# The Real Time Threat List

*Thomas Wegele, Avira GmbH*
*Righard Zwienenberg, ESET*
*Richard Ford, Florida Institute of Technology*

amtso

Anti-Malware Testing Standards Organization

# Thank You

AVIRA

eset®

Florida Institute of Technology

Harris Institute for Assured Information

amtso

Anti-Malware Testing Standards Organization

# Agenda

- Introduction
- A Quick Update
- Real Time Threat List
- Demo

amtso

Anti-Malware Testing Standards Organization

# AMTSO, a Quick Update

amtso

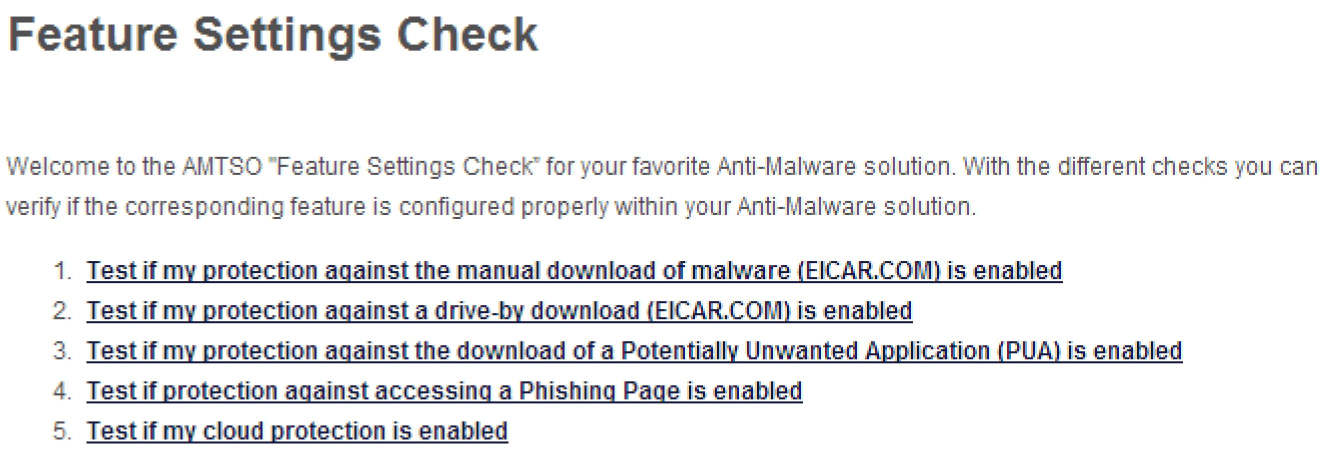
Anti-Malware Testing Standards Organization

# AMTSO, a Quick Update

- New structure

# AMTSO, a Quick Update

- New structure
- Security Features Check



## Feature Settings Check

Welcome to the AMTSO "Feature Settings Check" for your favorite Anti-Malware solution. With the different checks you can verify if the corresponding feature is configured properly within your Anti-Malware solution.

1. Test if my protection against the manual download of malware (EICAR.COM) is enabled
2. Test if my protection against a drive-by download (EICAR.COM) is enabled
3. Test if my protection against the download of a Potentially Unwanted Application (PUA) is enabled
4. Test if protection against accessing a Phishing Page is enabled
5. Test if my cloud protection is enabled

amtso

Anti-Malware Testing Standards Organization

# AMTSO, a Quick Update

- New structure
- Security Features Check
- Compendium

amtso

Anti-Malware Testing Standards Organization

# AMTSO, a Quick Update

- New structure
- Security Features Check
- Compendium
- Ecosystem Cleanup (IEEE)

amtso

Anti-Malware Testing Standards Organization

# AMTSO, a Quick Update

- New structure
- Security Features Check
- Compendium
- Ecosystem Cleanup (IEEE)
- Real Time Threat List

amtso

Anti-Malware Testing Standards Organization

# The WildList

# The WildList

- The WildList was created in 1993 by Joe Wells for a simple purpose: to see which viruses were really “In the Wild” (ItW), as reported by CARO members. If two or more CARO members reported the virus as seen at more than one site, the virus would make the WildList.

# The Problem

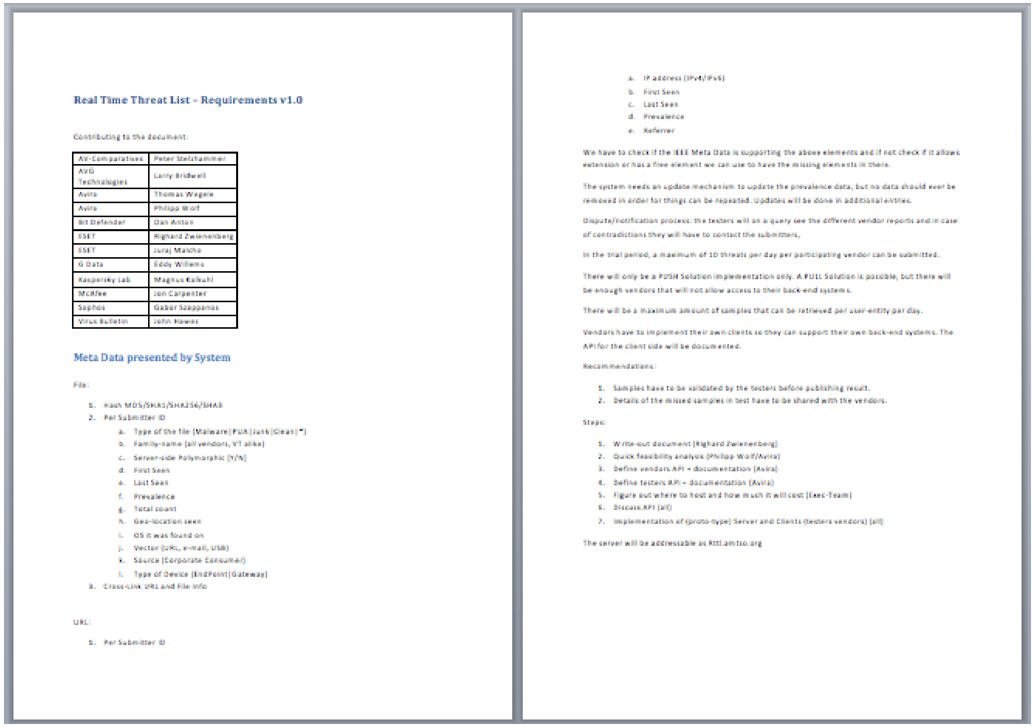
# The WildList

- Something new, fast and “accurate” had to be created, which eventually resulted in the conception of the Real Time Threat List.

# The Real Time Threat List (RTTL)

# RTTL: The Basics

- The idea of the Real Time Threat List is to share new threats with additional meta-data incorporated into the system.



## Real Time Threat List – Requirements v1.0

Contributing to the document:

| | |
|---|---|
| AV-Comparatives | Peter Stelzhammer |
| AVG Technologies | Larry Bridwell |
| Avira | Thomas Wegele |
| Avira | Philipp Wolf |
| Bit Defender | Dan Anton |
| ESET | Righard Zwienenberg |
| ESET | Juraj Malcho |
| G Data | Eddy Willems |
| Kaspersky Lab | Magnus Kalkuhl |
| McAfee | Jon Carpenter |
| Sophos | Gabor Szappanos |
| Virus Bulletin | John Hawes |

## Meta Data presented by System

File:

1. Hash MD5/SHA1/SHA256/SHA8
2. Per Submitter ID
   a. Type of the file [Malware|PUA|Junk|Clean|*]
   b. Family-name (all vendors, VT alike)
   c. Server-side Polymorphic (Y/N)
   d. First Seen
   e. Last Seen
   f. Prevalence
   g. Total count
   h. Geo-location seen
   i. OS it was found on
   j. Vector (URL, e-mail, USB)
   k. Source (Corporate Consumer)
   l. Type of Device [EndPoint|Gateway]
3. Cross-Link URL and File info

URL:

1. Per Submitter ID
   a. IP address (IPv4/IPv6)
   b. First Seen
   c. Last Seen
   d. Prevalence
   e. Referrer

We have to check if the IEEE Meta Data is supporting the above elements and if not check if it allows extension or has a free element we can use to have the missing elements in there.

The system needs an update mechanism to update the prevalence data, but no data should ever be removed in order for things can be repeated. Updates will be done in additional entries.

Dispute/notification process: the testers will on a query see the different vendor reports and in case of contradictions they will have to contact the submitters,

In the trial period, a maximum of 10 threats per day per participating vendor can be submitted.

There will only be a PUSH Solution implementation only. A PULL Solution is possible, but there will be enough vendors that will not allow access to their back-end systems.

