Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2021-11-01 00:00:00
To: 2021-12-01 00:00:00

Report

Report run by
jens

SMC version
6.10.3, build 11135

Update version
1408

Report started
2021-12-01 08:40:45

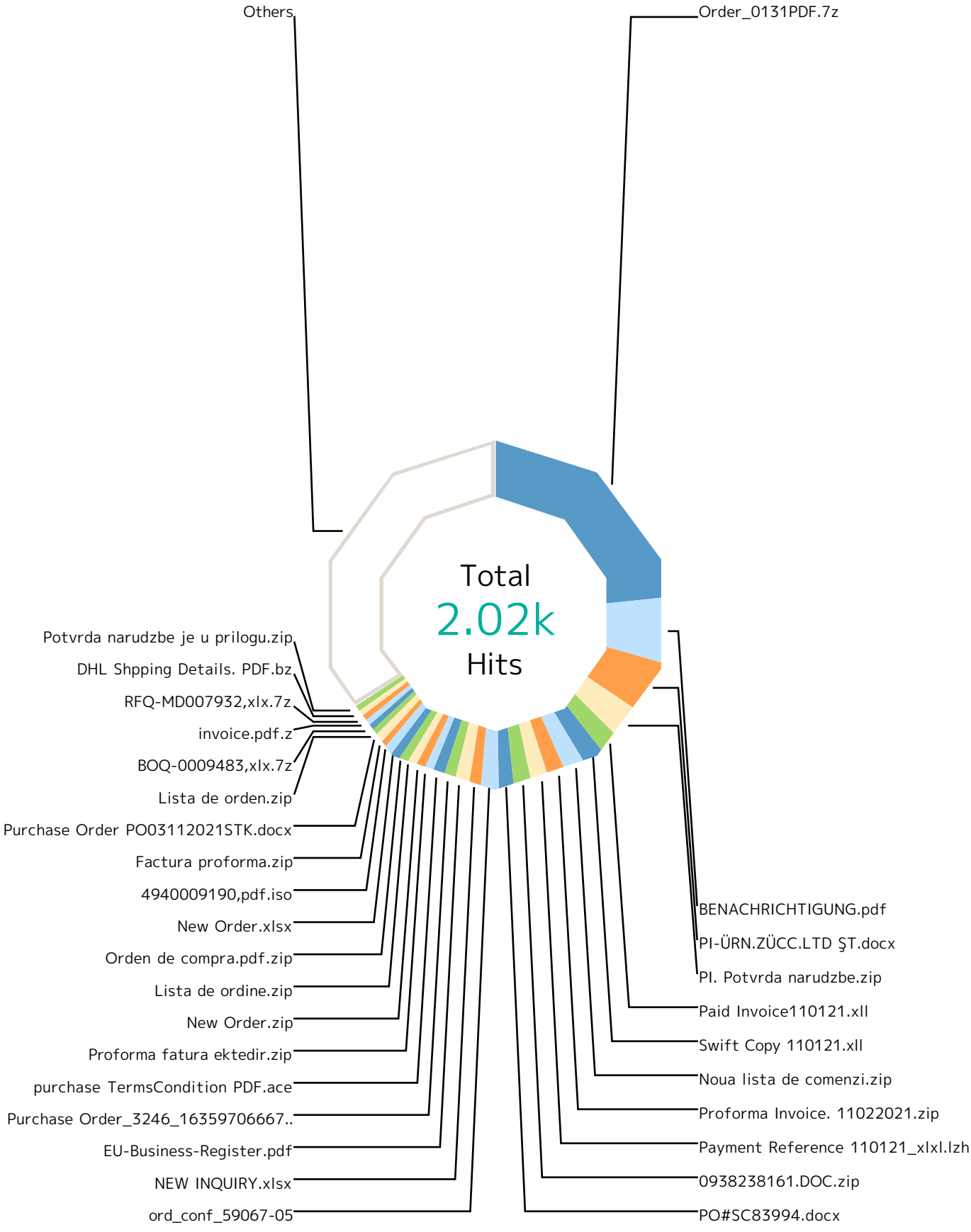
Report run time
01:33:43

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



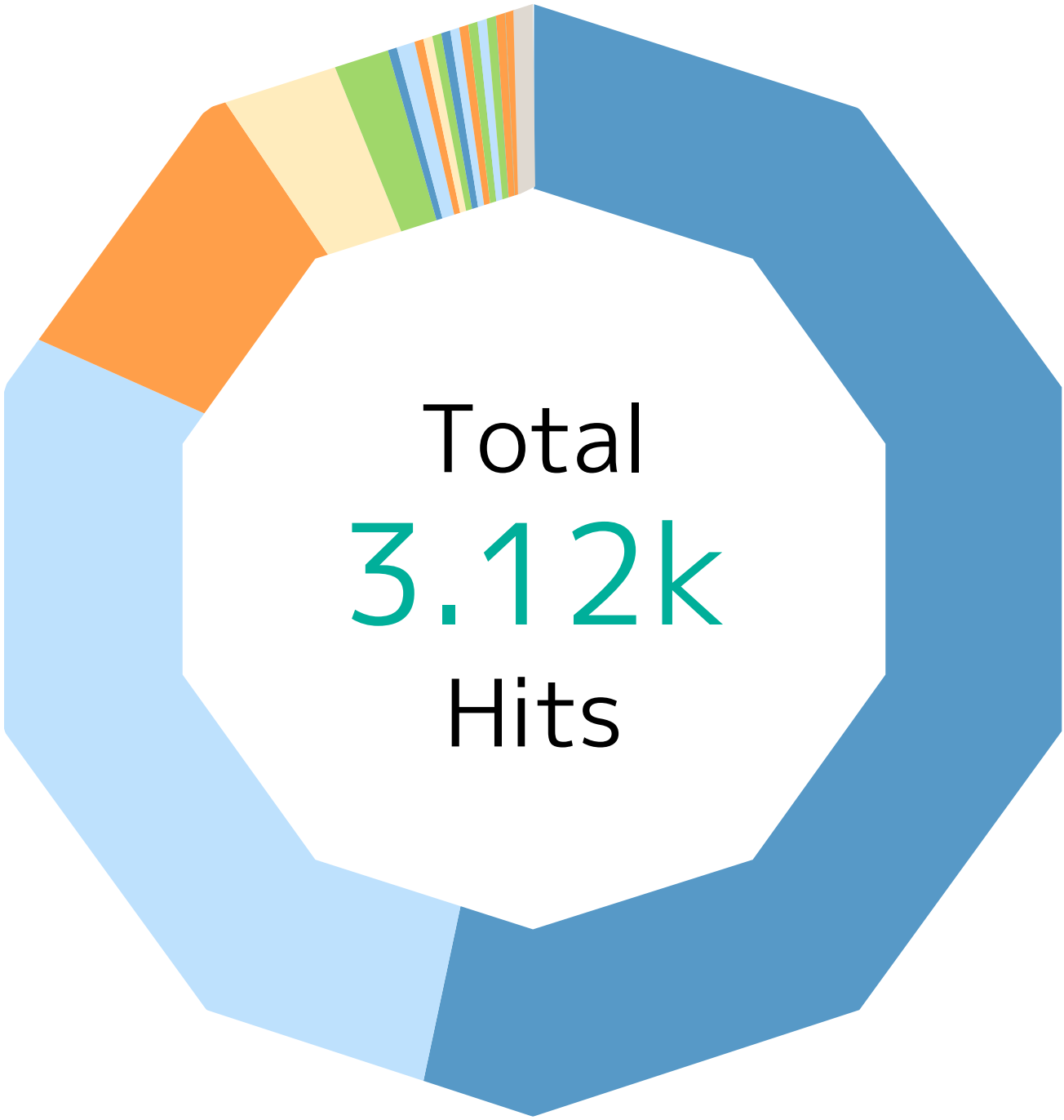
Report

Records by file name	Hits	%
Order_0131PDF.7z	474	23.4 %
BENACHRICHTIGUNG.pdf	124	6.1 %
PI-ÜRN.ZÜCC.LTD ŞT.docx	98	4.8 %
PI. Potvrda narudzbe.zip	63	3.1 %
Paid Invoice110121.xll	39	1.9 %
Swift Copy 110121.xll	39	1.9 %
Noua lista de comenzi.zip	37	1.8 %
Proforma Invoice. 11022021.zip	34	1.7 %
Payment Reference 110121_xlxl.lzh	34	1.7 %
0938238161.DOC.zip	34	1.7 %
PO#SC83994.docx	32	1.6 %
ord_conf_59067-05	29	1.4 %
NEW INQUIRY.xlsx	27	1.3 %
EU-Business-Register.pdf	26	1.3 %
Purchase Order_3246_1635970666745 PDF.ace	22	1.1 %
purchase TermsCondition PDF.ace	21	1.0 %
Proforma fatura ektedir.zip	19	0.9 %
New Order.zip	18	0.9 %
Lista de ordine.zip	17	0.8 %
Orden de compra.pdf.zip	17	0.8 %
New Order.xlsx	16	0.8 %
4940009190,pdf.iso	15	0.7 %
Factura proforma.zip	14	0.7 %
Purchase Order PO03112021STK.docx	13	0.6 %
Lista de orden.zip	13	0.6 %
BOQ-0009483,xlx.7z	12	0.6 %
invoice.pdf.z	12	0.6 %
RFQ-MD007932,xlx.7z	12	0.6 %
DHL Shpping Details. PDF.bz	11	0.5 %
