Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2021-09-01 00:00:00
To: 2021-10-01 00:00:00

Report

Report run by
jens

SMC version
6.10.2, build 11131

Update version
1391

Report started
2021-10-01 08:29:15

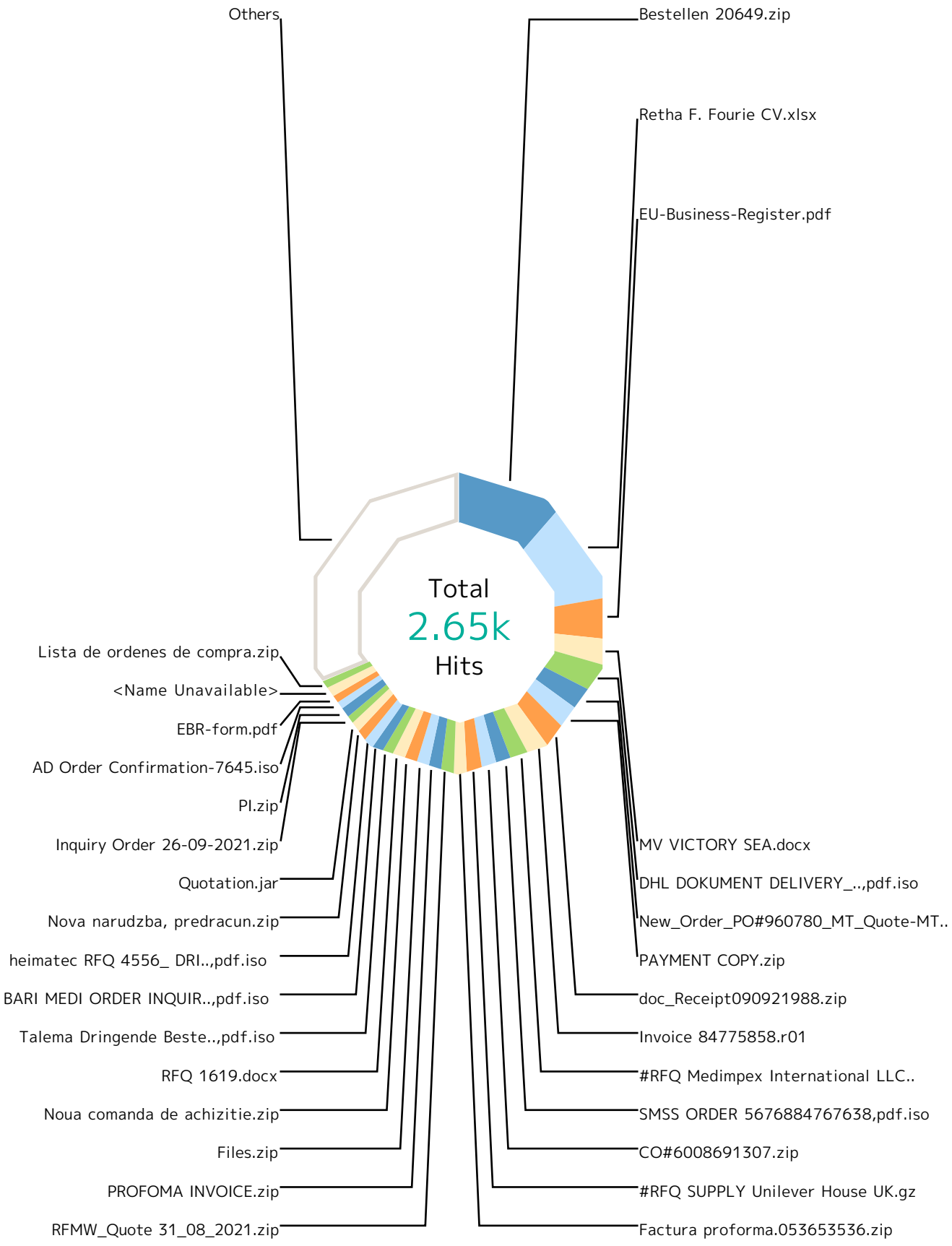
Report run time
01:49:23

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



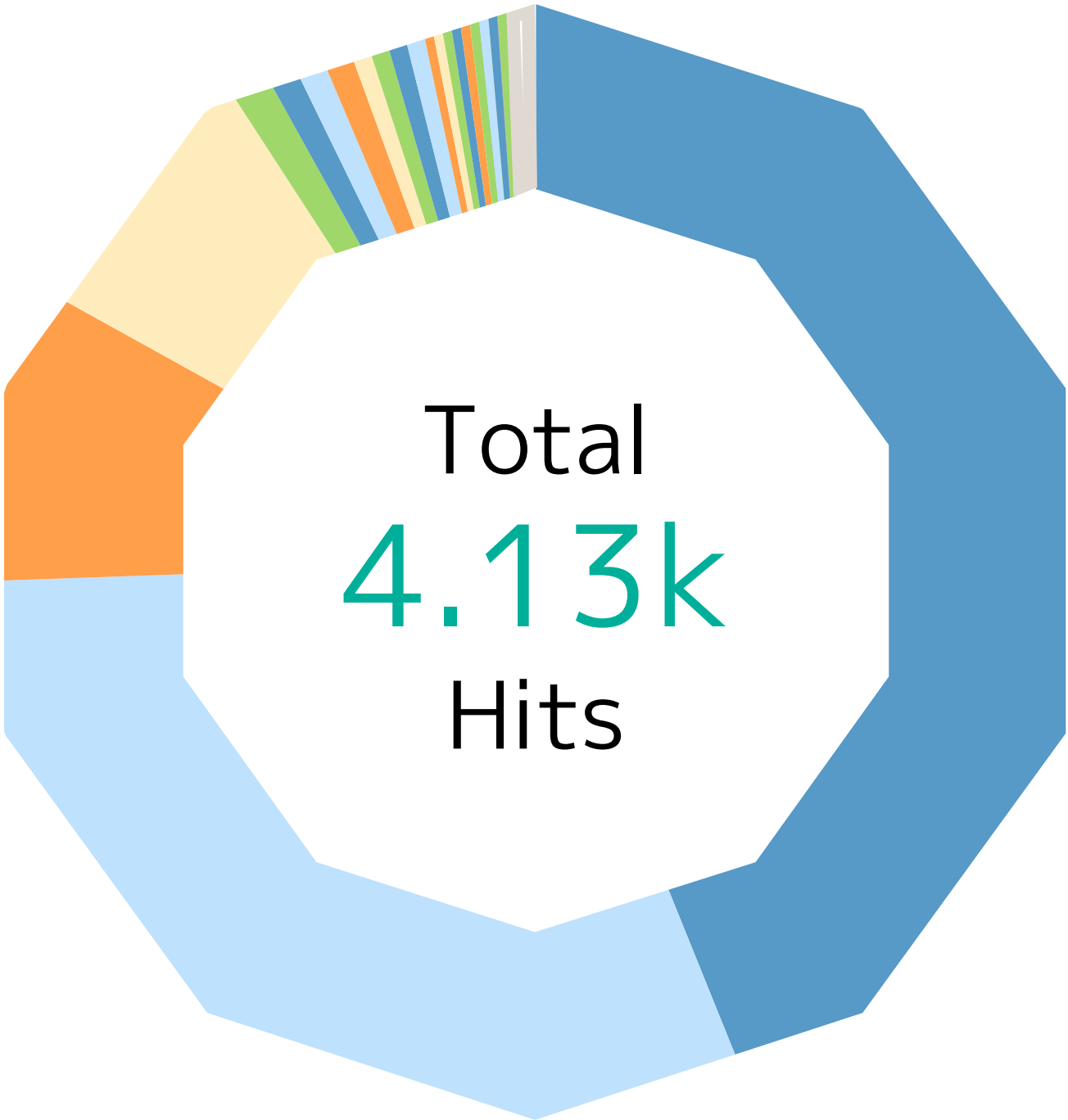
Report

Records by file name	Hits	%
Bestellen 20649.zip	301	11.4 %
Retha F. Fourie CV.xlsx	289	10.9 %
EU-Business-Register.pdf	114	4.3 %
MV VICTORY SEA.docx	78	2.9 %
DHL DOKUMENT DELIVERY_09-27-21,pdf.iso	76	2.9 %
New_Order_PO#960780_MT_Quote-MT.gz	71	2.7 %
PAYMENT COPY.zip	68	2.6 %
doc_Receipt090921988.zip	64	2.4 %
Invoice 84775858.r01	55	2.1 %
#RFQ Medimpex International LLC.gz	52	2.0 %
SMSS ORDER 5676884767638,pdf.iso	46	1.7 %
CO#6008691307.zip	45	1.7 %
#RFQ SUPPLY Unilever House UK.gz	43	1.6 %
Factura proforma.053653536.zip	39	1.5 %
RFMW_Quote 31_08_2021.zip	39	1.5 %
PROFOMA INVOICE.zip	37	1.4 %
Files.zip	36	1.4 %
Noua comanda de achizitie.zip	35	1.3 %
RFQ 1619.docx	34	1.3 %
Talema Dringende Bestellung92121,pdf.iso	31	1.2 %
BARI MEDI ORDER INQUIRY 3756653,pdf.iso	31	1.2 %
heimatec RFQ 4556_ DRINGEND,pdf.iso	29	1.1 %
Nova narudzba, predracun.zip	28	1.1 %
Quotation.jar	28	1.1 %
Inquiry Order 26-09-2021.zip	27	1.0 %
PI.zip	26	1.0 %
AD Order Confirmation-7645.iso	24	0.9 %
EBR-form.pdf	24	0.9 %
<Name Unavailable>	24	0.9 %
Lista de ordenes de compra.zip	21	0.8 %
Others	835	31.5 %
Total	**2.65k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
4.13k
Hits

