

Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-10-01 00:00:00 CEST

To: 2022-11-01 00:00:00 CET

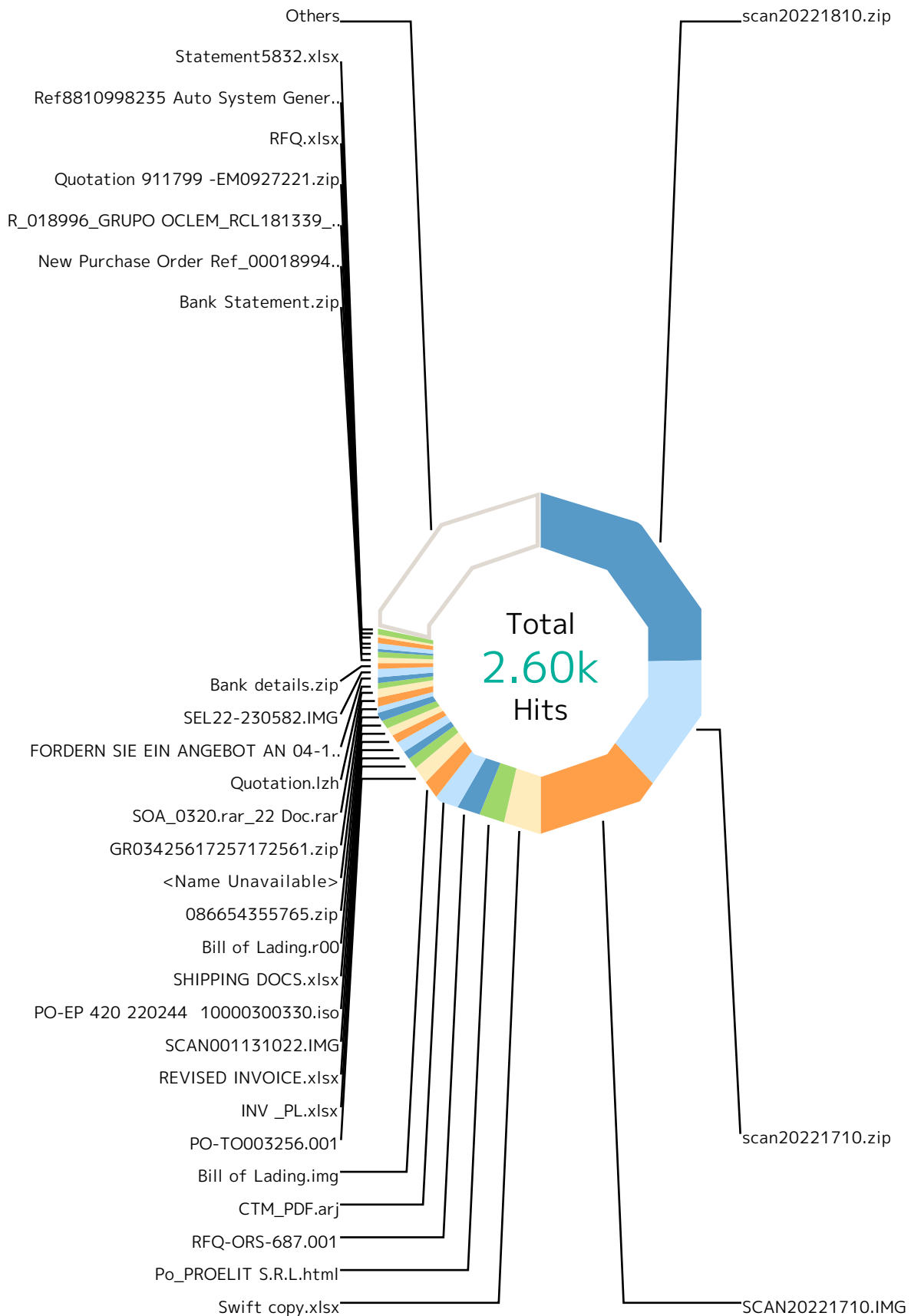
Report

Table of Contents

Report run by jens	Virenfilterung MXe	3
SMC version 6.11.2, build 11221	Top File Types by Scan Result	5
Update version 1522	Top Scan Results by Responding Scanner	10
Report started 2022-11-03 12:08:09 CET	Top File Types by Responding Scanner	15
Report run time 02:38:36	Virenfilterung SRC IPs	17
Filters used Match All	SMTP Virus Filtering by Time	19

