Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-02-01 00:00:00 CET
To: 2023-03-01 00:00:00 CET

Report

Report run by
jens

SMC version
7.0.1, build 11318

Update version
1560

Report started
2023-03-02 13:56:14 CET

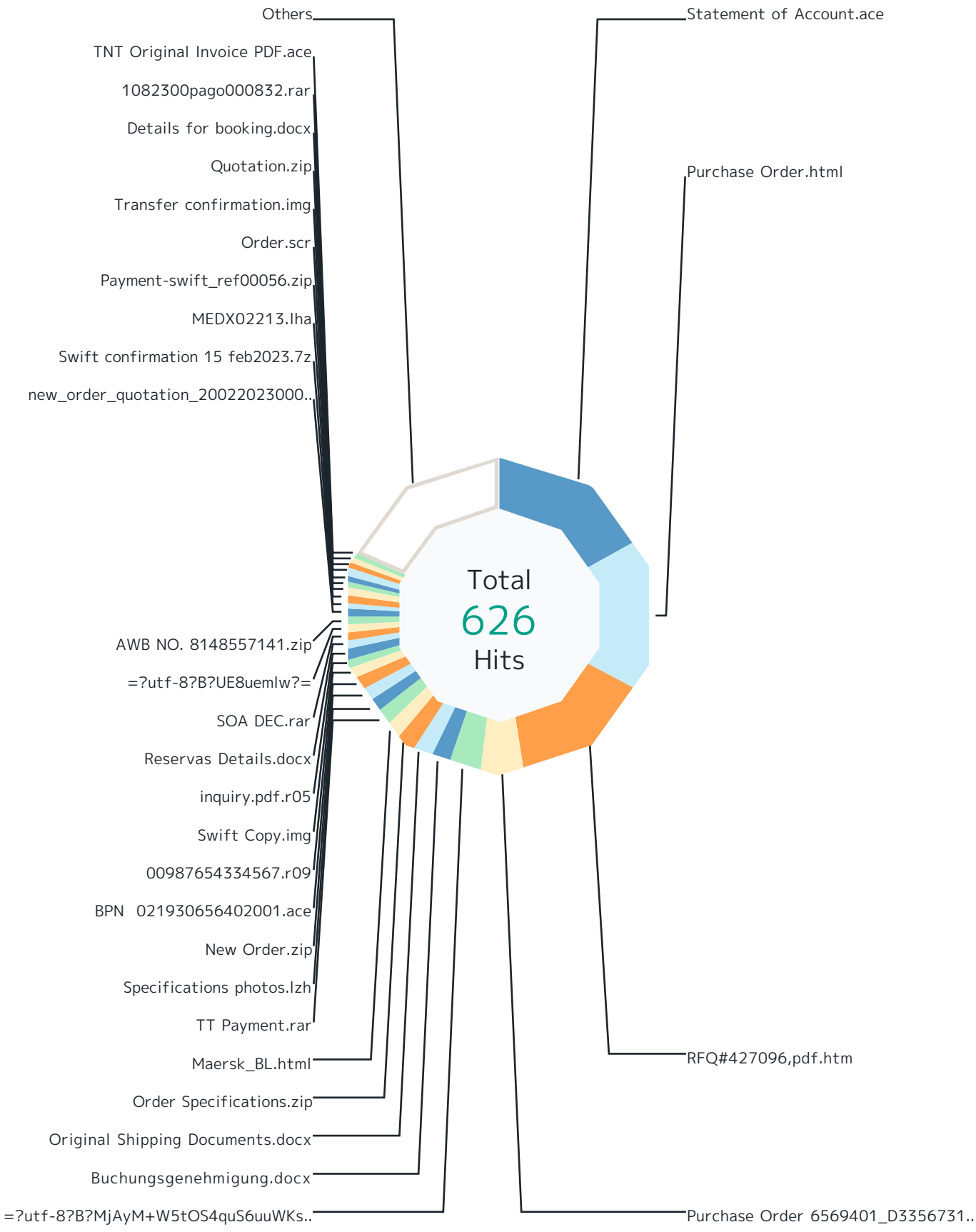
Report run time
07:30:49

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



Report

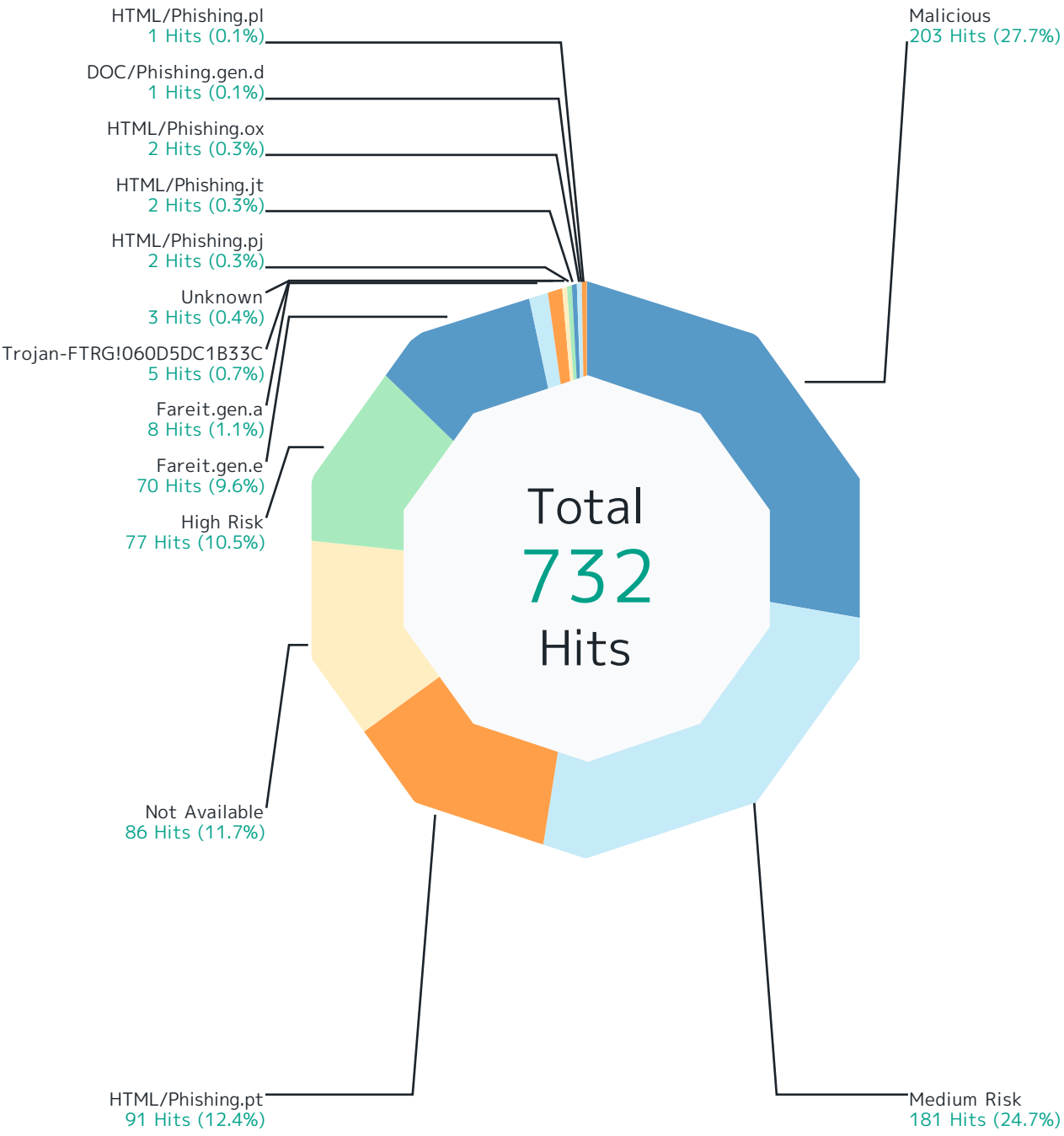
Records by file name	Hits	%
Statement of Account.ace	106	16.9 %
Purchase Order.html	100	16.0 %
RFQ#427096,pdf.htm	91	14.5 %
Purchase Order 6569401_D3356731 buy 1118_02.27.23.zip	28	4.5 %
=?utf-8?B?MjAyM+W5tOS4quS6uuWKs+WKqOihpei0tC5kb2N4?=	21	3.4 %
Buchungsgenehmigung.docx	13	2.1 %
Original Shipping Documents.docx	12	1.9 %
Order Specifications.zip	11	1.8 %
Maersk_BL.html	11	1.8 %
TT Payment.rar	10	1.6 %
Specifications photos.lzh	9	1.4 %
New Order.zip	9	1.4 %
BPN 021930656402001.ace	8	1.3 %
00987654334567.r09	7	1.1 %
Swift Copy.img	6	1.0 %
inquiry.pdf.r05	6	1.0 %
Reservas Details.docx	6	1.0 %
SOA DEC.rar	5	0.8 %
=?utf-8?B?UE8uemlw?=	5	0.8 %
AWB NO. 8148557141.zip	5	0.8 %
new_order_quotation_2002202300000000000000001_PDF.cab	5	0.8 %
Swift confirmation 15 feb2023.7z	5	0.8 %
MEDX02213.lha	5	0.8 %
Payment-swift_ref00056.zip	4	0.6 %
Order.scr	4	0.6 %
Transfer confirmation.img	4	0.6 %
Quotation.zip	4	0.6 %
Details for booking.docx	4	0.6 %
1082300pago000832.rar	4	0.6 %
TNT Original Invoice PDF.ace	4	0.6 %
Others	114	18.2 %
Total	**626**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report



