Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period
From: 2022-02-01 00:00:00
To: 2022-03-01 00:00:00

Report

Report run by
jens

SMC version
6.10.6, build 11161

Update version
1439

Report started
2022-03-01 07:40:21

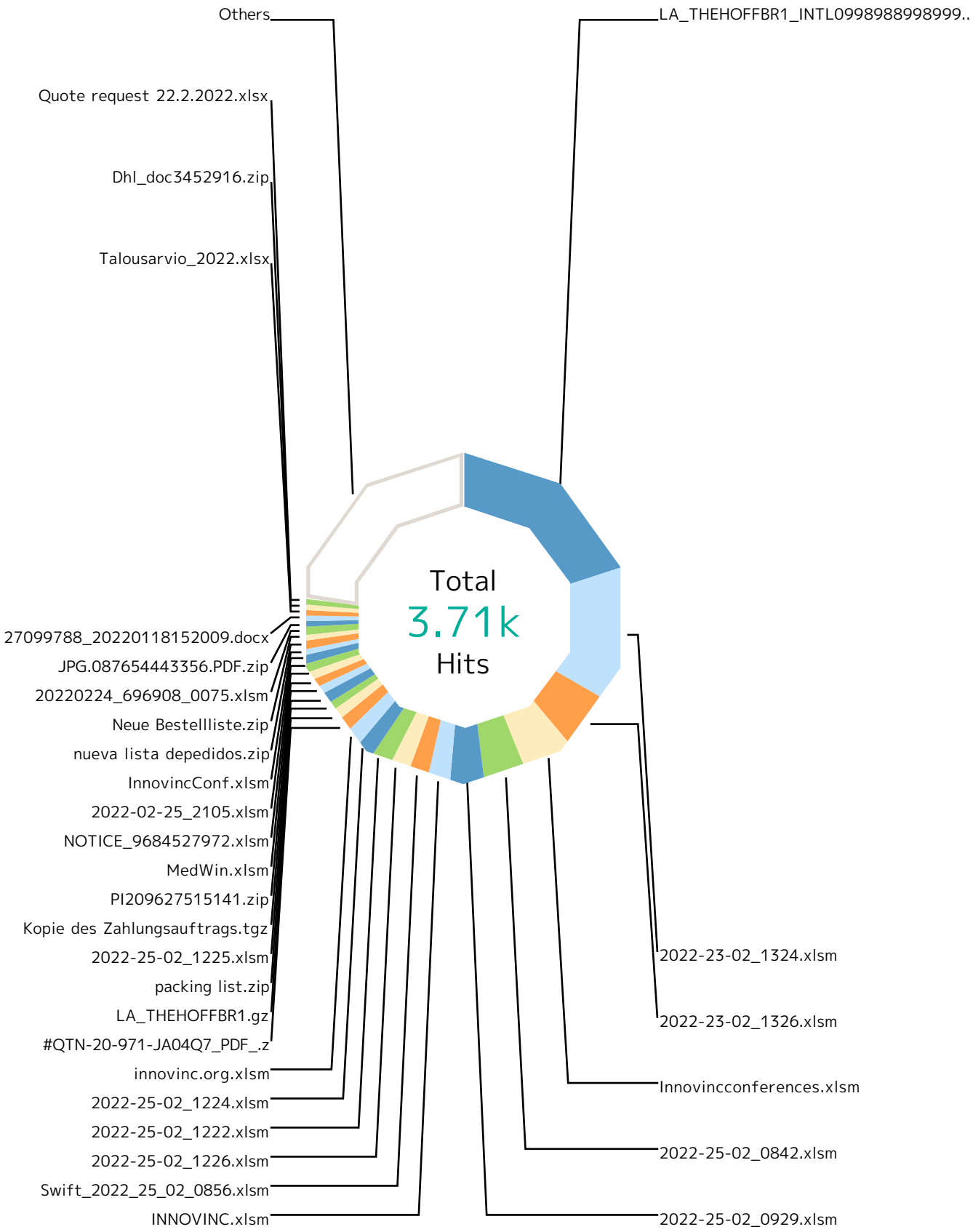
Report run time
01:45:38

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



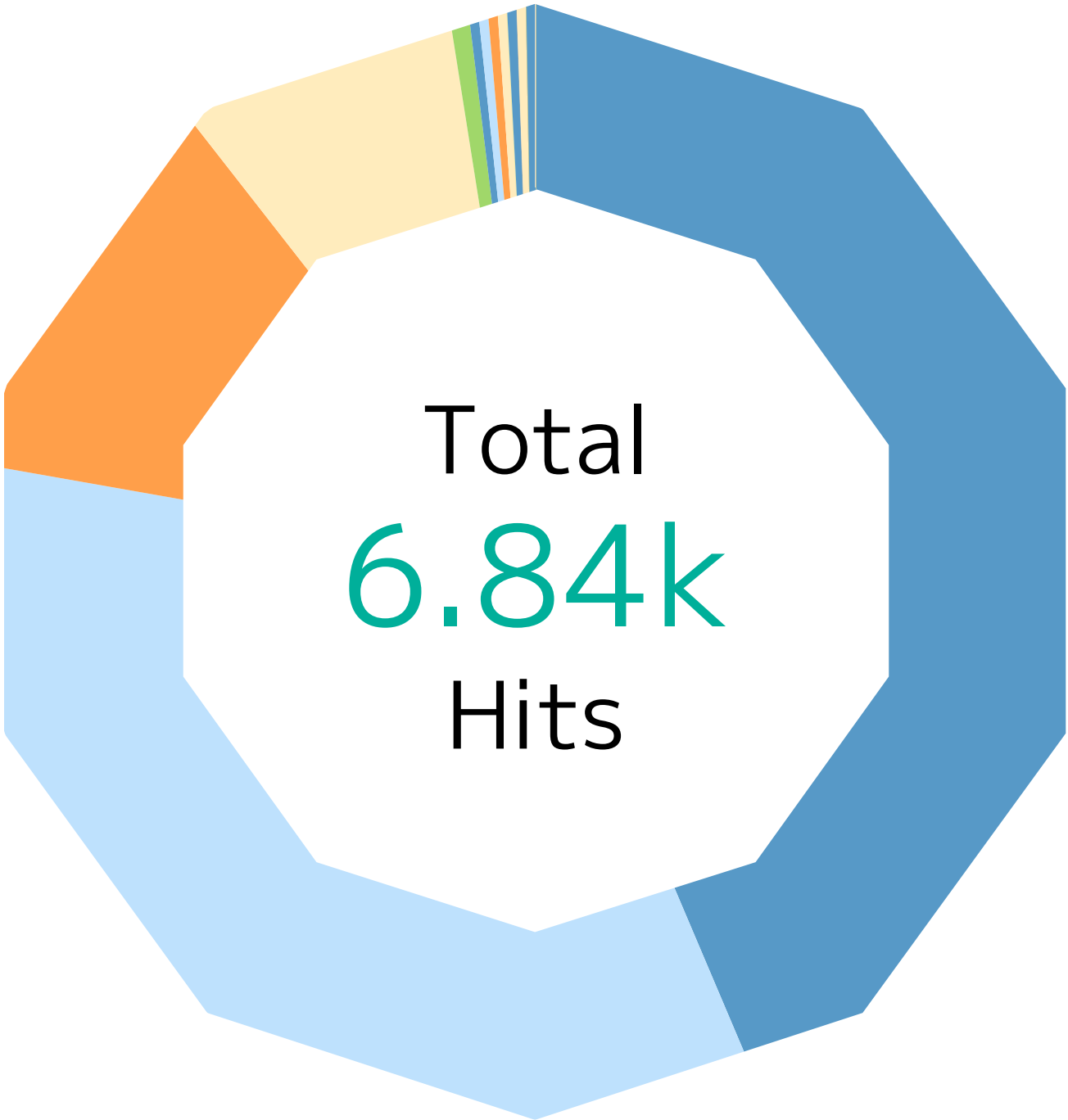
Report

Records by file name	Hits	%
LA_THEHOFFBR1_INTL09989889989999.lzh	743	20.0 %
2022-23-02_1324.xlsm	496	13.4 %
2022-23-02_1326.xlsm	201	5.4 %
Innovincconferences.xlsm	188	5.1 %
2022-25-02_0842.xlsm	151	4.1 %
2022-25-02_0929.xlsm	124	3.3 %
INNOVINC.xlsm	85	2.3 %
Swift_2022_25_02_0856.xlsm	77	2.1 %
2022-25-02_1226.xlsm	73	2.0 %
2022-25-02_1222.xlsm	71	1.9 %
2022-25-02_1224.xlsm	64	1.7 %
innovinc.org.xlsm	54	1.5 %
#QTN-20-971-JA04Q7_PDF_.z	52	1.4 %
LA_THEHOFFBR1.gz	39	1.1 %
packing list.zip	38	1.0 %
2022-25-02_1225.xlsm	36	1.0 %
