Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period
From: 2021-12-01 00:00:00
To: 2022-01-01 00:00:00

Report

Report run by
jens

SMC version
6.10.5, build 11136

Update version
1422

Report started
2022-01-01 20:56:59

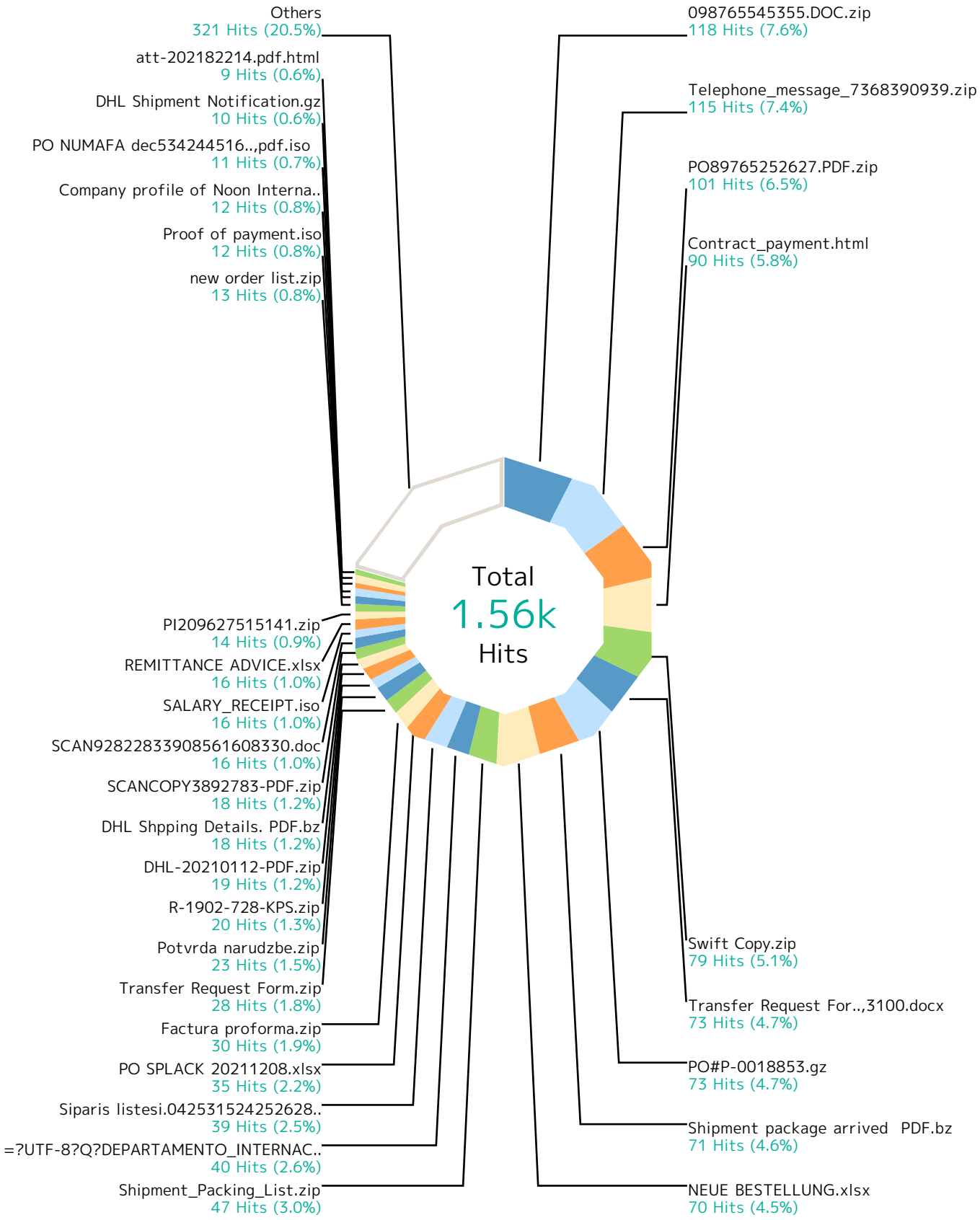
Report run time
01:16:40

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



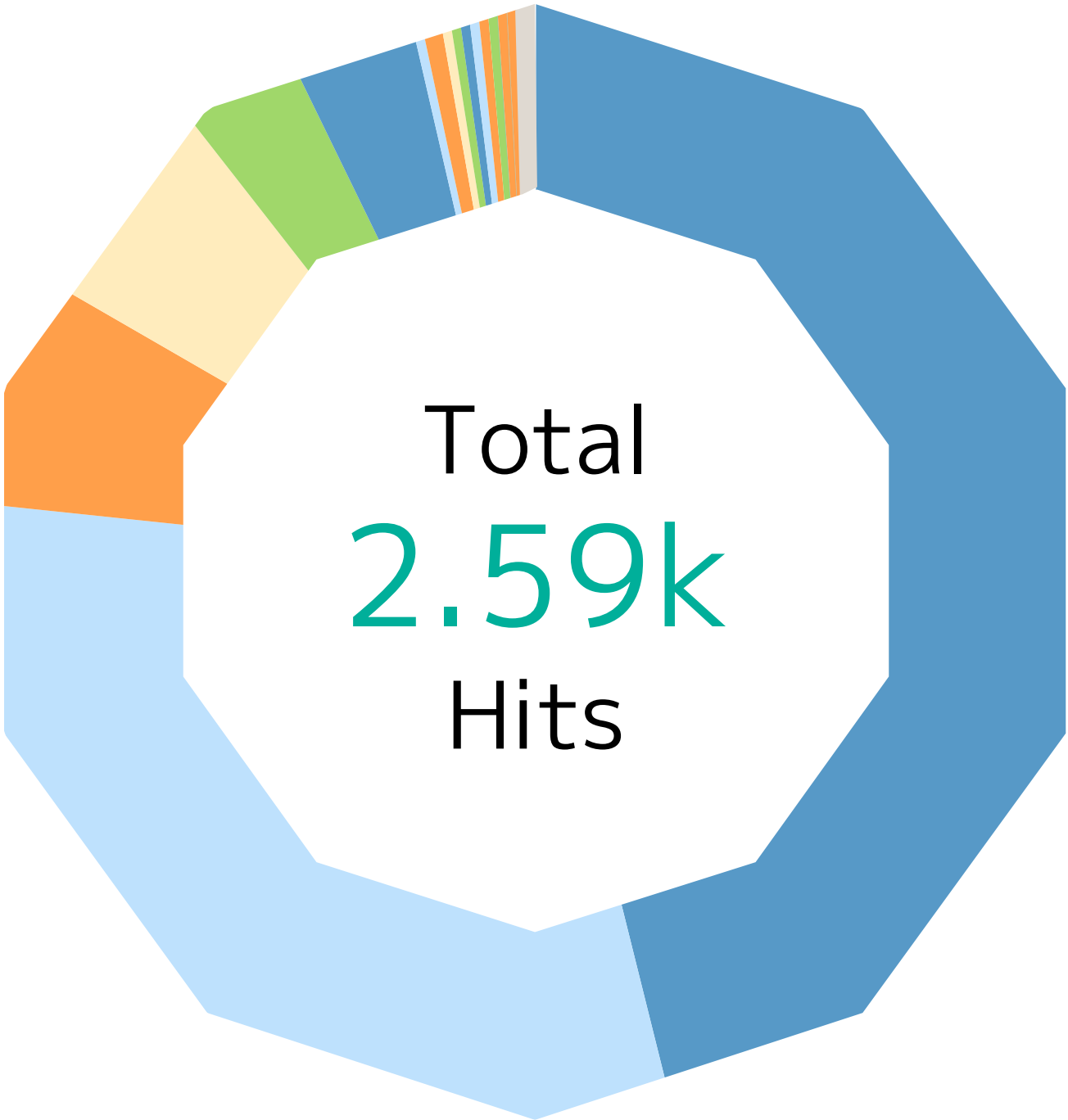
Report

Records by file name	Hits	%
098765545355.DOC.zip	118	7.6 %
Telephone_message_7368390939.zip	115	7.4 %
PO89765252627.PDF.zip	101	6.5 %
Contract_payment.html	90	5.8 %
Swift Copy.zip	79	5.1 %
Transfer Request Form of $57,3100.docx	73	4.7 %
PO#P-0018853.gz	73	4.7 %
Shipment package arrived PDF.bz	71	4.6 %
NEUE BESTELLUNG.xlsx	70	4.5 %
Shipment_Packing_List.zip	47	3.0 %
=?UTF-8?Q?DEPARTAMENTO_INTERNACIONAL_DE_MOLOTER=C3=8DA=2E=2Edocx?=	40	2.6 %
Siparis listesi.042531524252628827.PDF.zip	39	2.5 %
PO SPLACK 20211208.xlsx	35	2.2 %
