Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-04-01 00:00:00
To: 2022-05-01 00:00:00

Report

Report run by
jens

SMC version
6.10.7, build 11163

Update version
1459

Report started
2022-05-01 09:57:20

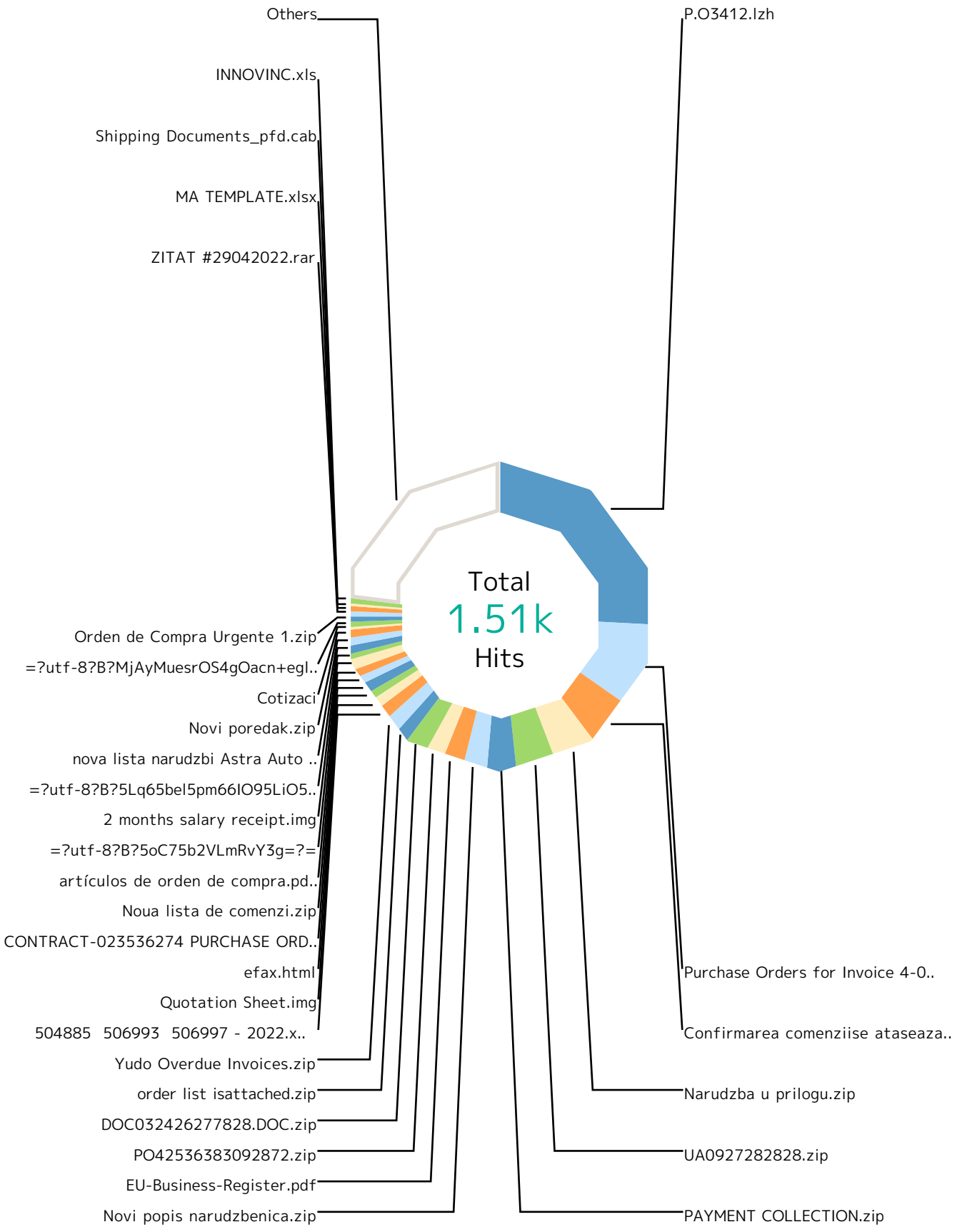
Report run time
01:50:44

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



Report

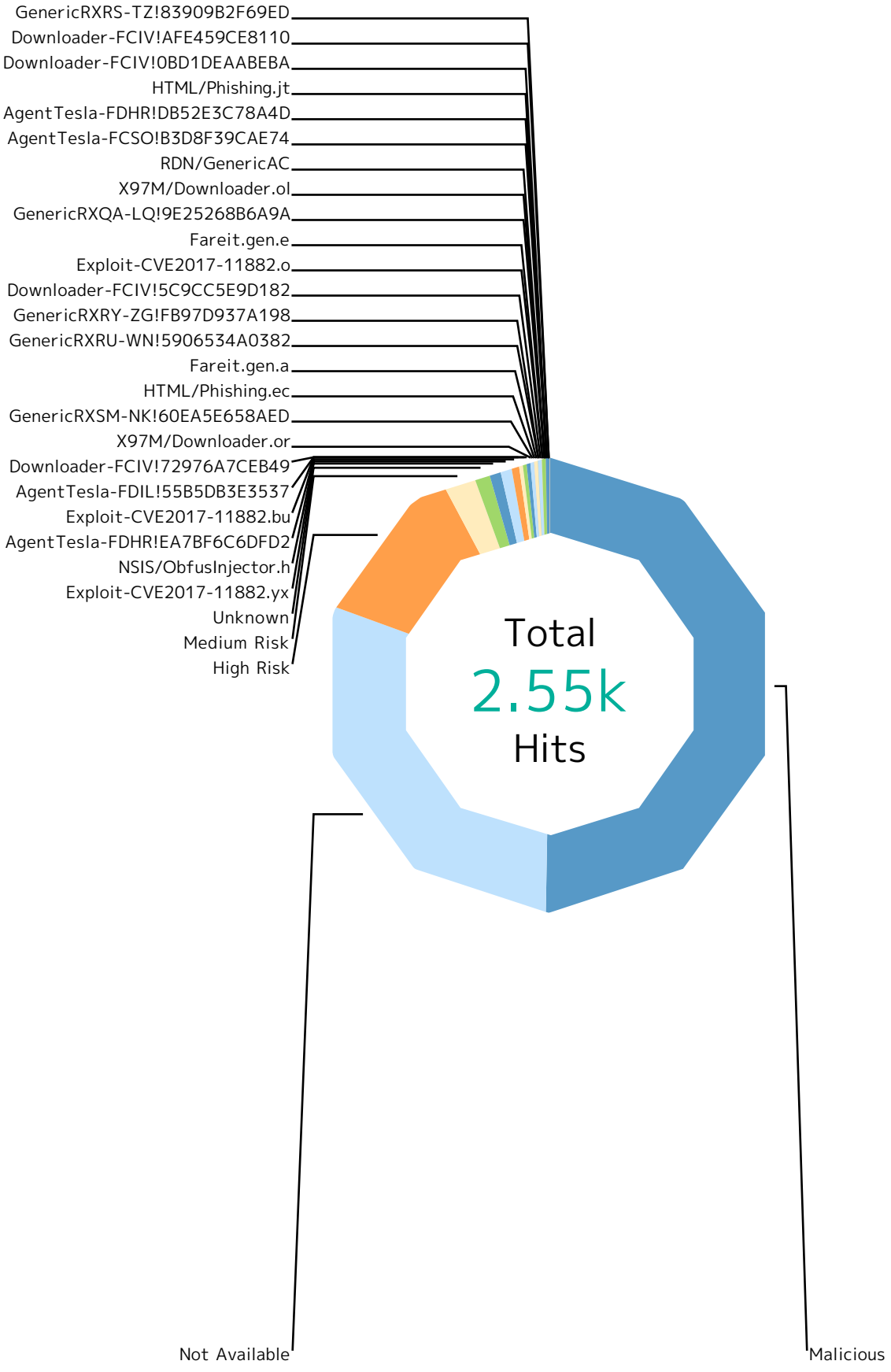
Records by file name	Hits	%
P.O3412.lzh	390	25.9 %
Purchase Orders for Invoice 4-04-22_pdf.cab	133	8.8 %
Confirmarea comenziise ataseaza.zip	77	5.1 %
Narudzba u prilogu.zip	68	4.5 %
UA0927282828.zip	60	4.0 %
PAYMENT COLLECTION.zip	48	3.2 %
Novi popis narudzbenica.zip	38	2.5 %
EU-Business-Register.pdf	33	2.2 %
PO42536383092872.zip	30	2.0 %
DOC032426277828.DOC.zip	30	2.0 %
order list isattached.zip	24	1.6 %
