

---

# Forcepoint FlexEdge Secure SD-WAN

## E-Mail Virenterung Server Firewall

### Report period

From: 2024-05-01 00:00:00+0200

To: 2024-06-01 00:00:00+0200

**Forcepoint**

# Table of Contents

**Report run by**  
jens

**SD-WAN Manager Console version**  
7.1.3, build 11429

**Update version**  
1732

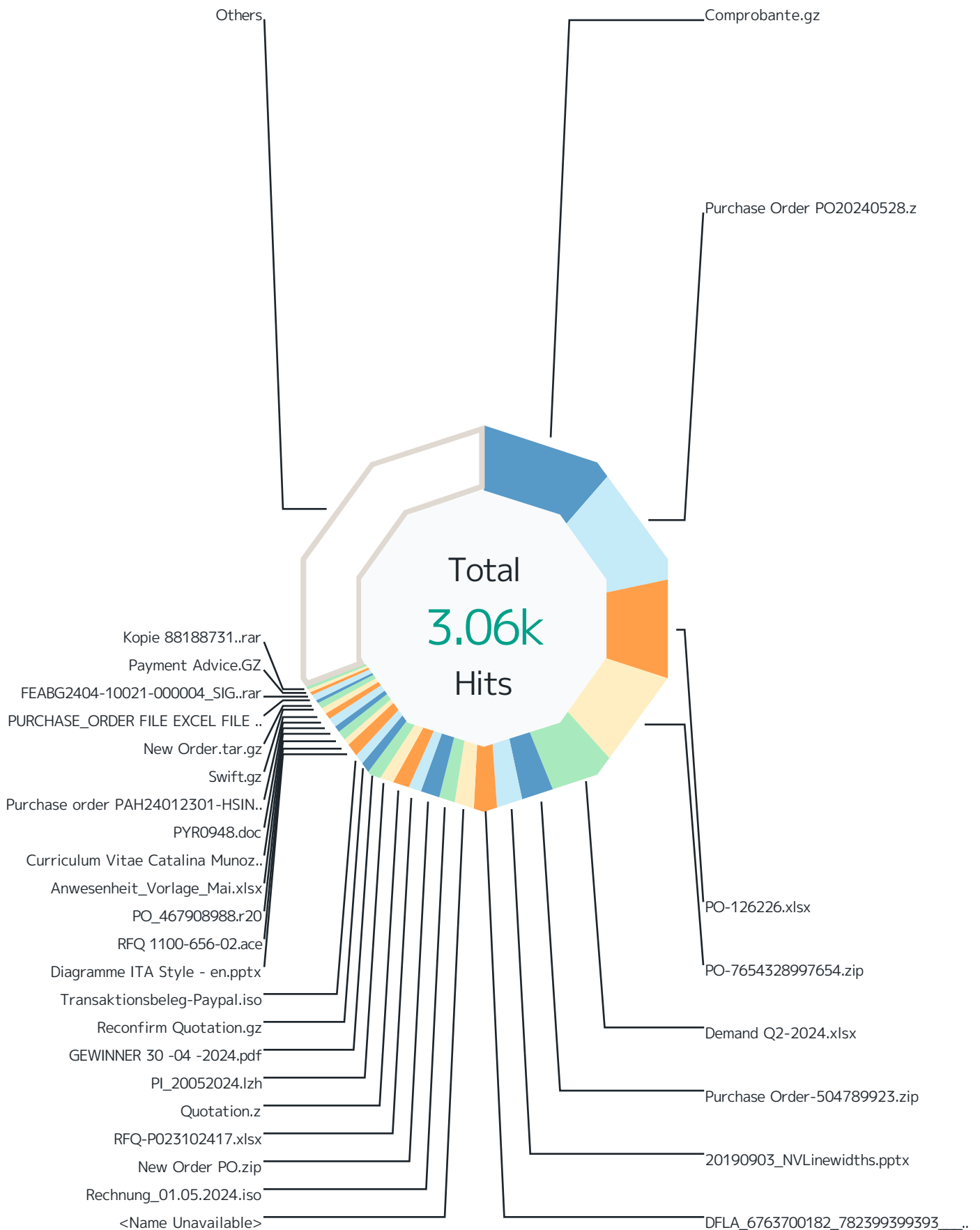
**Report started**  
2024-06-03 13:32:19+0200