Report

Virenterung MXe



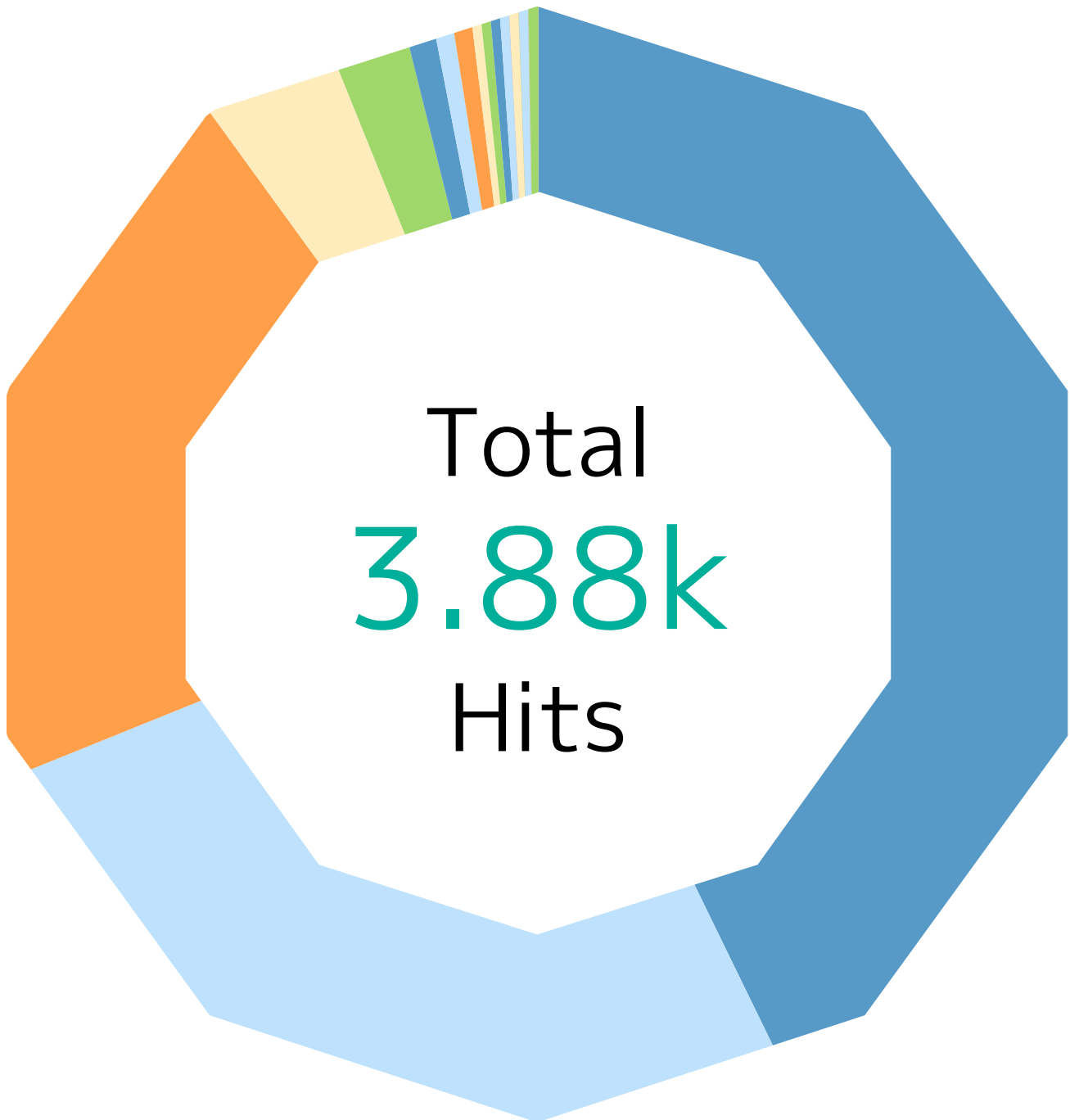
Report

Records by file name	Hits	%
scan20221810.zip	645	24.8 %
scan20221710.zip	345	13.3 %
SCAN20221710.IMG	310	11.9 %
Swift copy.xlsx	95	3.7 %
Po_PROELIT S.R.L.html	63	2.4 %
RFQ-ORS-687.001	62	2.4 %
CTM_PDF.arj	53	2.0 %
Bill of Lading.img	45	1.7 %
PO-TO003256.001	42	1.6 %
INV _PL.xlsx	31	1.2 %
REVISED INVOICE.xlsx	24	0.9 %
SCAN001131022.IMG	23	0.9 %
PO-EP 420 220244 10000300330.iso	22	0.8 %
SHIPPING DOCS.xlsx	22	0.8 %
Bill of Lading.r00	21	0.8 %
086654355765.zip	21	0.8 %
<Name Unavailable>	20	0.8 %
GR03425617257172561.zip	20	0.8 %
SOA_0320.rar_22 Doc.rar	19	0.7 %
Quotation.lzh	17	0.7 %
FORDERN SIE EIN ANGEBOT AN 04-10-2022.xlsx	17	0.7 %
SEL22-230582.IMG	16	0.6 %
Bank details.zip	15	0.6 %
Bank Statement.zip	14	0.5 %
New Purchase Order Ref_00018994224.zip	14	0.5 %
R_018996_GRUPO OCLEM_RCL181339_SEPTEMBER_2022.rar	13	0.5 %
Quotation 911799 -EM0927221.zip	13	0.5 %
RFQ.xlsx	12	0.5 %
Ref8810998235 Auto System Generated Order Form 051022.pdf.z	11	0.4 %
Statement5832.xlsx	11	0.4 %
Others	564	21.7 %
Total	2.60k	100 %

Report

Top File Types by Scan Result

Top 10 file types by scan result.



Report

Scan Result	Hits	%
