Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-03-01 00:00:00 CET
To: 2023-04-01 00:00:00 CEST

Report

Table of Contents

Report run by
jens

SMC version
7.0.2, build 11323

Update version
1573

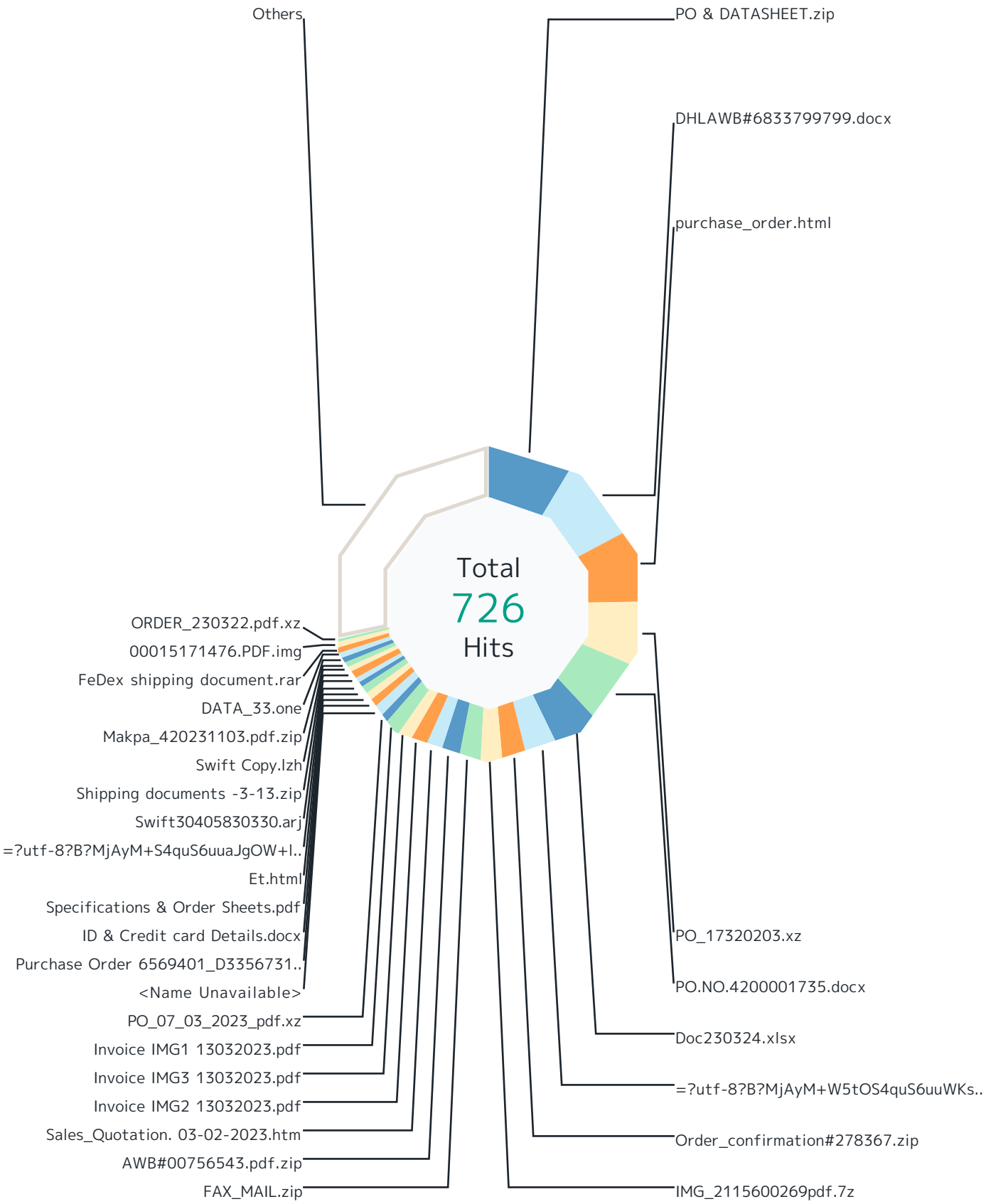
Report started
2023-04-01 09:13:30 CEST

Report run time
08:07:23

Filters used
Match All

Report

Virenfilterung MXe



Report

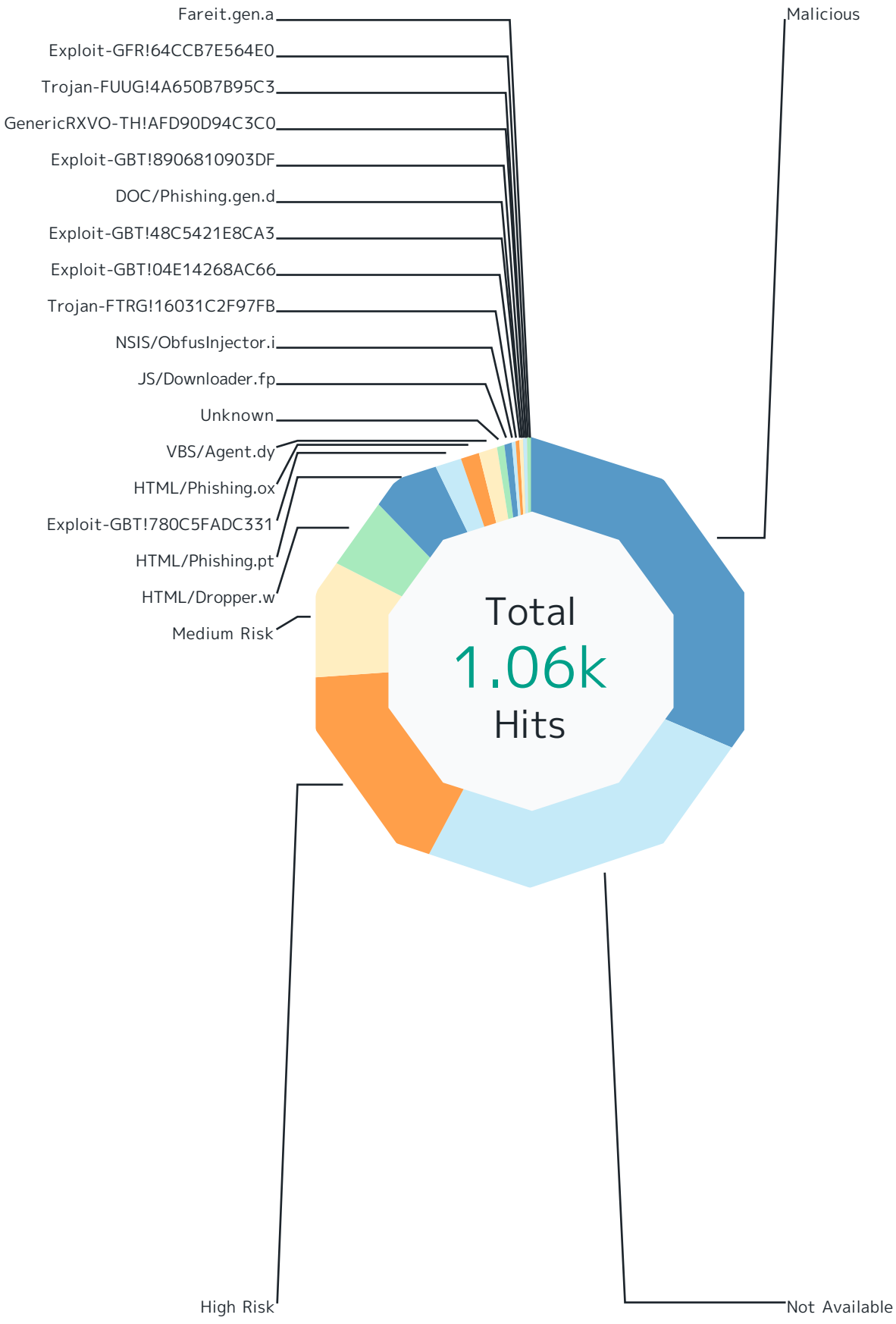
Records by file name	Hits	%
PO & DATASHEET.zip	63	8.7 %
DHLAWB#6833799799.docx	62	8.5 %
purchase_order.html	55	7.6 %
PO_17320203.xz	48	6.6 %
PO.NO.4200001735.docx	48	6.6 %
Doc230324.xlsx	35	4.8 %
=?utf-8?B?MjAyM+W5tOS4quS6uuWKs+WKqOihpei0tC5kb2N4?=	23	3.2 %
Order_confirmation#278367.zip	19	2.6 %
IMG_2115600269pdf.7z	17	2.3 %
FAX_MAIL.zip	16	2.2 %
