Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-06-01 00:00:00 CEST
To: 2022-07-01 00:00:00 CEST

Report

Report run by
jens

SMC version
6.11.1, build 11219

Update version
1480

Report started
2022-07-01 07:49:22 CEST

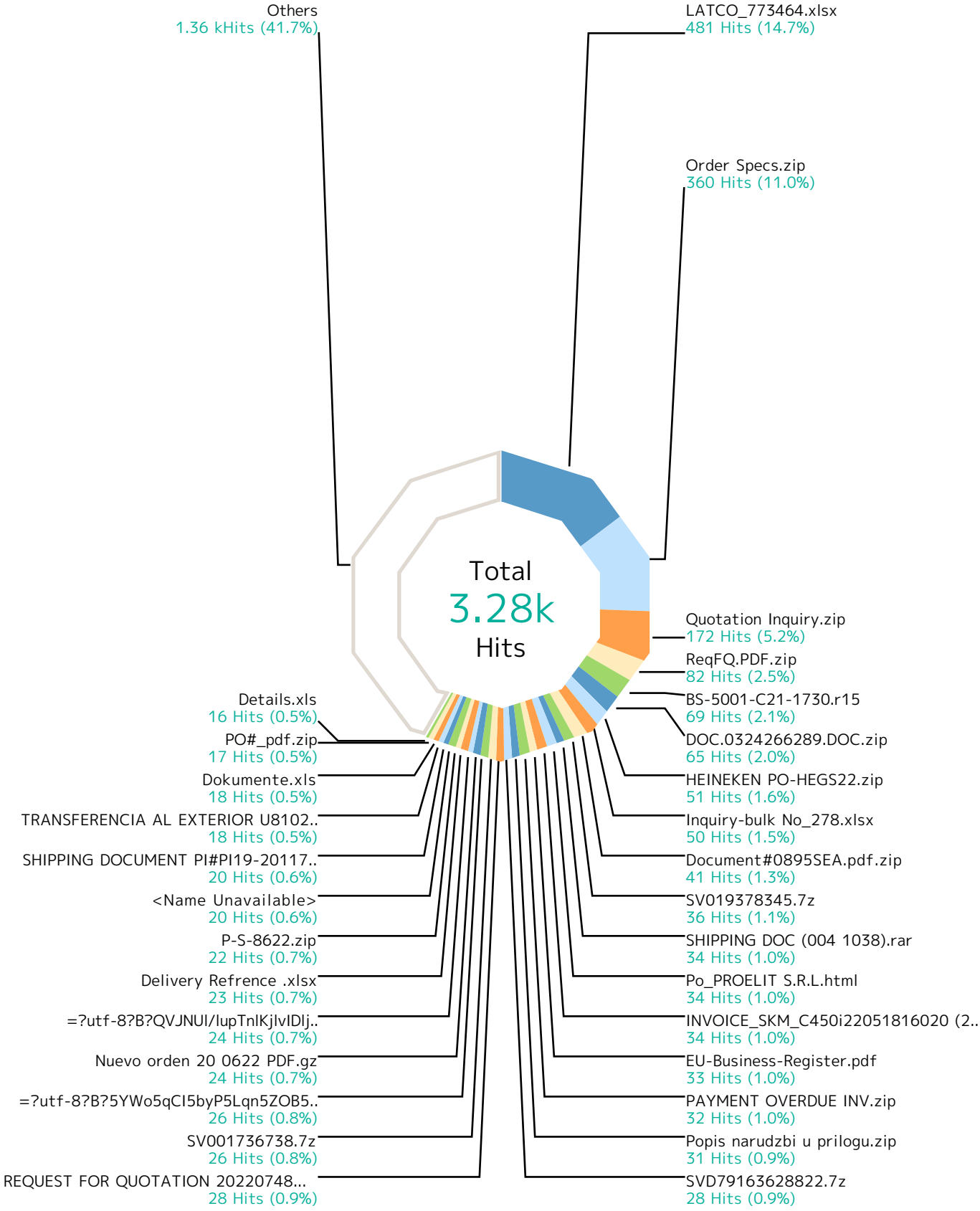
Report run time
02:08:54

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



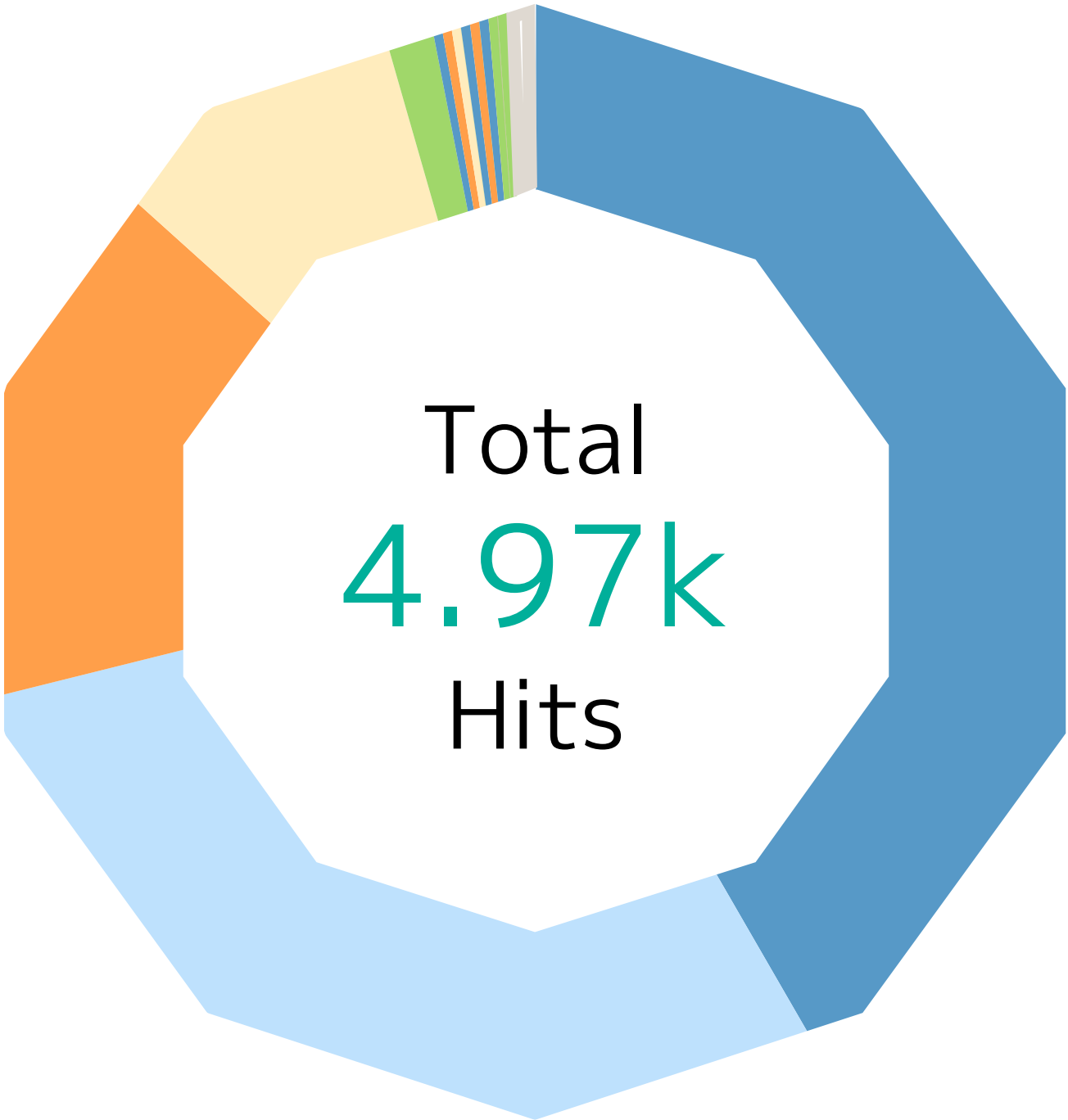
Report

Records by file name	Hits	%
LATCO_773464.xlsx	481	14.7 %
Order Specs.zip	360	11.0 %
Quotation Inquiry.zip	172	5.2 %
ReqFQ.PDF.zip	82	2.5 %
BS-5001-C21-1730.r15	69	2.1 %
DOC.0324266289.DOC.zip	65	2.0 %
HEINEKEN PO-HEGS22.zip	51	1.6 %
Inquiry-bulk No_278.xlsx	50	1.5 %
Document#0895SEA.pdf.zip	41	1.3 %
SV019378345.7z	36	1.1 %
SHIPPING DOC (004 1038).rar	34	1.0 %
Po_PROELIT S.R.L.html	34	1.0 %
INVOICE_SKM_C450i22051816020 (2).pdf	34	1.0 %
EU-Business-Register.pdf	33	1.0 %
PAYMENT OVERDUE INV.zip	32	1.0 %
Popis narudzbi u prilogu.zip	31	0.9 %
SVD79163628822.7z	28	0.9 %
REQUEST FOR QUOTATION 20220748.rar	28	0.9 %
SV001736738.7z	26	0.8 %
=?utf-8?B?5YWo5qCI5byP5Lqn5ZOB5Lqk5LqS6K6+6K6hLmRvY3g=?=	26	0.8 %
Nuevo orden 20 0622 PDF.gz	24	0.7 %
=?utf-8?B?QVJNUI/lupTnlKjlvIDlj5EuZG9jeA==?=	24	0.7 %
Delivery Refrence .xlsx	23	0.7 %
P-S-8622.zip	22	0.7 %
<Name Unavailable>	20	0.6 %
SHIPPING DOCUMENT PI#PI19-201171.zip	20	0.6 %
TRANSFERENCIA AL EXTERIOR U810295.z	18	0.5 %
