Forcepoint FlexEdge Secure SD-WAN

E-Mail Virenfilterung Server Firewall

Report period
From: 2024-09-01 00:00:00+0200
To: 2024-10-01 00:00:00+0200

Forcepoint

Table of Contents

Report run by
jens

SD-WAN Manager Console version
7.1.4, build 11432

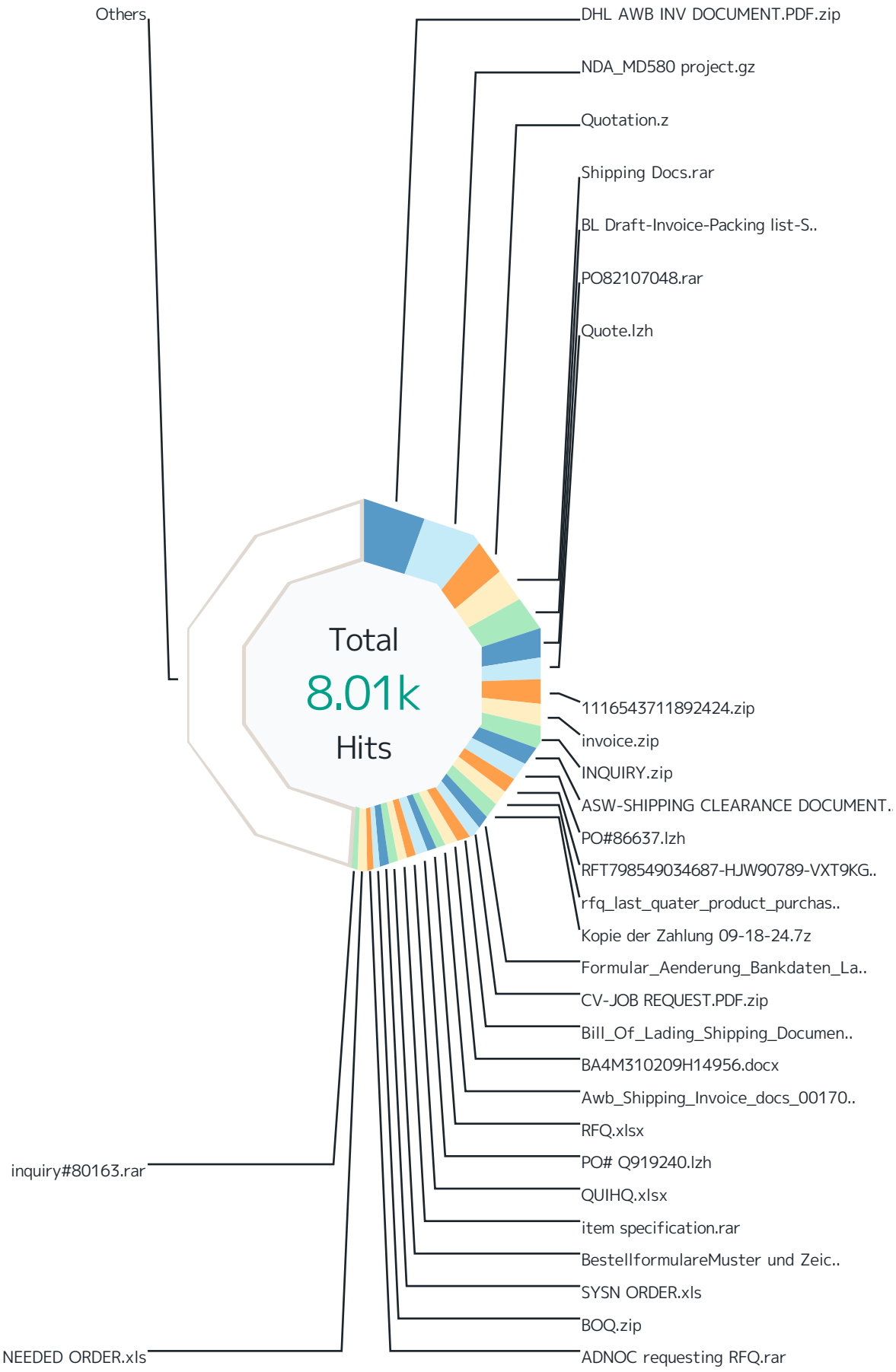
Update version
1783

Report started
2024-10-01 10:02:09+0200

Report run time
02:48:09

Filters used
Match All

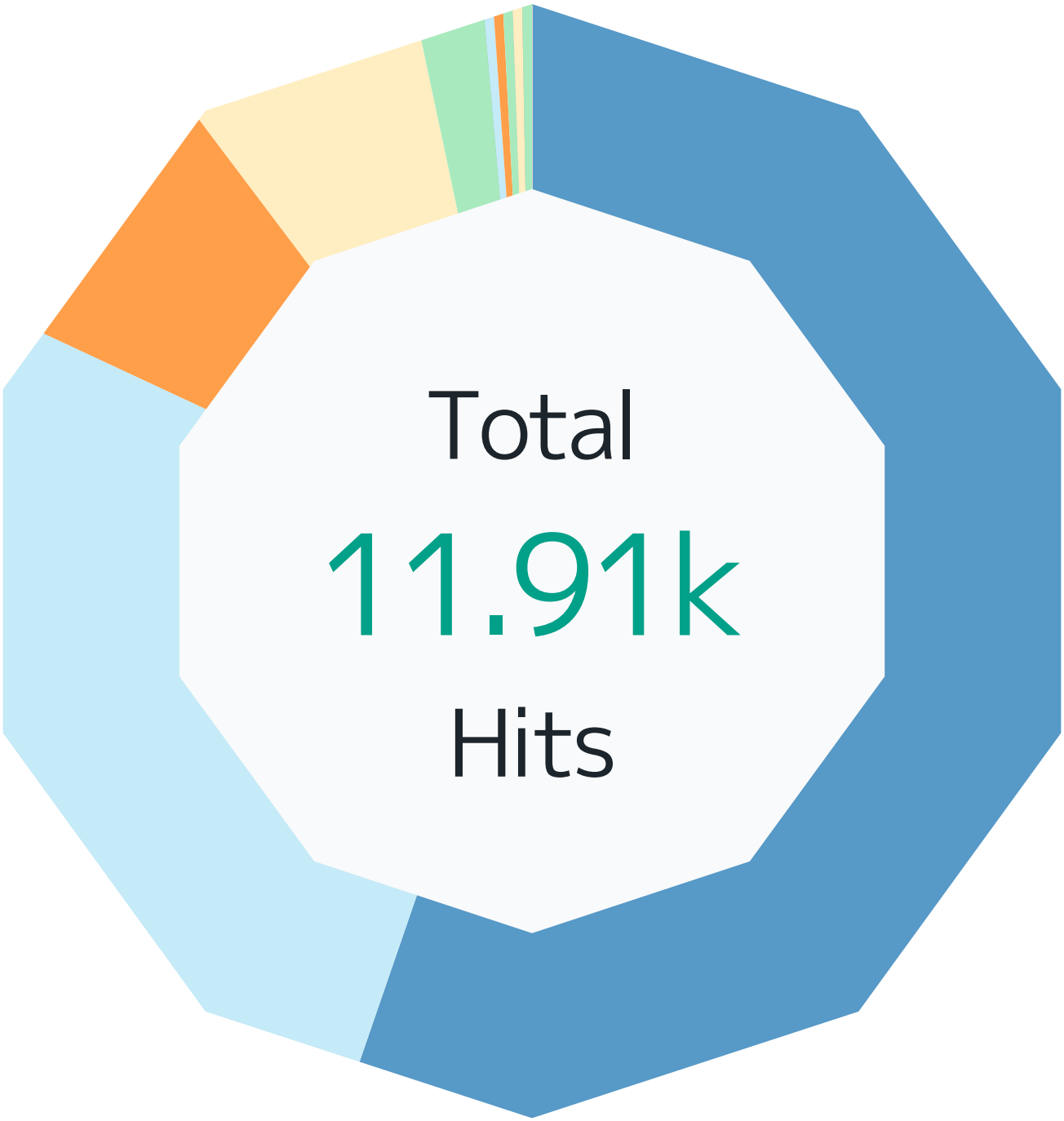
Virenfilterung MXe



Records by file name	Hits	%
DHL AWB INV DOCUMENT.PDF.zip	439	5.5 %
NDA_MD580 project.gz	429	5.4 %
Quotation.z	249	3.1 %
Shipping Docs.rar	248	3.1 %
BL Draft-Invoice-Packing list-Shipping Document.pif	245	3.1 %
PO82107048.rar	186	2.3 %
Quote.lzh	171	2.1 %
1116543711892424.zip	169	2.1 %
invoice.zip	163	2.0 %
INQUIRY.zip	151	1.9 %
ASW-SHIPPING CLEARANCE DOCUMENT 0382--0000.zip	138	1.7 %
PO#86637.lzh	129	1.6 %
RFT798549034687-HJW90789-VXT9KGUINUII.7z	118	1.5 %
rfq_last_quater_product_purchase_order_import_list_11_06_2024_0000001 10924.7z	110	1.4 %