Scan Result	Hits	%
Malicious	**203**	**27.7 %**

Report

Scan Result	Hits	%
File_Microsoft-Windows-Executable	60	8.2 %
File_ACE-Archive	49	6.7 %
File_Rar-Archive	20	2.7 %
File_Zip-Archive	14	1.9 %
File_LhArc-Archive	14	1.9 %
File_ISO-9660-Disk-Image	13	1.8 %
File_Office-Open-XML-Package-Relations-Item	12	1.6 %
File_Type-Unknown	6	0.8 %
File_Microsoft-Cabinet-Archive	6	0.8 %
File_7z-Archive	5	0.7 %
File_OneNote-Document	2	0.3 %
File_HTML	1	0.1 %
File_XZ-Archive	1	0.1 %
Medium Risk	**181**	**24.7 %**
File_JavaScript	102	13.9 %
File_Rar-Archive	19	2.6 %
File_Zip-Archive	18	2.5 %
File_Microsoft-Office-Open-XML-Document	15	2.0 %
File_HTML	14	1.9 %
File_Office-Open-XML-Package-Relations-Item	8	1.1 %
File_ISO-9660-Disk-Image	2	0.3 %
File_Type-Unknown	2	0.3 %
File_Microsoft-Windows-Executable	1	0.1 %
HTML/Phishing.pt	**91**	**12.4 %**
File_HTML	91	12.4 %
Not Available	**86**	**11.7 %**
File_Zip-Archive	75	10.2 %
File_Microsoft-Office-Open-XML-Document	10	1.4 %
File_Microsoft-Excel-Spreadsheet	1	0.1 %
High Risk	**77**	**10.5 %**
File_Rar-Archive	28	3.8 %
File_Microsoft-Windows-Executable	23	3.1 %
File_Zip-Archive	8	1.1 %
File_ISO-9660-Disk-Image	8	1.1 %
File_LhArc-Archive	3	0.4 %
File_Type-Unknown	3	0.4 %

