Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-06-01 00:00:00+0200
To: 2024-07-01 00:00:00+0200

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.3, build 11429

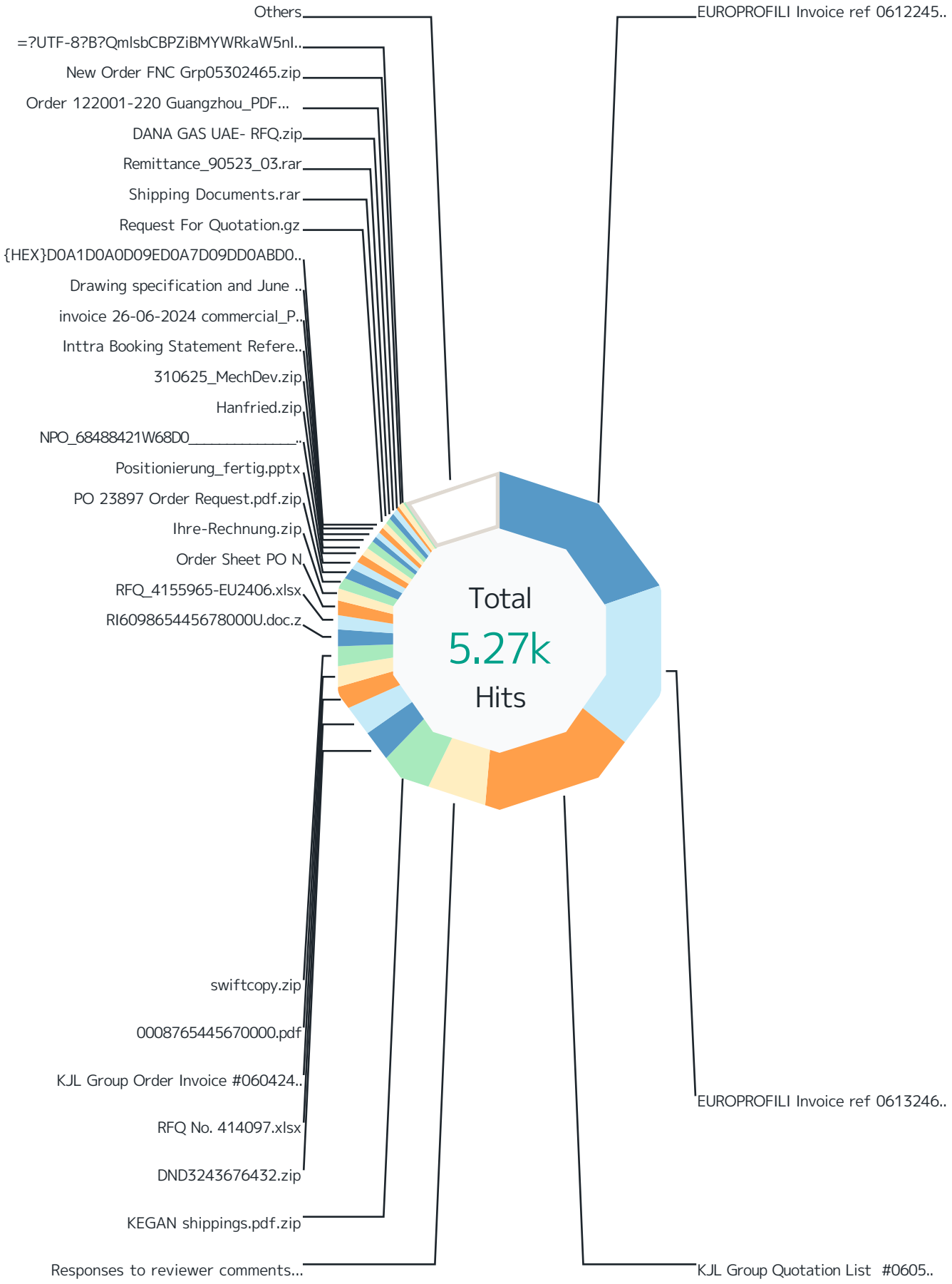
Update version
1746

Report started
2024-07-01 12:27:05+0200

Report run time
03:00:51

Filters used
Match All

Virenfilterung MXe



Records by file name	Hits	%
EUROPROFILI Invoice ref 06122456.zip	1.04k	19.7 %
EUROPROFILI Invoice ref 06132467.zip	858	16.3 %
KJL Group Quotation List #060524768.zip	816	15.5 %
Responses to reviewer comments.docx	310	5.9 %
KEGAN shippings.pdf.zip	253	4.8 %
DND3243676432.zip	167	3.2 %
RFQ No. 414097.xlsx	156	3.0 %
KJL Group Order Invoice #06042436.zip	124	2.4 %
0008765445670000.pdf	104	2.0 %
swiftcopy.zip	100	1.9 %
RI609865445678000U.doc.z	93	1.8 %
