Forcepoint

# NGFW Security Management Center

## E-Mail Virenfilterung Server Firewall

**Report period**

From: 2023-04-01 00:00:00 CEST
To: 2023-05-01 00:00:00 CEST

# Report

**Report run by**
jens

**SMC version**
7.0.2, build 11323

**Update version**
1581

**Report started**
2023-05-02 07:34:49 CEST

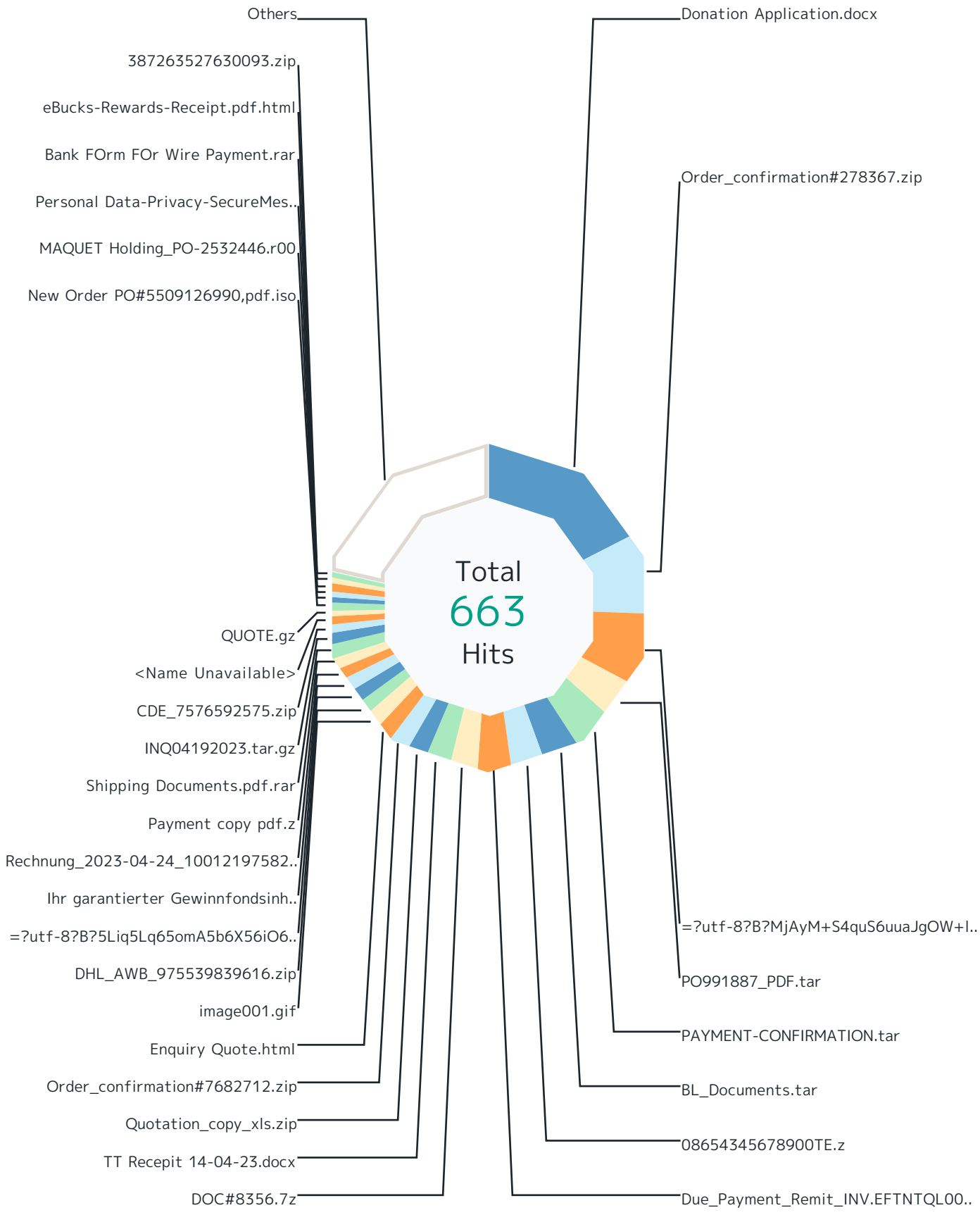
**Report run time**
14:25:46

**Filters used**
Match All

## Table of Contents

# Report

## Virenfilterung MXe



# Report

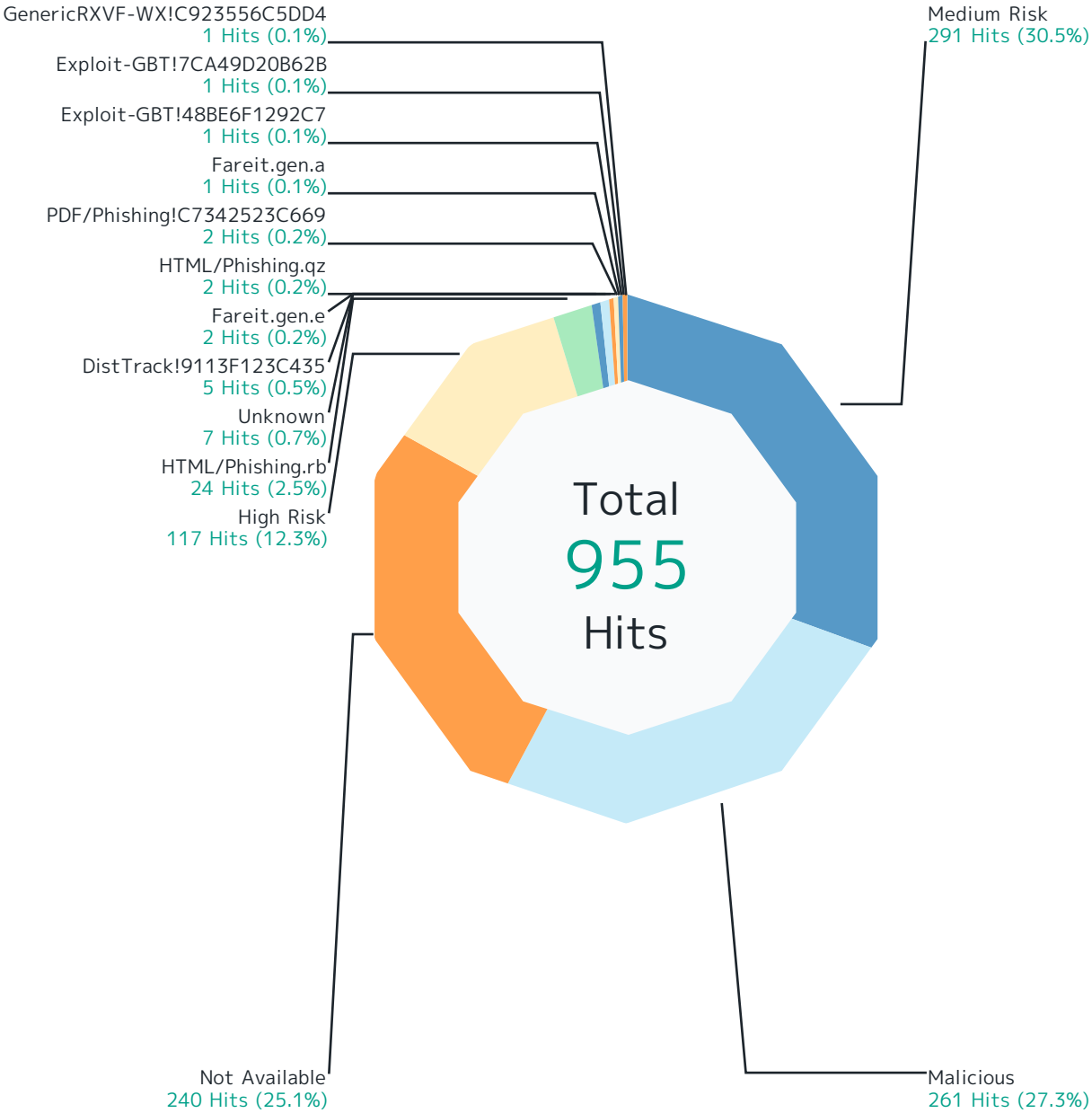
| Records by file name | Hits | % |
|---|---|---|
| Donation Application.docx | 116 | 17.5 % |
| Order_confirmation#278367.zip | 53 | 8.0 % |