Report

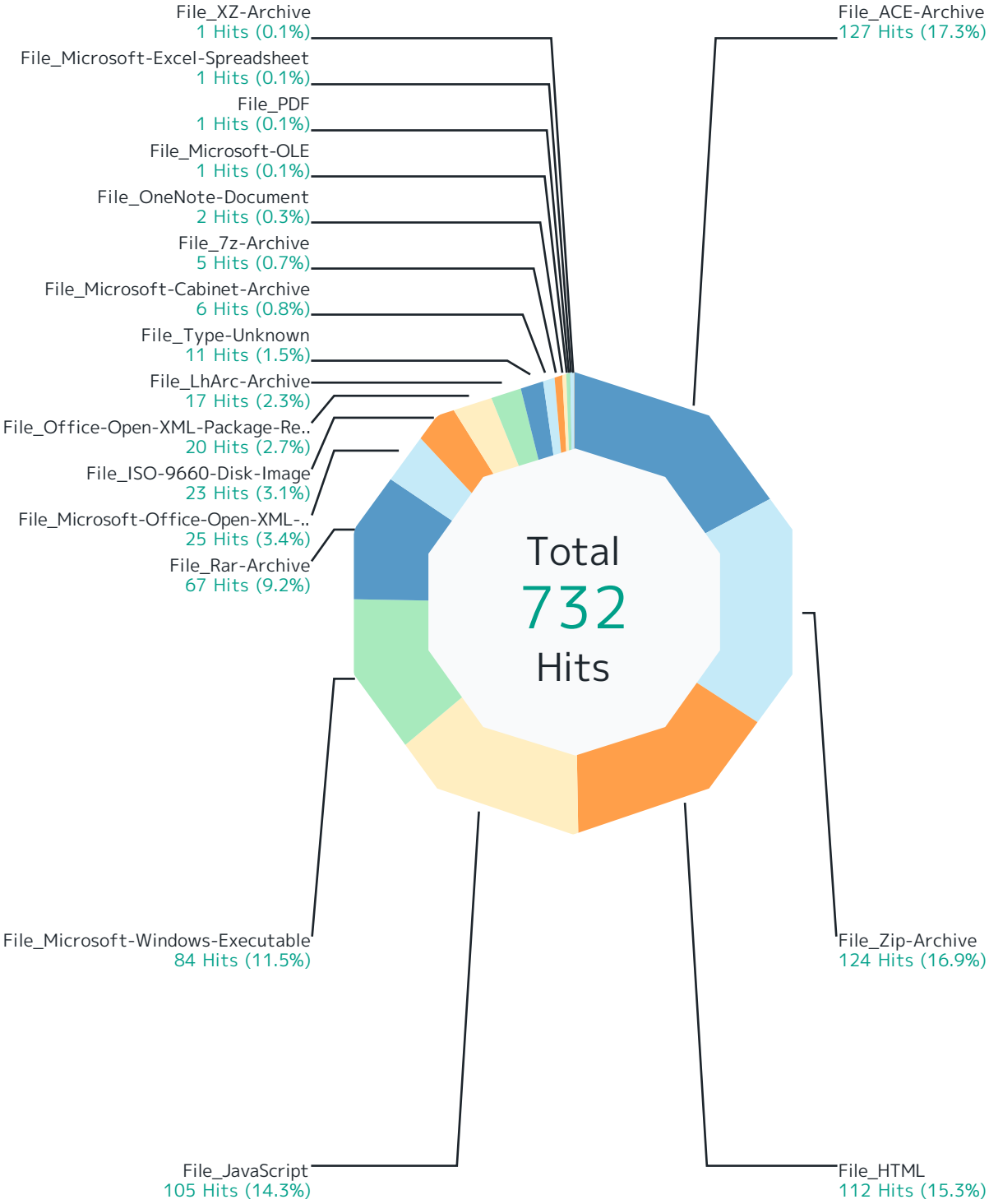
Scan Result	Hits	%
File_HTML	2	0.3 %
File_Microsoft-OLE	1	0.1 %
File_PDF	1	0.1 %
Fareit.gen.e	**70**	**9.6 %**
File_ACE-Archive	70	9.6 %
Fareit.gen.a	**8**	**1.1 %**
File_ACE-Archive	8	1.1 %
Trojan-FTRG!060D5DC1B33C	**5**	**0.7 %**
File_Zip-Archive	5	0.7 %
Unknown	**3**	**0.4 %**
File_Zip-Archive	3	0.4 %
HTML/Phishing.pj	**2**	**0.3 %**
File_JavaScript	2	0.3 %
HTML/Phishing.jt	**2**	**0.3 %**
File_HTML	2	0.3 %
HTML/Phishing.ox	**2**	**0.3 %**
File_HTML	2	0.3 %
DOC/Phishing.gen.d	**1**	**0.1 %**
File_Zip-Archive	1	0.1 %
HTML/Phishing.pl	**1**	**0.1 %**
File_JavaScript	1	0.1 %
Total	**732**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_XZ-Archive
1 Hits (0.1%)
File_Microsoft-Excel-Spreadsheet
1 Hits (0.1%)
File_PDF
1 Hits (0.1%)
File_Microsoft-OLE
1 Hits (0.1%)
File_OneNote-Document
2 Hits (0.3%)
File_7z-Archive
5 Hits (0.7%)
File_Microsoft-Cabinet-Archive
6 Hits (0.8%)
File_Type-Unknown
11 Hits (1.5%)
File_LhArc-Archive
17 Hits (2.3%)
File_Office-Open-XML-Package-Re..
20 Hits (2.7%)
File_ISO-9660-Disk-Image
23 Hits (3.1%)
File_Microsoft-Office-Open-XML-..
25 Hits (3.4%)
File_Rar-Archive
67 Hits (9.2%)
File_ACE-Archive
127 Hits (17.3%)
Total
732
Hits
File_Microsoft-Windows-Executable
84 Hits (11.5%)
File_Zip-Archive
124 Hits (16.9%)
File_JavaScript
105 Hits (14.3%)
File_HTML
112 Hits (15.3%)

