Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period
From: 2022-03-01 00:00:00
To: 2022-04-01 00:00:00

Report

Report run by
jens

SMC version
6.10.7, build 11163

Update version
1450

Report started
2022-04-03 09:50:04

Report run time
01:50:47

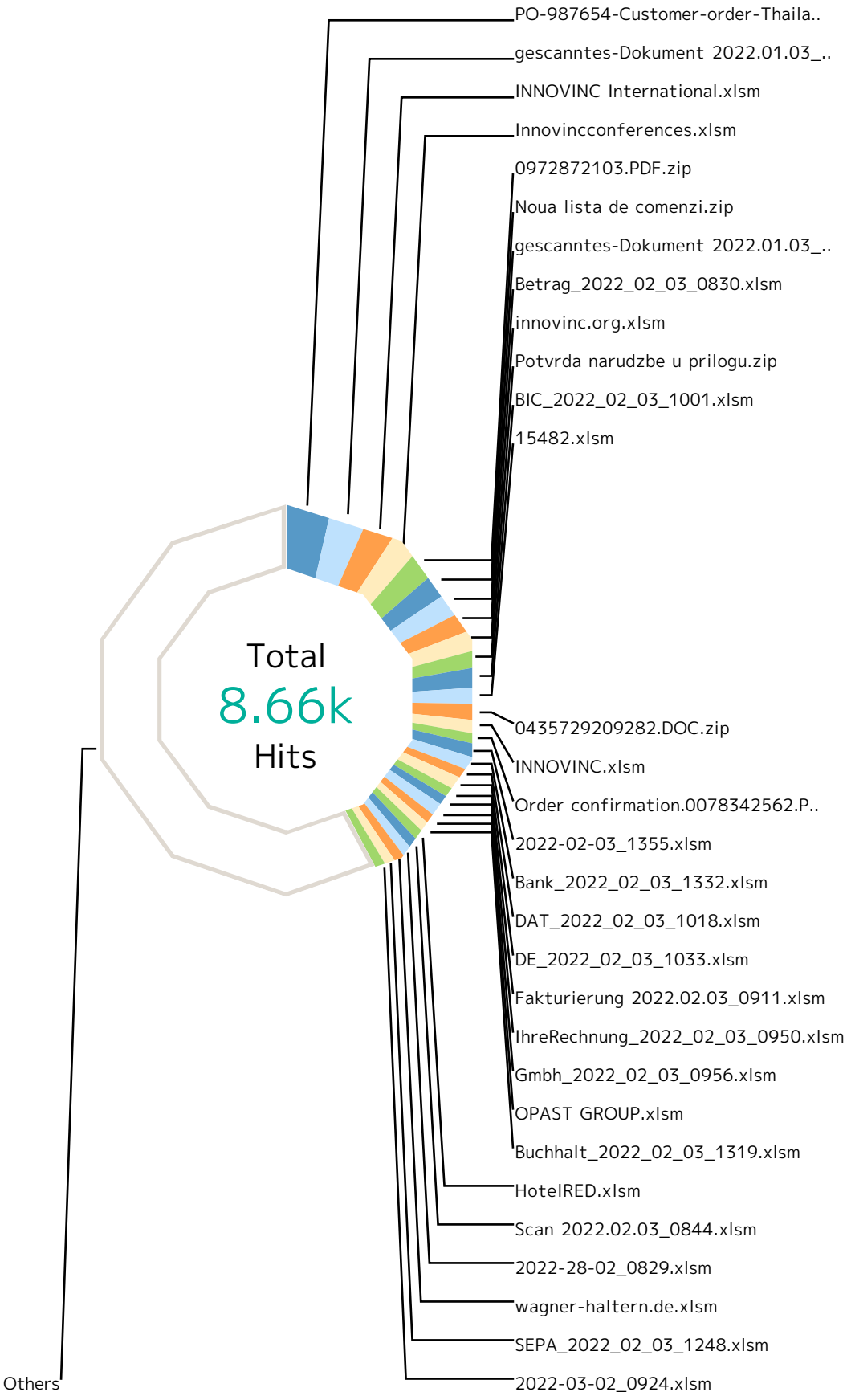
Filters used
Match All

Table of Contents

Virenfilterung MXe 3
Top File Types by Scan Result 5
Top Scan Results by Responding Scanner 11
Top File Types by Responding Scanner 17
Virenfilterung SRC IPs 20
SMTP Virus Filtering by Time 22