Kopie des Zahlungsauftrags.tgz	36	1.0 %
PI209627515141.zip	33	0.9 %
MedWin.xlsm	31	0.8 %
NOTICE_9684527972.xlsm	29	0.8 %
2022-02-25_2105.xlsm	27	0.7 %
InnovincConf.xlsm	27	0.7 %
nueva lista depedidos.zip	25	0.7 %
Neue Bestellliste.zip	24	0.6 %
20220224_696908_0075.xlsm	24	0.6 %
JPG.087654443356.PDF.zip	22	0.6 %
27099788_20220118152009.docx	22	0.6 %
Talousarvio_2022.xlsx	22	0.6 %
Dhl_doc3452916.zip	22	0.6 %
Quote request 22.2.2022.xlsx	22	0.6 %
Others	854	23.0 %
Total	**3.71k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
6.84k
Hits

Report

Scan Result	Hits	%
Not Available	**2.98k**	**43.6 %**
File_Zip-Archive	2.91k	42.6 %
File_Microsoft-Excel-Spreadsheet	27	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	24	0.4 %
File_Microsoft-Office-Open-XML-Document	17	0.2 %
Malicious	**2.35k**	**34.3 %**
File_Microsoft-Windows-Executable	1.04k	15.2 %
File_XML	918	13.4 %
File_Zip-Archive	88	1.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	70	1.0 %
File_Rar-Archive	68	1.0 %
File_Type-Unknown	44	0.6 %
File_Office-Open-XML-Application-Properties-Part	28	0.4 %
File_ISO-9660-Disk-Image	26	0.4 %
File_PDF	23	0.3 %
File_Microsoft-Excel-97-Spreadsheet	13	0.2 %
File_Office-Open-XML-Package-Relations-Item	11	0.2 %
File_Microsoft-OLE	4	0.1 %
File_Microsoft-Equation-Editor-Document	4	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
File_ACE-Archive	2	0.0 %
File_XZ-Archive	2	0.0 %
File_JavaScript	2	0.0 %
File_7z-Archive	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	1	0.0 %
High Risk	**793**	**11.6 %**
File_XML	515	7.5 %
File_Microsoft-Windows-Executable	68	1.0 %
File_Zip-Archive	56	0.8 %
File_ISO-9660-Disk-Image	44	0.6 %
File_Rar-Archive	31	0.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	24	0.4 %
File_Office-Open-XML-Package-Relations-Item	15	0.2 %
File_7z-Archive	9	0.1 %
File_Type-Unknown	8	0.1 %