There will be a maximum amount of samples that can be retrieved per user-entity per day.

Vendors have to implement their own clients so they can support their own back-end systems. The API for the client side will be documented.

Recommendations:

1. Samples have to be validated by the testers before publishing result.
2. Details of the missed samples in test have to be shared with the vendors.

Steps:

1. Write-out document (Righard Zwienenberg)
2. Quick feasibility analysis (Philipp Wolf/Avira)
3. Define vendors API + documentation (Avira)
4. Define testers API + documentation (Avira)
5. Figure out where to host and how much it will cost (Exec-Team)
6. Discuss API (all)
7. Implementation of (proto-type) Server and Clients (testers vendors) (all)

The server will be addressable as Rttl.amtso.org

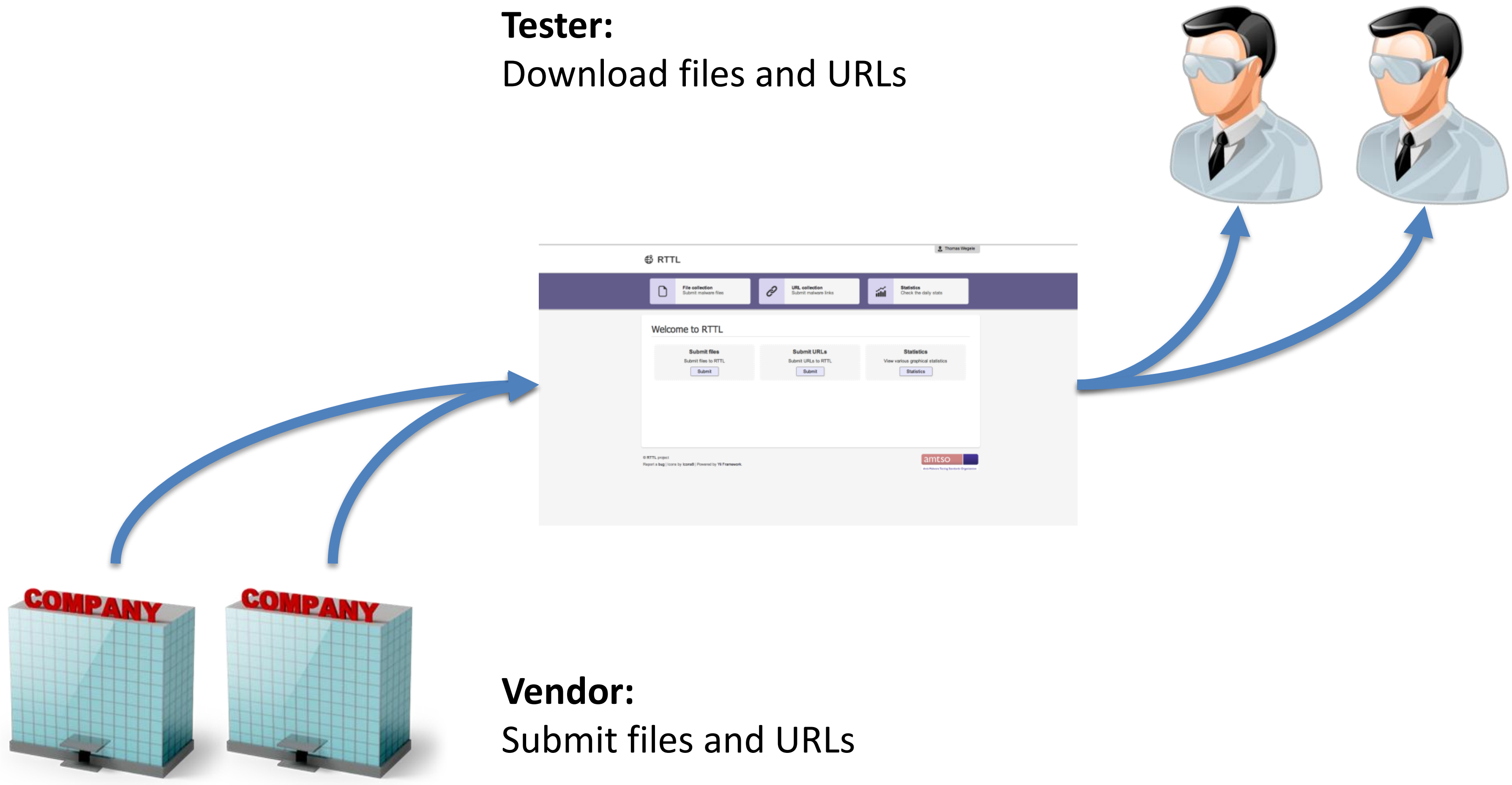
amtso

Anti-Malware Testing Standards Organization

# The Background of RTTL

# RTTL: System Overview

**Tester:**
Download files and URLs



Welcome to RTTL

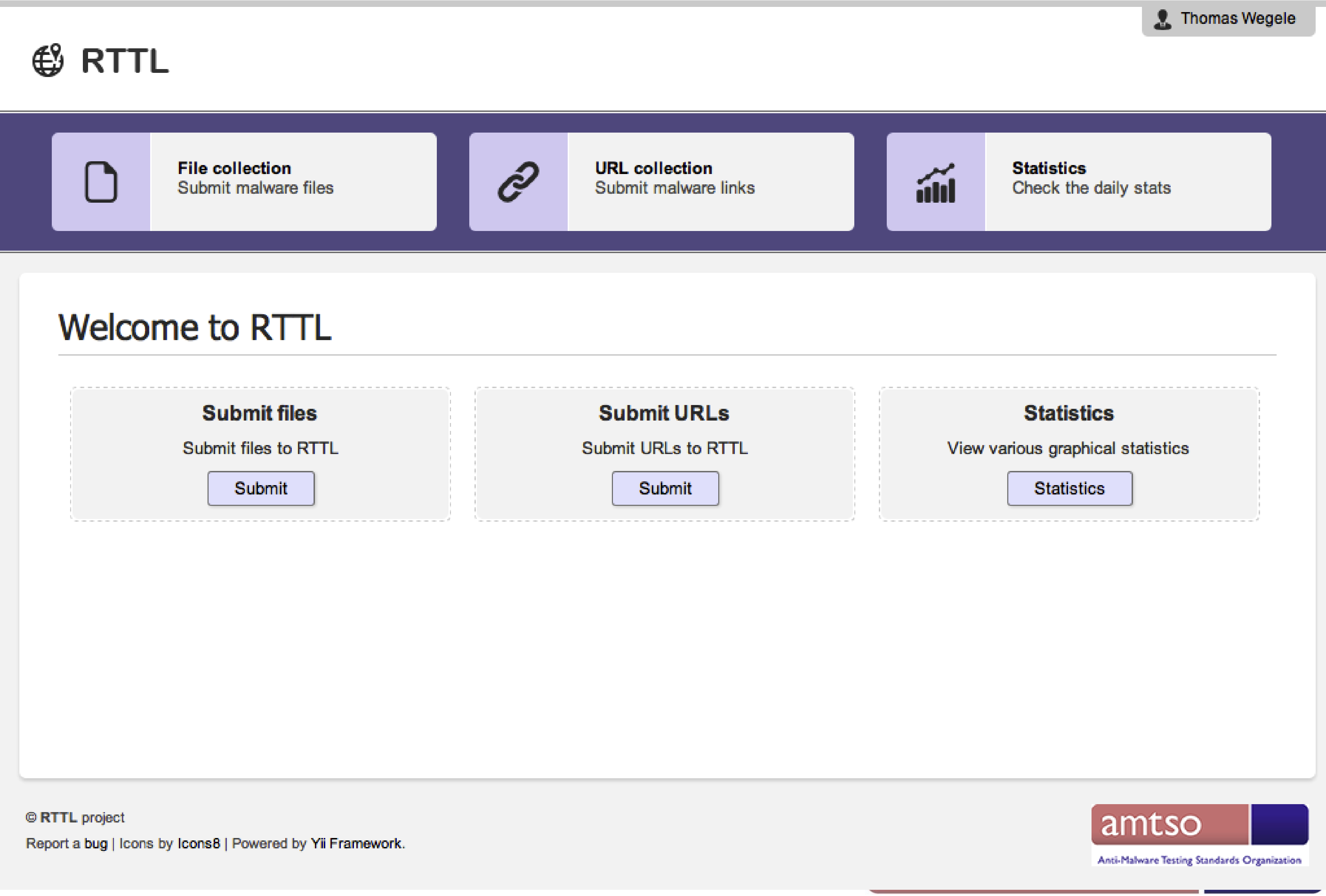
**Submit files**
Submit files to RTTL

**Submit URLs**
Submit URLs to RTTL

**Statistics**
View various graphical statistics

© RTTL project
Report a bug | Icons by Icons8 | Powered by Yii Framework.

