Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2023-05-01 00:00:00 CEST
To: 2023-06-01 00:00:00 CEST

Report

Report run by
jens

SMC version
7.0.3, build 11326

Update version
1595

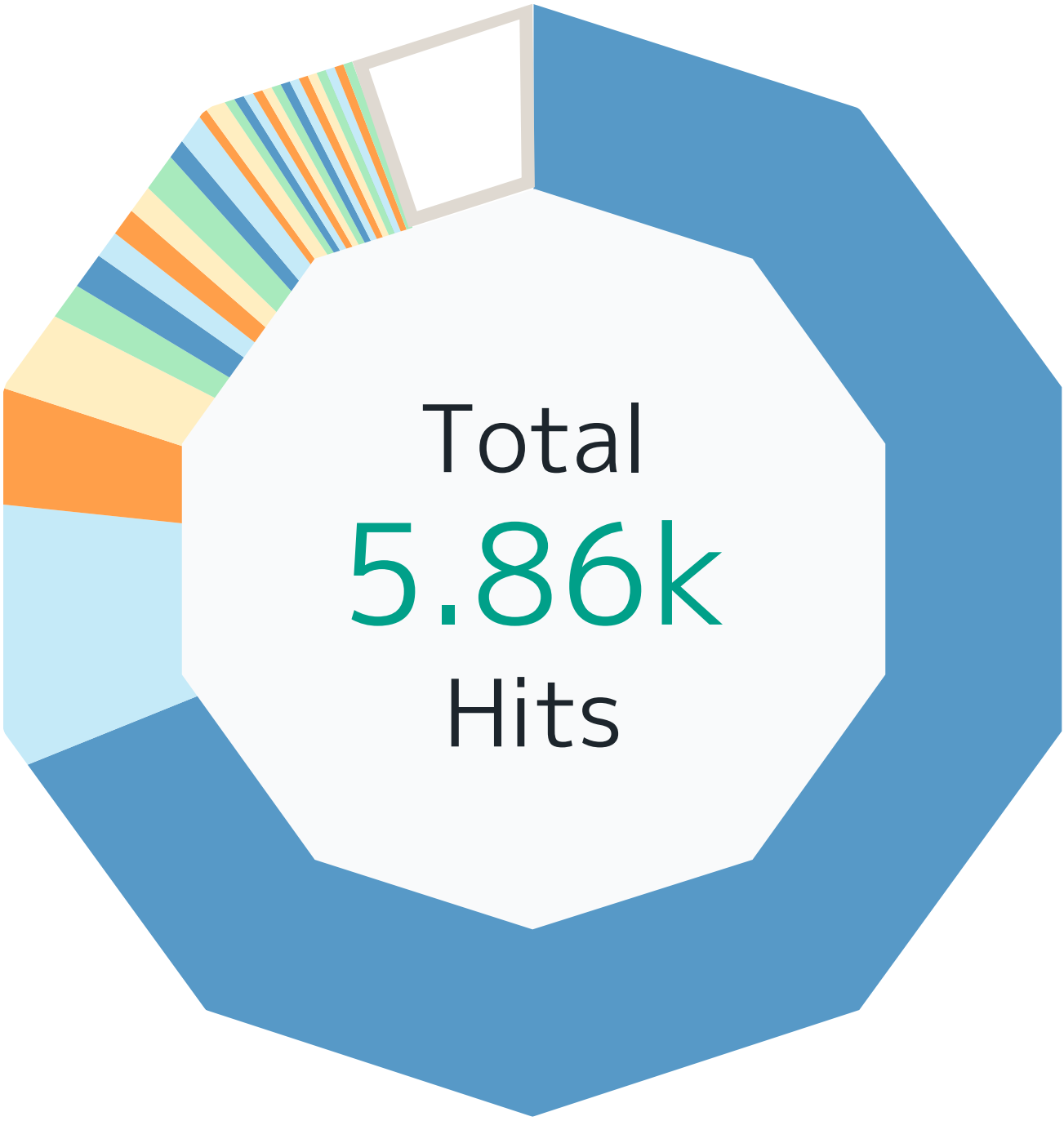
Report started
2023-06-01 09:08:06 CEST

Report run time
07:34:11

Filters used
Match All

Table of Contents

Virenfilterung MXe



Report

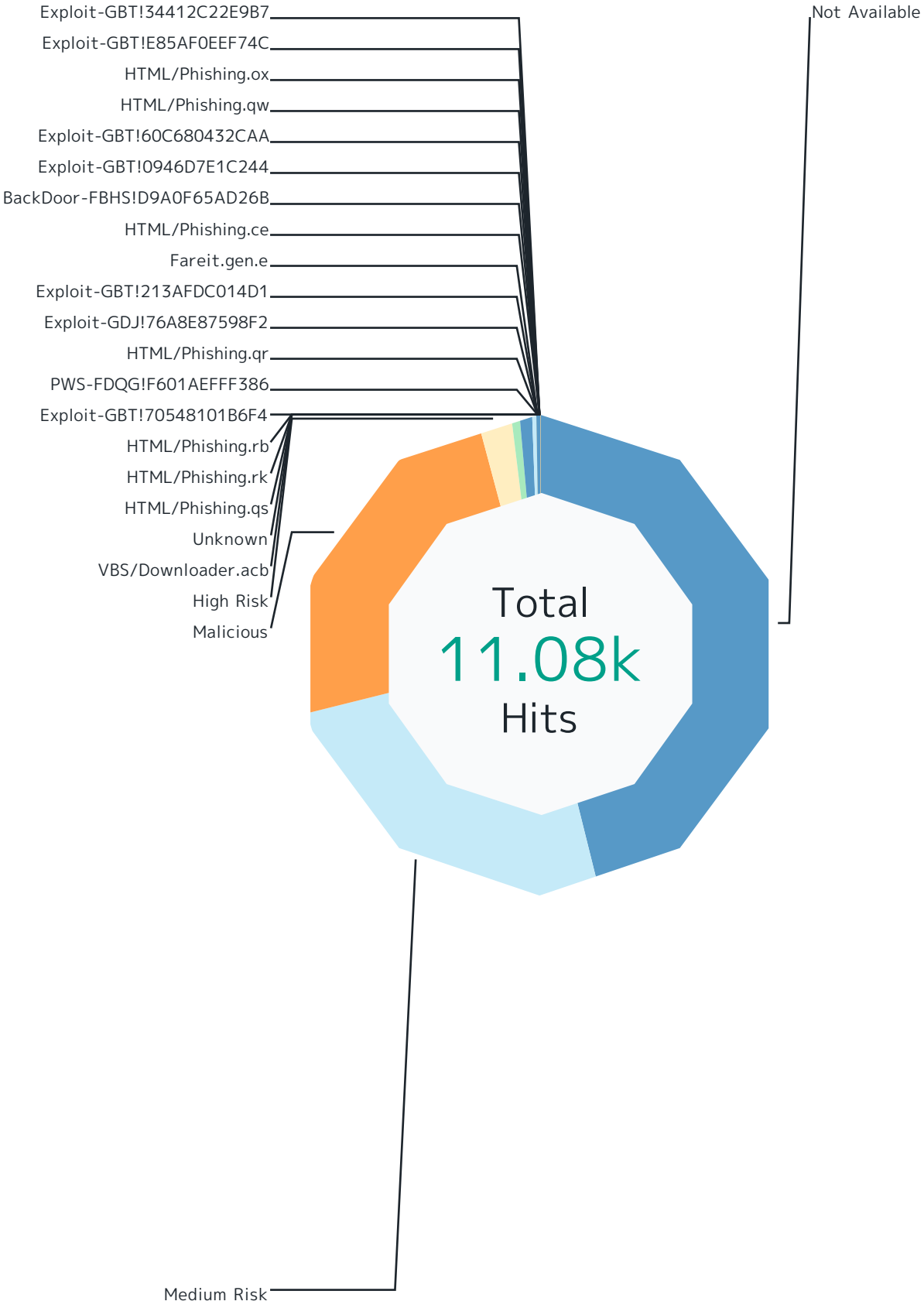
Records by file name	Hits	%
ACH Remittance.zip	4.03k	68.8 %
20230509_PPS.pptx	463	7.9 %
Quotation request.uue	194	3.3 %
Mitarbeiter_innen-Umfrage zu Child Safeguarding_2023.pptx	152	2.6 %
PO2723030194.docx	61	1.0 %
00382562524253626.zip	60	1.0 %
Stammdaten-Formular_ACC_4.0 (1).xlsx	54	0.9 %
Stammdaten-Formular_ACC_4.0.xlsx	53	0.9 %
image001.gif	50	0.9 %
230426 M8 Unterbringung Wiesbaden.xlsx	50	0.9 %
INVOICE TX 3931 2023 LO.xz	43	0.7 %
PACKING LIST TX 3931 2023 LO.xz	43	0.7 %
