Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2025-04-01 00:00:00+0200
To: 2025-05-01 00:00:00+0200

Forcepoint

Table of Contents

Report run by
jens

Secure SD-WAN Manager Console version
7.2.4, build 11588

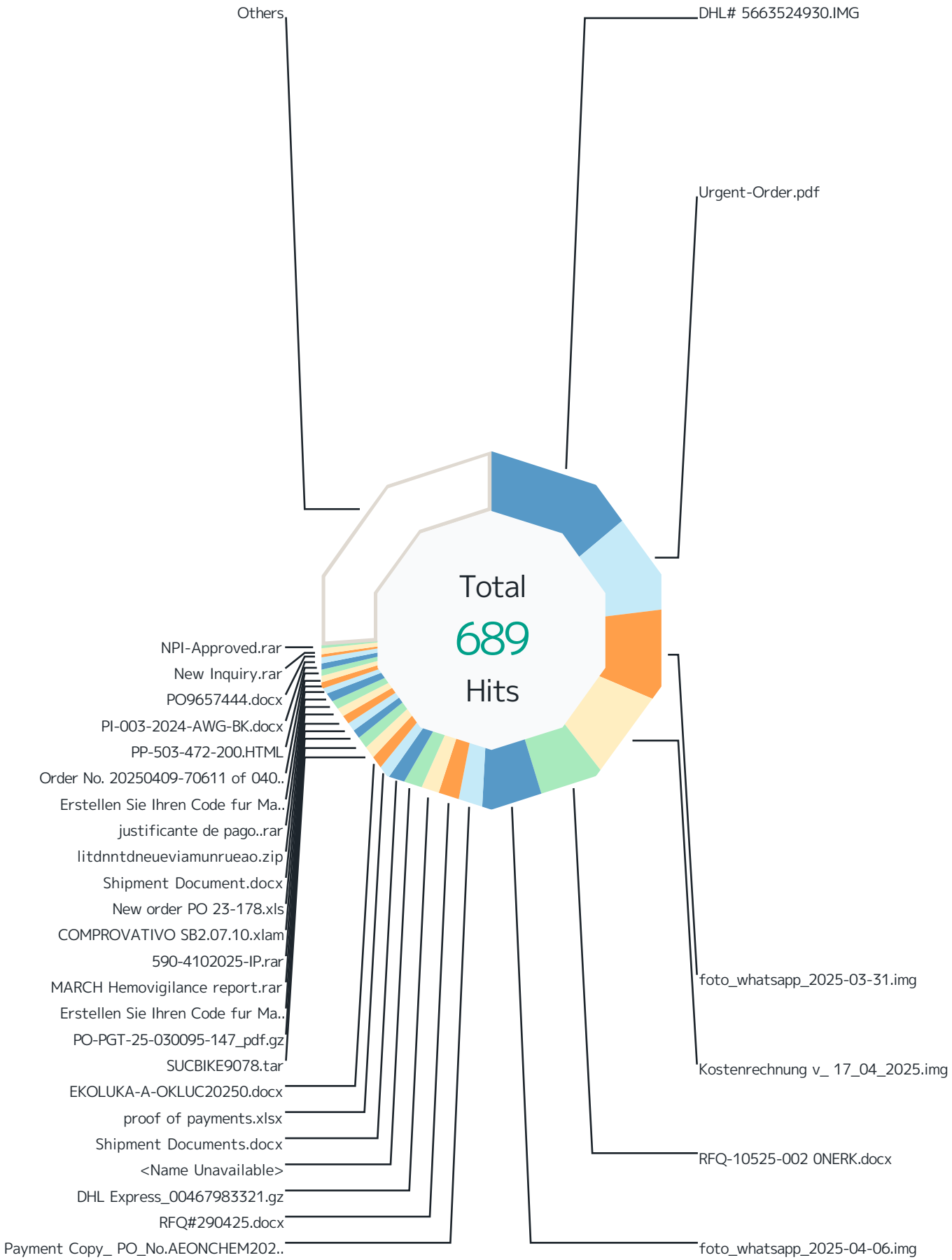
Update version
1877

Report started
2025-05-12 14:06:57+0200

Report run time
03:43:58

Filters used
Match All

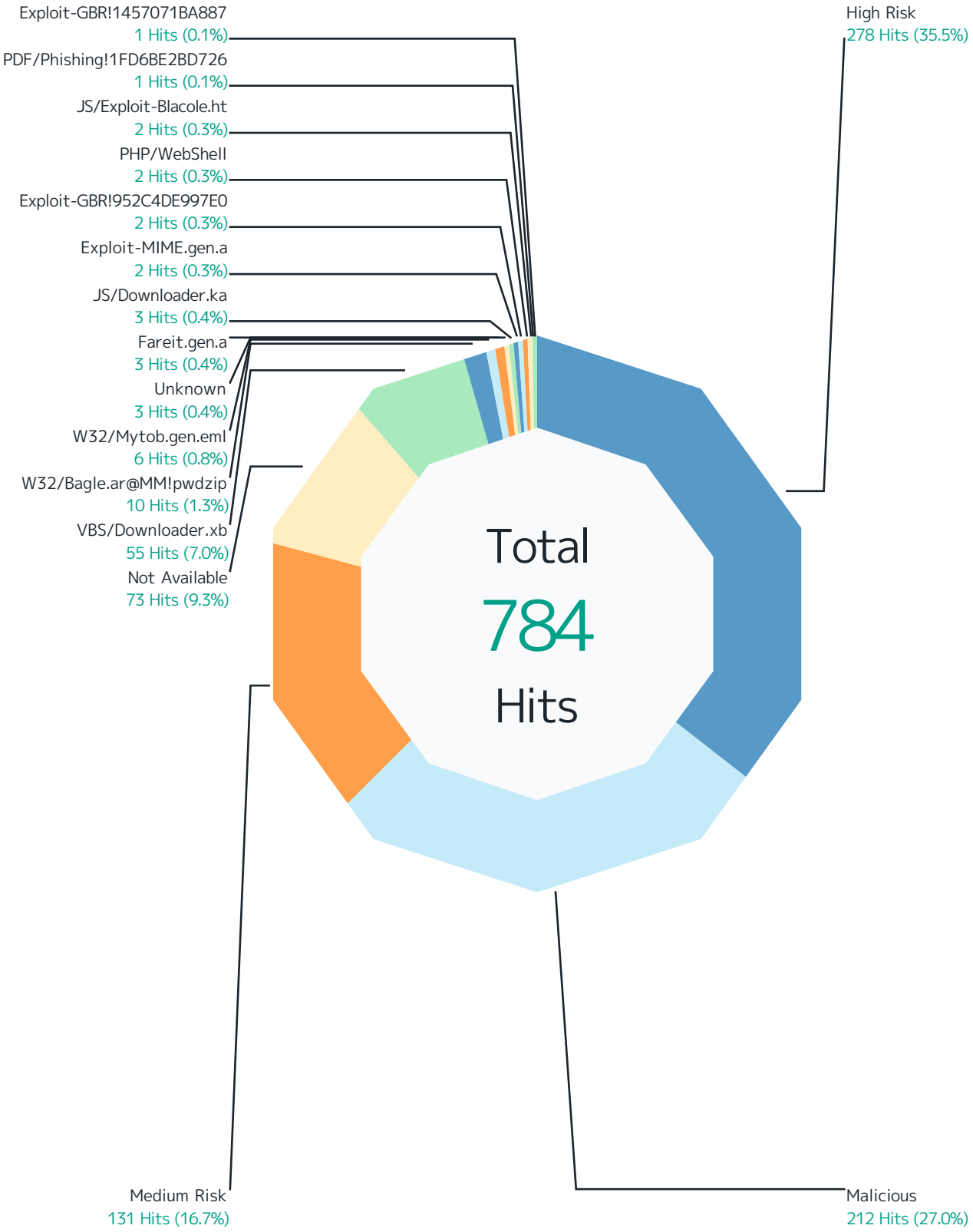
Virenfilterung MXe



Records by file name	Hits	%
DHL# 5663524930.IMG	95	13.8 %
Urgent-Order.pdf	63	9.1 %
foto_whatsapp_2025-03-31.img	59	8.6 %
Kostenrechnung v_ 17_04_2025.img	55	8.0 %
RFQ-10525-002 0NERK.docx	40	5.8 %
foto_whatsapp_2025-04-06.img	39	5.7 %
Payment Copy_ PO_No.AEONCHEM2025-25007.zip	14	2.0 %
RFQ#290425.docx	13	1.9 %
DHL Express_00467983321.gz	13	1.9 %
<Name Unavailable>	11	1.6 %