AWB#00756543.pdf.zip	14	1.9 %
Sales_Quotation. 03-02-2023.htm	12	1.7 %
Invoice IMG2 13032023.pdf	11	1.5 %
Invoice IMG3 13032023.pdf	11	1.5 %
Invoice IMG1 13032023.pdf	11	1.5 %
PO_07_03_2023_pdf.xz	7	1.0 %
<Name Unavailable>	7	1.0 %
Purchase Order 6569401_D3356731 buy 1118_02.27.23.zip	7	1.0 %
ID & Credit card Details.docx	6	0.8 %
Specifications & Order Sheets.pdf	5	0.7 %
Et.html	5	0.7 %
=?utf-8?B?MjAyM+S4quS6uuaJgOW+l+eojuihpei0tOi1hOaWmeeUs+mihi5kb2N4?=	5	0.7 %
Swift30405830330.arj	5	0.7 %
Shipping documents -3-13.zip	4	0.6 %
Swift Copy.lzh	4	0.6 %
Makpa_420231103.pdf.zip	4	0.6 %
DATA_33.one	4	0.6 %
FeDex shipping document.rar	4	0.6 %
00015171476.PDF.img	4	0.6 %
ORDER_230322.pdf.xz	3	0.4 %
Others	207	28.5 %
Total	**726**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