Report

Virenfilterung MXe



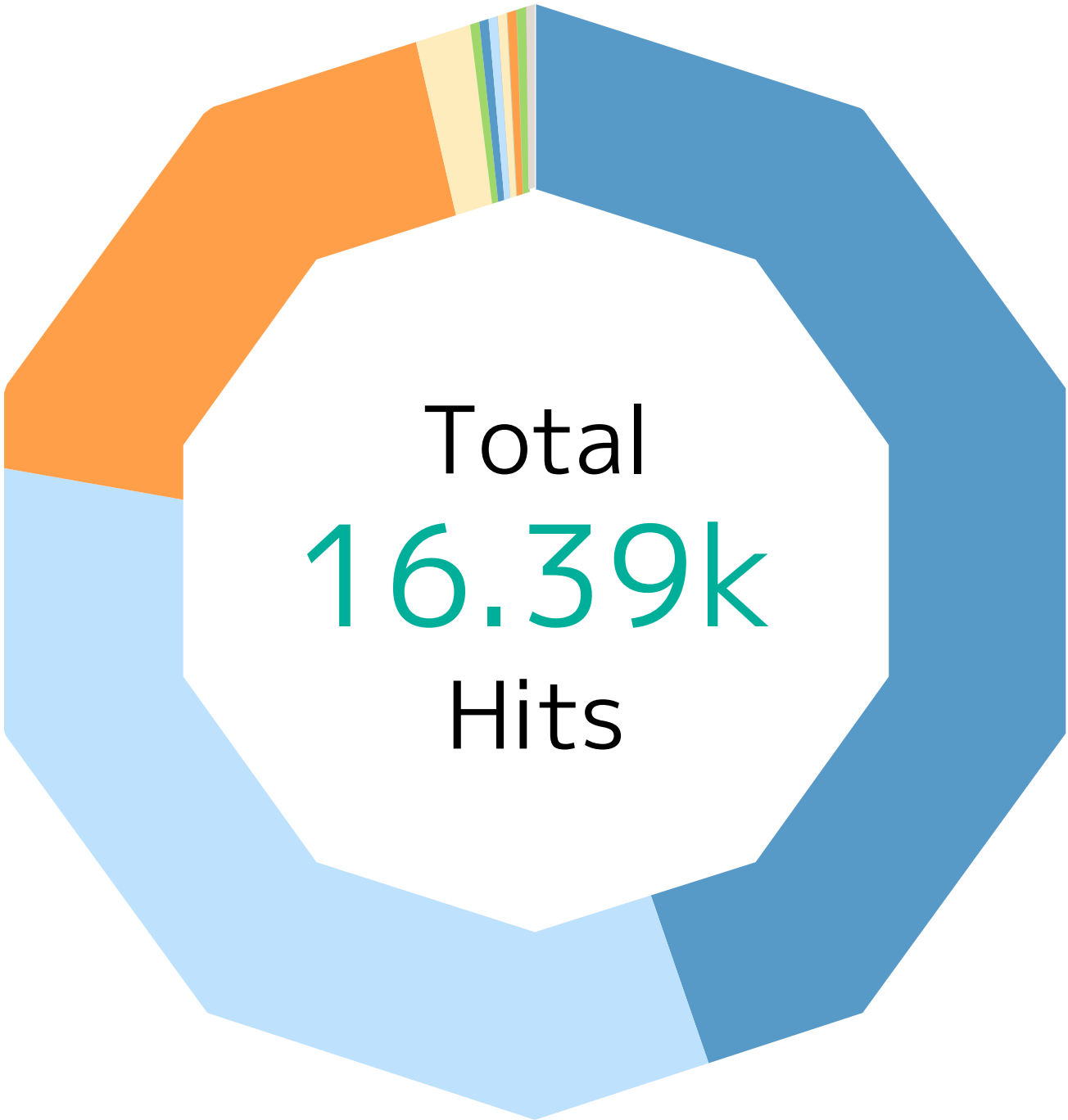
Report

Records by file name	Hits	%
PO-987654-Customer-order-Thailand007.xlsx	309	3.6 %
gescanntes-Dokument 2022.01.03_0930.xlsm	272	3.1 %
INNOVINC International.xlsm	216	2.5 %
Innovincconferences.xlsm	194	2.2 %
0972872103.PDF.zip	184	2.1 %
Noua lista de comenzi.zip	174	2.0 %
gescanntes-Dokument 2022.01.03_0929.xlsm	159	1.8 %
Betrag_2022_02_03_0830.xlsm	145	1.7 %
innovinc.org.xlsm	142	1.6 %
Potvrda narudzbe u prilogu.zip	139	1.6 %
BIC_2022_02_03_1001.xlsm	134	1.5 %
15482.xlsm	131	1.5 %
0435729209282.DOC.zip	100	1.2 %
INNOVINC.xlsm	94	1.1 %
Order confirmation.0078342562.PDF.zip	93	1.1 %
2022-02-03_1355.xlsm	89	1.0 %
Bank_2022_02_03_1332.xlsm	88	1.0 %
DAT_2022_02_03_1018.xlsm	85	1.0 %
DE_2022_02_03_1033.xlsm	83	1.0 %
Fakturierung 2022.02.03_0911.xlsm	79	0.9 %
IhreRechnung_2022_02_03_0950.xlsm	79	0.9 %
Gmbh_2022_02_03_0956.xlsm	79	0.9 %
OPAST GROUP.xlsm	78	0.9 %
Buchhalt_2022_02_03_1319.xlsm	76	0.9 %
HotelRED.xlsm	73	0.8 %
Scan 2022.02.03_0844.xlsm	73	0.8 %
2022-28-02_0829.xlsm	72	0.8 %
wagner-haltern.de.xlsm	71	0.8 %
SEPA_2022_02_03_1248.xlsm	67	0.8 %
2022-03-02_0924.xlsm	66	0.8 %
Others	5.01k	57.9 %
Total	**8.66k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
16.39k
Hits

Report

Scan Result	Hits	%
Not Available	**7.34k**	**44.8 %**
File_Zip-Archive	7.01k	42.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	313	1.9 %
File_Microsoft-Office-Open-XML-Document	8	0.0 %
File_Microsoft-Excel-Spreadsheet	3	0.0 %
High Risk	**5.41k**	**33.0 %**
File_XML	4.90k	29.9 %
File_Microsoft-Equation-Editor-Document	306	1.9 %
File_Zip-Archive	61	0.4 %
File_Rar-Archive	33	0.2 %
File_Microsoft-Windows-Executable	32	0.2 %
File_ISO-9660-Disk-Image	30	0.2 %
File_7z-Archive	23	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.0 %
File_Type-Unknown	4	0.0 %
File_Office-Open-XML-Package-Relations-Item	4	0.0 %
