

---

# Forcepoint FlexEdge Secure SD-WAN

## E-Mail Virenterung Server Firewall

### Report period

From: 2023-12-01 00:00:00+0100

To: 2024-01-01 00:00:00+0100

**Forcepoint**

# Table of Contents

**Report run by**  
jens

**SD-WAN Manager Console version**  
7.1.2, build 11426

**Update version**  
1669

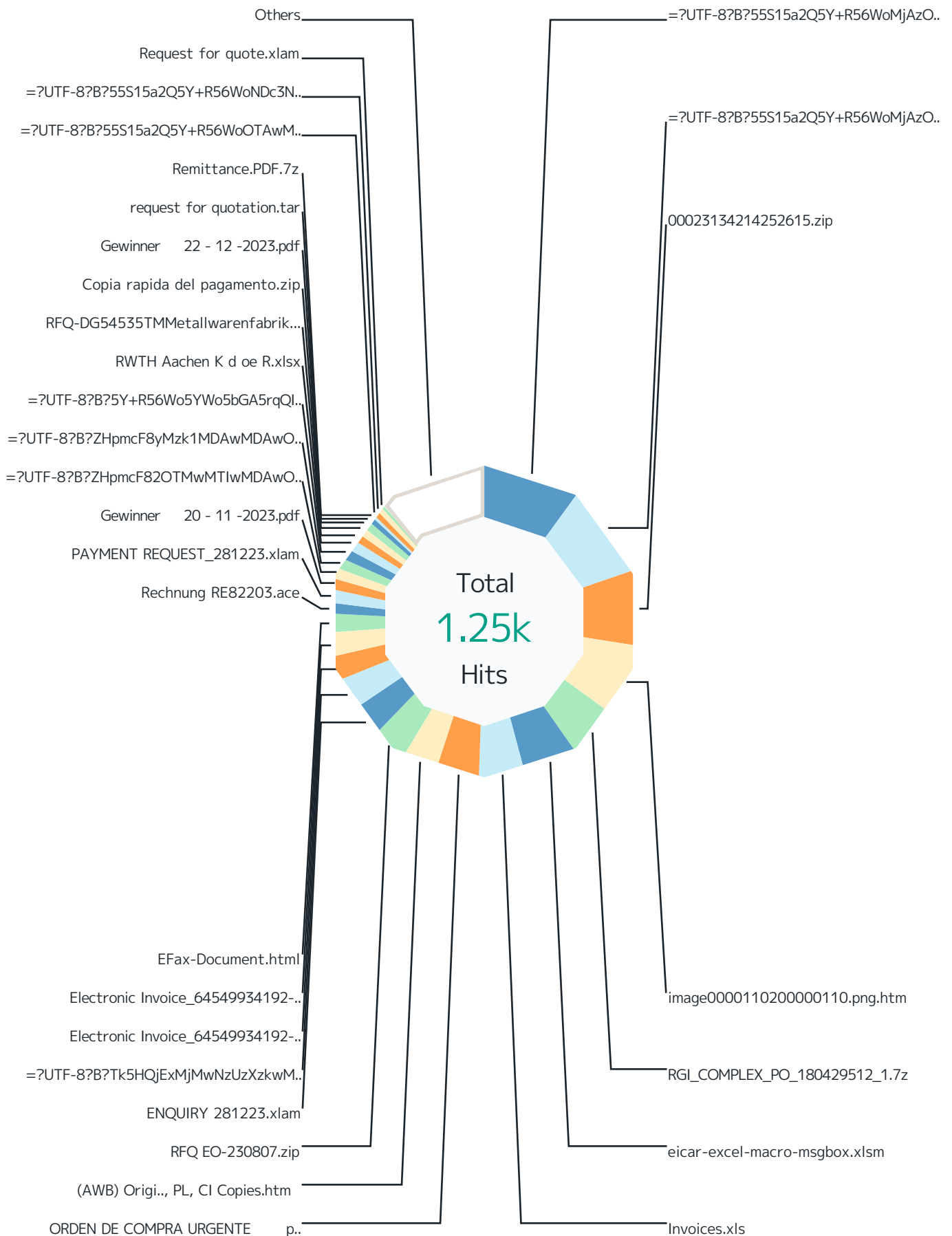
**Report started**  
2024-01-01 21:08:18+0100

**Report run time**  
07:11:10

**Filters used**  
Match All

Virentfilterung MXe .....	3
Top File Types by Scan Result .....	5
Top Scan Results by Responding Scanner .....	10
Top File Types by Responding Scanner .....	14
Virentfilterung SRC IPs .....	15
SMTP Virus Filtering by Time .....	17