Yudo Overdue Invoices.zip	23	1.5 %
504885 506993 506997 - 2022.xlsx	22	1.5 %
Quotation Sheet.img	16	1.1 %
efax.html	15	1.0 %
CONTRACT-023536274 PURCHASE ORDER PROFORMA.img	14	0.9 %
Noua lista de comenzi.zip	14	0.9 %
artículos de orden de compra.pdf.zip	14	0.9 %
=?utf-8?B?5oC75b2VLmRvY3g=?=	13	0.9 %
2 months salary receipt.img	12	0.8 %
=?utf-8?B?5Lq65bel5pm66IO95LiO5py65Zmo6KeG6KeJ566X5rOV5a6e5oiYLmRvY3g=?=	12	0.8 %
nova lista narudzbi Astra Auto d.o.o.zip	12	0.8 %
Novi poredak.zip	10	0.7 %
Cotizaci	8	0.5 %
=?utf-8?B?MjAyMuesrOS4gOacn+eglOS/ruePrei1hOaWmS5kb2N4?=	8	0.5 %
Orden de Compra Urgente 1.zip	8	0.5 %
ZITAT #29042022.rar	7	0.5 %
MA TEMPLATE.xlsx	7	0.5 %
Shipping Documents_pfd.cab	7	0.5 %
INNOVINC.xls	7	0.5 %
Others	348	23.1 %
Total	**1.51k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