Report

Scan Result	Hits	%
Malicious	**1.81k**	**44.0 %**
File_Microsoft-Windows-Executable	679	16.5 %
File_Type-Unknown	310	7.5 %
File_Rar-Archive	268	6.5 %
File_Zip-Archive	142	3.4 %
File_Office-Open-XML-Package-Relations-Item	132	3.2 %
File_PDF	80	1.9 %
File_ISO-9660-Disk-Image	61	1.5 %
File_Microsoft-Equation-Editor-Document	52	1.3 %
File_Java-Archive	28	0.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	26	0.6 %
File_Microsoft-Office-Open-XML-Document	17	0.4 %
File_Microsoft-Excel-97-Spreadsheet	6	0.1 %
File_HTML	5	0.1 %
File_ACE-Archive	5	0.1 %
File_Microsoft-PowerPoint-97-Add-In	2	0.0 %
File_Microsoft-OLE	1	0.0 %
Not Available	**1.25k**	**30.3 %**
File_Zip-Archive	890	21.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	292	7.1 %
File_Microsoft-Office-Open-XML-Document	64	1.6 %
File_Microsoft-Excel-XLSB-Filename-Extension	5	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Medium Risk	**357**	**8.7 %**
File_XML	237	5.7 %
File_PDF	56	1.4 %
File_Microsoft-Windows-Executable	11	0.3 %
File_Rar-Archive	10	0.2 %
File_Microsoft-Word-97-Document	10	0.2 %
File_Type-Unknown	8	0.2 %
File_HTML	8	0.2 %
File_Zip-Archive	6	0.1 %
File_Office-Open-XML-Application-Properties-Part	6	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.1 %
File_7z-Archive	2	0.0 %
High Risk	**320**	**7.8 %**

Report

Scan Result	Hits	%
File_ISO-9660-Disk-Image	110	2.7 %
File_Rar-Archive	66	1.6 %
File_Zip-Archive	57	1.4 %
File_Microsoft-Windows-Executable	30	0.7 %
File_Office-Open-XML-Package-Relations-Item	28	0.7 %
File_Type-Unknown	18	0.4 %
File_7z-Archive	4	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
File_PDF	2	0.0 %
File_Microsoft-Equation-Editor-Document	1	0.0 %
File_LhArc-Archive	1	0.0 %
Fareit-FCVN!937E78726308	**46**	**1.1 %**
File_ISO-9660-Disk-Image	46	1.1 %
Fareit-FCVN!6C43B38F2F78	**40**	**1.0 %**
File_ISO-9660-Disk-Image	40	1.0 %
Fareit-FCVN!6A4F90CAB77A	**32**	**0.8 %**
File_ISO-9660-Disk-Image	32	0.8 %
Fareit-FCVN!71934084E549	**31**	**0.8 %**
File_ISO-9660-Disk-Image	31	0.8 %
HTML/Phishing.ge	**31**	**0.8 %**
File_HTML	31	0.8 %
Unknown	**21**	**0.5 %**
File_Zip-Archive	21	0.5 %
Exploit-CVE2017-11882.yx	**21**	**0.5 %**
File_Microsoft-Excel-XLSX-Filename-Extension	20	0.5 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
HTML/Phish-SiteFraud.ag	**21**	**0.5 %**
File_JavaScript	21	0.5 %
HTML/Phishing.bh	**15**	**0.4 %**
File_HTML	15	0.4 %
GenericRXCD-ZZ!253637FD81B5	**13**	**0.3 %**
File_Rar-Archive	13	0.3 %
Exploit-CVE2017-11882.bu	**11**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.2 %
File_Microsoft-Office-Open-XML-Document	2	0.0 %
Packed-GDV!26B878CD6C11	**8**	**0.2 %**

