Virex sharing application

Author: Philipp Wolf

Function: Director Protection Labs

Date: 2012-05-14

Agenda

- Norman sharing standard, history & statistics
- Virex: Requirements & installation
- Virex: User management
- Virex: External view
- Virex: Statistics
- Virex: Help document
- Live Demo
- Virex: Notes

History of the Norman Sample Sharing framework

- The idea for the Norman Sample Sharing framework was born at VB2009 and was introduced at Caro2010 by employees of Norman (hence the name)

- Norman completely switched to the Norman Sample Sharing framework in January 2011 for any exchange of malware samples

History of Avira's sample sharing

Frequent (monthly) exchange with other vendors:

- **2001 – 6 vendors**
- **2003 – 12 vendors**
- **2006 – 20 vendors**
- **2009 – 37 vendors**
- **2011 – 58 vendors**

Statistics of Avira's sample sharing

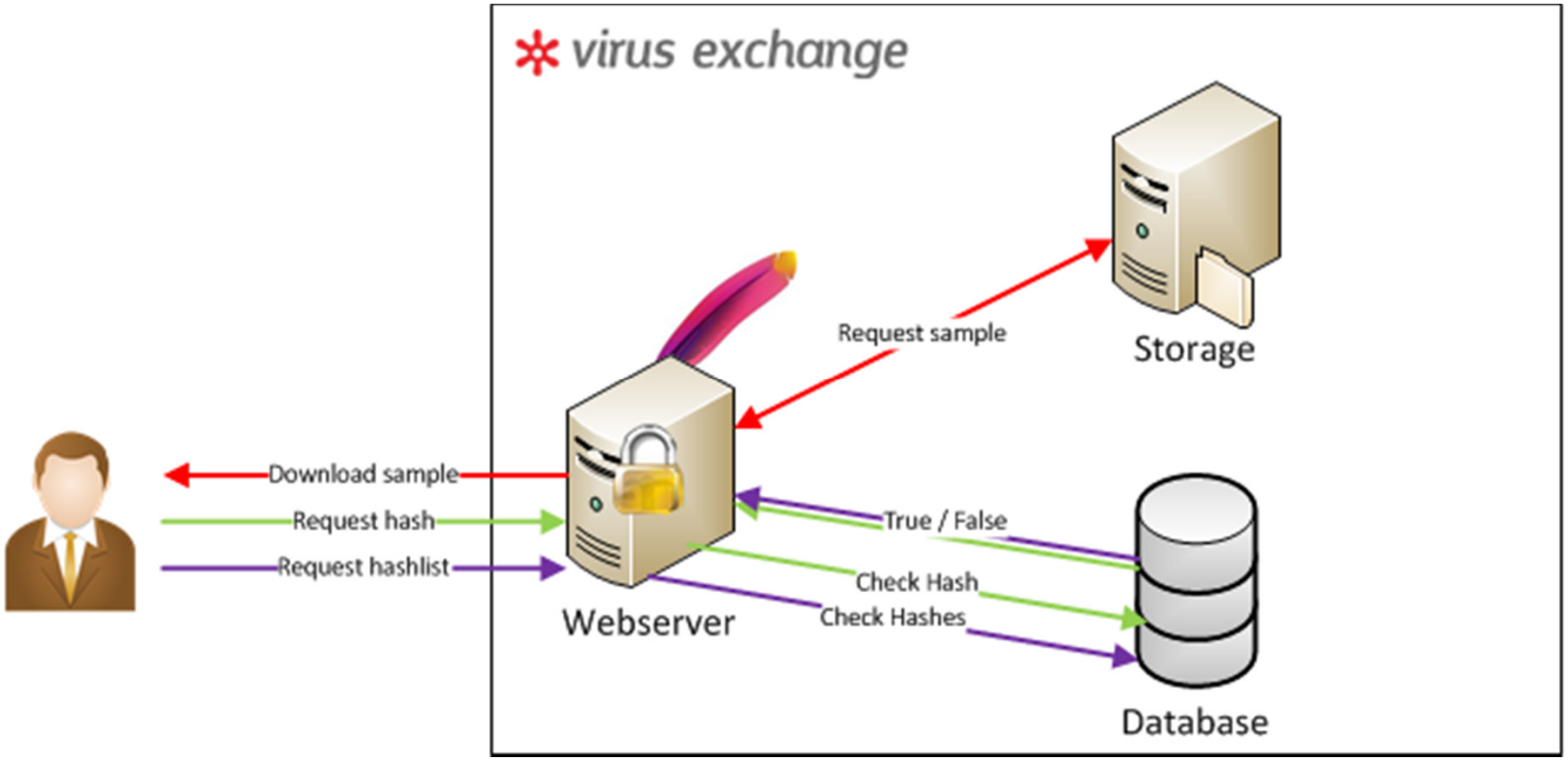
- **Avira is currently sharing malware collections with 58 companies**

