Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-09-01 00:00:00 CEST
To: 2022-10-01 00:00:00 CEST

Report

Report run by
jens

SMC version
6.11.1, build 11219

Update version
1509

Report started
2022-10-04 10:02:59 CEST

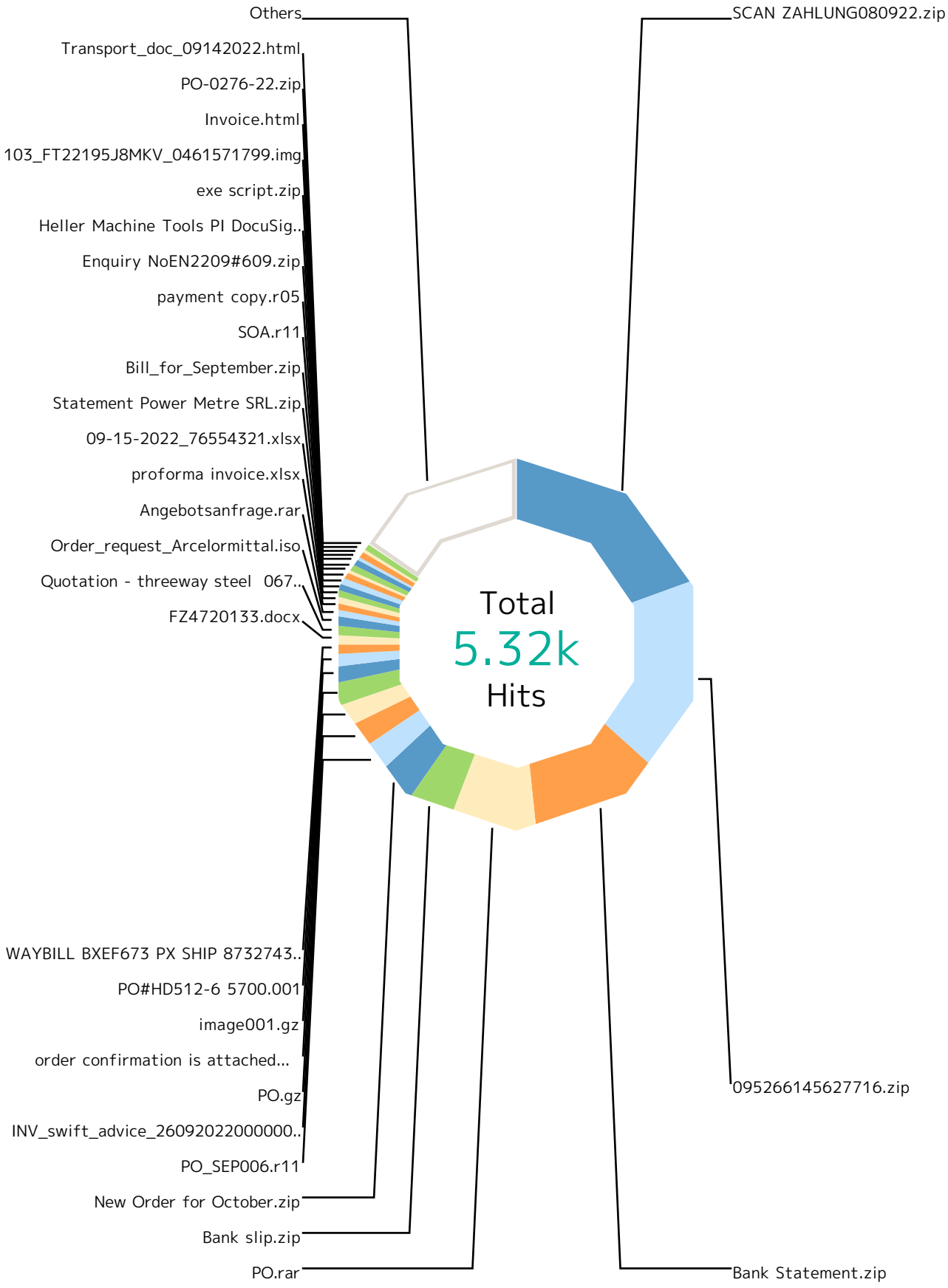
Report run time
02:31:20

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



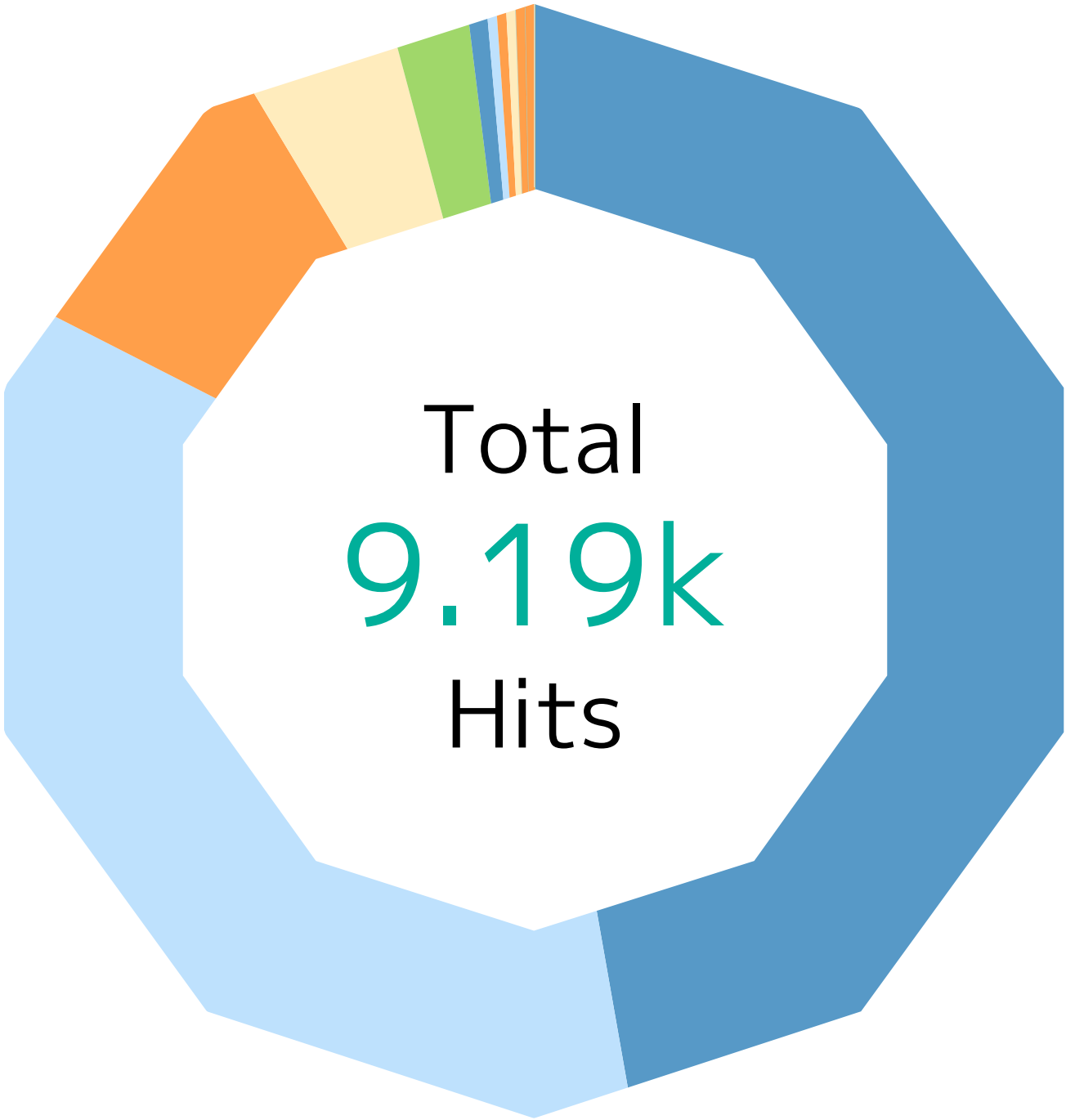
Report

Records by file name	Hits	%
SCAN ZAHLUNG080922.zip	1.03k	19.3 %
095266145627716.zip	924	17.4 %
Bank Statement.zip	622	11.7 %
PO.rar	391	7.4 %
Bank slip.zip	219	4.1 %
New Order for October.zip	167	3.1 %
PO_SEP006.r11	139	2.6 %
INV_swift_advice_26092022000000000000000.zip	113	2.1 %
PO.gz	110	2.1 %
order confirmation is attached.zip	97	1.8 %
image001.gz	82	1.5 %
PO#HD512-6 5700.001	56	1.1 %
WAYBILL BXEF673 PX SHIP 87327438239.zip	44	0.8 %
FZ4720133.docx	43	0.8 %
Quotation - threeway steel 06718.xlsx	42	0.8 %
Order_request_Arcelormittal.iso	40	0.8 %
Angebotsanfrage.rar	34	0.6 %
proforma invoice.xlsx	33	0.6 %
09-15-2022_76554321.xlsx	31	0.6 %
Statement Power Metre SRL.zip	30	0.6 %
Bill_for_September.zip	27	0.5 %
SOA.r11	27	0.5 %
payment copy.r05	26	0.5 %
Enquiry NoEN2209#609.zip	26	0.5 %
Heller Machine Tools PI DocuSign for payment..xlsx	25	0.5 %
exe script.zip	24	0.5 %
103_FT22195J8MKV_0461571799.img	23	0.4 %
Invoice.html	23	0.4 %
PO-0276-22.zip	21	0.4 %
Transport_doc_09142022.html	21	0.4 %