| =?utf-8?B?MjAyM+S4quS6uuaJgOW+l+eojuihpei0tOi1hOaWmeeUs+mihiAuZG9jeA==?= | 49 | 7.4 % |
| PO991887_PDF.tar | 26 | 3.9 % |
| PAYMENT-CONFIRMATION.tar | 26 | 3.9 % |
| BL_Documents.tar | 25 | 3.8 % |
| 08654345678900TE.z | 22 | 3.3 % |
| Due_Payment_Remit_INV.EFTNTQL00705VxTsndUGFbuYAz5b6SAd6 .html | 22 | 3.3 % |
| DOC#8356.7z | 19 | 2.9 % |
| TT Recepit 14-04-23.docx | 15 | 2.3 % |
| Quotation_copy_xls.zip | 13 | 2.0 % |
| Order_confirmation#7682712.zip | 13 | 2.0 % |
| Enquiry Quote.html | 12 | 1.8 % |
| image001.gif | 10 | 1.5 % |
| DHL_AWB_975539839616.zip | 10 | 1.5 % |
| =?utf-8?B?5Liq5Lq65omA5b6X56iO6LWE5paZ6KGI5YWF77yBLmRvY3g=?= | 9 | 1.4 % |
| Ihr garantierter Gewinnfondsinhalt.pdf | 9 | 1.4 % |
| Rechnung_2023-04-24_100121975828_V47487970.pdf.html | 8 | 1.2 % |
| Payment copy pdf.z | 8 | 1.2 % |
| Shipping Documents.pdf.rar | 8 | 1.2 % |
| INQ04192023.tar.gz | 7 | 1.1 % |
| CDE_7576592575.zip | 6 | 0.9 % |
| <Name Unavailable> | 5 | 0.8 % |
| QUOTE.gz | 5 | 0.8 % |
| New Order PO#5509126990,pdf.iso | 5 | 0.8 % |
| MAQUET Holding_PO-2532446.r00 | 4 | 0.6 % |
| Personal Data-Privacy-SecureMessageAtt.html | 4 | 0.6 % |
| Bank FOrm FOr Wire Payment.rar | 4 | 0.6 % |
| eBucks-Rewards-Receipt.pdf.html | 4 | 0.6 % |
| 387263527630093.zip | 4 | 0.6 % |
| Others | 142 | 21.4 % |
| **Total** | **663** | **100 %** |