**Report run time**  
03:06:52

**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 .....	15
Virentfilterung SRC IPs .....	17
SMTP Virus Filtering by Time .....	19

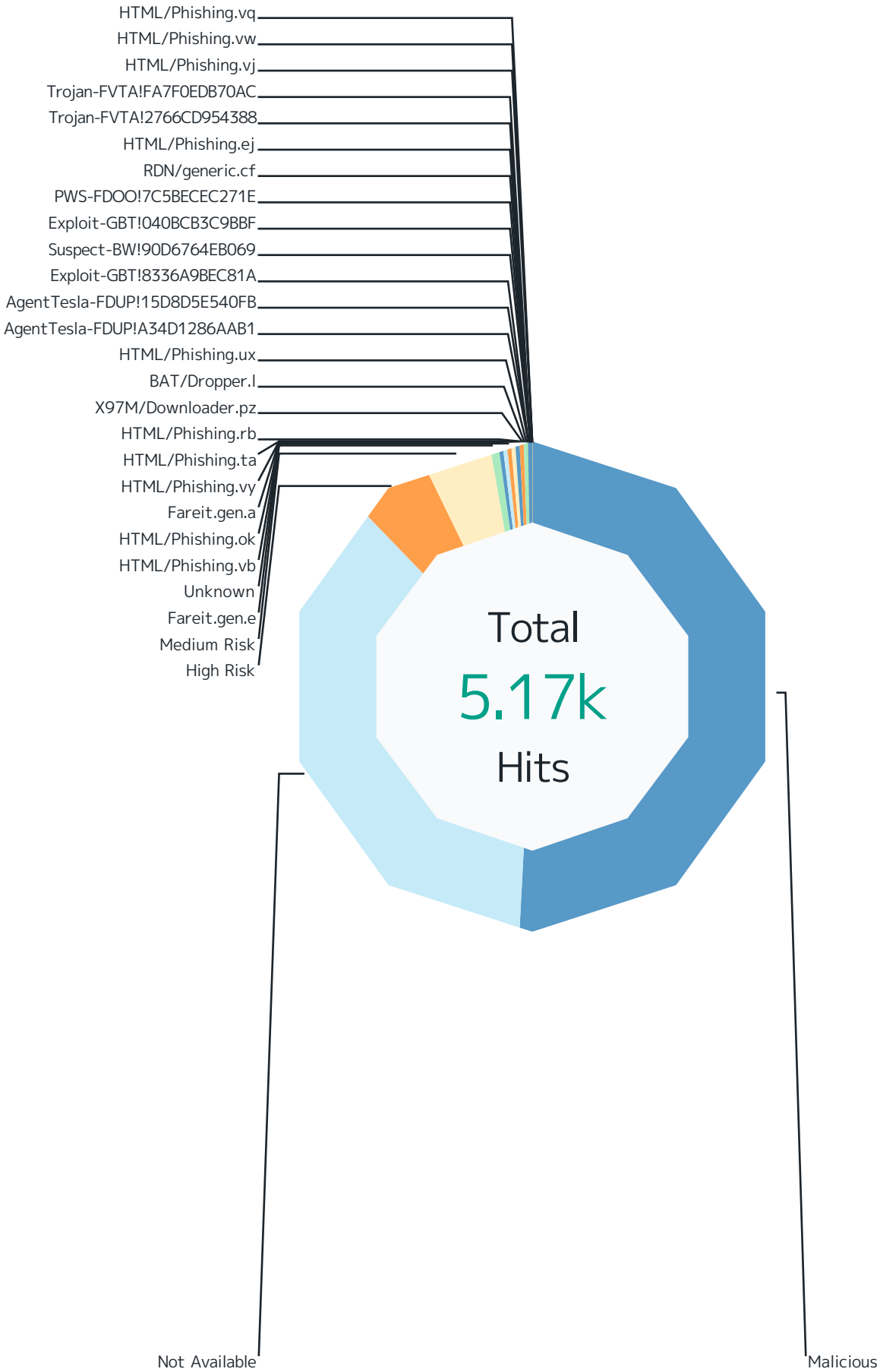
# Virenfiterung Mx



Records by file name	Hits	%
Comprobante.gz	345	11.3 %
Purchase Order PO20240528.z	317	10.3 %
PO-126226.xlsx	261	8.5 %
PO-7654328997654.zip	251	8.2 %
Demand Q2-2024.xlsx	167	5.5 %
Purchase Order-504789923.zip	89	2.9 %
20190903_NVLinewidths.pptx	65	2.1 %
DFLA_6763700182_782399399393_____.r13	63	2.1 %
<Name Unavailable>	48	1.6 %
Rechnung_01.05.2024.iso	48	1.6 %
New Order PO.zip	44	1.4 %
RFQ-P023102417.xlsx	40	1.3 %
Quotation.z	40	1.3 %
PI_20052024.lzh	36	1.2 %
GEWINNER 30 -04 -2024.pdf	32	1.0 %
Reconfirm Quotation.gz	29	0.9 %
Transaktionsbeleg-Paypal.iso	27	0.9 %
Diagramme ITA Style - en.pptx	27	0.9 %
RFQ 1100-656-02.ace	23	0.8 %
PO_467908988.r20	23	0.8 %
Anwesenheit_Vorlage_Mai.xlsx	20	0.7 %
Curriculum Vitae Catalina Munoz.zip	18	0.6 %
PYR0948.doc	18	0.6 %
Purchase order PAH24012301-HSIN.rar	17	0.6 %
Swift.gz	17	0.6 %
New Order.tar.gz	13	0.4 %
PURCHASE_ORDER FILE EXCEL FILE .shtml	12	0.4 %
FEABG2404-10021-000004_SIG..rar	11	0.4 %
Payment Advice.GZ	11	0.4 %
Kopie 88188731..rar	11	0.4 %
Others	941	30.7 %
<b>Total</b>	<b>3.06k</b>	<b>100 %</b>

## Top File Types by Scan Result

Top 10 file types by scan result.



