Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2022-11-01 00:00:00 CET
To: 2022-12-01 00:00:00 CET

Report

Table of Contents

Report run by
jens

SMC version
6.11.2, build 11221

Update version
1531

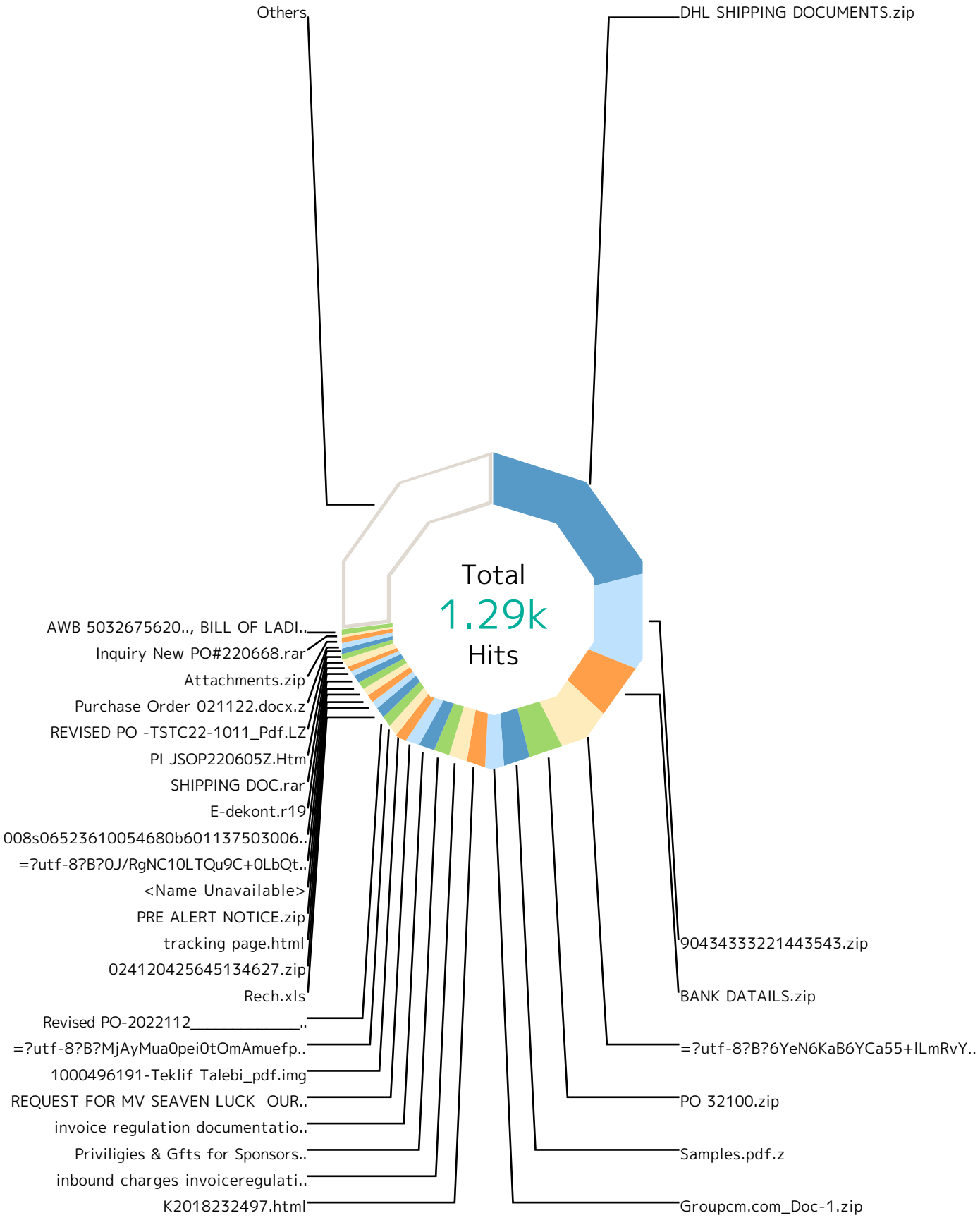
Report started
2022-12-01 10:38:39 CET

Report run time
02:10:47

Filters used
Match All

Report

Virenfilterung MXe



Report

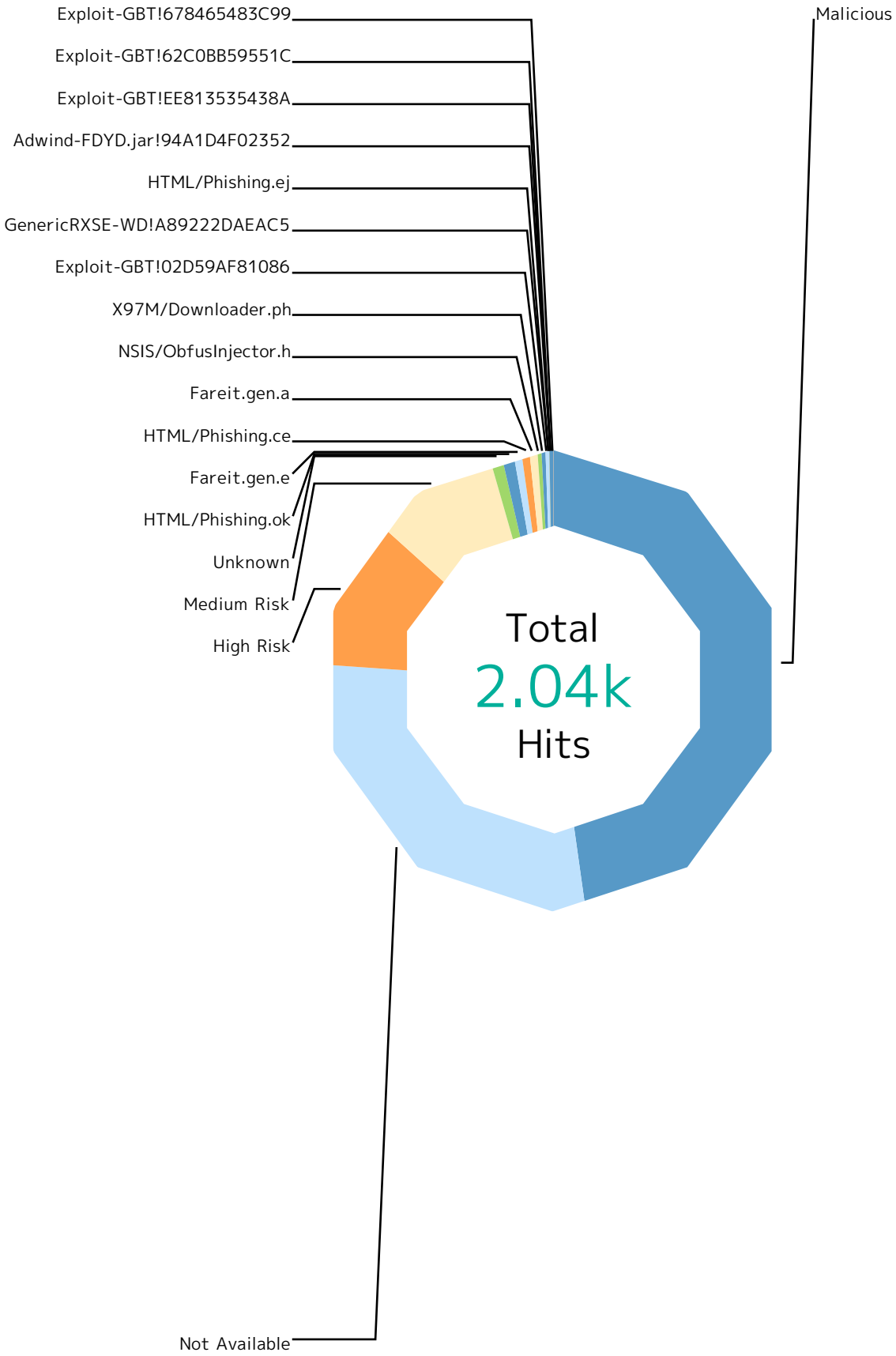
Records by file name	Hits	%
DHL SHIPPING DOCUMENTS.zip	272	21.2 %
90434333221443543.zip	127	9.9 %
BANK DATAILS.zip	77	6.0 %
=?utf-8?B?6YeN6KaB6YCa55+ILmRvY3g=?=	70	5.4 %
PO 32100.zip	48	3.7 %
Samples.pdf.z	33	2.6 %
Groupcm.com_Doc-1.zip	28	2.2 %
K2018232497.html	25	1.9 %
inbound charges invoiceregulations.jpg.zip	25	1.9 %
Priviligies & Gfts for Sponsors & for Ye	21	1.6 %
invoice regulation documentation.JPG.zip	20	1.6 %
