2 %
File_Microsoft-Excel-97-Spreadsheet	**29**	**0.2 %**
Malicious	25	0.2 %
High Risk	3	0.0 %
Medium Risk	1	0.0 %
File_PDF	**15**	**0.1 %**
High Risk	7	0.0 %
Medium Risk	6	0.0 %
Malicious	2	0.0 %
File_Microsoft-Office-Open-XML-Document	**15**	**0.1 %**
Not Available	11	0.1 %
Malicious	3	0.0 %
High Risk	1	0.0 %
File_ACE-Archive	**8**	**0.1 %**
Malicious	8	0.1 %
File_Type-Unknown	**8**	**0.1 %**
Malicious	8	0.1 %
File_Text-US-Ascii-Text-File	**6**	**0.0 %**
Malicious	3	0.0 %
High Risk	1	0.0 %
HTML/Phishing.zy	1	0.0 %
HTML/Phishing.rb	1	0.0 %
File_Tar-Archive	**2**	**0.0 %**
Malicious	2	0.0 %
File_ISO-9660-Disk-Image	**2**	**0.0 %**
Malicious	2	0.0 %
File_BZip2-Compressed	**2**	**0.0 %**
Malicious	2	0.0 %
File_SVG	**1**	**0.0 %**
High Risk	1	0.0 %
Total	**15.14k**	**100 %**

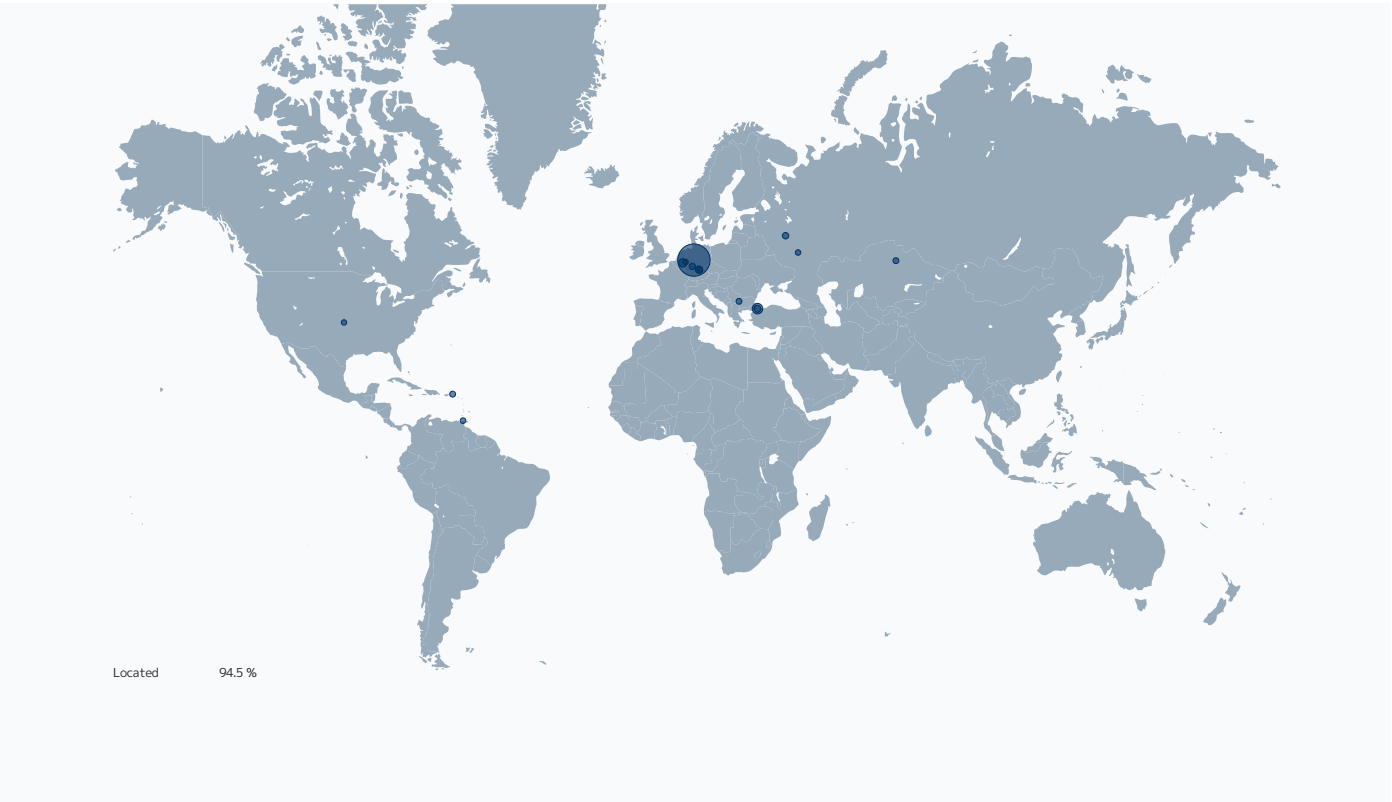
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**15.08k**	**99.6 %**
File_Zip-Archive	7.28k	48.1 %
File_JavaScript	5.01k	33.1 %
File_Microsoft-Windows-Executable	1.98k	13.1 %
File_Rar-Archive	231	1.5 %