Report

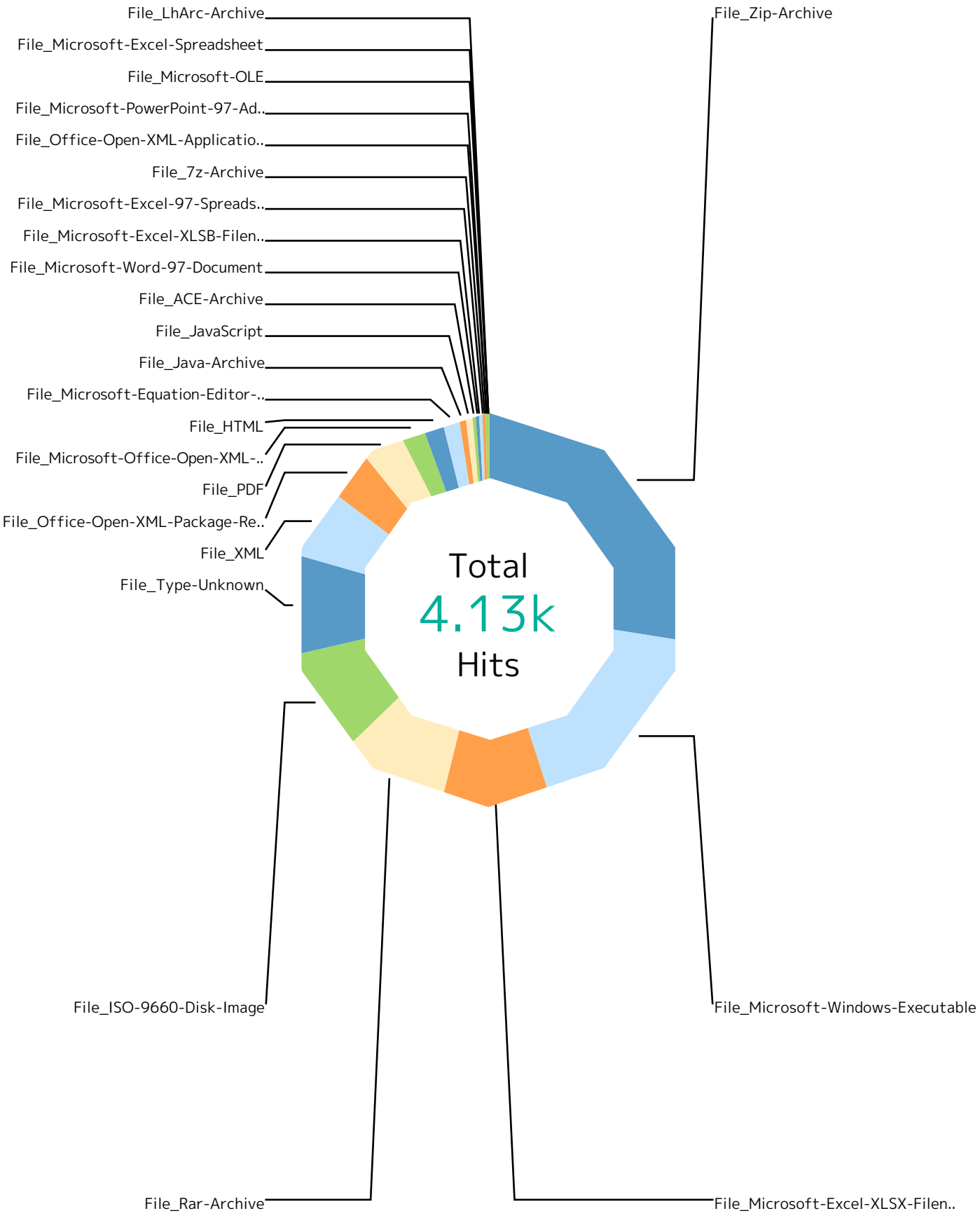
Scan Result	Hits	%
File_Rar-Archive	8	0.2 %
Fareit.gen.a	**6**	**0.1 %**
File_ACE-Archive	6	0.1 %
Exploit-CVE2017-11882.bx	**6**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.1 %
Exploit-GBT!D9732F76500E	**6**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.1 %
Fareit-FCVN!7B67892FCFA8	**4**	**0.1 %**
File_ISO-9660-Disk-Image	4	0.1 %
Fareit-FCVN!4E527C6F012D	**4**	**0.1 %**
File_ISO-9660-Disk-Image	4	0.1 %
DistTrack!C3B9E14FAA4D	**4**	**0.1 %**
File_ISO-9660-Disk-Image	4	0.1 %
X97M/Downloader.la	**4**	**0.1 %**
File_Microsoft-Excel-XLSB-Filename-Extension	4	0.1 %
Trojan-FICC!1479371EF075	**3**	**0.1 %**
File_Zip-Archive	3	0.1 %
Exploit-GBT!4AE3CCFE581F	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
HTML/Phishing.ec	**3**	**0.1 %**
File_HTML	3	0.1 %
AgentTesla-FCSO!6A2F6C6A513D	**3**	**0.1 %**
File_ISO-9660-Disk-Image	3	0.1 %
Fareit-FCVN!6BEB8F028BA0	**3**	**0.1 %**
File_ISO-9660-Disk-Image	3	0.1 %
Exploit-GBT!2E6B34EDC84B	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
DistTrack!A7A966A764FE	**2**	**0.0 %**
File_ISO-9660-Disk-Image	2	0.0 %
Others	**39**	**0.9 %**
Total	**4.13k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_LhArc-Archive
File_Microsoft-Excel-Spreadsheet
File_Microsoft-OLE
File_Microsoft-PowerPoint-97-Ad..
File_Office-Open-XML-Applicatio..
File_7z-Archive
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Excel-XLSB-Filen..
File_Microsoft-Word-97-Document
File_ACE-Archive
File_JavaScript
File_Java-Archive
File_Microsoft-Equation-Editor-..
File_HTML
File_Microsoft-Office-Open-XML-..
File_PDF
File_Office-Open-XML-Package-Re..
File_XML
File_Type-Unknown
Total
4.13k
Hits
File_Zip-Archive
File_ISO-9660-Disk-Image
File_Microsoft-Windows-Executable
File_Rar-Archive
File_Microsoft-Excel-XLSX-Filen..