Others	832	15.6 %
Total	**5.32k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
9.19k
Hits

Report

Scan Result	Hits	%
Malicious	**4.35k**	**47.4 %**
File_Microsoft-Windows-Executable	3.10k	33.7 %
File_Rar-Archive	479	5.2 %
File_JavaScript	373	4.1 %
File_Zip-Archive	191	2.1 %
File_ISO-9660-Disk-Image	82	0.9 %
File_Office-Open-XML-Package-Relations-Item	45	0.5 %
File_Microsoft-Equation-Editor-Document	23	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.1 %
File_7z-Archive	9	0.1 %
File_Microsoft-Cabinet-Archive	9	0.1 %
File_LhArc-Archive	8	0.1 %
File_Microsoft-PowerPoint-97-Add-In	7	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_Microsoft-Office-Open-XML-Document	4	0.0 %
File_Type-Unknown	3	0.0 %
File_ACE-Archive	3	0.0 %
File_PDF	1	0.0 %
File_Tar-Archive	1	0.0 %
File_Microsoft-MS-DOS-Executable	1	0.0 %
File_Java-Class	1	0.0 %
Not Available	**3.23k**	**35.2 %**
File_Zip-Archive	3.16k	34.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	62	0.7 %
File_Microsoft-Office-Open-XML-Document	6	0.1 %
High Risk	**824**	**9.0 %**
File_Rar-Archive	370	4.0 %
File_Microsoft-Windows-Executable	226	2.5 %
File_ISO-9660-Disk-Image	78	0.8 %
File_Zip-Archive	53	0.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	44	0.5 %
File_Office-Open-XML-Package-Relations-Item	17	0.2 %
File_PDF	12	0.1 %
File_7z-Archive	6	0.1 %
File_Microsoft-Cabinet-Archive	5	0.1 %
File_Type-Unknown	4	0.0 %