Shipment Documents.docx	9	1.3 %
proof of payments.xlsx	8	1.2 %
EKOLUKA-A-OKLUC20250.docx	8	1.2 %
SUCBIKE9078.tar	8	1.2 %
PO-PGT-25-030095-147_pdf.gz	7	1.0 %
Erstellen Sie Ihren Code fur MasterCard SecureCode oder Verified byVISA.html	6	0.9 %
MARCH Hemovigilance report.rar	6	0.9 %
590-4102025-IP.rar	6	0.9 %
COMPROVATIVO SB2.07.10.xlam	6	0.9 %
New order PO 23-178.xls	5	0.7 %
Shipment Document.docx	5	0.7 %
litdnntdneueviamunrueao.zip	4	0.6 %
justificante de pago..rar	4	0.6 %
Erstellen Sie Ihren Code fur MasterCard SecureCode oder Verified byVISA .zip	4	0.6 %
Order No. 20250409-70611 of 04092025.gz	4	0.6 %
PP-503-472-200.HTML	4	0.6 %
PI-003-2024-AWG-BK.docx	3	0.4 %
PO9657444.docx	3	0.4 %
New Inquiry.rar	3	0.4 %
NPI-Approved.rar	3	0.4 %
Others	181	26.3 %
Total	**689**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.