Report

Responding Scanner	Hits	%
File_Zip-Archive	**1.13k**	**27.5 %**
Not Available	890	21.6 %
Malicious	142	3.4 %
High Risk	57	1.4 %
Unknown	21	0.5 %
Medium Risk	6	0.1 %
Trojan-FICC!1479371EF075	3	0.1 %
AgentTesla-FDBQ!B816F9C4E04D	2	0.0 %
AgentTesla-FDDA!473AB1B7B953	2	0.0 %
Fareit-FDBI!F43FDE788495	2	0.0 %
Fareit-FCVN!C3EF249AC219	1	0.0 %
AgentTesla-FDBQ!B69EE418F4CD	1	0.0 %
PWS-FCSU!36587E10F917	1	0.0 %
Suspect-BW!A39E429F8E69	1	0.0 %
Fareit-FDBI!655DBD26433A	1	0.0 %
Suspect-BW!B31791E4F584	1	0.0 %
Fareit-FCVN!7A910EFFD4B2	1	0.0 %
AgentTesla-FDBQ!FEC4E429AD03	1	0.0 %
File_Microsoft-Windows-Executable	**720**	**17.5 %**
Malicious	679	16.5 %
High Risk	30	0.7 %
Medium Risk	11	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	**372**	**9.0 %**
Not Available	292	7.1 %
Malicious	26	0.6 %
Exploit-CVE2017-11882.yx	20	0.5 %
Exploit-CVE2017-11882.bu	9	0.2 %
Exploit-CVE2017-11882.bx	6	0.1 %
Exploit-GBT!D9732F76500E	6	0.1 %
High Risk	3	0.1 %
Exploit-GBT!4AE3CCFE581F	3	0.1 %
Exploit-GBT!2E6B34EDC84B	3	0.1 %
Exploit-GBT!1787D88A5F20	2	0.0 %
Exploit-GBT!09752B7F4143	1	0.0 %
Exploit-GBT!5CB4D7E829F0	1	0.0 %
File_Rar-Archive	**368**	**8.9 %**

Report

Responding Scanner	Hits	%
Malicious	268	6.5 %
High Risk	66	1.6 %
GenericRXCD-ZZ!253637FD81B5	13	0.3 %
Medium Risk	10	0.2 %
Packed-GDV!26B878CD6C11	8	0.2 %
Packed-GDT!084B996DF729	1	0.0 %
GenericRXPG-MF!7FE43763C24C	1	0.0 %
PWS-FCZF!30A96082B046	1	0.0 %
File_ISO-9660-Disk-Image	**348**	**8.4 %**
High Risk	110	2.7 %
Malicious	61	1.5 %
Fareit-FCVN!937E78726308	46	1.1 %
Fareit-FCVN!6C43B38F2F78	40	1.0 %
Fareit-FCVN!6A4F90CAB77A	32	0.8 %
Fareit-FCVN!71934084E549	31	0.8 %
Fareit-FCVN!7B67892FCFA8	4	0.1 %
Fareit-FCVN!4E527C6F012D	4	0.1 %
DistTrack!C3B9E14FAA4D	4	0.1 %
AgentTesla-FCSO!6A2F6C6A513D	3	0.1 %
Fareit-FCVN!6BEB8F028BA0	3	0.1 %
DistTrack!A7A966A764FE	2	0.0 %
Fareit-FDBI!949707A6ACA2	2	0.0 %
Adwind-FDYD.jar!98D347D4BDC0	2	0.0 %
Fareit-FCVN!1317C6D5E19D	1	0.0 %
Fareit-FDBI!2F90245DCCCE	1	0.0 %
Fareit-FDBI!4002930DB05C	1	0.0 %
Fareit-FCVN!73A2067A271C	1	0.0 %
File_Type-Unknown	**337**	**8.2 %**
Malicious	310	7.5 %
High Risk	18	0.4 %
Medium Risk	8	0.2 %
AgentTesla-FDBQ!4F9FBFD1D338	1	0.0 %
File_XML	**237**	**5.7 %**
Medium Risk	237	5.7 %
File_Office-Open-XML-Package-Relations-Item	**160**	**3.9 %**
Malicious	132	3.2 %