REQUEST FOR MV SEAVEN LUCK OUR REF SLU15022_pdf ..	17	1.3 %
1000496191-Teklif Talebi_pdf.img	17	1.3 %
=?utf-8?B?MjAyMua0pei0tOmAmuefpS5kb2N4?=	14	1.1 %
Revised PO-2022112_____.gz.zip	14	1.1 %
Rech.xls	13	1.0 %
024120425645134627.zip	13	1.0 %
tracking page.html	10	0.8 %
PRE ALERT NOTICE.zip	10	0.8 %
<Name Unavailable>	10	0.8 %
=?utf-8?B?0J/RgNC10LTQu9C+0LbQtdC90LjQtS5kb2N4?=	10	0.8 %
008s06523610054680b6011375030062022.pdf.rar	9	0.7 %
E-dekont.r19	8	0.6 %
SHIPPING DOC.rar	8	0.6 %
PI JSOP220605Z.Htm	7	0.5 %
REVISED PO -TSTC22-1011_Pdf.LZ	7	0.5 %
Purchase Order 021122.docx.z	7	0.5 %
Attachments.zip	7	0.5 %
Inquiry New PO#220668.rar	6	0.5 %
AWB 5032675620 - COMMERCIAL INVOICE, BILL OF LADING.zip	6	0.5 %
Others	347	27.0 %
Total	**1.29k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.

