Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-08-01 00:00:00 CEST
To: 2022-09-01 00:00:00 CEST

Report

Report run by
jens

SMC version
6.11.1, build 11219

Update version
1499

Report started
2022-09-02 11:44:55 CEST

Report run time
02:12:00

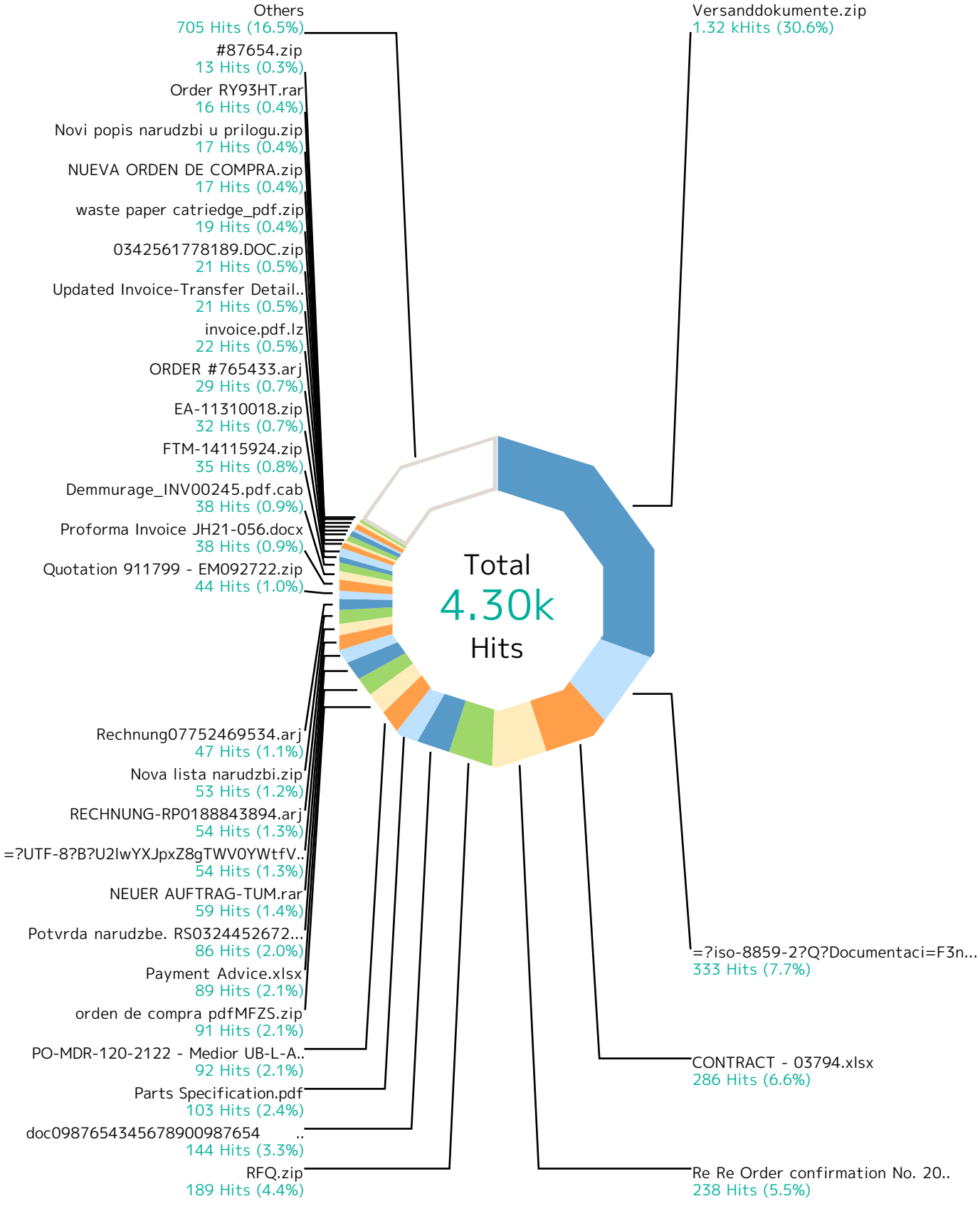
Filters used
Match All

Table of Contents

Virenfilterung MXe 3
Top File Types by Scan Result 5
Top Scan Results by Responding Scanner 10
Top File Types by Responding Scanner 15
Virenfilterung SRC IPs 17
SMTP Virus Filtering by Time 19