Dokumente.xls	18	0.5 %
PO#_pdf.zip	17	0.5 %
Details.xls	16	0.5 %
Others	1.36k	41.6 %
Total	**3.28k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
4.97k
Hits

Report

Scan Result	Hits	%
Malicious	**2.08k**	**41.8 %**
File_Microsoft-Windows-Executable	968	19.5 %
File_Microsoft-Excel-97-Spreadsheet	366	7.4 %
File_Rar-Archive	212	4.3 %
File_Zip-Archive	193	3.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	81	1.6 %
File_PDF	68	1.4 %
File_ISO-9660-Disk-Image	41	0.8 %
File_7z-Archive	41	0.8 %
File_Type-Unknown	29	0.6 %
File_Microsoft-OLE	17	0.3 %
File_Microsoft-Equation-Editor-Document	15	0.3 %
File_JavaScript	12	0.2 %
File_Self-Extracting-Zip-Archive	8	0.2 %
File_Microsoft-Cabinet-Archive	8	0.2 %
File_ACE-Archive	7	0.1 %
File_HTML	5	0.1 %
File_LhArc-Archive	2	0.0 %
File_BZip2-Compressed	1	0.0 %
File_RTF	1	0.0 %
Not Available	**1.46k**	**29.4 %**
File_Zip-Archive	908	18.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	551	11.1 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Medium Risk	**775**	**15.6 %**
File_XML	452	9.1 %
File_Rar-Archive	95	1.9 %
File_Type-Unknown	87	1.8 %
File_Microsoft-Office-Open-XML-Document	83	1.7 %
File_Microsoft-Windows-Executable	41	0.8 %
File_ISO-9660-Disk-Image	7	0.1 %
File_HTML	5	0.1 %
File_Self-Extracting-Zip-Archive	4	0.1 %
File_JavaScript	1	0.0 %