Report


Exploit-GBT!678465483C99
Exploit-GBT!62C0BB59551C
Exploit-GBT!EE813535438A
Adwind-FDYD.jar!94A1D4F02352
HTML/Phishing.ej
GenericRXSE-WD!A89222DAEAC5
Exploit-GBT!02D59AF81086
X97M/Downloader.ph
NSIS/ObfusInjector.h
Fareit.gen.a
HTML/Phishing.ce
Fareit.gen.e
HTML/Phishing.ok
Unknown
Medium Risk
High Risk
Not Available
Malicious
Total
2.04k
Hits

Report

Scan Result	Hits	%
Malicious	**974**	**47.8 %**
File_Microsoft-Windows-Executable	601	29.5 %
File_Zip-Archive	134	6.6 %
File_Microsoft-Excel-97-Spreadsheet	81	4.0 %
File_Rar-Archive	49	2.4 %
File_HTML	29	1.4 %
File_ISO-9660-Disk-Image	28	1.4 %
File_XML	18	0.9 %
File_Microsoft-PowerPoint-97-Add-In	8	0.4 %
File_JavaScript	5	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.2 %
File_Microsoft-Cabinet-Archive	5	0.2 %
File_LhArc-Archive	4	0.2 %
File_PDF	3	0.1 %
File_Type-Unknown	2	0.1 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_XZ-Archive	1	0.0 %
Not Available	**575**	**28.2 %**
File_Zip-Archive	575	28.2 %
High Risk	**218**	**10.7 %**
File_Microsoft-Windows-Executable	52	2.6 %
File_Rar-Archive	44	2.2 %
File_ISO-9660-Disk-Image	33	1.6 %
File_Java-Archive	29	1.4 %
File_Zip-Archive	16	0.8 %
File_Microsoft-Excel-97-Spreadsheet	8	0.4 %
File_PDF	7	0.3 %
File_Microsoft-PowerPoint-97-Add-In	6	0.3 %
File_ACE-Archive	4	0.2 %
File_7z-Archive	4	0.2 %
File_Self-Extracting-Zip-Archive	4	0.2 %
File_Microsoft-Cabinet-Archive	3	0.1 %
File_HTML	2	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
File_RTF	2	0.1 %
File_JavaScript	1	0.0 %