Report

Virenfilterung MXe



Report

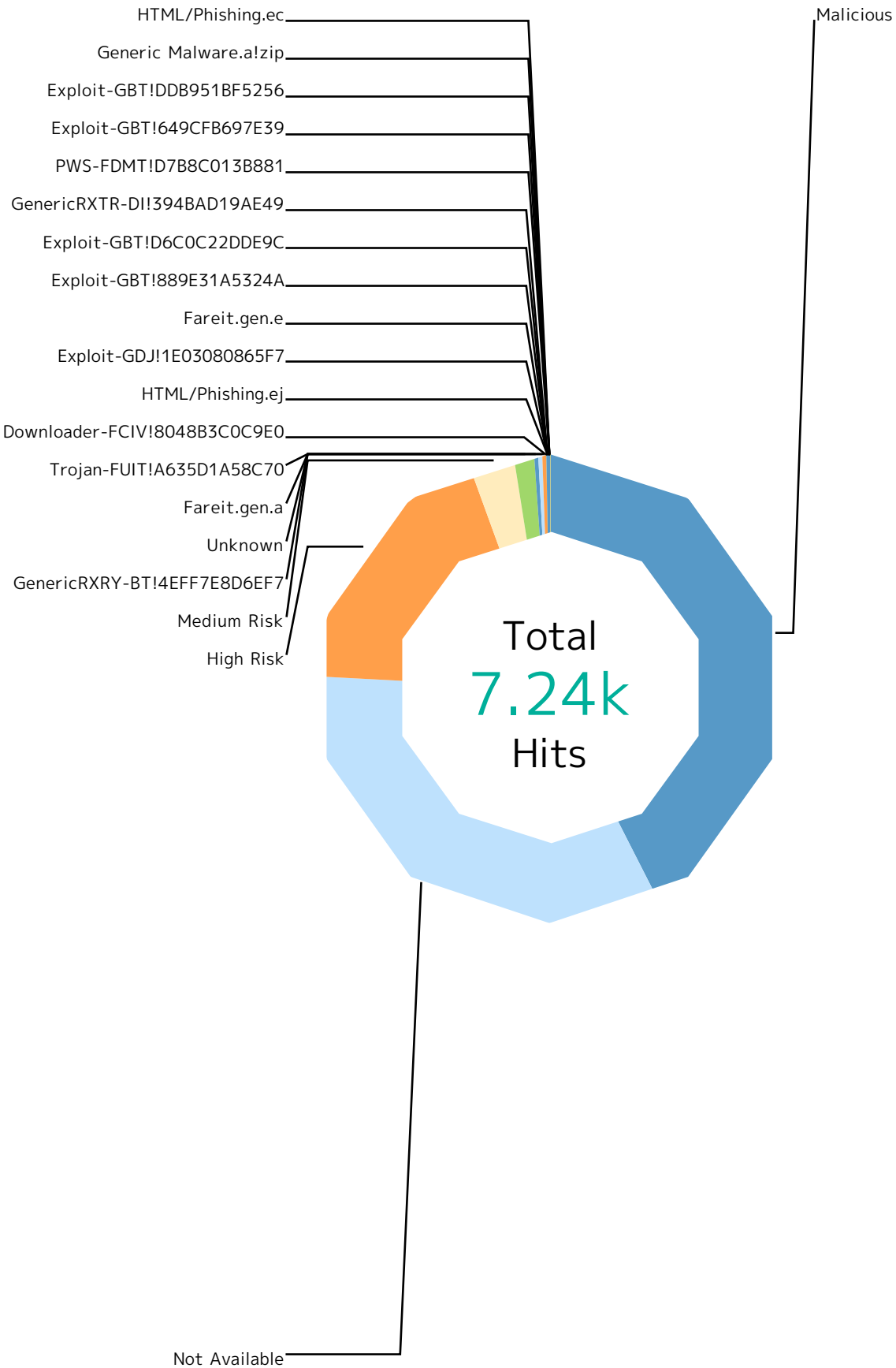
Records by file name	Hits	%
Versanddokumente.zip	1.32k	30.6 %
=?iso-8859-2?Q?Documentaci=F3n.zip?=	333	7.7 %
CONTRACT - 03794.xlsx	286	6.6 %
Re Re Order confirmation No. 2005739 PO SSEPLSBI00717-22.rar	238	5.5 %
RFQ.zip	189	4.4 %
doc0987654345678900987654 .img	144	3.3 %
Parts Specification.pdf	103	2.4 %
PO-MDR-120-2122 - Medior UB-L-Asparaginase.rar	92	2.1 %
orden de compra pdfMFZS.zip	91	2.1 %
Payment Advice.xlsx	89	2.1 %
Potvrda narudzbe. RS0324452672.DOC.zip	86	2.0 %
NEUER AUFTRAG-TUM.rar	59	1.4 %
=?UTF-8?B?U2lwYXJpxZ8gTWV0YWtfV0pPLTAwMS5kb2N4?=	54	1.3 %
RECHNUNG-RP0188843894.arj	54	1.3 %
Nova lista narudzbi.zip	53	1.2 %
Rechnung07752469534.arj	47	1.1 %
Quotation 911799 - EM092722.zip	44	1.0 %
Proforma Invoice JH21-056.docx	38	0.9 %
Demmurage_INV00245.pdf.cab	38	0.9 %
FTM-14115924.zip	35	0.8 %
EA-11310018.zip	32	0.7 %
ORDER #765433.arj	29	0.7 %
invoice.pdf.lz	22	0.5 %
Updated Invoice-Transfer Details 17082022.docx	21	0.5 %
0342561778189.DOC.zip	21	0.5 %
waste paper catriedge_pdf.zip	19	0.4 %
NUEVA ORDEN DE COMPRA.zip	17	0.4 %
Novi popis narudzbi u prilogu.zip	17	0.4 %
Order RY93HT.rar	16	0.4 %
#87654.zip	13	0.3 %
Others	705	16.4 %
Total	**4.30k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