Report

Scan Result	Hits	%
File_LhArc-Archive	3	0.0 %
File_RTF	3	0.0 %
File_HTML	1	0.0 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
File_ACE-Archive	1	0.0 %
Unknown	**402**	**4.4 %**
File_Zip-Archive	402	4.4 %
Medium Risk	**209**	**2.3 %**
File_Rar-Archive	53	0.6 %
File_Microsoft-Windows-Executable	51	0.6 %
File_XML	44	0.5 %
File_Zip-Archive	41	0.4 %
File_JavaScript	12	0.1 %
File_Microsoft-Office-Open-XML-Document	3	0.0 %
File_ISO-9660-Disk-Image	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
File_7z-Archive	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	1	0.0 %
HTML/Phishing.ce	**35**	**0.4 %**
File_HTML	35	0.4 %
Exploit-GBT!CC05FE0508A9	**28**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	28	0.3 %
Exploit-GBT!D7D67BC71481	**25**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	25	0.3 %
HTML/Phishing.jt	**23**	**0.3 %**
File_HTML	23	0.3 %
Exploit-GBT!4A7345D1404C	**8**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.1 %
Fareit-FDBI!F7BE6AB1521E	**8**	**0.1 %**
File_Rar-Archive	8	0.1 %
Exploit-GBT!0A7E0D291E85	**4**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.0 %
Exploit-GBT!7143FA304594	**4**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.0 %
Adwind-FDYD.jar!B80DE29430ED	**4**	**0.0 %**
File_ISO-9660-Disk-Image	4	0.0 %