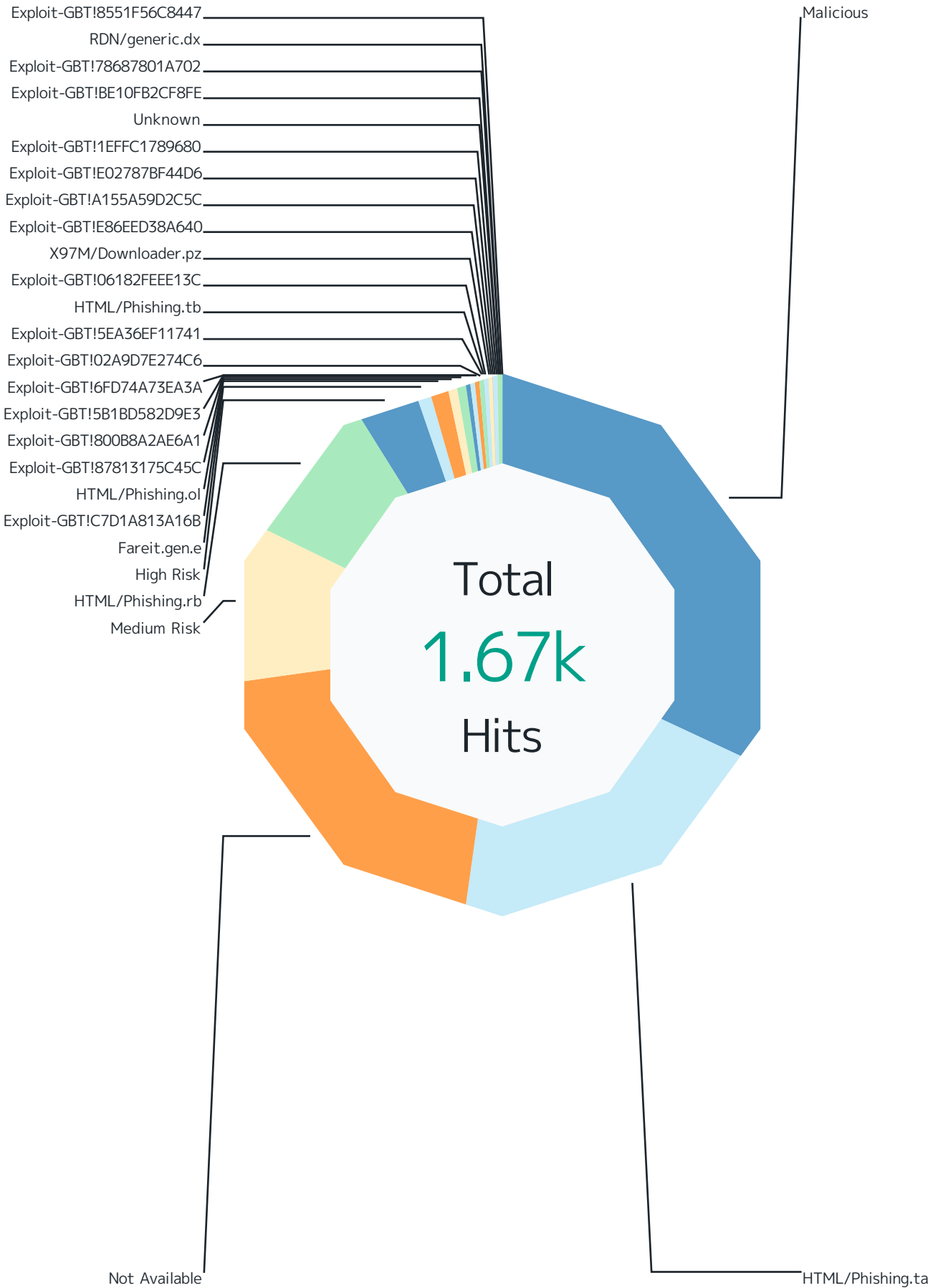
# Virenterung MXe



Records by file name	Hits	%
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTEtMjAyMy5qcGcuaHRtbA==?=	124	9.9 %
=?UTF-8?B?55S15a2Q5Y+R56WoMjAzOTkyMDEwMTEtMjAyMy5wZGYuc2h0bWw=?=	124	9.9 %
00023134214252615.zip	98	7.8 %
image0000110200000110.png.htm	91	7.3 %
RGI_COMPLEX_PO_180429512_1.7z	69	5.5 %
eicar-excel-macro-msgbox.xlsm	67	5.4 %
Invoices.xls	59	4.7 %
ORDEN DE COMPRA URGENTE pdf.zip	56	4.5 %
(AWB) Original BL, PL, CI Copies.htm	46	3.7 %
RFQ EO-230807.zip	44	3.5 %
ENQUIRY 281223.xlam	44	3.5 %
=?UTF-8?B?Tk5HQjExMjMwNzUzXzkwMjMxMzQ2M19OR0JJTDIzMTEwMjExMS5wZG YueHRtbA==?=	40	3.2 %
Electronic Invoice_64549934192-2023_JPG.htm	31	2.5 %
Electronic Invoice_64549934192-2023 PDF.htm	31	2.5 %
EFax-Document.html	24	1.9 %
Rechnung RE82203.ace	17	1.4 %
PAYMENT REQUEST_281223.xlam	16	1.3 %
Gewinner 20 - 11 -2023.pdf	15	1.2 %
=?UTF-8?B?ZHpmcF82OTMwMTIwMDAwOTE3NzgxOF9qcGcuaHRtbA==?=	14	1.1 %
=?UTF-8?B?ZHpmcF8yMzk1MDAwMDAwOTE3NzgxOF9wZGYuc2h0bWw=?=	14	1.1 %
=?UTF-8?B?5Y+R56Wo5YWo5bGA5rqQIGRvY3VtZW50Lmh0bWw=?=	14	1.1 %
RWTH Aachen K d oe R.xlsx	13	1.0 %
RFQ-DG54535TMMetallwarenfabrik.xlsx	11	0.9 %
Copia rapida del pagamento.zip	10	0.8 %
Gewinner 22 - 12 -2023.pdf	8	0.6 %
request for quotation.tar	7	0.6 %
Remittance.PDF.7z	6	0.5 %
=?UTF-8?B?55S15a2Q5Y+R56WoOTAwMjYzMDEwMjIzLnBkZi5zaHRtbA==?=	6	0.5 %
=?UTF-8?B?55S15a2Q5Y+R56WoNDc3Njk5MzAyMCOuanBnLmh0bWw=?=	6	0.5 %
Request for quote.xlam	6	0.5 %