Report

Scan Result	Hits	%
File_Microsoft-OLE	7	0.1 %
File_Microsoft-Excel-97-Spreadsheet	6	0.1 %
File_ACE-Archive	5	0.1 %
File_HTML	2	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_XZ-Archive	1	0.0 %
File_LhArc-Archive	1	0.0 %
Medium Risk	**560**	**8.2 %**
File_XML	502	7.3 %
File_Office-Open-XML-Package-Relations-Item	22	0.3 %
File_Zip-Archive	16	0.2 %
File_ISO-9660-Disk-Image	6	0.1 %
File_Microsoft-Windows-Executable	4	0.1 %
File_Type-Unknown	4	0.1 %
File_Rar-Archive	2	0.0 %
File_LhArc-Archive	2	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
HTML/Phishing.he	**28**	**0.4 %**
File_HTML	28	0.4 %
Exploit-CVE2017-11882.yx	**23**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	23	0.3 %
GenericRXRS-TZ!D04A14C98614	**21**	**0.3 %**
File_Rar-Archive	21	0.3 %
X97M/Downloader.lz	**16**	**0.2 %**
File_Microsoft-Excel-97-Spreadsheet	16	0.2 %
Downloader-FCHG!98025E4203FA	**13**	**0.2 %**
File_Microsoft-Excel-Spreadsheet	13	0.2 %
GenericRXRS-TZ!7837EB46B5A9	**11**	**0.2 %**
File_Rar-Archive	11	0.2 %
Unknown	**10**	**0.1 %**
File_Zip-Archive	8	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
AgentTesla-FDFM!B3FE0E0A0DED	**5**	**0.1 %**
File_Rar-Archive	5	0.1 %
NSIS/ObfusInjector.h	**4**	**0.1 %**

Report

Scan Result	Hits	%
File_Zip-Archive	2	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
PWS-FCXE!F51A00EA96E3	**4**	**0.1 %**
File_ISO-9660-Disk-Image	4	0.1 %
Exploit-CVE2017-11882.bu	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Exploit-GBT!9CB1168C103A	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Exploit-GBT!825FBB7E0EED	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Fareit.gen.f	**2**	**0.0 %**
File_ACE-Archive	2	0.0 %
Downloader-FCHG!DFC0E36703AD	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCHG!FC95FB489588	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
HTML/Phishing.mx	**1**	**0.0 %**
File_HTML	1	0.0 %
GenericRXRS-TZ!5A3983C7E1F2	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
Downloader-FCHG!306D0DC9C048	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Exploit-GBT!AAAEC3638DF1	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Downloader-FCHG!32DFBDCE751F	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
GenericRXRW-AA!9B02E42C35C1	**1**	**0.0 %**
File_ISO-9660-Disk-Image	1	0.0 %
GenericRXRS-TZ!9393236026EE	**1**	**0.0 %**
File_Type-Unknown	1	0.0 %
Exploit-GBS!E1A81B8EBA52	**1**	**0.0 %**
File_Type-Unknown	1	0.0 %
BackDoor-FEOD!0A61FB8B8D2A	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
HTML/Phishing.jw	**1**	**0.0 %**
File_HTML	1	0.0 %