# Report

## Top File Types by Scan Result

Top 10 file types by scan result.

# Report




| Scan Result | Hits | % |
|---|---|---|
| **Medium Risk** | **291** | **30.5 %** |

# Report

| Scan Result | Hits | % |
|---|---|---|
| File_Microsoft-OLE | 116 | 12.1 % |
| File_Zip-Archive | 74 | 7.7 % |
| File_Tar-Archive | 53 | 5.5 % |
| File_GIF-Image | 12 | 1.3 % |
| File_Rar-Archive | 11 | 1.2 % |
| File_Microsoft-Windows-Executable | 10 | 1.0 % |
| File_HTML | 7 | 0.7 % |
| File_7z-Archive | 5 | 0.5 % |
| File_Self-Extracting-Zip-Archive | 1 | 0.1 % |
| File_JavaScript | 1 | 0.1 % |
| File_XZ-Archive | 1 | 0.1 % |
| **Malicious** | **261** | **27.3 %** |
| File_Microsoft-Windows-Executable | 124 | 13.0 % |
| File_Zip-Archive | 31 | 3.2 % |
| File_Rar-Archive | 22 | 2.3 % |
| File_HTML | 21 | 2.2 % |
| File_Self-Extracting-Zip-Archive | 20 | 2.1 % |
| File_Office-Open-XML-Package-Relations-Item | 15 | 1.6 % |
| File_JavaScript | 14 | 1.5 % |
| File_Type-Unknown | 6 | 0.6 % |
| File_ISO-9660-Disk-Image | 3 | 0.3 % |
| File_Microsoft-Office-Open-XML-Document | 2 | 0.2 % |
| File_Microsoft-Cabinet-Archive | 2 | 0.2 % |
| File_XZ-Archive | 1 | 0.1 % |
| **Not Available** | **240** | **25.1 %** |
| File_Zip-Archive | 238 | 24.9 % |
| File_Microsoft-Office-Open-XML-Document | 2 | 0.2 % |
| **High Risk** | **117** | **12.3 %** |
| File_Rar-Archive | 33 | 3.5 % |
| File_Tar-Archive | 25 | 2.6 % |
| File_Zip-Archive | 15 | 1.6 % |
| File_7z-Archive | 14 | 1.5 % |
| File_Microsoft-Windows-Executable | 13 | 1.4 % |
| File_PDF | 9 | 0.9 % |
| File_ISO-9660-Disk-Image | 3 | 0.3 % |
| File_Type-Unknown | 3 | 0.3 % |

