Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period
From: 2022-01-01 00:00:00
To: 2022-02-01 00:00:00

Report

Report run by
jens

SMC version
6.10.5, build 11136

Update version
1430

Report started
2022-02-01 08:23:52

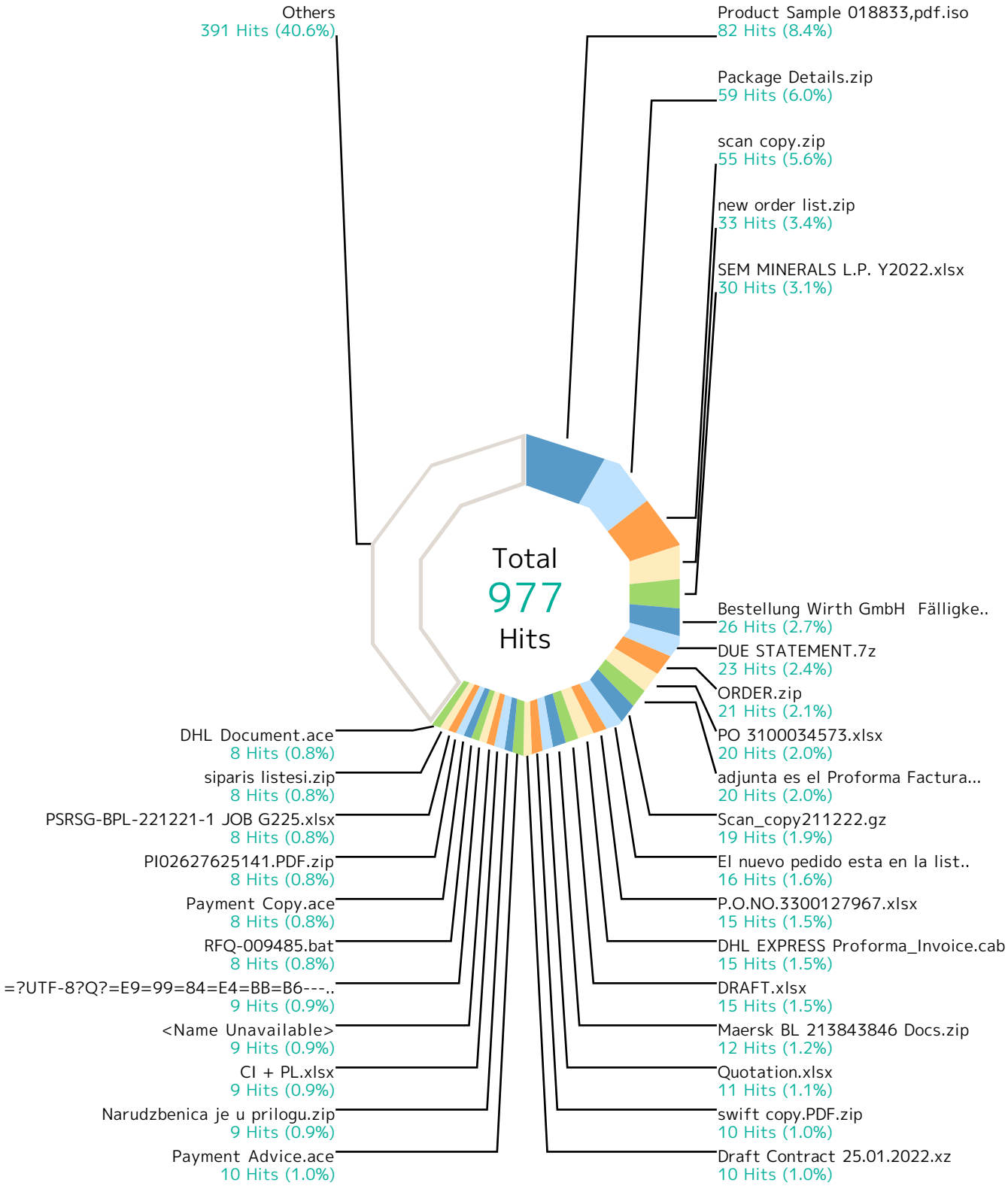
Report run time
01:51:23

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



Report

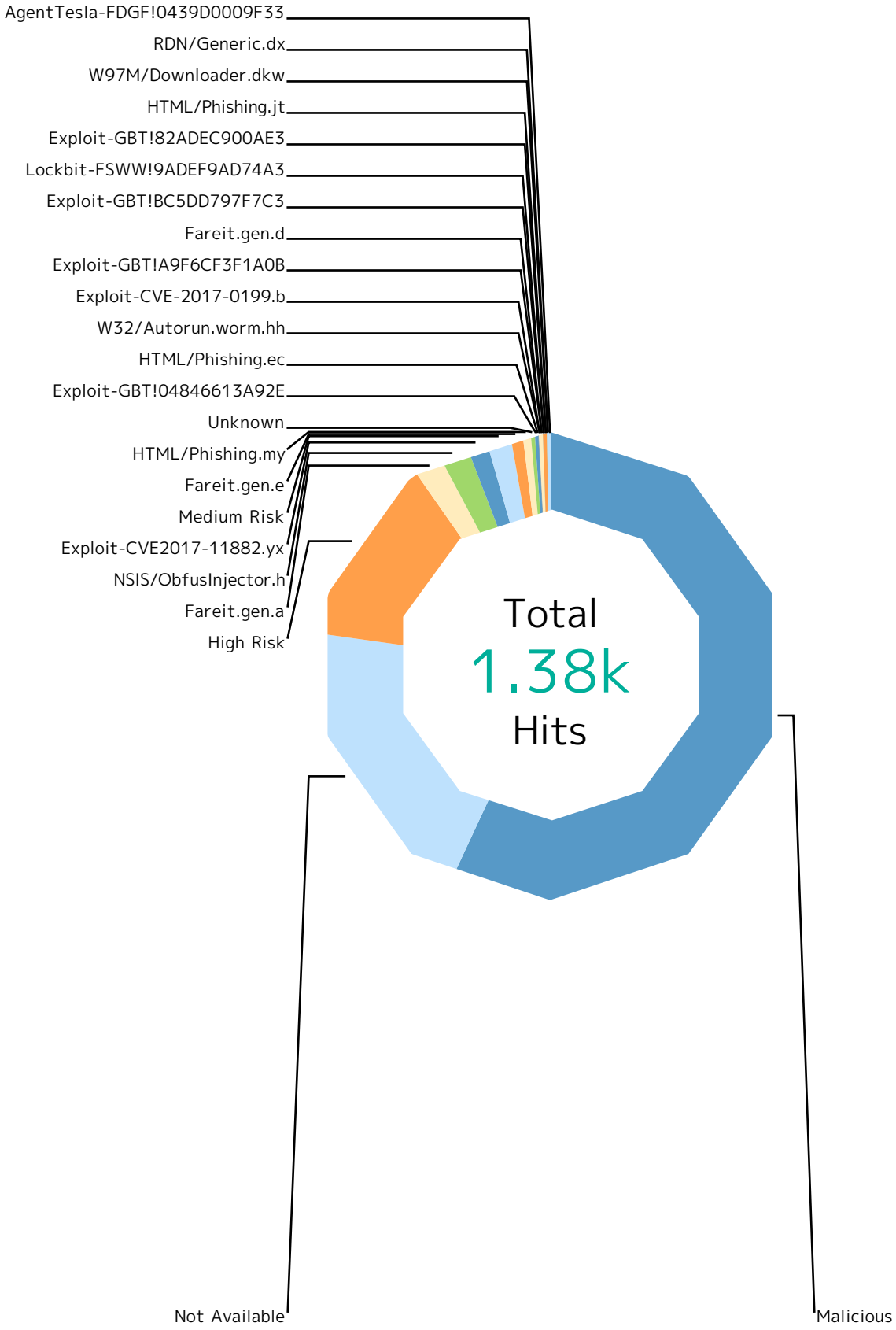
Records by file name	Hits	%
Product Sample 018833,pdf.iso	82	8.4 %
Package Details.zip	59	6.0 %
scan copy.zip	55	5.6 %
new order list.zip	33	3.4 %
SEM MINERALS L.P. Y2022.xlsx	30	3.1 %
Bestellung Wirth GmbH Fälligkeit 30.01	26	2.7 %
DUE STATEMENT.7z	23	2.4 %
ORDER.zip	21	2.1 %
PO 3100034573.xlsx	20	2.0 %
adjunta es el Proforma Factura.zip	20	2.0 %
Scan_copy211222.gz	19	1.9 %
El nuevo pedido esta en la lista..zip	16	1.6 %
P.O.NO.3300127967.xlsx	15	1.5 %
DHL EXPRESS Proforma_Invoice.cab	15	1.5 %
DRAFT.xlsx	15	1.5 %
Maersk BL 213843846 Docs.zip	12	1.2 %
Quotation.xlsx	11	1.1 %
swift copy.PDF.zip	10	1.0 %
Draft Contract 25.01.2022.xz	10	1.0 %
Payment Advice.ace	10	1.0 %
Narudzbenica je u prilogu.zip	9	0.9 %
CI + PL.xlsx	9	0.9 %
<Name Unavailable>	9	0.9 %
=?UTF-8?Q?=E9=99=84=E4=BB=B6----Python.docx?=	9	0.9 %
RFQ-009485.bat	8	0.8 %
Payment Copy.ace	8	0.8 %
PI02627625141.PDF.zip	8	0.8 %
PSRSG-BPL-221221-1 JOB G225.xlsx	8	0.8 %
siparis listesi.zip	8	0.8 %
DHL Document.ace	8	0.8 %
Others	391	40.0 %
Total	**977**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