Potvrda narudzbe je u prilogu.zip	11	0.5 %
Others	690	34.1 %
Total	**2.02k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
3.12k
Hits

Report

Scan Result	Hits	%
Malicious	**1.66k**	**53.3 %**
File_Microsoft-Windows-Executable	928	29.8 %
File_Rar-Archive	189	6.1 %
File_Zip-Archive	163	5.2 %
File_PDF	141	4.5 %
File_Microsoft-Excel-XLSX-Filename-Extension	65	2.1 %
File_Office-Open-XML-Package-Relations-Item	55	1.8 %
File_Microsoft-Office-Open-XML-Document	25	0.8 %
File_ISO-9660-Disk-Image	19	0.6 %
File_Microsoft-Cabinet-Archive	17	0.5 %
File_ACE-Archive	16	0.5 %
File_Type-Unknown	11	0.4 %
File_Microsoft-OLE	7	0.2 %
File_7z-Archive	5	0.2 %
File_LhArc-Archive	5	0.2 %
File_Microsoft-Windows-Compiled-Help	4	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	3	0.1 %
File_Microsoft-Equation-Editor-Document	3	0.1 %
File_XZ-Archive	2	0.1 %
File_HTML	1	0.0 %
File_RTF	1	0.0 %
File_Microsoft-Word-97-Document	1	0.0 %
File_JavaScript	1	0.0 %
Not Available	**885**	**28.4 %**
File_Zip-Archive	798	25.6 %
File_Microsoft-Office-Open-XML-Document	73	2.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	8	0.3 %
File_Microsoft-Excel-XLSB-Filename-Extension	6	0.2 %
High Risk	**275**	**8.8 %**
File_Office-Open-XML-Package-Relations-Item	98	3.1 %
File_Rar-Archive	38	1.2 %
File_ACE-Archive	31	1.0 %
File_7z-Archive	27	0.9 %