Factura proforma.zip	30	1.9 %
Transfer Request Form.zip	28	1.8 %
Potvrda narudzbe.zip	23	1.5 %
R-1902-728-KPS.zip	20	1.3 %
DHL-20210112-PDF.zip	19	1.2 %
DHL Shpping Details. PDF.bz	18	1.2 %
SCANCOPY3892783-PDF.zip	18	1.2 %
SCAN928228333908561608330.doc	16	1.0 %
SALARY_RECEIPT.iso	16	1.0 %
REMITTANCE ADVICE.xlsx	16	1.0 %
PI209627515141.zip	14	0.9 %
new order list.zip	13	0.8 %
Proof of payment.iso	12	0.8 %
Company profile of Noon International (Pvt) Ltd.xlsx	12	0.8 %
PO NUMAFA dec534244516876562,pdf.iso	11	0.7 %
DHL Shipment Notification.gz	10	0.6 %
att-202182214.pdf.html	9	0.6 %
Others	321	20.6 %
Total	**1.56k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
2.59k
Hits

Report

Scan Result	Hits	%
Malicious	**1.20k**	**46.2 %**
File_Microsoft-Windows-Executable	632	24.4 %
File_Zip-Archive	230	8.9 %
File_HTML	115	4.4 %
File_Office-Open-XML-Package-Relations-Item	78	3.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	34	1.3 %