Kopie der Zahlung 09-18-24.7z	108	1.3 %
Formular_Aenderung_Bankdaten_Lastschriftmandat (1).docx	87	1.1 %
CV-JOB REQUEST.PDF.zip	85	1.1 %
Bill_Of_Lading_Shipping_Documents_Invoice_Awb_CI_PL0000000000000000 00000.7z	84	1.0 %
BA4M310209H14956.docx	83	1.0 %
Awb_Shipping_Invoice_docs_00170072024224782002003180817 4CN18003170072024.gz	79	1.0 %
RFQ.xlsx	76	0.9 %
PO# Q919240.lzh	74	0.9 %
QUIHQ.xlsx	73	0.9 %
item specification.rar	68	0.8 %
BestellformulareMuster und Zeichnungen_pdf.7z	62	0.8 %
SYSN ORDER.xls	57	0.7 %
BOQ.zip	55	0.7 %
ADNOC requesting RFQ.rar	54	0.7 %
NEEDED ORDER.xls	53	0.7 %
inquiry#80163.rar	48	0.6 %
Others	3.92k	48.9 %
Total	**8.01k**	**100 %**

Top File Types by Scan Result

Top 10 file types by scan result.


Total
11.91k
Hits

Scan Result	Hits	%
Malicious	**6.58k**	**55.3 %**
File_Microsoft-Windows-Executable	2.76k	23.2 %
File_Rar-Archive	1.87k	15.7 %
File_Zip-Archive	403	3.4 %
File_Type-Unknown	392	3.3 %
File_Text-US-Ascii-Text-File	337	2.8 %
File_LhArc-Archive	237	2.0 %