**Vendor:**
Submit files and URLs



## Welcome to RTTL

**Submit files**

Submit files to RTTL

**Submit URLs**

Submit URLs to RTTL

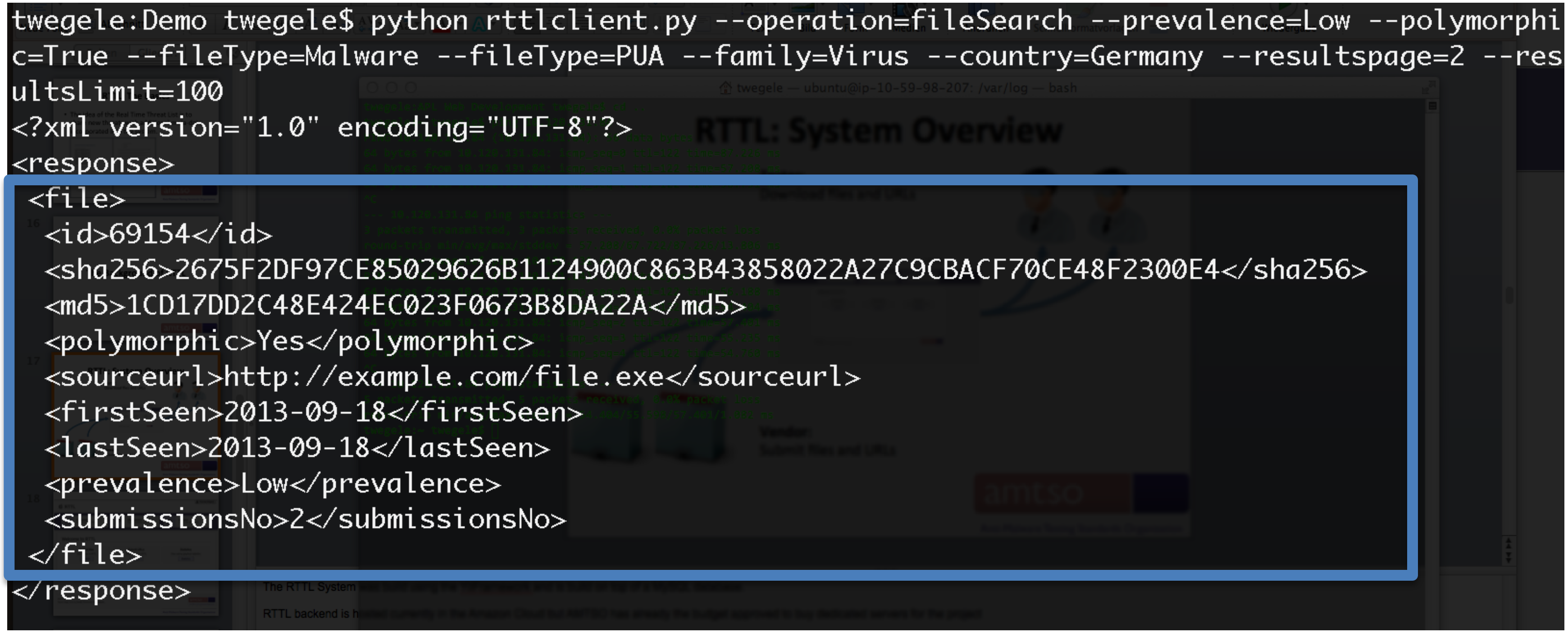
**Statistics**

View various graphical statistics

© **RTTL** project

Report a **bug** | Icons by **Icons8** | Powered by **Yii Framework**.

# RTTL: Client example



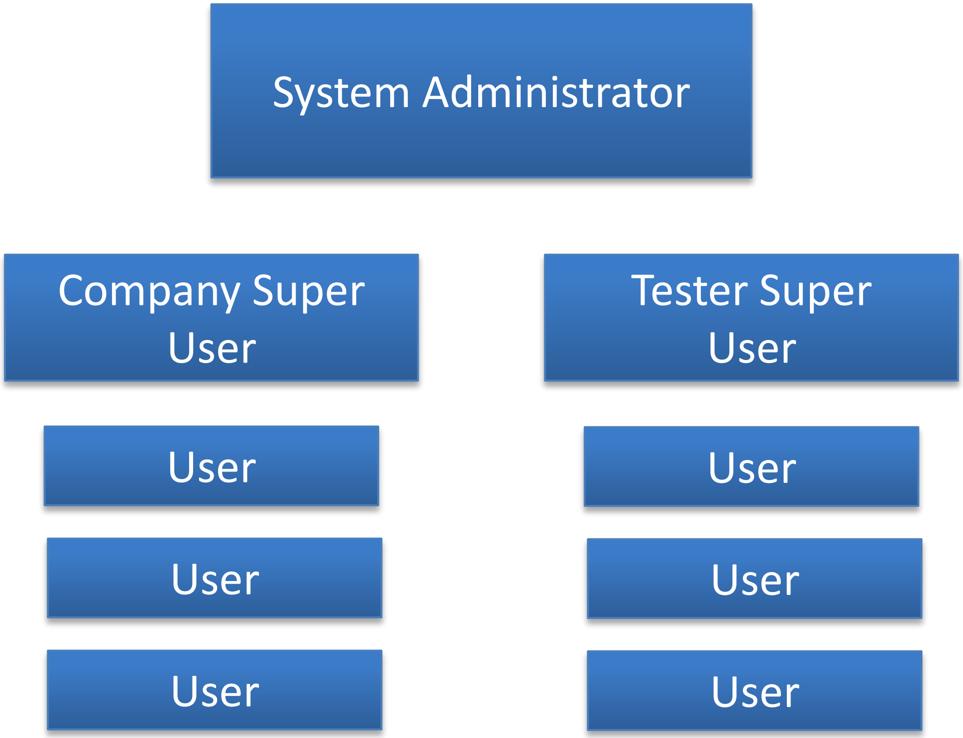
```
twegele:Demo twegele$ python rttlclient.py --operation=fileSearch --prevalence=Low --polymorphi
c=True --fileType=Malware --fileType=PUA --family=Virus --country=Germany --resultspage=2 --res
ultsLimit=100
<?xml version="1.0" encoding="UTF-8"?>
<response>
 <file>
  <id>69154</id>
  <sha256>2675F2DF97CE85029626B1124900C863B43858022A27C9CBACF70CE48F2300E4</sha256>
  <md5>1CD17DD2C48E424EC023F0673B8DA22A</md5>
  <polymorphic>Yes</polymorphic>
  <sourceurl>http://example.com/file.exe</sourceurl>
  <firstSeen>2013-09-18</firstSeen>
  <lastSeen>2013-09-18</lastSeen>
  <prevalence>Low</prevalence>
  <submissionsNo>2</submissionsNo>
 </file>
</response>
```

