Forcepoint

# NGFW Security Management Center

## E-Mail Virenfilterung Server Firewall

**Report period**

From: 2022-07-01 00:00:00 CEST
To: 2022-08-01 00:00:00 CEST

# Report

**Report run by**
bk228682

**SMC version**
6.11.1, build 11219

**Update version**
1488

**Report started**
2022-08-01 11:24:34 CEST

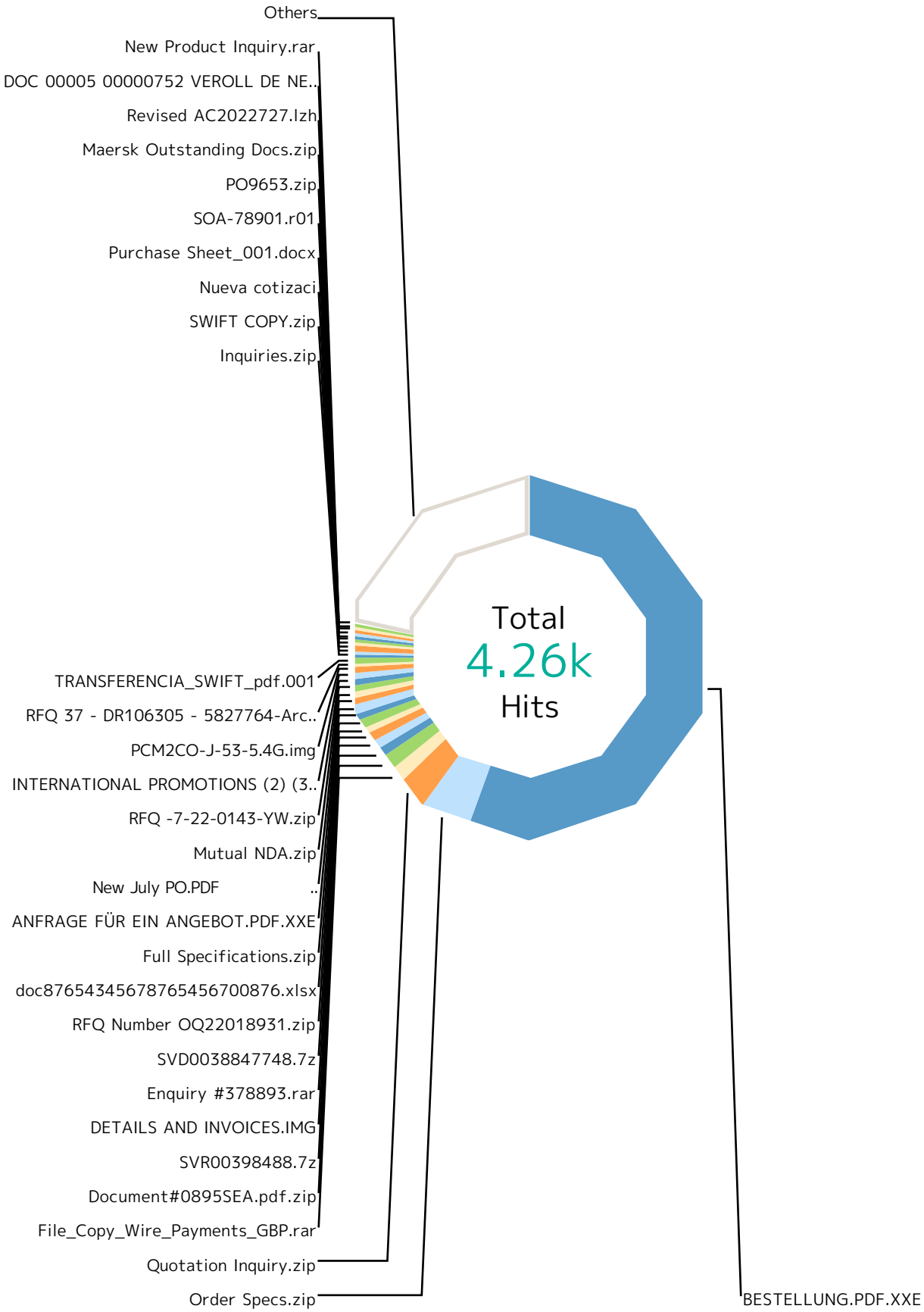
**Report run time**
02:08:08

**Filters used**
Match All

## Table of Contents

# Report

## Virenfilterung MXe



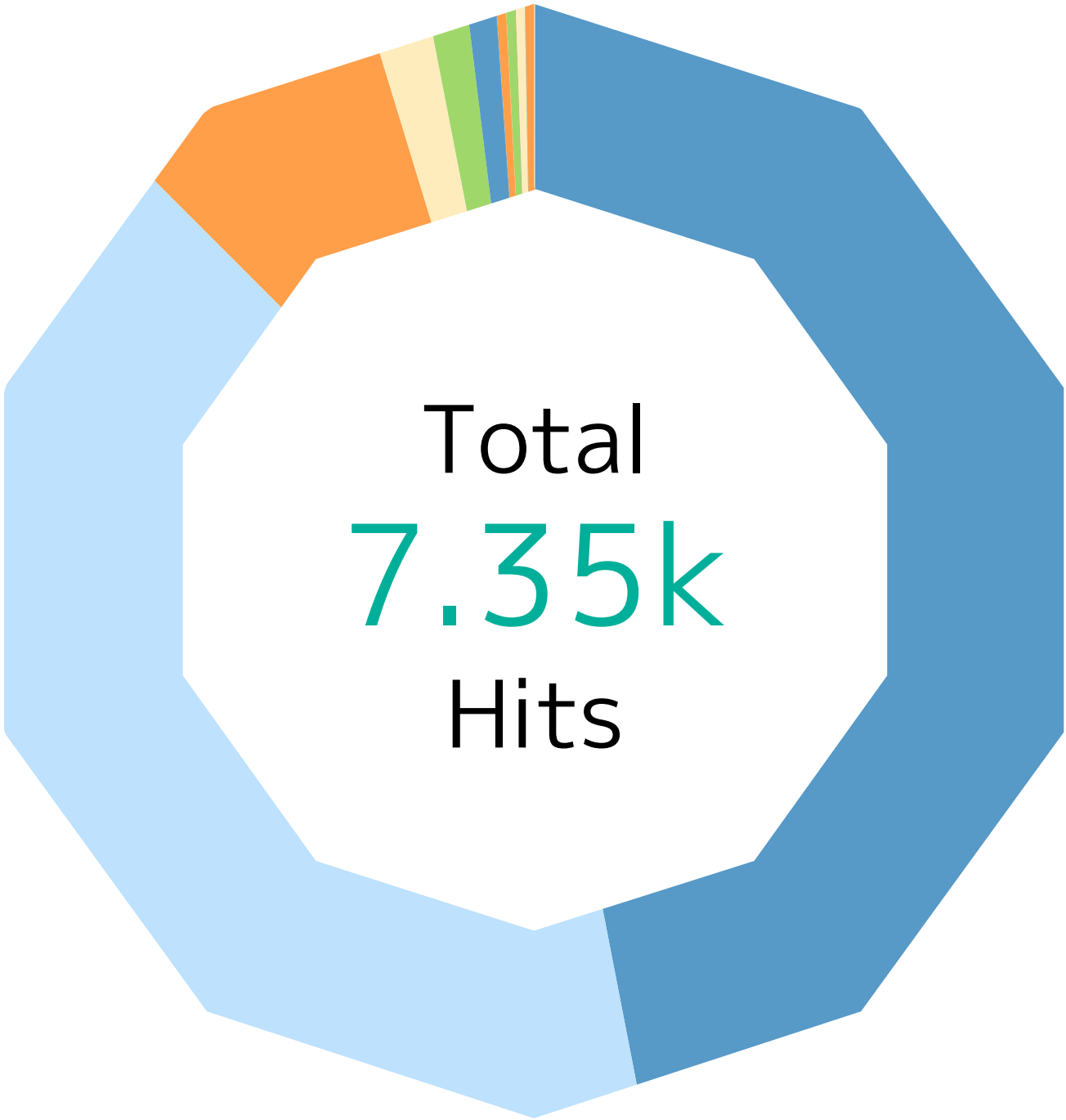
# Report

| Records by file name | Hits | % |
|---|---|---|
| BESTELLUNG.PDF.XXE | 2.37k | 55.7 % |
| Order Specs.zip | 183 | 4.3 % |
| Quotation Inquiry.zip | 124 | 2.9 % |
| File_Copy_Wire_Payments_GBP.rar | 58 | 1.4 % |
| Document#0895SEA.pdf.zip | 53 | 1.2 % |
| SVR00398488.7z | 40 | 0.9 % |
| DETAILS AND INVOICES.IMG | 37 | 0.9 % |
| Enquiry #378893.rar | 31 | 0.7 % |
| SVD0038847748.7z | 30 | 0.7 % |
| RFQ Number OQ22018931.zip | 29 | 0.7 % |