Download_ Tracking Reference.doc.docx	22	0.4 %
RFQ 89990043.rar	22	0.4 %
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtSAtINC60L7QvdGC0LXQutGB0YLQvdCw?==?utf-8?B?0Y8g0YDQtdC60Lv..	20	0.3 %
Offer - contextual advertising.docx	20	0.3 %
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtS5kb2N4?=	20	0.3 %
SV0077006565650655.7z	18	0.3 %
Ihr garantierter Gewinnfondsinhalt.pdf	18	0.3 %
New Order - Sample Request.iso	17	0.3 %
confirm_Quote.html	14	0.2 %
RFQ#01942.rar	14	0.2 %
Bankovni podaci u prilogu.zip	14	0.2 %
Drawing sheet SO# M404 Cut off 328 PO611233 EMS ex Taoyuan to Miami.rar	13	0.2 %
ZD_395_2023_pdf .img	13	0.2 %
RFQ#57325.rar	12	0.2 %
RFQ 100-519639_pdf .img	12	0.2 %
Quotations_DECQ00276531_OFI_127239_Aerotact_VN_Co_Ltd.2023.html	11	0.2 %
RFQ.7889375.rar	10	0.2 %
OPTIMUM INSURANCE MAY PO567887.rar	9	0.2 %
Others	326	5.6 %
Total	**5.86k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