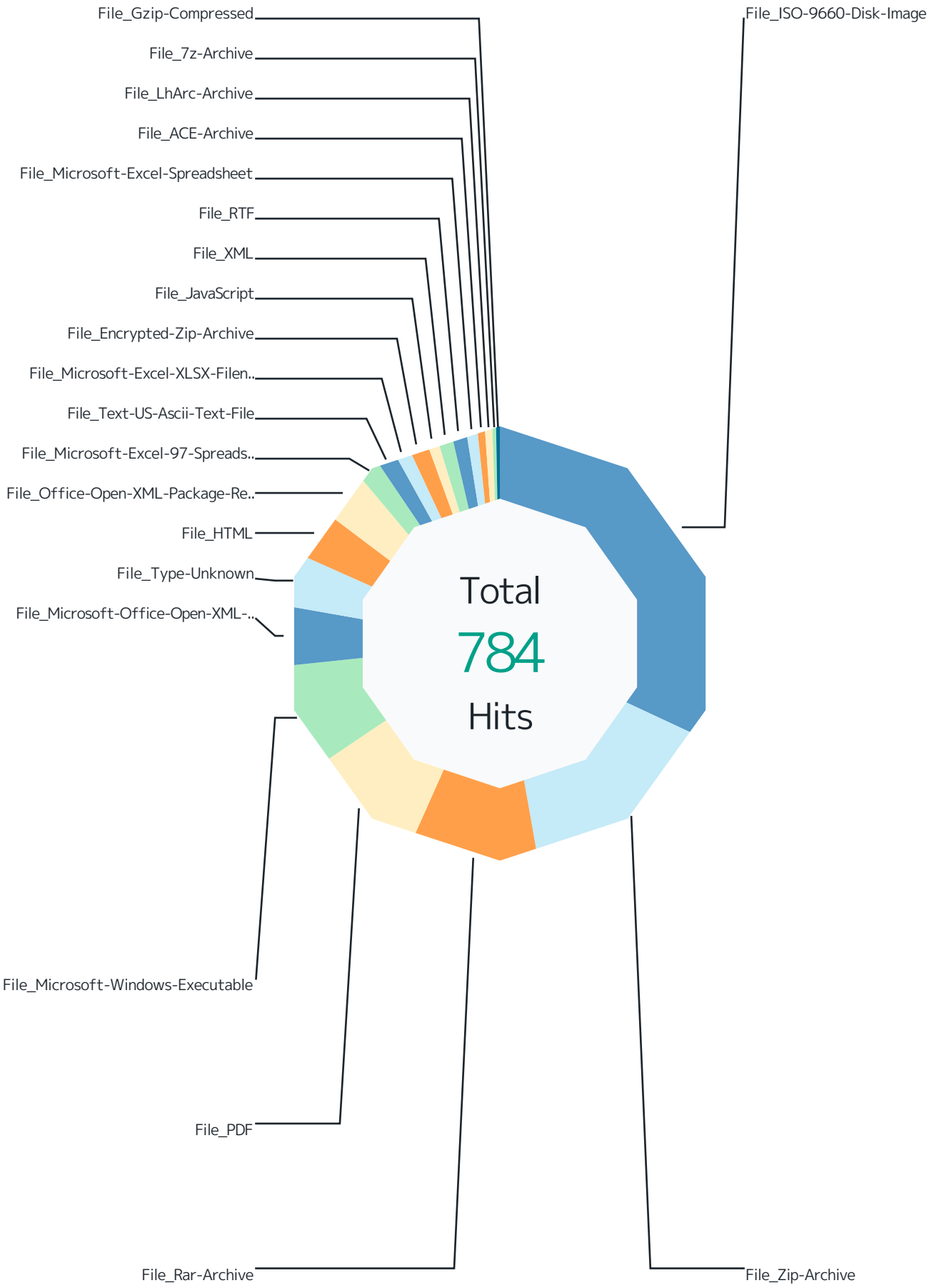

Exploit-GBR!1457071BA887
1 Hits (0.1%)
PDF/Phishing!1FD6BE2BD726
1 Hits (0.1%)
JS/Exploit-Blacole.ht
2 Hits (0.3%)
PHP/WebShell
2 Hits (0.3%)
Exploit-GBR!952C4DE997E0
2 Hits (0.3%)
Exploit-MIME.gen.a
2 Hits (0.3%)
JS/Downloader.ka
3 Hits (0.4%)
Fareit.gen.a
3 Hits (0.4%)
Unknown
3 Hits (0.4%)
W32/Mytob.gen.eml
6 Hits (0.8%)
W32/Bagle.ar@MM!pwdzip
10 Hits (1.3%)
VBS/Downloader.xb
55 Hits (7.0%)
Not Available
73 Hits (9.3%)
High Risk
278 Hits (35.5%)
Total
784
Hits
Medium Risk
131 Hits (16.7%)
Malicious
212 Hits (27.0%)

Scan Result	Hits	%
High Risk	**278**	**35.5 %**
File_ISO-9660-Disk-Image	163	20.8 %
File_PDF	66	8.4 %
File_Office-Open-XML-Package-Relations-Item	20	2.6 %
File_Rar-Archive	14	1.8 %
File_RTF	5	0.6 %
File_HTML	4	0.5 %
File_Microsoft-Windows-Executable	3	0.4 %
File_Zip-Archive	1	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %
File_Type-Unknown	1	0.1 %