| doc87654345678765456700876.xlsx | 29 | 0.7 % |
| Full Specifications.zip | 28 | 0.7 % |
| ANFRAGE FÜR EIN ANGEBOT.PDF.XXE | 28 | 0.7 % |
| New July PO.PDF .HTML | 27 | 0.6 % |
| Mutual NDA.zip | 25 | 0.6 % |
| RFQ -7-22-0143-YW.zip | 23 | 0.5 % |
| INTERNATIONAL PROMOTIONS (2) (3).pdf | 21 | 0.5 % |
| PCM2CO-J-53-5.4G.img | 19 | 0.4 % |
| RFQ 37 - DR106305 - 5827764-ArcelorMittal.img | 18 | 0.4 % |
| TRANSFERENCIA_SWIFT_pdf.001 | 17 | 0.4 % |
| Inquiries.zip | 16 | 0.4 % |
| SWIFT COPY.zip | 16 | 0.4 % |
| Nueva cotizaci | 15 | 0.4 % |
| Purchase Sheet_001.docx | 15 | 0.4 % |
| SOA-78901.r01 | 13 | 0.3 % |
| PO9653.zip | 13 | 0.3 % |
| Maersk Outstanding Docs.zip | 12 | 0.3 % |
| Revised AC2022727.lzh | 12 | 0.3 % |
| DOC 00005 00000752 VEROLL DE NERBRIS SA.xlsx | 12 | 0.3 % |
| New Product Inquiry.rar | 11 | 0.3 % |
| Others | 933 | 21.9 % |
| **Total** | **4.26k** | **100 %** |

# Report

## Top File Types by Scan Result

Top 10 file types by scan result.