Exploit-GBT!34412C22E9B7
Exploit-GBT!E85AF0EEF74C
HTML/Phishing.ox
HTML/Phishing.qw
Exploit-GBT!60C680432CAA
Exploit-GBT!0946D7E1C244
BackDoor-FBHS!D9A0F65AD26B
HTML/Phishing.ce
Fareit.gen.e
Exploit-GBT!213AFDC014D1
Exploit-GDJ!76A8E87598F2
HTML/Phishing.qr
PWS-FDQG!F601AEFFF386
Exploit-GBT!70548101B6F4
HTML/Phishing.rb
HTML/Phishing.rk
HTML/Phishing.qs
Unknown
VBS/Downloader.acb
High Risk
Malicious
Not Available
Total
11.08k
Hits
Medium Risk

Report

Scan Result	Hits	%
Not Available	**5.10k**	**46.0 %**
File_Zip-Archive	4.94k	44.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	158	1.4 %
Medium Risk	**2.79k**	**25.2 %**
File_JavaScript	1.59k	14.4 %
File_Office-Open-XML-Package-Relations-Item	772	7.0 %
File_Microsoft-Windows-Executable	202	1.8 %
File_PDF	74	0.7 %
File_GIF-Image	64	0.6 %
File_JPEG-Image	55	0.5 %
File_Rar-Archive	23	0.2 %
File_Zip-Archive	6	0.1 %
File_HTML	5	0.0 %
Malicious	**2.72k**	**24.6 %**
File_JavaScript	2.44k	22.0 %
File_Microsoft-Office-Open-XML-Document	72	0.6 %
File_Rar-Archive	53	0.5 %
File_Microsoft-Windows-Executable	52	0.5 %
File_PDF	24	0.2 %
File_ISO-9660-Disk-Image	22	0.2 %
File_Generic-OLE-Package	19	0.2 %
File_Zip-Archive	16	0.1 %
File_7z-Archive	16	0.1 %
File_HTML	6	0.1 %
File_XZ-Archive	4	0.0 %
File_Type-Unknown	3	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_LhArc-Archive	1	0.0 %
High Risk	**239**	**2.2 %**
File_Rar-Archive	82	0.7 %
File_Microsoft-Windows-Executable	79	0.7 %
File_ISO-9660-Disk-Image	35	0.3 %
File_Zip-Archive	23	0.2 %
File_PDF	8	0.1 %
File_Generic-OLE-Package	3	0.0 %
File_7z-Archive	3	0.0 %