Malicious	**212**	**27.0 %**
File_Rar-Archive	60	7.7 %
File_Microsoft-Windows-Executable	43	5.5 %
File_Type-Unknown	30	3.8 %
File_Zip-Archive	19	2.4 %
File_HTML	17	2.2 %
File_Microsoft-Excel-97-Spreadsheet	10	1.3 %
File_Microsoft-Office-Open-XML-Document	8	1.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.6 %
File_JavaScript	4	0.5 %
File_LhArc-Archive	4	0.5 %
File_RTF	3	0.4 %
File_PDF	2	0.3 %
File_Text-US-Ascii-Text-File	2	0.3 %
File_Microsoft-Excel-Spreadsheet	2	0.3 %
File_ACE-Archive	2	0.3 %
File_ISO-9660-Disk-Image	1	0.1 %
Medium Risk	**131**	**16.7 %**
File_Zip-Archive	47	6.0 %
File_ISO-9660-Disk-Image	32	4.1 %
File_Microsoft-Windows-Executable	15	1.9 %
File_HTML	8	1.0 %
File_Office-Open-XML-Package-Relations-Item	8	1.0 %
File_XML	8	1.0 %
File_Microsoft-Office-Open-XML-Document	4	0.5 %
File_Microsoft-Excel-97-Spreadsheet	3	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.3 %
File_JavaScript	2	0.3 %