File_Microsoft-OLE	3	0.0 %
File_HTML	2	0.0 %
File_Microsoft-Cabinet-Archive	2	0.0 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
Malicious	**3.07k**	**18.7 %**
File_Microsoft-Windows-Executable	1.32k	8.0 %
File_XML	975	5.9 %
File_Zip-Archive	299	1.8 %
File_Rar-Archive	156	1.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	131	0.8 %
File_ISO-9660-Disk-Image	73	0.4 %
File_Type-Unknown	20	0.1 %
File_Microsoft-Cabinet-Archive	13	0.1 %
File_Microsoft-Excel-97-Spreadsheet	13	0.1 %
File_7z-Archive	12	0.1 %
File_PDF	12	0.1 %
File_Self-Extracting-Zip-Archive	10	0.1 %
File_Microsoft-Excel-Spreadsheet	8	0.0 %
File_Microsoft-Equation-Editor-Document	7	0.0 %
File_ACE-Archive	7	0.0 %

Report

Scan Result	Hits	%
File_Office-Open-XML-Package-Relations-Item	4	0.0 %
File_BZip2-Compressed	3	0.0 %
File_HTML	2	0.0 %
File_Microsoft-Office-Open-XML-Document	2	0.0 %
File_PNG-Image	2	0.0 %
File_Java-Archive	1	0.0 %
File_Microsoft-OLE	1	0.0 %
File_LhArc-Archive	1	0.0 %
Medium Risk	**268**	**1.6 %**
File_XML	163	1.0 %
File_HTML	52	0.3 %
File_Rar-Archive	30	0.2 %
File_Microsoft-Windows-Executable	16	0.1 %
File_Type-Unknown	4	0.0 %
File_Zip-Archive	1	0.0 %
File_ISO-9660-Disk-Image	1	0.0 %
File_PDF	1	0.0 %
Exploit-CVE2017-11882.yx	**42**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	40	0.2 %
File_Rar-Archive	2	0.0 %
Unknown	**39**	**0.2 %**
File_Zip-Archive	39	0.2 %
X97M/Downloader.kj	**33**	**0.2 %**
File_Microsoft-Excel-Spreadsheet	33	0.2 %
Java/Agent!1B9D7F73DB7A	**23**	**0.1 %**
File_Java-Archive	23	0.1 %
Downloader-FCIV!1AF36BAE9A5D	**20**	**0.1 %**
File_Rar-Archive	20	0.1 %
Exploit-GBT!5C9421DADC9D	**13**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.1 %
Fareit-FDBI!D835FC8635DB	**11**	**0.1 %**
File_Rar-Archive	11	0.1 %
Fareit.gen.e	**11**	**0.1 %**
File_ACE-Archive	11	0.1 %
NSIS/ObfusInjector.h	**11**	**0.1 %**
File_Rar-Archive	9	0.1 %