Report

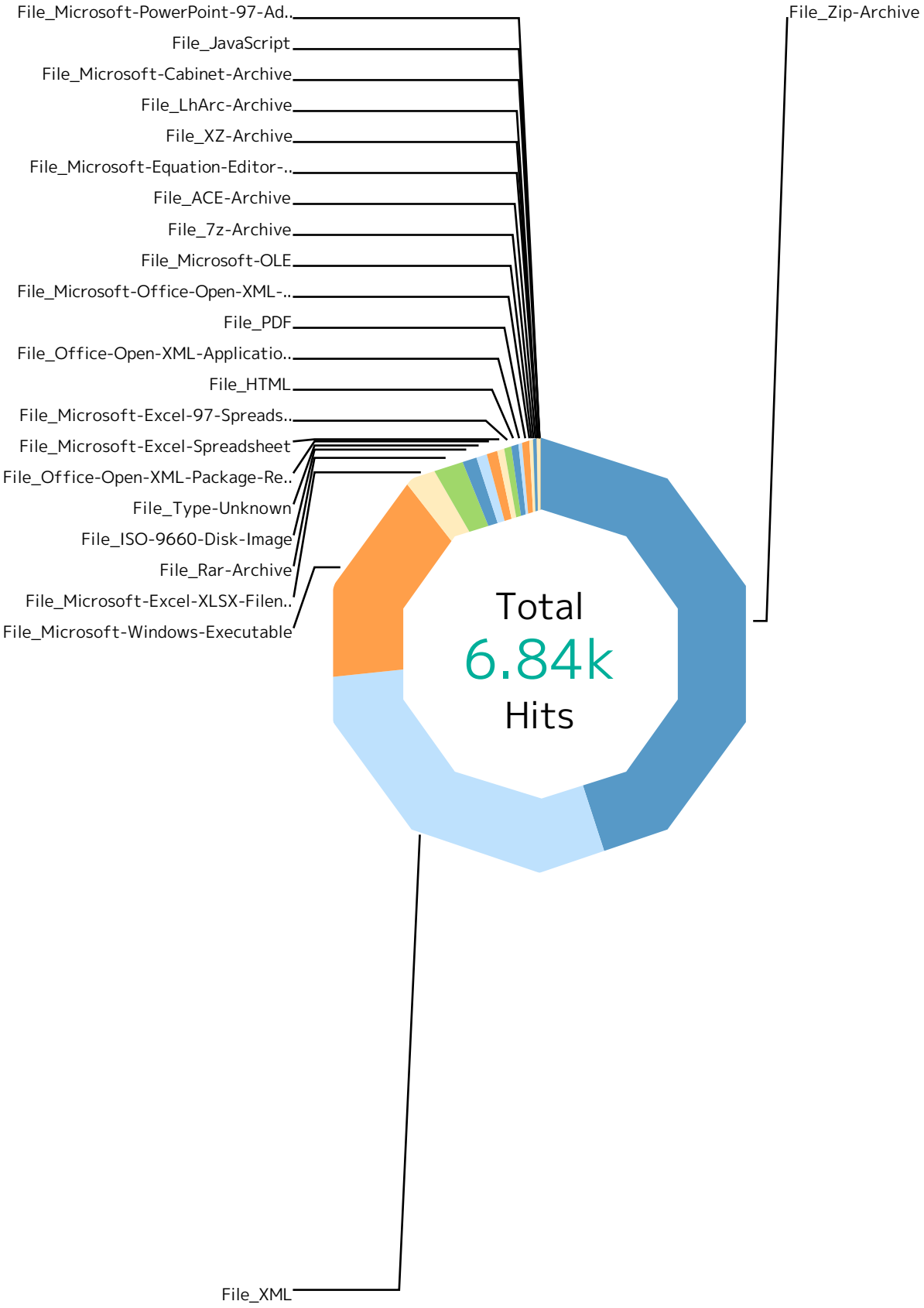
Scan Result	Hits	%
Others	5	0.1 %
Total	**6.84k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Microsoft-PowerPoint-97-Ad..
File_JavaScript
File_Microsoft-Cabinet-Archive
File_LhArc-Archive
File_XZ-Archive
File_Microsoft-Equation-Editor-..
File_ACE-Archive
File_7z-Archive
File_Microsoft-OLE
File_Microsoft-Office-Open-XML-..
File_PDF
File_Office-Open-XML-Applicatio..
File_HTML
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Excel-Spreadsheet
File_Office-Open-XML-Package-Re..
File_Type-Unknown
File_ISO-9660-Disk-Image
File_Rar-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Windows-Executable
File_Zip-Archive
File_XML
Total
6.84k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**3.09k**	**45.1 %**
Not Available	2.91k	42.6 %
Malicious	88	1.3 %
High Risk	56	0.8 %
Medium Risk	16	0.2 %
Unknown	8	0.1 %
NSIS/ObfusInjector.h	2	0.0 %
GenericRXRS-TZ!5A3983C7E1F2	1	0.0 %
BackDoor-FEOD!0A61FB8B8D2A	1	0.0 %
File_XML	**1.94k**	**28.3 %**
Malicious	918	13.4 %
High Risk	515	7.5 %
Medium Risk	502	7.3 %
File_Microsoft-Windows-Executable	**1.11k**	**16.2 %**
Malicious	1.04k	15.2 %
High Risk	68	1.0 %
Medium Risk	4	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**152**	**2.2 %**
Malicious	70	1.0 %
Not Available	24	0.4 %
High Risk	24	0.4 %
Exploit-CVE2017-11882.yx	23	0.3 %
Exploit-CVE2017-11882.bu	3	0.0 %
Exploit-GBT!9CB1168C103A	3	0.0 %
Exploit-GBT!825FBB7E0EED	2	0.0 %
Exploit-GBT!AAAEC3638DF1	1	0.0 %
Exploit-GDJ!05ADC85AB6CE	1	0.0 %
Exploit-GBT!61A653E9DFD8	1	0.0 %
File_Rar-Archive	**139**	**2.0 %**
Malicious	68	1.0 %
High Risk	31	0.5 %
GenericRXRS-TZ!D04A14C98614	21	0.3 %
GenericRXRS-TZ!7837EB46B5A9	11	0.2 %
AgentTesla-FDFM!B3FE0E0A0DED	5	0.1 %
Medium Risk	2	0.0 %
AgentTesla-FCSO!E22683916DE5	1	0.0 %