File_Microsoft-Excel-97-Spreadsheet	137	1.2 %
File_7z-Archive	112	0.9 %
File_Office-Open-XML-Package-Relations-Item	73	0.6 %
File_HTML	72	0.6 %
File_Visual-Basic-Script-Filename	42	0.4 %
File_ISO-9660-Disk-Image	40	0.3 %
File_PDF	33	0.3 %
File_JavaScript	21	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	19	0.2 %
File_Microsoft-Office-Open-XML-Document	8	0.1 %
File_Java-Archive-Manifest	6	0.1 %
File_Tar-Archive	5	0.0 %
File_ACE-Archive	3	0.0 %
File_BZip2-Compressed	1	0.0 %
File_Perl-Interpreted-Script	1	0.0 %
File_ELF-Executable	1	0.0 %
File_RTF	1	0.0 %
File_XZ-Archive	1	0.0 %
Not Available	**3.17k**	**26.6 %**
File_Zip-Archive	2.89k	24.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	158	1.3 %
File_Microsoft-Office-Open-XML-Document	115	1.0 %
File_Java-Archive	6	0.1 %
Medium Risk	**946**	**7.9 %**
File_Microsoft-Windows-Executable	607	5.1 %
File_PDF	174	1.5 %
File_XML	88	0.7 %
File_Type-Unknown	22	0.2 %
File_LhArc-Archive	15	0.1 %
File_Zip-Archive	8	0.1 %
File_Rar-Archive	8	0.1 %
File_7z-Archive	7	0.1 %