Report

Scan Result	Hits	%
File_ISO-9660-Disk-Image	2	0.0 %
Exploit-GBT!ADA3076D159E	**10**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.1 %
Downloader-FCHG!4335B3637DC9	**10**	**0.1 %**
File_Microsoft-Excel-Spreadsheet	10	0.1 %
Downloader-FCHG!CAB6670DF74A	**5**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	5	0.0 %
Downloader-FCHG!753C62E81BCB	**4**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	4	0.0 %
Downloader-FCHG!C94800ECBE9E	**4**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	4	0.0 %
GenericRXPA-ZY!66841AAACC00	**4**	**0.0 %**
File_Rar-Archive	4	0.0 %
Exploit-GBT!F3CA796408BD	**4**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.0 %
HTML/Phishing.io	**3**	**0.0 %**
File_HTML	3	0.0 %
GenericRXRU-WN!C00254FDCAFB	**3**	**0.0 %**
File_Microsoft-Cabinet-Archive	3	0.0 %
AgentTesla-FDFR!566D25225195	**3**	**0.0 %**
File_Rar-Archive	3	0.0 %
Exploit-GBT!4AC858D4C487	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
AgentTesla-FDFM!5A83CE89276D	**2**	**0.0 %**
File_Zip-Archive	2	0.0 %
HTML/Phishing.bb	**2**	**0.0 %**
File_HTML	2	0.0 %
Fareit-FDBI!1D683D326E4B	**2**	**0.0 %**
File_7z-Archive	2	0.0 %
HTML/Phishing.dy	**2**	**0.0 %**
File_HTML	2	0.0 %
Downloader-FCIV!DC3F0E876146	**2**	**0.0 %**
File_7z-Archive	2	0.0 %
Packed-GDT!589F99C1E71E	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
Others	**41**	**0.3 %**