# Report

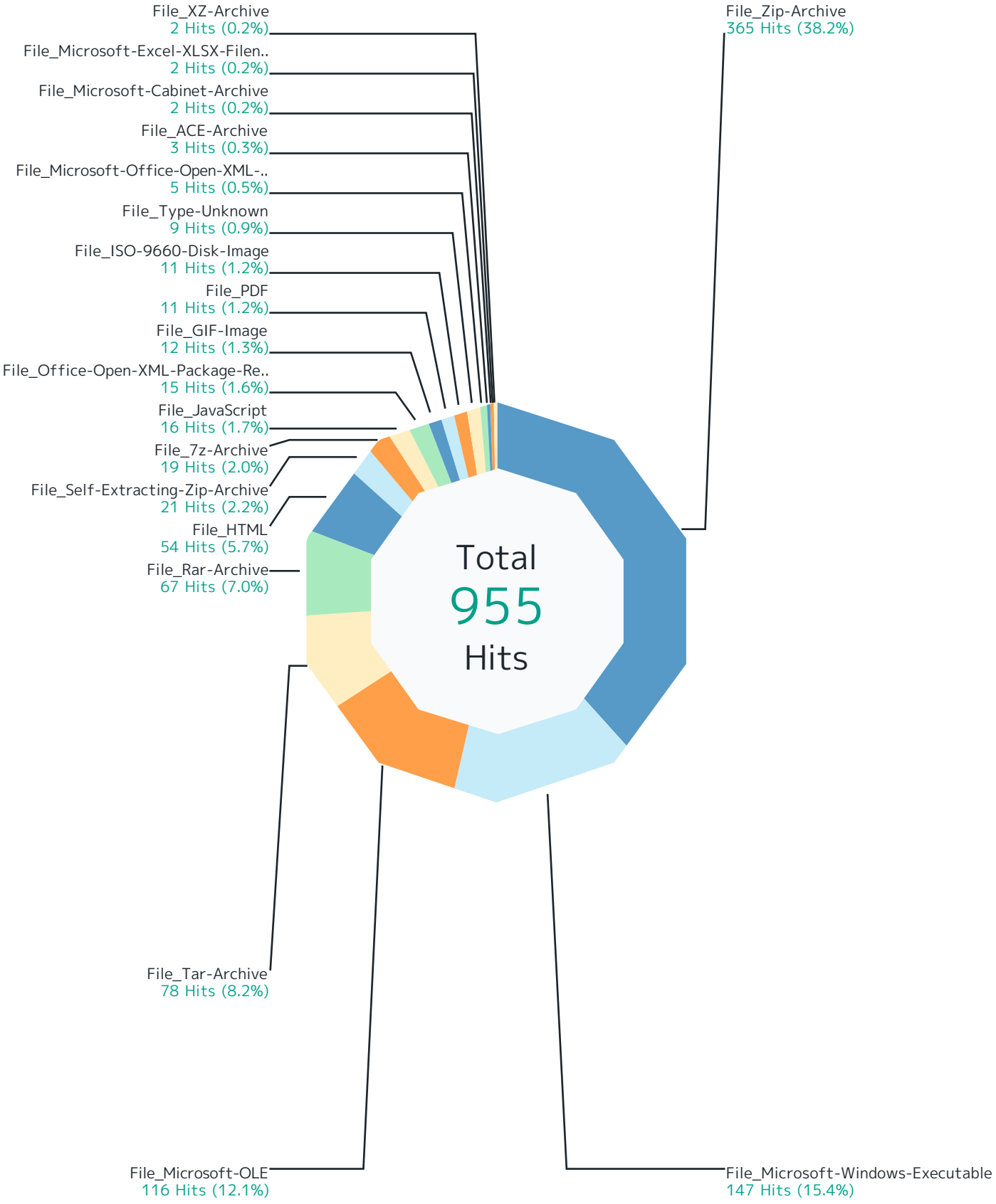
| Scan Result | Hits | % |
|---|---|---|
| File_JavaScript | 1 | 0.1 % |
| File_Microsoft-Office-Open-XML-Document | 1 | 0.1 % |
| **HTML/Phishing.rb** | **24** | **2.5 %** |
| File_HTML | 24 | 2.5 % |
| **Unknown** | **7** | **0.7 %** |
| File_Zip-Archive | 7 | 0.7 % |
| **DistTrack!9113F123C435** | **5** | **0.5 %** |
| File_ISO-9660-Disk-Image | 5 | 0.5 % |
| **Fareit.gen.e** | **2** | **0.2 %** |
| File_ACE-Archive | 2 | 0.2 % |
| **HTML/Phishing.qz** | **2** | **0.2 %** |
| File_HTML | 2 | 0.2 % |
| **PDF/Phishing!C7342523C669** | **2** | **0.2 %** |
| File_PDF | 2 | 0.2 % |
| **Fareit.gen.a** | **1** | **0.1 %** |
| File_ACE-Archive | 1 | 0.1 % |
| **Exploit-GBT!48BE6F1292C7** | **1** | **0.1 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.1 % |
| **Exploit-GBT!7CA49D20B62B** | **1** | **0.1 %** |
| File_Microsoft-Excel-XLSX-Filename-Extension | 1 | 0.1 % |
| **GenericRXVF-WX!C923556C5DD4** | **1** | **0.1 %** |
| File_Rar-Archive | 1 | 0.1 % |
| **Total** | **955** | **100 %** |