RFQ_4155965-EU2406.xlsx	71	1.3 %
Order Sheet PO N	67	1.3 %
Ihre-Rechnung.zip	64	1.2 %
PO 23897 Order Request.pdf.zip	58	1.1 %
Positionierung_fertig.pptx	54	1.0 %
NPO_68488421W68D0_____.LZH	50	0.9 %
Hanfried.zip	43	0.8 %
310625_MechDev.zip	41	0.8 %
Inttra Booking Statement Reference Number #2024604085.zip	40	0.8 %
invoice 26-06-2024 commercial_PDF.zip	34	0.6 %
Drawing specification and June PO #07329.tar	32	0.6 %
{HEX}D0A1D0A0D09ED0A7D09DD0ABD09920D097D0	31	0.6 %
Request For Quotation.gz	30	0.6 %
Shipping Documents.rar	27	0.5 %
Remittance_90523_03.rar	25	0.5 %
DANA GAS UAE- RFQ.zip	23	0.4 %
Order 122001-220 Guangzhou_PDF.zip	22	0.4 %
New Order FNC Grp05302465.zip	22	0.4 %
=?UTF-8?B?QmlsbCBPZiBMYWRkaW5nIENvcHkuaHRtbA==?=	20	0.4 %
Others	498	9.5 %
Total	**5.27k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.


