Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-12-01 00:00:00 CET
To: 2023-01-01 00:00:00 CET

Report

Report run by
jens

SMC version
7.0.1, build 11318

Update version
1540

Report started
2023-01-01 11:49:53 CET

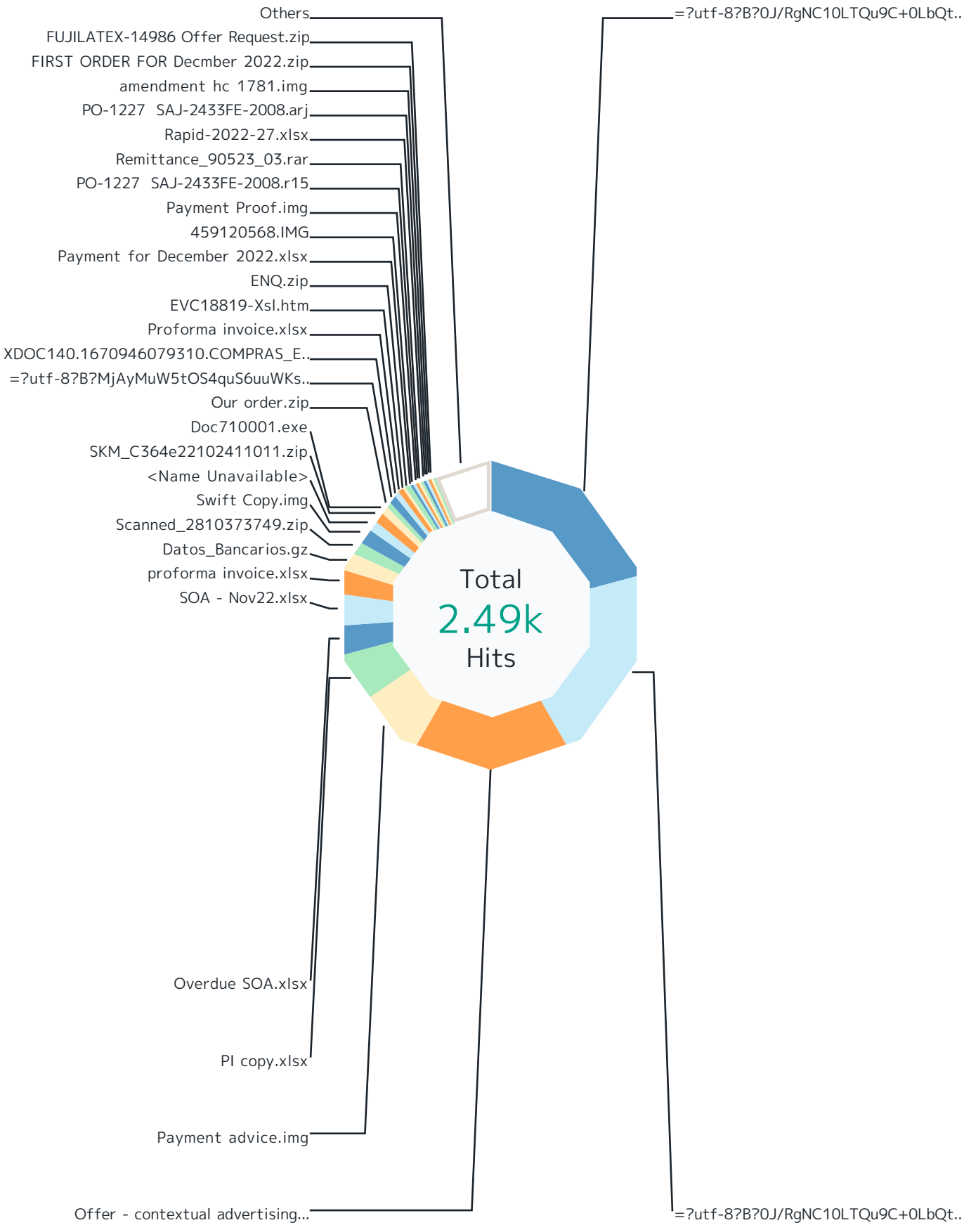
Report run time
04:46:50

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



Report

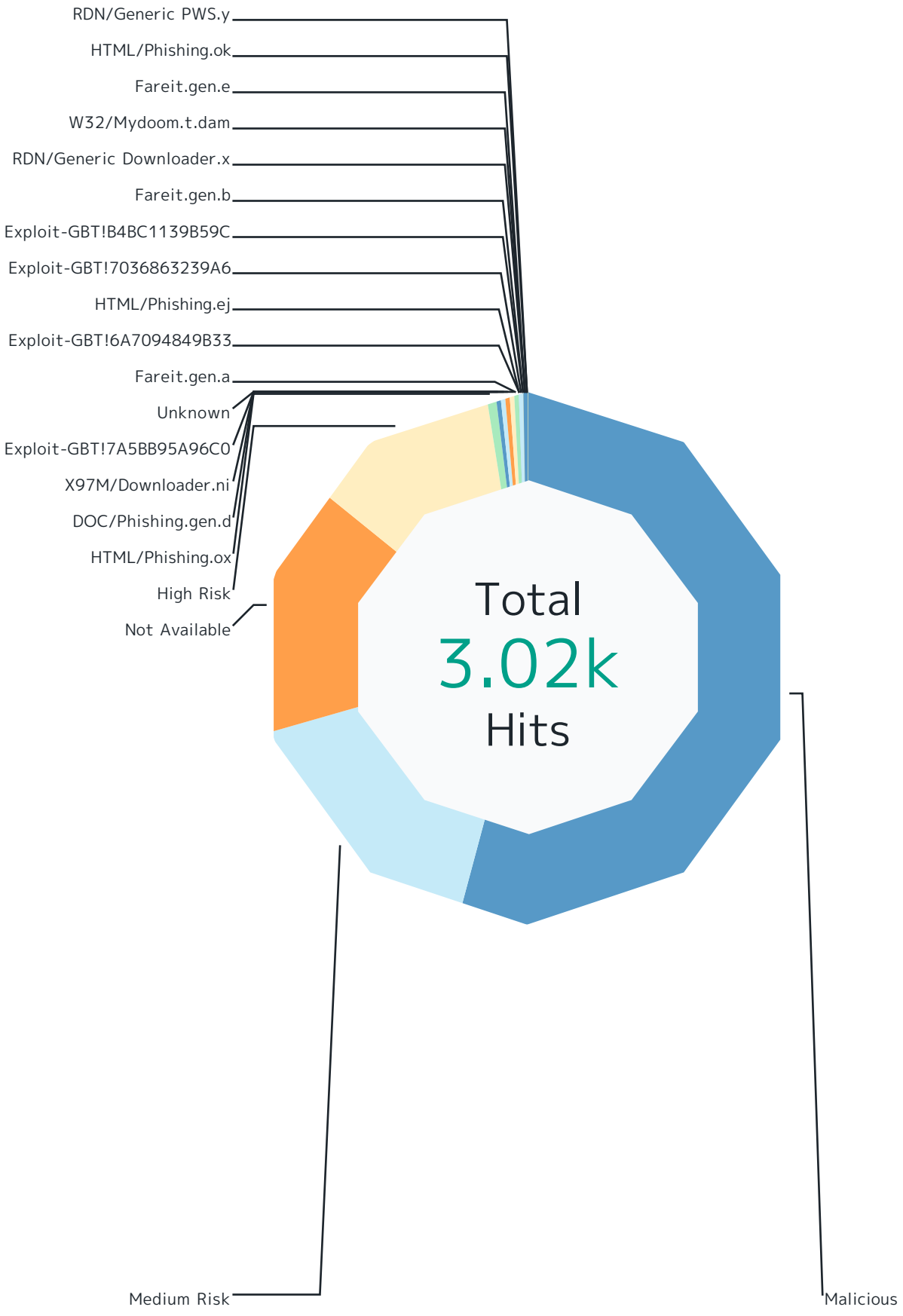
Records by file name	Hits	%
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtSAtINC60L7QvdGC0LXQutGB0YLQvdCw?==?utf-8?B?0Y8g0YDQtdC60Lv..	517	20.8 %
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtS5kb2N4?=	517	20.8 %
Offer - contextual advertising.docx	419	16.8 %
Payment advice.img	180	7.2 %
PI copy.xlsx	129	5.2 %
Overdue SOA.xlsx	79	3.2 %
SOA - Nov22.xlsx	77	3.1 %
proforma invoice.xlsx	66	2.7 %