- **Only 7 companies are using the Norman Sampleshare Framework (12%)**

- **Average of duplicate downloaded files:**

  - 12.000 malware samples per day (4.4 million samples per year)
  - 7 GB daily traffic (2.5 TB traffic per year)

Norman sharing standard



Virex: Requirements

virus exchange

Hardware requirements

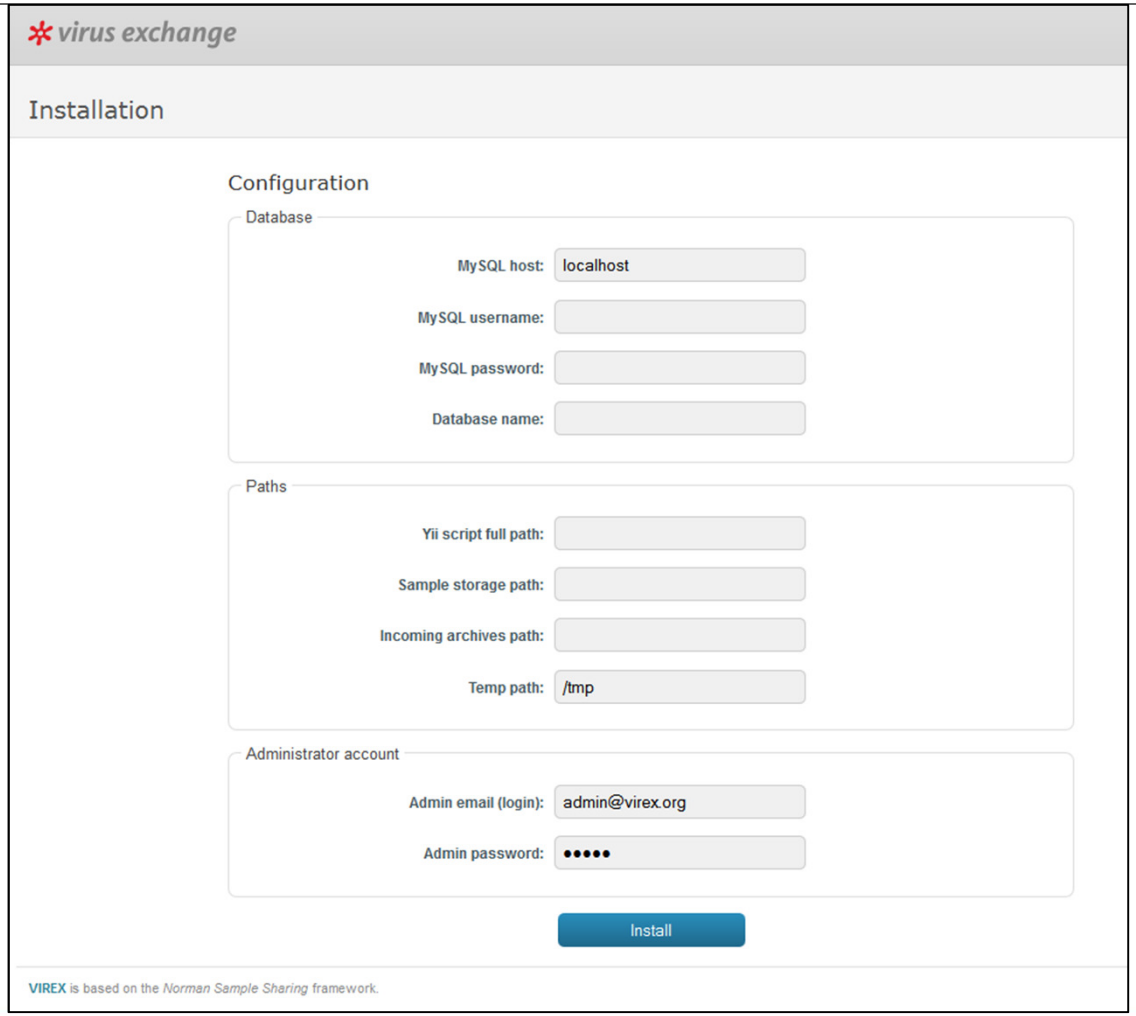
- depend on the amount of samples and users you want to handle in the system. Basically a web-server with 512 MB RAM & 50 GB HD is fine.