Report

Responding Scanner	Hits	%
File_ISO-9660-Disk-Image	**84**	**1.2 %**
High Risk	44	0.6 %
Malicious	26	0.4 %
Medium Risk	6	0.1 %
PWS-FCXE!F51A00EA96E3	4	0.1 %
NSIS/ObfusInjector.h	2	0.0 %
GenericRXRW-AA!9B02E42C35C1	1	0.0 %
AgentTesla-FCSO!98345AB9B909	1	0.0 %
File_Type-Unknown	**58**	**0.8 %**
Malicious	44	0.6 %
High Risk	8	0.1 %
Medium Risk	4	0.1 %
GenericRXRS-TZ!9393236026EE	1	0.0 %
Exploit-GBS!E1A81B8EBA52	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**48**	**0.7 %**
Medium Risk	22	0.3 %
High Risk	15	0.2 %
Malicious	11	0.2 %
File_Microsoft-Excel-Spreadsheet	**48**	**0.7 %**
Not Available	27	0.4 %
Downloader-FCHG!98025E4203FA	13	0.2 %
Unknown	2	0.0 %
High Risk	1	0.0 %
Downloader-FCHG!DFC0E36703AD	1	0.0 %
Downloader-FCHG!FC95FB489588	1	0.0 %
Downloader-FCHG!306D0DC9C048	1	0.0 %
Downloader-FCHG!32DFBDCE751F	1	0.0 %
Downloader-FCHG!4165230D58CD	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**36**	**0.5 %**
X97M/Downloader.lz	16	0.2 %
Malicious	13	0.2 %
High Risk	6	0.1 %
Medium Risk	1	0.0 %
File_HTML	**32**	**0.5 %**
HTML/Phishing.he	28	0.4 %
High Risk	2	0.0 %