# RTTL: User Management

- Different user groups
  - Vendor
  - Tester

- Each company can administrate their own users for the system

# RTTL: User Management



System Administrator

Company Super User

Tester Super User

User

User

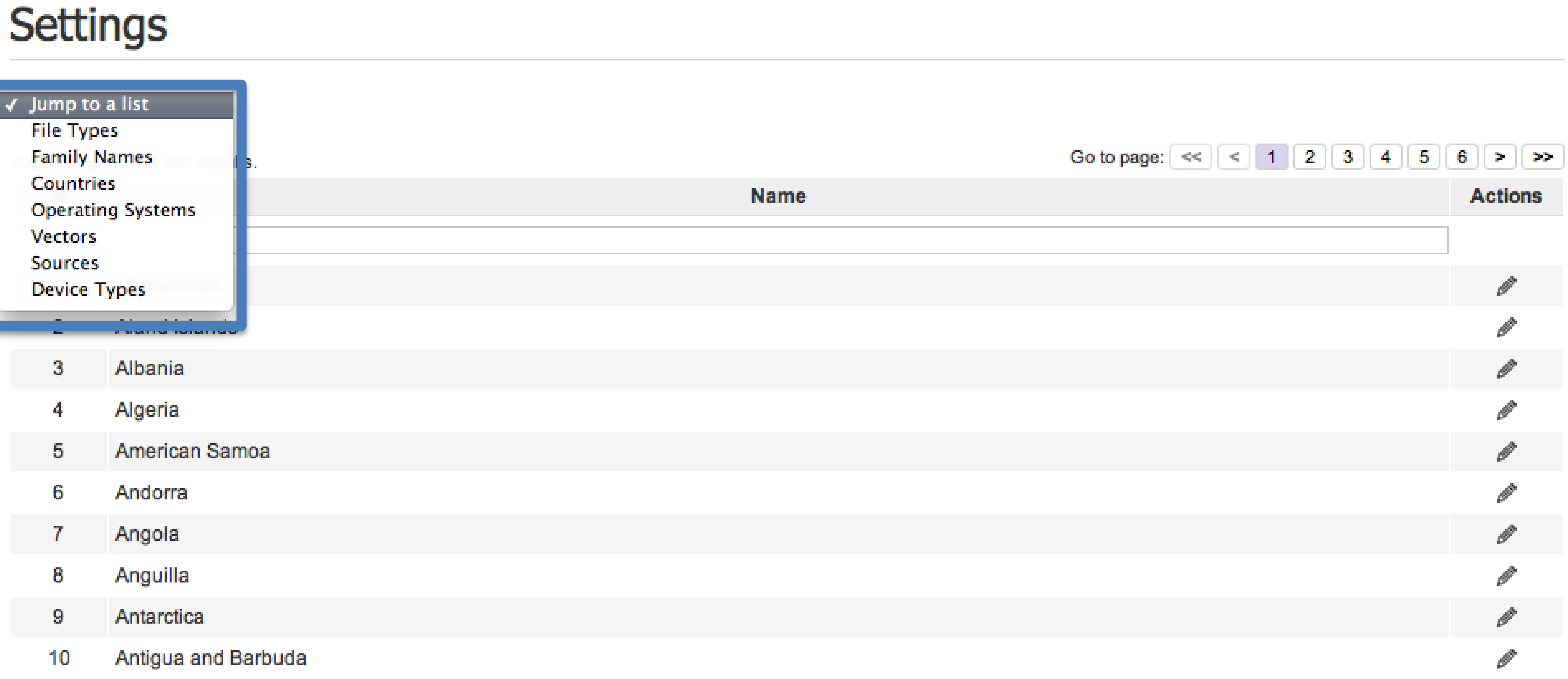
User

User

User

User

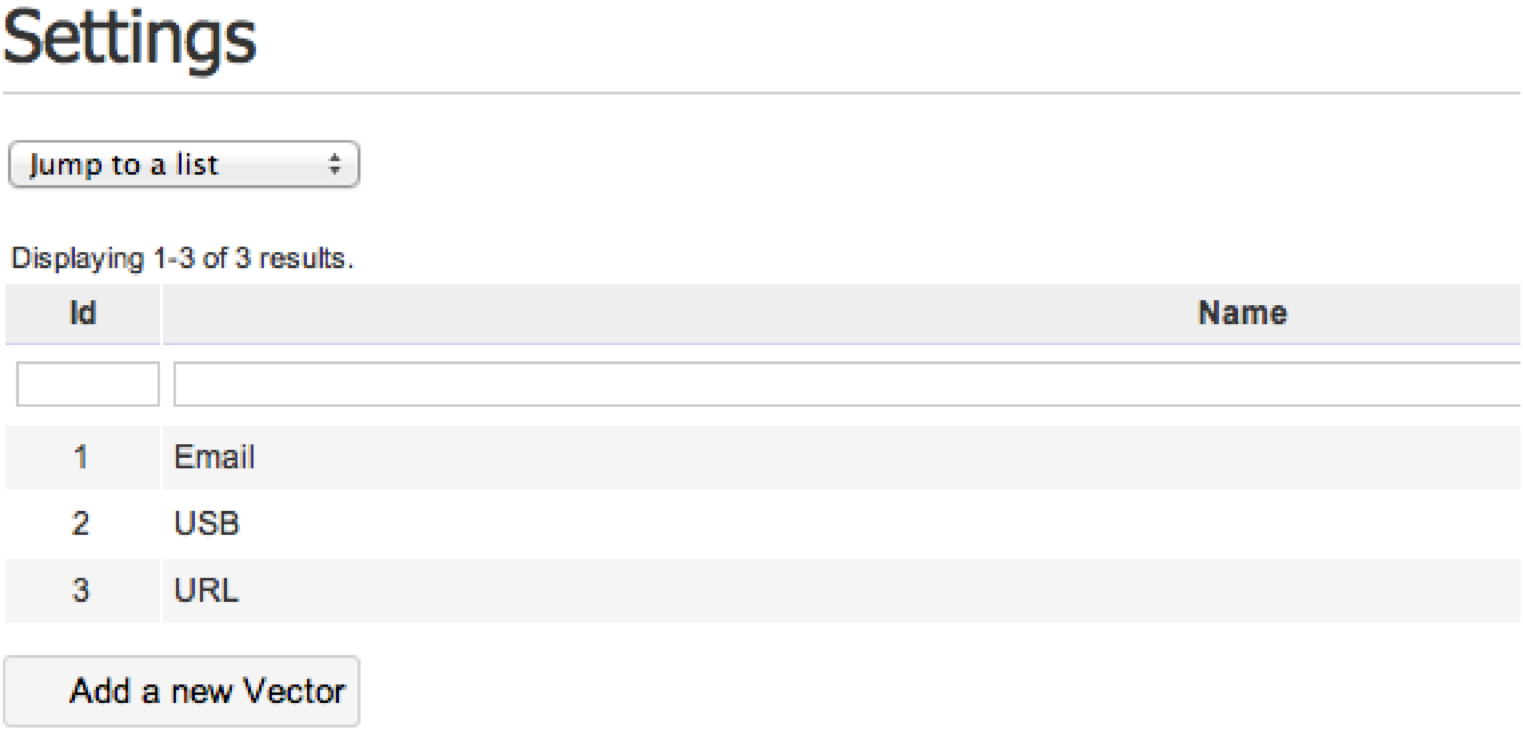
# RTTL: System Configuration



|  | Name | Actions |
|---|---|---|
| 2 | Aland Islands | ✎ |
| 3 | Albania | ✎ |
| 4 | Algeria | ✎ |
| 5 | American Samoa | ✎ |
| 6 | Andorra | ✎ |
| 7 | Angola | ✎ |
| 8 | Anguilla | ✎ |
| 9 | Antarctica | ✎ |
| 10 | Antigua and Barbuda | ✎ |

The pre-configured elements e.g. source of the sample or the country can be added by each company in order to build a flexible system

Anti-Malware Testing Standards Organization



# Settings

Displaying 1-3 of 3 results.

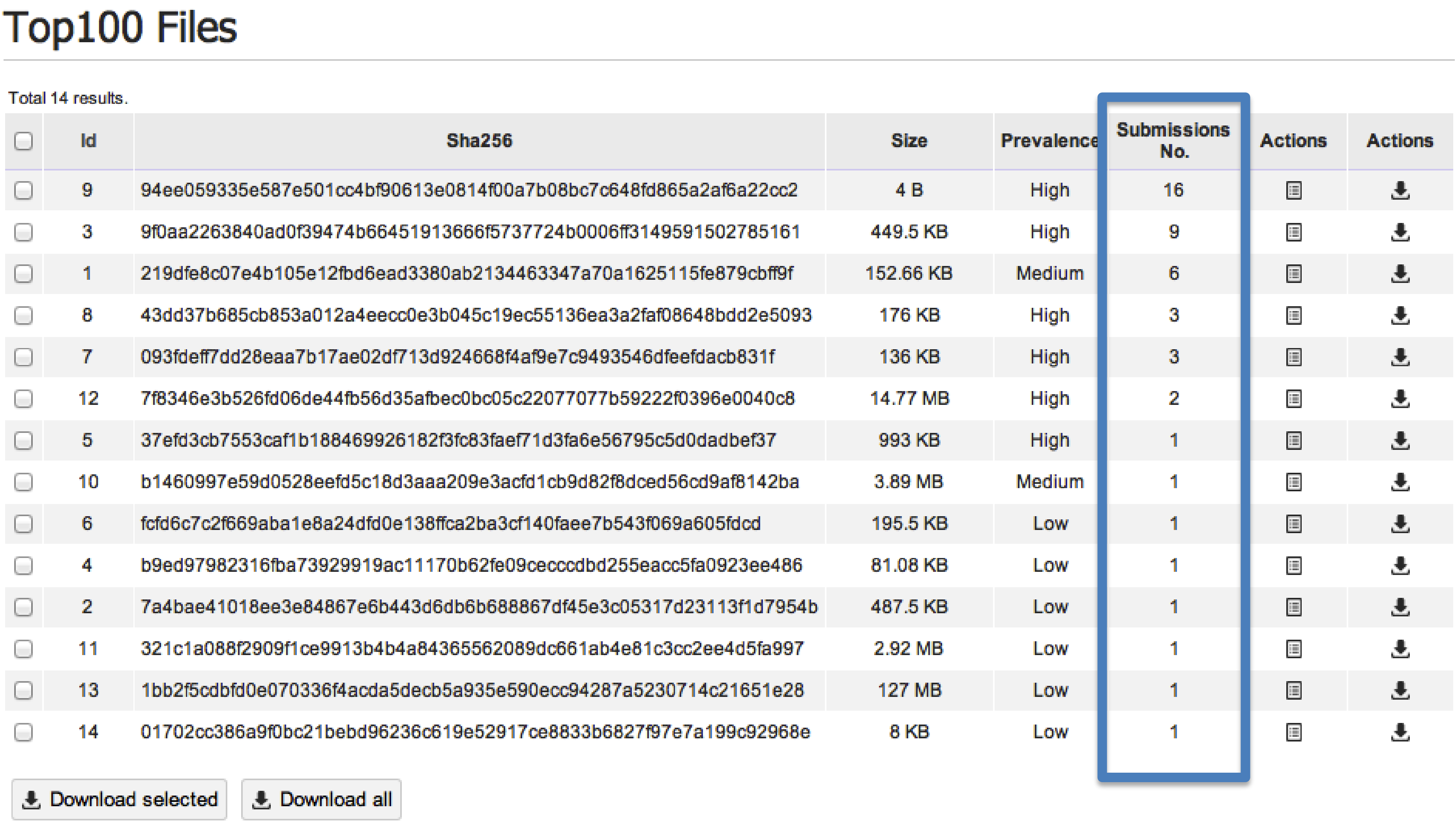
| Id | Name |
|---|---|
| | |
| 1 | Email |
| 2 | USB |
| 3 | URL |