Software requirements

- UNIX or Microsoft Windows based operating system
- Apache2
- PHP5
- MySQL
- Yii framework
- Fusion Charts
- SMTP Server
- GnuPG
- 7zip

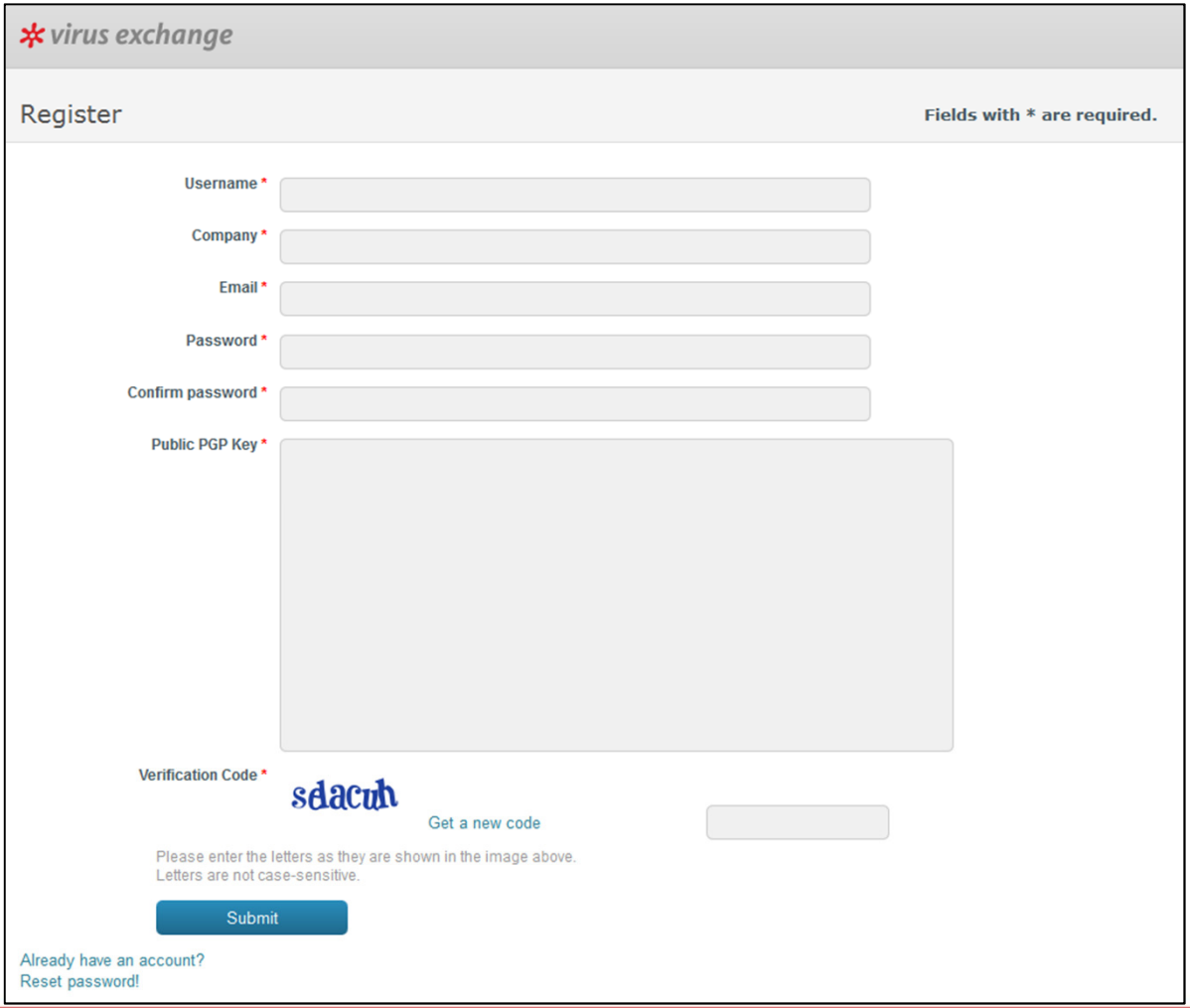
Virex: Installation

virus exchange



Virex: User management

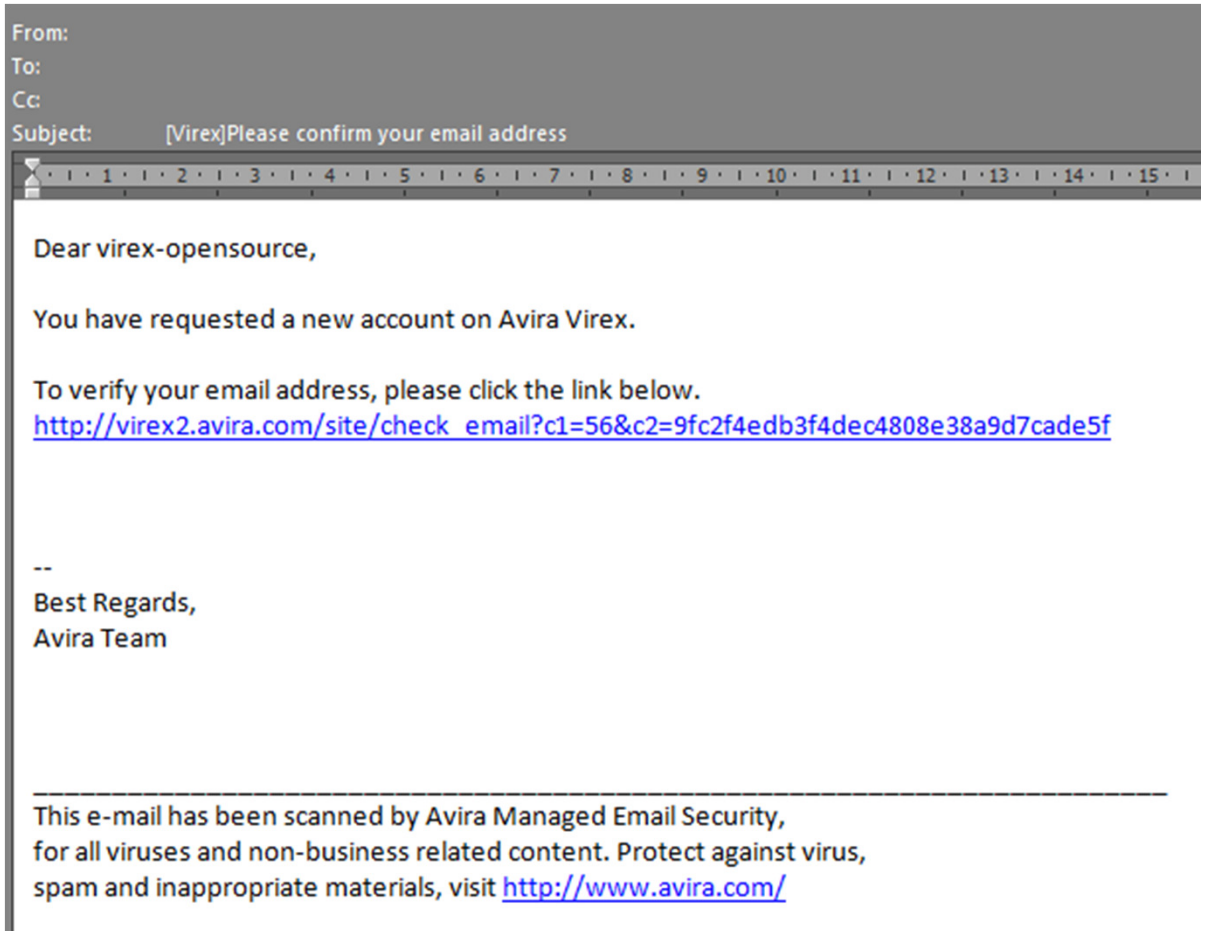
virus exchange



Virex: User management

virus exchange

User's email


From:
To:
Cc:
Subject: [Virex]Please confirm your email address

Dear virex-opensource,

You have requested a new account on Avira Virex.

To verify your email address, please click the link below.
http://virex2.avira.com/site/check_email?c1=56&c2=9fc2f4edb3f4dec4808e38a9d7cade5f