GenericRXRS-TZ!83909B2F69ED
Downloader-FCIV!AFE459CE8110
Downloader-FCIV!0BD1DEAABEBA
HTML/Phishing.jt
AgentTesla-FDHR!DB52E3C78A4D
AgentTesla-FCSO!B3D8F39CAE74
RDN/GenericAC
X97M/Downloader.ol
GenericRXQA-LQ!9E25268B6A9A
Fareit.gen.e
Exploit-CVE2017-11882.o
Downloader-FCIV!5C9CC5E9D182
GenericRXRY-ZG!FB97D937A198
GenericRXRU-WN!5906534A0382
Fareit.gen.a
HTML/Phishing.ec
GenericRXSM-NK!60EA5E658AED
X97M/Downloader.or
Downloader-FCIV!72976A7CEB49
AgentTesla-FDIL!55B5DB3E3537
Exploit-CVE2017-11882.bu
AgentTesla-FDHR!EA7BF6C6DFD2
NSIS/ObfusInjector.h
Exploit-CVE2017-11882.yx
Unknown
Medium Risk
High Risk
Total
2.55k
Hits
Not Available
Malicious

Report

Scan Result	Hits	%
Malicious	**1.28k**	**50.2 %**
File_Microsoft-Windows-Executable	878	34.4 %
File_Zip-Archive	180	7.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	69	2.7 %
File_Rar-Archive	67	2.6 %
File_PDF	24	0.9 %
File_ISO-9660-Disk-Image	22	0.9 %
File_HTML	15	0.6 %
File_7z-Archive	9	0.4 %
File_Type-Unknown	6	0.2 %
File_Microsoft-Excel-97-Spreadsheet	2	0.1 %
File_Microsoft-Equation-Editor-Document	2	0.1 %
File_LhArc-Archive	2	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %
File_ACE-Archive	1	0.0 %
File_XZ-Archive	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	1	0.0 %
Not Available	**776**	**30.4 %**
File_Zip-Archive	767	30.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.4 %
High Risk	**295**	**11.6 %**
File_Microsoft-Windows-Executable	151	5.9 %
File_Zip-Archive	63	2.5 %
File_Microsoft-Cabinet-Archive	23	0.9 %
File_Rar-Archive	19	0.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	16	0.6 %
File_Microsoft-Excel-97-Spreadsheet	7	0.3 %
File_Microsoft-Equation-Editor-Document	6	0.2 %
File_ISO-9660-Disk-Image	5	0.2 %
File_Type-Unknown	3	0.1 %
File_HTML	1	0.0 %
File_7z-Archive	1	0.0 %
Medium Risk	**59**	**2.3 %**
File_Zip-Archive	21	0.8 %
File_PDF	14	0.5 %