Datos_Bancarios.gz	47	1.9 %
Scanned_2810373749.zip	38	1.5 %
Swift Copy.img	35	1.4 %
<Name Unavailable>	30	1.2 %
SKM_C364e22102411011.zip	26	1.0 %
Doc710001.exe	20	0.8 %
Our order.zip	19	0.8 %
=?utf-8?B?MjAyMuW5tOS4quS6uuWKs+WKqOihpei0tC5kb2N4?=	18	0.7 %
XDOC140.1670946079310.COMPRAS_ESP_pdf.img	15	0.6 %
Proforma invoice.xlsx	11	0.4 %
EVC18819-Xsl.htm	11	0.4 %
ENQ.zip	11	0.4 %
Payment for December 2022.xlsx	8	0.3 %
459120568.IMG	8	0.3 %
Payment Proof.img	8	0.3 %
PO-1227 SAJ-2433FE-2008.r15	7	0.3 %
Remittance_90523_03.rar	7	0.3 %
Rapid-2022-27.xlsx	7	0.3 %
PO-1227 SAJ-2433FE-2008.arj	7	0.3 %
amendment hc 1781.img	6	0.2 %
FIRST ORDER FOR Decmber 2022.zip	5	0.2 %
FUJILATEX-14986 Offer Request.zip	5	0.2 %
Others	154	6.2 %
Total	**2.49k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