High Risk	**437**	**8.8 %**
File_Rar-Archive	131	2.6 %

Report

Scan Result	Hits	%
File_Microsoft-Windows-Executable	107	2.2 %
File_Type-Unknown	53	1.1 %
File_Microsoft-Excel-97-Spreadsheet	36	0.7 %
File_Zip-Archive	30	0.6 %
File_ISO-9660-Disk-Image	30	0.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	22	0.4 %
File_HTML	19	0.4 %
File_PDF	4	0.1 %
File_Microsoft-Office-Open-XML-Document	2	0.0 %
File_BZip2-Compressed	2	0.0 %
File_XML	1	0.0 %
X97M/Downloader.or	**65**	**1.3 %**
File_Microsoft-Excel-97-Spreadsheet	65	1.3 %
JS/Nemucod.akz	**11**	**0.2 %**
File_JavaScript	10	0.2 %
File_Rar-Archive	1	0.0 %
Fareit-FDBI!67D8A71D7711	**10**	**0.2 %**
File_Zip-Archive	10	0.2 %
Downloader-FCIV!F4C0FC1E47D8	**10**	**0.2 %**
File_Zip-Archive	10	0.2 %
Fareit-FDBI!C87C32E52882	**8**	**0.2 %**
File_Zip-Archive	8	0.2 %
Unknown	**7**	**0.1 %**
File_Zip-Archive	7	0.1 %
Exploit-GBT!A75855AC226D	**7**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	7	0.1 %
AgentTesla-FDFR!779C83EB8844	**7**	**0.1 %**
File_Rar-Archive	7	0.1 %
Exploit-GBT!2250EF455FF7	**6**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.1 %
GenericRXSA-MT!0218559E0051	**5**	**0.1 %**
File_Zip-Archive	5	0.1 %
Exploit-GBT!AD517B03DE00	**5**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.1 %
Exploit-GBT!2E0DEA1CA1A5	**4**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %

Report

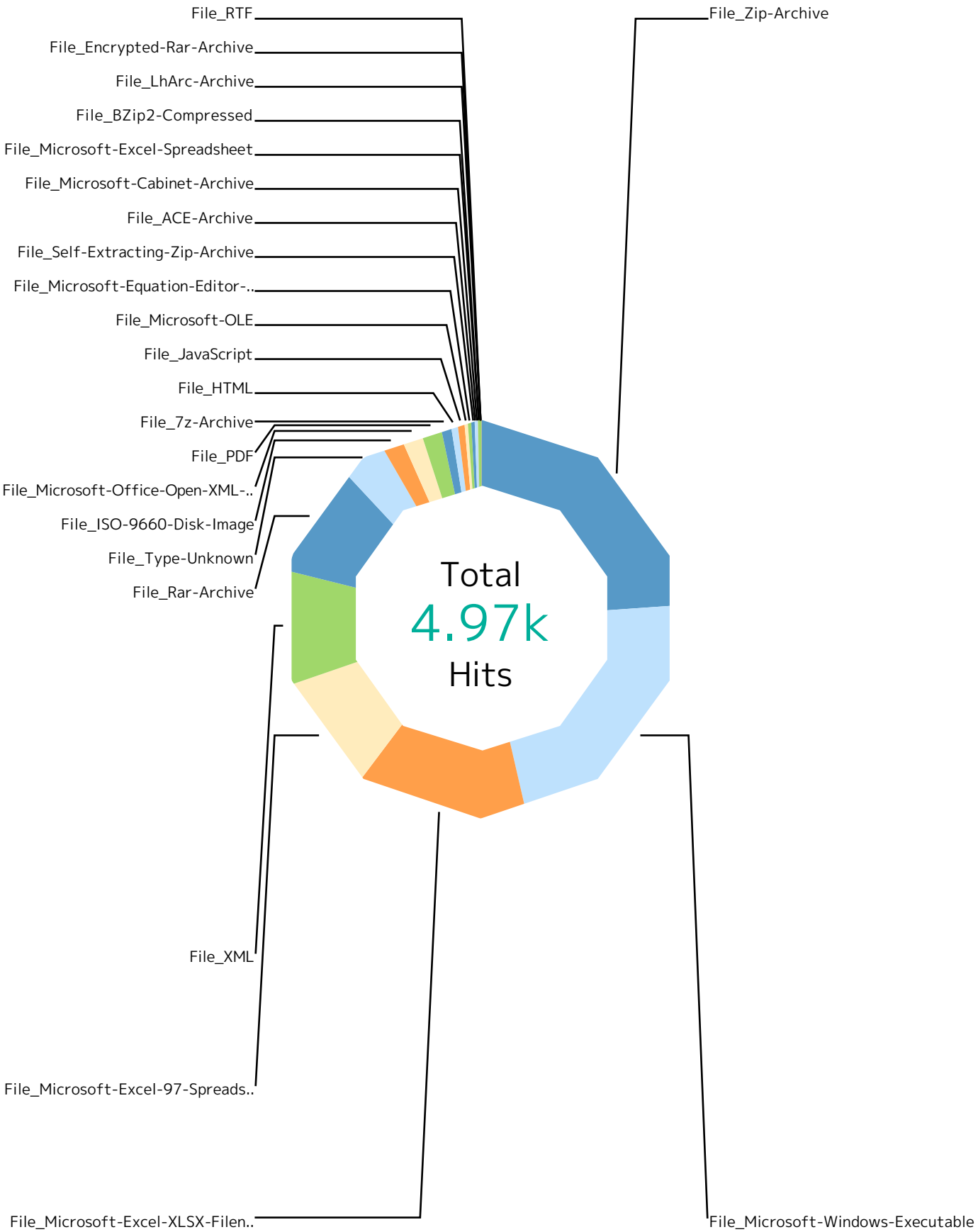
Scan Result	Hits	%
X97M/Downloader.ph	**4**	**0.1 %**
File_Microsoft-Excel-97-Spreadsheet	4	0.1 %
Fareit-FDBI!D42750B1A0FE	**3**	**0.1 %**
File_Rar-Archive	3	0.1 %
Exploit-GBT!61A24F9A223A	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
Exploit-GBT!DB64F3B0C849	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
AgentTesla-FDFR!FF9ED59D07DF	**3**	**0.1 %**
File_ISO-9660-Disk-Image	3	0.1 %
Fareit-FDBI!6CA8A60F5C34	**3**	**0.1 %**
File_Zip-Archive	3	0.1 %
Exploit-GBS!E1905E8436BD	**3**	**0.1 %**
File_Type-Unknown	3	0.1 %
HTML/Phishing.ha	**3**	**0.1 %**
File_HTML	3	0.1 %
Exploit-GBT!1EFEF2011E06	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!D943DEE0D479	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBS!C7FC2A234B40	**2**	**0.0 %**
File_Type-Unknown	2	0.0 %
Exploit-GDJ!18D451184ABA	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Fareit-FDBI!250B580292FB	**2**	**0.0 %**
File_Zip-Archive	2	0.0 %
Exploit-CVE2017-11882.yx	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Others	**37**	**0.7 %**
Total	**4.97k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_RTF
File_Encrypted-Rar-Archive
File_LhArc-Archive
File_BZip2-Compressed
File_Microsoft-Excel-Spreadsheet
File_Microsoft-Cabinet-Archive
File_ACE-Archive
File_Self-Extracting-Zip-Archive
File_Microsoft-Equation-Editor-..