Total
7.35k
Hits

# Report

| Scan Result | Hits | % |
|---|---|---|
| **Malicious** | **3.46k** | **47.0 %** |
| File_Microsoft-Windows-Executable | 2.91k | 39.5 % |
| File_Microsoft-Excel-97-Spreadsheet | 122 | 1.7 % |
| File_Rar-Archive | 118 | 1.6 % |
| File_ISO-9660-Disk-Image | 108 | 1.5 % |
| File_Zip-Archive | 70 | 1.0 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 50 | 0.7 % |
| File_7z-Archive | 27 | 0.4 % |
| File_Office-Open-XML-Package-Relations-Item | 17 | 0.2 % |
| File_Self-Extracting-Zip-Archive | 16 | 0.2 % |
| File_ACE-Archive | 5 | 0.1 % |
| File_HTML | 4 | 0.1 % |
| File_Microsoft-Office-Open-XML-Document | 4 | 0.1 % |
| File_Microsoft-OLE | 4 | 0.1 % |
| File_Type-Unknown | 3 | 0.0 % |
| File_Microsoft-Equation-Editor-Document | 3 | 0.0 % |
| File_LhArc-Archive | 1 | 0.0 % |
| **Not Available** | **2.99k** | **40.6 %** |
| File_Zip-Archive | 2.98k | 40.5 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 7 | 0.1 % |
| File_Microsoft-Office-Open-XML-Document | 2 | 0.0 % |
| **High Risk** | **560** | **7.6 %** |
| File_Rar-Archive | 161 | 2.2 % |
| File_Microsoft-Windows-Executable | 113 | 1.5 % |
| File_ISO-9660-Disk-Image | 97 | 1.3 % |
| File_7z-Archive | 58 | 0.8 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 38 | 0.5 % |
| File_Zip-Archive | 27 | 0.4 % |
| File_PDF | 25 | 0.3 % |
| File_Type-Unknown | 13 | 0.2 % |
| File_Microsoft-Excel-97-Spreadsheet | 12 | 0.2 % |
| File_Office-Open-XML-Package-Relations-Item | 6 | 0.1 % |
| File_Microsoft-Cabinet-Archive | 3 | 0.0 % |
| File_Microsoft-Office-Open-XML-Document | 2 | 0.0 % |
| File_ACE-Archive | 1 | 0.0 % |
| File_Microsoft-OLE | 1 | 0.0 % |

# Report

| Scan Result | Hits | % |
|---|---|---|
| File_Microsoft-Equation-Editor-Document | 1 | 0.0 % |
| File_Visual-Basic-Script-Filename | 1 | 0.0 % |
| File_XZ-Archive | 1 | 0.0 % |
| **Medium Risk** | **125** | **1.7 %** |
| File_Microsoft-Windows-Executable | 28 | 0.4 % |
| File_JavaScript | 27 | 0.4 % |
| File_ISO-9660-Disk-Image | 22 | 0.3 % |
| File_7z-Archive | 13 | 0.2 % |
| File_Rar-Archive | 11 | 0.1 % |
| File_Zip-Archive | 9 | 0.1 % |
| File_Type-Unknown | 6 | 0.1 % |
| File_ACE-Archive | 5 | 0.1 % |
| File_XML | 2 | 0.0 % |
| File_HTML | 1 | 0.0 % |
| File_Microsoft-Office-Open-XML-Document | 1 | 0.0 % |
| **X97M/Downloader.ph** | **76** | **1.0 %** |
| File_Microsoft-Excel-97-Spreadsheet | 76 | 1.0 % |
| **GenericRXRU-WN!4138156A2540** | **57** | **0.8 %** |
| File_Rar-Archive | 57 | 0.8 % |
| **Exploit-GBT!5C235A9C3F5F** | **15** | **0.2 %** |
| File_Microsoft-Excel-Spreadsheet | 15 | 0.2 % |
| **AgentTesla-FDIL!32DF082BFBE3** | **11** | **0.1 %** |
| File_Rar-Archive | 11 | 0.1 % |
| **Exploit-GBT!955711D0775A** | **8** | **0.1 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 8 | 0.1 % |
| **Unknown** | **7** | **0.1 %** |
| File_Zip-Archive | 7 | 0.1 % |
| **Fareit.gen.a** | **7** | **0.1 %** |
| File_ACE-Archive | 7 | 0.1 % |
| **HTML/Phishing.ca** | **7** | **0.1 %** |
| File_HTML | 7 | 0.1 % |
| **Downloader-FCIV!5A14D9202389** | **5** | **0.1 %** |
| File_ISO-9660-Disk-Image | 5 | 0.1 % |
| **Fareit-FCVN!44D34FAFE191** | **5** | **0.1 %** |
| File_Rar-Archive | 5 | 0.1 % |
| **Fareit.gen.e** | **3** | **0.0 %** |

