Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-01-01 00:00:00 CET
To: 2023-02-01 00:00:00 CET

Report

Table of Contents

Report run by
jens

SMC version
7.0.1, build 11318

Update version
1551

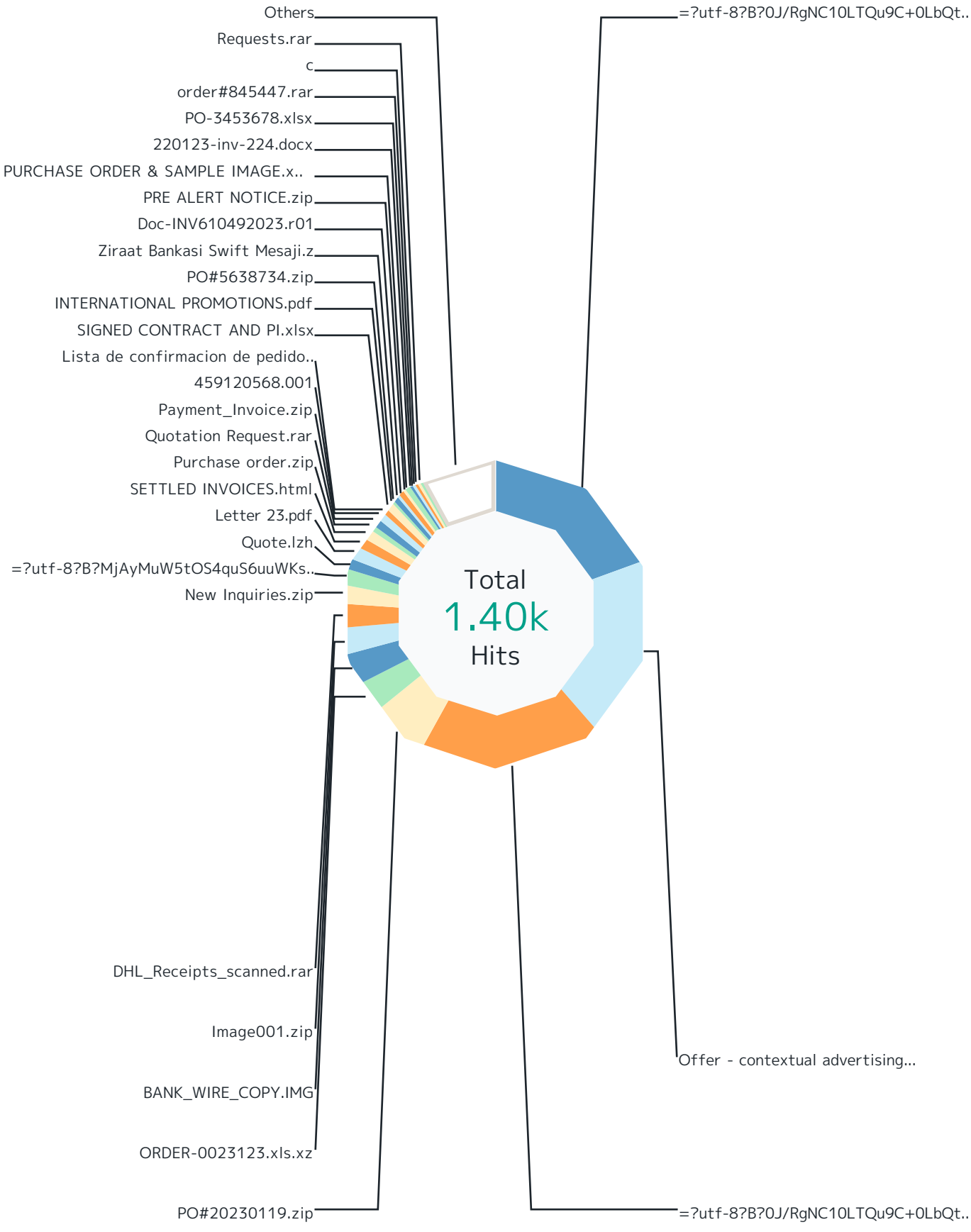
Report started
2023-02-02 14:33:45 CET

Report run time
07:09:30

Filters used
Match All

Report

Virenfilterung MXe



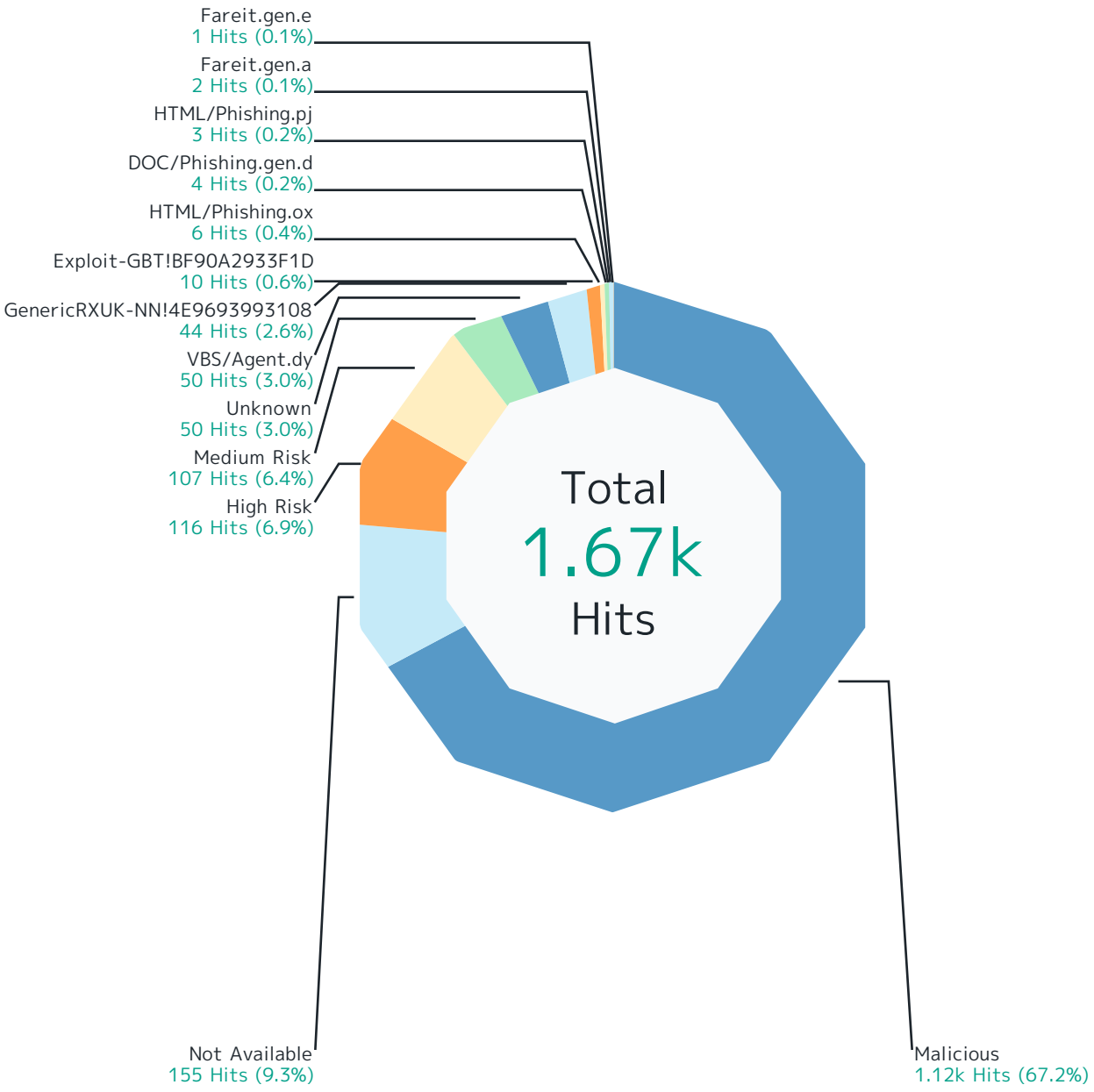
Report

Records by file name	Hits	%
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtSAtINC60L7QvdGC0LXQutGB0YLQvdCw?==?utf-8?B?0Y8g0YDQtdC60Lv..	271	19.3 %
Offer - contextual advertising.docx	271	19.3 %
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtS5kb2N4?=	271	19.3 %
PO#20230119.zip	88	6.3 %
ORDER-0023123.xls.xz	47	3.3 %
BANK_WIRE_COPY.IMG	45	3.2 %
Image001.zip	38	2.7 %
DHL_Receipts_scanned.rar	36	2.6 %
New Inquiries.zip	30	2.1 %
=?utf-8?B?MjAyMuW5tOS4quS6uuWKs+WKqOihpei0tC5kb2N4?=	20	1.4 %