File_Rar-Archive	34	1.3 %
File_ISO-9660-Disk-Image	21	0.8 %
File_Microsoft-OLE	21	0.8 %
File_Microsoft-Equation-Editor-Document	15	0.6 %
File_ACE-Archive	10	0.4 %
File_Type-Unknown	4	0.2 %
File_PDF	3	0.1 %
File_XZ-Archive	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
Not Available	**792**	**30.5 %**
File_Zip-Archive	674	26.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	118	4.6 %
High Risk	**173**	**6.7 %**
File_ISO-9660-Disk-Image	54	2.1 %
File_Rar-Archive	32	1.2 %
File_Microsoft-Equation-Editor-Document	30	1.2 %
File_Zip-Archive	21	0.8 %
File_Microsoft-Windows-Executable	17	0.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.4 %
File_Microsoft-OLE	6	0.2 %
File_Type-Unknown	2	0.1 %
File_ACE-Archive	1	0.0 %
Medium Risk	**152**	**5.9 %**
File_XML	99	3.8 %
File_Microsoft-Windows-Executable	23	0.9 %
File_Type-Unknown	17	0.7 %
File_Zip-Archive	3	0.1 %
File_PDF	3	0.1 %
File_HTML	2	0.1 %
File_7z-Archive	2	0.1 %