# Report

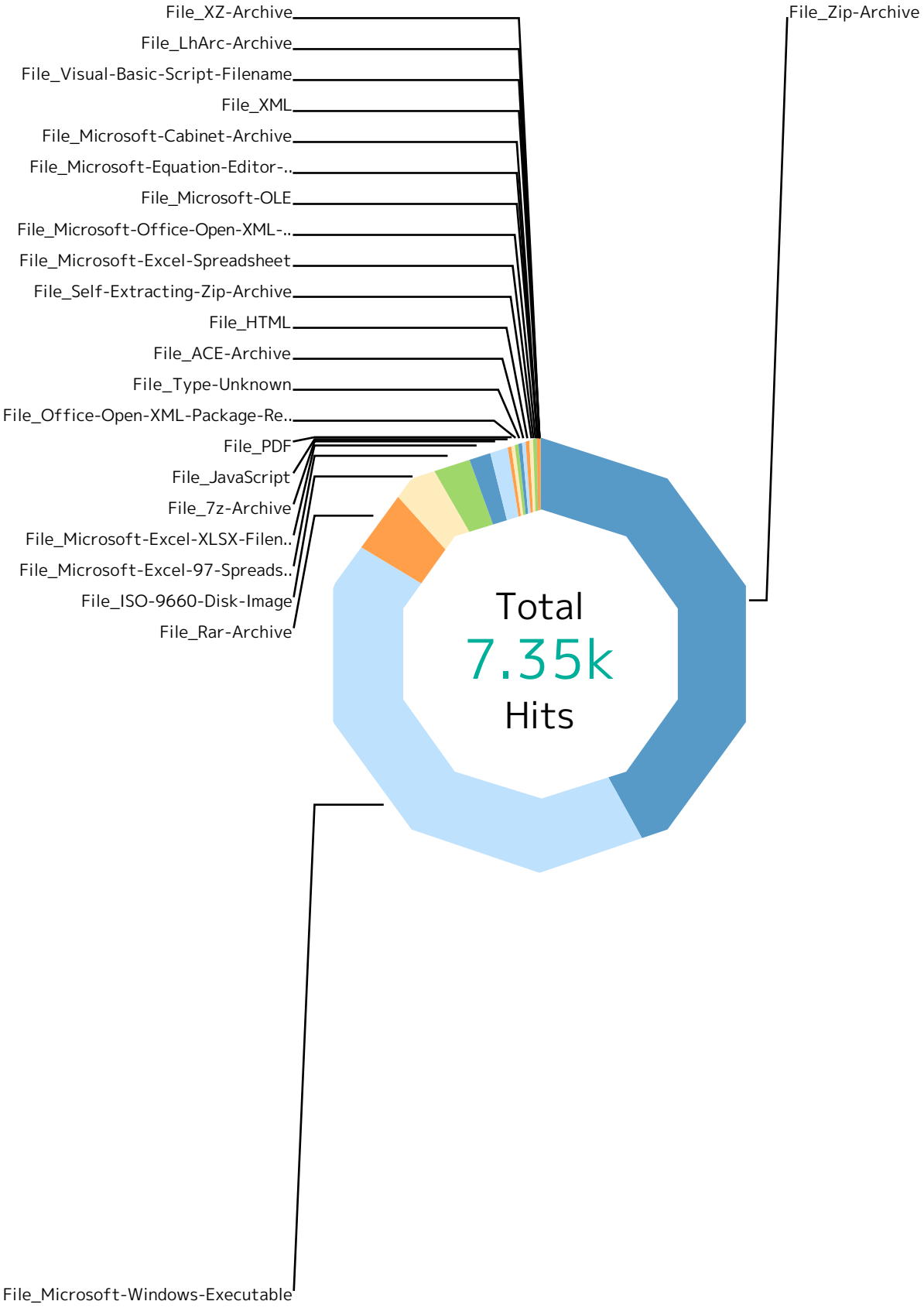
| Scan Result | Hits | % |
|---|---|---|
| File_ACE-Archive | 3 | 0.0 % |
| **HTML/Phishing.iz** | **3** | **0.0 %** |
| File_HTML | 3 | 0.0 % |
| **Exploit-GBT!ADB1EE34A42F** | **3** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 3 | 0.0 % |
| **Exploit-GBT!1B86B93A344E** | **2** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 2 | 0.0 % |
| **GenericRXTL-OB!AAB495E0DDEE** | **1** | **0.0 %** |
| File_ISO-9660-Disk-Image | 1 | 0.0 % |
| **Exploit-GBT!208B5239E60E** | **1** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.0 % |
| **GenericRXRV-YQ!35B67E168324** | **1** | **0.0 %** |
| File_Rar-Archive | 1 | 0.0 % |
| **Exploit-GBT!F8F18FA0786B** | **1** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.0 % |
| **HTML/Phishing.hx** | **1** | **0.0 %** |
| File_HTML | 1 | 0.0 % |
| **W32/Mydoom.t@MM!zip** | **1** | **0.0 %** |
| File_Zip-Archive | 1 | 0.0 % |
| **Exploit-GBT!BBCBAF5772A8** | **1** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.0 % |
| **HTML/Phishing.ej** | **1** | **0.0 %** |
| File_HTML | 1 | 0.0 % |
| **HTML/Phishing.mb** | **1** | **0.0 %** |
| File_HTML | 1 | 0.0 % |
| **PWS-FDBP!1328CC103AF2** | **1** | **0.0 %** |
| File_Rar-Archive | 1 | 0.0 % |
| **Exploit-GBT!D9C94276B60B** | **1** | **0.0 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.0 % |
| **Downloader-FCIV!C35B54DAEE72** | **1** | **0.0 %** |
| File_ISO-9660-Disk-Image | 1 | 0.0 % |
| **Others** | **3** | **0.0 %** |
| **Total** | **7.35k** | **100 %** |