RDN/Generic PWS.y
HTML/Phishing.ok
Fareit.gen.e
W32/Mydoom.t.dam
RDN/Generic Downloader.x
Fareit.gen.b
Exploit-GBT!B4BC1139B59C
Exploit-GBT!7036863239A6
HTML/Phishing.ej
Exploit-GBT!6A7094849B33
Fareit.gen.a
Unknown
Exploit-GBT!7A5BB95A96C0
X97M/Downloader.ni
DOC/Phishing.gen.d
HTML/Phishing.ox
High Risk
Not Available
Total
3.02k
Hits
Medium Risk
Malicious

Report

Scan Result	Hits	%
Malicious	**1.64k**	**54.2 %**
File_Microsoft-Office-Open-XML-Document	1.10k	36.4 %
File_ISO-9660-Disk-Image	233	7.7 %
File_Microsoft-Windows-Executable	109	3.6 %
File_Microsoft-Equation-Editor-Document	91	3.0 %
File_Zip-Archive	47	1.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	25	0.8 %
File_Rar-Archive	17	0.6 %
File_Type-Unknown	5	0.2 %
File_HTML	3	0.1 %
File_Batch-File	3	0.1 %
File_PDF	2	0.1 %
File_7z-Archive	2	0.1 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_ACE-Archive	1	0.0 %
Medium Risk	**491**	**16.3 %**
File_XML	260	8.6 %
File_Microsoft-Office-Open-XML-Document	140	4.6 %
File_Microsoft-Windows-Executable	25	0.8 %
File_ISO-9660-Disk-Image	21	0.7 %
File_PDF	16	0.5 %
File_Zip-Archive	12	0.4 %
File_Self-Extracting-Zip-Archive	8	0.3 %
File_Type-Unknown	3	0.1 %
File_JavaScript	3	0.1 %
File_OneNote-Document	2	0.1 %
File_Rar-Archive	1	0.0 %
Not Available	**462**	**15.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	337	11.2 %
File_Zip-Archive	125	4.1 %
High Risk	**353**	**11.7 %**
File_Microsoft-Office-Open-XML-Document	217	7.2 %
File_Microsoft-Windows-Executable	39	1.3 %
File_Zip-Archive	27	0.9 %
File_ISO-9660-Disk-Image	19	0.6 %
File_Microsoft-OLE	14	0.5 %