Scan Result	Hits	%
File_Office-Open-XML-Package-Relations-Item	5	0.0 %
File_Microsoft-Office-Open-XML-Document	4	0.0 %
File_Microsoft-Excel-97-Spreadsheet	3	0.0 %
File_HTML	2	0.0 %
File_Visual-Basic-Script-Filename	1	0.0 %
File_JavaScript	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
High Risk	**807**	**6.8 %**
File_PDF	355	3.0 %
File_Microsoft-Equation-Editor-Document	105	0.9 %
File_Office-Open-XML-Package-Relations-Item	92	0.8 %
File_Zip-Archive	88	0.7 %
File_LhArc-Archive	44	0.4 %
File_HTML	40	0.3 %
File_Rar-Archive	29	0.2 %
File_Microsoft-Windows-Executable	22	0.2 %
File_Type-Unknown	17	0.1 %
File_Microsoft-Office-Open-XML-Document	5	0.0 %
File_7z-Archive	5	0.0 %
File_Microsoft-Excel-97-Spreadsheet	2	0.0 %
File_Text-US-Ascii-Text-File	1	0.0 %
File_ISO-9660-Disk-Image	1	0.0 %
File_Tar-Archive	1	0.0 %
Unknown	**234**	**2.0 %**
File_Zip-Archive	209	1.8 %
File_Microsoft-Office-Open-XML-Document	24	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
HTML/Phishing.rb	**25**	**0.2 %**
File_HTML	18	0.2 %
File_Text-US-Ascii-Text-File	7	0.1 %
HTML/Phishing.wl	**22**	**0.2 %**
File_HTML	22	0.2 %
HTML/Phishing.ta	**20**	**0.2 %**
File_HTML	20	0.2 %
HTML/Phishing.rj	**19**	**0.2 %**
File_Text-US-Ascii-Text-File	19	0.2 %
HTML/Phishing.vf	**16**	**0.1 %**
File_HTML	16	0.1 %
HTML/Phishing.ux	**12**	**0.1 %**

Scan Result	Hits	%
File_Text-US-Ascii-Text-File	12	0.1 %
HTML/Phishing.wb	**6**	**0.1 %**
File_HTML	6	0.1 %
HTML/Phishing.yn	**5**	**0.0 %**
File_HTML	5	0.0 %
W32/Bagle.ar@MM!pwdzip	**5**	**0.0 %**
File_Encrypted-Zip-Archive	5	0.0 %
Fareit.gen.d	**4**	**0.0 %**
File_ACE-Archive	4	0.0 %
Exploit-GBR!0BAF9224E118	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
HTML/Phishing.yp	**3**	**0.0 %**
File_HTML	3	0.0 %
Linux/Mechbot.a	**3**	**0.0 %**
File_Gzip-Compressed	3	0.0 %
Exploit-GBR!1E5C64A8611D	**3**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	3	0.0 %
W32/Mytob.gen.eml	**3**	**0.0 %**
File_Text-US-Ascii-Text-File	3	0.0 %
HTML/Phishing.xz	**3**	**0.0 %**
File_HTML	3	0.0 %
AgentTesla-FDKB!F7766FB8FD23	**2**	**0.0 %**
File_ISO-9660-Disk-Image	2	0.0 %
VBS/Soraci	**2**	**0.0 %**
File_Gzip-Compressed	1	0.0 %
File_PGP-Message	1	0.0 %
Trojan-FWEL!A0F7EB1E7ABB	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
Exploit-MIME.gen.a	**2**	**0.0 %**
File_Text-US-Ascii-Text-File	1	0.0 %
File_HTML	1	0.0 %
W32/Mydoom.o.o@MM!zip	**2**	**0.0 %**
File_Zip-Archive	2	0.0 %
Perl/Shellbot	**2**	**0.0 %**
File_Text-US-Ascii-Text-File	1	0.0 %
File_Perl-Interpreted-Script	1	0.0 %
Linux/Rst.b	**2**	**0.0 %**
File_BZip2-Compressed	2	0.0 %
PDF/Phishing!1FD6BE2BD726	**1**	**0.0 %**