File_Zip-Archive	23	0.7 %
File_ISO-9660-Disk-Image	22	0.7 %
File_Microsoft-Windows-Executable	19	0.6 %

Report

Scan Result	Hits	%
File_Microsoft-Equation-Editor-Document	6	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	2	0.1 %
File_Microsoft-Cabinet-Archive	2	0.1 %
File_PDF	1	0.0 %
File_Type-Unknown	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	1	0.0 %
Medium Risk	**103**	**3.3 %**
File_XML	30	1.0 %
File_Microsoft-Windows-Executable	26	0.8 %
File_Microsoft-Office-Open-XML-Document	13	0.4 %
File_Zip-Archive	11	0.4 %
File_PDF	9	0.3 %
File_HTML	4	0.1 %
File_Rar-Archive	3	0.1 %
File_ISO-9660-Disk-Image	3	0.1 %
File_7z-Archive	2	0.1 %
File_Type-Unknown	2	0.1 %
Exploit-CVE2017-11882.yx	**53**	**1.7 %**
File_Microsoft-Excel-XLSX-Filename-Extension	53	1.7 %
PWS-FCZF!B4CEAD8429A4	**15**	**0.5 %**
File_ISO-9660-Disk-Image	15	0.5 %
Fareit.gen.a	**14**	**0.4 %**
File_ACE-Archive	14	0.4 %
Exploit-GBT!98DDA446A27D	**11**	**0.4 %**
File_Microsoft-Excel-XLSX-Filename-Extension	11	0.4 %
HTML/Phishing.ge	**10**	**0.3 %**
File_HTML	10	0.3 %
X97M/Downloader.md	**8**	**0.3 %**
File_Microsoft-Excel-XLSB-Filename-Extension	8	0.3 %
Unknown	**7**	**0.2 %**
File_Zip-Archive	7	0.2 %
Fareit-FDBI!20939219D975	**7**	**0.2 %**
File_Zip-Archive	7	0.2 %
X97M/Downloader.ft	**6**	**0.2 %**
File_Microsoft-Excel-XLSB-Filename-Extension	6	0.2 %