Report

Responding Scanner	Hits	%
File_ACE-Archive	**127**	**17.3 %**
Fareit.gen.e	70	9.6 %
Malicious	49	6.7 %
Fareit.gen.a	8	1.1 %
File_Zip-Archive	**124**	**16.9 %**
Not Available	75	10.2 %
Medium Risk	18	2.5 %
Malicious	14	1.9 %
High Risk	8	1.1 %
Trojan-FTRG!060D5DC1B33C	5	0.7 %
Unknown	3	0.4 %
DOC/Phishing.gen.d	1	0.1 %
File_HTML	**112**	**15.3 %**
HTML/Phishing.pt	91	12.4 %
Medium Risk	14	1.9 %
High Risk	2	0.3 %
HTML/Phishing.jt	2	0.3 %
HTML/Phishing.ox	2	0.3 %
Malicious	1	0.1 %
File_JavaScript	**105**	**14.3 %**
Medium Risk	102	13.9 %
HTML/Phishing.pj	2	0.3 %
HTML/Phishing.pl	1	0.1 %
File_Microsoft-Windows-Executable	**84**	**11.5 %**
Malicious	60	8.2 %
High Risk	23	3.1 %
Medium Risk	1	0.1 %
File_Rar-Archive	**67**	**9.2 %**
High Risk	28	3.8 %
Malicious	20	2.7 %
Medium Risk	19	2.6 %
File_Microsoft-Office-Open-XML-Document	**25**	**3.4 %**
Medium Risk	15	2.0 %
Not Available	10	1.4 %
File_ISO-9660-Disk-Image	**23**	**3.1 %**
Malicious	13	1.8 %