Scan Result	Hits	%
File_PDF	1	0.0 %
GenericRXSM-NK!24C949732111	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Others	**8**	**0.1 %**
Total	**11.91k**	**100 %**

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.


Total
11.91k
Hits

Responding Scanner	Hits	%
File_Zip-Archive	**3.60k**	**30.2 %**
Not Available	2.89k	24.2 %
Malicious	403	3.4 %
Unknown	209	1.8 %
High Risk	88	0.7 %
Medium Risk	8	0.1 %
W32/Mydoom.o.o@MM!zip	2	0.0 %
Remcos-FDQO!A741F1861AB7	1	0.0 %
File_Microsoft-Windows-Executable	**3.39k**	**28.5 %**
Malicious	2.76k	23.2 %
Medium Risk	607	5.1 %
High Risk	22	0.2 %
Adware-KeenValue.i	1	0.0 %
GenericRXUL-YC!23EAC694F631	1	0.0 %
File_Rar-Archive	**1.92k**	**16.1 %**
Malicious	1.87k	15.7 %
High Risk	29	0.2 %
Medium Risk	8	0.1 %
Trojan-FWEL!A0F7EB1E7ABB	2	0.0 %
GenericRXSM-NK!24C949732111	1	0.0 %
AgentTesla-FDKB!E4A071F45D59	1	0.0 %
W32/Sdbot.k.gen	1	0.0 %
File_PDF	**563**	**4.7 %**
High Risk	355	3.0 %
Medium Risk	174	1.5 %
Malicious	33	0.3 %
PDF/Phishing!1FD6BE2BD726	1	0.0 %
File_Type-Unknown	**431**	**3.6 %**
Malicious	392	3.3 %
Medium Risk	22	0.2 %
High Risk	17	0.1 %
File_Text-US-Ascii-Text-File	**381**	**3.2 %**
Malicious	337	2.8 %
HTML/Phishing.rj	19	0.2 %
HTML/Phishing.ux	12	0.1 %
HTML/Phishing.rb	7	0.1 %
W32/Mytob.gen.eml	3	0.0 %
High Risk	1	0.0 %
Exploit-MIME.gen.a	1	0.0 %