# RTTL: Features

- Real time list of the Top100 samples based on the amount of submissions
- Submissions are possible via the web interface and the API
- Searches are possible via the web interface and the API
- All information is updated in real time, there is no delay between submitting a sample and being available for testers

amtso

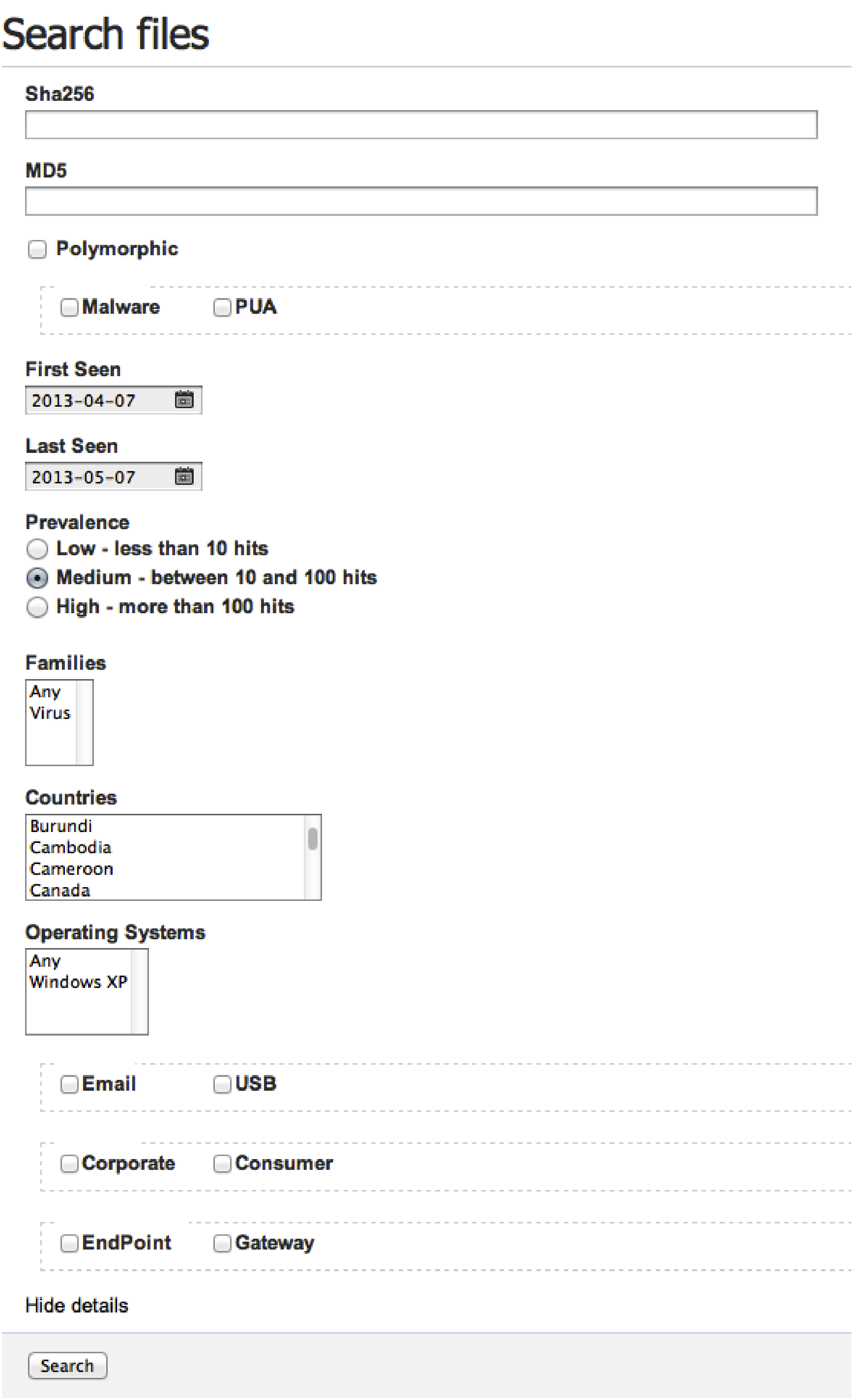
Anti-Malware Testing Standards Organization



# Top100 Files

Total 14 results.

| □ | Id | Sha256 | Size | Prevalence | Submissions No. | Actions | Actions |
|---|---|---|---|---|---|---|---|
| □ | 9 | 94ee059335e587e501cc4bf90613e0814f00a7b08bc7c648fd865a2af6a22cc2 | 4 B | High | 16 | ≣ | ⬇ |
| □ | 3 | 9f0aa2263840ad0f39474b66451913666f5737724b0006ff3149591502785161 | 449.5 KB | High | 9 | ≣ | ⬇ |
| □ | 1 | 219dfe8c07e4b105e12fbd6ead3380ab2134463347a70a1625115fe879cbff9f | 152.66 KB | Medium | 6 | ≣ | ⬇ |
| □ | 8 | 43dd37b685cb853a012a4eecc0e3b045c19ec55136ea3a2faf08648bdd2e5093 | 176 KB | High | 3 | ≣ | ⬇ |
| □ | 7 | 093fdeff7dd28eaa7b17ae02df713d924668f4af9e7c9493546dfeefdacb831f | 136 KB | High | 3 | ≣ | ⬇ |
| □ | 12 | 7f8346e3b526fd06de44fb56d35afbec0bc05c22077077b59222f0396e0040c8 | 14.77 MB | High | 2 | ≣ | ⬇ |
| □ | 5 | 37efd3cb7553caf1b188469926182f3fc83faef71d3fa6e56795c5d0dadbef37 | 993 KB | High | 1 | ≣ | ⬇ |
| □ | 10 | b1460997e59d0528eefd5c18d3aaa209e3acfd1cb9d82f8dced56cd9af8142ba | 3.89 MB | Medium | 1 | ≣ | ⬇ |
| □ | 6 | fcfd6c7c2f669aba1e8a24dfd0e138ffca2ba3cf140faee7b543f069a605fdcd | 195.5 KB | Low | 1 | ≣ | ⬇ |
| □ | 4 | b9ed97982316fba73929919ac11170b62fe09cecccdbd255eacc5fa0923ee486 | 81.08 KB | Low | 1 | ≣ | ⬇ |
| □ | 2 | 7a4bae41018ee3e84867e6b443d6db6b688867df45e3c05317d23113f1d7954b | 487.5 KB | Low | 1 | ≣ | ⬇ |
| □ | 11 | 321c1a088f2909f1ce9913b4b4a84365562089dc661ab4e81c3cc2ee4d5fa997 | 2.92 MB | Low | 1 | ≣ | ⬇ |
| □ | 13 | 1bb2f5cdbfd0e070336f4acda5decb5a935e590ecc94287a5230714c21651e28 | 127 MB | Low | 1 | ≣ | ⬇ |
| □ | 14 | 01702cc386a9f0bc21bebd96236c619e52917ce8833b6827f97e7a199c92968e | 8 KB | Low | 1 | ≣ | ⬇ |



# Search files

Sha256

MD5

□ Polymorphic

□ Malware □ PUA

First Seen
2013-04-07

Last Seen
2013-05-07

Prevalence
○ Low - less than 10 hits
● Medium - between 10 and 100 hits
○ High - more than 100 hits