Report

Scan Result	Hits	%
File_LhArc-Archive	1	0.0 %
Medium Risk	**179**	**8.8 %**
File_Zip-Archive	97	4.8 %
File_Microsoft-Office-Open-XML-Document	35	1.7 %
File_Rar-Archive	12	0.6 %
File_ISO-9660-Disk-Image	10	0.5 %
File_JavaScript	10	0.5 %
File_Microsoft-Windows-Executable	6	0.3 %
File_PDF	3	0.1 %
File_HTML	1	0.0 %
File_XML	1	0.0 %
File_Type-Unknown	1	0.0 %
File_LhArc-Archive	1	0.0 %
File_7z-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %
Unknown	**21**	**1.0 %**
File_Zip-Archive	21	1.0 %
HTML/Phishing.ok	**16**	**0.8 %**
File_HTML	16	0.8 %
Fareit.gen.e	**11**	**0.5 %**
File_ACE-Archive	11	0.5 %
HTML/Phishing.ce	**10**	**0.5 %**
File_HTML	10	0.5 %
Fareit.gen.a	**10**	**0.5 %**
File_ACE-Archive	10	0.5 %
NSIS/ObfusInjector.h	**7**	**0.3 %**
File_Type-Unknown	7	0.3 %
X97M/Downloader.ph	**7**	**0.3 %**
File_Microsoft-Excel-97-Spreadsheet	7	0.3 %
Exploit-GBT!02D59AF81086	**3**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
GenericRXSE-WD!A89222DAEAC5	**2**	**0.1 %**
File_Zip-Archive	2	0.1 %
HTML/Phishing.ej	**1**	**0.0 %**
File_HTML	1	0.0 %
Adwind-FDYD.jar!94A1D4F02352	**1**	**0.0 %**

Report

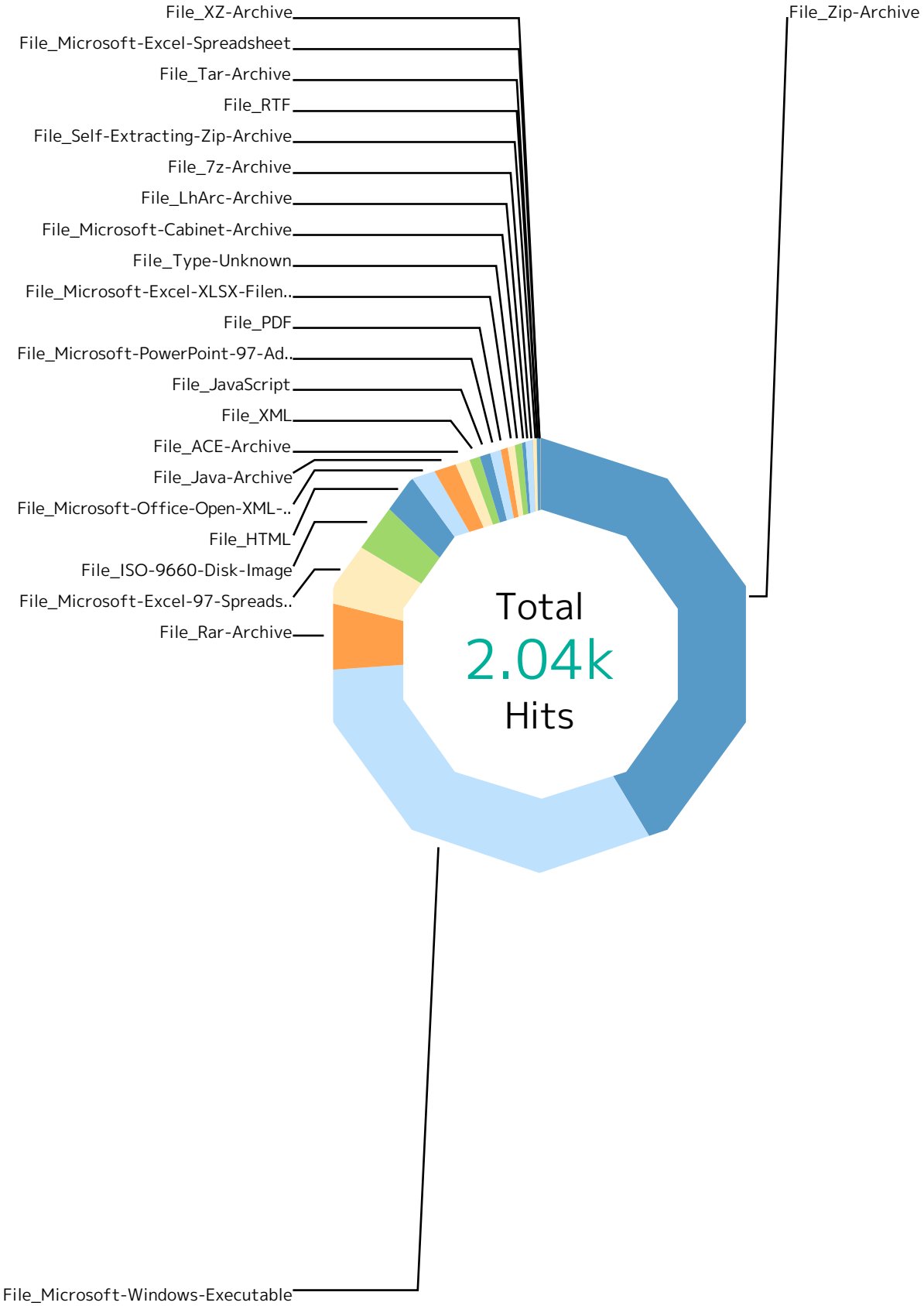
Scan Result	Hits	%
File_Java-Archive	1	0.0 %
Exploit-GBT!EE813535438A	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!62C0BB59551C	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Exploit-GBT!678465483C99	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
Total	**2.04k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_XZ-Archive
File_Microsoft-Excel-Spreadsheet
File_Tar-Archive
File_RTF
File_Self-Extracting-Zip-Archive
File_7z-Archive
File_LhArc-Archive
File_Microsoft-Cabinet-Archive
File_Type-Unknown
File_Microsoft-Excel-XLSX-Filen..
File_PDF
File_Microsoft-PowerPoint-97-Ad..
File_JavaScript
File_XML
File_ACE-Archive
File_Java-Archive
File_Microsoft-Office-Open-XML-..
File_HTML
File_ISO-9660-Disk-Image
File_Microsoft-Excel-97-Spreads..
File_Rar-Archive
File_Zip-Archive
File_Microsoft-Windows-Executable
Total
2.04k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**845**	**41.5 %**
Not Available	575	28.2 %
Malicious	134	6.6 %
Medium Risk	97	4.8 %
Unknown	21	1.0 %
High Risk	16	0.8 %
GenericRXSE-WD!A89222DAEAC5	2	0.1 %
File_Microsoft-Windows-Executable	**659**	**32.3 %**
Malicious	601	29.5 %
High Risk	52	2.6 %
Medium Risk	6	0.3 %
File_Rar-Archive	**105**	**5.2 %**
Malicious	49	2.4 %
High Risk	44	2.2 %
Medium Risk	12	0.6 %
File_Microsoft-Excel-97-Spreadsheet	**96**	**4.7 %**
Malicious	81	4.0 %
High Risk	8	0.4 %
X97M/Downloader.ph	7	0.3 %
File_ISO-9660-Disk-Image	**71**	**3.5 %**
High Risk	33	1.6 %
Malicious	28	1.4 %
Medium Risk	10	0.5 %
File_HTML	**59**	**2.9 %**
Malicious	29	1.4 %
HTML/Phishing.ok	16	0.8 %
HTML/Phishing.ce	10	0.5 %
High Risk	2	0.1 %
Medium Risk	1	0.0 %
HTML/Phishing.ej	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**35**	**1.7 %**
Medium Risk	35	1.7 %
File_Java-Archive	**30**	**1.5 %**
High Risk	29	1.4 %
Adwind-FDYD.jar!94A1D4F02352	1	0.0 %
File_ACE-Archive	**25**	**1.2 %**