File_Self-Extracting-Zip-Archive	114	0.8 %
File_HTML	90	0.6 %
File_RTF	86	0.6 %
File_ELF-Executable	72	0.5 %
File_Office-Open-XML-Package-Relations-Item	64	0.4 %
File_LhArc-Archive	34	0.2 %
File_7z-Archive	32	0.2 %
File_Microsoft-Excel-97-Spreadsheet	29	0.2 %
File_PDF	15	0.1 %
File_Microsoft-Office-Open-XML-Document	15	0.1 %
File_ACE-Archive	8	0.1 %
File_Type-Unknown	8	0.1 %
File_Text-US-Ascii-Text-File	4	0.0 %
File_Tar-Archive	2	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_BZip2-Compressed	2	0.0 %
File_SVG	1	0.0 %
Anti-Malware	**64**	**0.4 %**
File_Rar-Archive	50	0.3 %
File_HTML	10	0.1 %
File_Text-US-Ascii-Text-File	2	0.0 %
File_Zip-Archive	1	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
Total	**15.14k**	**100 %**

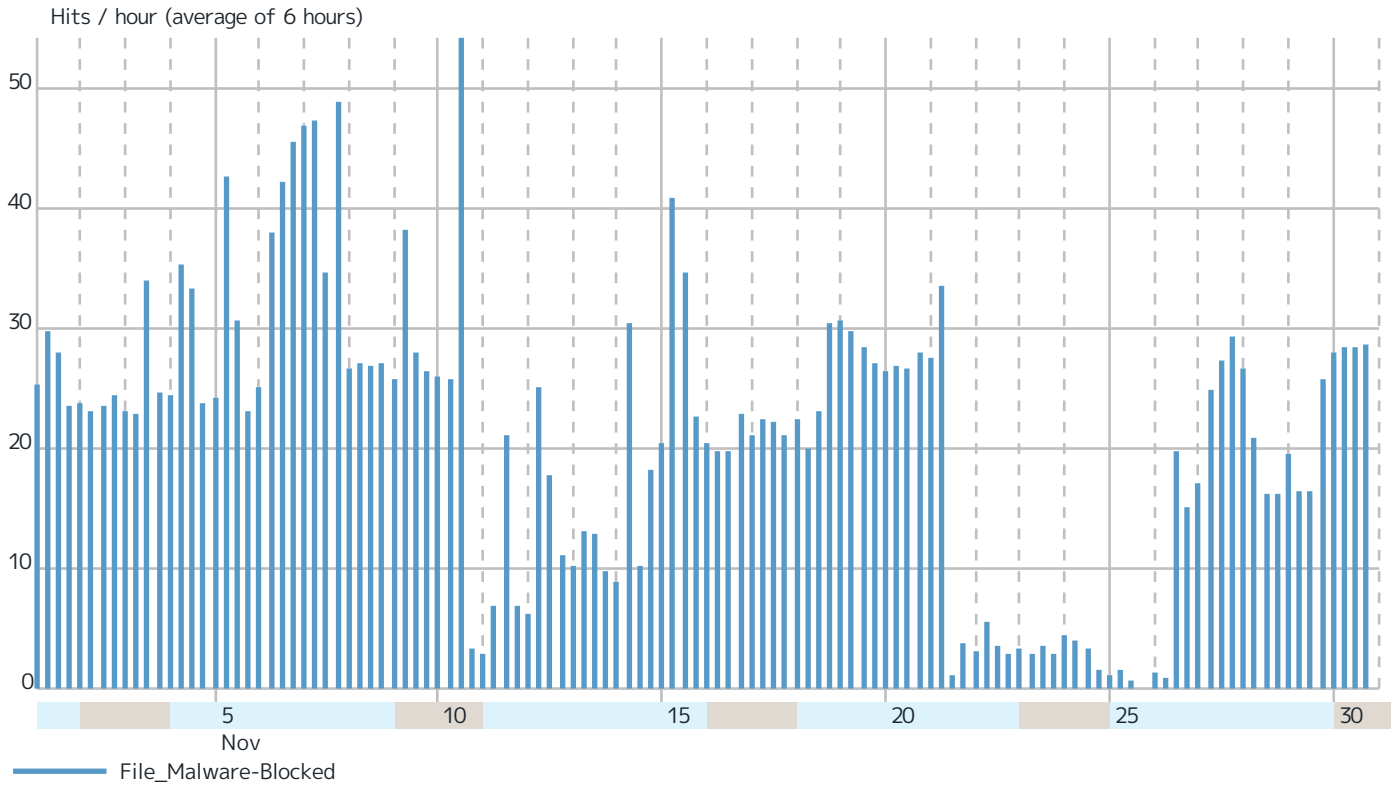
Virenfilterung SRC IPs



Records by src IP		Hits	%
89.107.187.19	Germany	5.39k	35.6 %
89.107.187.13	Germany	2.60k	17.2 %
94.138.192.121	Türkiye	1.27k	8.4 %
46.38.247.119	Nuremberg, Germany	652	4.3 %
46.229.45.53	Germany	638	4.2 %
45.90.89.221	Istanbul, Türkiye	538	3.6 %