File_Microsoft-OLE
File_JavaScript
File_HTML
File_7z-Archive
File_PDF
File_Microsoft-Office-Open-XML-..
File_ISO-9660-Disk-Image
File_Type-Unknown
File_Rar-Archive
File_Zip-Archive
Total
4.97k
Hits
File_XML
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**1.18k**	**23.8 %**
Not Available	908	18.3 %
Malicious	193	3.9 %
High Risk	30	0.6 %
Fareit-FDBI!67D8A71D7711	10	0.2 %
Downloader-FCIV!F4C0FC1E47D8	10	0.2 %
Fareit-FDBI!C87C32E52882	8	0.2 %
Unknown	7	0.1 %
GenericRXSA-MT!0218559E0051	5	0.1 %
Fareit-FDBI!6CA8A60F5C34	3	0.1 %
Fareit-FDBI!250B580292FB	2	0.0 %
Fareit-FDBI!DEC35D8523F0	2	0.0 %
Fareit-FDBI!D3222CB84141	1	0.0 %
Fareit-FCVN!0D0BCA0E0DEF	1	0.0 %
GenericRXTG-EZ!C391E7482EDE	1	0.0 %
File_Microsoft-Windows-Executable	**1.12k**	**22.5 %**
Malicious	968	19.5 %
High Risk	107	2.2 %
Medium Risk	41	0.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	**700**	**14.1 %**
Not Available	551	11.1 %
Malicious	81	1.6 %
High Risk	22	0.4 %
Exploit-GBT!A75855AC226D	7	0.1 %
Exploit-GBT!2250EF455FF7	6	0.1 %
Exploit-GBT!AD517B03DE00	5	0.1 %
Exploit-GBT!2E0DEA1CA1A5	4	0.1 %
Exploit-GBT!61A24F9A223A	3	0.1 %
Exploit-GBT!DB64F3B0C849	3	0.1 %
Exploit-GBT!1EFEF2011E06	2	0.0 %
Exploit-GBT!D943DEE0D479	2	0.0 %
Exploit-GDJ!18D451184ABA	2	0.0 %
Exploit-CVE2017-11882.yx	2	0.0 %
Exploit-GBT!259C53429423	2	0.0 %
Exploit-GBT!BF3B385AD9E8	1	0.0 %
Exploit-GBT!3812287611BE	1	0.0 %