AgentTesla-FDGF!0439D0009F33
RDN/Generic.dx
W97M/Downloader.dkw
HTML/Phishing.jt
Exploit-GBT!82ADEC900AE3
Lockbit-FSWW!9ADEF9AD74A3
Exploit-GBT!BC5DD797F7C3
Fareit.gen.d
Exploit-GBT!A9F6CF3F1A0B
Exploit-CVE-2017-0199.b
W32/Autorun.worm.hh
HTML/Phishing.ec
Exploit-GBT!04846613A92E
Unknown
HTML/Phishing.my
Fareit.gen.e
Medium Risk
Exploit-CVE2017-11882.yx
NSIS/ObfusInjector.h
Fareit.gen.a
High Risk
Total
1.38k
Hits
Not Available
Malicious

Report

Scan Result	Hits	%
Malicious	**783**	**56.9 %**
File_Microsoft-Windows-Executable	325	23.6 %
File_ISO-9660-Disk-Image	132	9.6 %
File_Zip-Archive	97	7.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	97	7.0 %
File_Rar-Archive	60	4.4 %
File_Microsoft-Equation-Editor-Document	20	1.5 %
File_Microsoft-Cabinet-Archive	13	0.9 %
File_ACE-Archive	10	0.7 %
File_Microsoft-Excel-97-Spreadsheet	8	0.6 %
File_Microsoft-PowerPoint-97-Add-In	6	0.4 %
File_HTML	5	0.4 %
File_Microsoft-OLE	4	0.3 %
File_Type-Unknown	2	0.1 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_PDF	1	0.1 %
File_Microsoft-Windows-Compiled-Help	1	0.1 %
Not Available	**280**	**20.3 %**
File_Zip-Archive	260	18.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	17	1.2 %
File_Microsoft-Office-Open-XML-Document	3	0.2 %
High Risk	**180**	**13.1 %**
File_Microsoft-Windows-Executable	47	3.4 %
File_Rar-Archive	33	2.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	25	1.8 %
File_7z-Archive	23	1.7 %
File_Zip-Archive	19	1.4 %
File_Type-Unknown	10	0.7 %
File_ISO-9660-Disk-Image	9	0.7 %
File_Microsoft-Excel-97-Spreadsheet	5	0.4 %
File_Microsoft-Cabinet-Archive	4	0.3 %
File_ACE-Archive	3	0.2 %
File_Microsoft-OLE	1	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.1 %
Fareit.gen.a	**26**	**1.9 %**
File_ACE-Archive	26	1.9 %

Report

Scan Result	Hits	%
NSIS/ObfusInjector.h	**25**	**1.8 %**
File_ISO-9660-Disk-Image	14	1.0 %
File_Rar-Archive	8	0.6 %
File_Microsoft-Windows-Executable	2	0.1 %
File_Zip-Archive	1	0.1 %
Exploit-CVE2017-11882.yx	**22**	**1.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	21	1.5 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %
Medium Risk	**21**	**1.5 %**
File_Zip-Archive	10	0.7 %
File_Microsoft-Windows-Executable	7	0.5 %
File_JavaScript	4	0.3 %
Fareit.gen.e	**11**	**0.8 %**
File_ACE-Archive	11	0.8 %
HTML/Phishing.my	**7**	**0.5 %**
File_HTML	7	0.5 %
Unknown	**6**	**0.4 %**
File_Zip-Archive	6	0.4 %
Exploit-GBT!04846613A92E	**2**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
HTML/Phishing.ec	**2**	**0.1 %**
File_HTML	2	0.1 %
W32/Autorun.worm.hh	**1**	**0.1 %**
File_Rar-Archive	1	0.1 %
Exploit-CVE-2017-0199.b	**1**	**0.1 %**
File_Microsoft-Office-Open-XML-Document	1	0.1 %
Exploit-GBT!A9F6CF3F1A0B	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
Fareit.gen.d	**1**	**0.1 %**
File_ACE-Archive	1	0.1 %
Exploit-GBT!BC5DD797F7C3	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
Lockbit-FSWW!9ADEF9AD74A3	**1**	**0.1 %**
File_Rar-Archive	1	0.1 %
Exploit-GBT!82ADEC900AE3	**1**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %

Report

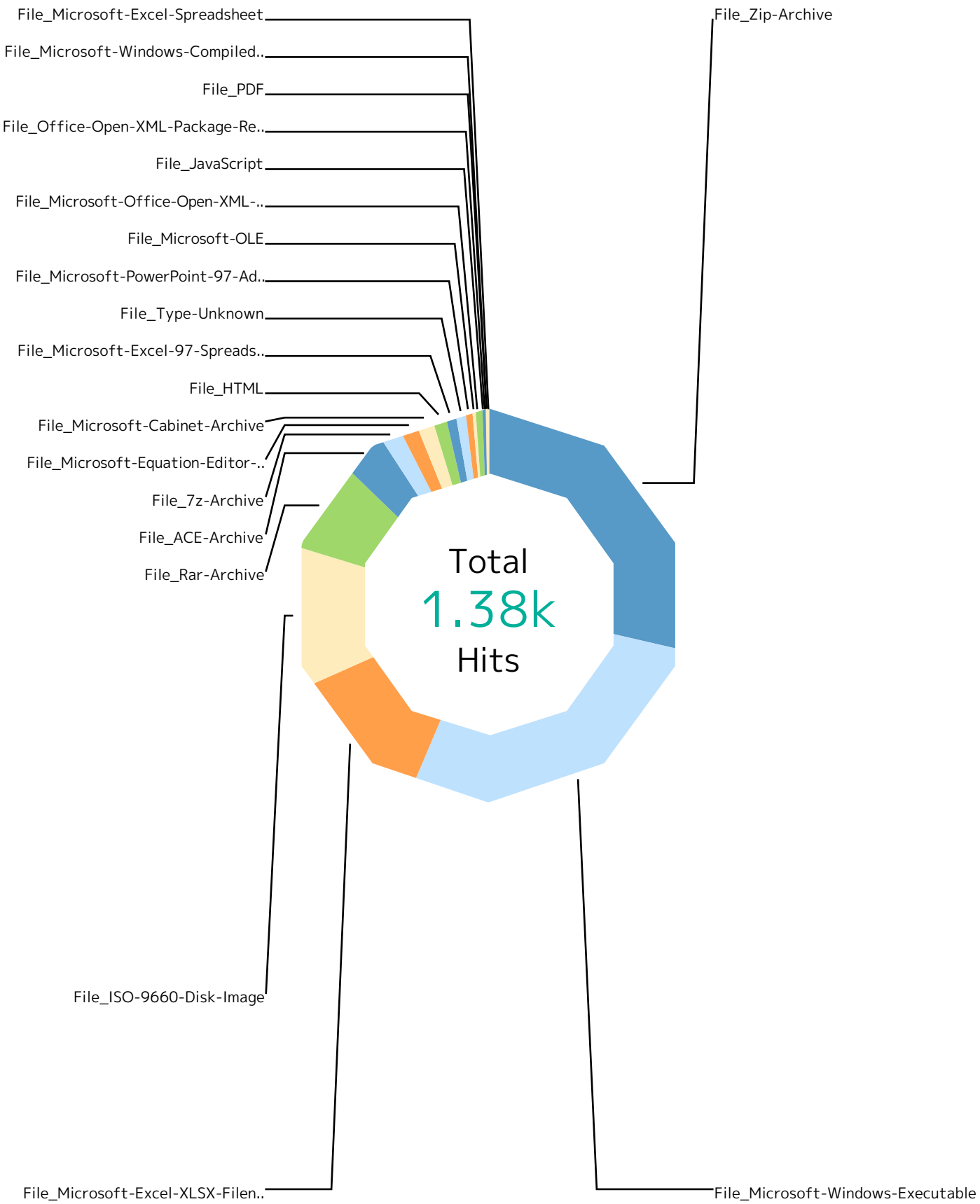
Scan Result	Hits	%
HTML/Phishing.jt	**1**	**0.1 %**
File_HTML	1	0.1 %
W97M/Downloader.dkw	**1**	**0.1 %**
File_Zip-Archive	1	0.1 %
RDN/Generic.dx	**1**	**0.1 %**
File_Zip-Archive	1	0.1 %
AgentTesla-FDGF!0439D0009F33	**1**	**0.1 %**
File_Microsoft-Cabinet-Archive	1	0.1 %
Total	**1.38k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Microsoft-Excel-Spreadsheet
File_Microsoft-Windows-Compiled..
File_PDF
File_Office-Open-XML-Package-Re..
File_JavaScript
File_Microsoft-Office-Open-XML-..
File_Microsoft-OLE
File_Microsoft-PowerPoint-97-Ad..
File_Type-Unknown
File_Microsoft-Excel-97-Spreads..
File_HTML
File_Microsoft-Cabinet-Archive
File_Microsoft-Equation-Editor-..
File_7z-Archive
File_ACE-Archive
File_Rar-Archive
File_Zip-Archive
Total
1.38k
Hits
File_ISO-9660-Disk-Image
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**395**	**28.7 %**
Not Available	260	18.9 %
Malicious	97	7.0 %
High Risk	19	1.4 %
Medium Risk	10	0.7 %
Unknown	6	0.4 %
NSIS/ObfusInjector.h	1	0.1 %
W97M/Downloader.dkw	1	0.1 %
RDN/Generic.dx	1	0.1 %
File_Microsoft-Windows-Executable	**381**	**27.7 %**
Malicious	325	23.6 %
High Risk	47	3.4 %
Medium Risk	7	0.5 %
NSIS/ObfusInjector.h	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**165**	**12.0 %**
Malicious	97	7.0 %
High Risk	25	1.8 %
Exploit-CVE2017-11882.yx	21	1.5 %
Not Available	17	1.2 %
Exploit-GBT!04846613A92E	2	0.1 %
Exploit-GBT!A9F6CF3F1A0B	1	0.1 %
Exploit-GBT!BC5DD797F7C3	1	0.1 %
Exploit-GBT!82ADEC900AE3	1	0.1 %
File_ISO-9660-Disk-Image	**155**	**11.3 %**
Malicious	132	9.6 %
NSIS/ObfusInjector.h	14	1.0 %
High Risk	9	0.7 %
File_Rar-Archive	**103**	**7.5 %**
Malicious	60	4.4 %
High Risk	33	2.4 %
NSIS/ObfusInjector.h	8	0.6 %
W32/Autorun.worm.hh	1	0.1 %
Lockbit-FSWW!9ADEF9AD74A3	1	0.1 %
File_ACE-Archive	**51**	**3.7 %**
Fareit.gen.a	26	1.9 %
Fareit.gen.e	11	0.8 %