94.138.192.122	Türkiye	414	2.7 %
195.63.103.234	Kahl am Main, Germany	313	2.1 %
2a00:8a60:1:11::1007	RWTH Aachen	236	1.6 %
80.85.156.120	Russia	234	1.5 %
2a00:8a60:1:11::1006	RWTH Aachen	220	1.5 %
2a00:8a60:1:11::1008	RWTH Aachen	220	1.5 %
2a00:8a60:1:11::1005	RWTH Aachen	220	1.5 %
37.221.64.208	Sofia, Bulgaria	178	1.2 %
62.146.106.22	Burgthann, Germany	134	0.9 %
45.88.3.205	British Virgin Islands	117	0.8 %
185.111.104.60	Astana, Kazakhstan	102	0.7 %
134.130.71.209	RWTH Aachen	99	0.7 %
181.188.28.140	D'Abadie, Trinidad and Tobago	93	0.6 %
185.111.104.62	Astana, Kazakhstan	88	0.6 %
80.85.156.144	Russia	82	0.5 %
78.132.141.85	Tambov, Russia	76	0.5 %
45.88.3.208	British Virgin Islands	74	0.5 %
82.165.122.100	Germany	64	0.4 %
62.146.106.25	Burgthann, Germany	50	0.3 %
109.194.1.168	Russia	50	0.3 %
91.198.228.73	Germany	46	0.3 %
80.237.138.250	Cologne, Germany	34	0.2 %
74.208.105.100	United States	32	0.2 %
62.146.106.26	Burgthann, Germany	30	0.2 %
Others		838	5.5 %
Total		**15.14k**	**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.