Families
Any
Virus

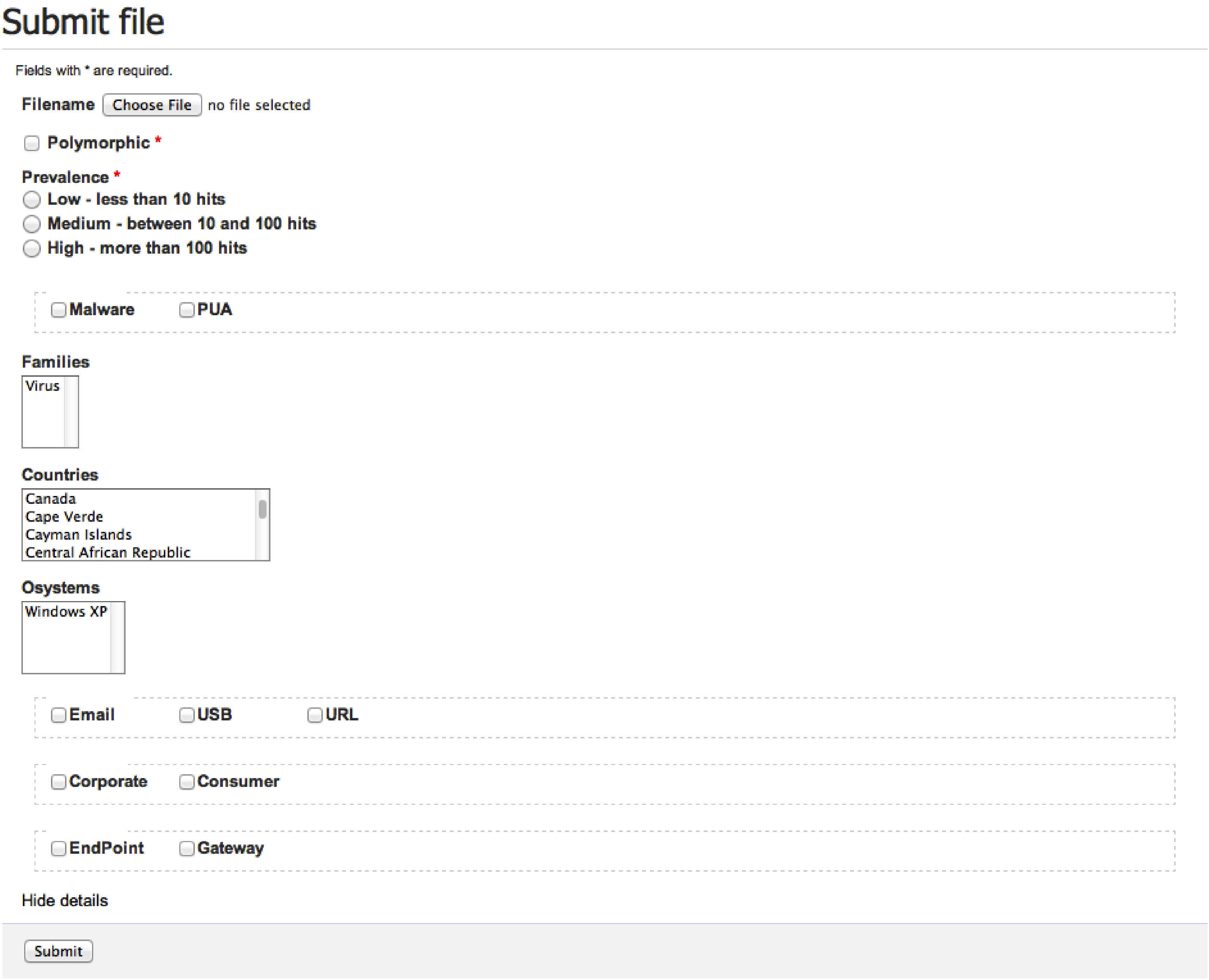
Countries
Burundi
Cambodia
Cameroon
Canada

Operating Systems
Any
Windows XP

□ Email □ USB

□ Corporate □ Consumer

□ EndPoint □ Gateway



# Submit file

Fields with * are required.

**Filename** Choose File no file selected

□ **Polymorphic** *

**Prevalence** *

○ **Low - less than 10 hits**

○ **Medium - between 10 and 100 hits**

○ **High - more than 100 hits**

□ **Malware** □ **PUA**

**Families**

Virus

**Countries**

Canada
Cape Verde
Cayman Islands
Central African Republic

**Osystems**

Windows XP

□ **Email** □ **USB** □ **URL**

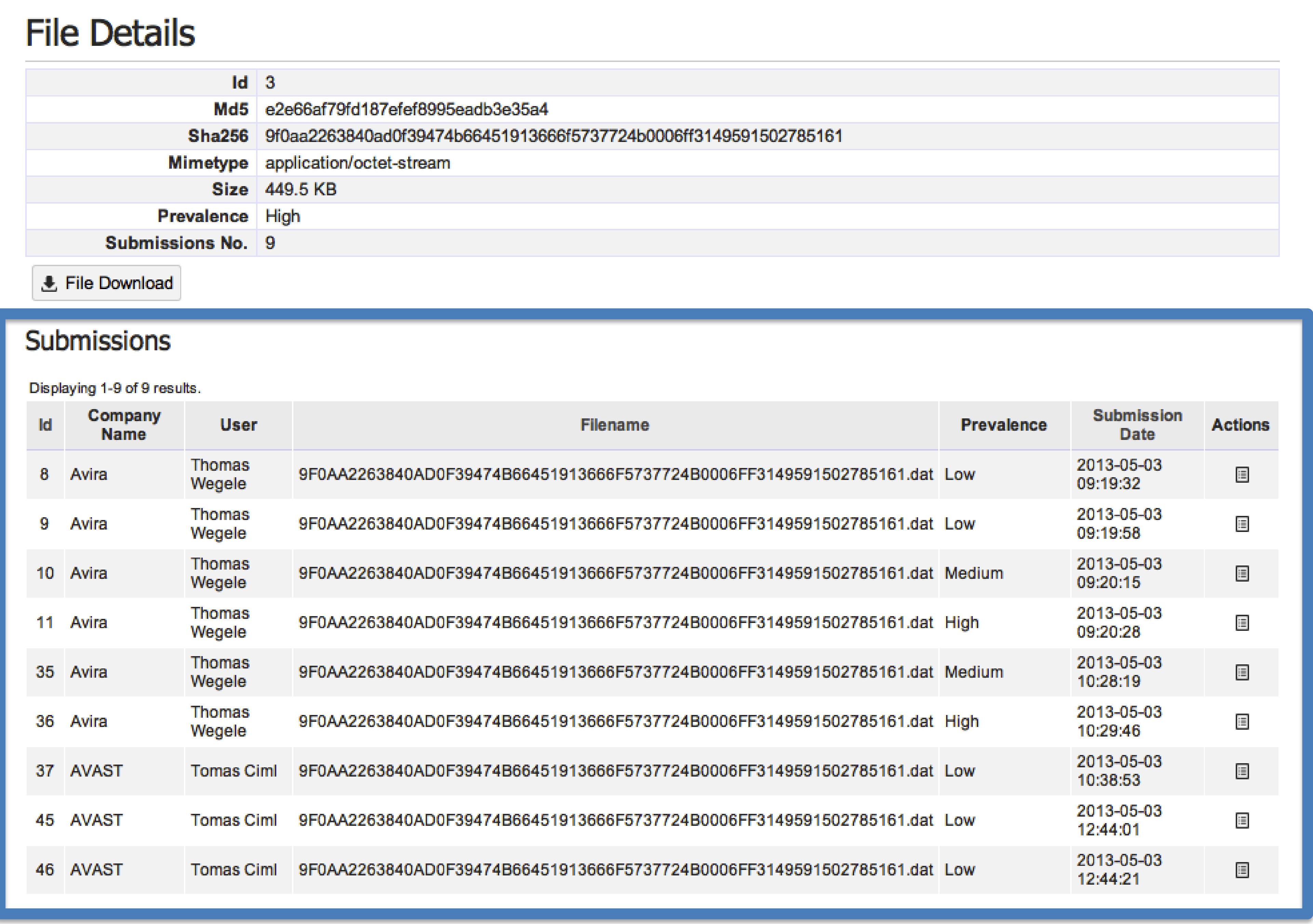
□ **Corporate** □ **Consumer**

□ **EndPoint** □ **Gateway**

Hide details

Submit

tion



## File Details

| | |
|---|---|
| **Id** | 3 |
| **Md5** | e2e66af79fd187efef8995eadb3e35a4 |
| **Sha256** | 9f0aa2263840ad0f39474b66451913666f5737724b0006ff3149591502785161 |
| **Mimetype** | application/octet-stream |
| **Size** | 449.5 KB |
| **Prevalence** | High |
| **Submissions No.** | 9 |