Malicious	1.66k	42.7 %
File_Microsoft-Windows-Compiled-Help	812	20.9 %
File_ISO-9660-Disk-Image	351	9.0 %
File_Microsoft-Windows-Executable	159	4.1 %
File_Rar-Archive	144	3.7 %
File_Zip-Archive	107	2.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	29	0.7 %
File_Microsoft-Cabinet-Archive	16	0.4 %
File_Type-Unknown	9	0.2 %
File_LhArc-Archive	6	0.2 %
File_7z-Archive	6	0.2 %
File_PDF	5	0.1 %
File_JavaScript	4	0.1 %
File_Encrypted-Rar-Archive	3	0.1 %
File_HTML	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
File_Tar-Archive	1	0.0 %
File_XZ-Archive	1	0.0 %
Not Available	1.01k	26.1 %
File_Zip-Archive	997	25.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	16	0.4 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
High Risk	818	21.1 %
File_Rar-Archive	164	4.2 %
File_Microsoft-Windows-Compiled-Help	158	4.1 %
File_ISO-9660-Disk-Image	134	3.5 %
File_Zip-Archive	131	3.4 %
File_Microsoft-Windows-Executable	73	1.9 %
File_Type-Unknown	71	1.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	34	0.9 %
File_HTML	22	0.6 %
File_Microsoft-Cabinet-Archive	14	0.4 %
File_LhArc-Archive	5	0.1 %
File_Encrypted-Rar-Archive	4	0.1 %
File_PDF	2	0.1 %
File_Microsoft-Excel-97-Spreadsheet	2	0.1 %