Report

Scan Result	Hits	%
File_HTML	2	0.0 %
File_XZ-Archive	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Microsoft-Equation-Editor-Document	1	0.0 %
File_RTF	1	0.0 %
VBS/Downloader.acb	**86**	**0.8 %**
File_Zip-Archive	86	0.8 %
Unknown	**86**	**0.8 %**
File_Zip-Archive	86	0.8 %
HTML/Phishing.qs	**14**	**0.1 %**
File_Type-Unknown	14	0.1 %
HTML/Phishing.rk	**14**	**0.1 %**
File_JavaScript	14	0.1 %
HTML/Phishing.rb	**7**	**0.1 %**
File_HTML	5	0.0 %
File_Type-Unknown	2	0.0 %
Exploit-GBT!70548101B6F4	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
PWS-FDQG!F601AEFFF386	**2**	**0.0 %**
File_Rar-Archive	2	0.0 %
HTML/Phishing.qr	**2**	**0.0 %**
File_HTML	2	0.0 %
Exploit-GDJ!76A8E87598F2	**2**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
Exploit-GBT!213AFDC014D1	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Fareit.gen.e	**1**	**0.0 %**
File_ACE-Archive	1	0.0 %
HTML/Phishing.ce	**1**	**0.0 %**
File_HTML	1	0.0 %
BackDoor-FBHS!D9A0F65AD26B	**1**	**0.0 %**
File_Microsoft-Windows-Executable	1	0.0 %
Exploit-GBT!0946D7E1C244	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!60C680432CAA	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %

Report

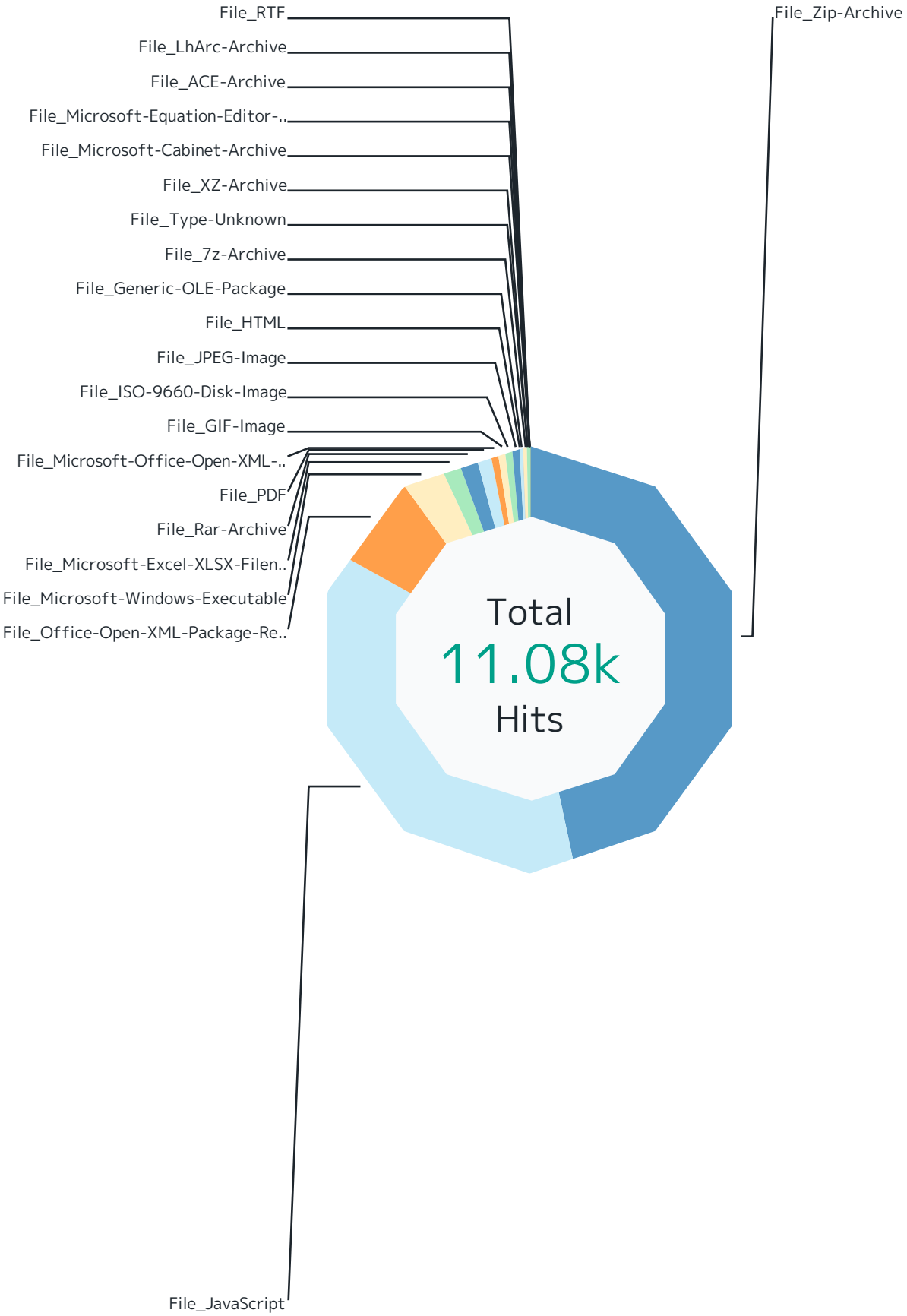
Scan Result	Hits	%
HTML/Phishing.qw	**1**	**0.0 %**
File_HTML	1	0.0 %
HTML/Phishing.ox	**1**	**0.0 %**
File_HTML	1	0.0 %
Exploit-GBT!E85AF0EEF74C	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!34412C22E9B7	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Total	**11.08k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_RTF
File_LhArc-Archive
File_ACE-Archive
File_Microsoft-Equation-Editor-..
File_Microsoft-Cabinet-Archive
File_XZ-Archive
File_Type-Unknown
File_7z-Archive
File_Generic-OLE-Package
File_HTML
File_JPEG-Image
File_ISO-9660-Disk-Image
File_GIF-Image
File_Microsoft-Office-Open-XML-..
File_PDF
File_Rar-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Windows-Executable
File_Office-Open-XML-Package-Re..
File_JavaScript
File_Zip-Archive
Total
11.08k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**5.15k**	**46.5 %**
Not Available	4.94k	44.6 %
VBS/Downloader.acb	86	0.8 %
Unknown	86	0.8 %
High Risk	23	0.2 %
Malicious	16	0.1 %
Medium Risk	6	0.1 %
File_JavaScript	**4.04k**	**36.5 %**
Malicious	2.44k	22.0 %
Medium Risk	1.59k	14.4 %
HTML/Phishing.rk	14	0.1 %
File_Office-Open-XML-Package-Relations-Item	**772**	**7.0 %**
Medium Risk	772	7.0 %
File_Microsoft-Windows-Executable	**334**	**3.0 %**
Medium Risk	202	1.8 %
High Risk	79	0.7 %
Malicious	52	0.5 %
BackDoor-FBHS!D9A0F65AD26B	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**168**	**1.5 %**
Not Available	158	1.4 %
Exploit-GBT!70548101B6F4	3	0.0 %
Exploit-GDJ!76A8E87598F2	2	0.0 %
Exploit-GBT!213AFDC014D1	1	0.0 %
Exploit-GBT!0946D7E1C244	1	0.0 %
Exploit-GBT!60C680432CAA	1	0.0 %
Exploit-GBT!E85AF0EEF74C	1	0.0 %
Exploit-GBT!34412C22E9B7	1	0.0 %
File_Rar-Archive	**160**	**1.4 %**
High Risk	82	0.7 %
Malicious	53	0.5 %
Medium Risk	23	0.2 %
PWS-FDQG!F601AEFFF386	2	0.0 %
File_PDF	**106**	**1.0 %**
Medium Risk	74	0.7 %
Malicious	24	0.2 %
High Risk	8	0.1 %