Report

Responding Scanner	Hits	%
Fareit.gen.e	11	0.5 %
Fareit.gen.a	10	0.5 %
High Risk	4	0.2 %
File_XML	**19**	**0.9 %**
Malicious	18	0.9 %
Medium Risk	1	0.0 %
File_JavaScript	**16**	**0.8 %**
Medium Risk	10	0.5 %
Malicious	5	0.2 %
High Risk	1	0.0 %
File_Microsoft-PowerPoint-97-Add-In	**14**	**0.7 %**
Malicious	8	0.4 %
High Risk	6	0.3 %
File_PDF	**13**	**0.6 %**
High Risk	7	0.3 %
Malicious	3	0.1 %
Medium Risk	3	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	**13**	**0.6 %**
Malicious	5	0.2 %
Exploit-GBT!02D59AF81086	3	0.1 %
High Risk	2	0.1 %
Exploit-GBT!EE813535438A	1	0.0 %
Exploit-GBT!62C0BB59551C	1	0.0 %
Exploit-GBT!678465483C99	1	0.0 %
File_Type-Unknown	**10**	**0.5 %**
NSIS/ObfusInjector.h	7	0.3 %
Malicious	2	0.1 %
Medium Risk	1	0.0 %
File_Microsoft-Cabinet-Archive	**8**	**0.4 %**
Malicious	5	0.2 %
High Risk	3	0.1 %
File_LhArc-Archive	**6**	**0.3 %**
Malicious	4	0.2 %
High Risk	1	0.0 %
Medium Risk	1	0.0 %
File_7z-Archive	**5**	**0.2 %**