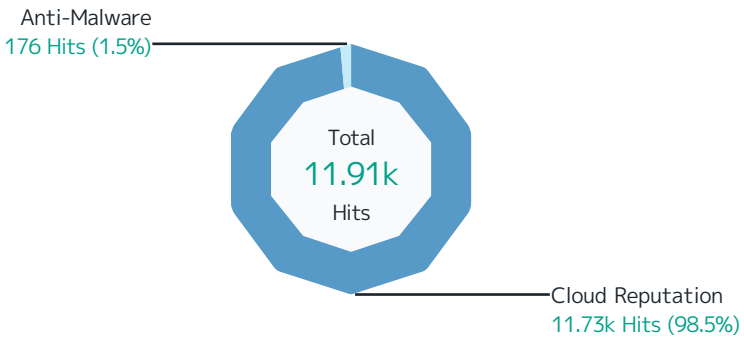
Responding Scanner	Hits	%
Perl/Shellbot	1	0.0 %
File_LhArc-Archive	**296**	**2.5 %**
Malicious	237	2.0 %
High Risk	44	0.4 %
Medium Risk	15	0.1 %
File_HTML	**208**	**1.7 %**
Malicious	72	0.6 %
High Risk	40	0.3 %
HTML/Phishing.wl	22	0.2 %
HTML/Phishing.ta	20	0.2 %
HTML/Phishing.rb	18	0.2 %
HTML/Phishing.vf	16	0.1 %
HTML/Phishing.wb	6	0.1 %
HTML/Phishing.yn	5	0.0 %
HTML/Phishing.yp	3	0.0 %
HTML/Phishing.xz	3	0.0 %
Medium Risk	2	0.0 %
Exploit-MIME.gen.a	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**181**	**1.5 %**
Not Available	158	1.3 %
Malicious	19	0.2 %
Exploit-GBR!0BAF9224E118	3	0.0 %
Unknown	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**170**	**1.4 %**
High Risk	92	0.8 %
Malicious	73	0.6 %
Medium Risk	5	0.0 %
File_Microsoft-Office-Open-XML-Document	**156**	**1.3 %**
Not Available	115	1.0 %
Unknown	24	0.2 %
Malicious	8	0.1 %
High Risk	5	0.0 %
Medium Risk	4	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**142**	**1.2 %**
Malicious	137	1.2 %
Medium Risk	3	0.0 %
High Risk	2	0.0 %
File_7z-Archive	**124**	**1.0 %**
Malicious	112	0.9 %

Responding Scanner	Hits	%
Medium Risk	7	0.1 %
High Risk	5	0.0 %
File_Microsoft-Equation-Editor-Document	**105**	**0.9 %**
High Risk	105	0.9 %
File_XML	**88**	**0.7 %**
Medium Risk	88	0.7 %
File_Visual-Basic-Script-Filename	**43**	**0.4 %**
Malicious	42	0.4 %
Medium Risk	1	0.0 %
File_ISO-9660-Disk-Image	**43**	**0.4 %**
Malicious	40	0.3 %
AgentTesla-FDKB!F7766FB8FD23	2	0.0 %
High Risk	1	0.0 %
File_JavaScript	**22**	**0.2 %**
Malicious	21	0.2 %
Medium Risk	1	0.0 %
File_ACE-Archive	**7**	**0.1 %**
Fareit.gen.d	4	0.0 %
Malicious	3	0.0 %
File_Tar-Archive	**6**	**0.1 %**
Malicious	5	0.0 %
High Risk	1	0.0 %
File_Java-Archive	**6**	**0.1 %**
Not Available	6	0.1 %
File_Java-Archive-Manifest	**6**	**0.1 %**
Malicious	6	0.1 %
File_Gzip-Compressed	**6**	**0.1 %**
Linux/Mechbot.a	3	0.0 %
VBS/Soraci	1	0.0 %
IRC/Generic Flooder	1	0.0 %
W32/Sdbot.worm.h	1	0.0 %
File_Encrypted-Zip-Archive	**5**	**0.0 %**
W32/Bagle.ar@MM!pwdzip	5	0.0 %
File_Microsoft-Excel-Spreadsheet	**4**	**0.0 %**
Exploit-GBR!1E5C64A8611D	3	0.0 %
Medium Risk	1	0.0 %
File_Perl-Interpreted-Script	**3**	**0.0 %**
Malicious	1	0.0 %
Perl/Shellbot	1	0.0 %

Responding Scanner	Hits	%
PERL/Agent.c	1	0.0 %
File_BZip2-Compressed	**3**	**0.0 %**
Linux/Rst.b	2	0.0 %
Malicious	1	0.0 %
File_ELF-Executable	**1**	**0.0 %**
Malicious	1	0.0 %
File_RTF	**1**	**0.0 %**
Malicious	1	0.0 %
File_PGP-Message	**1**	**0.0 %**
VBS/Soraci	1	0.0 %
Others	**1**	**0.0 %**
Total	**11.91k**	**100 %**