Quote.lzh	18	1.3 %
Letter 23.pdf	18	1.3 %
SETTLED INVOICES.html	16	1.1 %
Purchase order.zip	14	1.0 %
Quotation Request.rar	11	0.8 %
Payment_Invoice.zip	10	0.7 %
459120568.001	10	0.7 %
Lista de confirmacion de pedido.zip	10	0.7 %
SIGNED CONTRACT AND PI.xlsx	10	0.7 %
INTERNATIONAL PROMOTIONS.pdf	6	0.4 %
PO#5638734.zip	6	0.4 %
Ziraat Bankasi Swift Mesaji.z	6	0.4 %
Doc-INV610492023.r01	6	0.4 %
PRE ALERT NOTICE.zip	6	0.4 %
PURCHASE ORDER & SAMPLE IMAGE.xlsx	5	0.4 %
220123-inv-224.docx	4	0.3 %
PO-3453678.xlsx	4	0.3 %
order#845447.rar	4	0.3 %
c	4	0.3 %
Requests.rar	4	0.3 %
Others	114	8.1 %
Total	**1.40k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.



Report

Scan Result	Hits	%
Malicious	**1.12k**	**67.2 %**
File_Microsoft-Office-Open-XML-Document	815	48.7 %
File_Microsoft-Windows-Executable	178	10.6 %
File_Zip-Archive	54	3.2 %
File_Rar-Archive	22	1.3 %
File_HTML	19	1.1 %