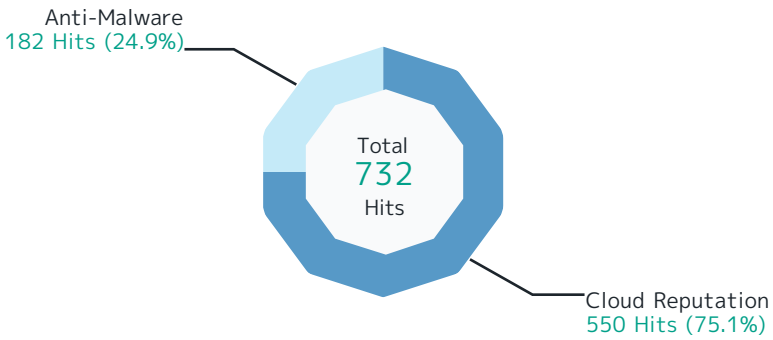
Report

Responding Scanner	Hits	%
High Risk	8	1.1 %
Medium Risk	2	0.3 %
File_Office-Open-XML-Package-Relations-Item	**20**	**2.7 %**
Malicious	12	1.6 %
Medium Risk	8	1.1 %
File_LhArc-Archive	**17**	**2.3 %**
Malicious	14	1.9 %
High Risk	3	0.4 %
File_Type-Unknown	**11**	**1.5 %**
Malicious	6	0.8 %
High Risk	3	0.4 %
Medium Risk	2	0.3 %
File_Microsoft-Cabinet-Archive	**6**	**0.8 %**
Malicious	6	0.8 %
File_7z-Archive	**5**	**0.7 %**
Malicious	5	0.7 %
File_OneNote-Document	**2**	**0.3 %**
Malicious	2	0.3 %
File_Microsoft-OLE	**1**	**0.1 %**
High Risk	1	0.1 %
File_PDF	**1**	**0.1 %**
High Risk	1	0.1 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.1 %**
Not Available	1	0.1 %
File_XZ-Archive	**1**	**0.1 %**
Malicious	1	0.1 %
Total	**732**	**100 %**

Report

Top File Types by Responding Scanner

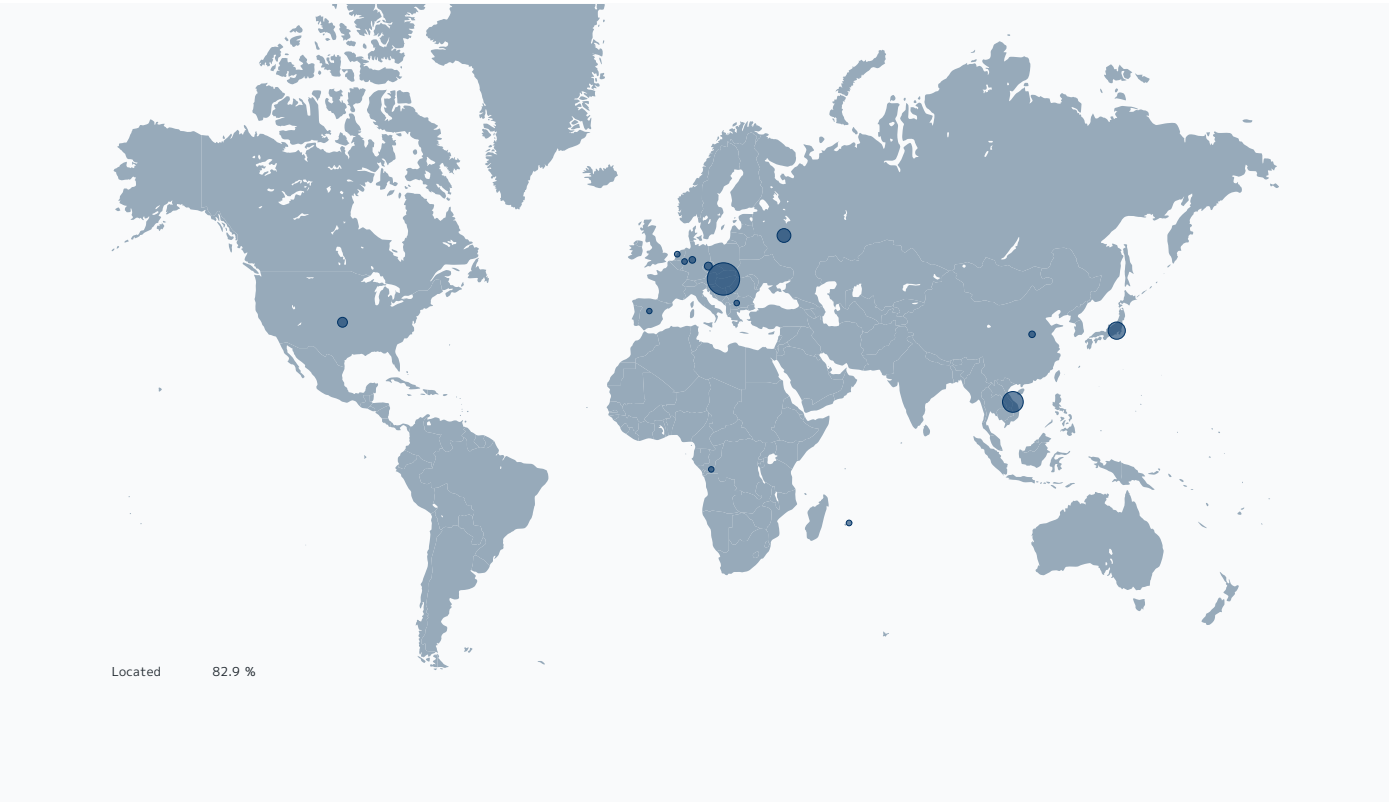
Top 10 file types by responding scanner.