Report

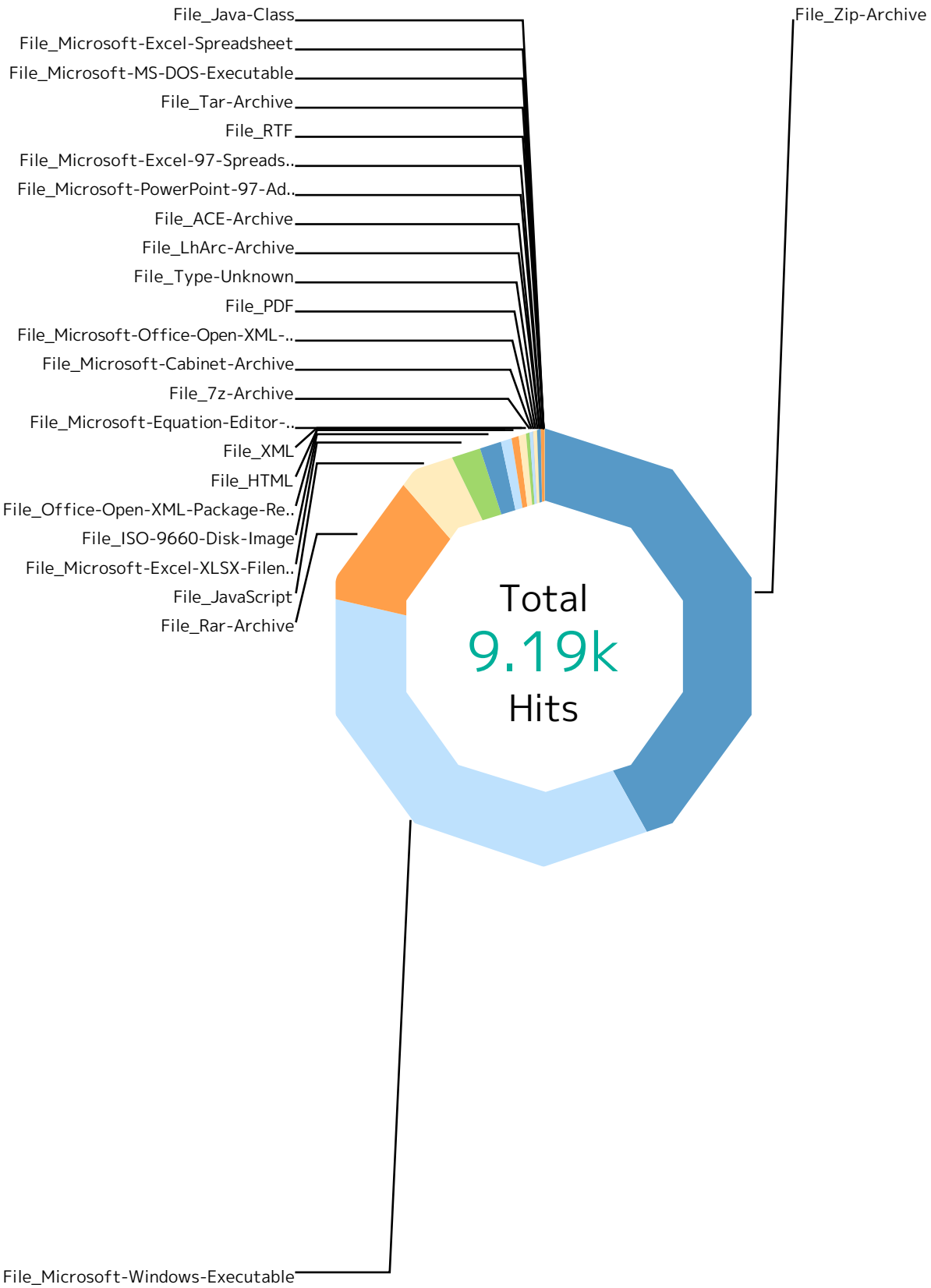
Scan Result	Hits	%
Exploit-GBS!7BAAC6F5DCFD	**4**	**0.0 %**
File_Type-Unknown	4	0.0 %
Fareit.gen.e	**4**	**0.0 %**
File_ACE-Archive	4	0.0 %
Exploit-GBT!7AEB9965C5AF	**4**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.0 %
Fareit-FDBI!D3BD37EC6A82	**3**	**0.0 %**
File_Zip-Archive	3	0.0 %
Exploit-GBT!9F041AA6DAB4	**3**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.0 %
Exploit-GBT!9349158354E7	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
GenericRXTR-DI!C4072867BCEC	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
Exploit-GBT!B70E42F39A1B	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!49018F564AA7	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
GenericRXTR-DI!3C1626EDA6B1	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
GenericRXRU-WN!E548C81C2426	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
GenericRXUB-LK!8681CEE77948	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Exploit-GBT!3443C0B3E1BD	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Adwind-FDYD.jar!ED00DA8BE942	**1**	**0.0 %**
File_ISO-9660-Disk-Image	1	0.0 %
Fareit-FDBI!62C42E22E7FD	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
HTML/Phishing.dy	**1**	**0.0 %**
File_HTML	1	0.0 %
Others	**5**	**0.1 %**
Total	**9.19k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Java-Class
File_Microsoft-Excel-Spreadsheet
File_Microsoft-MS-DOS-Executable
File_Tar-Archive
File_RTF
File_Microsoft-Excel-97-Spreads..