Report

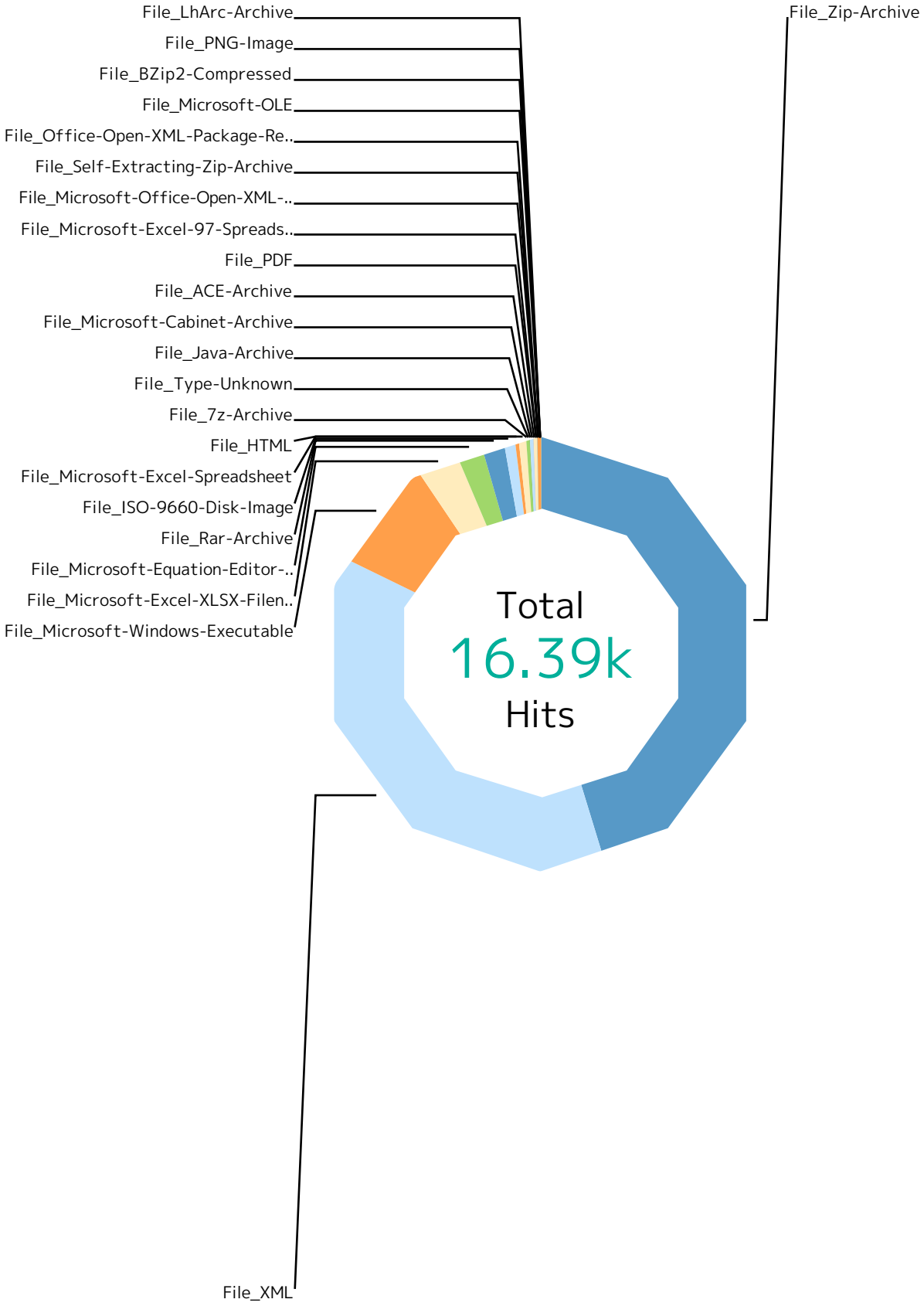
Scan Result	Hits	%
Total	**16.39k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_LhArc-Archive
File_PNG-Image
File_BZip2-Compressed
File_Microsoft-OLE
File_Office-Open-XML-Package-Re..
File_Self-Extracting-Zip-Archive
File_Microsoft-Office-Open-XML-..
File_Microsoft-Excel-97-Spreads..
File_PDF
File_ACE-Archive
File_Microsoft-Cabinet-Archive
File_Java-Archive
File_Type-Unknown
File_7z-Archive
File_HTML
File_Microsoft-Excel-Spreadsheet
File_ISO-9660-Disk-Image
File_Rar-Archive
File_Microsoft-Equation-Editor-..
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Windows-Executable
File_Zip-Archive
File_XML
Total
16.39k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**7.43k**	**45.3 %**
Not Available	7.01k	42.8 %
Malicious	299	1.8 %
High Risk	61	0.4 %
Unknown	39	0.2 %
AgentTesla-FDFM!5A83CE89276D	2	0.0 %
Medium Risk	1	0.0 %
Exploit-CVE-2017-0199.b	1	0.0 %
AgentTesla-FDFR!42A772066BF0	1	0.0 %
AgentTesla-FDFM!F916F3F8D7EA	1	0.0 %
Downloader-FCIV!33D5B6D2A768	1	0.0 %
AgentTesla-FDFR!1D1F327F10B9	1	0.0 %
GenericRXFU-GW!0D9590CEC876	1	0.0 %
AgentTesla-FDFR!E27E07896E0B	1	0.0 %
Exploit-CVE2017-11882.o	1	0.0 %
AgentTesla-FDAW!954B1079B637	1	0.0 %
W32/Mydoom.t@MM!zip	1	0.0 %
File_XML	**6.04k**	**36.9 %**
High Risk	4.90k	29.9 %
Malicious	975	5.9 %
Medium Risk	163	1.0 %
File_Microsoft-Windows-Executable	**1.37k**	**8.3 %**
Malicious	1.32k	8.0 %
High Risk	32	0.2 %
Medium Risk	16	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**529**	**3.2 %**
Not Available	313	1.9 %
Malicious	131	0.8 %
Exploit-CVE2017-11882.yx	40	0.2 %
Exploit-GBT!5C9421DADC9D	13	0.1 %
Exploit-GBT!ADA3076D159E	10	0.1 %
High Risk	4	0.0 %
Exploit-GBT!F3CA796408BD	4	0.0 %
Exploit-GBT!4AC858D4C487	3	0.0 %
Exploit-GBT!0AC3C1ABB937	2	0.0 %
Exploit-CVE2017-11882.bu	2	0.0 %