Fareit.gen.a
Exploit-GFR!64CCB7E564E0
Trojan-FUUG!4A650B7B95C3
GenericRXVO-TH!AFD90D94C3C0
Exploit-GBT!8906810903DF
DOC/Phishing.gen.d
Exploit-GBT!48C5421E8CA3
Exploit-GBT!04E14268AC66
Trojan-FTRG!16031C2F97FB
NSIS/ObfusInjector.i
JS/Downloader.fp
Unknown
VBS/Agent.dy
HTML/Phishing.ox
Exploit-GBT!780C5FADC331
HTML/Phishing.pt
HTML/Dropper.w
Medium Risk
Malicious
Total
1.06k
Hits
High Risk
Not Available

Report

Scan Result	Hits	%
Malicious	**334**	**31.5 %**
File_Microsoft-Windows-Executable	109	10.3 %
File_Office-Open-XML-Package-Relations-Item	105	9.9 %
File_Zip-Archive	24	2.3 %
File_7z-Archive	22	2.1 %
File_Rar-Archive	16	1.5 %
File_Java-Class	14	1.3 %
File_Microsoft-Office-Open-XML-Document	8	0.8 %
File_Type-Unknown	6	0.6 %
File_Microsoft-OLE	6	0.6 %
File_OneNote-Document	5	0.5 %
File_PDF	4	0.4 %
File_Microsoft-Excel-97-Spreadsheet	4	0.4 %
File_HTML	3	0.3 %
File_ISO-9660-Disk-Image	2	0.2 %
File_JavaScript	2	0.2 %
File_Microsoft-Cabinet-Archive	1	0.1 %
File_LhArc-Archive	1	0.1 %
File_RTF	1	0.1 %
File_XZ-Archive	1	0.1 %
Not Available	**280**	**26.4 %**
File_Zip-Archive	228	21.5 %
File_Microsoft-Office-Open-XML-Document	36	3.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	16	1.5 %
High Risk	**170**	**16.0 %**
File_Microsoft-Windows-Executable	58	5.5 %
File_PDF	35	3.3 %
File_Rar-Archive	29	2.7 %
File_Zip-Archive	18	1.7 %
File_ISO-9660-Disk-Image	10	0.9 %
File_Office-Open-XML-Package-Relations-Item	7	0.7 %
File_Microsoft-Cabinet-Archive	3	0.3 %
File_Self-Extracting-Zip-Archive	3	0.3 %
File_JavaScript	2	0.2 %
File_HTML	1	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %

Report

Scan Result	Hits	%
File_7z-Archive	1	0.1 %
File_Tar-Archive	1	0.1 %
File_Java-Archive	1	0.1 %
Medium Risk	**92**	**8.7 %**
File_Zip-Archive	34	3.2 %
File_HTML	17	1.6 %
File_XML	16	1.5 %
File_Rar-Archive	10	0.9 %
File_PDF	6	0.6 %
File_OneNote-Document	4	0.4 %
File_Type-Unknown	3	0.3 %
File_Microsoft-Windows-Executable	1	0.1 %
File_ISO-9660-Disk-Image	1	0.1 %
HTML/Dropper.w	**55**	**5.2 %**
File_HTML	55	5.2 %
HTML/Phishing.pt	**55**	**5.2 %**
File_HTML	55	5.2 %
Exploit-GBT!780C5FADC331	**20**	**1.9 %**
File_Microsoft-Excel-XLSX-Filename-Extension	20	1.9 %
HTML/Phishing.ox	**16**	**1.5 %**
File_HTML	16	1.5 %
VBS/Agent.dy	**13**	**1.2 %**
File_Rar-Archive	13	1.2 %
Unknown	**6**	**0.6 %**
File_Zip-Archive	6	0.6 %
JS/Downloader.fp	**6**	**0.6 %**
File_Zip-Archive	4	0.4 %
File_Type-Unknown	2	0.2 %
NSIS/ObfusInjector.i	**4**	**0.4 %**
File_Rar-Archive	4	0.4 %
Trojan-FTRG!16031C2F97FB	**2**	**0.2 %**
File_Rar-Archive	2	0.2 %
Exploit-GBT!04E14268AC66	**2**	**0.2 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.2 %
Exploit-GBT!48C5421E8CA3	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %

Report

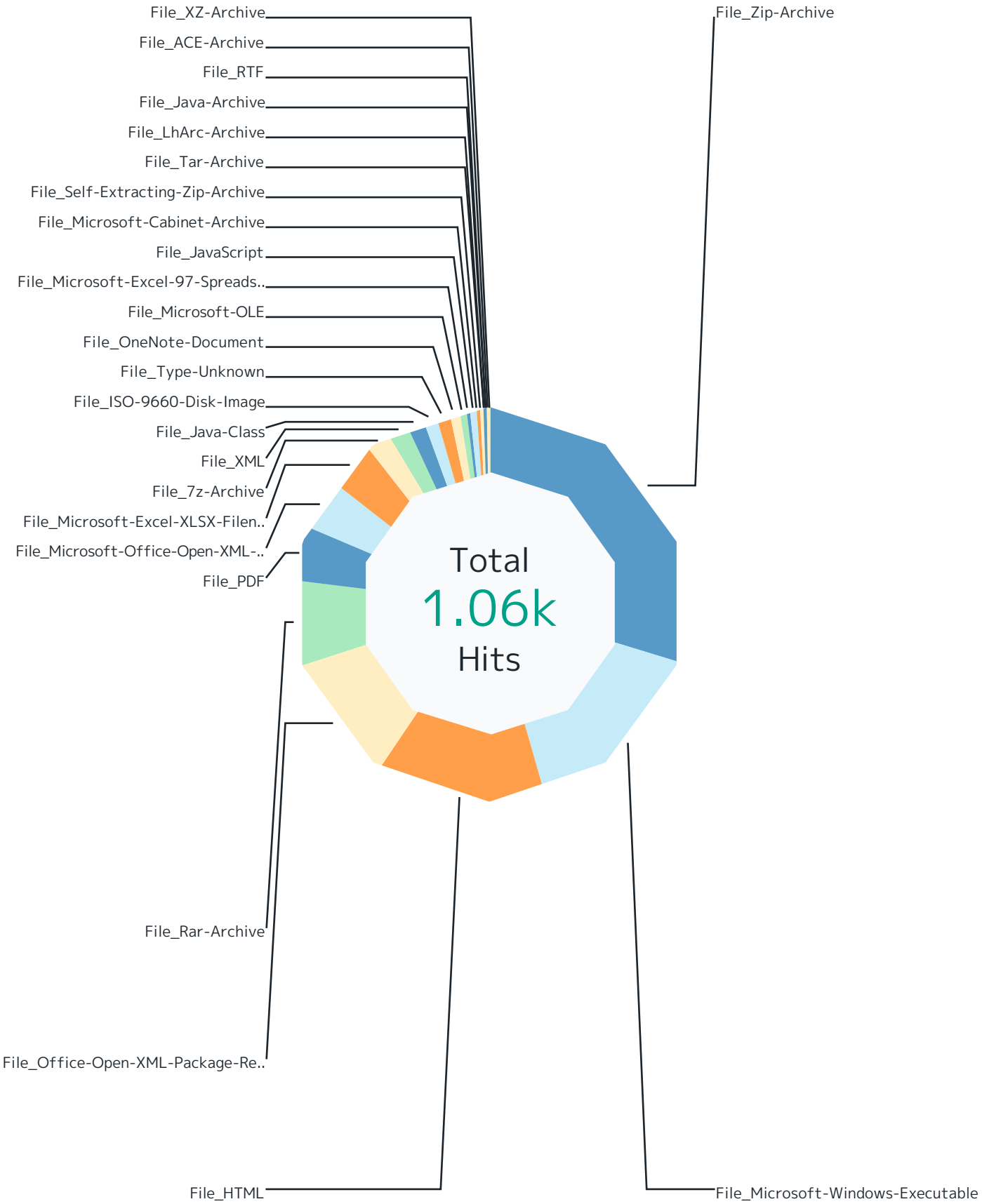
Scan Result	Hits	%
DOC/Phishing.gen.d	**1**	**0.1 %**
File_Zip-Archive	1	0.1 %
Exploit-GBT!8906810903DF	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
GenericRXVO-TH!AFD90D94C3C0	**1**	**0.1 %**
File_Rar-Archive	1	0.1 %
Trojan-FUUG!4A650B7B95C3	**1**	**0.1 %**
File_Rar-Archive	1	0.1 %
Exploit-GFR!64CCB7E564E0	**1**	**0.1 %**
File_Microsoft-Office-Open-XML-Document	1	0.1 %
Fareit.gen.a	**1**	**0.1 %**
File_ACE-Archive	1	0.1 %
Total	**1.06k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_XZ-Archive
File_ACE-Archive
File_RTF
File_Java-Archive
File_LhArc-Archive
File_Tar-Archive
File_Self-Extracting-Zip-Archive
File_Microsoft-Cabinet-Archive
File_JavaScript
File_Microsoft-Excel-97-Spreads..
File_Microsoft-OLE
File_OneNote-Document
File_Type-Unknown
File_ISO-9660-Disk-Image
File_Java-Class
File_XML
File_7z-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Office-Open-XML-..
File_PDF
File_Zip-Archive
Total
1.06k
Hits
File_Rar-Archive
File_Office-Open-XML-Package-Re..
File_HTML
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**315**	**29.7 %**
Not Available	228	21.5 %
Medium Risk	34	3.2 %
Malicious	24	2.3 %
High Risk	18	1.7 %
Unknown	6	0.6 %
JS/Downloader.fp	4	0.4 %
DOC/Phishing.gen.d	1	0.1 %
File_Microsoft-Windows-Executable	**168**	**15.8 %**
Malicious	109	10.3 %
High Risk	58	5.5 %
Medium Risk	1	0.1 %
File_HTML	**147**	**13.8 %**
HTML/Dropper.w	55	5.2 %
HTML/Phishing.pt	55	5.2 %
Medium Risk	17	1.6 %
HTML/Phishing.ox	16	1.5 %
Malicious	3	0.3 %
High Risk	1	0.1 %
File_Office-Open-XML-Package-Relations-Item	**112**	**10.5 %**
Malicious	105	9.9 %
High Risk	7	0.7 %
File_Rar-Archive	**76**	**7.2 %**
High Risk	29	2.7 %
Malicious	16	1.5 %
VBS/Agent.dy	13	1.2 %
Medium Risk	10	0.9 %
NSIS/ObfusInjector.i	4	0.4 %
Trojan-FTRG!16031C2F97FB	2	0.2 %
GenericRXVO-TH!AFD90D94C3C0	1	0.1 %
Trojan-FUUG!4A650B7B95C3	1	0.1 %
File_PDF	**45**	**4.2 %**
High Risk	35	3.3 %
Medium Risk	6	0.6 %
Malicious	4	0.4 %
File_Microsoft-Office-Open-XML-Document	**45**	**4.2 %**

Report

Responding Scanner	Hits	%
Not Available	36	3.4 %
Malicious	8	0.8 %
Exploit-GFR!64CCB7E564E0	1	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**41**	**3.9 %**
Exploit-GBT!780C5FADC331	20	1.9 %
Not Available	16	1.5 %
Exploit-GBT!04E14268AC66	2	0.2 %
High Risk	1	0.1 %
Exploit-GBT!48C5421E8CA3	1	0.1 %
Exploit-GBT!8906810903DF	1	0.1 %
File_7z-Archive	**23**	**2.2 %**
Malicious	22	2.1 %
High Risk	1	0.1 %
File_XML	**16**	**1.5 %**
Medium Risk	16	1.5 %
File_Java-Class	**14**	**1.3 %**
Malicious	14	1.3 %
File_ISO-9660-Disk-Image	**13**	**1.2 %**
High Risk	10	0.9 %
Malicious	2	0.2 %
Medium Risk	1	0.1 %
File_Type-Unknown	**11**	**1.0 %**
Malicious	6	0.6 %
Medium Risk	3	0.3 %
JS/Downloader.fp	2	0.2 %
File_OneNote-Document	**9**	**0.8 %**
Malicious	5	0.5 %
Medium Risk	4	0.4 %
File_Microsoft-OLE	**6**	**0.6 %**
Malicious	6	0.6 %
File_Microsoft-Excel-97-Spreadsheet	**4**	**0.4 %**
Malicious	4	0.4 %
File_JavaScript	**4**	**0.4 %**
Malicious	2	0.2 %
High Risk	2	0.2 %
File_Microsoft-Cabinet-Archive	**4**	**0.4 %**