Responding Scanner	Hits	%
Cloud Reputation	**550**	**75.1 %**
File_Zip-Archive	118	16.1 %
File_JavaScript	102	13.9 %
File_Microsoft-Windows-Executable	84	11.5 %
File_Rar-Archive	67	9.2 %
File_ACE-Archive	49	6.7 %
File_Microsoft-Office-Open-XML-Document	25	3.4 %
File_ISO-9660-Disk-Image	23	3.1 %
File_Office-Open-XML-Package-Relations-Item	20	2.7 %
File_HTML	17	2.3 %
File_LhArc-Archive	17	2.3 %
File_Type-Unknown	11	1.5 %
File_Microsoft-Cabinet-Archive	6	0.8 %
File_7z-Archive	5	0.7 %
File_OneNote-Document	2	0.3 %
File_Microsoft-OLE	1	0.1 %
File_PDF	1	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.1 %
File_XZ-Archive	1	0.1 %
Anti-Malware	**182**	**24.9 %**
File_HTML	95	13.0 %
File_ACE-Archive	78	10.7 %
File_Zip-Archive	6	0.8 %
File_JavaScript	3	0.4 %
Total	**732**	**100 %**

Report

Virenfilterung SRC IPs



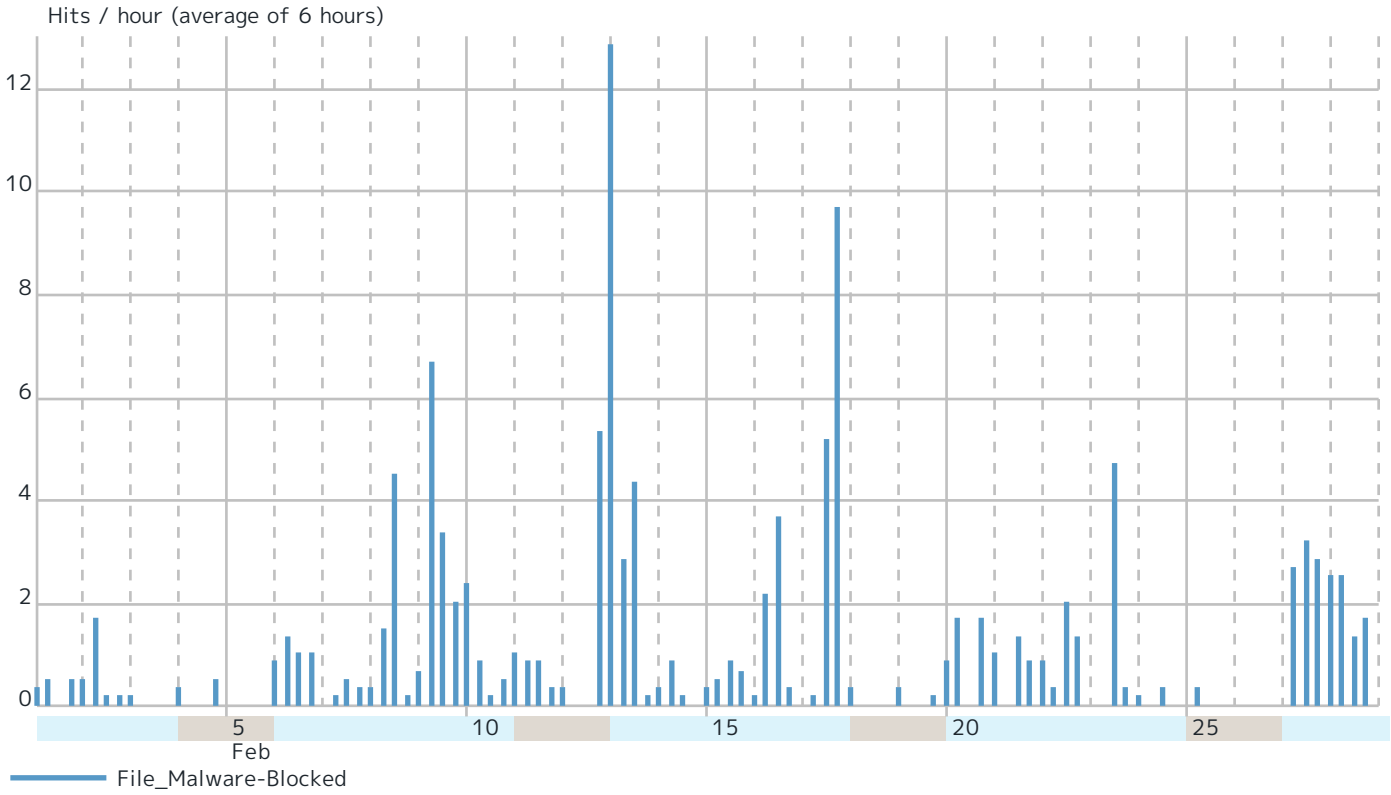
Report

Records by src IP		Hits	%
92.52.217.221	Hungary	106	14.5 %
103.176.111.45	Vietnam	100	13.7 %
61.120.105.58	Japan	91	12.4 %