Report

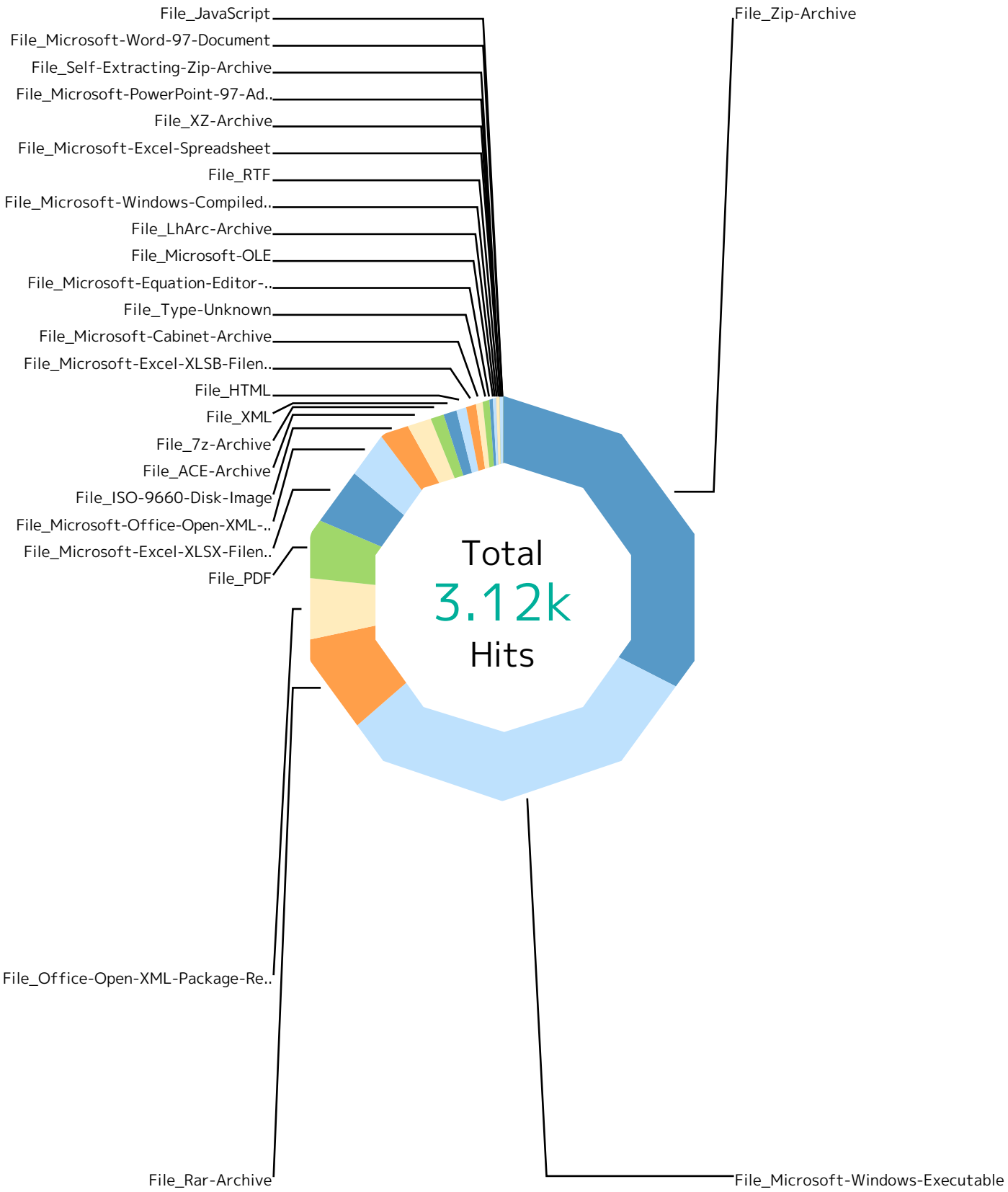
Scan Result	Hits	%
Exploit-CVE2017-11882.bu	**6**	**0.2 %**
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.2 %
GenericRXMK-GR!2A64D99A0646	**5**	**0.2 %**
File_Rar-Archive	5	0.2 %
PWS-FCZF!BD3C521A30B3	**4**	**0.1 %**
File_Rar-Archive	4	0.1 %
GenericRXQE-VF!4475F42E2338	**3**	**0.1 %**
File_Rar-Archive	3	0.1 %
HTML/Phishing.ij	**3**	**0.1 %**
File_HTML	3	0.1 %
HTML/Phishing.ec	**3**	**0.1 %**
File_HTML	3	0.1 %
Exploit-GBT!B521B46E56A1	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
X97M/Downloader.mj	**2**	**0.1 %**
File_Microsoft-Excel-XLSB-Filename-Extension	2	0.1 %
HTML/Phishing.iy	**2**	**0.1 %**
File_HTML	2	0.1 %
Exploit-GBT!246189510786	**2**	**0.1 %**
File_Microsoft-Excel-Spreadsheet	2	0.1 %
Fareit-FCVN!BBCB2B7F0099	**2**	**0.1 %**
File_Zip-Archive	2	0.1 %
Exploit-GAN!ED7DF6A82BBB	**2**	**0.1 %**
File_RTF	2	0.1 %
GenericRXQO-WD!B9A02EA2D3E8	**2**	**0.1 %**
File_7z-Archive	2	0.1 %
PWS-FCUF!51C49DEDA5AB	**2**	**0.1 %**
File_ISO-9660-Disk-Image	2	0.1 %
HTML/Phishing.jw	**2**	**0.1 %**
File_HTML	2	0.1 %
Trojan-FTMC!B8E2DD5E5A71	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
HTML/Phishing.jt	**2**	**0.1 %**
File_HTML	2	0.1 %
Others	**16**	**0.5 %**
Total	**3.12k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_JavaScript
File_Microsoft-Word-97-Document
File_Self-Extracting-Zip-Archive
File_Microsoft-PowerPoint-97-Ad..
File_XZ-Archive
File_Microsoft-Excel-Spreadsheet
File_RTF
File_Microsoft-Windows-Compiled..