Scan Result	Hits	%
File_Rar-Archive	1	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.1 %
Not Available	**73**	**9.3 %**
File_Zip-Archive	49	6.3 %
File_Microsoft-Office-Open-XML-Document	21	2.7 %
File_Microsoft-Excel-Spreadsheet	3	0.4 %
VBS/Downloader.xb	**55**	**7.0 %**
File_ISO-9660-Disk-Image	55	7.0 %
W32/Bagle.ar@MM!pwdzip	**10**	**1.3 %**
File_Encrypted-Zip-Archive	10	1.3 %
W32/Mytob.gen.eml	**6**	**0.8 %**
File_Text-US-Ascii-Text-File	6	0.8 %
Unknown	**3**	**0.4 %**
File_Zip-Archive	3	0.4 %
Fareit.gen.a	**3**	**0.4 %**
File_ACE-Archive	3	0.4 %
JS/Downloader.ka	**3**	**0.4 %**
File_7z-Archive	3	0.4 %
Exploit-MIME.gen.a	**2**	**0.3 %**
File_Text-US-Ascii-Text-File	2	0.3 %
Exploit-GBR!952C4DE997E0	**2**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.3 %
PHP/WebShell	**2**	**0.3 %**
File_Gzip-Compressed	2	0.3 %
JS/Exploit-Blacole.ht	**2**	**0.3 %**
File_JavaScript	2	0.3 %
PDF/Phishing!1FD6BE2BD726	**1**	**0.1 %**
File_PDF	1	0.1 %
Exploit-GBR!1457071BA887	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
Total	**784**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

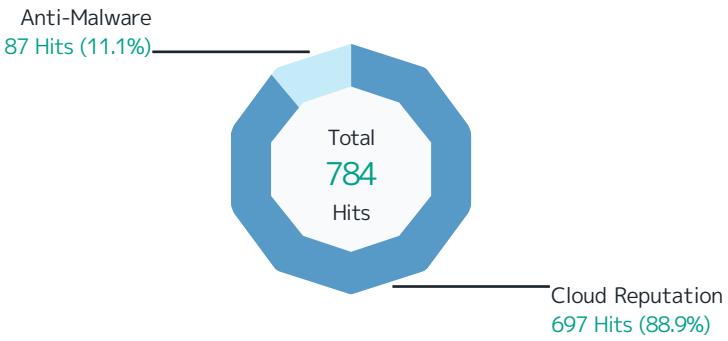

File_Gzip-Compressed
File_7z-Archive
File_LhArc-Archive
File_ACE-Archive
File_Microsoft-Excel-Spreadsheet
File_RTF
File_XML
File_JavaScript
File_Encrypted-Zip-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Text-US-Ascii-Text-File
File_Microsoft-Excel-97-Spreads..
File_Office-Open-XML-Package-Re..
File_HTML
File_Type-Unknown
File_Microsoft-Office-Open-XML-..
File_Microsoft-Windows-Executable
File_PDF
File_Rar-Archive
File_ISO-9660-Disk-Image
File_Zip-Archive
Total
784
Hits

Responding Scanner	Hits	%
File_ISO-9660-Disk-Image	**251**	**32.0 %**
High Risk	163	20.8 %
VBS/Downloader.xb	55	7.0 %
Medium Risk	32	4.1 %
Malicious	1	0.1 %
File_Zip-Archive	**119**	**15.2 %**
Not Available	49	6.3 %
Medium Risk	47	6.0 %
Malicious	19	2.4 %
Unknown	3	0.4 %
High Risk	1	0.1 %
File_Rar-Archive	**75**	**9.6 %**
Malicious	60	7.7 %
High Risk	14	1.8 %
Medium Risk	1	0.1 %
File_PDF	**69**	**8.8 %**
High Risk	66	8.4 %
Malicious	2	0.3 %
PDF/Phishing!1FD6BE2BD726	1	0.1 %
File_Microsoft-Windows-Executable	**61**	**7.8 %**
Malicious	43	5.5 %
Medium Risk	15	1.9 %
High Risk	3	0.4 %
File_Microsoft-Office-Open-XML-Document	**34**	**4.3 %**
Not Available	21	2.7 %
Malicious	8	1.0 %
Medium Risk	4	0.5 %
High Risk	1	0.1 %
File_Type-Unknown	**31**	**4.0 %**
Malicious	30	3.8 %
High Risk	1	0.1 %
File_HTML	**29**	**3.7 %**
Malicious	17	2.2 %
Medium Risk	8	1.0 %
High Risk	4	0.5 %
File_Office-Open-XML-Package-Relations-Item	**28**	**3.6 %**
High Risk	20	2.6 %
Medium Risk	8	1.0 %
File_Microsoft-Excel-97-Spreadsheet	**13**	**1.7 %**