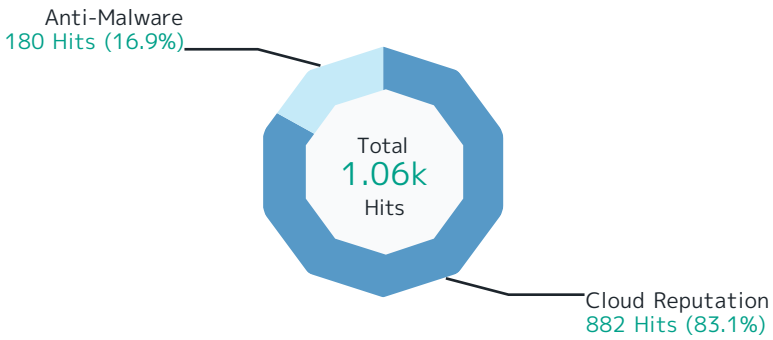
Report

Responding Scanner	Hits	%
High Risk	3	0.3 %
Malicious	1	0.1 %
File_Self-Extracting-Zip-Archive	**3**	**0.3 %**
High Risk	3	0.3 %
File_Tar-Archive	**1**	**0.1 %**
High Risk	1	0.1 %
File_LhArc-Archive	**1**	**0.1 %**
Malicious	1	0.1 %
File_Java-Archive	**1**	**0.1 %**
High Risk	1	0.1 %
File_RTF	**1**	**0.1 %**
Malicious	1	0.1 %
File_ACE-Archive	**1**	**0.1 %**
Fareit.gen.a	1	0.1 %
File_XZ-Archive	**1**	**0.1 %**
Malicious	1	0.1 %
Total	**1.06k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.