Report

Scan Result	Hits	%
File_Microsoft-Office-Open-XML-Document	2	0.1 %
File_Self-Extracting-Zip-Archive	1	0.0 %
HTML/Phishing.eh	**92**	**3.5 %**
File_Type-Unknown	92	3.5 %
NSIS/ObfusInjector.h	**90**	**3.5 %**
File_Type-Unknown	83	3.2 %
File_Rar-Archive	4	0.2 %
File_Zip-Archive	3	0.1 %
Unknown	**10**	**0.4 %**
File_Zip-Archive	10	0.4 %
Exploit-CVE2017-11882.yx	**10**	**0.4 %**
File_Microsoft-Excel-XLSX-Filename-Extension	10	0.4 %
PWS-FCUF!6EE193BD9216	**9**	**0.3 %**
File_ISO-9660-Disk-Image	9	0.3 %
Exploit-GBT!2C41E2F11ED4	**9**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.3 %
HTML/Phishing.ge	**9**	**0.3 %**
File_HTML	9	0.3 %
Exploit-GBT!605B8E928306	**6**	**0.2 %**
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.2 %
PWS-FCUF!ED016B16865E	**5**	**0.2 %**
File_Zip-Archive	5	0.2 %
HTML/Phishing.is	**3**	**0.1 %**
File_HTML	3	0.1 %
HTML/Phishing.mg	**3**	**0.1 %**
File_HTML	3	0.1 %
Fareit.gen.a	**3**	**0.1 %**
File_ACE-Archive	3	0.1 %
JS/Nemucod.akz	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
Exploit-GBT!3C2E0762BEA0	**2**	**0.1 %**
File_Microsoft-Excel-Spreadsheet	2	0.1 %
X97M/Downloader.la	**2**	**0.1 %**
File_Microsoft-Excel-XLSB-Filename-Extension	2	0.1 %
AgentTesla-FDBQ!74488DB96204	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %

Report

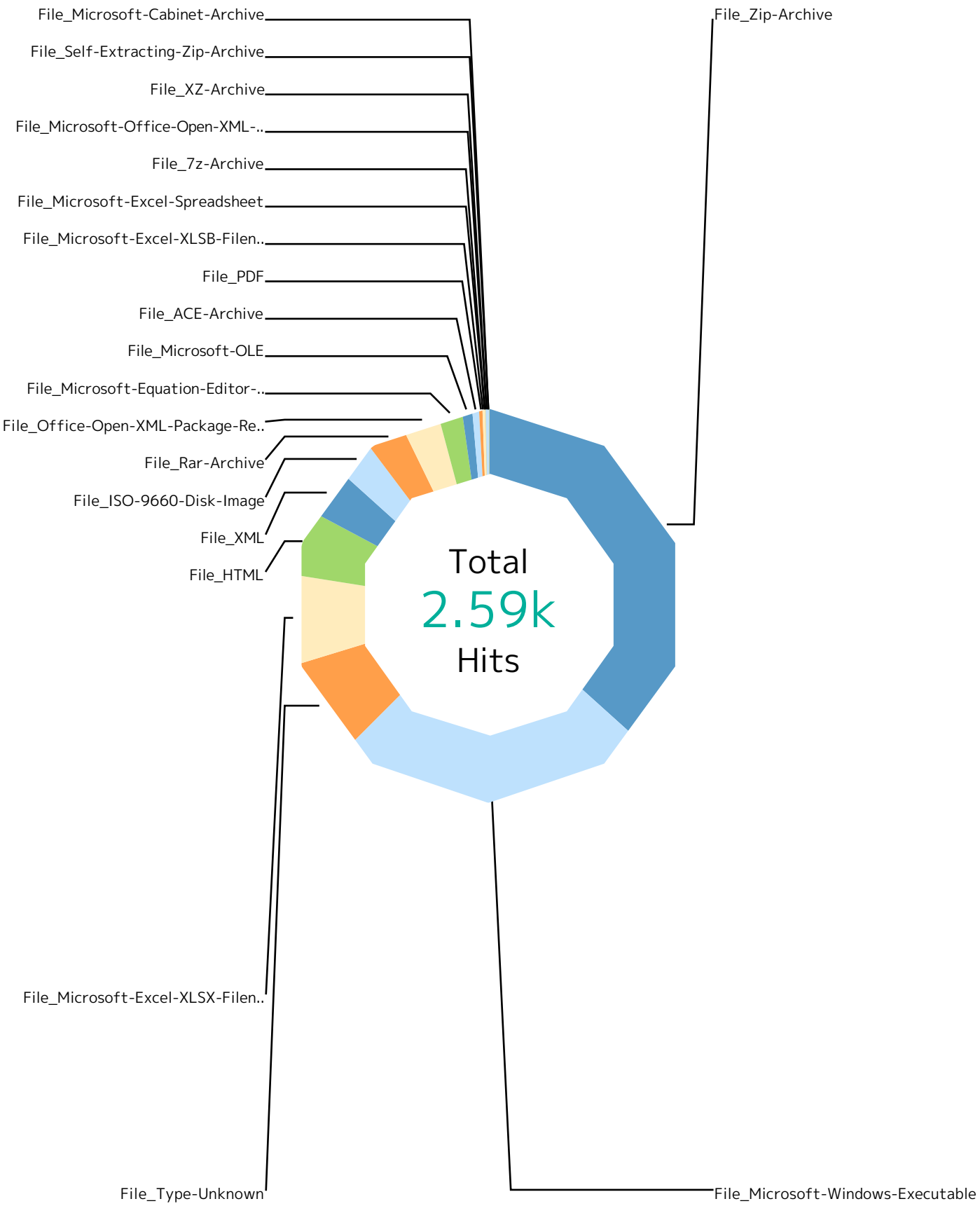
Scan Result	Hits	%
AgentTesla-FDBQ!85C3EF2C655C	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
HTML/Phishing.iy	**1**	**0.0 %**
File_HTML	1	0.0 %
AgentTesla-FDBQ!7A0D167C7CA1	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Exploit-GBT!D6FAA84AA7EC	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!21A3D304A9C4	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!F0FDC2C4F80C	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
AgentTesla-FDBQ!F7D01903492F	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
X97M/Downloader.ft	**1**	**0.0 %**
File_Microsoft-Excel-XLSB-Filename-Extension	1	0.0 %
PWS-FCZF!E616498EAA38	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
PWS-FCZF!27F2A9688EC3	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Others	**11**	**0.4 %**
Total	**2.59k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Microsoft-Cabinet-Archive
File_Self-Extracting-Zip-Archive
File_XZ-Archive
File_Microsoft-Office-Open-XML-..
File_7z-Archive
File_Microsoft-Excel-Spreadsheet
File_Microsoft-Excel-XLSB-Filen..
File_PDF
File_ACE-Archive
File_Microsoft-OLE
File_Microsoft-Equation-Editor-..
File_Office-Open-XML-Package-Re..
File_Rar-Archive
File_ISO-9660-Disk-Image
File_XML
File_HTML
File_Zip-Archive
Total
2.59k
Hits
File_Microsoft-Excel-XLSX-Filen..
File_Type-Unknown
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**952**	**36.7 %**
Not Available	674	26.0 %
Malicious	230	8.9 %
High Risk	21	0.8 %
Unknown	10	0.4 %
PWS-FCUF!ED016B16865E	5	0.2 %
Medium Risk	3	0.1 %
NSIS/ObfusInjector.h	3	0.1 %
AgentTesla-FDBQ!74488DB96204	1	0.0 %
AgentTesla-FDBQ!F7D01903492F	1	0.0 %
Fareit-FCVN!A287C06529C0	1	0.0 %
PWS-FCZF!A1AF0E78164F	1	0.0 %
PWS-FCUF!9F306B998395	1	0.0 %
AgentTesla-FDBQ!253D3BD7111B	1	0.0 %
File_Microsoft-Windows-Executable	**672**	**25.9 %**
Malicious	632	24.4 %
Medium Risk	23	0.9 %
High Risk	17	0.7 %
File_Type-Unknown	**198**	**7.6 %**
HTML/Phishing.eh	92	3.5 %
NSIS/ObfusInjector.h	83	3.2 %
Medium Risk	17	0.7 %
Malicious	4	0.2 %
High Risk	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**190**	**7.3 %**
Not Available	118	4.6 %
Malicious	34	1.3 %
High Risk	10	0.4 %
Exploit-CVE2017-11882.yx	10	0.4 %
Exploit-GBT!2C41E2F11ED4	9	0.3 %
Exploit-GBT!605B8E928306	6	0.2 %
Exploit-GBT!D6FAA84AA7EC	1	0.0 %
Exploit-GBT!21A3D304A9C4	1	0.0 %
Exploit-GBT!A0E26F3DCAA9	1	0.0 %
File_HTML	**134**	**5.2 %**
Malicious	115	4.4 %