Report

Responding Scanner	Hits	%
Exploit-GBT!EAA9CADC3093	1	0.0 %
Exploit-GBT!DA3ACB69BE59	1	0.0 %
Exploit-GBT!D4AF543E03F8	1	0.0 %
Exploit-GBT!BEA45E9D8D64	1	0.0 %
Exploit-GBT!DE036FE6A3E5	1	0.0 %
Exploit-GBT!45F3F8D439C7	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**471**	**9.5 %**
Malicious	366	7.4 %
X97M/Downloader.or	65	1.3 %
High Risk	36	0.7 %
X97M/Downloader.ph	4	0.1 %
File_XML	**453**	**9.1 %**
Medium Risk	452	9.1 %
High Risk	1	0.0 %
File_Rar-Archive	**451**	**9.1 %**
Malicious	212	4.3 %
High Risk	131	2.6 %
Medium Risk	95	1.9 %
AgentTesla-FDFR!779C83EB8844	7	0.1 %
Fareit-FDBI!D42750B1A0FE	3	0.1 %
JS/Nemucod.akz	1	0.0 %
AgentTesla-FCSO!ED39A5A45D9F	1	0.0 %
PWS-FCSU!21381EFAF0CA	1	0.0 %
File_Type-Unknown	**178**	**3.6 %**
Medium Risk	87	1.8 %
High Risk	53	1.1 %
Malicious	29	0.6 %
Exploit-GBS!E1905E8436BD	3	0.1 %
Exploit-GBS!C7FC2A234B40	2	0.0 %
Exploit-GBS!47BCBB3F2A8B	2	0.0 %
Exploit-GBS!5CE278496E41	2	0.0 %
File_ISO-9660-Disk-Image	**87**	**1.8 %**
Malicious	41	0.8 %
High Risk	30	0.6 %
Medium Risk	7	0.1 %
AgentTesla-FDFR!FF9ED59D07DF	3	0.1 %

Report

Responding Scanner	Hits	%
Fareit-FDBI!182F6C267EC8	2	0.0 %
GenericRXQS-MP!0ED74FE69173	2	0.0 %
Fareit-FDBI!8983CC11E7F7	1	0.0 %
Downloader-FCIV!DA9FC8EF06DD	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**86**	**1.7 %**
Medium Risk	83	1.7 %
High Risk	2	0.0 %
Exploit-GAF!72D93687CC8D	1	0.0 %
File_PDF	**72**	**1.4 %**
Malicious	68	1.4 %
High Risk	4	0.1 %
File_7z-Archive	**45**	**0.9 %**
Malicious	41	0.8 %
Fareit-FDBI!A2C91A48E633	2	0.0 %
Fareit-FDBI!975DFDB90346	1	0.0 %
Fareit-FDBI!E7798ED2C8A2	1	0.0 %
File_HTML	**32**	**0.6 %**
High Risk	19	0.4 %
Malicious	5	0.1 %
Medium Risk	5	0.1 %
HTML/Phishing.ha	3	0.1 %
File_JavaScript	**23**	**0.5 %**
Malicious	12	0.2 %
JS/Nemucod.akz	10	0.2 %
Medium Risk	1	0.0 %
File_Microsoft-OLE	**17**	**0.3 %**
Malicious	17	0.3 %
File_Microsoft-Equation-Editor-Document	**15**	**0.3 %**
Malicious	15	0.3 %
File_Self-Extracting-Zip-Archive	**12**	**0.2 %**
Malicious	8	0.2 %
Medium Risk	4	0.1 %
File_ACE-Archive	**9**	**0.2 %**
Malicious	7	0.1 %
Fareit.gen.e	1	0.0 %
Fareit.gen.a	1	0.0 %