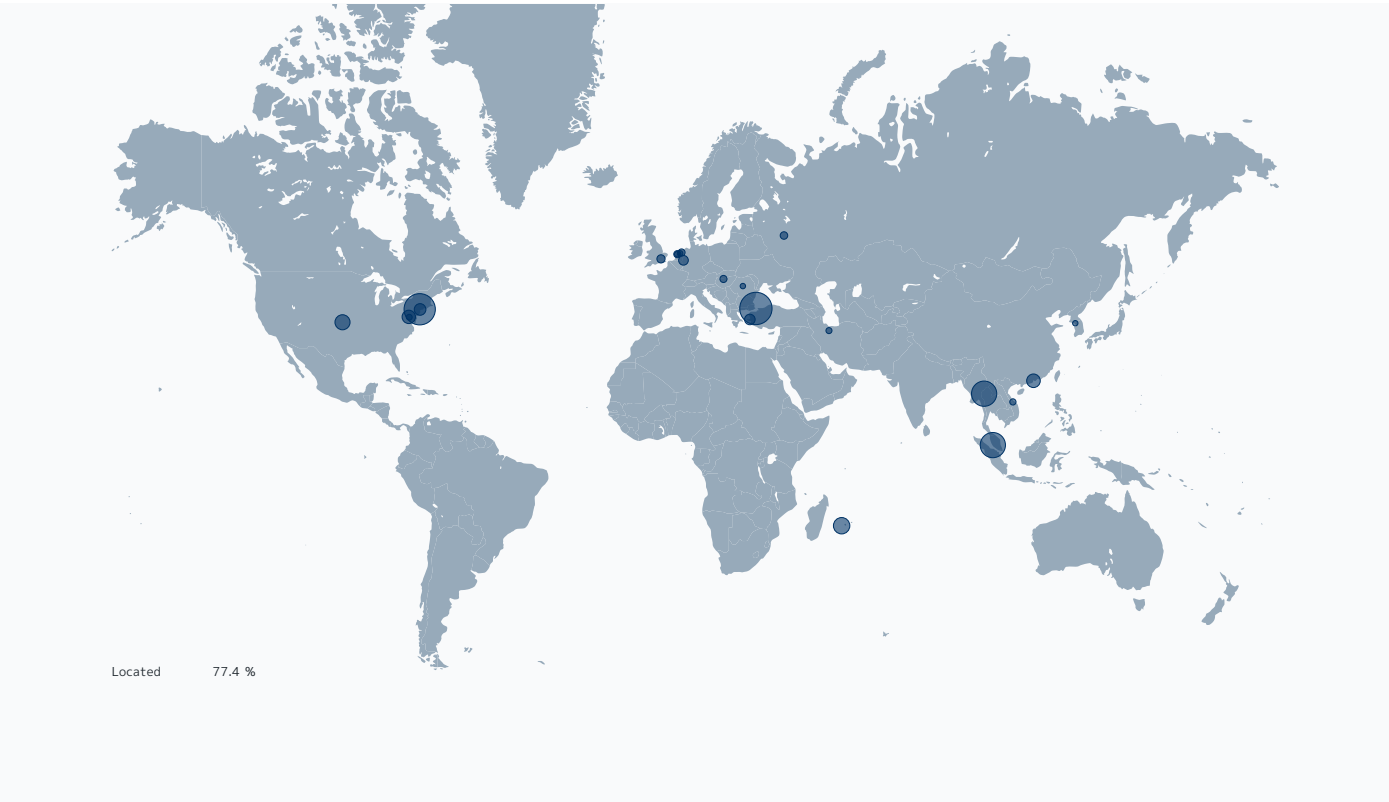


Report

Responding Scanner	Hits	%
Cloud Reputation	**882**	**83.1 %**
File_Zip-Archive	310	29.2 %
File_Microsoft-Windows-Executable	168	15.8 %
File_Office-Open-XML-Package-Relations-Item	112	10.5 %
File_Rar-Archive	55	5.2 %
File_PDF	45	4.2 %
File_Microsoft-Office-Open-XML-Document	44	4.1 %
File_7z-Archive	23	2.2 %
File_HTML	21	2.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	17	1.6 %
File_XML	16	1.5 %
File_Java-Class	14	1.3 %
File_ISO-9660-Disk-Image	13	1.2 %
File_Type-Unknown	9	0.8 %
File_OneNote-Document	9	0.8 %
File_Microsoft-OLE	6	0.6 %
File_Microsoft-Excel-97-Spreadsheet	4	0.4 %
File_JavaScript	4	0.4 %
File_Microsoft-Cabinet-Archive	4	0.4 %
File_Self-Extracting-Zip-Archive	3	0.3 %
File_Tar-Archive	1	0.1 %
File_LhArc-Archive	1	0.1 %
File_Java-Archive	1	0.1 %
File_RTF	1	0.1 %
File_XZ-Archive	1	0.1 %
Anti-Malware	**180**	**16.9 %**
File_HTML	126	11.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	24	2.3 %
File_Rar-Archive	21	2.0 %
File_Zip-Archive	5	0.5 %
File_Type-Unknown	2	0.2 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %
File_ACE-Archive	1	0.1 %
Total	**1.06k**	**100 %**