Total
9.96k
Hits

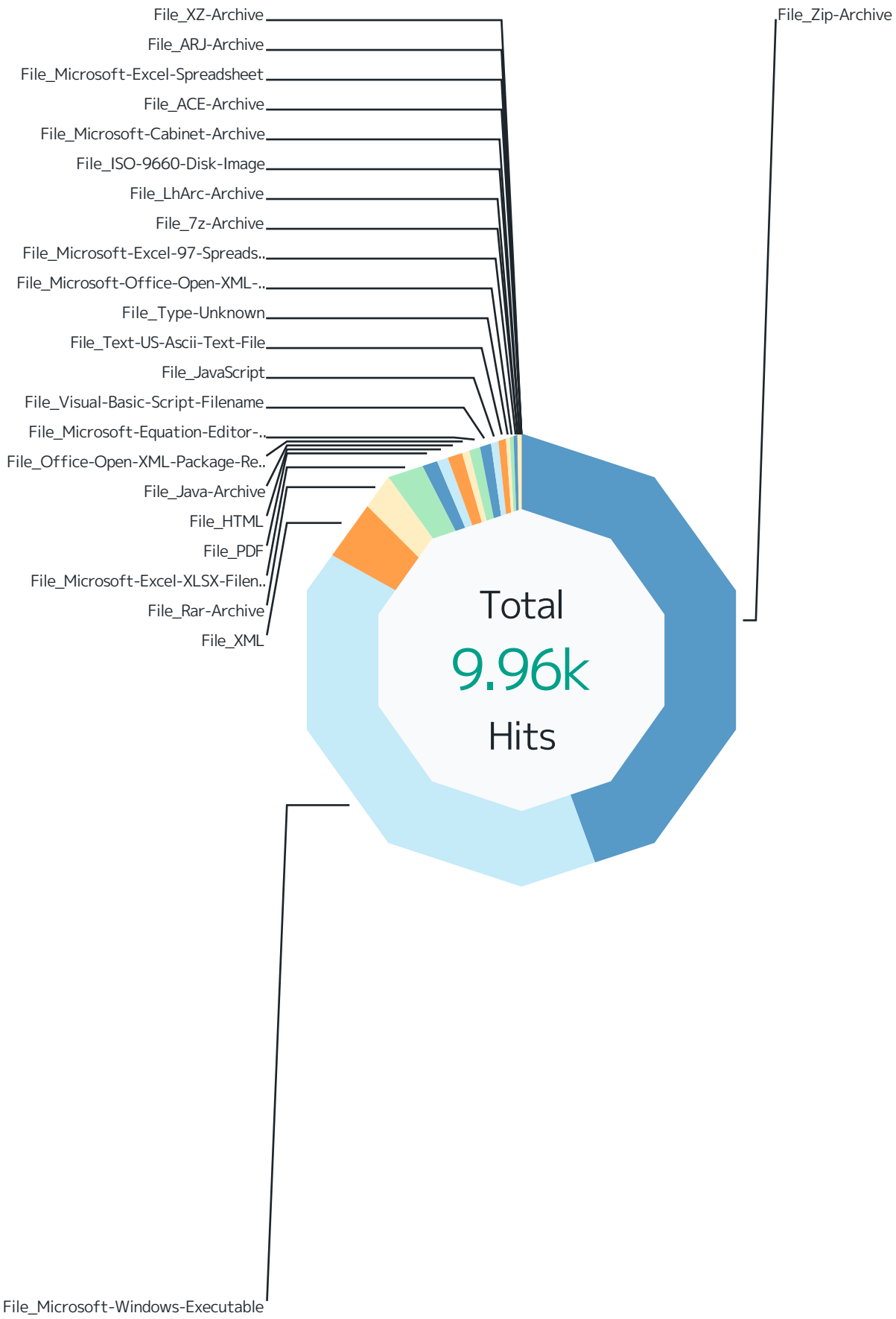
Scan Result	Hits	%
Malicious	**4.62k**	**46.4 %**
File_Microsoft-Windows-Executable	3.70k	37.1 %
File_Zip-Archive	414	4.2 %
File_Rar-Archive	215	2.2 %
File_PDF	106	1.1 %
File_Visual-Basic-Script-Filename	71	0.7 %
File_Microsoft-Excel-97-Spreadsheet	23	0.2 %
File_HTML	22	0.2 %
File_Type-Unknown	19	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	15	0.2 %
File_7z-Archive	8	0.1 %
File_LhArc-Archive	7	0.1 %
File_ISO-9660-Disk-Image	6	0.1 %
File_Microsoft-Cabinet-Archive	5	0.1 %
File_Text-US-Ascii-Text-File	3	0.0 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
File_Java-Archive	2	0.0 %
File_ACE-Archive	2	0.0 %
File_JavaScript	1	0.0 %
File_ARJ-Archive	1	0.0 %
File_XZ-Archive	1	0.0 %
Not Available	**4.17k**	**41.9 %**
File_Zip-Archive	3.93k	39.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	221	2.2 %
File_Microsoft-Office-Open-XML-Document	18	0.2 %
Medium Risk	**775**	**7.8 %**
File_XML	428	4.3 %
File_Microsoft-Windows-Executable	154	1.5 %
File_Java-Archive	84	0.8 %
File_Office-Open-XML-Package-Relations-Item	61	0.6 %
File_Text-US-Ascii-Text-File	38	0.4 %
File_PDF	7	0.1 %
File_Rar-Archive	2	0.0 %
File_Type-Unknown	1	0.0 %
High Risk	**164**	**1.6 %**
File_Microsoft-Equation-Editor-Document	75	0.8 %
File_JavaScript	64	0.6 %
File_Office-Open-XML-Package-Relations-Item	16	0.2 %
File_Type-Unknown	6	0.1 %