File_PDF	18	1.1 %
File_Office-Open-XML-Package-Relations-Item	6	0.4 %
File_7z-Archive	5	0.3 %
File_ISO-9660-Disk-Image	3	0.2 %
File_Microsoft-OLE	2	0.1 %
File_OneNote-Document	1	0.1 %
File_Tar-Archive	1	0.1 %
Not Available	**155**	**9.3 %**
File_Zip-Archive	142	8.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.5 %
File_Microsoft-Office-Open-XML-Document	4	0.2 %
High Risk	**116**	**6.9 %**
File_Rar-Archive	70	4.2 %
File_Microsoft-Windows-Executable	14	0.8 %
File_Zip-Archive	9	0.5 %
File_PDF	6	0.4 %
File_RTF	5	0.3 %
File_JavaScript	4	0.2 %
File_ISO-9660-Disk-Image	3	0.2 %
File_Microsoft-Cabinet-Archive	3	0.2 %
File_HTML	1	0.1 %
File_Type-Unknown	1	0.1 %
Medium Risk	**107**	**6.4 %**
File_Microsoft-Windows-Executable	64	3.8 %
File_Zip-Archive	18	1.1 %
File_XML	9	0.5 %
File_HTML	8	0.5 %
File_Microsoft-Cabinet-Archive	2	0.1 %
File_Type-Unknown	2	0.1 %
File_ISO-9660-Disk-Image	1	0.1 %