Report

Responding Scanner	Hits	%
File_Microsoft-Office-Open-XML-Document	**72**	**0.6 %**
Malicious	72	0.6 %
File_GIF-Image	**64**	**0.6 %**
Medium Risk	64	0.6 %
File_ISO-9660-Disk-Image	**57**	**0.5 %**
High Risk	35	0.3 %
Malicious	22	0.2 %
File_JPEG-Image	**55**	**0.5 %**
Medium Risk	55	0.5 %
File_HTML	**23**	**0.2 %**
Malicious	6	0.1 %
Medium Risk	5	0.0 %
HTML/Phishing.rb	5	0.0 %
High Risk	2	0.0 %
HTML/Phishing.qr	2	0.0 %
HTML/Phishing.ce	1	0.0 %
HTML/Phishing.qw	1	0.0 %
HTML/Phishing.ox	1	0.0 %
File_Generic-OLE-Package	**22**	**0.2 %**
Malicious	19	0.2 %
High Risk	3	0.0 %
File_7z-Archive	**19**	**0.2 %**
Malicious	16	0.1 %
High Risk	3	0.0 %
File_Type-Unknown	**19**	**0.2 %**
HTML/Phishing.qs	14	0.1 %
Malicious	3	0.0 %
HTML/Phishing.rb	2	0.0 %
File_XZ-Archive	**5**	**0.0 %**
Malicious	4	0.0 %
High Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	**2**	**0.0 %**
Malicious	1	0.0 %
High Risk	1	0.0 %
File_Microsoft-Equation-Editor-Document	**1**	**0.0 %**
High Risk	1	0.0 %

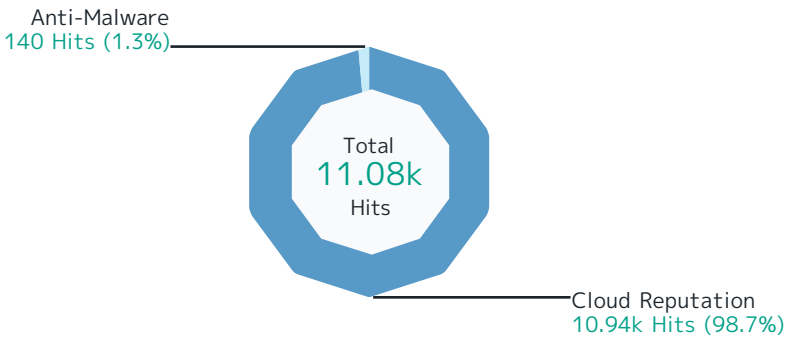
Report

Responding Scanner	Hits	%
File_ACE-Archive	**1**	**0.0 %**
Fareit.gen.e	1	0.0 %
File_LhArc-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_RTF	**1**	**0.0 %**
High Risk	1	0.0 %
Total	**11.08k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.