Scan Result	Hits	%
File_Rar-Archive	2	0.0 %
File_7z-Archive	1	0.0 %
Unknown	**91**	**0.9 %**
File_Zip-Archive	86	0.9 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
HTML/Phishing.vf	**30**	**0.3 %**
File_HTML	30	0.3 %
BAT/Dropper.l	**17**	**0.2 %**
File_Rar-Archive	14	0.1 %
File_Zip-Archive	1	0.0 %
File_Type-Unknown	1	0.0 %
File_7z-Archive	1	0.0 %
HTML/Phishing.ta	**15**	**0.2 %**
File_HTML	15	0.2 %
HTML/Phishing.vy	**15**	**0.2 %**
File_Text-US-Ascii-Text-File	15	0.2 %
AgentTesla-FDKB!EB0369D72BBE	**13**	**0.1 %**
File_Rar-Archive	13	0.1 %
HTML/Phishing.rb	**7**	**0.1 %**
File_HTML	7	0.1 %
AgentTesla-FDKB!D943C20F62D2	**5**	**0.1 %**
File_Rar-Archive	5	0.1 %
HTML/Phishing.wb	**5**	**0.1 %**
File_HTML	5	0.1 %
AgentTesla-FDUP!D8E8E474972D	**5**	**0.1 %**
File_Rar-Archive	5	0.1 %
RDN/Generic.dx	**4**	**0.0 %**
File_PDF	4	0.0 %
AgentTesla-FDUP!4B627853343E	**3**	**0.0 %**
File_Rar-Archive	3	0.0 %
AgentTesla-FDUP!30F8C5E5D64F	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
Fareit.gen.e	**2**	**0.0 %**
File_ACE-Archive	2	0.0 %
HTML/Phishing.ok	**2**	**0.0 %**
File_HTML	2	0.0 %
Exploit-GBT!3DF22A53F9EF	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %

Scan Result	Hits	%
HTML/Phishing.vq	**2**	**0.0 %**
File_HTML	2	0.0 %
PDF/Phishing.gen.u	**1**	**0.0 %**
File_PDF	1	0.0 %
HTML/Phishing.vb	**1**	**0.0 %**
File_HTML	1	0.0 %
Exploit-GBT!093747FDC040	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.cx	**1**	**0.0 %**
File_HTML	1	0.0 %
AgentTesla-FDUP!1A0560F13B44	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Exploit-GBT!CB33A99E7CEA	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.wd	**1**	**0.0 %**
File_HTML	1	0.0 %
Trojan-FVJV!A46A3492163D	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
Total	**9.96k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.


File_XZ-Archive
File_ARJ-Archive
File_Microsoft-Excel-Spreadsheet
File_ACE-Archive
File_Microsoft-Cabinet-Archive
File_ISO-9660-Disk-Image
File_LhArc-Archive
File_7z-Archive
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Office-Open-XML-..
File_Type-Unknown
File_Text-US-Ascii-Text-File
File_JavaScript
File_Visual-Basic-Script-Filename
File_Microsoft-Equation-Editor-..
File_Office-Open-XML-Package-Re..
File_Java-Archive
File_HTML
File_PDF
File_Microsoft-Excel-XLSX-Filen..
File_Rar-Archive
File_XML
File_Zip-Archive
Total
9.96k
Hits
File_Microsoft-Windows-Executable