Others	141	11.3 %
<b>Total</b>	<b>1.25k</b>	<b>100 %</b>

## Top File Types by Scan Result

Top 10 file types by scan result.



Scan Result	Hits	%
<b>Malicious</b>	<b>532</b>	<b>31.8 %</b>
File_Microsoft-Windows-Executable	286	17.1 %
File_Microsoft-OLE	67	4.0 %
File_Zip-Archive	52	3.1 %
File_Microsoft-Excel-97-Spreadsheet	52	3.1 %
File_Rar-Archive	29	1.7 %
File_HTML	26	1.6 %
File_PDF	5	0.3 %
File_ISO-9660-Disk-Image	3	0.2 %
File_Microsoft-Cabinet-Archive	3	0.2 %
File_RTF	3	0.2 %
File_Office-Open-XML-Package-Relations-Item	2	0.1 %
File_Type-Unknown	2	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %
File_Encrypted-Rar-Archive	1	0.1 %
<b>HTML/Phishing.ta</b>	<b>343</b>	<b>20.5 %</b>
File_HTML	343	20.5 %
<b>Not Available</b>	<b>343</b>	<b>20.5 %</b>
File_Zip-Archive	329	19.7 %
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.8 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %
<b>Medium Risk</b>	<b>158</b>	<b>9.4 %</b>
File_HTML	91	5.4 %
File_XML	44	2.6 %
File_GIF-Image	19	1.1 %
File_PDF	2	0.1 %
File_Rar-Archive	1	0.1 %
File_Tar-Archive	1	0.1 %
<b>HTML/Phishing.rb</b>	<b>146</b>	<b>8.7 %</b>
File_HTML	146	8.7 %
<b>High Risk</b>	<b>60</b>	<b>3.6 %</b>
File_PDF	23	1.4 %
File_Zip-Archive	22	1.3 %
File_Microsoft-Excel-97-Spreadsheet	10	0.6 %
File_Microsoft-Windows-Executable	1	0.1 %
File_Rar-Archive	1	0.1 %
File_ISO-9660-Disk-Image	1	0.1 %
File_Office-Open-XML-Package-Relations-Item	1	0.1 %
File_Microsoft-Office-Open-XML-Document	1	0.1 %