Report

Virenfilterung SRC IPs



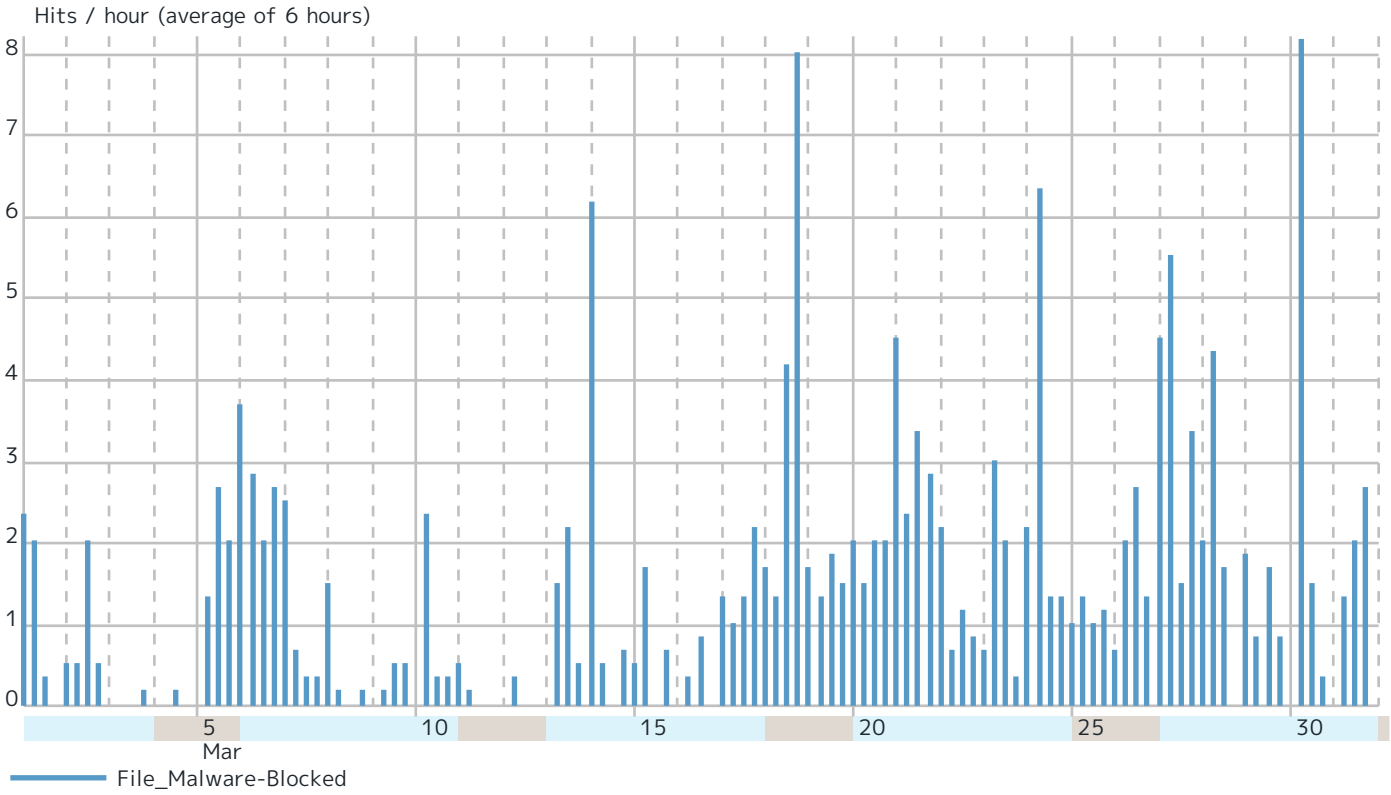
Report

Records by src IP		Hits	%
212.68.46.101	Turkey	129	12.1 %
45.55.144.104	Clifton, New Jersey 07014, United States	124	11.7 %
111.90.143.104	Kuala Lumpur, Malaysia	96	9.0 %
61.7.233.62	Lamphun, Thailand	96	9.0 %
165.169.241.29	Les Trois-Bassins, 97426 Réunion	55	5.2 %
47.243.140.251	Central, Hong Kong	42	4.0 %
45.84.199.169	Ashburn, Virginia 20149, United States	41	3.9 %
67.205.130.16	North Bergen, New Jersey 07047, United States	33	3.1 %
194.116.190.155	Izmir, Turkey	28	2.6 %
184.174.34.158	Düsseldorf, Germany	24	2.3 %
77.88.226.134	United Kingdom	17	1.6 %
167.89.10.181	United States	16	1.5 %
193.19.66.22	Russia	14	1.3 %
209.142.64.192	United States	12	1.1 %
80.92.206.125	Meppel, Netherlands	12	1.1 %
168.245.59.205	United States	12	1.1 %
83.137.158.181	Hungary	8	0.8 %
45.92.94.63	Iran	7	0.7 %
193.42.33.211	Netherlands	6	0.6 %
212.87.204.147	Reston, Virginia 20190, United States	6	0.6 %
95.211.156.157	Netherlands	6	0.6 %
212.86.109.237	Dronten, Netherlands	5	0.5 %
192.236.192.129	United States	5	0.5 %
83.137.158.154	Hungary	4	0.4 %
45.137.22.141	Amsterdam, Netherlands	4	0.4 %
45.124.84.10	Vietnam	4	0.4 %
222.231.1.120	South Korea	4	0.4 %
162.214.97.106	United States	4	0.4 %
91.235.116.67	Romania	4	0.4 %
210.2.86.112	Vietnam	4	0.4 %
Others		240	22.6 %
Total		**1.06k**	**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.