Report

Responding Scanner	Hits	%
HTML/Phishing.ge	9	0.3 %
HTML/Phishing.is	3	0.1 %
HTML/Phishing.mg	3	0.1 %
Medium Risk	2	0.1 %
HTML/Phishing.iy	1	0.0 %
HTML/Phishing.hj	1	0.0 %
File_XML	**99**	**3.8 %**
Medium Risk	99	3.8 %
File_ISO-9660-Disk-Image	**84**	**3.2 %**
High Risk	54	2.1 %
Malicious	21	0.8 %
PWS-FCUF!6EE193BD9216	9	0.3 %
File_Rar-Archive	**80**	**3.1 %**
Malicious	34	1.3 %
High Risk	32	1.2 %
NSIS/ObfusInjector.h	4	0.2 %
JS/Nemucod.akz	2	0.1 %
AgentTesla-FDBQ!85C3EF2C655C	1	0.0 %
AgentTesla-FDBQ!7A0D167C7CA1	1	0.0 %
PWS-FCZF!E616498EAA38	1	0.0 %
PWS-FCZF!27F2A9688EC3	1	0.0 %
AgentTesla-FDBQ!F791EF2ECA19	1	0.0 %
AgentTesla-FDBQ!A1A3B0D58F94	1	0.0 %
Trojan-FTMC!99962D2D35B0	1	0.0 %
RDN/Generic PWS.y	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**78**	**3.0 %**
Malicious	78	3.0 %
File_Microsoft-Equation-Editor-Document	**45**	**1.7 %**
High Risk	30	1.2 %
Malicious	15	0.6 %
File_Microsoft-OLE	**27**	**1.0 %**
Malicious	21	0.8 %
High Risk	6	0.2 %
File_ACE-Archive	**15**	**0.6 %**
Malicious	10	0.4 %
Fareit.gen.a	3	0.1 %