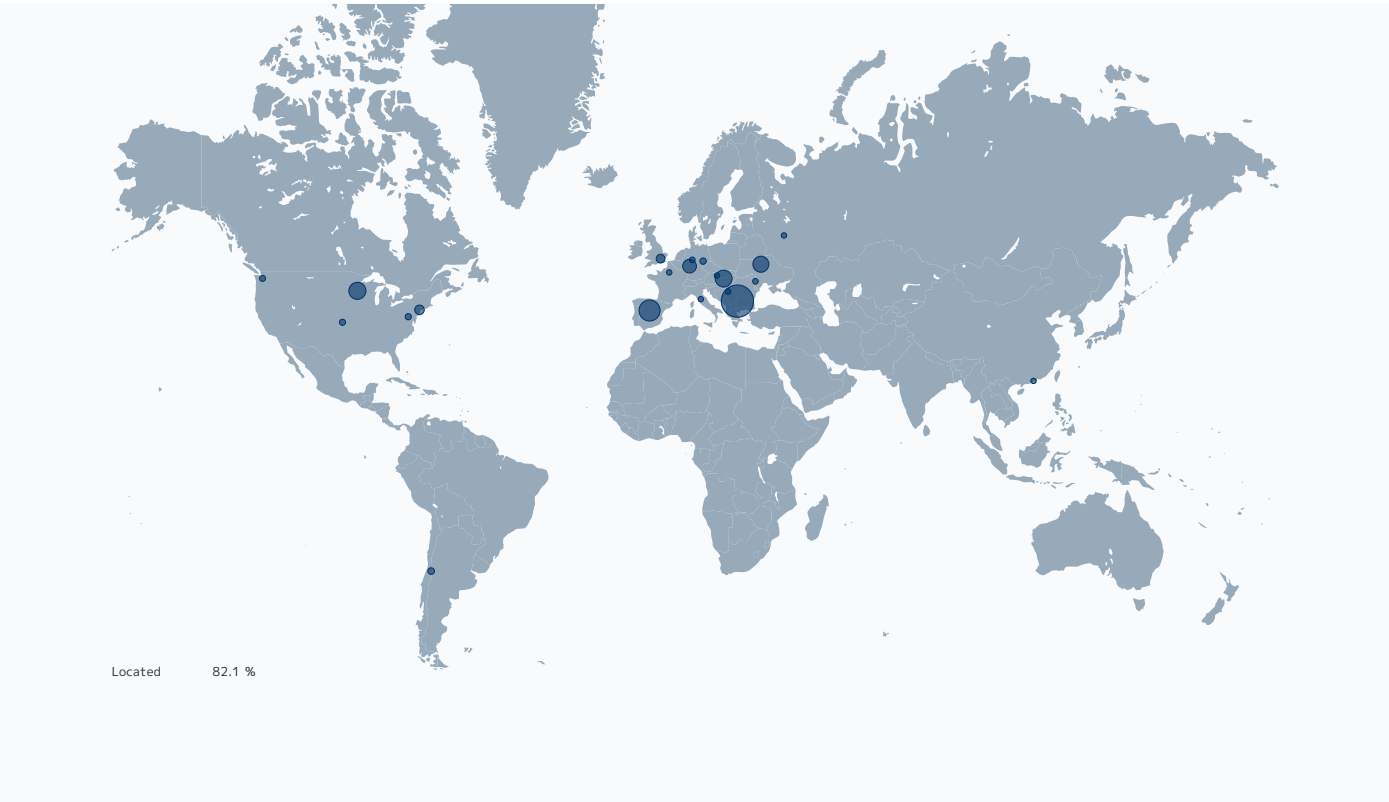


Report

Responding Scanner	Hits	%
Cloud Reputation	**10.94k**	**98.7 %**
File_Zip-Archive	5.07k	45.8 %
File_JavaScript	4.03k	36.4 %
File_Office-Open-XML-Package-Relations-Item	772	7.0 %
File_Microsoft-Windows-Executable	333	3.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	158	1.4 %
File_Rar-Archive	158	1.4 %
File_PDF	106	1.0 %
File_Microsoft-Office-Open-XML-Document	72	0.6 %
File_GIF-Image	64	0.6 %
File_ISO-9660-Disk-Image	57	0.5 %
File_JPEG-Image	55	0.5 %
File_Generic-OLE-Package	22	0.2 %
File_7z-Archive	19	0.2 %
File_HTML	13	0.1 %
File_XZ-Archive	5	0.0 %
File_Type-Unknown	3	0.0 %
File_Microsoft-Cabinet-Archive	2	0.0 %
File_Microsoft-Equation-Editor-Document	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_RTF	1	0.0 %
Anti-Malware	**140**	**1.3 %**
File_Zip-Archive	86	0.8 %
File_Type-Unknown	16	0.1 %
File_JavaScript	14	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.1 %
File_HTML	10	0.1 %
File_Rar-Archive	2	0.0 %
File_Microsoft-Windows-Executable	1	0.0 %
File_ACE-Archive	1	0.0 %
Total	**11.08k**	**100 %**