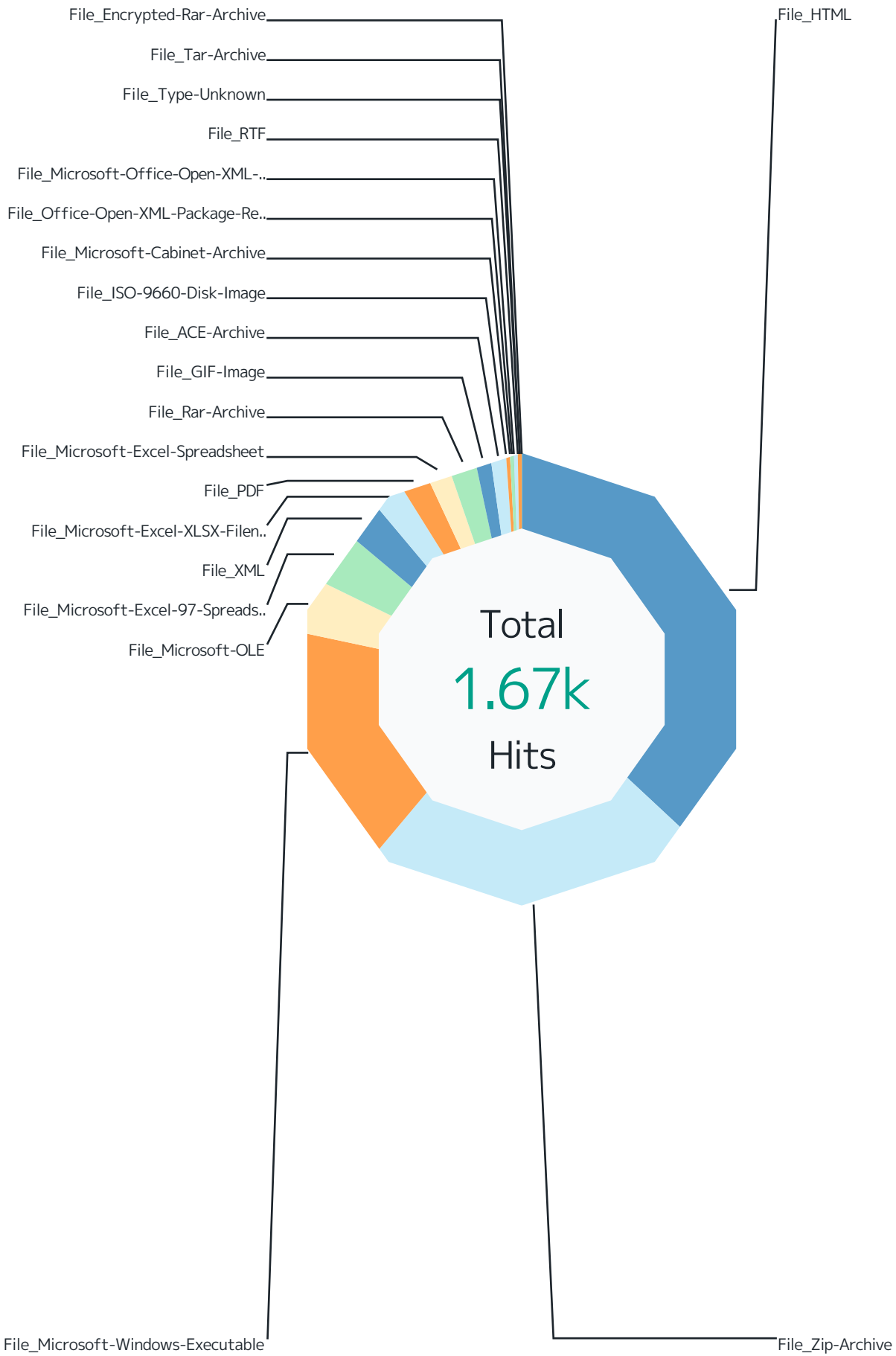
Scan Result	Hits	%
<b>Fareit.gen.e</b>	<b>17</b>	<b>1.0 %</b>
File_ACE-Archive	17	1.0 %
<b>Exploit-GBT!C7D1A813A16B</b>	<b>16</b>	<b>1.0 %</b>
File_Microsoft-Excel-Spreadsheet	16	1.0 %
<b>HTML/Phishing.ol</b>	<b>11</b>	<b>0.7 %</b>
File_HTML	11	0.7 %
<b>Exploit-GBT!87813175C45C</b>	<b>9</b>	<b>0.5 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.5 %
<b>Exploit-GBT!800B8A2AE6A1</b>	<b>6</b>	<b>0.4 %</b>
File_Microsoft-Excel-Spreadsheet	6	0.4 %
<b>Exploit-GBT!5B1BD582D9E3</b>	<b>4</b>	<b>0.2 %</b>
File_Microsoft-Excel-Spreadsheet	4	0.2 %
<b>Exploit-GBT!6FD74A73EA3A</b>	<b>3</b>	<b>0.2 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.2 %
<b>Exploit-GBT!02A9D7E274C6</b>	<b>3</b>	<b>0.2 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.2 %
<b>Exploit-GBT!5EA36EF11741</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
<b>HTML/Phishing.tb</b>	<b>2</b>	<b>0.1 %</b>
File_HTML	2	0.1 %
<b>Exploit-GBT!06182FEEE13C</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-Spreadsheet	2	0.1 %
<b>X97M/Downloader.pz</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-97-Spreadsheet	2	0.1 %
<b>Exploit-GBT!E86EED38A640</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
<b>Exploit-GBT!A155A59D2C5C</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
<b>Exploit-GBT!E02787BF44D6</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-Spreadsheet	2	0.1 %
<b>Exploit-GBT!1EFFC1789680</b>	<b>2</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
<b>Unknown</b>	<b>1</b>	<b>0.1 %</b>
File_Zip-Archive	1	0.1 %
<b>Exploit-GBT!BE10FB2CF8FE</b>	<b>1</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
<b>Exploit-GBT!78687801A702</b>	<b>1</b>	<b>0.1 %</b>
File_Microsoft-Excel-Spreadsheet	1	0.1 %
<b>RDN/generic.dx</b>	<b>1</b>	<b>0.1 %</b>