Report

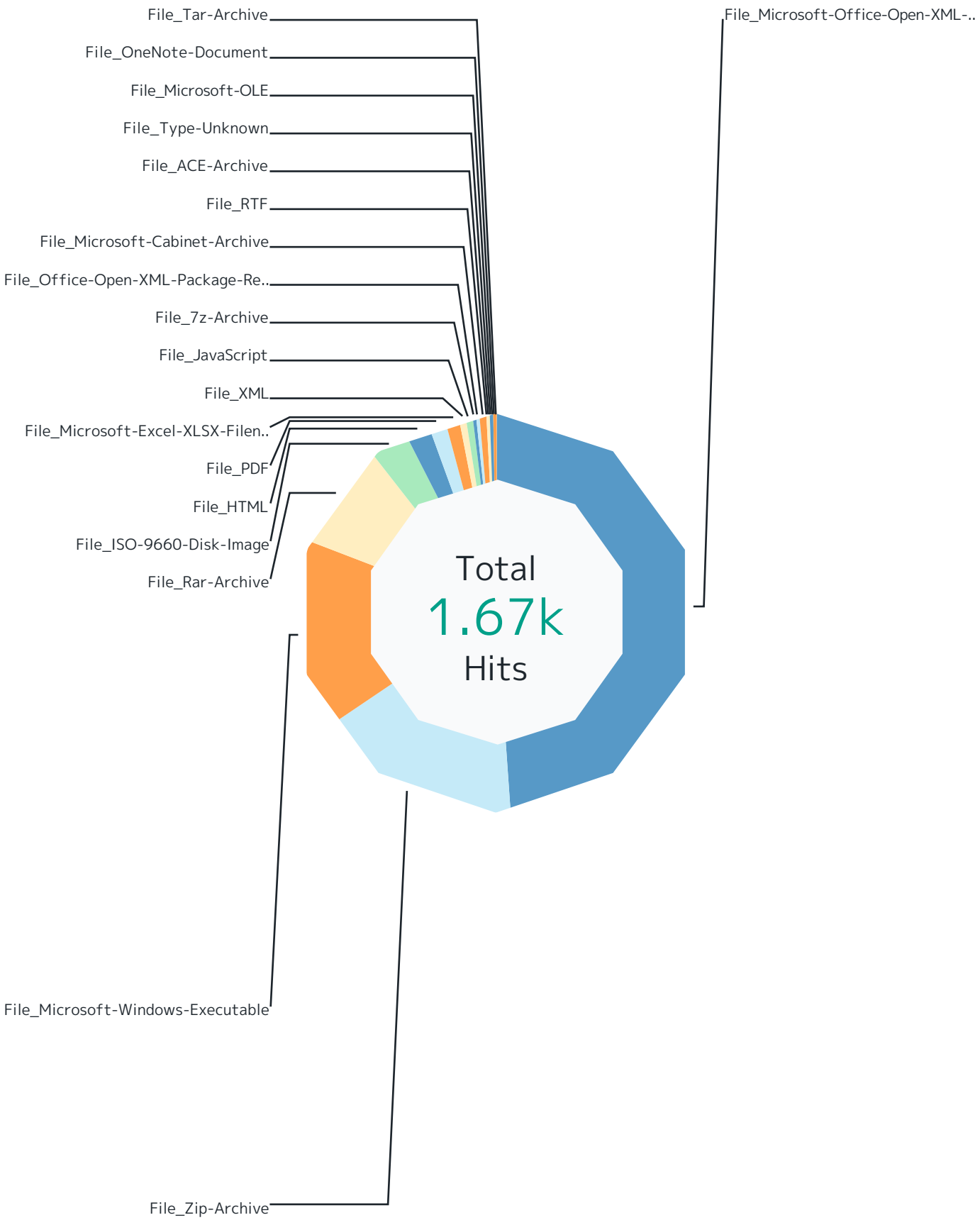
Scan Result	Hits	%
File_JavaScript	1	0.1 %
File_7z-Archive	1	0.1 %
File_OneNote-Document	1	0.1 %
Unknown	**50**	**3.0 %**
File_Zip-Archive	50	3.0 %
VBS/Agent.dy	**50**	**3.0 %**
File_Rar-Archive	50	3.0 %
GenericRXUK-NN!4E9693993108	**44**	**2.6 %**
File_ISO-9660-Disk-Image	44	2.6 %
Exploit-GBT!BF90A2933F1D	**10**	**0.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.6 %
HTML/Phishing.ox	**6**	**0.4 %**
File_HTML	6	0.4 %
DOC/Phishing.gen.d	**4**	**0.2 %**
File_Zip-Archive	4	0.2 %
HTML/Phishing.pj	**3**	**0.2 %**
File_JavaScript	3	0.2 %
Fareit.gen.a	**2**	**0.1 %**
File_ACE-Archive	2	0.1 %
Fareit.gen.e	**1**	**0.1 %**
File_ACE-Archive	1	0.1 %
Total	**1.67k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Tar-Archive
File_OneNote-Document
File_Microsoft-OLE
File_Type-Unknown
File_ACE-Archive
File_RTF
File_Microsoft-Cabinet-Archive
File_Office-Open-XML-Package-Re..
File_7z-Archive
File_JavaScript
File_XML
File_Microsoft-Excel-XLSX-Filen..
File_PDF
File_HTML
File_ISO-9660-Disk-Image
File_Rar-Archive
File_Microsoft-Office-Open-XML-..
File_Microsoft-Windows-Executable
File_Zip-Archive
Total
1.67k
Hits