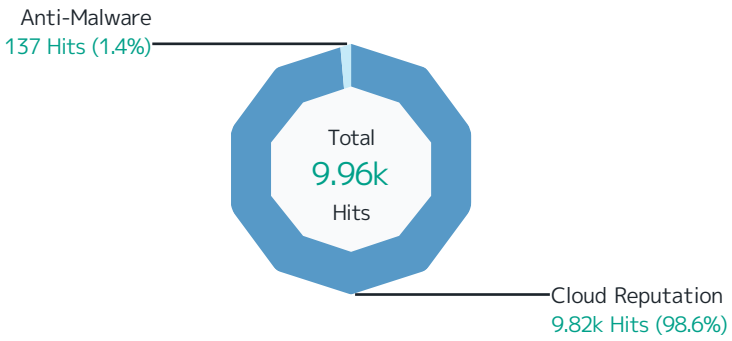
Responding Scanner	Hits	%
File_Zip-Archive	**4.43k**	**44.5 %**
Not Available	3.93k	39.5 %
Malicious	414	4.2 %
Unknown	86	0.9 %
BAT/Dropper.I	1	0.0 %
Trojan-FVJV!A46A3492163D	1	0.0 %
File_Microsoft-Windows-Executable	**3.85k**	**38.7 %**
Malicious	3.70k	37.1 %
Medium Risk	154	1.5 %
File_XML	**428**	**4.3 %**
Medium Risk	428	4.3 %
File_Rar-Archive	**262**	**2.6 %**
Malicious	215	2.2 %
BAT/Dropper.I	14	0.1 %
AgentTesla-FDKB!EB0369D72BBE	13	0.1 %
AgentTesla-FDKB!D943C20F62D2	5	0.1 %
AgentTesla-FDUP!D8E8E474972D	5	0.1 %
AgentTesla-FDUP!4B627853343E	3	0.0 %
Medium Risk	2	0.0 %
High Risk	2	0.0 %
AgentTesla-FDUP!30F8C5E5D64F	2	0.0 %
AgentTesla-FDUP!1A0560F13B44	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**240**	**2.4 %**
Not Available	221	2.2 %
Malicious	15	0.2 %
Unknown	2	0.0 %
Exploit-GBT!3DF22A53F9EF	2	0.0 %
File_PDF	**118**	**1.2 %**
Malicious	106	1.1 %
Medium Risk	7	0.1 %
RDN/Generic.dx	4	0.0 %
PDF/Phishing.gen.u	1	0.0 %
File_HTML	**86**	**0.9 %**
HTML/Phishing.vf	30	0.3 %
Malicious	22	0.2 %
HTML/Phishing.ta	15	0.2 %
HTML/Phishing.rb	7	0.1 %
HTML/Phishing.wb	5	0.1 %
HTML/Phishing.ok	2	0.0 %

Responding Scanner	Hits	%
HTML/Phishing.vq	2	0.0 %
HTML/Phishing.vb	1	0.0 %
HTML/Phishing.cx	1	0.0 %
HTML/Phishing.wd	1	0.0 %
File_Java-Archive	**86**	**0.9 %**
Medium Risk	84	0.8 %
Malicious	2	0.0 %
File_Office-Open-XML-Package-Relations-Item	**77**	**0.8 %**
Medium Risk	61	0.6 %
High Risk	16	0.2 %
File_Microsoft-Equation-Editor-Document	**75**	**0.8 %**
High Risk	75	0.8 %
File_Visual-Basic-Script-Filename	**71**	**0.7 %**
Malicious	71	0.7 %
File_JavaScript	**65**	**0.7 %**
High Risk	64	0.6 %
Malicious	1	0.0 %
File_Text-US-Ascii-Text-File	**56**	**0.6 %**
Medium Risk	38	0.4 %
HTML/Phishing.vy	15	0.2 %
Malicious	3	0.0 %
File_Type-Unknown	**27**	**0.3 %**
Malicious	19	0.2 %
High Risk	6	0.1 %
Medium Risk	1	0.0 %
BAT/Dropper.I	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**24**	**0.2 %**
Not Available	18	0.2 %
Malicious	3	0.0 %
Unknown	3	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**23**	**0.2 %**
Malicious	23	0.2 %
File_7z-Archive	**10**	**0.1 %**
Malicious	8	0.1 %
High Risk	1	0.0 %
BAT/Dropper.I	1	0.0 %
File_LhArc-Archive	**7**	**0.1 %**
Malicious	7	0.1 %
File_ISO-9660-Disk-Image	**6**	**0.1 %**