Scan Result	Hits	%
File_PDF	1	0.1 %
<b>Exploit-GBT!8551F56C8447</b>	<b>1</b>	<b>0.1 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.1 %
<b>Total</b>	<b>1.67k</b>	<b>100 %</b>

## Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

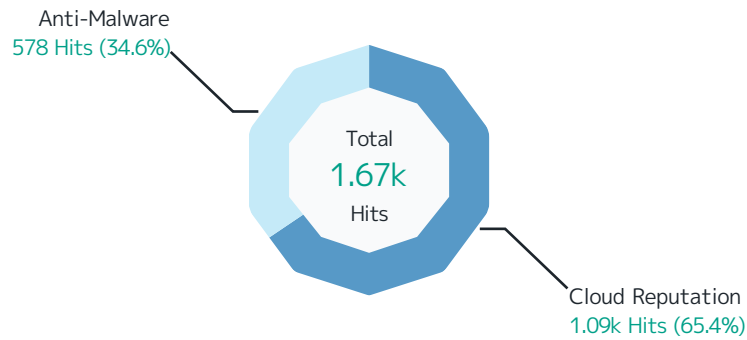


Responding Scanner	Hits	%
<b>File_HTML</b>	<b>619</b>	<b>37.0 %</b>
HTML/Phishing.ta	343	20.5 %
HTML/Phishing.rb	146	8.7 %
Medium Risk	91	5.4 %
Malicious	26	1.6 %
HTML/Phishing.ol	11	0.7 %
HTML/Phishing.tb	2	0.1 %
<b>File_Zip-Archive</b>	<b>404</b>	<b>24.2 %</b>
Not Available	329	19.7 %
Malicious	52	3.1 %
High Risk	22	1.3 %
Unknown	1	0.1 %
<b>File_Microsoft-Windows-Executable</b>	<b>287</b>	<b>17.2 %</b>
Malicious	286	17.1 %
High Risk	1	0.1 %
<b>File_Microsoft-OLE</b>	<b>67</b>	<b>4.0 %</b>
Malicious	67	4.0 %
<b>File_Microsoft-Excel-97-Spreadsheet</b>	<b>64</b>	<b>3.8 %</b>
Malicious	52	3.1 %
High Risk	10	0.6 %
X97M/Downloader.pz	2	0.1 %
<b>File_XML</b>	<b>44</b>	<b>2.6 %</b>
Medium Risk	44	2.6 %
<b>File_Microsoft-Excel-XLSX-Filename-Extension</b>	<b>38</b>	<b>2.3 %</b>
Not Available	13	0.8 %
Exploit-GBT!87813175C45C	9	0.5 %
Exploit-GBT!6FD74A73EA3A	3	0.2 %
Exploit-GBT!02A9D7E274C6	3	0.2 %
Exploit-GBT!5EA36EF11741	2	0.1 %
Exploit-GBT!E86EED38A640	2	0.1 %
Exploit-GBT!A155A59D2C5C	2	0.1 %
Exploit-GBT!1EFFF1789680	2	0.1 %
Exploit-GBT!BE10FB2CF8FE	1	0.1 %
Exploit-GBT!8551F56C8447	1	0.1 %
<b>File_PDF</b>	<b>31</b>	<b>1.9 %</b>
High Risk	23	1.4 %
Malicious	5	0.3 %
Medium Risk	2	0.1 %
RDN/generic.dx	1	0.1 %