Report

Scan Result	Hits	%
File_Microsoft-Office-Open-XML-Document	14	0.5 %
File_Microsoft-OLE	3	0.1 %
File_Microsoft-Windows-Executable	2	0.1 %
File_Microsoft-Cabinet-Archive	2	0.1 %
File_XML	2	0.1 %
File_Encrypted-Zip-Archive	1	0.0 %
Unknown	**28**	**1.1 %**
File_Zip-Archive	28	1.1 %
Exploit-CVE2017-11882.yx	**23**	**0.9 %**
File_Microsoft-Excel-XLSX-Filename-Extension	22	0.9 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
NSIS/ObfusInjector.h	**18**	**0.7 %**
File_ISO-9660-Disk-Image	16	0.6 %
File_Rar-Archive	2	0.1 %
AgentTesla-FDHR!EA7BF6C6DFD2	**13**	**0.5 %**
File_ISO-9660-Disk-Image	13	0.5 %
Exploit-CVE2017-11882.bu	**9**	**0.4 %**
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.4 %
AgentTesla-FDIL!55B5DB3E3537	**7**	**0.3 %**
File_Rar-Archive	7	0.3 %
Downloader-FCIV!72976A7CEB49	**6**	**0.2 %**
File_ISO-9660-Disk-Image	6	0.2 %
X97M/Downloader.or	**6**	**0.2 %**
File_Microsoft-Excel-97-Spreadsheet	5	0.2 %
File_Zip-Archive	1	0.0 %
GenericRXSM-NK!60EA5E658AED	**5**	**0.2 %**
File_Tar-Archive	5	0.2 %
HTML/Phishing.ec	**3**	**0.1 %**
File_HTML	3	0.1 %
Fareit.gen.a	**3**	**0.1 %**
File_ACE-Archive	3	0.1 %
GenericRXRU-WN!5906534A0382	**2**	**0.1 %**
File_Rar-Archive	1	0.0 %
File_ISO-9660-Disk-Image	1	0.0 %
GenericRXRY-ZG!FB97D937A198	**2**	**0.1 %**
File_7z-Archive	2	0.1 %