Report

Scan Result	Hits	%
File_Rar-Archive	12	0.4 %
File_PDF	10	0.3 %
File_Type-Unknown	5	0.2 %
File_Microsoft-Cabinet-Archive	3	0.1 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
File_RTF	2	0.1 %
File_Self-Extracting-Zip-Archive	1	0.0 %
File_7z-Archive	1	0.0 %
HTML/Phishing.ox	**16**	**0.5 %**
File_HTML	16	0.5 %
DOC/Phishing.gen.d	**11**	**0.4 %**
File_Zip-Archive	11	0.4 %
X97M/Downloader.ni	**10**	**0.3 %**
File_Zip-Archive	10	0.3 %
Exploit-GBT!7A5BB95A96C0	**9**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.3 %
Unknown	**8**	**0.3 %**
File_Zip-Archive	8	0.3 %
Fareit.gen.a	**4**	**0.1 %**
File_ACE-Archive	4	0.1 %
Exploit-GBT!6A7094849B33	**4**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
HTML/Phishing.ej	**2**	**0.1 %**
File_HTML	2	0.1 %
Exploit-GBT!7036863239A6	**2**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
Exploit-GBT!B4BC1139B59C	**2**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
Fareit.gen.b	**2**	**0.1 %**
File_ACE-Archive	2	0.1 %
RDN/Generic Downloader.x	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
W32/Mydoom.t.dam	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
Fareit.gen.e	**1**	**0.0 %**
File_ACE-Archive	1	0.0 %

Report

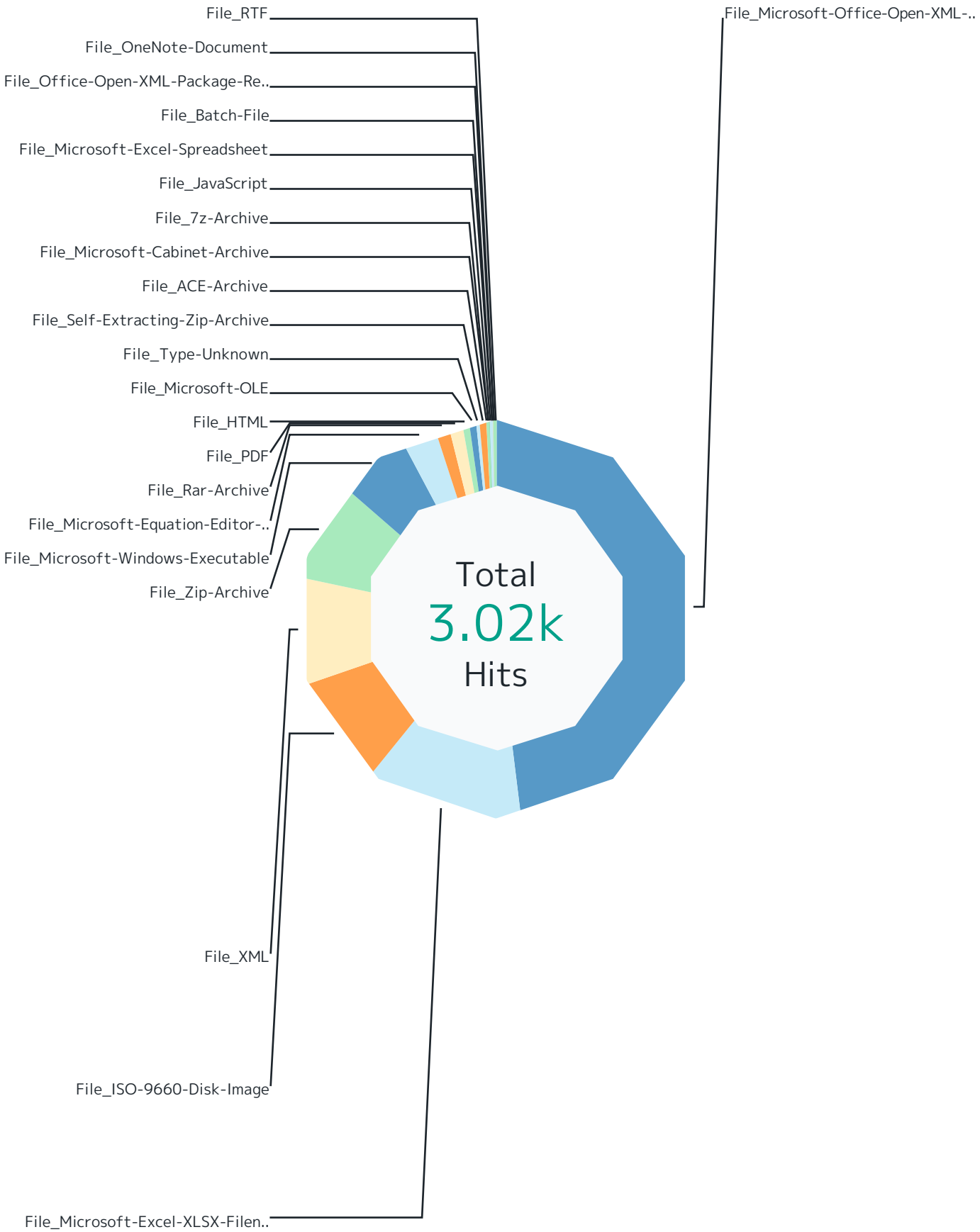
Scan Result	Hits	%
HTML/Phishing.ok	**1**	**0.0 %**
File_HTML	1	0.0 %
RDN/Generic PWS.y	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Total	**3.02k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_RTF
File_OneNote-Document
File_Office-Open-XML-Package-Re..
File_Batch-File
File_Microsoft-Excel-Spreadsheet
File_JavaScript
File_7z-Archive
File_Microsoft-Cabinet-Archive
File_ACE-Archive
File_Self-Extracting-Zip-Archive
File_Type-Unknown
File_Microsoft-OLE
File_HTML
File_PDF
File_Rar-Archive
File_Microsoft-Equation-Editor-..
File_Microsoft-Windows-Executable
File_Zip-Archive
File_XML
File_ISO-9660-Disk-Image
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Office-Open-XML-..
Total
3.02k
Hits