Report

Responding Scanner	Hits	%
Exploit-GBT!ECFC836C88C3	1	0.0 %
Exploit-GBT!957845D00C91	1	0.0 %
Exploit-GBT!F3BEBF1D69A3	1	0.0 %
Exploit-GBT!6065F7FCE20E	1	0.0 %
Exploit-GBT!4D4FD48FD131	1	0.0 %
Exploit-GBT!22DFD8EDD4CC	1	0.0 %
Exploit-GBT!FB8CADB894F7	1	0.0 %
File_Microsoft-Equation-Editor-Document	**313**	**1.9 %**
High Risk	306	1.9 %
Malicious	7	0.0 %
File_Rar-Archive	**275**	**1.7 %**
Malicious	156	1.0 %
High Risk	33	0.2 %
Medium Risk	30	0.2 %
Downloader-FCIV!1AF36BAE9A5D	20	0.1 %
Fareit-FDBI!D835FC8635DB	11	0.1 %
NSIS/ObfusInjector.h	9	0.1 %
GenericRXPA-ZY!66841AAACC00	4	0.0 %
AgentTesla-FDFR!566D25225195	3	0.0 %
Exploit-CVE2017-11882.yx	2	0.0 %
Packed-GDT!589F99C1E71E	2	0.0 %
GenericRXRQ-ZB!0BB8A5002630	2	0.0 %
AgentTesla-FDFM!0DD118B6CE47	1	0.0 %
GenericRXRV-YQ!27A502888EFE	1	0.0 %
AgentTesla-FDFR!6CA4252672CC	1	0.0 %
File_ISO-9660-Disk-Image	**108**	**0.7 %**
Malicious	73	0.4 %
High Risk	30	0.2 %
NSIS/ObfusInjector.h	2	0.0 %
Medium Risk	1	0.0 %
Downloader-FCIV!C4F0F4DAA225	1	0.0 %
Trojan-FNTX!0132D6C799EA	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**67**	**0.4 %**
X97M/Downloader.kj	33	0.2 %
Downloader-FCHG!4335B3637DC9	10	0.1 %
Malicious	8	0.0 %

Report

Responding Scanner	Hits	%
Downloader-FCHG!CAB6670DF74A	5	0.0 %
Downloader-FCHG!753C62E81BCB	4	0.0 %
Downloader-FCHG!C94800ECBE9E	4	0.0 %
Not Available	3	0.0 %
File_HTML	**66**	**0.4 %**
Medium Risk	52	0.3 %
HTML/Phishing.io	3	0.0 %
High Risk	2	0.0 %
Malicious	2	0.0 %
HTML/Phishing.dy	2	0.0 %
HTML/Phishing.jt	2	0.0 %
HTML/Phishing.bb	2	0.0 %
HTML/Phishing.ec	1	0.0 %
File_7z-Archive	**44**	**0.3 %**
High Risk	23	0.1 %
Malicious	12	0.1 %
Fareit-FDBI!1D683D326E4B	2	0.0 %
Downloader-FCIV!DC3F0E876146	2	0.0 %
Downloader-FCIV!F88F6D3AF7FC	2	0.0 %
Trojan-FNTX!56B7E1105720	1	0.0 %
Downloader-FCIV!86837B8E1C46	1	0.0 %
GenericRXCD-ZZ!7307E2691191	1	0.0 %
File_Type-Unknown	**30**	**0.2 %**
Malicious	20	0.1 %
High Risk	4	0.0 %
Medium Risk	4	0.0 %
AgentTesla-FDIG!927836B39CF5	1	0.0 %
Exploit-Generic.src	1	0.0 %
File_Java-Archive	**24**	**0.1 %**
Java/Agent!1B9D7F73DB7A	23	0.1 %
Malicious	1	0.0 %
File_Microsoft-Cabinet-Archive	**20**	**0.1 %**
Malicious	13	0.1 %
GenericRXRU-WN!C00254FDCAFB	3	0.0 %
High Risk	2	0.0 %
GenericRXRU-WN!758286140C20	1	0.0 %