Scan Result	Hits	%
<b>Malicious</b>	<b>2.63k</b>	<b>50.7 %</b>
File_Microsoft-Windows-Executable	1.48k	28.6 %
File_Rar-Archive	364	7.0 %
File_Microsoft-Equation-Editor-Document	261	5.0 %
File_Zip-Archive	171	3.3 %
File_ISO-9660-Disk-Image	114	2.2 %
File_HTML	66	1.3 %
File_LhArc-Archive	54	1.0 %
File_7z-Archive	33	0.6 %
File_Type-Unknown	24	0.5 %
File_Microsoft-Cabinet-Archive	17	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	13	0.3 %
File_PDF	8	0.2 %
File_Encrypted-Rar-Archive	5	0.1 %
File_PNG-Image	4	0.1 %
File_Microsoft-OLE	4	0.1 %
File_Java-Archive	3	0.1 %
File_JavaScript	1	0.0 %
File_XZ-Archive	1	0.0 %
<b>Not Available</b>	<b>1.92k</b>	<b>37.0 %</b>
File_Zip-Archive	1.42k	27.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	496	9.6 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
<b>High Risk</b>	<b>255</b>	<b>4.9 %</b>
File_Microsoft-Equation-Editor-Document	228	4.4 %
File_Rar-Archive	8	0.2 %
File_PDF	6	0.1 %
File_7z-Archive	5	0.1 %
File_Microsoft-Windows-Executable	4	0.1 %
File_LhArc-Archive	3	0.1 %
File_SVG	1	0.0 %
<b>Medium Risk</b>	<b>231</b>	<b>4.5 %</b>
File_Office-Open-XML-Package-Relations-Item	112	2.2 %
File_PDF	39	0.8 %
File_Microsoft-Windows-Executable	21	0.4 %
File_Type-Unknown	18	0.3 %
File_Microsoft-Excel-97-Spreadsheet	15	0.3 %
File_HTML	12	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.2 %