# Report

## Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

# Report


File_XZ-Archive
File_LhArc-Archive
File_Visual-Basic-Script-Filename
File_XML
File_Microsoft-Cabinet-Archive
File_Microsoft-Equation-Editor-..
File_Microsoft-OLE
File_Microsoft-Office-Open-XML-..
File_Microsoft-Excel-Spreadsheet
File_Self-Extracting-Zip-Archive
File_HTML
File_ACE-Archive
File_Type-Unknown
File_Office-Open-XML-Package-Re..
File_PDF
File_JavaScript
File_7z-Archive
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Excel-97-Spreads..
File_ISO-9660-Disk-Image
File_Rar-Archive
File_Zip-Archive
Total
7.35k
Hits
File_Microsoft-Windows-Executable

# Report

| Responding Scanner | Hits | % |
|---|---|---|
| **File_Zip-Archive** | **3.09k** | **42.0 %** |
| Not Available | 2.98k | 40.5 % |
| Malicious | 70 | 1.0 % |
| High Risk | 27 | 0.4 % |
| Medium Risk | 9 | 0.1 % |
| Unknown | 7 | 0.1 % |
| W32/Mydoom.t@MM!zip | 1 | 0.0 % |
| X97M/Downloader.pf | 1 | 0.0 % |
| **File_Microsoft-Windows-Executable** | **3.05k** | **41.5 %** |
| Malicious | 2.91k | 39.5 % |
| High Risk | 113 | 1.5 % |
| Medium Risk | 28 | 0.4 % |
| **File_Rar-Archive** | **365** | **5.0 %** |
| High Risk | 161 | 2.2 % |
| Malicious | 118 | 1.6 % |
| GenericRXRU-WN!4138156A2540 | 57 | 0.8 % |
| Medium Risk | 11 | 0.1 % |
| AgentTesla-FDIL!32DF082BFBE3 | 11 | 0.1 % |
| Fareit-FCVN!44D34FAFE191 | 5 | 0.1 % |
| GenericRXRV-YQ!35B67E168324 | 1 | 0.0 % |
| PWS-FDBP!1328CC103AF2 | 1 | 0.0 % |
| **File_ISO-9660-Disk-Image** | **234** | **3.2 %** |
| Malicious | 108 | 1.5 % |
| High Risk | 97 | 1.3 % |
| Medium Risk | 22 | 0.3 % |
| Downloader-FCIV!5A14D9202389 | 5 | 0.1 % |
| GenericRXTL-OB!AAB495E0DDEE | 1 | 0.0 % |
| Downloader-FCIV!C35B54DAEE72 | 1 | 0.0 % |
| **File_Microsoft-Excel-97-Spreadsheet** | **210** | **2.9 %** |
| Malicious | 122 | 1.7 % |
| X97M/Downloader.ph | 76 | 1.0 % |
| High Risk | 12 | 0.2 % |
| **File_Microsoft-Excel-XLSX-Filename-Extension** | **114** | **1.6 %** |
| Malicious | 50 | 0.7 % |
| High Risk | 38 | 0.5 % |
| Exploit-GBT!955711D0775A | 8 | 0.1 % |