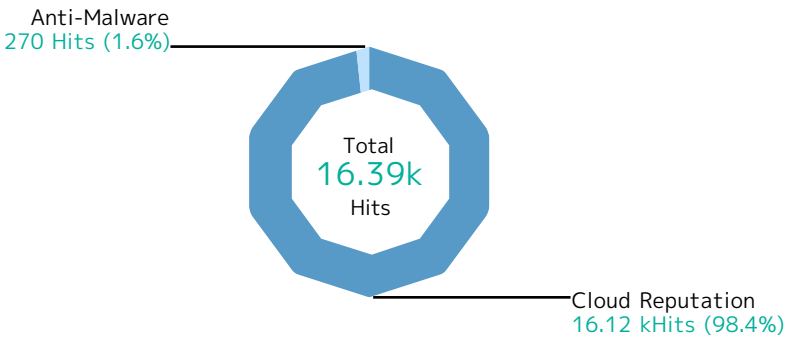
Report

Responding Scanner	Hits	%
GenericRXRU-WN!E1CE44994382	1	0.0 %
File_ACE-Archive	**19**	**0.1 %**
Fareit.gen.e	11	0.1 %
Malicious	7	0.0 %
Fareit.gen.a	1	0.0 %
File_PDF	**13**	**0.1 %**
Malicious	12	0.1 %
Medium Risk	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**13**	**0.1 %**
Malicious	13	0.1 %
File_Microsoft-Office-Open-XML-Document	**11**	**0.1 %**
Not Available	8	0.0 %
Malicious	2	0.0 %
High Risk	1	0.0 %
File_Self-Extracting-Zip-Archive	**10**	**0.1 %**
Malicious	10	0.1 %
File_Office-Open-XML-Package-Relations-Item	**8**	**0.0 %**
High Risk	4	0.0 %
Malicious	4	0.0 %
File_Microsoft-OLE	**4**	**0.0 %**
High Risk	3	0.0 %
Malicious	1	0.0 %
File_BZip2-Compressed	**3**	**0.0 %**
Malicious	3	0.0 %
File_PNG-Image	**2**	**0.0 %**
Malicious	2	0.0 %
File_LhArc-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**16.39k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**16.12k**	**98.4 %**
File_Zip-Archive	7.41k	45.2 %
File_XML	6.04k	36.9 %
File_Microsoft-Windows-Executable	1.37k	8.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	448	2.7 %
File_Microsoft-Equation-Editor-Document	313	1.9 %
File_Rar-Archive	219	1.3 %
File_ISO-9660-Disk-Image	104	0.6 %
File_HTML	56	0.3 %
File_7z-Archive	35	0.2 %
File_Type-Unknown	28	0.2 %
File_Microsoft-Cabinet-Archive	15	0.1 %
File_PDF	13	0.1 %
File_Microsoft-Excel-97-Spreadsheet	13	0.1 %
File_Microsoft-Excel-Spreadsheet	11	0.1 %
File_Microsoft-Office-Open-XML-Document	11	0.1 %
File_Self-Extracting-Zip-Archive	10	0.1 %
File_Office-Open-XML-Package-Relations-Item	8	0.0 %
File_ACE-Archive	7	0.0 %
File_Microsoft-OLE	4	0.0 %
File_BZip2-Compressed	3	0.0 %
File_PNG-Image	2	0.0 %
File_Java-Archive	1	0.0 %
File_LhArc-Archive	1	0.0 %
Anti-Malware	**270**	**1.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	81	0.5 %
File_Rar-Archive	56	0.3 %
File_Microsoft-Excel-Spreadsheet	56	0.3 %
File_Java-Archive	23	0.1 %
File_Zip-Archive	12	0.1 %
File_ACE-Archive	12	0.1 %
File_HTML	10	0.1 %
File_7z-Archive	9	0.1 %
File_Microsoft-Cabinet-Archive	5	0.0 %
File_ISO-9660-Disk-Image	4	0.0 %
File_Type-Unknown	2	0.0 %