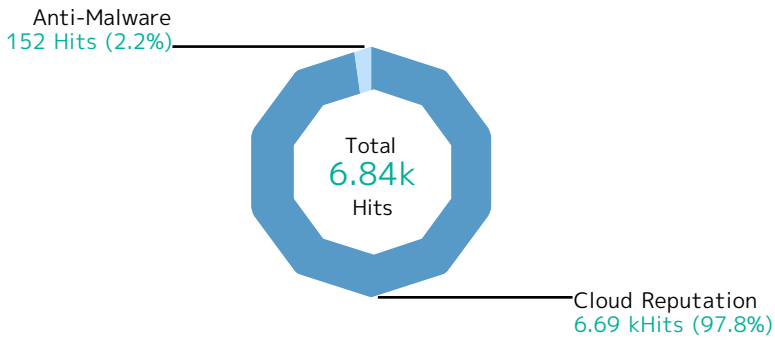
Report

Responding Scanner	Hits	%
HTML/Phishing.mx	1	0.0 %
HTML/Phishing.jw	1	0.0 %
File_Office-Open-XML-Application-Properties-Part	**28**	**0.4 %**
Malicious	28	0.4 %
File_PDF	**23**	**0.3 %**
Malicious	23	0.3 %
File_Microsoft-Office-Open-XML-Document	**20**	**0.3 %**
Not Available	17	0.2 %
Malicious	3	0.0 %
File_Microsoft-OLE	**11**	**0.2 %**
High Risk	7	0.1 %
Malicious	4	0.1 %
File_7z-Archive	**10**	**0.1 %**
High Risk	9	0.1 %
Malicious	1	0.0 %
File_ACE-Archive	**9**	**0.1 %**
High Risk	5	0.1 %
Malicious	2	0.0 %
Fareit.gen.f	2	0.0 %
File_Microsoft-Equation-Editor-Document	**4**	**0.1 %**
Malicious	4	0.1 %
File_XZ-Archive	**3**	**0.0 %**
Malicious	2	0.0 %
High Risk	1	0.0 %
File_LhArc-Archive	**3**	**0.0 %**
Medium Risk	2	0.0 %
High Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	**2**	**0.0 %**
Malicious	1	0.0 %
Medium Risk	1	0.0 %
File_JavaScript	**2**	**0.0 %**
Malicious	2	0.0 %
File_Microsoft-PowerPoint-97-Add-In	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**6.84k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**6.69k**	**97.8 %**
File_Zip-Archive	3.08k	45.0 %
File_XML	1.94k	28.3 %
File_Microsoft-Windows-Executable	1.11k	16.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	118	1.7 %
File_Rar-Archive	101	1.5 %
File_ISO-9660-Disk-Image	76	1.1 %
File_Type-Unknown	56	0.8 %
File_Office-Open-XML-Package-Relations-Item	48	0.7 %
File_Microsoft-Excel-Spreadsheet	30	0.4 %
File_Office-Open-XML-Application-Properties-Part	28	0.4 %
File_PDF	23	0.3 %
File_Microsoft-Excel-97-Spreadsheet	20	0.3 %
File_Microsoft-Office-Open-XML-Document	20	0.3 %
File_Microsoft-OLE	11	0.2 %
File_7z-Archive	10	0.1 %
File_ACE-Archive	7	0.1 %
File_Microsoft-Equation-Editor-Document	4	0.1 %
File_XZ-Archive	3	0.0 %
File_LhArc-Archive	3	0.0 %
File_HTML	2	0.0 %
File_Microsoft-Cabinet-Archive	2	0.0 %
File_JavaScript	2	0.0 %
File_Microsoft-PowerPoint-97-Add-In	1	0.0 %
Anti-Malware	**152**	**2.2 %**
File_Rar-Archive	38	0.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	34	0.5 %
File_HTML	30	0.4 %
File_Microsoft-Excel-Spreadsheet	18	0.3 %
File_Microsoft-Excel-97-Spreadsheet	16	0.2 %
File_ISO-9660-Disk-Image	8	0.1 %
File_Zip-Archive	4	0.1 %
File_Type-Unknown	2	0.0 %
File_ACE-Archive	2	0.0 %
Total	**6.84k**	**100 %**