Report

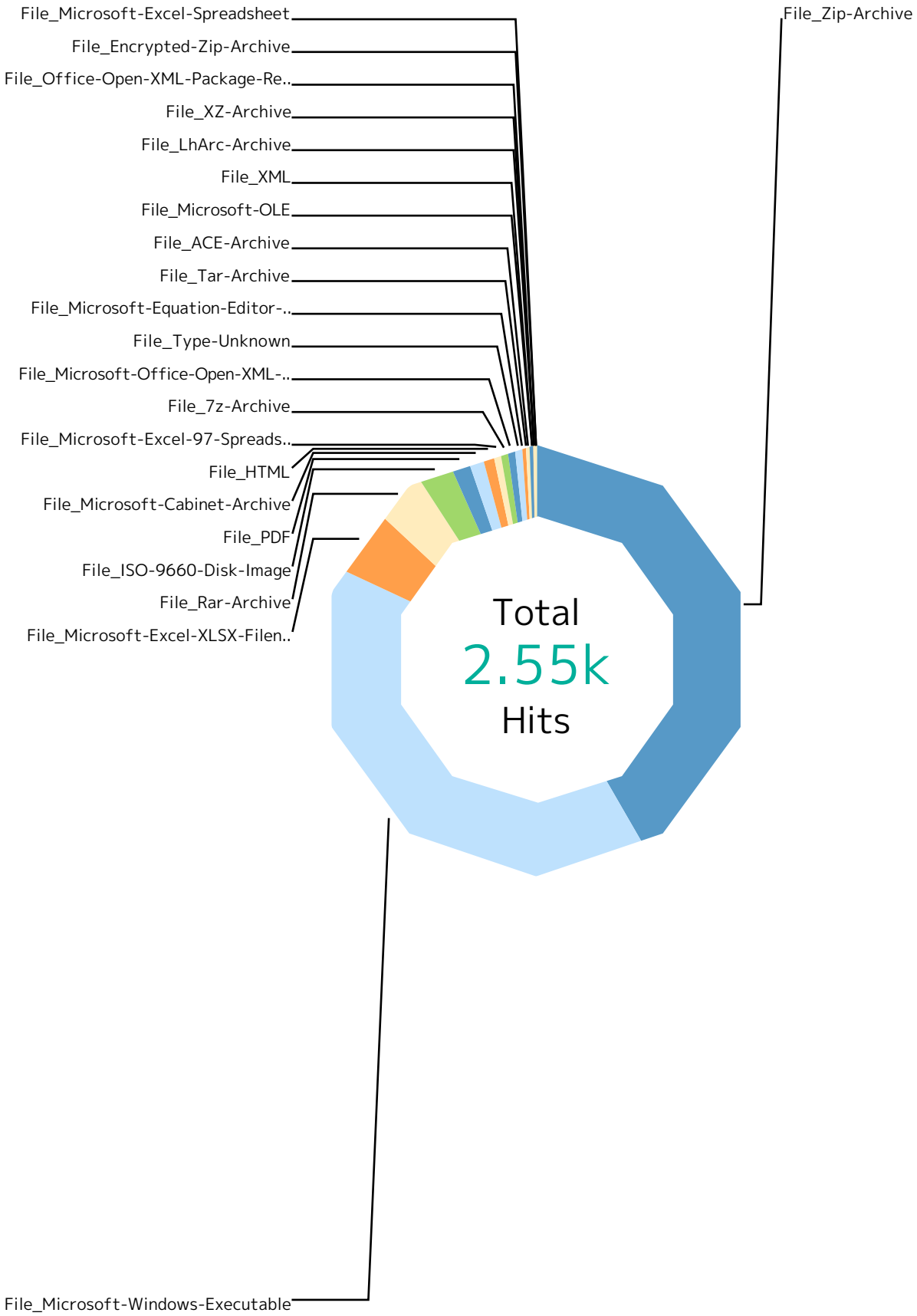
Scan Result	Hits	%
Downloader-FCIV!5C9CC5E9D182	**2**	**0.1 %**
File_Zip-Archive	2	0.1 %
Exploit-CVE2017-11882.o	**2**	**0.1 %**
File_Type-Unknown	2	0.1 %
Fareit.gen.e	**2**	**0.1 %**
File_ACE-Archive	2	0.1 %
GenericRXQA-LQ!9E25268B6A9A	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
X97M/Downloader.ol	**1**	**0.0 %**
File_Microsoft-Excel-97-Spreadsheet	1	0.0 %
RDN/GenericAC	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
AgentTesla-FCSO!B3D8F39CAE74	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
AgentTesla-FDHR!DB52E3C78A4D	**1**	**0.0 %**
File_ISO-9660-Disk-Image	1	0.0 %
HTML/Phishing.jt	**1**	**0.0 %**
File_HTML	1	0.0 %
Downloader-FCIV!0BD1DEAABEBA	**1**	**0.0 %**
File_7z-Archive	1	0.0 %
Downloader-FCIV!AFE459CE8110	**1**	**0.0 %**
File_7z-Archive	1	0.0 %
GenericRXRS-TZ!83909B2F69ED	**1**	**0.0 %**
File_Microsoft-Cabinet-Archive	1	0.0 %
Total	**2.55k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Microsoft-Excel-Spreadsheet
File_Encrypted-Zip-Archive
File_Office-Open-XML-Package-Re..
File_XZ-Archive
File_LhArc-Archive
File_XML
File_Microsoft-OLE
File_ACE-Archive
File_Tar-Archive
File_Microsoft-Equation-Editor-..
File_Type-Unknown
File_Microsoft-Office-Open-XML-..
File_7z-Archive
File_Microsoft-Excel-97-Spreads..
File_HTML
File_Microsoft-Cabinet-Archive
File_PDF
File_ISO-9660-Disk-Image
File_Rar-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Zip-Archive
File_Microsoft-Windows-Executable
Total
2.55k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**1.06k**	**41.7 %**
Not Available	767	30.1 %
Malicious	180	7.1 %
High Risk	63	2.5 %
Unknown	28	1.1 %
Medium Risk	21	0.8 %
Downloader-FCIV!5C9CC5E9D182	2	0.1 %
X97M/Downloader.or	1	0.0 %
AgentTesla-FCSO!B3D8F39CAE74	1	0.0 %
File_Microsoft-Windows-Executable	**1.03k**	**40.4 %**
Malicious	878	34.4 %
High Risk	151	5.9 %
Medium Risk	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**125**	**4.9 %**
Malicious	69	2.7 %
Exploit-CVE2017-11882.yx	22	0.9 %
High Risk	16	0.6 %
Not Available	9	0.4 %
Exploit-CVE2017-11882.bu	9	0.4 %
File_Rar-Archive	**99**	**3.9 %**
Malicious	67	2.6 %
High Risk	19	0.7 %
AgentTesla-FDIL!55B5DB3E3537	7	0.3 %
NSIS/ObfusInjector.h	2	0.1 %
GenericRXQA-LQ!9E25268B6A9A	2	0.1 %
GenericRXRU-WN!5906534A0382	1	0.0 %
RDN/GenericAC	1	0.0 %
File_ISO-9660-Disk-Image	**64**	**2.5 %**
Malicious	22	0.9 %
NSIS/ObfusInjector.h	16	0.6 %
AgentTesla-FDHR!EA7BF6C6DFD2	13	0.5 %
Downloader-FCIV!72976A7CEB49	6	0.2 %
High Risk	5	0.2 %
GenericRXRU-WN!5906534A0382	1	0.0 %
AgentTesla-FDHR!DB52E3C78A4D	1	0.0 %
File_PDF	**38**	**1.5 %**