File_Microsoft-PowerPoint-97-Ad..
File_ACE-Archive
File_LhArc-Archive
File_Type-Unknown
File_PDF
File_Microsoft-Office-Open-XML-..
File_Microsoft-Cabinet-Archive
File_7z-Archive
File_Microsoft-Equation-Editor-..
File_XML
File_HTML
File_Office-Open-XML-Package-Re..
File_ISO-9660-Disk-Image
File_Microsoft-Excel-XLSX-Filen..
File_JavaScript
File_Rar-Archive
File_Zip-Archive
File_Microsoft-Windows-Executable
Total
9.19k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**3.86k**	**42.0 %**
Not Available	3.16k	34.4 %
Unknown	402	4.4 %
Malicious	191	2.1 %
High Risk	53	0.6 %
Medium Risk	41	0.4 %
Fareit-FDBI!D3BD37EC6A82	3	0.0 %
GenericRXTR-DI!C4072867BCEC	1	0.0 %
GenericRXTR-DI!3C1626EDA6B1	1	0.0 %
GenericRXRU-WN!E548C81C2426	1	0.0 %
Fareit-FDBI!62C42E22E7FD	1	0.0 %
File_Microsoft-Windows-Executable	**3.37k**	**36.7 %**
Malicious	3.10k	33.7 %
High Risk	226	2.5 %
Medium Risk	51	0.6 %
File_Rar-Archive	**911**	**9.9 %**
Malicious	479	5.2 %
High Risk	370	4.0 %
Medium Risk	53	0.6 %
Fareit-FDBI!F7BE6AB1521E	8	0.1 %
GenericRXUB-LK!8681CEE77948	1	0.0 %
File_JavaScript	**385**	**4.2 %**
Malicious	373	4.1 %
Medium Risk	12	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**200**	**2.2 %**
Not Available	62	0.7 %
High Risk	44	0.5 %
Exploit-GBT!CC05FE0508A9	28	0.3 %
Exploit-GBT!D7D67BC71481	25	0.3 %
Malicious	10	0.1 %
Exploit-GBT!4A7345D1404C	8	0.1 %
Exploit-GBT!0A7E0D291E85	4	0.0 %
Exploit-GBT!7143FA304594	4	0.0 %
Exploit-GBT!7AEB9965C5AF	4	0.0 %
Exploit-GBT!9F041AA6DAB4	3	0.0 %
Medium Risk	1	0.0 %