HTML/Phishing.ec
Generic Malware.a!zip
Exploit-GBT!DDB951BF5256
Exploit-GBT!649CFB697E39
PWS-FDMT!D7B8C013B881
GenericRXTR-DI!394BAD19AE49
Exploit-GBT!D6C0C22DDE9C
Exploit-GBT!889E31A5324A
Fareit.gen.e
Exploit-GDJ!1E03080865F7
HTML/Phishing.ej
Downloader-FCIV!8048B3C0C9E0
Trojan-FUIT!A635D1A58C70
Fareit.gen.a
Unknown
GenericRXRY-BT!4EFF7E8D6EF7
Medium Risk
High Risk
Malicious
Not Available
Total
7.24k
Hits

Report

Scan Result	Hits	%
Malicious	**3.08k**	**42.5 %**
File_Microsoft-Windows-Executable	2.31k	31.9 %
File_Zip-Archive	310	4.3 %
File_Rar-Archive	204	2.8 %
File_Office-Open-XML-Package-Relations-Item	65	0.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	58	0.8 %
File_ISO-9660-Disk-Image	38	0.5 %
File_Microsoft-OLE	29	0.4 %
File_Microsoft-Office-Open-XML-Document	19	0.3 %
File_Type-Unknown	16	0.2 %
File_HTML	11	0.2 %
File_JavaScript	5	0.1 %
File_Microsoft-Cabinet-Archive	4	0.1 %
File_7z-Archive	4	0.1 %
File_LhArc-Archive	2	0.0 %
File_Microsoft-Equation-Editor-Document	1	0.0 %
File_Tar-Archive	1	0.0 %
Not Available	**2.42k**	**33.4 %**
File_Zip-Archive	2.14k	29.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	245	3.4 %
File_Microsoft-Office-Open-XML-Document	36	0.5 %
File_Java-Archive	2	0.0 %
High Risk	**1.34k**	**18.6 %**
File_Rar-Archive	515	7.1 %
File_Microsoft-Equation-Editor-Document	286	4.0 %
File_ISO-9660-Disk-Image	171	2.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	135	1.9 %
File_Microsoft-Windows-Executable	83	1.1 %
File_Office-Open-XML-Package-Relations-Item	76	1.1 %
File_Zip-Archive	20	0.3 %
File_Type-Unknown	20	0.3 %
File_HTML	12	0.2 %
File_Microsoft-Cabinet-Archive	12	0.2 %
File_7z-Archive	5	0.1 %
File_JavaScript	4	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %

Report

Scan Result	Hits	%
File_PDF	2	0.0 %
Medium Risk	**222**	**3.1 %**
File_PDF	106	1.5 %
File_PNG-Image	73	1.0 %
File_Rar-Archive	14	0.2 %
File_Microsoft-Windows-Executable	12	0.2 %
File_Zip-Archive	9	0.1 %
File_ISO-9660-Disk-Image	3	0.0 %
File_7z-Archive	2	0.0 %
File_Office-Open-XML-Package-Relations-Item	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_XML	1	0.0 %
GenericRXRY-BT!4EFF7E8D6EF7	**92**	**1.3 %**
File_Rar-Archive	92	1.3 %
Unknown	**29**	**0.4 %**
File_Zip-Archive	27	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Fareit.gen.a	**19**	**0.3 %**
File_ACE-Archive	19	0.3 %
Trojan-FUIT!A635D1A58C70	**11**	**0.2 %**
File_Rar-Archive	11	0.2 %
Downloader-FCIV!8048B3C0C9E0	**7**	**0.1 %**
File_Zip-Archive	7	0.1 %
HTML/Phishing.ej	**4**	**0.1 %**
File_HTML	4	0.1 %
Exploit-GDJ!1E03080865F7	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Fareit.gen.e	**2**	**0.0 %**
File_ACE-Archive	2	0.0 %
Exploit-GBT!889E31A5324A	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!D6C0C22DDE9C	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
GenericRXTR-DI!394BAD19AE49	**1**	**0.0 %**
File_Tar-Archive	1	0.0 %
PWS-FDMT!D7B8C013B881	**1**	**0.0 %**