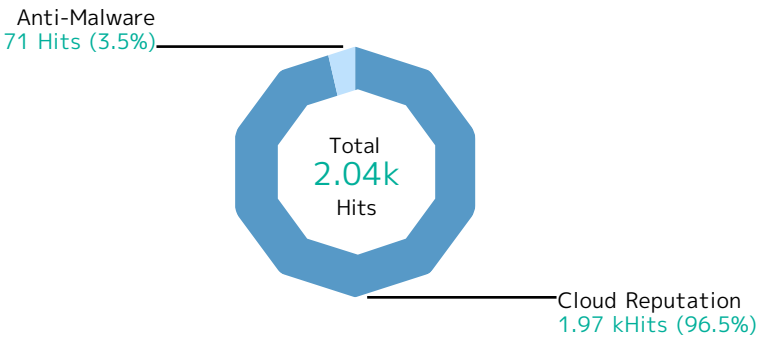
Report

Responding Scanner	Hits	%
High Risk	4	0.2 %
Medium Risk	1	0.0 %
File_Self-Extracting-Zip-Archive	**4**	**0.2 %**
High Risk	4	0.2 %
File_RTF	**2**	**0.1 %**
High Risk	2	0.1 %
File_Tar-Archive	**1**	**0.0 %**
Medium Risk	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**1**	**0.0 %**
Malicious	1	0.0 %
File_XZ-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**2.04k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**1.97k**	**96.5 %**
File_Zip-Archive	843	41.4 %
File_Microsoft-Windows-Executable	659	32.3 %
File_Rar-Archive	105	5.2 %
File_Microsoft-Excel-97-Spreadsheet	89	4.4 %
File_ISO-9660-Disk-Image	71	3.5 %
File_Microsoft-Office-Open-XML-Document	35	1.7 %
File_HTML	32	1.6 %
File_Java-Archive	29	1.4 %
File_XML	19	0.9 %
File_JavaScript	16	0.8 %
File_Microsoft-PowerPoint-97-Add-In	14	0.7 %
File_PDF	13	0.6 %
File_Microsoft-Cabinet-Archive	8	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	7	0.3 %
File_LhArc-Archive	6	0.3 %
File_7z-Archive	5	0.2 %
File_ACE-Archive	4	0.2 %
File_Self-Extracting-Zip-Archive	4	0.2 %
File_Type-Unknown	3	0.1 %
File_RTF	2	0.1 %
File_Tar-Archive	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
File_XZ-Archive	1	0.0 %
Anti-Malware	**71**	**3.5 %**
File_HTML	27	1.3 %
File_ACE-Archive	21	1.0 %
File_Microsoft-Excel-97-Spreadsheet	7	0.3 %
File_Type-Unknown	7	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	6	0.3 %
File_Zip-Archive	2	0.1 %
File_Java-Archive	1	0.0 %
Total	**2.04k**	**100 %**