Report

Scan Result	Hits	%
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_7z-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %
Medium Risk	151	3.9 %
File_Rar-Archive	38	1.0 %
File_Microsoft-Windows-Compiled-Help	20	0.5 %
File_XML	16	0.4 %
File_Java-Class	15	0.4 %
File_Microsoft-Windows-Executable	13	0.3 %
File_Zip-Archive	10	0.3 %
File_PDF	10	0.3 %
File_JavaScript	9	0.2 %
File_HTML	8	0.2 %
File_ISO-9660-Disk-Image	5	0.1 %
File_Type-Unknown	5	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_7z-Archive	1	0.0 %
Exploit-GBT!C3D769A32BFF	95	2.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	95	2.4 %
Exploit-GBT!4F39A12876D5	31	0.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	31	0.8 %
Unknown	22	0.6 %
File_Zip-Archive	22	0.6 %
Exploit-GBW!90FAE257C7DE	17	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	17	0.4 %
HTML/Phishing.ce	13	0.3 %
File_HTML	13	0.3 %
Exploit-GBT!9891CA91A818	12	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	12	0.3 %
Fareit.gen.e	10	0.3 %
File_ACE-Archive	10	0.3 %
Exploit-GBT!0837827B6480	8	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.2 %
Exploit-GBT!DC089CB17D24	5	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.1 %
GenericRXSX-EU!7AA54A589541	5	0.1 %