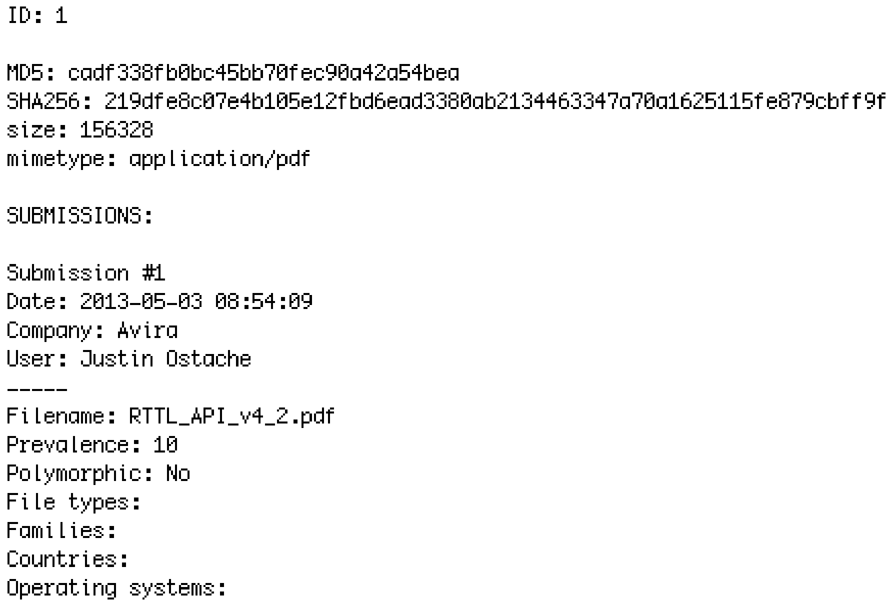
## Submissions

Displaying 1-9 of 9 results.

| Id | Company Name | User | Filename | Prevalence | Submission Date | Actions |
|---|---|---|---|---|---|---|
| 8 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Low | 2013-05-03 09:19:32 | ▤ |
| 9 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Low | 2013-05-03 09:19:58 | ▤ |
| 10 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Medium | 2013-05-03 09:20:15 | ▤ |
| 11 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | High | 2013-05-03 09:20:28 | ▤ |
| 35 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Medium | 2013-05-03 10:28:19 | ▤ |
| 36 | Avira | Thomas Wegele | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | High | 2013-05-03 10:29:46 | ▤ |
| 37 | AVAST | Tomas Ciml | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Low | 2013-05-03 10:38:53 | ▤ |
| 45 | AVAST | Tomas Ciml | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Low | 2013-05-03 12:44:01 | ▤ |
| 46 | AVAST | Tomas Ciml | 9F0AA2263840AD0F39474B66451913666F5737724B0006FF3149591502785161.dat | Low | 2013-05-03 12:44:21 | ▤ |

# RTTL: Download Sample

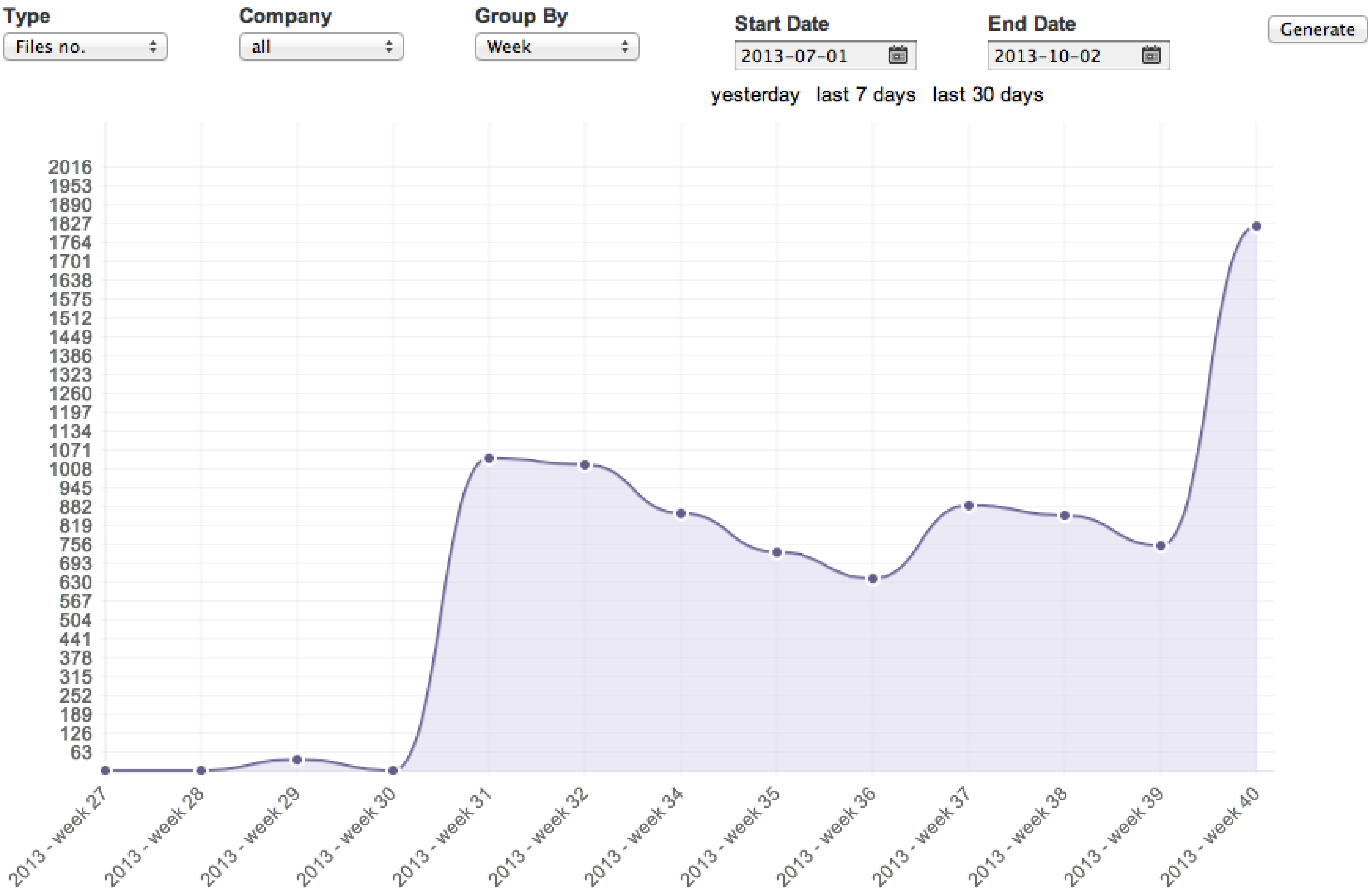
- For each download a ZIP archive is generated which contains the selected amount of samples and for each sample a SHA256_info.txt file with the submission information is generated
- Example:



```
ID: 1

MD5: cadf338fb0bc45bb70fec90a42a54bea
SHA256: 219dfe8c07e4b105e12fbd6ead3380ab2134463347a70a1625115fe879cbff9f
size: 156328
mimetype: application/pdf

SUBMISSIONS:

Submission #1
Date: 2013-05-03 08:54:09
Company: Avira
User: Justin Ostache
------
Filename: RTTL_API_v4_2.pdf
Prevalence: 10
Polymorphic: No
File types:
Families:
Countries:
Operating systems:
```

amtso

Anti-Malware Testing Standards Organization



Type: Files no.