Responding Scanner	Hits	%
<b>File_Microsoft-Excel-Spreadsheet</b>	<b>31</b>	<b>1.9%</b>
Exploit-GBT!C7D1A813A16B	16	1.0%
Exploit-GBT!800B8A2AE6A1	6	0.4%
Exploit-GBT!5B1BD582D9E3	4	0.2%
Exploit-GBT!06182FEEE13C	2	0.1%
Exploit-GBT!E02787BF44D6	2	0.1%
Exploit-GBT!78687801A702	1	0.1%
<b>File_Rar-Archive</b>	<b>31</b>	<b>1.9%</b>
Malicious	29	1.7%
Medium Risk	1	0.1%
High Risk	1	0.1%
<b>File_GIF-Image</b>	<b>19</b>	<b>1.1%</b>
Medium Risk	19	1.1%
<b>File_ACE-Archive</b>	<b>17</b>	<b>1.0%</b>
Fareit.gen.e	17	1.0%
<b>File_ISO-9660-Disk-Image</b>	<b>4</b>	<b>0.2%</b>
Malicious	3	0.2%
High Risk	1	0.1%
<b>File_Microsoft-Cabinet-Archive</b>	<b>3</b>	<b>0.2%</b>
Malicious	3	0.2%
<b>File_Office-Open-XML-Package-Relations-Item</b>	<b>3</b>	<b>0.2%</b>
Malicious	2	0.1%
High Risk	1	0.1%
<b>File_Microsoft-Office-Open-XML-Document</b>	<b>3</b>	<b>0.2%</b>
Malicious	1	0.1%
Not Available	1	0.1%
High Risk	1	0.1%
<b>File_RTF</b>	<b>3</b>	<b>0.2%</b>
Malicious	3	0.2%
<b>File_Type-Unknown</b>	<b>2</b>	<b>0.1%</b>
Malicious	2	0.1%
<b>File_Tar-Archive</b>	<b>1</b>	<b>0.1%</b>
Medium Risk	1	0.1%
<b>File_Encrypted-Rar-Archive</b>	<b>1</b>	<b>0.1%</b>
Malicious	1	0.1%
<b>Total</b>	<b>1.67k</b>	<b>100%</b>