Report

Responding Scanner	Hits	%
Malicious	24	0.9 %
Medium Risk	14	0.5 %
File_Microsoft-Cabinet-Archive	**27**	**1.1 %**
High Risk	23	0.9 %
Medium Risk	2	0.1 %
Malicious	1	0.0 %
GenericRXRS-TZ!83909B2F69ED	1	0.0 %
File_HTML	**20**	**0.8 %**
Malicious	15	0.6 %
HTML/Phishing.ec	3	0.1 %
High Risk	1	0.0 %
HTML/Phishing.jt	1	0.0 %
File_Microsoft-Excel-97-Spreadsheet	**15**	**0.6 %**
High Risk	7	0.3 %
X97M/Downloader.or	5	0.2 %
Malicious	2	0.1 %
X97M/Downloader.ol	1	0.0 %
File_7z-Archive	**14**	**0.5 %**
Malicious	9	0.4 %
GenericRXRY-ZG!FB97D937A198	2	0.1 %
High Risk	1	0.0 %
Downloader-FCIV!0BD1DEAABEBA	1	0.0 %
Downloader-FCIV!AFE459CE8110	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**14**	**0.5 %**
Medium Risk	14	0.5 %
File_Type-Unknown	**11**	**0.4 %**
Malicious	6	0.2 %
High Risk	3	0.1 %
Exploit-CVE2017-11882.o	2	0.1 %
File_Microsoft-Equation-Editor-Document	**8**	**0.3 %**
High Risk	6	0.2 %
Malicious	2	0.1 %
File_Tar-Archive	**6**	**0.2 %**
GenericRXSM-NK!60EA5E658AED	5	0.2 %
Malicious	1	0.0 %
File_ACE-Archive	**6**	**0.2 %**