Report

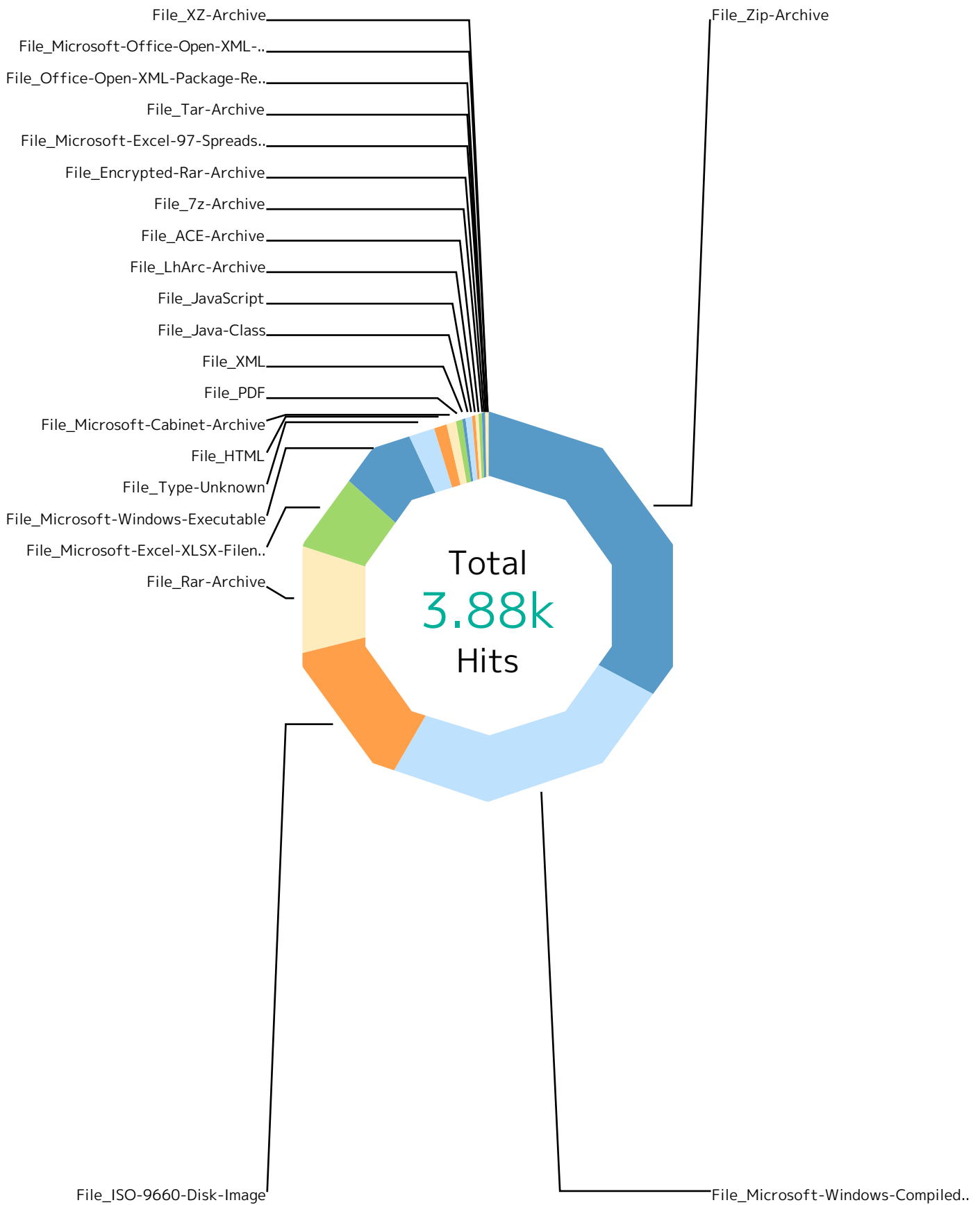
Scan Result	Hits	%
File_ISO-9660-Disk-Image	5	0.1 %
Exploit-GBT!B5AD313AF09E	4	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
Exploit-GBT!9035BFAC537C	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
Exploit-GBT!7A5BFB6B4B69	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
Fareit-FZT!8396E6F6CD0B	2	0.1 %
File_Microsoft-Windows-Executable	2	0.1 %
Exploit-GBT!1F8CAA0D577D	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
GenericRXTZ-AS!AA0658F07E09	1	0.0 %
File_Rar-Archive	1	0.0 %
GenericRXTZ-AS!A142794D45A7	1	0.0 %
File_Zip-Archive	1	0.0 %
W32/Mydoom.p.bf@MM!zip	1	0.0 %
File_Zip-Archive	1	0.0 %
Exploit-GBT!AD2B9241A87B	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
PWS-FCB!C610F2FCB87E	1	0.0 %
File_Zip-Archive	1	0.0 %
Exploit-GBT!78C6A096FD49	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
HTML/Phishing.ok	1	0.0 %
File_HTML	1	0.0 %
GenericRXRU-WN!1B80C9CA51B9	1	0.0 %
File_Zip-Archive	1	0.0 %
GenericRXTZ-AS!070AE05ACA4B	1	0.0 %
File_Rar-Archive	1	0.0 %
GenericRXQA-LQ!86582712C181	1	0.0 %
File_Zip-Archive	1	0.0 %
Exploit-GBT!9FAE059B4575	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Total	3.88k	100 %