# Report

| Responding Scanner | Hits | % |
|---|---|---|
| Not Available | 7 | 0.1 % |
| Exploit-GBT!ADB1EE34A42F | 3 | 0.0 % |
| Exploit-GBT!1B86B93A344E | 2 | 0.0 % |
| Exploit-GBT!208B5239E60E | 1 | 0.0 % |
| Exploit-GBT!F8F18FA0786B | 1 | 0.0 % |
| Exploit-GBT!BBCBAF5772A8 | 1 | 0.0 % |
| Exploit-GBT!D9C94276B60B | 1 | 0.0 % |
| Exploit-GBT!D016A51B3EF1 | 1 | 0.0 % |
| Exploit-CVE2017-11882.yx | 1 | 0.0 % |
| **File_7z-Archive** | **98** | **1.3 %** |
| High Risk | 58 | 0.8 % |
| Malicious | 27 | 0.4 % |
| Medium Risk | 13 | 0.2 % |
| **File_JavaScript** | **27** | **0.4 %** |
| Medium Risk | 27 | 0.4 % |
| **File_PDF** | **25** | **0.3 %** |
| High Risk | 25 | 0.3 % |
| **File_Office-Open-XML-Package-Relations-Item** | **23** | **0.3 %** |
| Malicious | 17 | 0.2 % |
| High Risk | 6 | 0.1 % |
| **File_Type-Unknown** | **22** | **0.3 %** |
| High Risk | 13 | 0.2 % |
| Medium Risk | 6 | 0.1 % |
| Malicious | 3 | 0.0 % |
| **File_ACE-Archive** | **21** | **0.3 %** |
| Fareit.gen.a | 7 | 0.1 % |
| Malicious | 5 | 0.1 % |
| Medium Risk | 5 | 0.1 % |
| Fareit.gen.e | 3 | 0.0 % |
| High Risk | 1 | 0.0 % |
| **File_HTML** | **18** | **0.2 %** |
| HTML/Phishing.ca | 7 | 0.1 % |
| Malicious | 4 | 0.1 % |
| HTML/Phishing.iz | 3 | 0.0 % |
| Medium Risk | 1 | 0.0 % |
| HTML/Phishing.hx | 1 | 0.0 % |

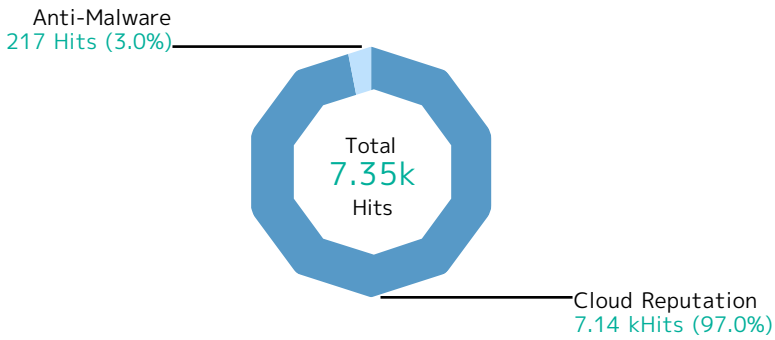
# Report

| Responding Scanner | Hits | % |
|---|---|---|
| HTML/Phishing.ej | 1 | 0.0 % |
| HTML/Phishing.mb | 1 | 0.0 % |
| **File_Self-Extracting-Zip-Archive** | **16** | **0.2 %** |
| Malicious | 16 | 0.2 % |
| **File_Microsoft-Excel-Spreadsheet** | **15** | **0.2 %** |
| Exploit-GBT!5C235A9C3F5F | 15 | 0.2 % |
| **File_Microsoft-Office-Open-XML-Document** | **9** | **0.1 %** |
| Malicious | 4 | 0.1 % |
| Not Available | 2 | 0.0 % |
| High Risk | 2 | 0.0 % |
| Medium Risk | 1 | 0.0 % |
| **File_Microsoft-OLE** | **5** | **0.1 %** |
| Malicious | 4 | 0.1 % |
| High Risk | 1 | 0.0 % |
| **File_Microsoft-Equation-Editor-Document** | **4** | **0.1 %** |
| Malicious | 3 | 0.0 % |
| High Risk | 1 | 0.0 % |
| **File_Microsoft-Cabinet-Archive** | **3** | **0.0 %** |
| High Risk | 3 | 0.0 % |
| **File_XML** | **2** | **0.0 %** |
| Medium Risk | 2 | 0.0 % |
| **File_Visual-Basic-Script-Filename** | **1** | **0.0 %** |
| High Risk | 1 | 0.0 % |
| **File_LhArc-Archive** | **1** | **0.0 %** |
| Malicious | 1 | 0.0 % |
| **File_XZ-Archive** | **1** | **0.0 %** |
| High Risk | 1 | 0.0 % |
| **Total** | **7.35k** | **100 %** |

# Report

## Top File Types by Responding Scanner

Top 10 file types by responding scanner.