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**11.73k**	**98.5 %**
File_Zip-Archive	3.59k	30.2 %
File_Microsoft-Windows-Executable	3.39k	28.5 %
File_Rar-Archive	1.91k	16.0 %
File_PDF	562	4.7 %
File_Type-Unknown	431	3.6 %
File_Text-US-Ascii-Text-File	338	2.8 %
File_LhArc-Archive	296	2.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	178	1.5 %
File_Office-Open-XML-Package-Relations-Item	170	1.4 %
File_Microsoft-Office-Open-XML-Document	156	1.3 %
File_Microsoft-Excel-97-Spreadsheet	142	1.2 %
File_7z-Archive	124	1.0 %
File_HTML	114	1.0 %
File_Microsoft-Equation-Editor-Document	105	0.9 %
File_XML	88	0.7 %
File_Visual-Basic-Script-Filename	43	0.4 %
File_ISO-9660-Disk-Image	41	0.3 %
File_JavaScript	22	0.2 %
File_Tar-Archive	6	0.1 %
File_Java-Archive	6	0.1 %
File_Java-Archive-Manifest	6	0.1 %
File_ACE-Archive	3	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_Perl-Interpreted-Script	1	0.0 %
File_BZip2-Compressed	1	0.0 %
File_ELF-Executable	1	0.0 %
File_RTF	1	0.0 %
File_XZ-Archive	1	0.0 %
Anti-Malware	**176**	**1.5 %**
File_HTML	94	0.8 %
File_Text-US-Ascii-Text-File	43	0.4 %
File_Gzip-Compressed	6	0.1 %
File_Rar-Archive	5	0.0 %
File_Encrypted-Zip-Archive	5	0.0 %
File_ACE-Archive	4	0.0 %
File_Zip-Archive	3	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
File_Microsoft-Excel-Spreadsheet	3	0.0 %

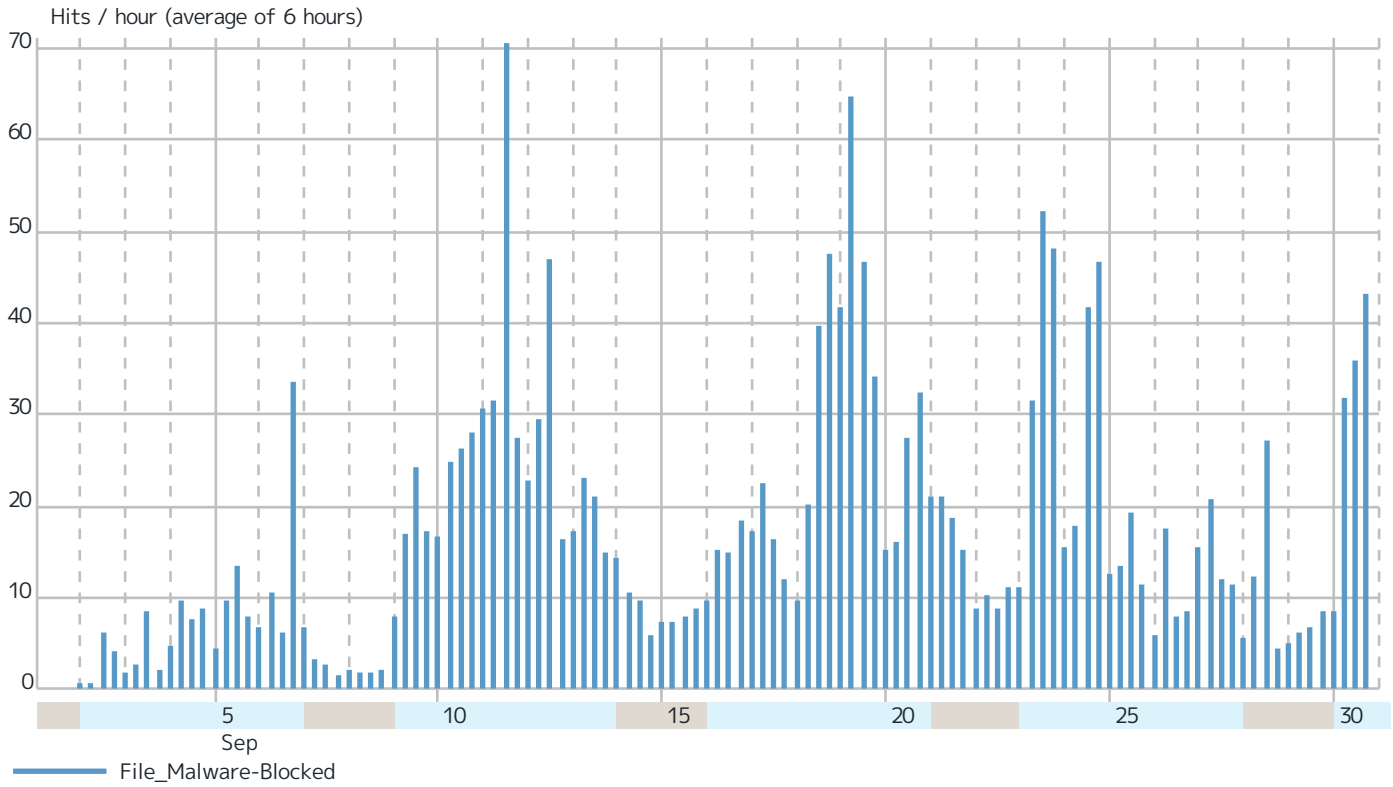
Responding Scanner	Hits	%
File_Microsoft-Windows-Executable	2	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_Perl-Interpreted-Script	2	0.0 %
File_BZip2-Compressed	2	0.0 %
File_PDF	1	0.0 %
File_PGP-Message	1	0.0 %
Total	**11.91k**	**100 %**