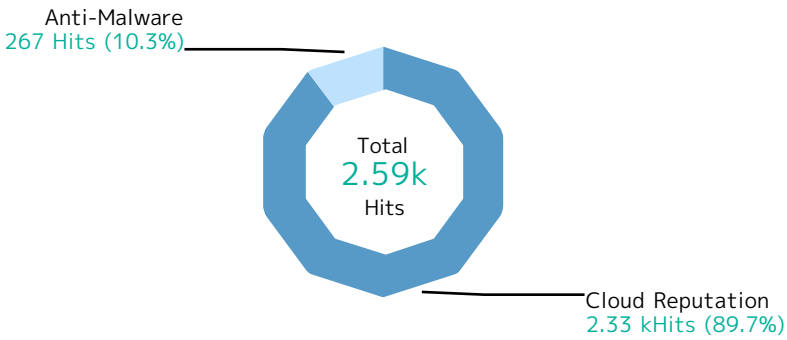
Report

Responding Scanner	Hits	%
High Risk	1	0.0 %
Fareit.gen.e	1	0.0 %
File_PDF	**6**	**0.2 %**
Malicious	3	0.1 %
Medium Risk	3	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	**3**	**0.1 %**
X97M/Downloader.la	2	0.1 %
X97M/Downloader.ft	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**3**	**0.1 %**
Exploit-GBT!3C2E0762BEA0	2	0.1 %
Exploit-GBT!F0FDC2C4F80C	1	0.0 %
File_7z-Archive	**2**	**0.1 %**
Medium Risk	2	0.1 %
File_Microsoft-Office-Open-XML-Document	**2**	**0.1 %**
Medium Risk	2	0.1 %
File_XZ-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_Self-Extracting-Zip-Archive	**1**	**0.0 %**
Medium Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**2.59k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**2.33k**	**89.7 %**
File_Zip-Archive	938	36.2 %
File_Microsoft-Windows-Executable	672	25.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	162	6.2 %
File_HTML	117	4.5 %
File_XML	99	3.8 %
File_Office-Open-XML-Package-Relations-Item	78	3.0 %
File_ISO-9660-Disk-Image	75	2.9 %
File_Rar-Archive	66	2.5 %
File_Microsoft-Equation-Editor-Document	45	1.7 %
File_Microsoft-OLE	27	1.0 %
File_Type-Unknown	23	0.9 %
File_ACE-Archive	11	0.4 %
File_PDF	6	0.2 %
File_7z-Archive	2	0.1 %
File_Microsoft-Office-Open-XML-Document	2	0.1 %
File_XZ-Archive	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
Anti-Malware	**267**	**10.3 %**
File_Type-Unknown	175	6.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	28	1.1 %
File_HTML	17	0.7 %
File_Zip-Archive	14	0.5 %
File_Rar-Archive	14	0.5 %
File_ISO-9660-Disk-Image	9	0.3 %
File_ACE-Archive	4	0.2 %
File_Microsoft-Excel-XLSB-Filename-Extension	3	0.1 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
Total	**2.59k**	**100 %**