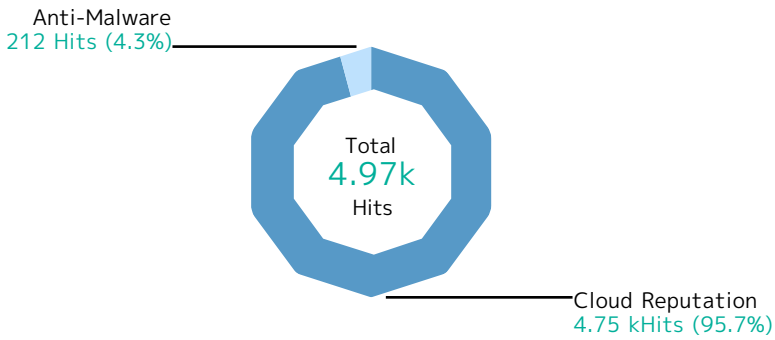
Report

Responding Scanner	Hits	%
File_Microsoft-Cabinet-Archive	**8**	**0.2 %**
Malicious	8	0.2 %
File_Microsoft-Excel-Spreadsheet	**3**	**0.1 %**
Exploit-GBT!9CBF798B0477	2	0.0 %
Not Available	1	0.0 %
File_BZip2-Compressed	**3**	**0.1 %**
High Risk	2	0.0 %
Malicious	1	0.0 %
File_LhArc-Archive	**2**	**0.0 %**
Malicious	2	0.0 %
File_Encrypted-Rar-Archive	**1**	**0.0 %**
GenericRXRU-WN!3F9D8FEA8F86	1	0.0 %
File_RTF	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**4.97k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**4.75k**	**95.7 %**
File_Zip-Archive	1.14k	22.9 %
File_Microsoft-Windows-Executable	1.12k	22.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	654	13.2 %
File_XML	453	9.1 %
File_Rar-Archive	438	8.8 %
File_Microsoft-Excel-97-Spreadsheet	402	8.1 %
File_Type-Unknown	169	3.4 %
File_Microsoft-Office-Open-XML-Document	85	1.7 %
File_ISO-9660-Disk-Image	78	1.6 %
File_PDF	72	1.4 %
File_7z-Archive	41	0.8 %
File_HTML	29	0.6 %
File_Microsoft-OLE	17	0.3 %
File_Microsoft-Equation-Editor-Document	15	0.3 %
File_JavaScript	13	0.3 %
File_Self-Extracting-Zip-Archive	12	0.2 %
File_Microsoft-Cabinet-Archive	8	0.2 %
File_ACE-Archive	7	0.1 %
File_BZip2-Compressed	3	0.1 %
File_LhArc-Archive	2	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_RTF	1	0.0 %
Anti-Malware	**212**	**4.3 %**
File_Microsoft-Excel-97-Spreadsheet	69	1.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	46	0.9 %
File_Zip-Archive	43	0.9 %
File_Rar-Archive	13	0.3 %
File_JavaScript	10	0.2 %
File_Type-Unknown	9	0.2 %
File_ISO-9660-Disk-Image	9	0.2 %
File_7z-Archive	4	0.1 %
File_HTML	3	0.1 %
File_ACE-Archive	2	0.0 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %

Report

Responding Scanner	Hits	%
File_Encrypted-Rar-Archive	1	0.0 %
Total	**4.97k**	**100 %**