193.19.66.22	Russia	56	7.7 %
92.52.217.12	Hungary	24	3.3 %
212.193.30.60	Czechia	24	3.3 %
92.52.217.90	Hungary	22	3.0 %
209.142.66.204	United States	18	2.5 %
65.60.40.105	United States	15	2.0 %
92.52.217.245	Hungary	13	1.8 %
92.52.217.179	Hungary	11	1.5 %
85.92.108.222	Russia	10	1.4 %
168.119.145.178	Germany	9	1.2 %
219.134.125.148	China	9	1.2 %
144.76.135.78	Bergisch Gladbach, Germany	8	1.1 %
45.195.25.131	Mauritius	8	1.1 %
202.55.135.90	Vietnam	8	1.1 %
103.167.84.207	Vietnam	8	1.1 %
185.222.57.144	Amsterdam, Netherlands	8	1.1 %
217.171.88.115	Kinshasa, DR Congo	7	1.0 %
78.142.63.233	Dupnitsa, Bulgaria	7	1.0 %
188.40.240.227	Germany	6	0.8 %
178.33.167.180	Madrid, Spain	6	0.8 %
92.52.217.42	Hungary	5	0.7 %
88.209.254.183	Hungary	5	0.7 %
88.209.254.29	Hungary	5	0.7 %
121.205.3.183	China	5	0.7 %
192.3.248.207	United States	5	0.7 %
92.52.217.113	Hungary	4	0.5 %
194.41.47.206	Hungary	4	0.5 %
Others		125	17.1 %
Total		**732**	**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.