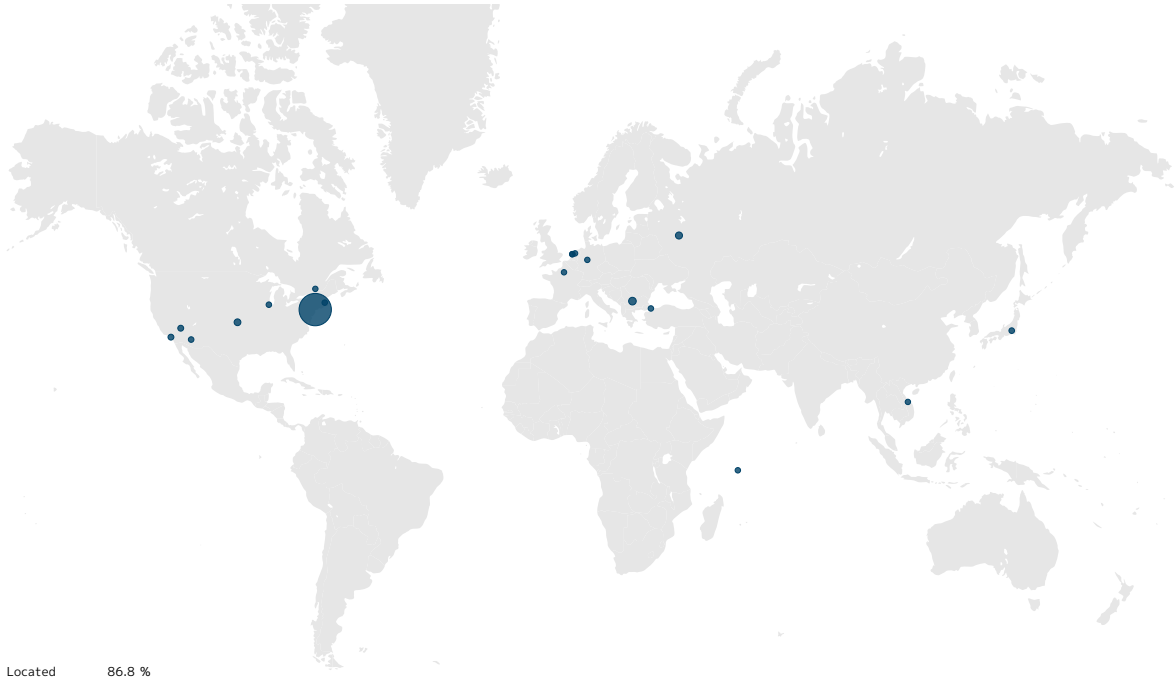


# Report

| Responding Scanner | Hits | % |
|---|---|---|
| **Cloud Reputation** | **7.14k** | **97.0 %** |
| File_Zip-Archive | 3.09k | 42.0 % |
| File_Microsoft-Windows-Executable | 3.05k | 41.5 % |
| File_Rar-Archive | 290 | 3.9 % |
| File_ISO-9660-Disk-Image | 227 | 3.1 % |
| File_Microsoft-Excel-97-Spreadsheet | 134 | 1.8 % |
| File_7z-Archive | 98 | 1.3 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 95 | 1.3 % |
| File_JavaScript | 27 | 0.4 % |
| File_PDF | 25 | 0.3 % |
| File_Office-Open-XML-Package-Relations-Item | 23 | 0.3 % |
| File_Type-Unknown | 22 | 0.3 % |
| File_Self-Extracting-Zip-Archive | 16 | 0.2 % |
| File_ACE-Archive | 11 | 0.1 % |
| File_Microsoft-Office-Open-XML-Document | 9 | 0.1 % |
| File_HTML | 5 | 0.1 % |
| File_Microsoft-OLE | 5 | 0.1 % |
| File_Microsoft-Equation-Editor-Document | 4 | 0.1 % |
| File_Microsoft-Cabinet-Archive | 3 | 0.0 % |
| File_XML | 2 | 0.0 % |
| File_Visual-Basic-Script-Filename | 1 | 0.0 % |
| File_LhArc-Archive | 1 | 0.0 % |
| File_XZ-Archive | 1 | 0.0 % |
| **Anti-Malware** | **217** | **3.0 %** |
| File_Microsoft-Excel-97-Spreadsheet | 76 | 1.0 % |
| File_Rar-Archive | 75 | 1.0 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 19 | 0.3 % |
| File_Microsoft-Excel-Spreadsheet | 15 | 0.2 % |
| File_HTML | 13 | 0.2 % |
| File_ACE-Archive | 10 | 0.1 % |
| File_ISO-9660-Disk-Image | 7 | 0.1 % |
| File_Zip-Archive | 2 | 0.0 % |
| **Total** | **7.35k** | **100 %** |