Responding Scanner	Hits	%
Malicious	6	0.1 %
File_Microsoft-Cabinet-Archive	**5**	**0.1 %**
Malicious	5	0.1 %
File_ACE-Archive	**4**	**0.0 %**
Malicious	2	0.0 %
Fareit.gen.e	2	0.0 %
File_Microsoft-Excel-Spreadsheet	**2**	**0.0 %**
Exploit-GBT!093747FDC040	1	0.0 %
Exploit-GBT!CB33A99E7CEA	1	0.0 %
File_ARJ-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_XZ-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**9.96k**	**100 %**

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



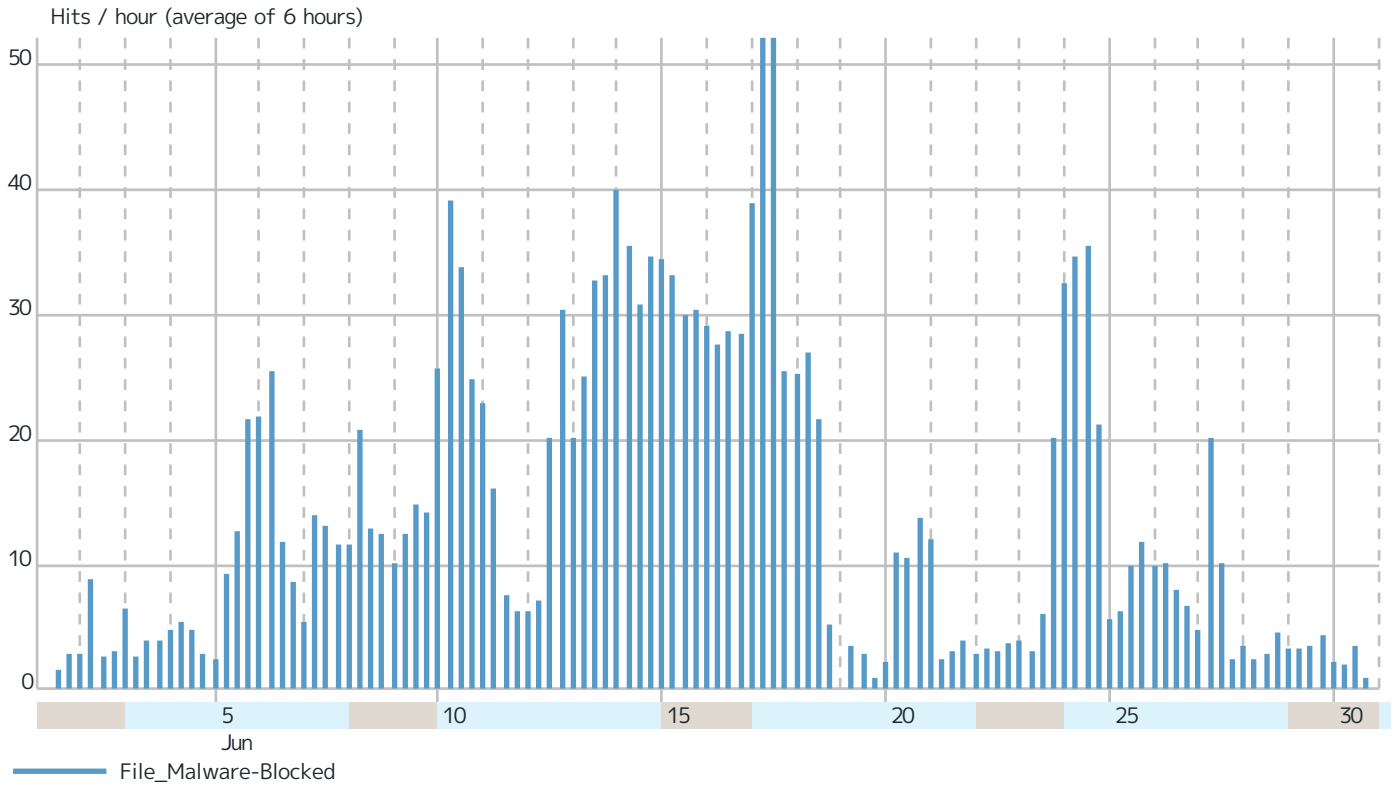
Responding Scanner	Hits	%
Cloud Reputation	**9.82k**	**98.6 %**
File_Zip-Archive	4.43k	44.5 %
File_Microsoft-Windows-Executable	3.85k	38.7 %
File_XML	428	4.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	238	2.4 %
File_Rar-Archive	219	2.2 %
File_PDF	113	1.1 %
File_Java-Archive	86	0.9 %
File_Office-Open-XML-Package-Relations-Item	77	0.8 %
File_Microsoft-Equation-Editor-Document	75	0.8 %
File_Visual-Basic-Script-Filename	71	0.7 %
File_JavaScript	65	0.7 %
File_Text-US-Ascii-Text-File	41	0.4 %
File_Type-Unknown	26	0.3 %
File_Microsoft-Office-Open-XML-Document	24	0.2 %
File_Microsoft-Excel-97-Spreadsheet	23	0.2 %
File_HTML	22	0.2 %
File_7z-Archive	9	0.1 %
File_LhArc-Archive	7	0.1 %
File_ISO-9660-Disk-Image	6	0.1 %
File_Microsoft-Cabinet-Archive	5	0.1 %
File_ACE-Archive	2	0.0 %
File_ARJ-Archive	1	0.0 %
File_XZ-Archive	1	0.0 %
Anti-Malware	**137**	**1.4 %**
File_HTML	64	0.6 %
File_Rar-Archive	43	0.4 %
File_Text-US-Ascii-Text-File	15	0.2 %
File_PDF	5	0.1 %
File_Zip-Archive	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
File_ACE-Archive	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
File_Type-Unknown	1	0.0 %
File_7z-Archive	1	0.0 %
Total	**9.96k**	**100 %**