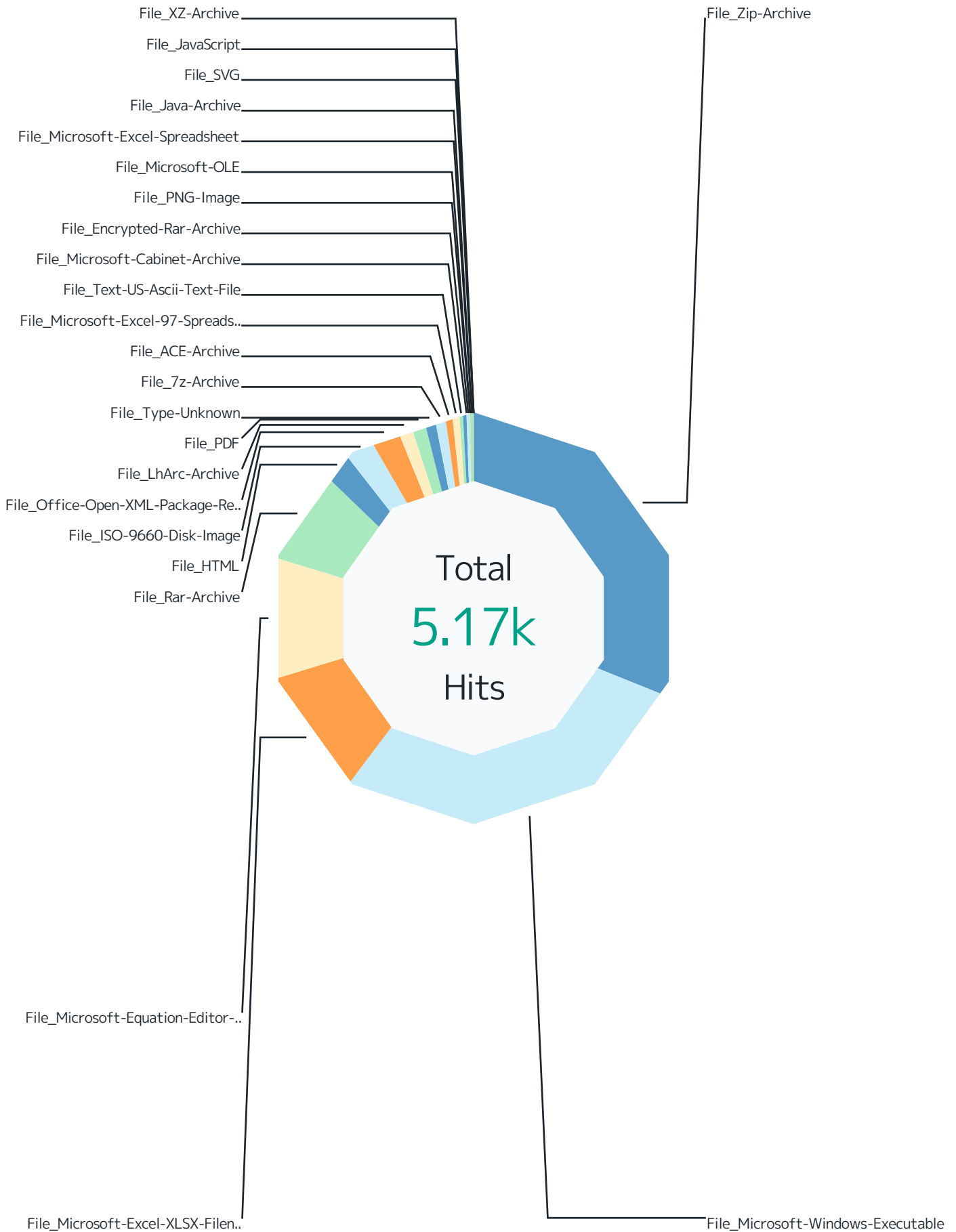
Scan Result	Hits	%
File_LhArc-Archive	3	0.1 %
File_Rar-Archive	1	0.0 %
File_Microsoft-Excel-Spreadsheet	1	0.0 %
<b>Fareit.gen.e</b>	<b>25</b>	<b>0.5 %</b>
File_ACE-Archive	25	0.5 %
<b>Unknown</b>	<b>18</b>	<b>0.3 %</b>
File_Zip-Archive	15	0.3 %
File_Microsoft-Excel-Spreadsheet	2	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
<b>HTML/Phishing.vb</b>	<b>17</b>	<b>0.3 %</b>
File_HTML	17	0.3 %
<b>HTML/Phishing.ok</b>	<b>13</b>	<b>0.3 %</b>
File_HTML	13	0.3 %
<b>Fareit.gen.a</b>	<b>12</b>	<b>0.2 %</b>
File_ACE-Archive	12	0.2 %
<b>HTML/Phishing.vy</b>	<b>10</b>	<b>0.2 %</b>
File_Text-US-Ascii-Text-File	10	0.2 %
<b>HTML/Phishing.ta</b>	<b>8</b>	<b>0.2 %</b>
File_HTML	8	0.2 %
<b>HTML/Phishing.rb</b>	<b>8</b>	<b>0.2 %</b>
File_HTML	5	0.1 %
File_Text-US-Ascii-Text-File	3	0.1 %
<b>X97M/Downloader.pz</b>	<b>8</b>	<b>0.2 %</b>
File_Microsoft-Excel-97-Spreadsheet	8	0.2 %
<b>BAT/Dropper.l</b>	<b>6</b>	<b>0.1 %</b>
File_Rar-Archive	5	0.1 %
File_Type-Unknown	1	0.0 %
<b>HTML/Phishing.ux</b>	<b>5</b>	<b>0.1 %</b>
File_Text-US-Ascii-Text-File	5	0.1 %
<b>AgentTesla-FDUP!A34D1286AAB1</b>	<b>3</b>	<b>0.1 %</b>
File_Rar-Archive	3	0.1 %
<b>AgentTesla-FDUP!15D8D5E540FB</b>	<b>2</b>	<b>0.0 %</b>
File_Rar-Archive	2	0.0 %
<b>Exploit-GBT!8336A9BEC81A</b>	<b>2</b>	<b>0.0 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.0 %
<b>Suspect-BW!90D6764EB069</b>	<b>1</b>	<b>0.0 %</b>
File_Zip-Archive	1	0.0 %
<b>Exploit-GBT!040BCB3C9BBF</b>	<b>1</b>	<b>0.0 %</b>
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %



Scan Result	Hits	%
<b>PWS-FDOO!7C5BECEC271E</b>	<b>1</b>	<b>0.0%</b>
File_Zip-Archive	1	0.0%
<b>RDN/generic.cf</b>	<b>1</b>	<b>0.0%</b>
File_PDF	1	0.0%
<b>HTML/Phishing.ej</b>	<b>1</b>	<b>0.0%</b>
File_HTML	1	0.0%
<b>Trojan-FVTA!2766CD954388</b>	<b>1</b>	<b>0.0%</b>
File_Rar-Archive	1	0.0%
<b>Trojan-FVTA!FA7F0EDB70AC</b>	<b>1</b>	<b>0.0%</b>
File_Rar-Archive	1	0.0%
<b>HTML/Phishing.vj</b>	<b>1</b>	<b>0.0%</b>
File_Text-US-Ascii-Text-File	1	0.0%
<b>HTML/Phishing.vw</b>	<b>1</b>	<b>0.0%</b>
File_HTML	1	0.0%
<b>HTML/Phishing.vq</b>	<b>1</b>	<b>0.0%</b>
File_HTML	1	0.0%
<b>Total</b>	<b>5.17k</b>	<b>100%</b>

## Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.



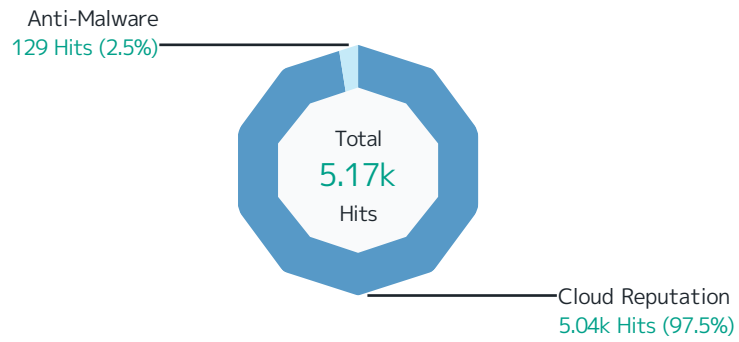
Responding Scanner	Hits	%
<b>File_Zip-Archive</b>	<b>1.61k</b>	<b>31.0 %</b>
Not Available	1.42k	27.4 %
Malicious	171	3.3 %
Unknown	15	0.3 %
Suspect-BW!90D6764EB069	1	0.0 %
PWS-FDOO!7C5BECEC271E	1	0.0 %
<b>File_Microsoft-Windows-Executable</b>	<b>1.51k</b>	<b>29.1 %</b>
Malicious	1.48k	28.6 %
Medium Risk	21	0.4 %
High Risk	4	0.1 %
<b>File_Microsoft-Excel-XLSX-Filename-Extension</b>	<b>522</b>	<b>10.1 %</b>
Not Available	496	9.6 %
Malicious	13	0.3 %
Medium Risk	9	0.2 %
Exploit-GBT!8336A9BEC81A	2	0.0 %
Unknown	1	0.0 %
Exploit-GBT!040BCB3C9BBF	1	0.0 %
<b>File_Microsoft-Equation-Editor-Document</b>	<b>489</b>	<b>9.5 %</b>
Malicious	261	5.0 %
High Risk	228	4.4 %
<b>File_Rar-Archive</b>	<b>385</b>	<b>7.4 %</b>
Malicious	364	7.0 %
High Risk	8	0.2 %
BAT/Dropper.l	5	0.1 %
Agent Tesla-FDUP!A34D1286AAB1	3	0.1 %
Agent Tesla-FDUP!15D8D5E540FB	2	0.0 %
Medium Risk	1	0.0 %