Report

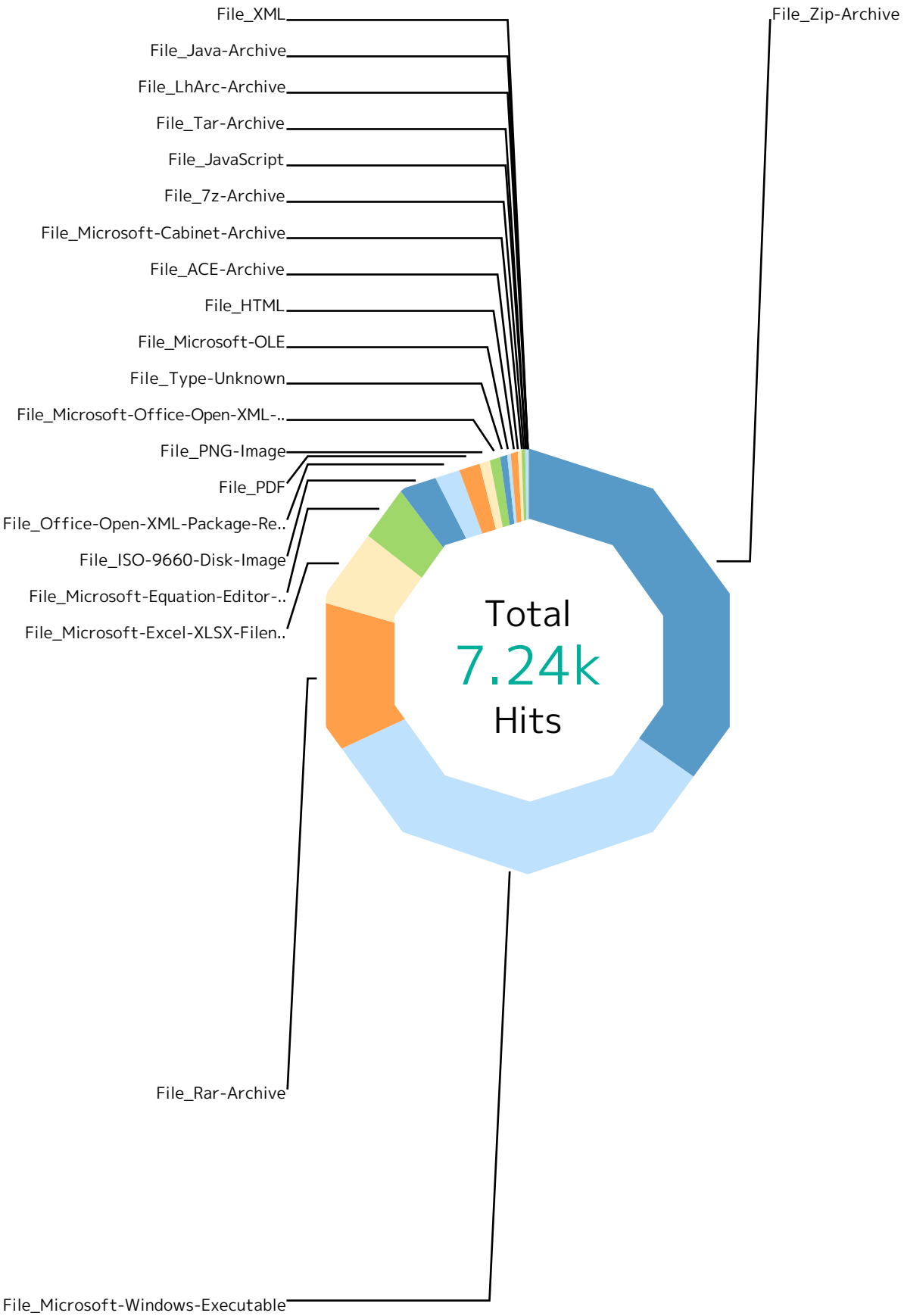
Scan Result	Hits	%
File_Microsoft-Windows-Executable	1	0.0 %
Exploit-GBT!649CFB697E39	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!DDB951BF5256	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Generic Malware.a!zip	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
HTML/Phishing.ec	**1**	**0.0 %**
File_HTML	1	0.0 %
Total	**7.24k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_XML
File_Java-Archive
File_LhArc-Archive
File_Tar-Archive
File_JavaScript
File_7z-Archive
File_Microsoft-Cabinet-Archive
File_ACE-Archive
File_HTML
File_Microsoft-OLE
File_Type-Unknown
File_Microsoft-Office-Open-XML-..
File_PNG-Image
File_PDF
File_Office-Open-XML-Package-Re..
File_ISO-9660-Disk-Image
File_Microsoft-Equation-Editor-..
File_Microsoft-Excel-XLSX-Filen..
File_Zip-Archive
Total
7.24k
Hits
File_Rar-Archive
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**2.51k**	**34.7 %**
Not Available	2.14k	29.5 %