File_LhArc-Archive
File_Microsoft-OLE
File_Microsoft-Equation-Editor-..
File_Type-Unknown
File_Microsoft-Cabinet-Archive
File_Microsoft-Excel-XLSB-Filen..
File_HTML
File_XML
File_7z-Archive
File_ACE-Archive
File_ISO-9660-Disk-Image
File_Microsoft-Office-Open-XML-..
File_Microsoft-Excel-XLSX-Filen..
File_PDF
File_Office-Open-XML-Package-Re..
File_Rar-Archive
File_Zip-Archive
File_Microsoft-Windows-Executable
Total
3.12k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**1.01k**	**32.5 %**
Not Available	798	25.6 %
Malicious	163	5.2 %
High Risk	23	0.7 %
Medium Risk	11	0.4 %
Unknown	7	0.2 %
Fareit-FDBI!20939219D975	7	0.2 %
Fareit-FCVN!BBCB2B7F0099	2	0.1 %
Fareit-FCVN!9E8FAA8C017D	1	0.0 %
PWS-FCUF!FEF527E7A108	1	0.0 %
PWS-FCUF!7DD83D33A846	1	0.0 %
File_Microsoft-Windows-Executable	**973**	**31.2 %**
Malicious	928	29.8 %
Medium Risk	26	0.8 %
High Risk	19	0.6 %
File_Rar-Archive	**249**	**8.0 %**
Malicious	189	6.1 %
High Risk	38	1.2 %
GenericRXMK-GR!2A64D99A0646	5	0.2 %
PWS-FCZF!BD3C521A30B3	4	0.1 %
Medium Risk	3	0.1 %
GenericRXQE-VF!4475F42E2338	3	0.1 %
Trojan-FTMC!B8E2DD5E5A71	2	0.1 %
PWS-FCZF!AA55C9BB0742	1	0.0 %
AgentTesla-FDBQ!54A11AE845AC	1	0.0 %
DistTrack!01AA5B91BBC5	1	0.0 %
PWS-FCZF!A5012296FA73	1	0.0 %
PWS-FCUF!412C3FCB237D	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**153**	**4.9 %**
High Risk	98	3.1 %
Malicious	55	1.8 %
File_PDF	**151**	**4.8 %**
Malicious	141	4.5 %
Medium Risk	9	0.3 %
High Risk	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**150**	**4.8 %**