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report



Report

Responding Scanner	Hits	%
File_Zip-Archive	1.27k	32.8 %
Not Available	997	25.7 %
High Risk	131	3.4 %
Malicious	107	2.8 %
Unknown	22	0.6 %
Medium Risk	10	0.3 %
GenericRXTZ-AS!A142794D45A7	1	0.0 %
W32/Mydoom.p.bf@MM!zip	1	0.0 %
PWS-FCTB!C610F2FCB87E	1	0.0 %
GenericRXRU-WN!1B80C9CA51B9	1	0.0 %
GenericRXQA-LQ!86582712C181	1	0.0 %
File_Microsoft-Windows-Compiled-Help	990	25.5 %
Malicious	812	20.9 %
High Risk	158	4.1 %
Medium Risk	20	0.5 %
File_ISO-9660-Disk-Image	495	12.8 %
Malicious	351	9.0 %
High Risk	134	3.5 %
Medium Risk	5	0.1 %
GenericRXSX-EU!7AA54A589541	5	0.1 %
File_Rar-Archive	348	9.0 %
High Risk	164	4.2 %
Malicious	144	3.7 %
Medium Risk	38	1.0 %
GenericRXTZ-AS!AA0658F07E09	1	0.0 %
GenericRXTZ-AS!070AE05ACA4B	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	260	6.7 %
Exploit-GBT!C3D769A32BFF	95	2.4 %
High Risk	34	0.9 %
Exploit-GBT!4F39A12876D5	31	0.8 %
Malicious	29	0.7 %
Exploit-GBW!90FAE257C7DE	17	0.4 %
Not Available	16	0.4 %
Exploit-GBT!9891CA91A818	12	0.3 %
Exploit-GBT!0837827B6480	8	0.2 %
Exploit-GBT!DC089CB17D24	5	0.1 %

Report

Responding Scanner	Hits	%
Exploit-GBT!B5AD313AF09E	4	0.1 %
Exploit-GBT!9035BFAC537C	2	0.1 %
Exploit-GBT!7A5BFB6B4B69	2	0.1 %
Exploit-GBT!1F8CAA0D577D	2	0.1 %
Exploit-GBT!AD2B9241A87B	1	0.0 %
Exploit-GBT!78C6A096FD49	1	0.0 %
Exploit-GBT!9FAE059B4575	1	0.0 %
File_Microsoft-Windows-Executable	247	6.4 %
Malicious	159	4.1 %
High Risk	73	1.9 %
Medium Risk	13	0.3 %
Fareit-FZT!8396E6F6CD0B	2	0.1 %
File_Type-Unknown	85	2.2 %
High Risk	71	1.8 %
Malicious	9	0.2 %
Medium Risk	5	0.1 %
File_HTML	45	1.2 %
High Risk	22	0.6 %
HTML/Phishing.ce	13	0.3 %
Medium Risk	8	0.2 %
Malicious	1	0.0 %
HTML/Phishing.ok	1	0.0 %
File_Microsoft-Cabinet-Archive	31	0.8 %
Malicious	16	0.4 %
High Risk	14	0.4 %
Medium Risk	1	0.0 %
File_PDF	17	0.4 %
Medium Risk	10	0.3 %
Malicious	5	0.1 %
High Risk	2	0.1 %
File_XML	16	0.4 %
Medium Risk	16	0.4 %
File_Java-Class	15	0.4 %
Medium Risk	15	0.4 %
File_JavaScript	13	0.3 %
Medium Risk	9	0.2 %