Malicious	310	4.3 %
Unknown	27	0.4 %
High Risk	20	0.3 %
Medium Risk	9	0.1 %
Downloader-FCIV!8048B3C0C9E0	7	0.1 %
Generic Malware.a!zip	1	0.0 %
File_Microsoft-Windows-Executable	**2.41k**	**33.2 %**
Malicious	2.31k	31.9 %
High Risk	83	1.1 %
Medium Risk	12	0.2 %
PWS-FDMT!D7B8C013B881	1	0.0 %
File_Rar-Archive	**836**	**11.6 %**
High Risk	515	7.1 %
Malicious	204	2.8 %
GenericRXRY-BT!4EFF7E8D6EF7	92	1.3 %
Medium Risk	14	0.2 %
Trojan-FUIT!A635D1A58C70	11	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	**447**	**6.2 %**
Not Available	245	3.4 %
High Risk	135	1.9 %
Malicious	58	0.8 %
Exploit-GDJ!1E03080865F7	3	0.0 %
Unknown	2	0.0 %
Exploit-GBT!889E31A5324A	1	0.0 %
Exploit-GBT!D6C0C22DDE9C	1	0.0 %
Exploit-GBT!649CFB697E39	1	0.0 %
Exploit-GBT!DDB951BF5256	1	0.0 %
File_Microsoft-Equation-Editor-Document	**287**	**4.0 %**
High Risk	286	4.0 %
Malicious	1	0.0 %
File_ISO-9660-Disk-Image	**212**	**2.9 %**
High Risk	171	2.4 %
Malicious	38	0.5 %
Medium Risk	3	0.0 %