Report

Responding Scanner	Hits	%
Exploit-GBT!9349158354E7	1	0.0 %
Exploit-GBT!B70E42F39A1B	1	0.0 %
Exploit-GBT!49018F564AA7	1	0.0 %
Exploit-GBT!36DFD52164BF	1	0.0 %
Exploit-GBT!E903E1B38E97	1	0.0 %
Exploit-GBT!861D6050B820	1	0.0 %
Exploit-GBT!B7AFB57066FA	1	0.0 %
File_ISO-9660-Disk-Image	**167**	**1.8 %**
Malicious	82	0.9 %
High Risk	78	0.8 %
Adwind-FDYD.jar!B80DE29430ED	4	0.0 %
Medium Risk	2	0.0 %
Adwind-FDYD.jar!ED00DA8BE942	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**62**	**0.7 %**
Malicious	45	0.5 %
High Risk	17	0.2 %
File_HTML	**60**	**0.7 %**
HTML/Phishing.ce	35	0.4 %
HTML/Phishing.jt	23	0.3 %
High Risk	1	0.0 %
HTML/Phishing.dy	1	0.0 %
File_XML	**44**	**0.5 %**
Medium Risk	44	0.5 %
File_Microsoft-Equation-Editor-Document	**23**	**0.3 %**
Malicious	23	0.3 %
File_7z-Archive	**16**	**0.2 %**
Malicious	9	0.1 %
High Risk	6	0.1 %
Medium Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	**14**	**0.2 %**
Malicious	9	0.1 %
High Risk	5	0.1 %
File_Microsoft-Office-Open-XML-Document	**14**	**0.2 %**
Not Available	6	0.1 %
Malicious	4	0.0 %
Medium Risk	3	0.0 %