Report

Virenfilterung SRC IPs

Located 84.5 %

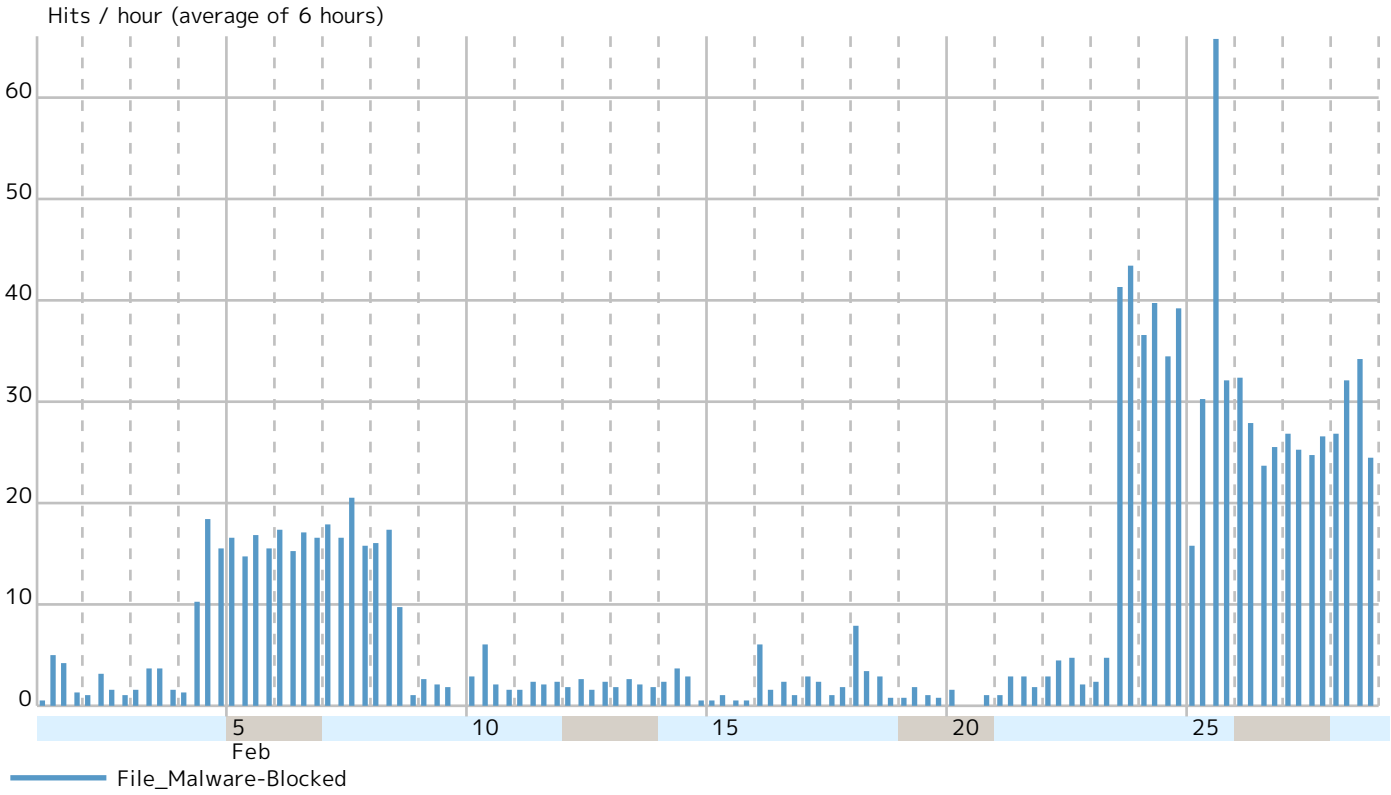
Report

Records by src IP		Hits	%
52.72.21.242	Ashburn, Virginia 20149, United States	1.49k	21.7 %
103.28.38.70	Vietnam	1.05k	15.3 %
200.30.145.122	Honduras	382	5.6 %
153.126.181.97	Japan	316	4.6 %
182.18.139.37	India	302	4.4 %
162.214.108.142	United States	294	4.3 %
80.86.231.190	Armenia	158	2.3 %
151.236.52.249	Reading, United Kingdom	154	2.3 %
153.122.99.225	Tokyo, Japan	146	2.1 %
103.35.65.182	Vietnam	144	2.1 %
150.95.255.193	Japan	130	1.9 %
45.133.203.99	Seychelles	114	1.7 %
210.233.71.197	Japan	106	1.5 %
37.187.254.26	France	104	1.5 %
160.16.226.165	Tokyo, Japan	102	1.5 %
185.46.188.30	Ukraine	86	1.3 %
185.176.9.73	Spain	76	1.1 %
103.89.5.51	Indonesia	72	1.1 %
54.218.189.74	Boardman, Oregon 97818, United States	72	1.1 %
173.249.144.158	United States	63	0.9 %
103.3.61.8	Singapore, 18 Singapore	58	0.8 %
95.216.7.94	Helsinki, Finland	50	0.7 %
122.17.173.168	Japan	48	0.7 %
82.130.63.84	Espoo, Finland	44	0.6 %
82.223.80.112	Spain	44	0.6 %
185.50.45.69	Spain	42	0.6 %
193.169.145.11	Romania	42	0.6 %
62.108.37.107	Germany	37	0.5 %
190.12.64.235	Lima, Peru	33	0.5 %
216.58.239.19	Grand Junction, Colorado 81504, United States	32	0.5 %
Others		1.06k	15.5 %
Total		**6.84k**	**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.