Report

Responding Scanner	Hits	%
File_Office-Open-XML-Package-Relations-Item	**142**	**2.0 %**
High Risk	76	1.1 %
Malicious	65	0.9 %
Medium Risk	1	0.0 %
File_PDF	**108**	**1.5 %**
Medium Risk	106	1.5 %
High Risk	2	0.0 %
File_PNG-Image	**73**	**1.0 %**
Medium Risk	73	1.0 %
File_Microsoft-Office-Open-XML-Document	**58**	**0.8 %**
Not Available	36	0.5 %
Malicious	19	0.3 %
High Risk	3	0.0 %
File_Type-Unknown	**36**	**0.5 %**
High Risk	20	0.3 %
Malicious	16	0.2 %
File_Microsoft-OLE	**29**	**0.4 %**
Malicious	29	0.4 %
File_HTML	**28**	**0.4 %**
High Risk	12	0.2 %
Malicious	11	0.2 %
HTML/Phishing.ej	4	0.1 %
HTML/Phishing.ec	1	0.0 %
File_ACE-Archive	**21**	**0.3 %**
Fareit.gen.a	19	0.3 %
Fareit.gen.e	2	0.0 %
File_Microsoft-Cabinet-Archive	**17**	**0.2 %**
High Risk	12	0.2 %
Malicious	4	0.1 %
Medium Risk	1	0.0 %
File_7z-Archive	**11**	**0.2 %**
High Risk	5	0.1 %
Malicious	4	0.1 %
Medium Risk	2	0.0 %
File_JavaScript	**9**	**0.1 %**
Malicious	5	0.1 %