# Report

## Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

# Report


File_XZ-Archive
2 Hits (0.2%)
File_Microsoft-Excel-XLSX-Filen..
2 Hits (0.2%)
File_Microsoft-Cabinet-Archive
2 Hits (0.2%)
File_ACE-Archive
3 Hits (0.3%)
File_Microsoft-Office-Open-XML-..
5 Hits (0.5%)
File_Type-Unknown
9 Hits (0.9%)
File_ISO-9660-Disk-Image
11 Hits (1.2%)
File_PDF
11 Hits (1.2%)
File_GIF-Image
12 Hits (1.3%)
File_Office-Open-XML-Package-Re..
15 Hits (1.6%)
File_JavaScript
16 Hits (1.7%)
File_7z-Archive
19 Hits (2.0%)
File_Self-Extracting-Zip-Archive
21 Hits (2.2%)
File_HTML
54 Hits (5.7%)
File_Rar-Archive
67 Hits (7.0%)
File_Zip-Archive
365 Hits (38.2%)
Total
955
Hits
File_Tar-Archive
78 Hits (8.2%)
File_Microsoft-OLE
116 Hits (12.1%)
File_Microsoft-Windows-Executable
147 Hits (15.4%)

# Report

| Responding Scanner | Hits | % |
|---|---|---|
| **File_Zip-Archive** | **365** | **38.2 %** |
| Not Available | 238 | 24.9 % |
| Medium Risk | 74 | 7.7 % |
| Malicious | 31 | 3.2 % |
| High Risk | 15 | 1.6 % |
| Unknown | 7 | 0.7 % |
| **File_Microsoft-Windows-Executable** | **147** | **15.4 %** |
| Malicious | 124 | 13.0 % |
| High Risk | 13 | 1.4 % |
| Medium Risk | 10 | 1.0 % |
| **File_Microsoft-OLE** | **116** | **12.1 %** |
| Medium Risk | 116 | 12.1 % |
| **File_Tar-Archive** | **78** | **8.2 %** |
| Medium Risk | 53 | 5.5 % |
| High Risk | 25 | 2.6 % |
| **File_Rar-Archive** | **67** | **7.0 %** |
| High Risk | 33 | 3.5 % |
| Malicious | 22 | 2.3 % |
| Medium Risk | 11 | 1.2 % |
| GenericRXVF-WX!C923556C5DD4 | 1 | 0.1 % |
| **File_HTML** | **54** | **5.7 %** |
| HTML/Phishing.rb | 24 | 2.5 % |
| Malicious | 21 | 2.2 % |
| Medium Risk | 7 | 0.7 % |
| HTML/Phishing.qz | 2 | 0.2 % |
| **File_Self-Extracting-Zip-Archive** | **21** | **2.2 %** |
| Malicious | 20 | 2.1 % |
| Medium Risk | 1 | 0.1 % |
| **File_7z-Archive** | **19** | **2.0 %** |
| High Risk | 14 | 1.5 % |
| Medium Risk | 5 | 0.5 % |
| **File_JavaScript** | **16** | **1.7 %** |
| Malicious | 14 | 1.5 % |
| Medium Risk | 1 | 0.1 % |
| High Risk | 1 | 0.1 % |
| **File_Office-Open-XML-Package-Relations-Item** | **15** | **1.6 %** |

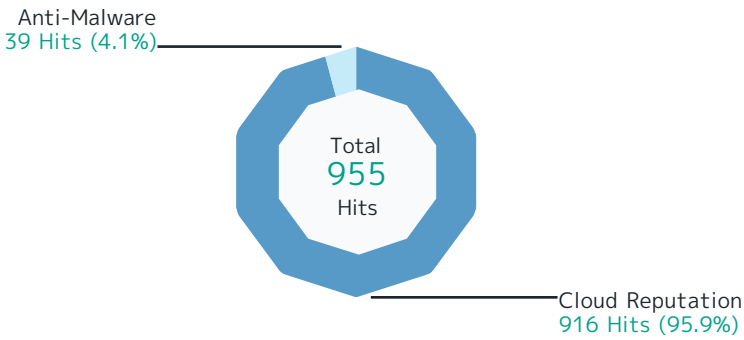
# Report

| Responding Scanner | Hits | % |
|---|---|---|
| Malicious | 15 | 1.6 % |
| **File_GIF-Image** | **12** | **1.3 %** |
| Medium Risk | 12 | 1.3 % |
| **File_PDF** | **11** | **1.2 %** |
| High Risk | 9 | 0.9 % |
| PDF/Phishing!C7342523C669 | 2 | 0.2 % |
| **File_ISO-9660-Disk-Image** | **11** | **1.2 %** |
| DistTrack!9113F123C435 | 5 | 0.5 % |
| Malicious | 3 | 0.3 % |
| High Risk | 3 | 0.3 % |
| **File_Type-Unknown** | **9** | **0.9 %** |
| Malicious | 6 | 0.6 % |
| High Risk | 3 | 0.3 % |
| **File_Microsoft-Office-Open-XML-Document** | **5** | **0.5 %** |
| Malicious | 2 | 0.2 % |
| Not Available | 2 | 0.2 % |
| High Risk | 1 | 0.1 % |
| **File_ACE-Archive** | **3** | **0.3 %** |
| Fareit.gen.e | 2 | 0.2 % |
| Fareit.gen.a | 1 | 0.1 % |
| **File_Microsoft-Cabinet-Archive** | **2** | **0.2 %** |
| Malicious | 2 | 0.2 % |
| **File_Microsoft-Excel-XLSX-Filename-Extension** | **2** | **0.2 %** |
| Exploit-GBT!48BE6F1292C7 | 1 | 0.1 % |
| Exploit-GBT!7CA49D20B62B | 1 | 0.1 % |
| **File_XZ-Archive** | **2** | **0.2 %** |
| Medium Risk | 1 | 0.1 % |
| Malicious | 1 | 0.1 % |
| **Total** | **955** | **100 %** |