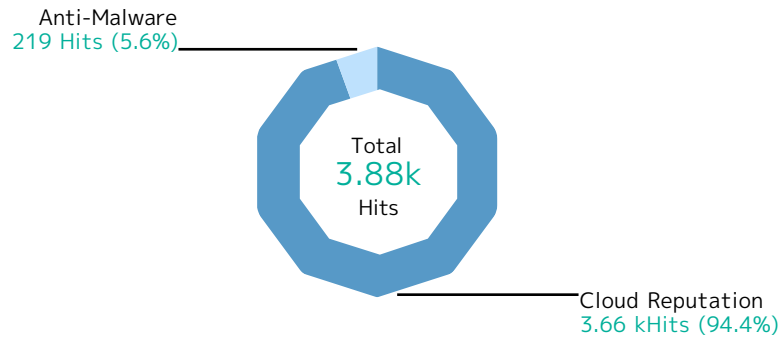
Report

Responding Scanner	Hits	%
Malicious	4	0.1 %
File_LhArc-Archive	11	0.3 %
Malicious	6	0.2 %
High Risk	5	0.1 %
File_ACE-Archive	10	0.3 %
Fareit.gen.e	10	0.3 %
File_7z-Archive	8	0.2 %
Malicious	6	0.2 %
High Risk	1	0.0 %
Medium Risk	1	0.0 %
File_Encrypted-Rar-Archive	7	0.2 %
High Risk	4	0.1 %
Malicious	3	0.1 %
File_Microsoft-Excel-97-Spreadsheet	3	0.1 %
High Risk	2	0.1 %
Malicious	1	0.0 %
File_Tar-Archive	2	0.1 %
Malicious	1	0.0 %
High Risk	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
High Risk	2	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
Not Available	1	0.0 %
File_XZ-Archive	1	0.0 %
Malicious	1	0.0 %
Total	3.88k	100 %

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	3.66k	94.4 %
File_Zip-Archive	1.27k	32.7 %
File_Microsoft-Windows-Compiled-Help	990	25.5 %
File_ISO-9660-Disk-Image	490	12.6 %
File_Rar-Archive	346	8.9 %
File_Microsoft-Windows-Executable	245	6.3 %
File_Type-Unknown	85	2.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	79	2.0 %
File_HTML	31	0.8 %
File_Microsoft-Cabinet-Archive	31	0.8 %
File_PDF	17	0.4 %
File_XML	16	0.4 %
File_Java-Class	15	0.4 %
File_JavaScript	13	0.3 %
File_LhArc-Archive	11	0.3 %
File_7z-Archive	8	0.2 %
File_Encrypted-Rar-Archive	7	0.2 %
File_Microsoft-Excel-97-Spreadsheet	3	0.1 %
File_Tar-Archive	2	0.1 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
File_XZ-Archive	1	0.0 %
Anti-Malware	219	5.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	181	4.7 %
File_HTML	14	0.4 %
File_ACE-Archive	10	0.3 %
File_Zip-Archive	5	0.1 %
File_ISO-9660-Disk-Image	5	0.1 %
File_Rar-Archive	2	0.1 %
File_Microsoft-Windows-Executable	2	0.1 %
Total	3.88k	100 %