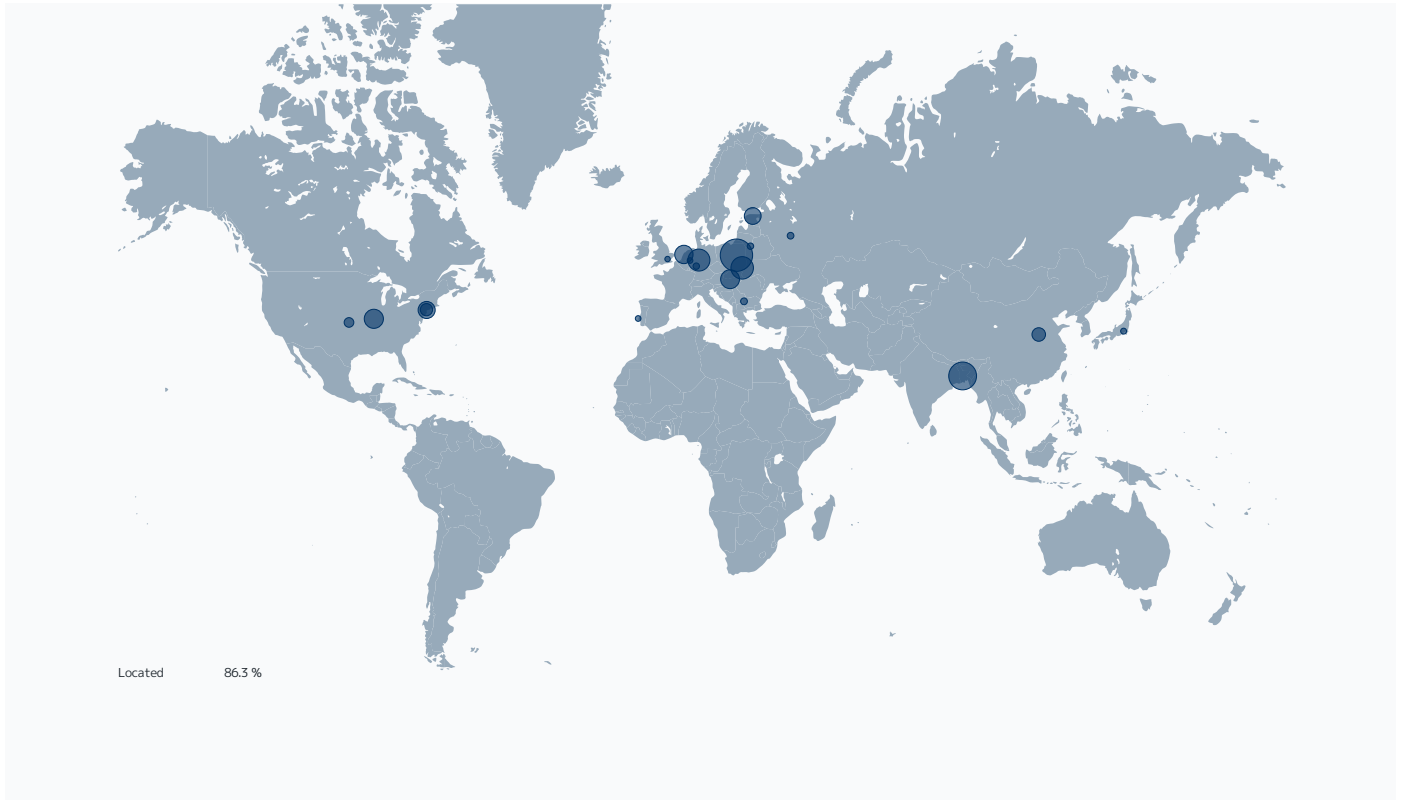
# Top File Types by Responding Scanner




























Top 10 file types by responding scanner.



Responding Scanner	Hits	%
<b>Cloud Reputation</b>	<b>1.09k</b>	<b>65.4 %</b>
File_Zip-Archive	404	24.2 %
File_Microsoft-Windows-Executable	287	17.2 %
File_HTML	117	7.0 %
File_Microsoft-OLE	67	4.0 %
File_Microsoft-Excel-97-Spreadsheet	62	3.7 %
File_XML	44	2.6 %
File_Rar-Archive	31	1.9 %
File_PDF	30	1.8 %
File_GIF-Image	19	1.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.8 %
File_ISO-9660-Disk-Image	4	0.2 %
File_Microsoft-Cabinet-Archive	3	0.2 %
File_Office-Open-XML-Package-Relations-Item	3	0.2 %
File_Microsoft-Office-Open-XML-Document	3	0.2 %
File_RTF	3	0.2 %
File_Type-Unknown	2	0.1 %
File_Tar-Archive	1	0.1 %
File_Encrypted-Rar-Archive	1	0.1 %
<b>Anti-Malware</b>	<b>578</b>	<b>34.6 %</b>
File_HTML	502	30.0 %
File_Microsoft-Excel-Spreadsheet	31	1.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	25	1.5 %
File_ACE-Archive	17	1.0 %
File_Microsoft-Excel-97-Spreadsheet	2	0.1 %
File_PDF	1	0.1 %
<b>Total</b>	<b>1.67k</b>	<b>100 %</b>