Report

Responding Scanner	Hits	%
High Risk	28	0.7 %
File_PDF	**138**	**3.3 %**
Malicious	80	1.9 %
Medium Risk	56	1.4 %
High Risk	2	0.0 %
File_Microsoft-Office-Open-XML-Document	**88**	**2.1 %**
Not Available	64	1.6 %
Malicious	17	0.4 %
Medium Risk	3	0.1 %
Exploit-CVE2017-11882.bu	2	0.0 %
Exploit-CVE2017-11882.yx	1	0.0 %
Exploit-GDR!D1C102798332	1	0.0 %
File_HTML	**66**	**1.6 %**
HTML/Phishing.ge	31	0.8 %
HTML/Phishing.bh	15	0.4 %
Medium Risk	8	0.2 %
Malicious	5	0.1 %
HTML/Phishing.ec	3	0.1 %
HTML/Phishing!2C7881B4DBF2	1	0.0 %
HTML/Phishing.hj	1	0.0 %
HTML/Phishing.da	1	0.0 %
HTML/Phishing!D782067AF536	1	0.0 %
File_Microsoft-Equation-Editor-Document	**53**	**1.3 %**
Malicious	52	1.3 %
High Risk	1	0.0 %
File_Java-Archive	**28**	**0.7 %**
Malicious	28	0.7 %
File_JavaScript	**21**	**0.5 %**
HTML/Phish-SiteFraud.ag	21	0.5 %
File_ACE-Archive	**14**	**0.3 %**
Fareit.gen.a	6	0.1 %
Malicious	5	0.1 %
Fareit.gen.e	2	0.0 %
Fareit.gen.b	1	0.0 %
File_Microsoft-Word-97-Document	**10**	**0.2 %**
Medium Risk	10	0.2 %

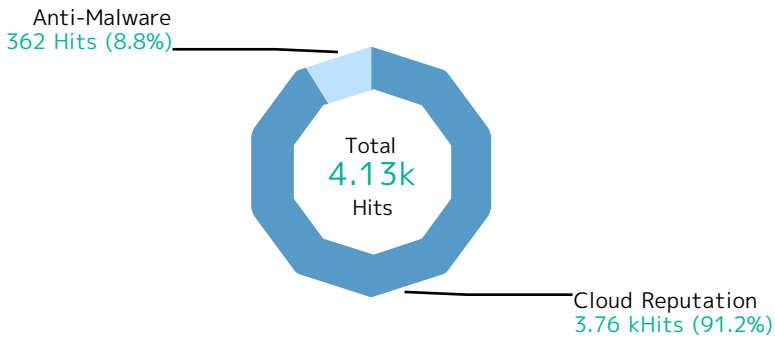
Report

Responding Scanner	Hits	%
File_Microsoft-Excel-XLSB-Filename-Extension	**9**	**0.2 %**
Not Available	5	0.1 %
X97M/Downloader.la	4	0.1 %
File_Microsoft-Excel-97-Spreadsheet	**7**	**0.2 %**
Malicious	6	0.1 %
W97M/Downloader.djz	1	0.0 %
File_7z-Archive	**6**	**0.1 %**
High Risk	4	0.1 %
Medium Risk	2	0.0 %
File_Office-Open-XML-Application-Properties-Part	**6**	**0.1 %**
Medium Risk	6	0.1 %
File_Microsoft-PowerPoint-97-Add-In	**2**	**0.0 %**
Malicious	2	0.0 %
File_Microsoft-OLE	**1**	**0.0 %**
Malicious	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.0 %**
Not Available	1	0.0 %
File_LhArc-Archive	**1**	**0.0 %**
High Risk	1	0.0 %
Total	**4.13k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