# Report

## Top File Types by Responding Scanner

Top 10 file types by responding scanner.




| Responding Scanner | Hits | % |
|---|---|---|
| **Cloud Reputation** | **916** | **95.9 %** |
| File_Zip-Archive | 365 | 38.2 % |
| File_Microsoft-Windows-Executable | 147 | 15.4 % |
| File_Microsoft-OLE | 116 | 12.1 % |
| File_Tar-Archive | 78 | 8.2 % |
| File_Rar-Archive | 66 | 6.9 % |
| File_HTML | 28 | 2.9 % |
| File_Self-Extracting-Zip-Archive | 21 | 2.2 % |
| File_7z-Archive | 19 | 2.0 % |
| File_JavaScript | 16 | 1.7 % |
| File_Office-Open-XML-Package-Relations-Item | 15 | 1.6 % |
| File_GIF-Image | 12 | 1.3 % |
| File_PDF | 9 | 0.9 % |
| File_Type-Unknown | 9 | 0.9 % |
| File_ISO-9660-Disk-Image | 6 | 0.6 % |
| File_Microsoft-Office-Open-XML-Document | 5 | 0.5 % |
| File_Microsoft-Cabinet-Archive | 2 | 0.2 % |
| File_XZ-Archive | 2 | 0.2 % |
| **Anti-Malware** | **39** | **4.1 %** |
| File_HTML | 26 | 2.7 % |
| File_ISO-9660-Disk-Image | 5 | 0.5 % |
| File_ACE-Archive | 3 | 0.3 % |
| File_PDF | 2 | 0.2 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 2 | 0.2 % |
| File_Rar-Archive | 1 | 0.1 % |
| **Total** | **955** | **100 %** |