Report

Responding Scanner	Hits	%
File_Microsoft-Office-Open-XML-Document	**819**	**49.0 %**
Malicious	815	48.7 %
Not Available	4	0.2 %
File_Zip-Archive	**277**	**16.6 %**
Not Available	142	8.5 %
Malicious	54	3.2 %
Unknown	50	3.0 %
Medium Risk	18	1.1 %
High Risk	9	0.5 %
DOC/Phishing.gen.d	4	0.2 %
File_Microsoft-Windows-Executable	**256**	**15.3 %**
Malicious	178	10.6 %
Medium Risk	64	3.8 %
High Risk	14	0.8 %
File_Rar-Archive	**142**	**8.5 %**
High Risk	70	4.2 %
VBS/Agent.dy	50	3.0 %
Malicious	22	1.3 %
File_ISO-9660-Disk-Image	**51**	**3.1 %**
GenericRXUK-NN!4E9693993108	44	2.6 %
Malicious	3	0.2 %
High Risk	3	0.2 %
Medium Risk	1	0.1 %
File_HTML	**34**	**2.0 %**
Malicious	19	1.1 %
Medium Risk	8	0.5 %
HTML/Phishing.ox	6	0.4 %
High Risk	1	0.1 %
File_PDF	**24**	**1.4 %**
Malicious	18	1.1 %
High Risk	6	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	**19**	**1.1 %**
Exploit-GBT!BF90A2933F1D	10	0.6 %
Not Available	9	0.5 %
File_XML	**9**	**0.5 %**
Medium Risk	9	0.5 %