Responding Scanner	Hits	%
Malicious	10	1.3 %
Medium Risk	3	0.4 %
File_Text-US-Ascii-Text-File	**10**	**1.3 %**
W32/Mytob.gen.eml	6	0.8 %
Malicious	2	0.3 %
Exploit-MIME.gen.a	2	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	**10**	**1.3 %**
Malicious	5	0.6 %
Medium Risk	2	0.3 %
Exploit-GBR!952C4DE997E0	2	0.3 %
Exploit-GBR!1457071BA887	1	0.1 %
File_Encrypted-Zip-Archive	**10**	**1.3 %**
W32/Bagle.ar@MM!pwdzip	10	1.3 %
File_JavaScript	**8**	**1.0 %**
Malicious	4	0.5 %
Medium Risk	2	0.3 %
JS/Exploit-Blacole.ht	2	0.3 %
File_XML	**8**	**1.0 %**
Medium Risk	8	1.0 %
File_RTF	**8**	**1.0 %**
High Risk	5	0.6 %
Malicious	3	0.4 %
File_Microsoft-Excel-Spreadsheet	**6**	**0.8 %**
Not Available	3	0.4 %
Malicious	2	0.3 %
Medium Risk	1	0.1 %
File_ACE-Archive	**5**	**0.6 %**
Fareit.gen.a	3	0.4 %
Malicious	2	0.3 %
File_LhArc-Archive	**4**	**0.5 %**
Malicious	4	0.5 %
File_7z-Archive	**3**	**0.4 %**
JS/Downloader.ka	3	0.4 %
File_Gzip-Compressed	**2**	**0.3 %**
PHP/WebShell	2	0.3 %
Total	**784**	**100 %**