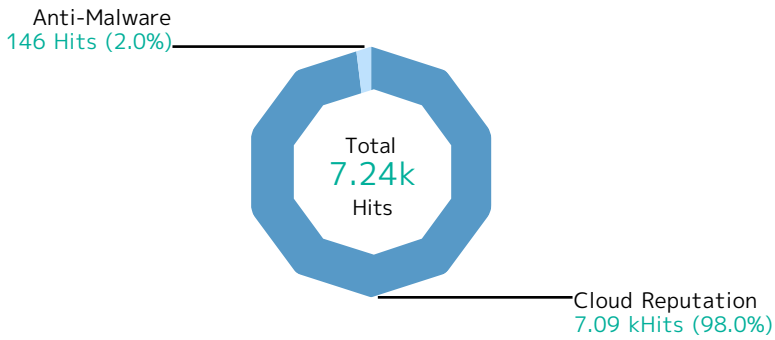
Report

Responding Scanner	Hits	%
High Risk	4	0.1 %
File_Tar-Archive	**2**	**0.0 %**
Malicious	1	0.0 %
GenericRXTR-DI!394BAD19AE49	1	0.0 %
File_LhArc-Archive	**2**	**0.0 %**
Malicious	2	0.0 %
File_Java-Archive	**2**	**0.0 %**
Not Available	2	0.0 %
File_XML	**1**	**0.0 %**
Medium Risk	1	0.0 %
Total	**7.24k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**7.09k**	**98.0 %**
File_Zip-Archive	2.50k	34.6 %
File_Microsoft-Windows-Executable	2.40k	33.2 %
File_Rar-Archive	733	10.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	440	6.1 %
File_Microsoft-Equation-Editor-Document	287	4.0 %
File_ISO-9660-Disk-Image	212	2.9 %
File_Office-Open-XML-Package-Relations-Item	142	2.0 %
File_PDF	108	1.5 %
File_PNG-Image	73	1.0 %
File_Microsoft-Office-Open-XML-Document	58	0.8 %
File_Type-Unknown	36	0.5 %
File_Microsoft-OLE	29	0.4 %
File_HTML	23	0.3 %
File_Microsoft-Cabinet-Archive	17	0.2 %
File_7z-Archive	11	0.2 %
File_JavaScript	9	0.1 %
File_LhArc-Archive	2	0.0 %
File_Java-Archive	2	0.0 %
File_Tar-Archive	1	0.0 %
File_XML	1	0.0 %
Anti-Malware	**146**	**2.0 %**
File_Rar-Archive	103	1.4 %
File_ACE-Archive	21	0.3 %
File_Zip-Archive	8	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	7	0.1 %
File_HTML	5	0.1 %
File_Microsoft-Windows-Executable	1	0.0 %
File_Tar-Archive	1	0.0 %
Total	**7.24k**	**100 %**