Report

Responding Scanner	Hits	%
File_Microsoft-Office-Open-XML-Document	**1.46k**	**48.2 %**
Malicious	1.10k	36.4 %
High Risk	217	7.2 %
Medium Risk	140	4.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	**379**	**12.5 %**
Not Available	337	11.2 %
Malicious	25	0.8 %
Exploit-GBT!7A5BB95A96C0	9	0.3 %
Exploit-GBT!6A7094849B33	4	0.1 %
Exploit-GBT!7036863239A6	2	0.1 %
Exploit-GBT!B4BC1139B59C	2	0.1 %
File_ISO-9660-Disk-Image	**273**	**9.0 %**
Malicious	233	7.7 %
Medium Risk	21	0.7 %
High Risk	19	0.6 %
File_XML	**260**	**8.6 %**
Medium Risk	260	8.6 %
File_Zip-Archive	**241**	**8.0 %**
Not Available	125	4.1 %
Malicious	47	1.6 %
High Risk	27	0.9 %
Medium Risk	12	0.4 %
DOC/Phishing.gen.d	11	0.4 %
X97M/Downloader.ni	10	0.3 %
Unknown	8	0.3 %
W32/Mydoom.t.dam	1	0.0 %
File_Microsoft-Windows-Executable	**173**	**5.7 %**
Malicious	109	3.6 %
High Risk	39	1.3 %
Medium Risk	25	0.8 %
File_Microsoft-Equation-Editor-Document	**91**	**3.0 %**
Malicious	91	3.0 %
File_Rar-Archive	**33**	**1.1 %**
Malicious	17	0.6 %
High Risk	12	0.4 %
RDN/Generic Downloader.x	2	0.1 %

Report

Responding Scanner	Hits	%
Medium Risk	1	0.0 %
RDN/Generic PWS.y	1	0.0 %
File_PDF	**28**	**0.9 %**
Medium Risk	16	0.5 %
High Risk	10	0.3 %
Malicious	2	0.1 %
File_HTML	**22**	**0.7 %**
HTML/Phishing.ox	16	0.5 %
Malicious	3	0.1 %
HTML/Phishing.ej	2	0.1 %
HTML/Phishing.ok	1	0.0 %
File_Microsoft-OLE	**14**	**0.5 %**
High Risk	14	0.5 %
File_Type-Unknown	**13**	**0.4 %**
Malicious	5	0.2 %
High Risk	5	0.2 %
Medium Risk	3	0.1 %
File_Self-Extracting-Zip-Archive	**9**	**0.3 %**
Medium Risk	8	0.3 %
High Risk	1	0.0 %
File_ACE-Archive	**8**	**0.3 %**
Fareit.gen.a	4	0.1 %
Fareit.gen.b	2	0.1 %
Malicious	1	0.0 %
Fareit.gen.e	1	0.0 %
File_Microsoft-Cabinet-Archive	**3**	**0.1 %**
High Risk	3	0.1 %
File_7z-Archive	**3**	**0.1 %**
Malicious	2	0.1 %
High Risk	1	0.0 %
File_JavaScript	**3**	**0.1 %**
Medium Risk	3	0.1 %
File_Microsoft-Excel-Spreadsheet	**3**	**0.1 %**
High Risk	3	0.1 %
File_Batch-File	**3**	**0.1 %**
Malicious	3	0.1 %