Report

Responding Scanner	Hits	%
Malicious	10	0.7 %
High Risk	3	0.2 %
Fareit.gen.d	1	0.1 %
File_7z-Archive	**23**	**1.7 %**
High Risk	23	1.7 %
File_Microsoft-Equation-Editor-Document	**20**	**1.5 %**
Malicious	20	1.5 %
File_Microsoft-Cabinet-Archive	**18**	**1.3 %**
Malicious	13	0.9 %
High Risk	4	0.3 %
AgentTesla-FDGF!0439D0009F33	1	0.1 %
File_HTML	**15**	**1.1 %**
HTML/Phishing.my	7	0.5 %
Malicious	5	0.4 %
HTML/Phishing.ec	2	0.1 %
HTML/Phishing.jt	1	0.1 %
File_Microsoft-Excel-97-Spreadsheet	**13**	**0.9 %**
Malicious	8	0.6 %
High Risk	5	0.4 %
File_Type-Unknown	**12**	**0.9 %**
High Risk	10	0.7 %
Malicious	2	0.1 %
File_Microsoft-PowerPoint-97-Add-In	**6**	**0.4 %**
Malicious	6	0.4 %
File_Microsoft-OLE	**5**	**0.4 %**
Malicious	4	0.3 %
High Risk	1	0.1 %
File_Microsoft-Office-Open-XML-Document	**5**	**0.4 %**
Not Available	3	0.2 %
Exploit-CVE2017-11882.yx	1	0.1 %
Exploit-CVE-2017-0199.b	1	0.1 %
File_JavaScript	**4**	**0.3 %**
Medium Risk	4	0.3 %
File_Office-Open-XML-Package-Relations-Item	**2**	**0.1 %**
Malicious	2	0.1 %
File_PDF	**1**	**0.1 %**