Trojan-FVTA!2766CD954388	1	0.0 %
Trojan-FVTA!FA7FOEDB70AC	1	0.0 %
<b>File_HTML</b>	<b>124</b>	<b>2.4 %</b>
Malicious	66	1.3 %
HTML/Phishing.vb	17	0.3 %
HTML/Phishing.ok	13	0.3 %
Medium Risk	12	0.2 %
HTML/Phishing.ta	8	0.2 %
HTML/Phishing.rb	5	0.1 %
HTML/Phishing.ej	1	0.0 %
HTML/Phishing.vw	1	0.0 %
HTML/Phishing.vq	1	0.0 %

Responding Scanner	Hits	%
<b>File_ISO-9660-Disk-Image</b>	<b>114</b>	<b>2.2 %</b>
Malicious	114	2.2 %
<b>File_Office-Open-XML-Package-Relations-Item</b>	<b>112</b>	<b>2.2 %</b>
Medium Risk	112	2.2 %
<b>File_LhArc-Archive</b>	<b>60</b>	<b>1.2 %</b>
Malicious	54	1.0 %
High Risk	3	0.1 %
Medium Risk	3	0.1 %
<b>File_PDF</b>	<b>54</b>	<b>1.0 %</b>
Medium Risk	39	0.8 %
Malicious	8	0.2 %
High Risk	6	0.1 %
RDN/generic.cf	1	0.0 %
<b>File_Type-Unknown</b>	<b>43</b>	<b>0.8 %</b>
Malicious	24	0.5 %
Medium Risk	18	0.3 %
BAT/Dropper.l	1	0.0 %
<b>File_7z-Archive</b>	<b>38</b>	<b>0.7 %</b>
Malicious	33	0.6 %
High Risk	5	0.1 %
<b>File_ACE-Archive</b>	<b>37</b>	<b>0.7 %</b>
Fareit.gen.e	25	0.5 %
Fareit.gen.a	12	0.2 %
<b>File_Microsoft-Excel-97-Spreadsheet</b>	<b>23</b>	<b>0.4 %</b>
Medium Risk	15	0.3 %
X97M/Downloader.pz	8	0.2 %
<b>File_Text-US-Ascii-Text-File</b>	<b>19</b>	<b>0.4 %</b>
HTML/Phishing.vy	10	0.2 %
HTML/Phishing.ux	5	0.1 %
HTML/Phishing.rb	3	0.1 %
HTML/Phishing.vj	1	0.0 %
<b>File_Microsoft-Cabinet-Archive</b>	<b>17</b>	<b>0.3 %</b>
Malicious	17	0.3 %
<b>File_Encrypted-Rar-Archive</b>	<b>5</b>	<b>0.1 %</b>
Malicious	5	0.1 %
<b>File_PNG-Image</b>	<b>4</b>	<b>0.1 %</b>
Malicious	4	0.1 %
<b>File_Microsoft-OLE</b>	<b>4</b>	<b>0.1 %</b>
Malicious	4	0.1 %