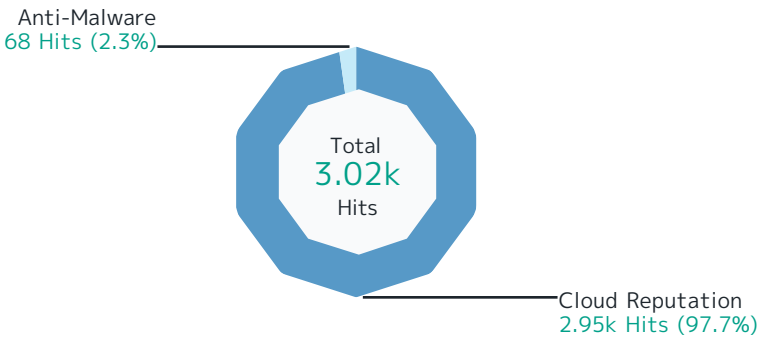
Report

Responding Scanner	Hits	%
File_Office-Open-XML-Package-Relations-Item	**2**	**0.1 %**
Malicious	2	0.1 %
File_OneNote-Document	**2**	**0.1 %**
Medium Risk	2	0.1 %
File_RTF	**2**	**0.1 %**
High Risk	2	0.1 %
Total	**3.02k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**2.95k**	**97.7 %**
File_Microsoft-Office-Open-XML-Document	1.46k	48.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	362	12.0 %
File_ISO-9660-Disk-Image	273	9.0 %
File_XML	260	8.6 %
File_Zip-Archive	219	7.3 %
File_Microsoft-Windows-Executable	173	5.7 %
File_Microsoft-Equation-Editor-Document	91	3.0 %
File_Rar-Archive	30	1.0 %
File_PDF	28	0.9 %
File_Microsoft-OLE	14	0.5 %
File_Type-Unknown	13	0.4 %
File_Self-Extracting-Zip-Archive	9	0.3 %
File_HTML	3	0.1 %
File_Microsoft-Cabinet-Archive	3	0.1 %
File_7z-Archive	3	0.1 %
File_JavaScript	3	0.1 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
File_Batch-File	3	0.1 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_OneNote-Document	2	0.1 %
File_RTF	2	0.1 %
File_ACE-Archive	1	0.0 %
Anti-Malware	**68**	**2.3 %**
File_Zip-Archive	22	0.7 %
File_HTML	19	0.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	17	0.6 %
File_ACE-Archive	7	0.2 %
File_Rar-Archive	3	0.1 %
Total	**3.02k**	**100 %**