Report

Responding Scanner	Hits	%
Malicious	65	2.1 %
Exploit-CVE2017-11882.yx	53	1.7 %
Exploit-GBT!98DDA446A27D	11	0.4 %
Not Available	8	0.3 %
Exploit-CVE2017-11882.bu	6	0.2 %
High Risk	4	0.1 %
Exploit-GBT!B521B46E56A1	3	0.1 %
File_Microsoft-Office-Open-XML-Document	**111**	**3.6 %**
Not Available	73	2.3 %
Malicious	25	0.8 %
Medium Risk	13	0.4 %
File_ISO-9660-Disk-Image	**63**	**2.0 %**
High Risk	22	0.7 %
Malicious	19	0.6 %
PWS-FCZF!B4CEAD8429A4	15	0.5 %
Medium Risk	3	0.1 %
PWS-FCUF!51C49DEDA5AB	2	0.1 %
Trojan-FNTX!4D67790A15CE	1	0.0 %
AgentTesla-FDBQ!6898BBA17F98	1	0.0 %
File_ACE-Archive	**63**	**2.0 %**
High Risk	31	1.0 %
Malicious	16	0.5 %
Fareit.gen.a	14	0.4 %
Fareit.gen.f	1	0.0 %
Fareit.gen.e	1	0.0 %
File_7z-Archive	**37**	**1.2 %**
High Risk	27	0.9 %
Malicious	5	0.2 %
Medium Risk	2	0.1 %
GenericRXQO-WD!B9A02EA2D3E8	2	0.1 %
GenericRXQE-VF!0B5EBA2C887C	1	0.0 %
File_XML	**30**	**1.0 %**
Medium Risk	30	1.0 %
File_HTML	**29**	**0.9 %**
HTML/Phishing.ge	10	0.3 %
Medium Risk	4	0.1 %

Report

Responding Scanner	Hits	%
HTML/Phishing.ij	3	0.1 %
HTML/Phishing.ec	3	0.1 %
HTML/Phishing.iy	2	0.1 %
HTML/Phishing.jw	2	0.1 %
HTML/Phishing.jt	2	0.1 %
Malicious	1	0.0 %
HTML/Phishing!DB07738C1569	1	0.0 %
HTML/Phishing.hh	1	0.0 %
File_Microsoft-Excel-XLSB-Filename-Extension	**27**	**0.9 %**
X97M/Downloader.md	8	0.3 %
Not Available	6	0.2 %
X97M/Downloader.ft	6	0.2 %
Malicious	3	0.1 %
High Risk	2	0.1 %
X97M/Downloader.mj	2	0.1 %
File_Microsoft-Cabinet-Archive	**19**	**0.6 %**
Malicious	17	0.5 %
High Risk	2	0.1 %
File_Type-Unknown	**14**	**0.4 %**
Malicious	11	0.4 %
Medium Risk	2	0.1 %
High Risk	1	0.0 %
File_Microsoft-Equation-Editor-Document	**9**	**0.3 %**
High Risk	6	0.2 %
Malicious	3	0.1 %
File_Microsoft-OLE	**7**	**0.2 %**
Malicious	7	0.2 %
File_LhArc-Archive	**5**	**0.2 %**
Malicious	5	0.2 %
File_Microsoft-Windows-Compiled-Help	**4**	**0.1 %**
Malicious	4	0.1 %
File_RTF	**3**	**0.1 %**
Exploit-GAN!ED7DF6A82BBB	2	0.1 %
Malicious	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**2**	**0.1 %**
Exploit-GBT!246189510786	2	0.1 %