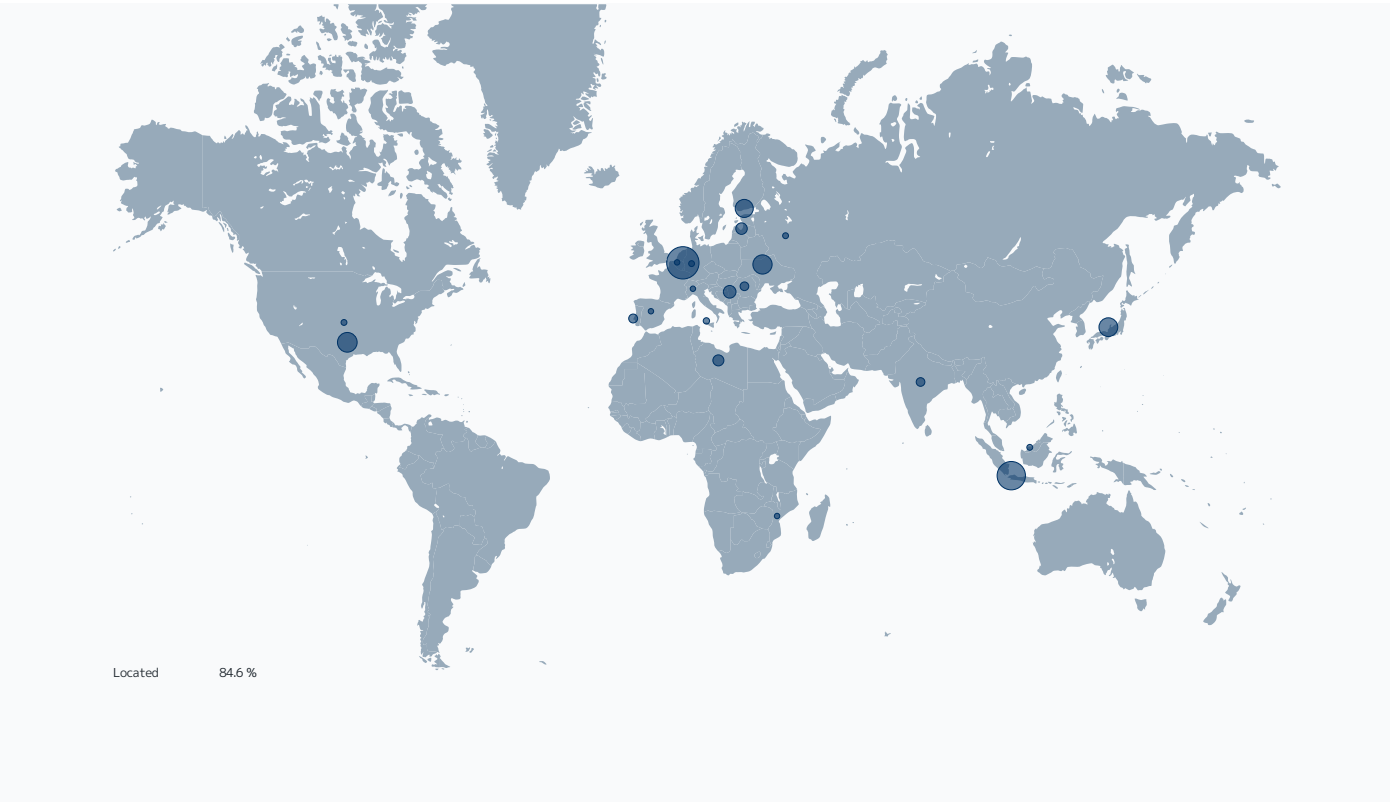
Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**697**	**88.9 %**
File_ISO-9660-Disk-Image	196	25.0 %
File_Zip-Archive	119	15.2 %
File_Rar-Archive	75	9.6 %
File_PDF	68	8.7 %
File_Microsoft-Windows-Executable	61	7.8 %
File_Microsoft-Office-Open-XML-Document	34	4.3 %
File_Type-Unknown	31	4.0 %
File_HTML	29	3.7 %
File_Office-Open-XML-Package-Relations-Item	28	3.6 %
File_Microsoft-Excel-97-Spreadsheet	13	1.7 %
File_XML	8	1.0 %
File_RTF	8	1.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	7	0.9 %
File_JavaScript	6	0.8 %
File_Microsoft-Excel-Spreadsheet	6	0.8 %
File_LhArc-Archive	4	0.5 %
File_Text-US-Ascii-Text-File	2	0.3 %
File_ACE-Archive	2	0.3 %
Anti-Malware	**87**	**11.1 %**
File_ISO-9660-Disk-Image	55	7.0 %
File_Encrypted-Zip-Archive	10	1.3 %
File_Text-US-Ascii-Text-File	8	1.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.4 %
File_ACE-Archive	3	0.4 %
File_7z-Archive	3	0.4 %
File_JavaScript	2	0.3 %
File_Gzip-Compressed	2	0.3 %
File_PDF	1	0.1 %
Total	**784**	**100 %**