# Report

## Virenfilterung SRC IPs

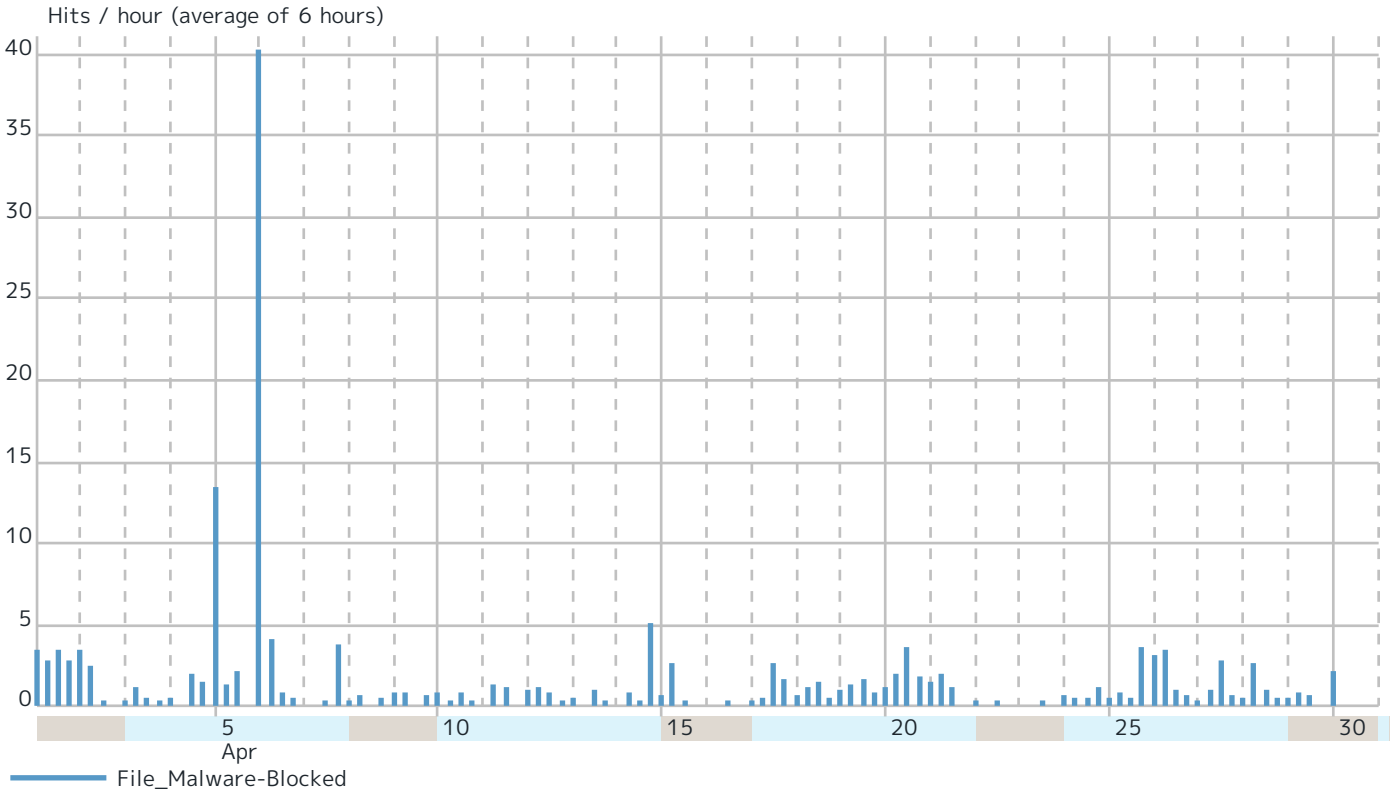
# Report

| Records by src IP | | Hits | % |
|---|---|---|---|
| 133.6.101.35 | Nagoya, Japan | 232 | 24.3 % |
| 47.243.140.251 | Central, Hong Kong | 106 | 11.1 % |
| 85.13.162.183 | Germany | 40 | 4.2 % |
| 192.162.12.29 | Spain | 38 | 4.0 % |
| 83.137.158.140 | Hungary | 30 | 3.1 % |
| 103.252.118.201 | Central, Hong Kong | 26 | 2.7 % |
| 104.128.66.223 | Santa Clara, California 95054, United States | 26 | 2.7 % |
| 185.166.163.158 | Los Angeles, California 90017, United States | 26 | 2.7 % |
| 117.53.155.52 | Malaysia | 26 | 2.7 % |
| 43.231.232.190 | Santa Clara, California 95054, United States | 25 | 2.6 % |
| 64.79.106.84 | United States | 22 | 2.3 % |
| 51.81.161.159 | Hillsboro, Oregon 97129, United States | 19 | 2.0 % |
| 201.131.96.184 | Mexico | 18 | 1.9 % |
| 213.142.130.54 | Turkey | 16 | 1.7 % |
| 168.119.152.251 | Germany | 13 | 1.4 % |
| 94.73.160.69 | Turkey | 10 | 1.0 % |
| 42.121.15.38 | China | 10 | 1.0 % |
| 121.199.7.209 | Hangzhou, China | 9 | 0.9 % |
| 209.160.40.54 | Seattle, Washington 98160, United States | 8 | 0.8 % |
| 104.223.76.195 | Los Angeles, California 90014, United States | 8 | 0.8 % |
| 85.13.134.172 | Germany | 8 | 0.8 % |
| 142.4.9.200 | United States | 7 | 0.7 % |
| 193.33.111.56 | Poland | 6 | 0.6 % |
| 155.94.136.27 | Los Angeles, California 90014, United States | 6 | 0.6 % |
| 185.222.57.140 | Amsterdam, Netherlands | 6 | 0.6 % |
| 103.14.224.79 | Vietnam | 5 | 0.5 % |
| 45.133.174.74 | Amsterdam, Netherlands | 5 | 0.5 % |
| 78.157.63.252 | Iran | 5 | 0.5 % |
| 136.0.111.34 | United States | 4 | 0.4 % |
| 116.212.184.163 | Bangladesh | 4 | 0.4 % |
| Others | | 191 | 20.0 % |
| **Total** | | **955** | **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.