Virenfilterung SRC IPs

Records by src IP		Hits	%
45.117.79.99	Vietnam	5.50k	55.2 %
182.163.99.254	Dhaka, Bangladesh	506	5.1 %
46.227.62.50	Greece	466	4.7 %
85.13.149.67	Germany	334	3.4 %
190.202.40.82	Venezuela	310	3.1 %
77.92.102.18	Istanbul, Türkiye	290	2.9 %
51.195.149.60	France	204	2.0 %
45.11.59.27	Amherst, Massachusetts 01004, United States	134	1.3 %
23.21.224.96	Ashburn, Virginia 20149, United States	130	1.3 %
102.212.245.40	Nairobi, Kenya	116	1.2 %
194.25.134.85	Roding, Germany	86	0.9 %
194.25.134.18	Roding, Germany	82	0.8 %
81.169.162.214	Germany	82	0.8 %
31.24.41.224	Spain	62	0.6 %
104.168.144.158	United States	60	0.6 %
173.236.113.130	United States	48	0.5 %
31.192.236.70	Madrid, Spain	46	0.5 %
80.85.154.196	Russia	44	0.4 %
5.9.68.209	Giessen, Germany	44	0.4 %
64.188.23.84	Amsterdam, The Netherlands	30	0.3 %
122.53.22.245	San Fernando City, Philippines	25	0.3 %
210.64.103.54	Tainan City, Taiwan	24	0.2 %
108.163.195.26	United States	19	0.2 %
89.105.220.79	New Jersey, United States	18	0.2 %
209.59.151.195	United States	15	0.2 %
87.251.86.179	Russia	15	0.2 %
195.242.110.235	British Virgin Islands	15	0.2 %
213.61.254.52	Munich, Germany	14	0.1 %
202.128.0.121	Tamuning, 96913 Guam	14	0.1 %
190.119.72.105	Lima, Peru	13	0.1 %
Others		1.21k	12.2 %
Total		**9.96k**	**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.