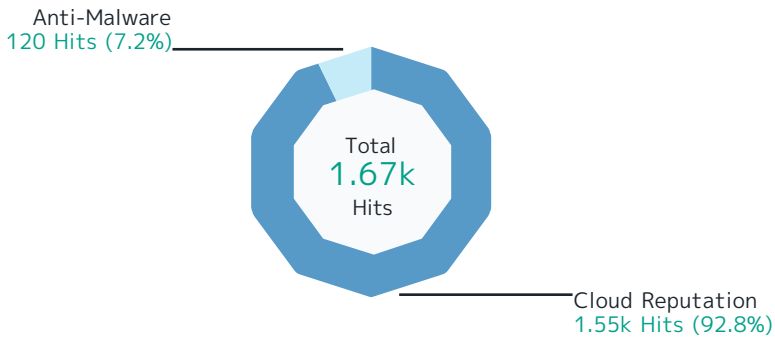
Report

Responding Scanner	Hits	%
File_JavaScript	**8**	**0.5 %**
High Risk	4	0.2 %
HTML/Phishing.pj	3	0.2 %
Medium Risk	1	0.1 %
File_7z-Archive	**6**	**0.4 %**
Malicious	5	0.3 %
Medium Risk	1	0.1 %
File_Office-Open-XML-Package-Relations-Item	**6**	**0.4 %**
Malicious	6	0.4 %
File_Microsoft-Cabinet-Archive	**5**	**0.3 %**
High Risk	3	0.2 %
Medium Risk	2	0.1 %
File_RTF	**5**	**0.3 %**
High Risk	5	0.3 %
File_ACE-Archive	**3**	**0.2 %**
Fareit.gen.a	2	0.1 %
Fareit.gen.e	1	0.1 %
File_Type-Unknown	**3**	**0.2 %**
Medium Risk	2	0.1 %
High Risk	1	0.1 %
File_Microsoft-OLE	**2**	**0.1 %**
Malicious	2	0.1 %
File_OneNote-Document	**2**	**0.1 %**
Malicious	1	0.1 %
Medium Risk	1	0.1 %
File_Tar-Archive	**1**	**0.1 %**
Malicious	1	0.1 %
Total	**1.67k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**1.55k**	**92.8 %**
File_Microsoft-Office-Open-XML-Document	819	49.0 %
File_Zip-Archive	273	16.3 %
File_Microsoft-Windows-Executable	256	15.3 %
File_Rar-Archive	92	5.5 %
File_HTML	28	1.7 %
File_PDF	24	1.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.5 %
File_XML	9	0.5 %
File_ISO-9660-Disk-Image	7	0.4 %
File_7z-Archive	6	0.4 %
File_Office-Open-XML-Package-Relations-Item	6	0.4 %
File_JavaScript	5	0.3 %
File_Microsoft-Cabinet-Archive	5	0.3 %
File_RTF	5	0.3 %
File_Type-Unknown	3	0.2 %
File_Microsoft-OLE	2	0.1 %
File_OneNote-Document	2	0.1 %
File_Tar-Archive	1	0.1 %
Anti-Malware	**120**	**7.2 %**
File_Rar-Archive	50	3.0 %
File_ISO-9660-Disk-Image	44	2.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.6 %
File_HTML	6	0.4 %
File_Zip-Archive	4	0.2 %
File_JavaScript	3	0.2 %
File_ACE-Archive	3	0.2 %
Total	**1.67k**	**100 %**