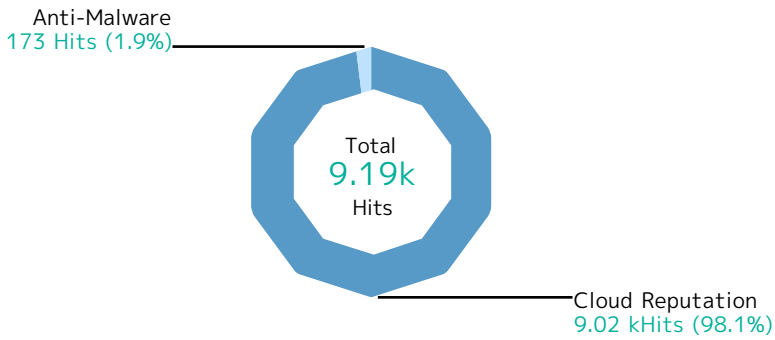
Report

Responding Scanner	Hits	%
High Risk	1	0.0 %
File_PDF	**13**	**0.1 %**
High Risk	12	0.1 %
Malicious	1	0.0 %
File_Type-Unknown	**11**	**0.1 %**
High Risk	4	0.0 %
Exploit-GBS!7BAAC6F5DCFD	4	0.0 %
Malicious	3	0.0 %
File_LhArc-Archive	**11**	**0.1 %**
Malicious	8	0.1 %
High Risk	3	0.0 %
File_ACE-Archive	**9**	**0.1 %**
Fareit.gen.e	4	0.0 %
Malicious	3	0.0 %
High Risk	1	0.0 %
Fareit.gen.a	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	**8**	**0.1 %**
Malicious	7	0.1 %
Medium Risk	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**5**	**0.1 %**
Malicious	5	0.1 %
File_RTF	**3**	**0.0 %**
High Risk	3	0.0 %
File_Tar-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_Microsoft-MS-DOS-Executable	**1**	**0.0 %**
Malicious	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.0 %**
Exploit-GBT!3443C0B3E1BD	1	0.0 %
File_Java-Class	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**9.19k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**9.02k**	**98.1 %**
File_Zip-Archive	3.85k	41.9 %
File_Microsoft-Windows-Executable	3.37k	36.7 %
File_Rar-Archive	902	9.8 %
File_JavaScript	385	4.2 %
File_ISO-9660-Disk-Image	162	1.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	117	1.3 %
File_Office-Open-XML-Package-Relations-Item	62	0.7 %
File_XML	44	0.5 %
File_Microsoft-Equation-Editor-Document	23	0.3 %
File_7z-Archive	16	0.2 %
File_Microsoft-Cabinet-Archive	14	0.2 %
File_Microsoft-Office-Open-XML-Document	14	0.2 %
File_PDF	13	0.1 %
File_LhArc-Archive	11	0.1 %
File_Microsoft-PowerPoint-97-Add-In	8	0.1 %
File_Type-Unknown	7	0.1 %
File_Microsoft-Excel-97-Spreadsheet	5	0.1 %
File_ACE-Archive	4	0.0 %
File_RTF	3	0.0 %
File_HTML	1	0.0 %
File_Tar-Archive	1	0.0 %
File_Microsoft-MS-DOS-Executable	1	0.0 %
File_Java-Class	1	0.0 %
Anti-Malware	**173**	**1.9 %**
File_Microsoft-Excel-XLSX-Filename-Extension	83	0.9 %
File_HTML	59	0.6 %
File_Rar-Archive	9	0.1 %
File_Zip-Archive	7	0.1 %
File_ISO-9660-Disk-Image	5	0.1 %
File_ACE-Archive	5	0.1 %
File_Type-Unknown	4	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Total	**9.19k**	**100 %**