Report

Responding Scanner	Hits	%
Total	**16.39k**	**100 %**

Report

Virenfilterung SRC IPs

Located 49.7 %

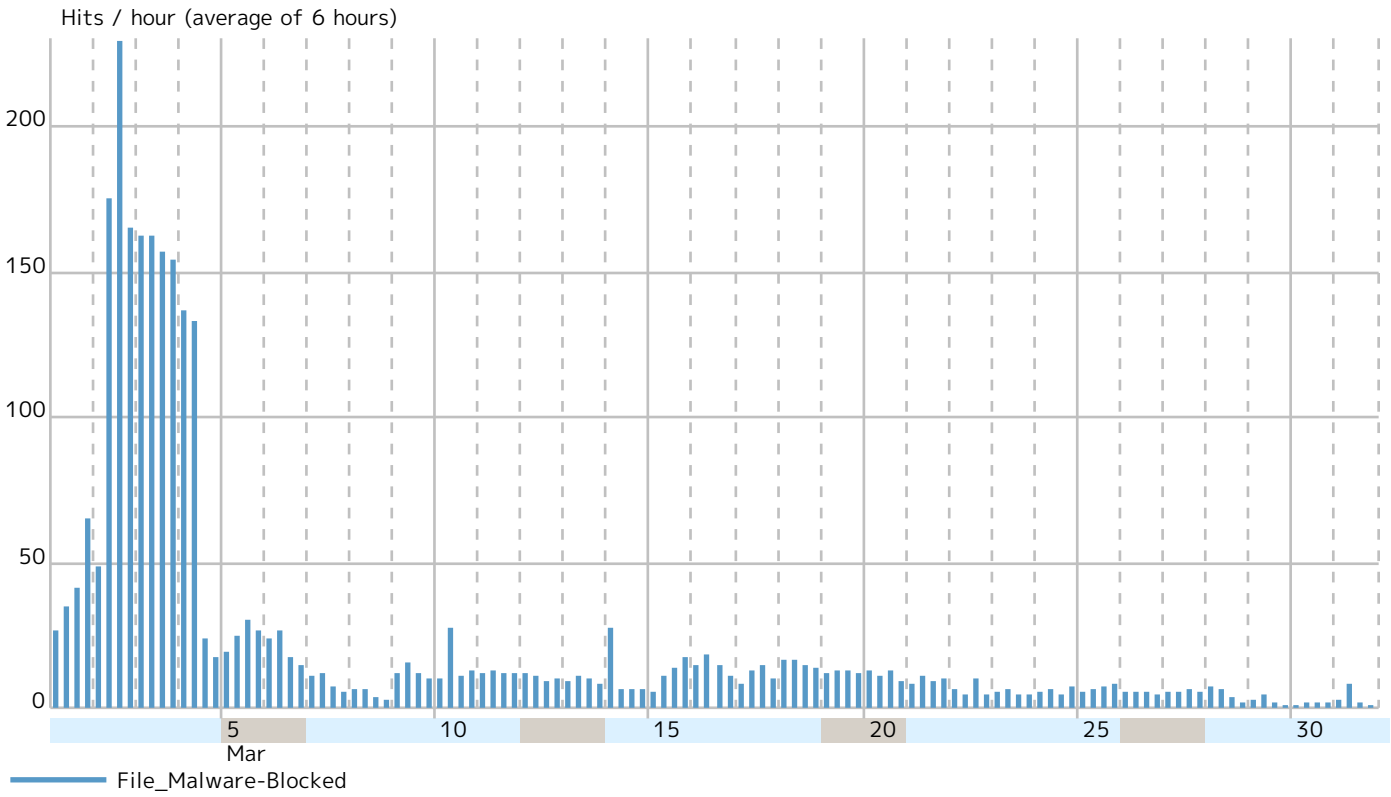
Report

Records by src IP		Hits	%
80.86.231.190	Armenia	753	4.6 %
52.49.14.50	Dublin, Ireland	544	3.3 %
195.33.210.155	Adapazarı, Turkey	498	3.0 %
103.35.65.182	Vietnam	446	2.7 %
203.145.232.197	Japan	426	2.6 %
219.99.208.167	Kanazawa, Japan	422	2.6 %
112.78.134.14	Yosorejo, Indonesia	318	1.9 %
193.169.145.11	Romania	310	1.9 %
203.146.58.55	Thailand	296	1.8 %
130.34.41.189	Sendai, Japan	276	1.7 %
190.12.64.235	Lima, Peru	268	1.6 %
203.183.70.150	Japan	264	1.6 %
211.1.226.34	Japan	260	1.6 %
203.160.60.245	Sukabumi, Indonesia	242	1.5 %
219.99.220.34	Kanazawa, Japan	228	1.4 %
203.137.113.193	Japan	218	1.3 %
210.158.176.22	Hiroshima, Japan	209	1.3 %
175.29.177.83	Bangladesh	202	1.2 %
136.40.66.242	Spanish Fork, Utah 84660, United States	190	1.2 %
202.3.225.198	Vaitape, French Polynesia	188	1.1 %
151.236.52.249	Reading, United Kingdom	186	1.1 %
89.31.72.48	Italy	186	1.1 %
185.46.188.30	Ukraine	178	1.1 %
153.127.31.83	Japan	168	1.0 %
210.167.8.2	Uozu, Japan	167	1.0 %
203.146.58.39	Thailand	148	0.9 %
203.146.58.7	Thailand	148	0.9 %
193.149.2.155	Bulgaria	144	0.9 %
202.224.55.50	Japan	134	0.8 %
60.43.195.153	Japan	132	0.8 %
Others		8.24k	50.3 %
Total		**16.39k**	**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.