# Report

## Virenfilterung SRC IPs



Located 86.8 %

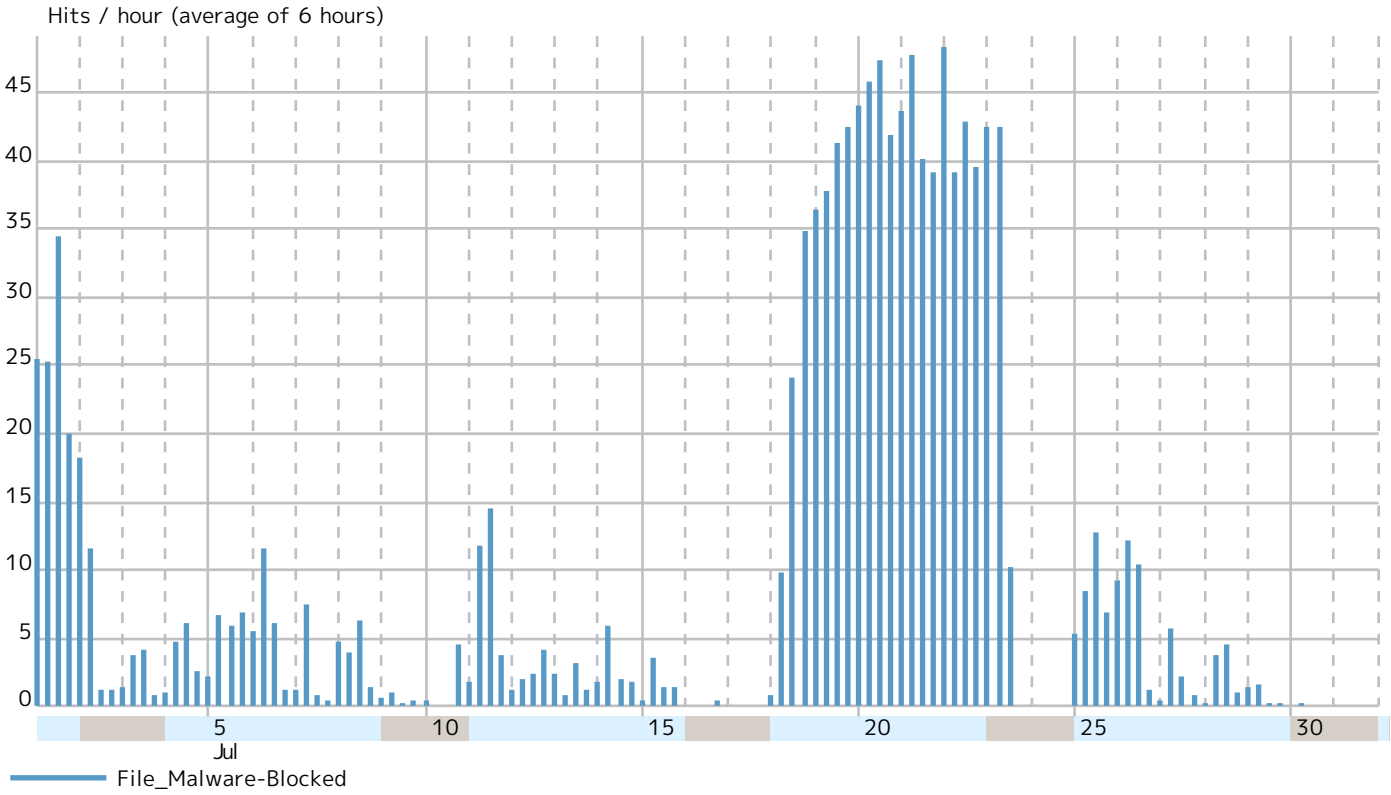
# Report

| Records by src IP | | Hits | % |
|---|---|---|---|
| 162.243.109.74 | New York, New York 10011, United States | 4.77k | 64.9 % |
| 87.121.98.44 | Bulgaria | 366 | 5.0 % |
| 45.95.235.79 | Russia | 248 | 3.4 % |
| 104.168.174.38 | United States | 106 | 1.4 % |
| 192.228.105.15 | Las Vegas, Nevada 89131, United States | 102 | 1.4 % |
| 74.201.28.144 | Los Angeles, California 90060, United States | 100 | 1.4 % |
| 162.240.1.83 | United States | 75 | 1.0 % |
| 193.111.30.131 | Tokyo, Japan | 58 | 0.8 % |
| 66.154.98.28 | Phoenix, Arizona 85034, United States | 50 | 0.7 % |
| 192.34.84.58 | Boston, Massachusetts 02266, United States | 37 | 0.5 % |
| 198.71.53.214 | United States | 32 | 0.4 % |
| 45.95.235.81 | Russia | 32 | 0.4 % |
| 185.238.2.45 | Seychelles | 30 | 0.4 % |
| 185.222.57.180 | Amsterdam, Netherlands | 30 | 0.4 % |
| 5.252.23.43 | Russia | 29 | 0.4 % |
| 185.28.62.201 | Turkey | 28 | 0.4 % |
| 202.4.37.25 | Samoa | 27 | 0.4 % |
| 185.246.220.234 | Bulgaria | 26 | 0.4 % |
| 172.93.193.179 | Chicago, Illinois 60185, United States | 24 | 0.3 % |
| 159.223.193.17 | United States | 24 | 0.3 % |
| 178.159.42.12 | Dronten, Netherlands | 21 | 0.3 % |
| 107.173.58.27 | United States | 20 | 0.3 % |
| 62.4.27.48 | France | 20 | 0.3 % |
| 79.124.60.85 | Bulgaria | 20 | 0.3 % |
| 185.222.57.211 | Amsterdam, Netherlands | 20 | 0.3 % |
| 45.117.164.146 | Vietnam | 19 | 0.3 % |
| 144.168.227.33 | Montreal, Quebec H9X , Canada | 18 | 0.2 % |
| 82.165.73.113 | Germany | 18 | 0.2 % |
| 45.141.239.121 | Netherlands | 18 | 0.2 % |
| 172.93.201.171 | Chicago, Illinois 60185, United States | 17 | 0.2 % |
| Others | | 969 | 13.2 % |
| **Total** | | **7.35k** | **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.