Report

Virenfilterung SRC IPs

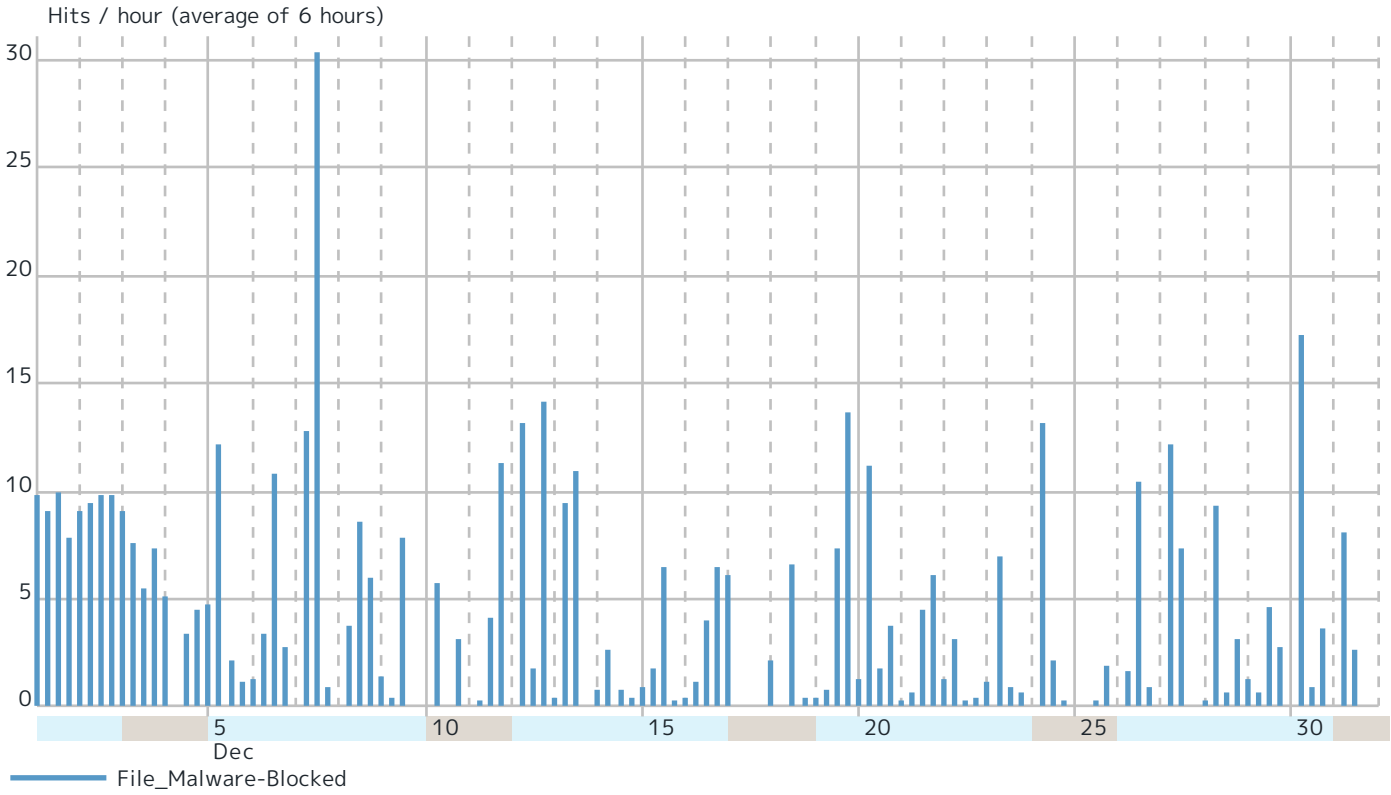
Report

Records by src IP		Hits	%
74.208.25.42	United States	702	23.2 %
95.214.55.190	Poland	180	6.0 %
119.75.6.251	Singapore	94	3.1 %
45.156.22.119	Hong Kong	76	2.5 %
45.141.76.94	Russia	66	2.2 %
147.135.125.95	Virginia, United States	44	1.5 %
84.21.172.150	Virginia, United States	38	1.3 %
185.216.71.120	Netherlands	35	1.2 %
77.223.106.106	Moscow, Russia	33	1.1 %
5.53.127.142	Moscow, Russia	33	1.1 %
45.130.42.171	Russia	33	1.1 %
45.130.8.118	Moscow, Russia	33	1.1 %
62.217.178.205	Russia	33	1.1 %
62.113.98.34	Russia	33	1.1 %
193.168.46.101	Russia	30	1.0 %
62.113.98.200	Russia	30	1.0 %
45.141.79.50	Russia	30	1.0 %
193.168.46.171	Russia	30	1.0 %
45.141.76.5	Russia	27	0.9 %
82.202.237.246	Moscow, Russia	27	0.9 %
96.125.164.115	United States	24	0.8 %
62.113.99.183	Russia	21	0.7 %
82.202.237.242	Moscow, Russia	21	0.7 %
45.147.176.138	Russia	20	0.7 %
45.130.8.14	Moscow, Russia	20	0.7 %
5.53.127.110	Moscow, Russia	20	0.7 %
81.163.24.163	Moscow, Russia	20	0.7 %
104.144.69.148	Amsterdam, Netherlands	20	0.7 %
94.156.33.175	Seychelles	16	0.5 %
5.188.76.92	Moscow, Russia	15	0.5 %
Others		1.22k	40.3 %
Total		**3.02k**	**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.