Virenfilterung SRC IPs

Records by src IP		Hits	%
80.85.152.111	Russia	878	7.4 %
46.254.34.170	Rome, Italy	794	6.7 %
23.254.217.117	United States	498	4.2 %
172.245.244.79	Buffalo, New York 14205, United States	493	4.1 %
148.135.111.208	Los Angeles, California 90017, United States	347	2.9 %
194.184.71.4	Turin, Italy	326	2.7 %
2a00:8a60:1:11::1004	RWTH Aachen	310	2.6 %
195.123.213.250	Riga, Latvia	303	2.5 %
200.0.183.43	Mar del Plata, Argentina	276	2.3 %
23.21.224.96	Ashburn, Virginia 20149, United States	264	2.2 %
173.236.110.195	United States	219	1.8 %
2a00:8a60:1:11::1008	RWTH Aachen	209	1.8 %
188.127.225.216	Russia	188	1.6 %
95.211.213.219	Zeist, The Netherlands	186	1.6 %
62.171.142.89	Nuremberg, Germany	174	1.5 %
103.198.26.192	Cyberjaya, Malaysia	170	1.4 %
80.85.152.237	Russia	170	1.4 %
107.189.159.165	Phoenix, Arizona 85034, United States	158	1.3 %
163.123.192.237	Phoenix, Arizona 85034, United States	156	1.3 %
103.186.117.149	Cyberjaya, Malaysia	151	1.3 %
103.231.249.87	Vietnam	149	1.3 %
2a00:8a60:1:11::1005	RWTH Aachen	136	1.1 %
208.117.57.140	United States	132	1.1 %
163.123.194.53	Dallas, Texas 75270, United States	124	1.0 %
209.59.151.195	United States	122	1.0 %
2a00:8a60:1:11::1006	RWTH Aachen	119	1.0 %
45.90.89.30	Istanbul, Türkiye	108	0.9 %
107.174.142.126	Los Angeles, California 90060, United States	108	0.9 %
192.227.144.43	Buffalo, New York 14205, United States	100	0.8 %
195.123.210.179	Riga, Latvia	96	0.8 %
Others		4.44k	37.3 %
Total		**11.91k**	**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.