Report

Virenfilterung SRC IPs



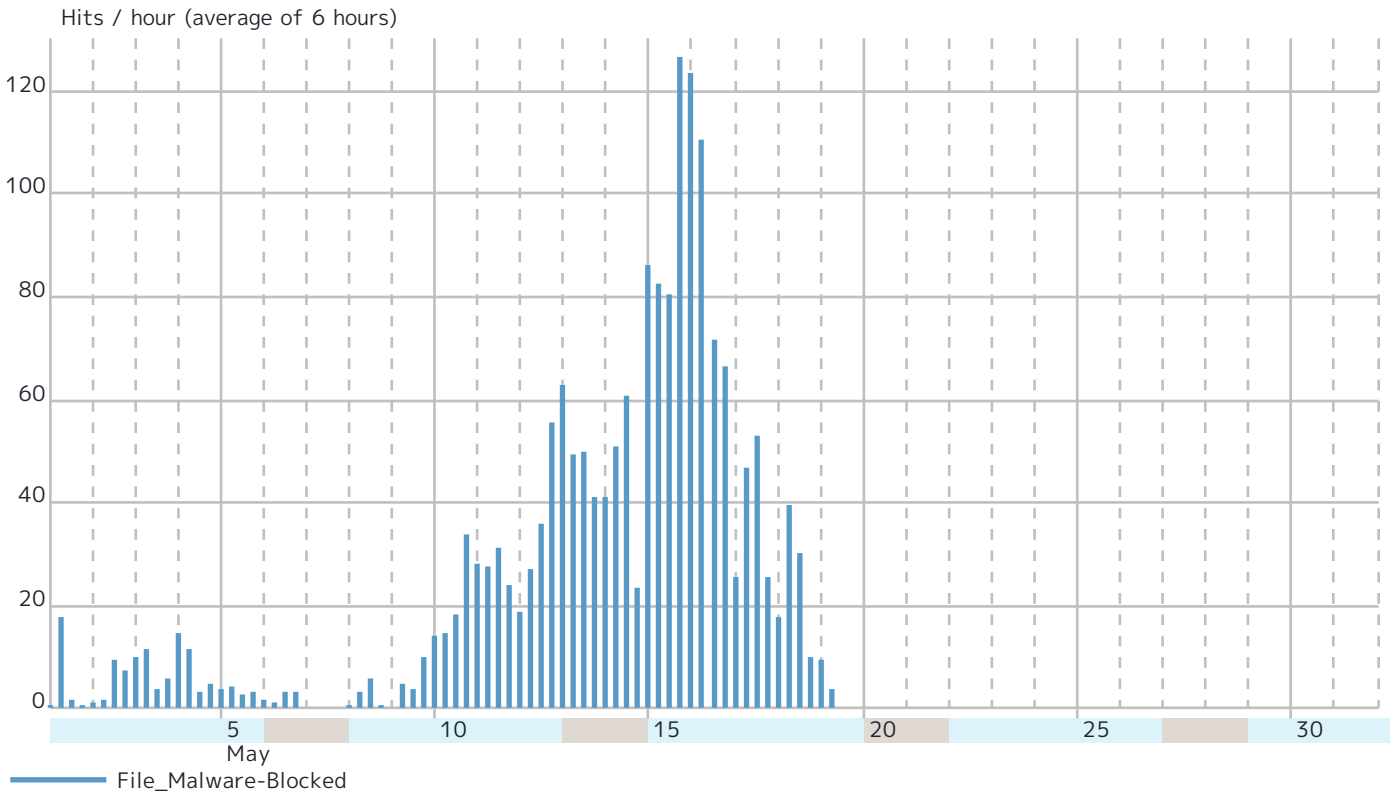
Report

Records by src IP		Hits	%
89.44.197.19	Sofia, Bulgaria	1.29k	11.6 %
89.44.197.39	Sofia, Bulgaria	1.15k	10.4 %
5.181.77.4	Budapest, Hungary	1.05k	9.5 %
95.85.72.135	Kyiv, Ukraine	974	8.8 %
5.189.222.191	Madrid, Spain	772	7.0 %
185.14.45.21	Frankfurt am Main, Germany	768	6.9 %
5.189.222.190	Madrid, Spain	656	5.9 %
92.223.102.26	Minneapolis, Minnesota 55415, United States	608	5.5 %
174.138.179.167	New Jersey, United States	388	3.5 %
5.181.27.103	Brent, United Kingdom	318	2.9 %
92.223.102.24	Minneapolis, Minnesota 55415, United States	318	2.9 %
92.223.102.27	Minneapolis, Minnesota 55415, United States	146	1.3 %
164.77.142.243	Providencia, Chile	122	1.1 %
93.240.132.20	Rochlitz, Germany	100	0.9 %
185.252.179.23	Ashburn, Virginia 20104, United States	86	0.8 %
209.160.40.54	Seattle, Washington 98160, United States	68	0.6 %
185.118.171.19	Serbia	44	0.4 %
45.142.214.2	Chisinau, Moldova	36	0.3 %
104.168.163.59	United States	26	0.2 %
198.44.97.81	United States	26	0.2 %
192.162.87.183	Germany	24	0.2 %
89.22.108.133	Germany	20	0.2 %
185.231.205.150	Paris, France	17	0.2 %
209.85.208.54	United States	14	0.1 %
5.252.23.74	Bratislava, Slovakia	13	0.1 %
211.154.133.141	Hong Kong	13	0.1 %
185.4.142.31	Italy	12	0.1 %
94.228.200.142	Moscow, Russia	12	0.1 %
185.145.97.143	United States	12	0.1 %
77.91.100.226	Sofia, Bulgaria	12	0.1 %
Others		1.98k	17.9 %
Total		**11.08k**	**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.