Responding Scanner	Hits	%
<b>File_Microsoft-Excel-Spreadsheet</b>	<b>4</b>	<b>0.1 %</b>
Unknown	2	0.0 %
Not Available	1	0.0 %
Medium Risk	1	0.0 %
<b>File_Java-Archive</b>	<b>3</b>	<b>0.1 %</b>
Malicious	3	0.1 %
<b>File_SVG</b>	<b>1</b>	<b>0.0 %</b>
High Risk	1	0.0 %
<b>File_JavaScript</b>	<b>1</b>	<b>0.0 %</b>
Malicious	1	0.0 %
<b>File_XZ-Archive</b>	<b>1</b>	<b>0.0 %</b>
Malicious	1	0.0 %
<b>Total</b>	<b>5.17k</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>5.04k</b>	<b>97.5 %</b>
File_Zip-Archive	1.60k	31.0 %
File_Microsoft-Windows-Executable	1.51k	29.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	519	10.0 %
File_Microsoft-Equation-Editor-Document	489	9.5 %
File_Rar-Archive	373	7.2 %
File_ISO-9660-Disk-Image	114	2.2 %
File_Office-Open-XML-Package-Relations-Item	112	2.2 %
File_HTML	78	1.5 %
File_LhArc-Archive	60	1.2 %
File_PDF	53	1.0 %
File_Type-Unknown	42	0.8 %
File_7z-Archive	38	0.7 %
File_Microsoft-Cabinet-Archive	17	0.3 %
File_Microsoft-Excel-97-Spreadsheet	15	0.3 %
File_Encrypted-Rar-Archive	5	0.1 %
File_PNG-Image	4	0.1 %
File_Microsoft-OLE	4	0.1 %
File_Microsoft-Excel-Spreadsheet	4	0.1 %
File_Java-Archive	3	0.1 %
File_SVG	1	0.0 %
File_JavaScript	1	0.0 %
File_XZ-Archive	1	0.0 %
<b>Anti-Malware</b>	<b>129</b>	<b>2.5 %</b>
File_HTML	46	0.9 %
File_ACE-Archive	37	0.7 %
File_Text-US-Ascii-Text-File	19	0.4 %
File_Rar-Archive	12	0.2 %
File_Microsoft-Excel-97-Spreadsheet	8	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	3	0.1 %
File_Zip-Archive	2	0.0 %
File_PDF	1	0.0 %
File_Type-Unknown	1	0.0 %
<b>Total</b>	<b>5.17k</b>	<b>100 %</b>