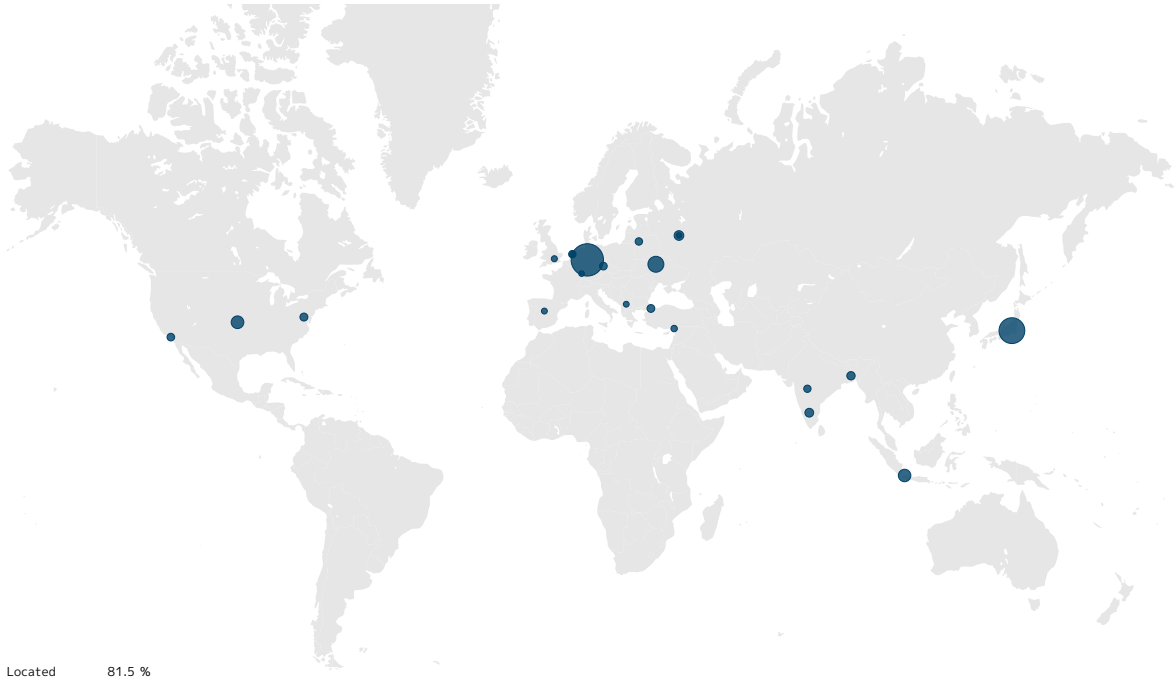
Responding Scanner	Hits	%
Cloud Reputation	**3.76k**	**91.2 %**
File_Zip-Archive	1.12k	27.0 %
File_Microsoft-Windows-Executable	720	17.5 %
File_Rar-Archive	344	8.3 %
File_Type-Unknown	336	8.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	321	7.8 %
File_XML	237	5.7 %
File_ISO-9660-Disk-Image	171	4.1 %
File_Office-Open-XML-Package-Relations-Item	160	3.9 %
File_PDF	138	3.3 %
File_Microsoft-Office-Open-XML-Document	84	2.0 %
File_Microsoft-Equation-Editor-Document	53	1.3 %
File_Java-Archive	28	0.7 %
File_HTML	13	0.3 %
File_Microsoft-Word-97-Document	10	0.2 %
File_Microsoft-Excel-97-Spreadsheet	6	0.1 %
File_7z-Archive	6	0.1 %
File_Office-Open-XML-Application-Properties-Part	6	0.1 %
File_ACE-Archive	5	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	5	0.1 %
File_Microsoft-PowerPoint-97-Add-In	2	0.0 %
File_Microsoft-OLE	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_LhArc-Archive	1	0.0 %
Anti-Malware	**362**	**8.8 %**
File_ISO-9660-Disk-Image	177	4.3 %
File_HTML	53	1.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	51	1.2 %
File_Rar-Archive	24	0.6 %
File_JavaScript	21	0.5 %
File_Zip-Archive	17	0.4 %
File_ACE-Archive	9	0.2 %
File_Microsoft-Office-Open-XML-Document	4	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	4	0.1 %
File_Type-Unknown	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %

Report

Responding Scanner	Hits	%
Total	**4.13k**	**100 %**

Report

Virenfilterung SRC IPs



Located 81.5 %

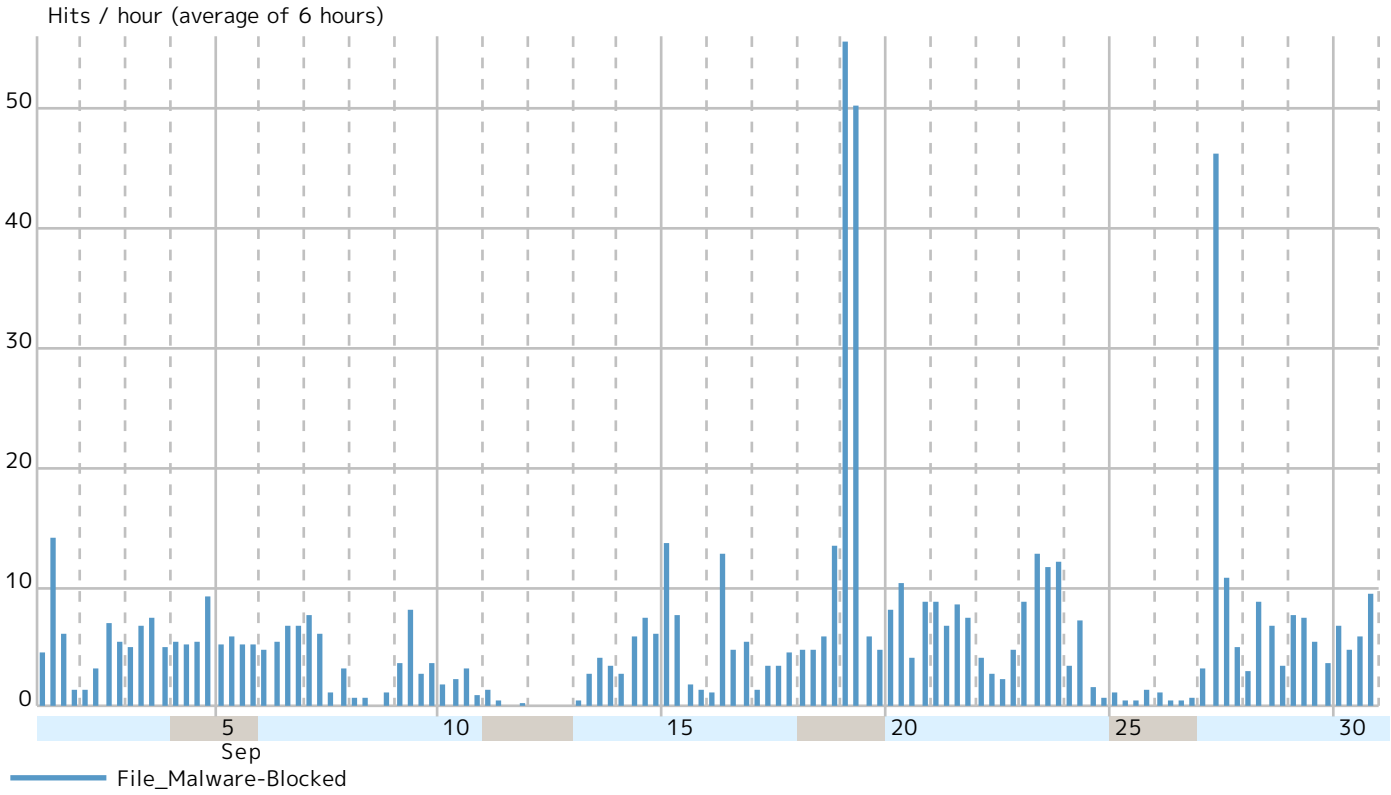
Report

Records by src IP		Hits	%
160.16.68.119	Tokyo, Japan	603	14.6 %
195.201.138.84	Germany	578	14.0 %
185.46.188.30	Ukraine	322	7.8 %
117.53.47.75	Indonesia	224	5.4 %
5.9.196.90	Germany	212	5.1 %
204.13.232.166	United States	128	3.1 %
89.253.224.78	Russia	110	2.7 %
38.103.244.230	United States	101	2.4 %
104.255.168.164	Los Angeles, California 90017, United States	86	2.1 %
45.144.225.128	Netherlands	79	1.9 %
92.62.129.23	Vilnius, Lithuania	79	1.9 %
45.137.20.129	Bangladesh	78	1.9 %
139.59.34.136	Bengaluru, India	78	1.9 %
103.87.172.226	India	77	1.9 %
195.133.18.63	Czechia	60	1.5 %
185.83.145.223	Turkey	52	1.3 %
2.56.59.124	Dulles, Virginia 20103, United States	52	1.3 %
195.33.210.155	Antakya, Turkey	51	1.2 %
2.56.59.128	Dulles, Virginia 20103, United States	43	1.0 %
143.110.243.34	Bengaluru, India	40	1.0 %
178.62.19.252	London, United Kingdom	40	1.0 %
185.85.207.154	Turkey	38	0.9 %
82.194.91.222	Spain	36	0.9 %
80.77.157.4	Skopje, 1000 North Macedonia	33	0.8 %
78.31.23.196	Russia	33	0.8 %
212.192.241.71	Czechia	28	0.7 %
185.222.58.104	Bangladesh	28	0.7 %
92.51.147.213	Strasbourg, France	28	0.7 %
46.183.221.24	Moscow, Russia	23	0.6 %
185.222.57.172	Amsterdam, Netherlands	22	0.5 %
Others		764	18.5 %
Total		**4.13k**	**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.