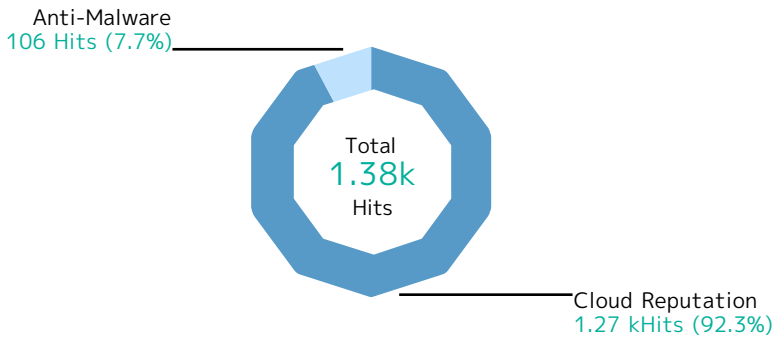
Report

Responding Scanner	Hits	%
Malicious	1	0.1 %
File_Microsoft-Windows-Compiled-Help	**1**	**0.1 %**
Malicious	1	0.1 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.1 %**
High Risk	1	0.1 %
Total	**1.38k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**1.27k**	**92.3 %**
File_Zip-Archive	392	28.5 %
File_Microsoft-Windows-Executable	379	27.5 %
File_ISO-9660-Disk-Image	141	10.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	139	10.1 %
File_Rar-Archive	93	6.8 %
File_7z-Archive	23	1.7 %
File_Microsoft-Equation-Editor-Document	20	1.5 %
File_Microsoft-Cabinet-Archive	17	1.2 %
File_ACE-Archive	13	0.9 %
File_Microsoft-Excel-97-Spreadsheet	13	0.9 %
File_Type-Unknown	12	0.9 %
File_Microsoft-PowerPoint-97-Add-In	6	0.4 %
File_HTML	5	0.4 %
File_Microsoft-OLE	5	0.4 %
File_JavaScript	4	0.3 %
File_Microsoft-Office-Open-XML-Document	3	0.2 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_PDF	1	0.1 %
File_Microsoft-Windows-Compiled-Help	1	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.1 %
Anti-Malware	**106**	**7.7 %**
File_ACE-Archive	38	2.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	26	1.9 %
File_ISO-9660-Disk-Image	14	1.0 %
File_Rar-Archive	10	0.7 %
File_HTML	10	0.7 %
File_Zip-Archive	3	0.2 %
File_Microsoft-Windows-Executable	2	0.1 %
File_Microsoft-Office-Open-XML-Document	2	0.1 %
File_Microsoft-Cabinet-Archive	1	0.1 %
Total	**1.38k**	**100 %**