Report

Virenfiterung SRC IPs



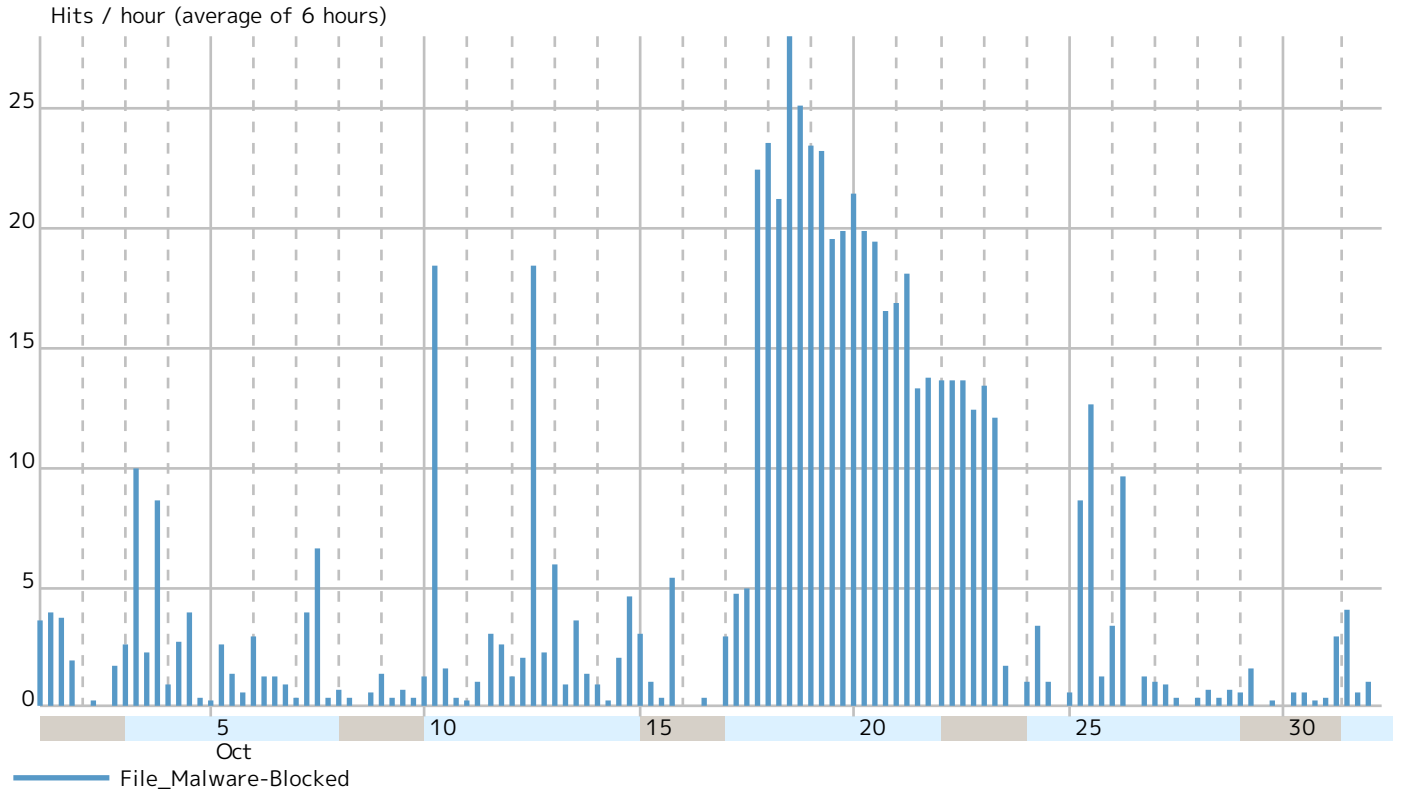
Report

Records by src IP		Hits	%
62.149.244.169	 Arezzo, Italy	2.29k	59.0 %
81.161.229.136	 Ashburn, Virginia 20147, United States	111	2.9 %
195.242.111.250	 Belize	104	2.7 %
195.178.120.206	 Reston, Virginia 20190, United States	66	1.7 %
123.56.88.208	 Beijing, China	63	1.6 %
80.86.231.190	 Abovyan, Armenia	52	1.3 %
171.22.30.180	 Ashburn, Virginia 20103, United States	52	1.3 %
213.142.151.150	 Turkey	50	1.3 %
77.235.61.81	 Cyprus	40	1.0 %
185.28.39.16	 Netherlands	31	0.8 %
103.117.180.241	 India	30	0.8 %
5.252.22.69	 Frankfurt am Main, Germany	30	0.8 %
103.74.100.229	 Vietnam	28	0.7 %
49.229.55.140	 Phitsanulok, Thailand	28	0.7 %
94.237.74.142	 Singapore	26	0.7 %
185.222.57.226	 Amsterdam, Netherlands	24	0.6 %
152.89.247.136	 Frankfurt am Main, Germany	22	0.6 %
185.222.57.228	 Amsterdam, Netherlands	22	0.6 %
78.135.111.89	 Turkey	21	0.5 %
45.139.105.30	 Bulgaria	20	0.5 %
107.174.202.140	 United States	19	0.5 %
85.217.145.102	 Reston, Virginia 20190, United States	18	0.5 %
45.85.219.222	 Germany	18	0.5 %
185.78.167.135	 Nonthaburi, Thailand	17	0.4 %
103.167.199.109	 Vietnam	17	0.4 %
77.239.64.29	 Bijeljina, Bosnia and Herzegovina	16	0.4 %
185.216.71.167	 Netherlands	16	0.4 %
217.160.168.231	 Germany	16	0.4 %
213.197.180.73	 Vilnius, Lithuania	16	0.4 %
51.159.54.49	 Paris, France	16	0.4 %
Others		600	15.5 %
Total		3.88k	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.