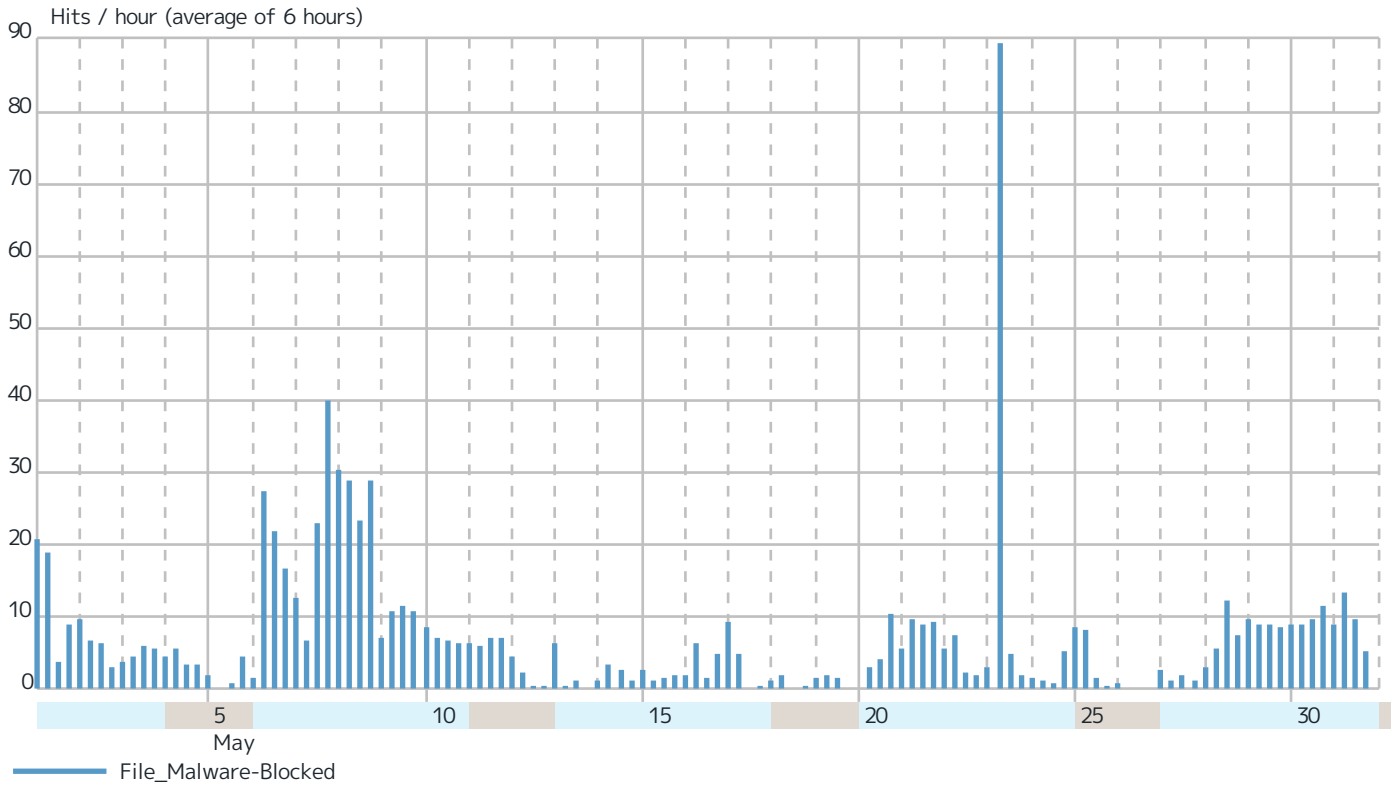
## Virenfilterung SRC IPs



Records by src IP		Hits	%
173.249.147.74	United States	856	16.5 %
217.111.48.171	Munich, Germany	690	13.3 %
104.168.132.251	United States	631	12.2 %
192.236.163.63	United States	504	9.7 %
134.17.4.170	Minsk, Belarus	220	4.3 %
23.254.253.96	United States	178	3.4 %
23.21.224.96	Ashburn, Virginia 20149, United States	128	2.5 %
69.169.224.18	Charlotte, North Carolina 28202, United States	90	1.7 %
69.169.224.14	Charlotte, North Carolina 28202, United States	90	1.7 %
172.104.156.238	Frankfurt am Main, Germany	88	1.7 %
69.169.224.17	Charlotte, North Carolina 28202, United States	86	1.7 %
69.169.224.13	Charlotte, North Carolina 28202, United States	84	1.6 %
209.159.150.110	United States	79	1.5 %
212.227.154.123	Germany	74	1.4 %
38.255.55.89	Dallas, Texas 75207, United States	46	0.9 %
213.61.254.52	Munich, Germany	40	0.8 %
82.194.67.103	Spain	39	0.8 %
89.46.33.172	Karaganda, Kazakhstan	38	0.7 %
190.210.9.116	Buenos Aires, Argentina	36	0.7 %
46.227.62.50	Greece	32	0.6 %
64.188.22.81	Amsterdam, The Netherlands	30	0.6 %
211.41.123.6	South Korea	29	0.6 %
31.24.158.19	Spain	29	0.6 %
213.142.149.243	Istanbul, Türkiye	26	0.5 %
179.43.122.78	Rosario, Argentina	22	0.4 %
5.175.40.110	Spain	22	0.4 %
36.50.232.93	Vietnam	20	0.4 %
107.174.244.98	Seattle, Washington 98160, United States	18	0.3 %
80.85.153.109	Russia	18	0.3 %
104.168.153.8	United States	17	0.3 %
Others		913	17.6 %
<b>Total</b>		<b>5.17k</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.