Report

Virenfilterung SRC IPs

Located 87.3 %

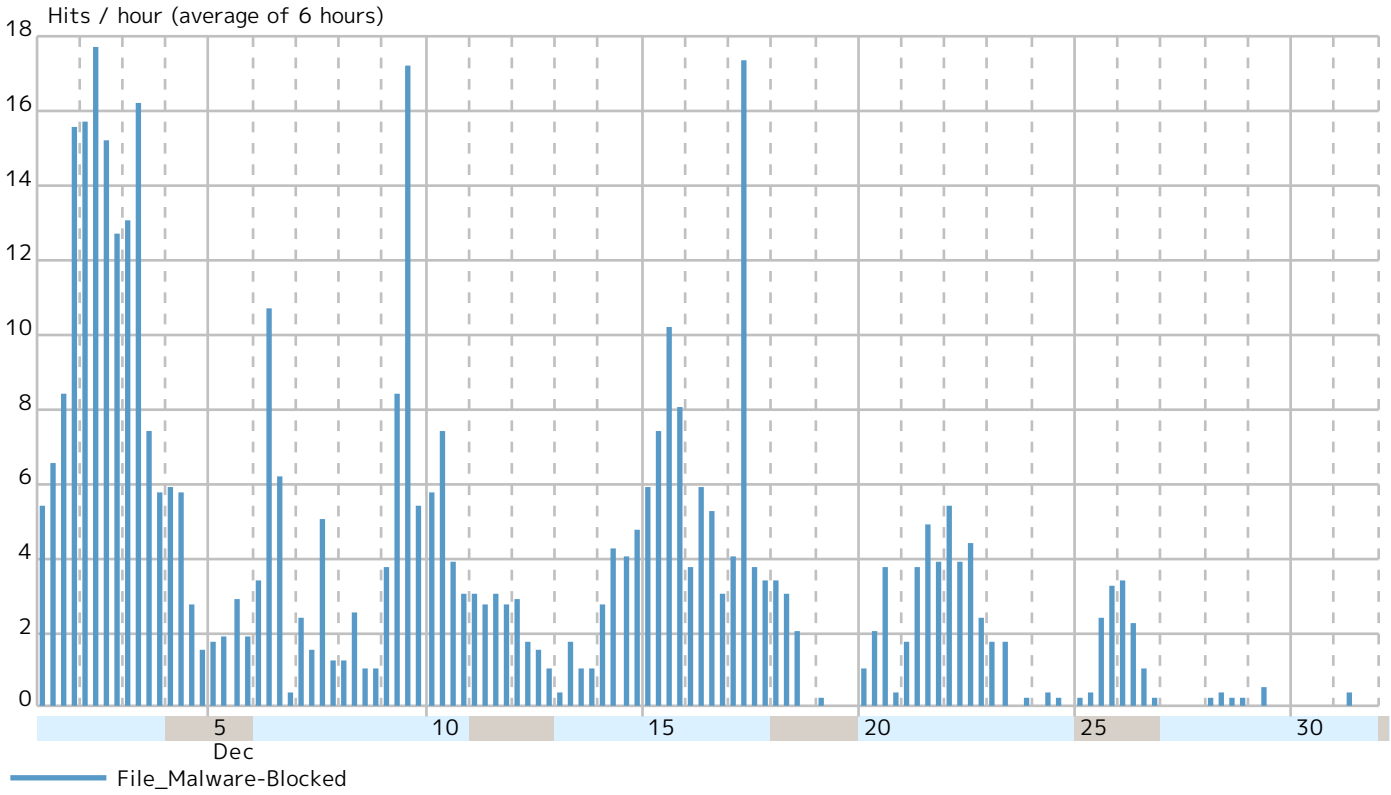
Report

Records by src IP		Hits	%
185.46.188.30	Ukraine	675	26.0 %
103.20.212.44	Faridabad, India	176	6.8 %
198.37.158.13	United States	146	5.6 %
193.107.26.3	Kyiv, Ukraine	144	5.6 %
168.100.174.215	United States	142	5.5 %
216.117.173.93	United States	141	5.4 %
159.223.79.123	Singapore, 62 Singapore	94	3.6 %
142.93.135.146	Amsterdam, Netherlands	92	3.5 %
216.117.136.131	United States	71	2.7 %
162.244.81.227	United States	70	2.7 %
67.205.154.71	North Bergen, New Jersey 07047, United States	60	2.3 %
185.59.31.151	Turkey	56	2.2 %
38.103.244.230	United States	54	2.1 %
128.199.20.186	Bengaluru, India	40	1.5 %
142.93.221.204	Bengaluru, India	36	1.4 %
94.103.34.154	Turkey	36	1.4 %
140.227.240.135	Japan	32	1.2 %
45.93.251.124	Offenbach, Germany	23	0.9 %
147.189.174.68	Germany	22	0.8 %
134.209.156.253	Bengaluru, India	19	0.7 %
162.244.80.45	United States	18	0.7 %
209.85.167.193	United States	17	0.7 %
38.103.244.232	United States	16	0.6 %
147.182.143.133	North Bergen, New Jersey 07047, United States	14	0.5 %
138.68.54.97	Santa Clara, California 95051, United States	13	0.5 %
209.85.167.196	United States	12	0.5 %
89.252.178.117	Turkey	12	0.5 %
159.203.174.203	Clifton, New Jersey 07014, United States	11	0.4 %
172.93.231.245	United States	11	0.4 %
138.68.28.209	Santa Clara, California 95051, United States	10	0.4 %
Others		330	12.7 %
Total		**2.59k**	**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.