Report

Virenfilterung SRC IPs

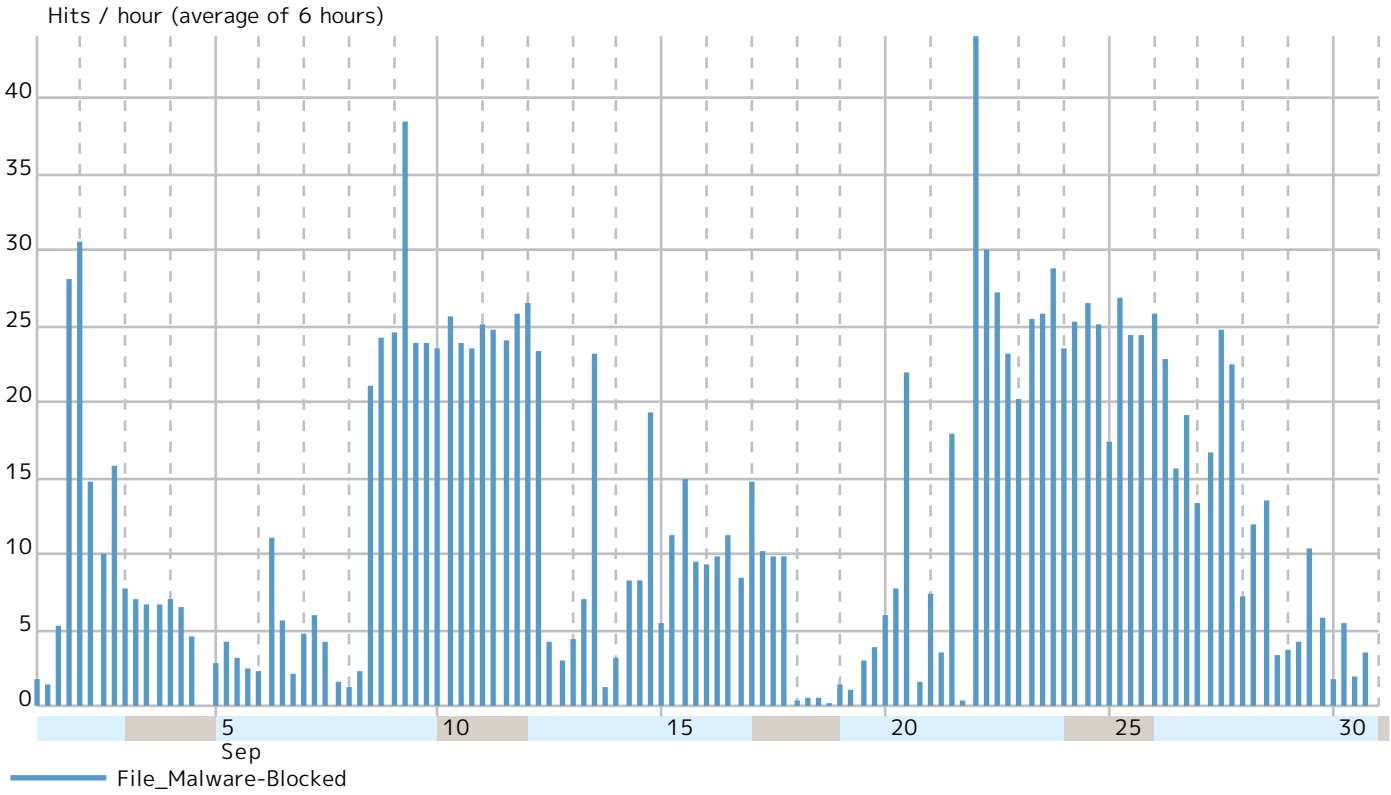
Report

Records by src IP		Hits	%
85.217.145.253	Reston, Virginia 20190, United States	2.05k	22.3 %
80.86.231.190	Armenia	1.94k	21.1 %
49.229.55.140	Bangkok, Thailand	1.24k	13.5 %
104.227.141.118	Piscataway, New Jersey 08854, United States	501	5.5 %
45.89.66.96	Russia	448	4.9 %
195.78.211.236	Rome, Italy	438	4.8 %
95.110.132.17	Arezzo, Italy	278	3.0 %
194.87.231.96	Amsterdam, Netherlands	226	2.5 %
178.216.212.81	Bishkek, Kyrgyzstan	213	2.3 %
89.149.201.46	Netherlands	100	1.1 %
61.95.179.221	Ongole, India	88	1.0 %
74.208.76.183	United States	86	0.9 %
83.149.118.154	Amsterdam, Netherlands	82	0.9 %
213.142.136.181	Turkey	72	0.8 %
103.180.134.230	Vietnam	72	0.8 %
23.106.160.140	Dallas, Texas 75207, United States	56	0.6 %
98.142.254.8	Canada	52	0.6 %
77.71.114.40	Bulgaria	50	0.5 %
85.31.46.112	Virginia, United States	42	0.5 %
104.222.188.104	Los Angeles, California 90060, United States	42	0.5 %
216.189.159.136	Dallas, Texas 75247, United States	40	0.4 %
207.180.198.241	Nuremberg, Germany	34	0.4 %
82.165.57.150	Germany	34	0.4 %
103.178.234.138	Vietnam	34	0.4 %
80.76.51.114	Virginia, United States	31	0.3 %
185.216.71.224	Ashburn, Virginia 20104, United States	30	0.3 %
217.12.212.20	Kharkiv, Ukraine	28	0.3 %
149.137.224.68	United States	25	0.3 %
139.99.53.216	Singapore, 06 Singapore	24	0.3 %
178.162.140.19	Netherlands	23	0.3 %
Others		810	8.8 %
Total		**9.19k**	**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.