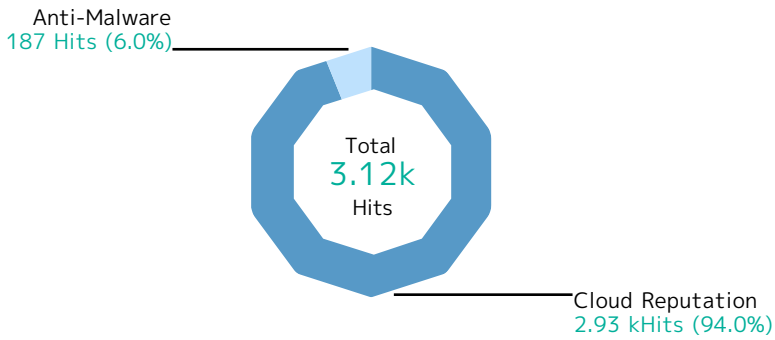
Report

Responding Scanner	Hits	%
File_XZ-Archive	**2**	**0.1 %**
Malicious	2	0.1 %
File_Microsoft-PowerPoint-97-Add-In	**1**	**0.0 %**
High Risk	1	0.0 %
File_Self-Extracting-Zip-Archive	**1**	**0.0 %**
GenericRXMK-GR!60979D9E81CB	1	0.0 %
File_Microsoft-Word-97-Document	**1**	**0.0 %**
Malicious	1	0.0 %
File_JavaScript	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**3.12k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**2.93k**	**94.0 %**
File_Zip-Archive	1.00k	32.1 %
File_Microsoft-Windows-Executable	973	31.2 %
File_Rar-Archive	230	7.4 %
File_Office-Open-XML-Package-Relations-Item	153	4.9 %
File_PDF	151	4.8 %
File_Microsoft-Office-Open-XML-Document	111	3.6 %
File_Microsoft-Excel-XLSX-Filename-Extension	77	2.5 %
File_ACE-Archive	47	1.5 %
File_ISO-9660-Disk-Image	44	1.4 %
File_7z-Archive	34	1.1 %
File_XML	30	1.0 %
File_Microsoft-Cabinet-Archive	19	0.6 %
File_Type-Unknown	14	0.4 %
File_Microsoft-Excel-XLSB-Filename-Extension	11	0.4 %
File_Microsoft-Equation-Editor-Document	9	0.3 %
File_Microsoft-OLE	7	0.2 %
File_HTML	5	0.2 %
File_LhArc-Archive	5	0.2 %
File_Microsoft-Windows-Compiled-Help	4	0.1 %
File_XZ-Archive	2	0.1 %
File_RTF	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	1	0.0 %
File_Microsoft-Word-97-Document	1	0.0 %
File_JavaScript	1	0.0 %
Anti-Malware	**187**	**6.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	73	2.3 %
File_HTML	24	0.8 %
File_Rar-Archive	19	0.6 %
File_ISO-9660-Disk-Image	19	0.6 %
File_ACE-Archive	16	0.5 %
File_Microsoft-Excel-XLSB-Filename-Extension	16	0.5 %
File_Zip-Archive	12	0.4 %
File_7z-Archive	3	0.1 %
File_RTF	2	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.1 %

Report

Responding Scanner	Hits	%
File_Self-Extracting-Zip-Archive	1	0.0 %
Total	**3.12k**	**100 %**