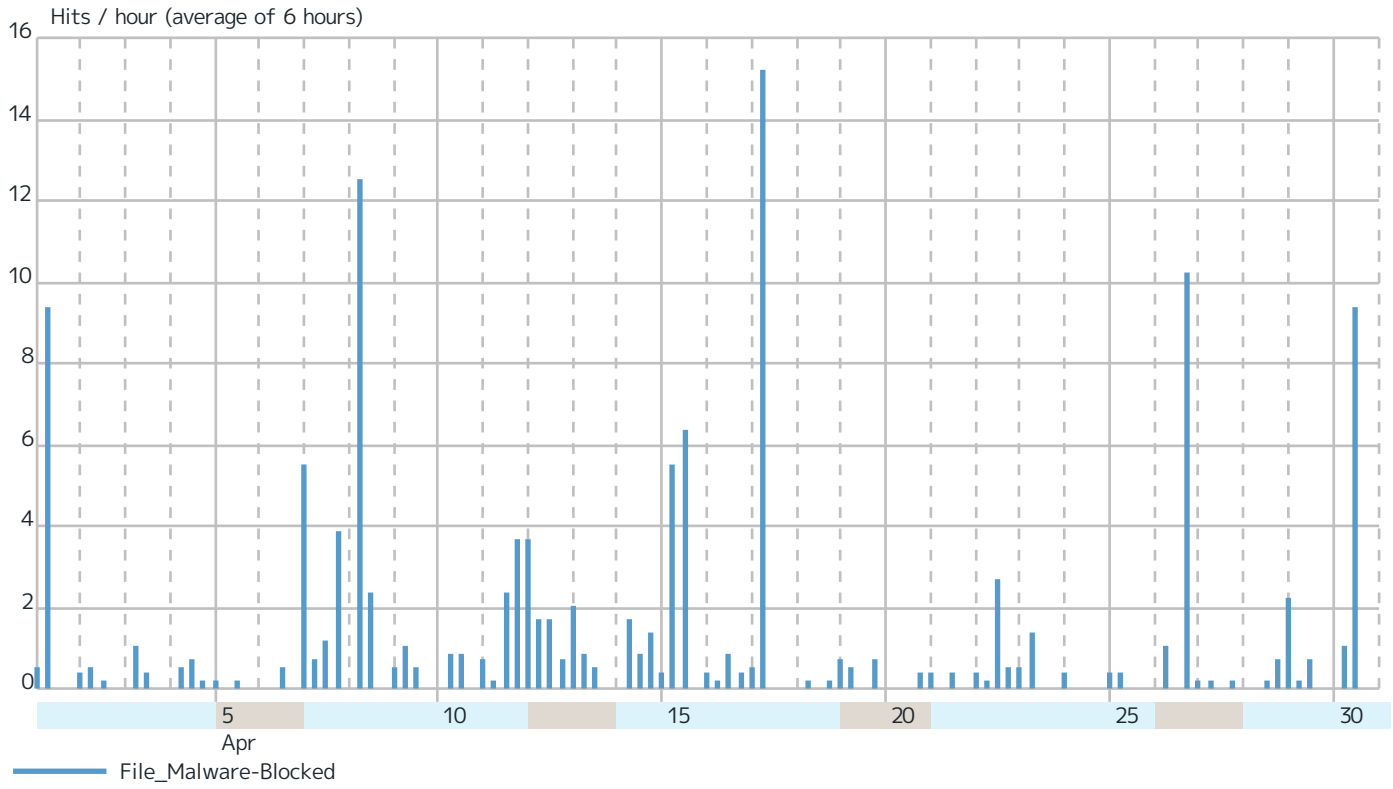
Virenfilterung SRC IPs



Records by src IP		Hits	%
103.102.0.11	Indonesia	96	12.2 %
114.142.191.85	Kanazawa, Japan	61	7.8 %
65.109.110.12	Helsinki, Finland	58	7.4 %
79.141.173.38	Dallas, Texas 75270, United States	57	7.3 %
195.160.220.213	Ukraine	55	7.0 %
2a00:8a60:1:12:4a11:d7d3:4454:270c	RWTH Aachen	54	6.9 %
2a00:8a60:1:11::100c	RWTH Aachen	51	6.5 %
195.123.210.36	Riga, Latvia	30	3.8 %
46.240.128.16	Belgrade, Serbia	28	3.6 %
41.208.70.32	Libya	28	3.6 %
176.61.148.97	Portugal	19	2.4 %
89.35.6.228	Romania	14	1.8 %
103.109.7.24	India	12	1.5 %
2a00:8a60:1:11::1007	RWTH Aachen	10	1.3 %
91.124.130.187	Dallas, Texas 75270, United States	8	1.0 %
45.86.231.220	Palermo, Italy	8	1.0 %
195.191.25.136	Ukraine	8	1.0 %
217.24.17.51	Belgrade, Serbia	7	0.9 %
160.187.54.64	India	6	0.8 %
178.255.127.159	Russia	6	0.8 %
43.252.212.55	Malaysia	6	0.8 %
70.39.234.137	United States	6	0.8 %
117.102.252.140	Indonesia	6	0.8 %
195.63.103.234	Großen Buseck, Germany	6	0.8 %
158.58.172.215	Milan, Italy	4	0.5 %
188.164.198.140	Spain	4	0.5 %
89.45.194.41	Romania	4	0.5 %
185.235.138.62	Brussels, Belgium	4	0.5 %
2a00:8a60:1:12:c1a2:d4cd:c6ed:f690	RWTH Aachen	4	0.5 %
41.223.152.25	Mozambique	4	0.5 %
Others		121	15.4 %
Total		**785**	**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.