Report

Virenfilterung SRC IPs

Located 80.9 %

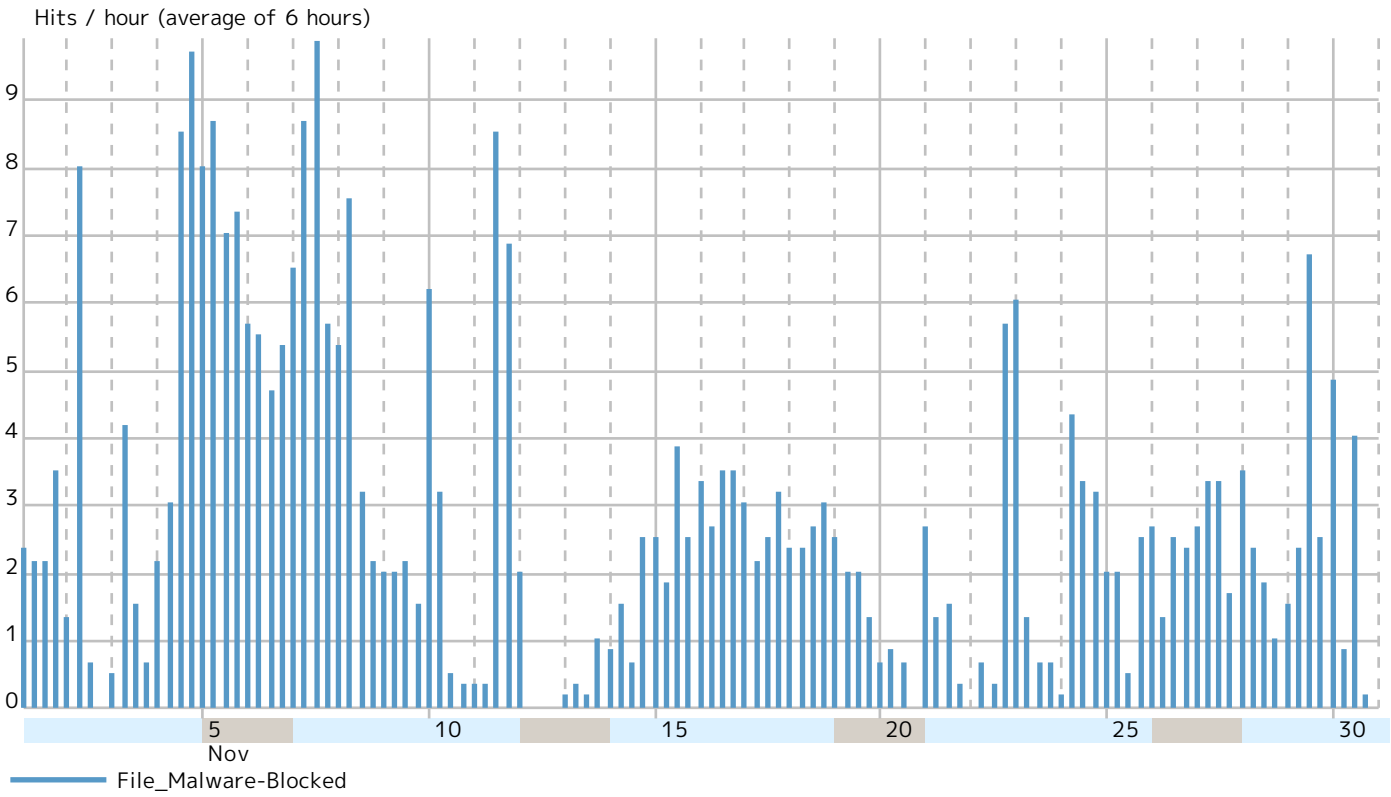
Report

Records by src IP		Hits	%
172.107.174.19	Dallas, Texas 75247, United States	538	26.4 %
176.88.51.4	Istanbul, Turkey	280	13.7 %
45.117.82.155	Vietnam	186	9.1 %
221.141.1.45	Suwon, South Korea	104	5.1 %
194.4.48.88	Madrid, Spain	81	4.0 %
85.31.44.220	Virginia, United States	74	3.6 %
158.199.173.240	Japan	57	2.8 %
210.13.193.243	China	29	1.4 %
91.245.254.117	Montreal, Quebec H5A , Canada	28	1.4 %
155.94.136.211	Los Angeles, California 90014, United States	28	1.4 %
193.19.66.22	Russia	24	1.2 %
185.164.6.198	Austria	21	1.0 %
194.4.48.39	Madrid, Spain	17	0.8 %
194.4.48.40	Madrid, Spain	17	0.8 %
85.217.145.102	Reston, Virginia 20190, United States	15	0.7 %
109.206.243.178	Ashburn, Virginia 20104, United States	14	0.7 %
89.253.228.12	Russia	14	0.7 %
109.206.243.187	Ashburn, Virginia 20104, United States	14	0.7 %
201.247.113.42	Antiguo Cuscatlan, El Salvador	12	0.6 %
193.47.61.158	Ashburn, Virginia 20149, United States	10	0.5 %
49.5.7.71	China	10	0.5 %
67.43.228.58	Canada	10	0.5 %
95.131.139.228	France	9	0.4 %
45.141.78.161	Russia	9	0.4 %
27.100.36.53	Sydney, Australia	8	0.4 %
141.94.227.131	France	8	0.4 %
23.235.223.152	United States	8	0.4 %
96.125.164.115	United States	8	0.4 %
192.210.213.216	United States	8	0.4 %
176.126.203.249	Romania	8	0.4 %
Others		389	19.1 %
Total		**2.04k**	**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.