Report

Virenfilterung SRC IPs

Located 76.2 %

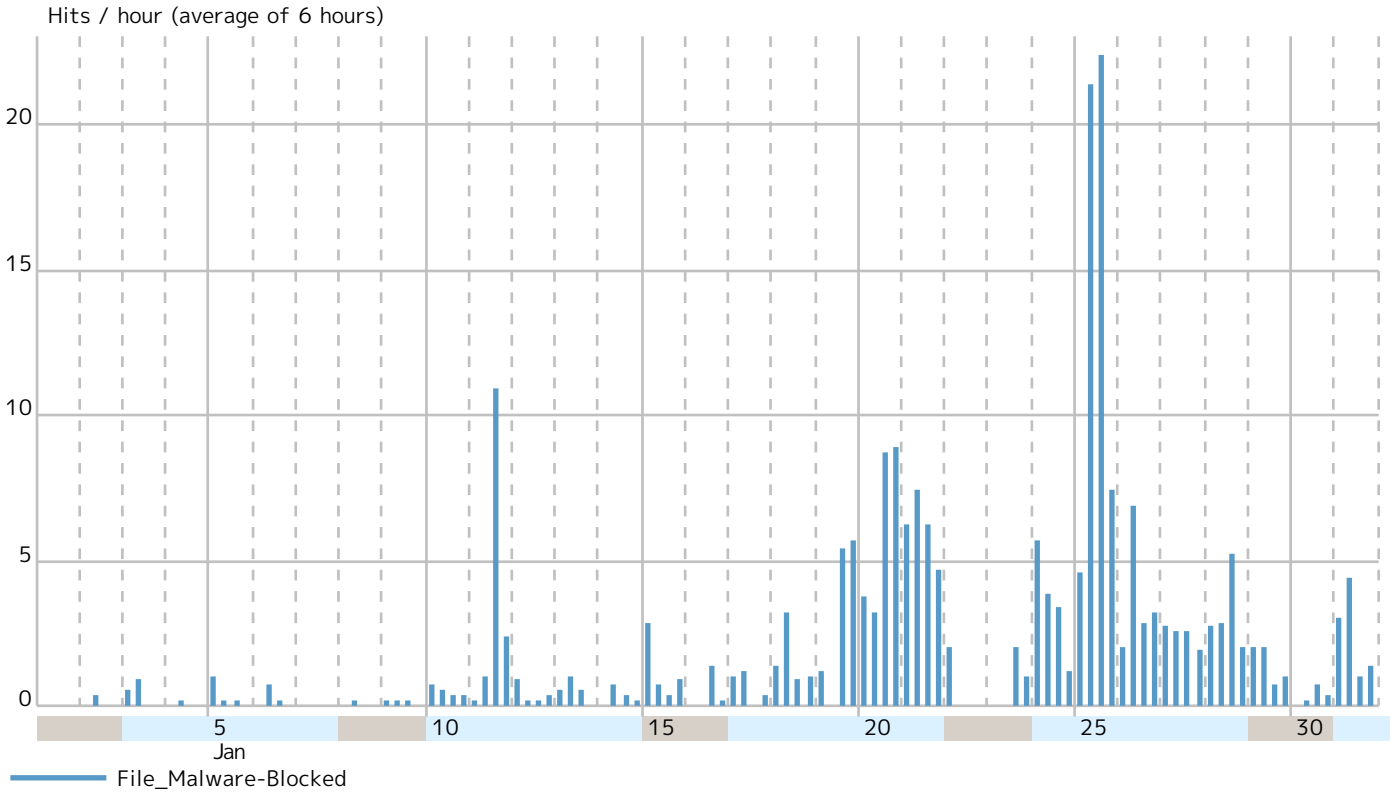
Report

Records by src IP		Hits	%
185.46.188.30	Ukraine	199	14.5 %
27.90.196.178	Itabashi-ku, Japan	117	8.5 %
103.108.48.251	India	110	8.0 %
89.163.209.160	Germany	82	6.0 %
103.82.21.65	Vietnam	56	4.1 %
45.137.22.134	Bangladesh	45	3.3 %
193.34.69.55	Germany	38	2.8 %
103.93.59.117	Indonesia	38	2.8 %
23.254.226.220	United States	38	2.8 %
192.254.160.121	United States	28	2.0 %
159.223.151.14	North Bergen, New Jersey 07047, United States	24	1.7 %
185.222.57.176	Amsterdam, Netherlands	23	1.7 %
2.58.149.111	Dulles, Virginia 20103, United States	20	1.5 %
185.4.132.177	Greece	19	1.4 %
117.20.109.230	Japan	18	1.3 %
82.223.80.112	Spain	16	1.2 %
159.89.156.42	Santa Clara, California 95051, United States	16	1.2 %
37.32.98.99	Spain	16	1.2 %
67.205.189.27	North Bergen, New Jersey 07047, United States	16	1.2 %
128.201.31.243	Salvador, Brazil	14	1.0 %
2.56.59.36	Dulles, Virginia 20103, United States	14	1.0 %
167.99.8.232	North Bergen, New Jersey 07047, United States	13	0.9 %
93.95.245.45	Kazakhstan	13	0.9 %
218.29.12.41	China	13	0.9 %
27.254.148.187	Thailand	11	0.8 %
103.28.52.162	Indonesia	11	0.8 %
167.172.183.104	Frankfurt am Main, Germany	10	0.7 %
94.75.199.75	Netherlands	10	0.7 %
89.252.178.117	Turkey	10	0.7 %
202.116.160.34	China	10	0.7 %
Others		328	23.8 %
Total		**1.38k**	**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.