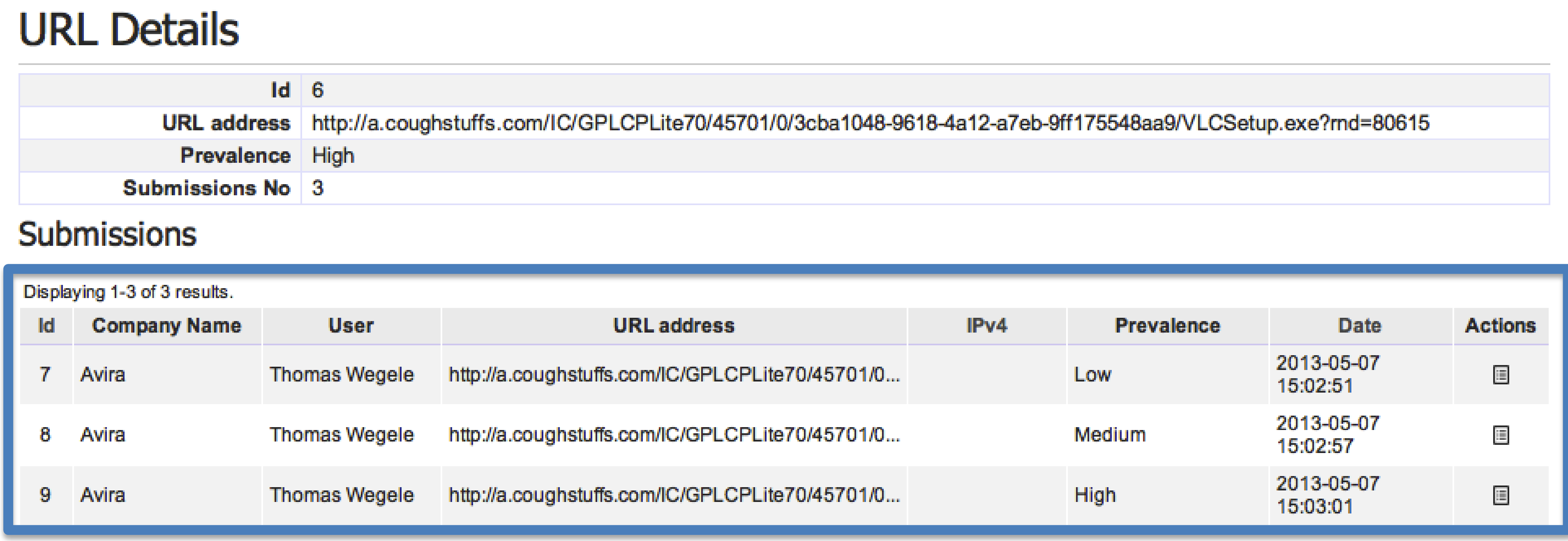
Company: all

Group By: Week

Start Date: 2013-07-01

End Date: 2013-10-02

# RTTL: URL Details



## URL Details

| | |
|---|---|
| **Id** | 6 |
| **URL address** | http://a.coughstuffs.com/IC/GPLCPLite70/45701/0/3cba1048-9618-4a12-a7eb-9ff175548aa9/VLCSetup.exe?rnd=80615 |
| **Prevalence** | High |
| **Submissions No** | 3 |

## Submissions

Displaying 1-3 of 3 results.

| Id | Company Name | User | URL address | IPv4 | Prevalence | Date | Actions |
|---|---|---|---|---|---|---|---|
| 7 | Avira | Thomas Wegele | http://a.coughstuffs.com/IC/GPLCPLite70/45701/0... | | Low | 2013-05-07 15:02:51 | ▤ |
| 8 | Avira | Thomas Wegele | http://a.coughstuffs.com/IC/GPLCPLite70/45701/0... | | Medium | 2013-05-07 15:02:57 | ▤ |
| 9 | Avira | Thomas Wegele | http://a.coughstuffs.com/IC/GPLCPLite70/45701/0... | | High | 2013-05-07 15:03:01 | ▤ |

amtso

Anti-Malware Testing Standards Organization

# RTTL: Download URLs

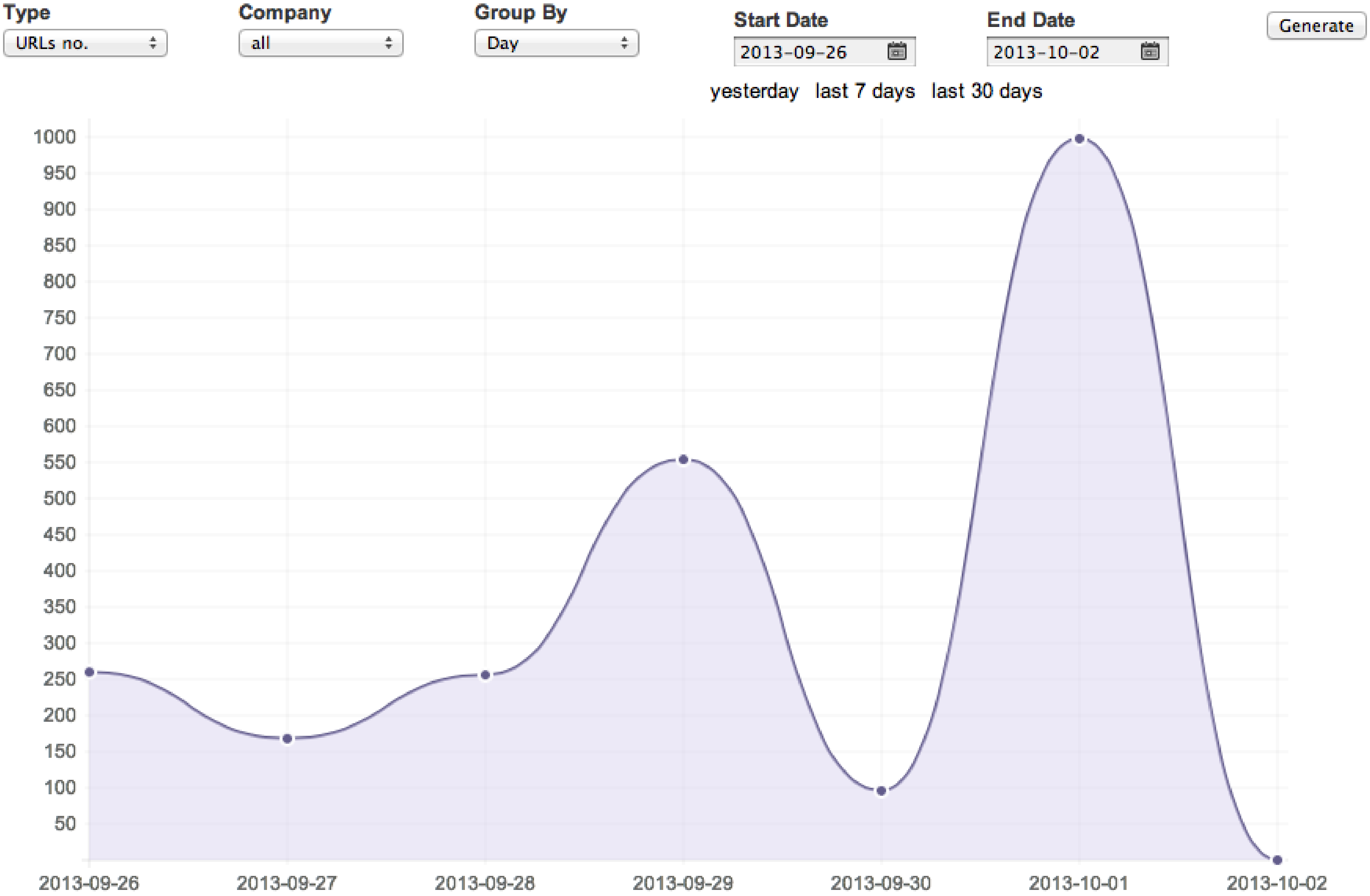
- via the Web Interface selected / all URLs can be downloaded by the testers

- Example:
  - http://www.wyztb.cn/xyxp/taihexinyuan.htm
  - http://www.apitsd.org/_mysql/dump/news-35.html
  - http://apdinfomedia.com/js/script.js
  - http://down.vaccinesecure.co.kr/app/partner/vaccinesecure_utiltop.exe
  - http://a.coughstuffs.com/IC/GPLCPLite70/45701/0/3cba1048-9618-4a12-a7eb-9ff175548aa9/VLCSetup.exe?rnd=80615
  - http://vskvai.best.lt.ua/dlimage4.php
  - http://a.coughstuffs.com/IC/GPLCPLite70/45701/0/121af350-2810-4183-9031-cf948157d987/XvidSetup.exe?rnd=83740
  - http://img.70e.com/code/img/gggg/s/83.gif
  - http://www.allinonespy.com/all-in-one-spy.exe

# RTTL: Download URLs

.. via the API you have a XML with all URLs you want use for testing:

```
<url>
 <id>40</id>
 <url>http://pds21.egloos.com/pds/201305/03/60/wel.exe</url>
 <IPv4Address/>
 <IPv6Address/>
 <firstSeen>2013-09-20</firstSeen>
 <lastSeen>2013-09-20</lastSeen>
 <prevalence>Medium</prevalence>
 <referrer/>
 <submissionsNo>2</submissionsNo>
</url>
<url>
```



Type: URLs no.

Company: all

Group By: Day

Start Date: 2013-09-26

End Date: 2013-10-02

# Demo

# Implementations & Future

# Questions?

AVIRA

eset

Florida Institute of Technology
Harris Institute for Assured Information

*Thomas Wegele, Avira GmbH*
*Righard Zwienenberg, ESET*
*Richard Ford, Florida Institute of Technology*

Contact us: info@amtso.org
Website: www.amtso.org

amtso
Anti-Malware Testing Standards Organization