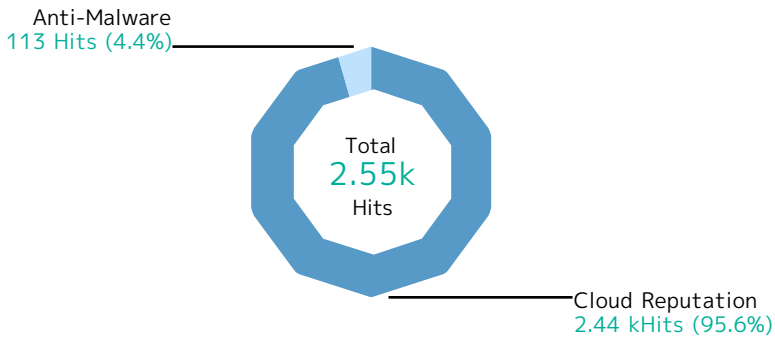
Report

Responding Scanner	Hits	%
Fareit.gen.a	3	0.1 %
Fareit.gen.e	2	0.1 %
Malicious	1	0.0 %
File_Microsoft-OLE	**3**	**0.1 %**
Medium Risk	3	0.1 %
File_XML	**2**	**0.1 %**
Medium Risk	2	0.1 %
File_LhArc-Archive	**2**	**0.1 %**
Malicious	2	0.1 %
File_XZ-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**1**	**0.0 %**
Malicious	1	0.0 %
File_Encrypted-Zip-Archive	**1**	**0.0 %**
Medium Risk	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.0 %**
Exploit-CVE2017-11882.yx	1	0.0 %
Total	**2.55k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**2.44k**	**95.6 %**
File_Zip-Archive	1.06k	41.5 %
File_Microsoft-Windows-Executable	1.03k	40.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	94	3.7 %
File_Rar-Archive	86	3.4 %
File_PDF	38	1.5 %
File_ISO-9660-Disk-Image	27	1.1 %
File_Microsoft-Cabinet-Archive	26	1.0 %
File_HTML	16	0.6 %
File_Microsoft-Office-Open-XML-Document	14	0.5 %
File_7z-Archive	10	0.4 %
File_Microsoft-Excel-97-Spreadsheet	9	0.4 %
File_Type-Unknown	9	0.4 %
File_Microsoft-Equation-Editor-Document	8	0.3 %
File_Microsoft-OLE	3	0.1 %
File_XML	2	0.1 %
File_LhArc-Archive	2	0.1 %
File_Tar-Archive	1	0.0 %
File_ACE-Archive	1	0.0 %
File_XZ-Archive	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	1	0.0 %
File_Encrypted-Zip-Archive	1	0.0 %
Anti-Malware	**113**	**4.4 %**
File_ISO-9660-Disk-Image	37	1.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	31	1.2 %
File_Rar-Archive	13	0.5 %
File_Microsoft-Excel-97-Spreadsheet	6	0.2 %
File_Tar-Archive	5	0.2 %
File_ACE-Archive	5	0.2 %
File_Zip-Archive	4	0.2 %
File_HTML	4	0.2 %
File_7z-Archive	4	0.2 %
File_Type-Unknown	2	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Total	**2.55k**	**100 %**