Report

Virenfilterung SRC IPs

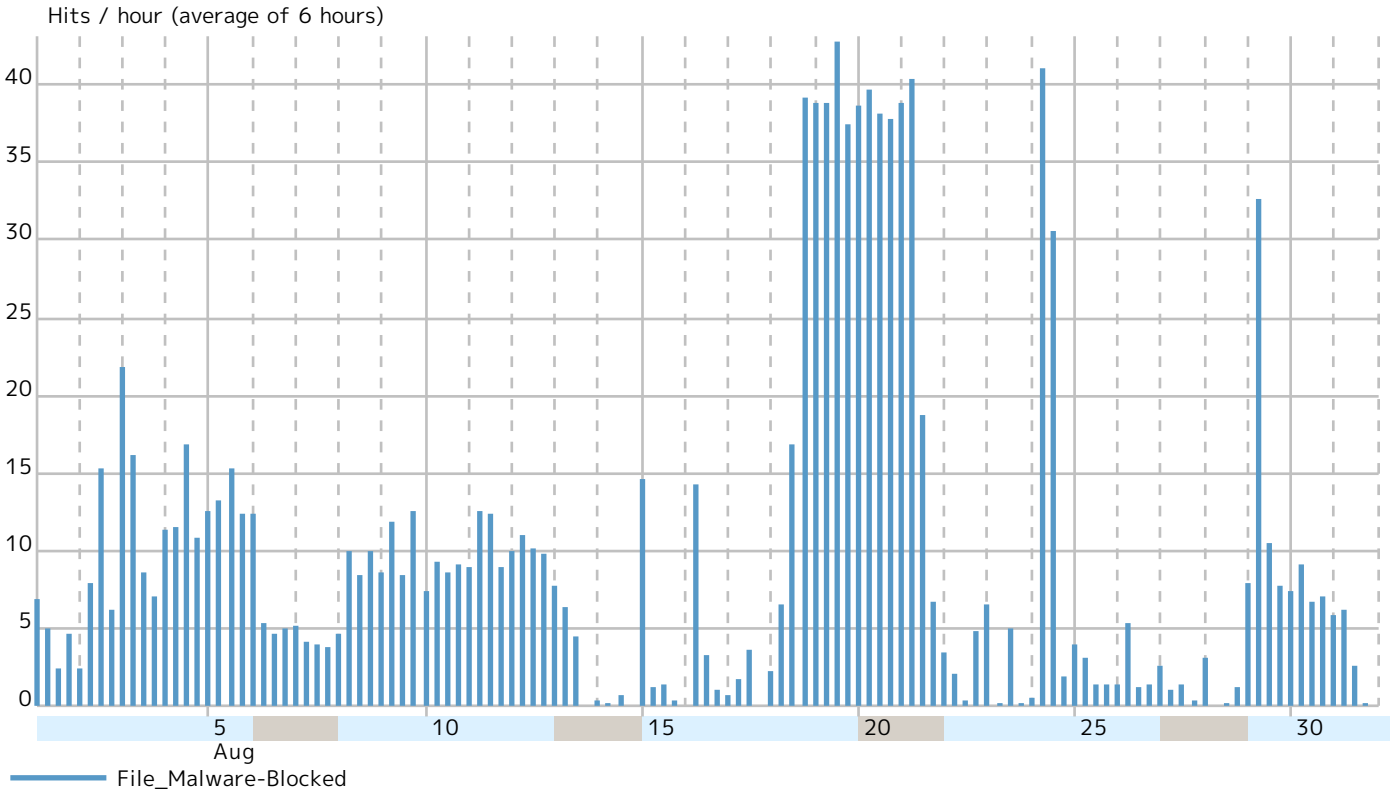
Report

Records by src IP		Hits	%
104.168.158.189	United States	2.64k	36.4 %
195.66.113.5	Romania	666	9.2 %
185.246.220.143	Bulgaria	572	7.9 %
87.121.98.46	Bulgaria	378	5.2 %
83.229.86.174	Frankfurt am Main, Germany	236	3.3 %
207.180.198.241	Nuremberg, Germany	208	2.9 %
172.96.181.132	Canada	182	2.5 %
45.57.161.58	Piscataway, New Jersey 08854, United States	179	2.5 %
5.252.23.215	Russia	145	2.0 %
95.111.193.67	Singapore	108	1.5 %
104.168.243.21	United States	108	1.5 %
185.248.59.9	Turkey	106	1.5 %
162.240.1.83	United States	104	1.4 %
95.85.61.94	Amsterdam, Netherlands	101	1.4 %
185.222.58.235	Amsterdam, Netherlands	93	1.3 %
185.222.57.178	Amsterdam, Netherlands	84	1.2 %
45.95.235.32	Russia	69	1.0 %
85.92.108.195	Russia	64	0.9 %
80.85.157.26	Russia	59	0.8 %
190.210.183.128	Buenos Aires, Argentina	58	0.8 %
46.4.214.206	Germany	42	0.6 %
208.67.106.177	Unknown	38	0.5 %
78.137.117.158	Poplar, United Kingdom	38	0.5 %
104.168.170.12	United States	36	0.5 %
162.214.69.222	United States	34	0.5 %
107.182.129.53	Dallas, Texas 75270, United States	33	0.5 %
176.9.41.172	Weimar, Germany	26	0.4 %
45.95.235.36	Russia	26	0.4 %
185.222.57.165	Amsterdam, Netherlands	24	0.3 %
208.67.104.43	Unknown	24	0.3 %
Others		758	10.5 %
Total		**7.24k**	**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.