Report

Virenfilterung SRC IPs

Located 70.3 %

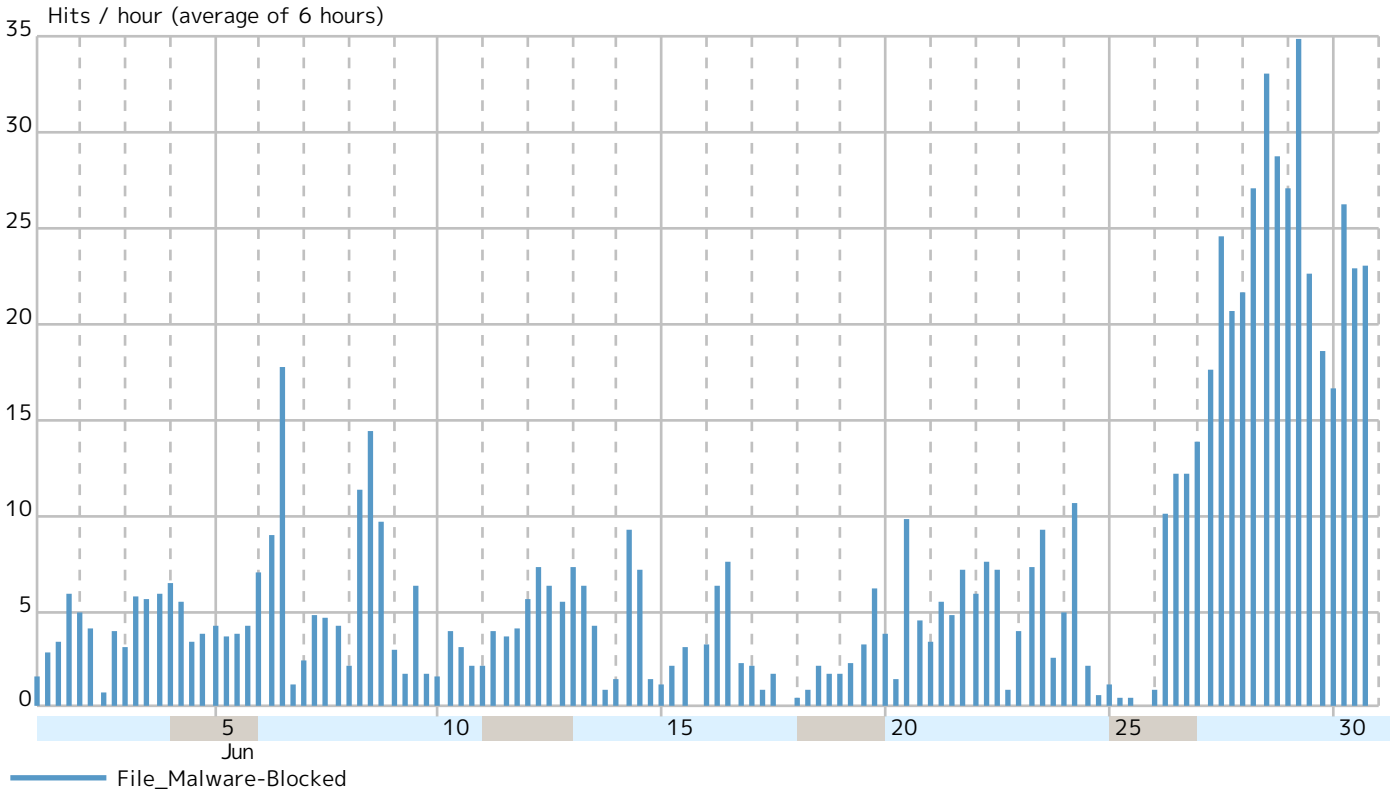
Report

Records by src IP		Hits	%
104.168.148.14	United States	962	19.4 %
87.121.98.44	Bulgaria	719	14.5 %
45.95.235.79	Russia	344	6.9 %
85.95.240.168	Turkey	193	3.9 %
202.72.215.108	Gambir, Indonesia	164	3.3 %
104.168.171.221	United States	102	2.1 %
85.217.170.253	Sofia, Bulgaria	100	2.0 %
104.168.174.38	United States	82	1.7 %
185.222.58.54	Amsterdam, Netherlands	72	1.4 %
5.175.42.19	Spain	65	1.3 %
194.31.98.179	Gambrills, Maryland 21054, United States	60	1.2 %
162.240.1.83	United States	54	1.1 %
89.252.151.33	Turkey	50	1.0 %
62.138.0.182	Strasbourg, France	48	1.0 %
193.233.182.50	Sterling, Virginia 20167, United States	44	0.9 %
103.227.62.97	India	40	0.8 %
78.137.117.158	Poplar, United Kingdom	34	0.7 %
37.48.119.7	Netherlands	34	0.7 %
104.168.136.172	United States	34	0.7 %
111.90.148.161	Kuala Lumpur, Malaysia	32	0.6 %
108.161.133.233	United States	31	0.6 %
107.182.128.55	Dallas, Texas 75270, United States	29	0.6 %
123.56.88.208	Beijing, China	28	0.6 %
143.198.30.228	Clifton, New Jersey 07014, United States	26	0.5 %
200.80.10.72	Buenos Aires, Argentina	26	0.5 %
38.242.214.34	United States	24	0.5 %
142.4.15.235	United States	24	0.5 %
2.56.56.204	Netherlands	23	0.5 %
185.248.59.9	Turkey	23	0.5 %
192.3.198.24	United States	22	0.4 %
Others		1.48k	29.7 %
Total		**4.97k**	**100 %**

Report

SMTP Virus Filtering by Time

Top 10 file filtering situations on a timeline.



About NGFW

Forcepoint Next-Generation Firewall (NGFW) protects enterprise networks while giving organizations back time to focus on their business. With it, even thousands of firewalls can be deployed and centrally managed from a single pane of glass. Uniquely built for performance and high availability, Forcepoint firewalls are resilient at all levels – links, clusters and management – and can be updated without downtime. Forcepoint NGFW combines smart, easy-to-comprehend policies with the industry's leading defenses against Advanced Evasion Techniques to deliver superior networking and security.

For further information, product demonstrations, how-to guides & videos, best practices and 3rd party reports, visit forcepoint.com/NGFW

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.