Report

Virenfilterung SRC IPs

Located 86.2 %

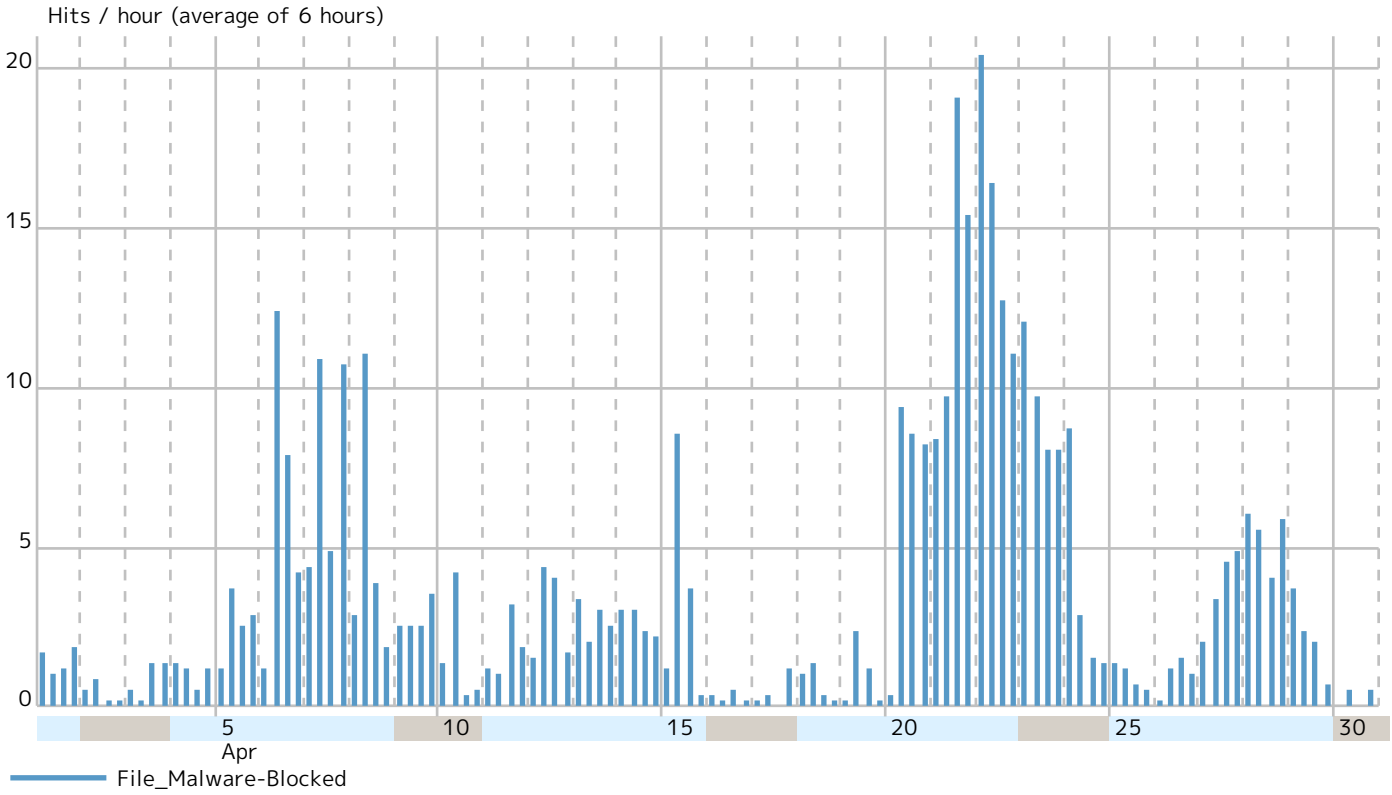
Report

Records by src IP		Hits	%
193.233.182.127	Sterling, Virginia 20167, United States	780	30.6 %
80.86.231.190	Armenia	310	12.1 %
46.101.115.6	Frankfurt am Main, Germany	266	10.4 %
103.132.95.100	Dhaka, Bangladesh	142	5.6 %
200.79.181.78	Pachuca, Mexico	130	5.1 %
37.221.123.179	Bulgaria	110	4.3 %
193.149.2.155	Bulgaria	89	3.5 %
78.111.59.147	Baku, Azerbaijan	54	2.1 %
200.155.36.3	Londrina, Brazil	38	1.5 %
180.149.253.33	Hong Kong	34	1.3 %
162.212.158.174	United States	29	1.1 %
185.102.170.230	Ashburn, Virginia 20149, United States	23	0.9 %
95.217.56.172	Helsinki, Finland	22	0.9 %
108.62.12.195	United States	16	0.6 %
178.159.240.152	Belarus	15	0.6 %
138.185.176.11	Orobo, Brazil	15	0.6 %
204.140.21.16	Rancho Cordova, California 95741, United States	14	0.5 %
195.62.47.177	Dallas, Texas 75247, United States	14	0.5 %
122.155.180.15	Thailand	12	0.5 %
45.144.153.211	Bulgaria	10	0.4 %
194.31.98.145	Gambrills, Maryland 21054, United States	10	0.4 %
212.192.246.40	Germany	9	0.4 %
45.144.178.180	Novosibirsk, Russia	8	0.3 %
23.254.215.52	Decatur, Texas 76234, United States	8	0.3 %
27.254.148.187	Thailand	8	0.3 %
170.39.212.249	Dallas, Texas 75247, United States	7	0.3 %
104.168.148.87	United States	7	0.3 %
203.101.175.37	Karachi, Pakistan	7	0.3 %
118.91.235.32	India	7	0.3 %
201.234.19.252	San Martin, Argentina	6	0.2 %
Others		352	13.8 %
Total		**2.55k**	**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.