Report

Virenfilterung SRC IPs

Located 79.4 %

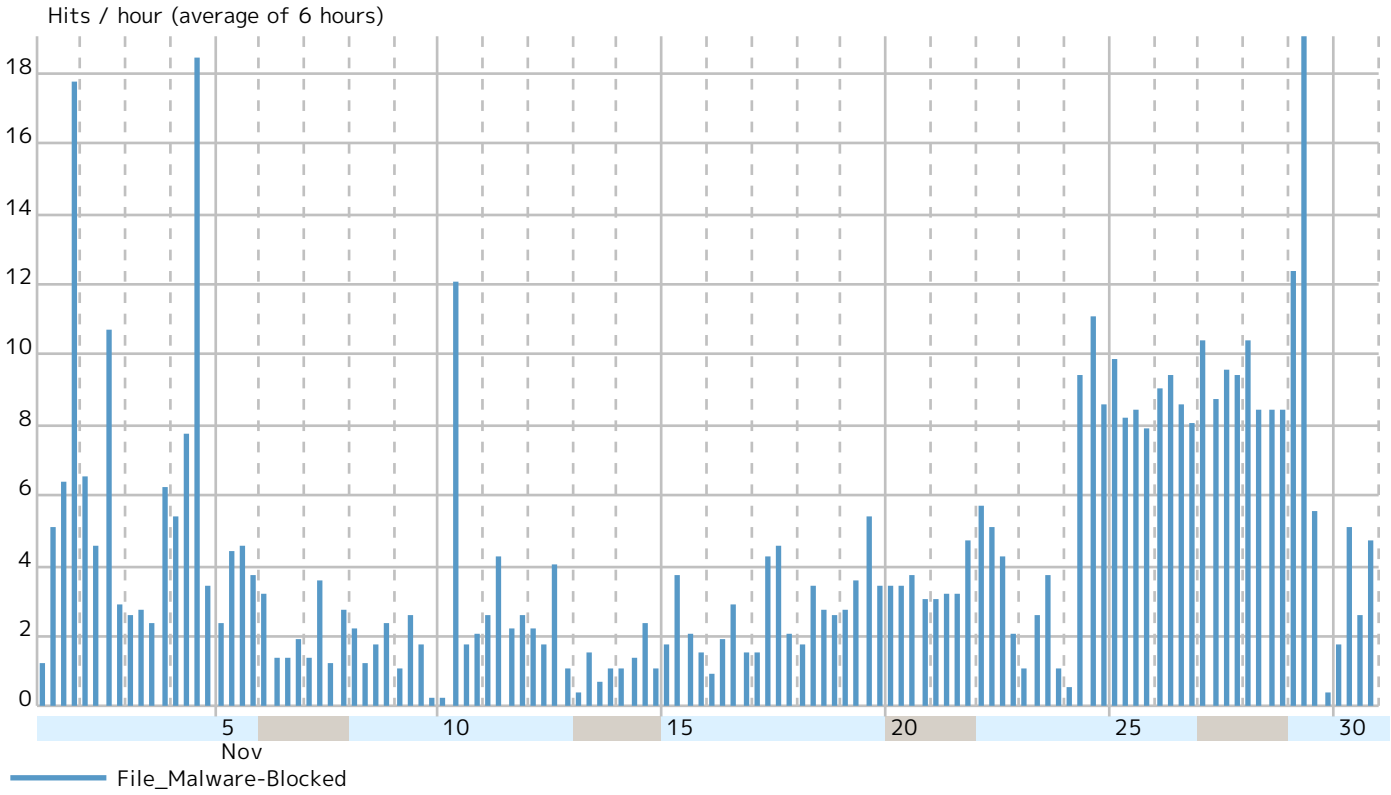
Report

Records by src IP		Hits	%
212.96.173.7	Znojmo, Czechia	948	30.4 %
185.46.188.30	Ukraine	400	12.8 %
144.76.223.108	Germany	216	6.9 %
195.33.210.155	Antakya, Turkey	182	5.8 %
188.166.226.213	Singapore, 62 Singapore	123	3.9 %
185.222.57.179	Amsterdam, Netherlands	112	3.6 %
202.27.215.17	Gisborne, New Zealand	64	2.1 %
190.210.132.129	Buenos Aires, Argentina	48	1.5 %
207.154.225.91	Frankfurt am Main, Germany	43	1.4 %
159.223.72.127	Singapore, 62 Singapore	30	1.0 %
2.56.59.69	Dulles, Virginia 20103, United States	27	0.9 %
5.175.40.32	Spain	26	0.8 %
103.232.55.201	Vietnam	25	0.8 %
212.192.241.173	Czechia	24	0.8 %
94.103.34.154	Turkey	22	0.7 %
185.222.57.209	Amsterdam, Netherlands	20	0.6 %
136.144.41.133	San Francisco, California 94119, United States	15	0.5 %
209.97.175.41	Singapore, 62 Singapore	15	0.5 %
31.210.20.153	Gambrills, Maryland 21054, United States	15	0.5 %
104.168.237.69	United States	14	0.4 %
103.90.242.54	India	12	0.4 %
137.184.106.83	North Bergen, New Jersey 07047, United States	12	0.4 %
178.62.192.207	Amsterdam, Netherlands	11	0.4 %
178.62.3.35	London, United Kingdom	11	0.4 %
209.85.160.194	United States	10	0.3 %
209.85.222.193	United States	10	0.3 %
45.133.1.29	Netherlands	10	0.3 %
174.136.57.143	United States	10	0.3 %
195.133.18.211	Czechia	10	0.3 %
45.137.22.137	Bangladesh	10	0.3 %
Others		644	20.6 %
Total		**3.12k**	**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.