## Virenfiterung SRC IPs

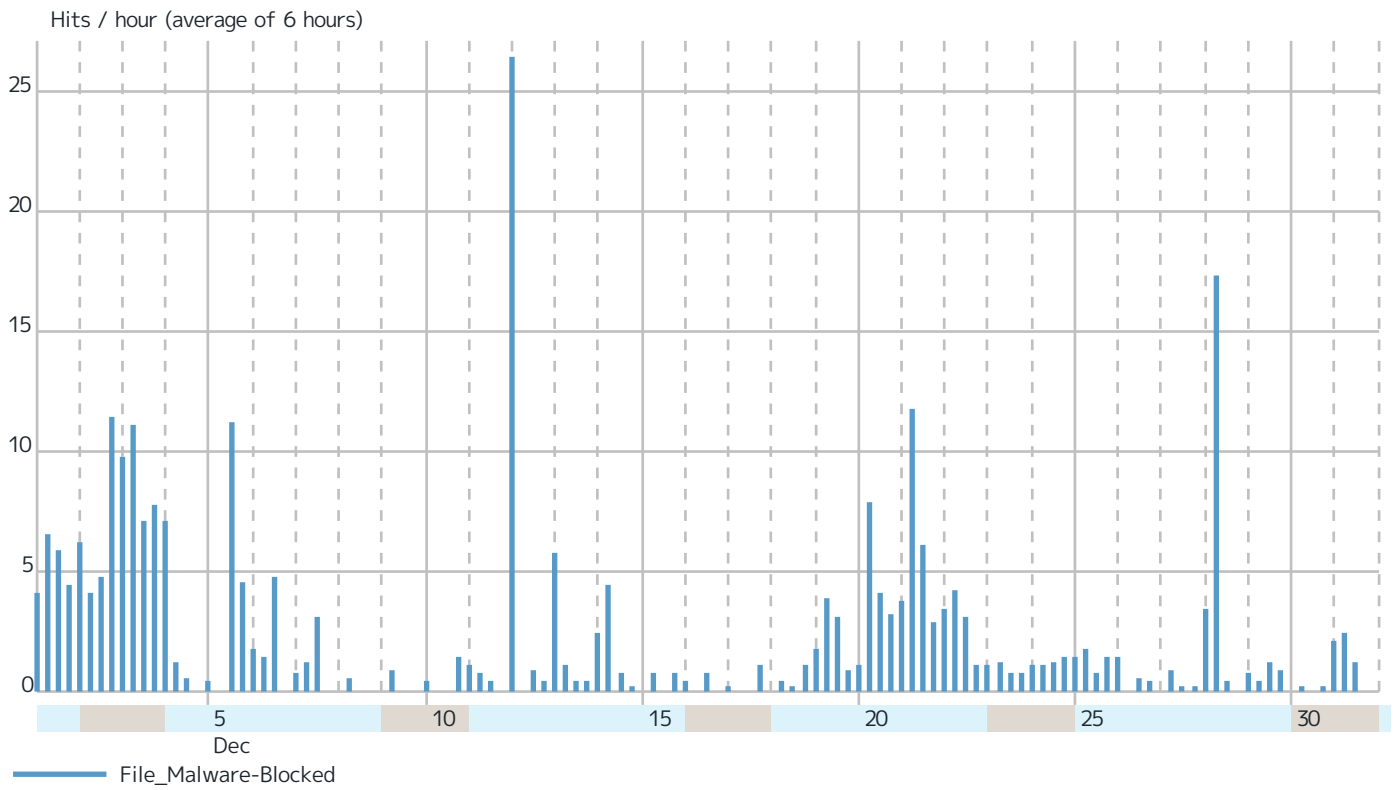


Records by src IP		Hits	%
51.77.61.156	 Warsaw, Poland	214	12.8 %
91.240.223.143	 Przemyśl, Poland	138	8.3 %
62.146.106.30	 Germany	134	8.0 %
148.72.176.68	 St Louis, Missouri 63169, United States	112	6.7 %
185.126.34.3	 Amsterdam, The Netherlands	106	6.3 %
205.234.244.43	 New York, New York 10118, United States	96	5.7 %
163.47.157.196	 Bangladesh	91	5.4 %
203.112.73.74	 Bangladesh	88	5.3 %
45.9.168.182	 Hungary	56	3.3 %
119.91.250.26	 China	45	2.7 %
188.127.227.203	 Estonia	42	2.5 %
23.92.179.183	 Secaucus, New Jersey 07094, United States	39	2.3 %
188.127.237.106	 Estonia	36	2.2 %
45.9.168.175	 Hungary	28	1.7 %
45.9.168.108	 Hungary	26	1.6 %
103.145.190.65	 China	24	1.4 %
173.247.255.168	 United States	23	1.4 %
23.92.176.189	 Secaucus, New Jersey 07094, United States	20	1.2 %
78.128.76.61	 Sofia, Bulgaria	17	1.0 %
192.232.236.18	 United States	16	1.0 %
82.209.195.14	 Lida, Belarus	14	0.8 %
31.192.237.58	 Frankfurt am Main, Germany	14	0.8 %
103.125.216.133	 Tokyo, Japan	10	0.6 %
188.127.237.142	 Estonia	8	0.5 %
2.58.95.47	 Düsseldorf, Germany	8	0.5 %
91.219.150.144	 Russia	8	0.5 %
91.219.150.21	 Russia	8	0.5 %
185.236.231.117	 Portugal	8	0.5 %
91.199.154.163	 Estonia	8	0.5 %
91.224.92.26	 United Kingdom	6	0.4 %
Others		229	13.7 %
<b>Total</b>		<b>1.67k</b>	<b>100 %</b>



# SMTP Virus Filtering by Time

Top 10 file filtering situations on a timeline.



---

# About the FlexEdge Secure SD-WAN

Forcepoint FlexEdge Secure SD-WAN enables distributed organizations to improve application performance, simplify network management, and increase security— ensuring users can safely access any application from anywhere. By combining multi-link networking and intrusion prevention with zero-touch deployment and updating, it provides centralized visibility and control with high performance that scales to thousands of sites. When used with the Forcepoint ONE SSE platform, FlexEdge Secure SD-WAN delivers true SASE and secure branch solutions that boost productivity, cut costs, reduce risk, and streamline compliance.

For further information visit [forcepoint.com/product/secure-sd-wan](https://forcepoint.com/product/secure-sd-wan).



[forcepoint.com](https://forcepoint.com)

## About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on [www.forcepoint.com](https://www.forcepoint.com), [Twitter](#) and [LinkedIn](#).

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.