Report

Virenfilterung SRC IPs

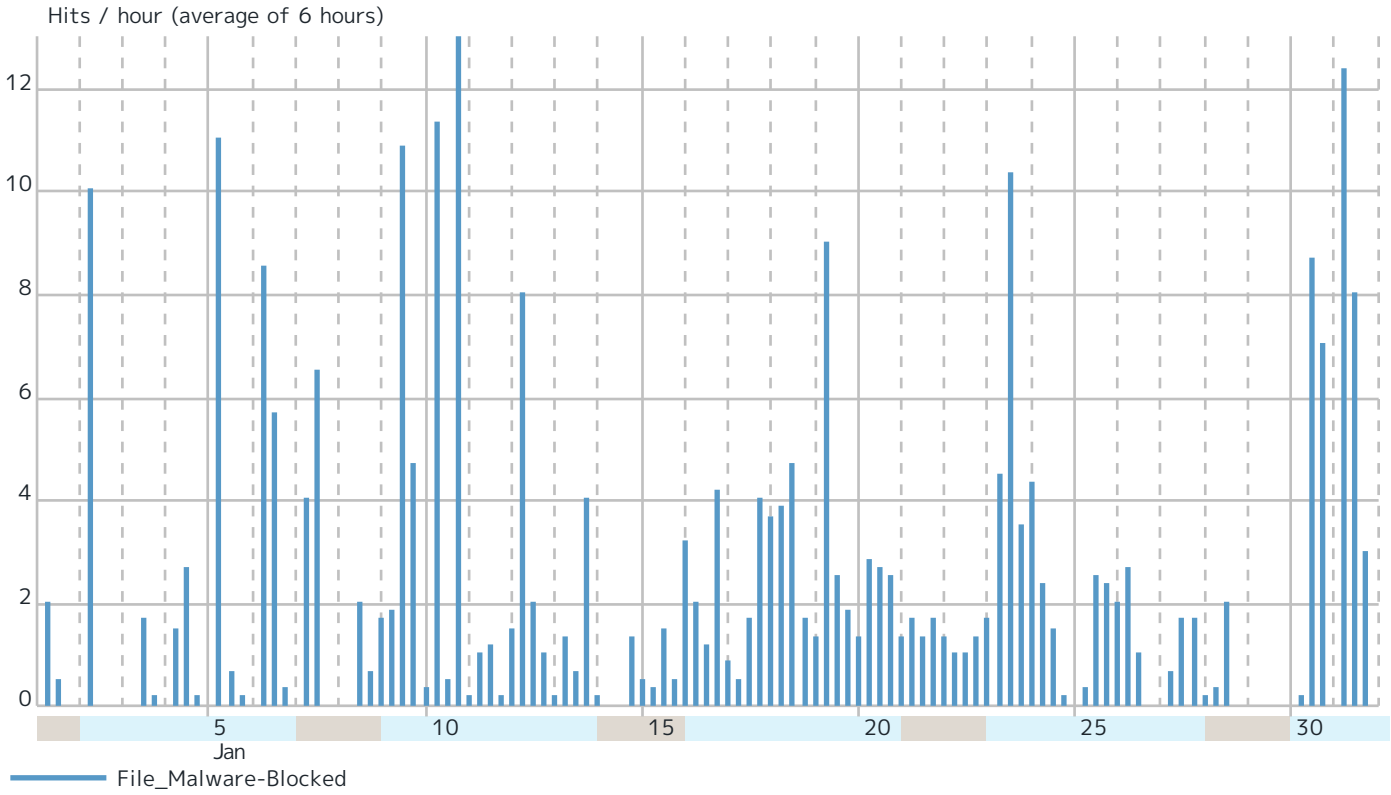
Report

Records by src IP		Hits	%
31.192.233.15	Atlanta, Georgia 30301, United States	176	10.5 %
103.14.12.131	Japan	76	4.5 %
62.217.181.96	Russia	63	3.8 %
45.95.235.83	Russia	60	3.6 %
108.167.176.71	United States	50	3.0 %
193.169.253.233	Poland	45	2.7 %
202.181.235.156	Hong Kong	36	2.2 %
45.147.251.112	Madrid, Spain	36	2.2 %
109.71.10.158	Moscow, Russia	33	2.0 %
94.26.250.110	St Petersburg, Russia	33	2.0 %
193.168.46.116	Russia	33	2.0 %
109.71.10.156	Moscow, Russia	33	2.0 %
45.141.79.123	Russia	33	2.0 %
213.232.228.5	Moscow, Russia	33	2.0 %
45.130.8.99	Moscow, Russia	33	2.0 %
92.52.217.47	Hungary	28	1.7 %
109.71.10.154	Moscow, Russia	24	1.4 %
77.83.100.158	Warsaw, Poland	21	1.3 %
88.198.10.91	Germany	20	1.2 %
217.116.192.52	Ankara, Turkey	20	1.2 %
187.108.207.81	Cananeia, Brazil	17	1.0 %
194.163.137.230	Düsseldorf, Germany	16	1.0 %
137.74.7.150	Warsaw, Poland	15	0.9 %
185.228.234.42	Moscow, Russia	15	0.9 %
185.135.81.25	Russia	15	0.9 %
45.130.42.159	Russia	15	0.9 %
109.71.10.155	Moscow, Russia	15	0.9 %
45.130.8.14	Moscow, Russia	15	0.9 %
91.194.3.82	Russia	12	0.7 %
77.72.131.7	Berlin, Germany	12	0.7 %
Others		639	38.2 %
Total		**1.67k**	**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.