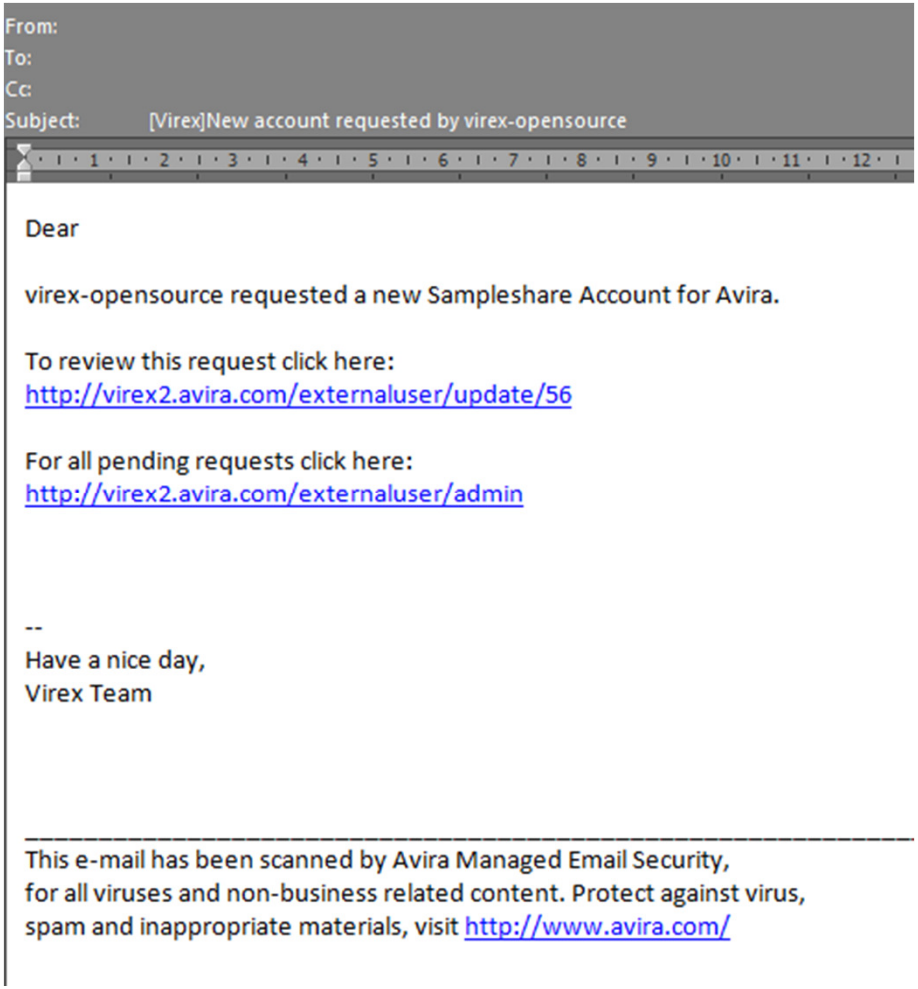
--
Best Regards,
Avira Team

This e-mail has been scanned by Avira Managed Email Security,
for all viruses and non-business related content. Protect against virus,
spam and inappropriate materials, visit http://www.avira.com/

Virex: User management

virus exchange

Your email



From:
To:
Cc:
Subject: [Virex]New account requested by virex-opensource

Dear

virex-opensource requested a new Sampleshare Account for Avira.

To review this request click here:
http://virex2.avira.com/externaluser/update/56

For all pending requests click here:
http://virex2.avira.com/externaluser/admin

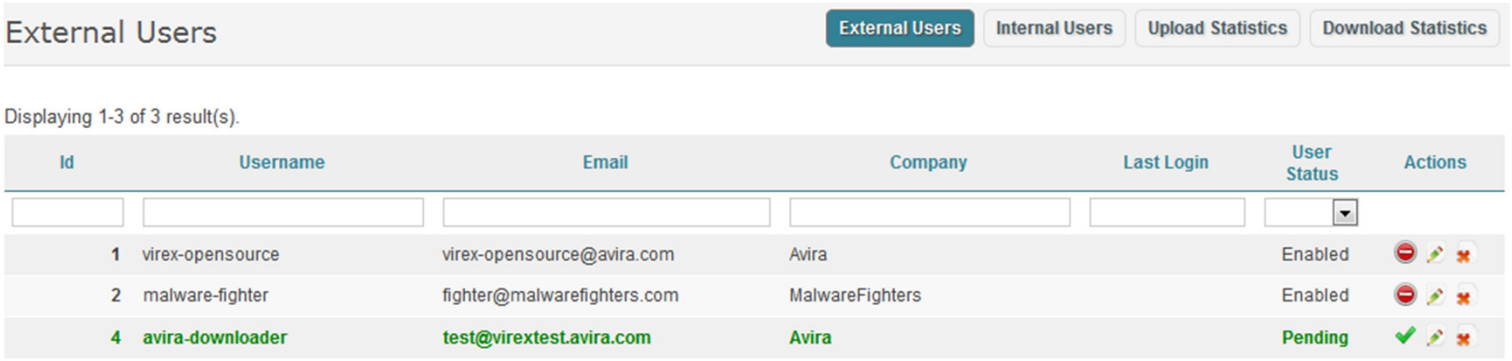
--
Have a nice day,
Virex Team

This e-mail has been scanned by Avira Managed Email Security,
for all viruses and non-business related content. Protect against virus,
spam and inappropriate materials, visit http://www.avira.com/

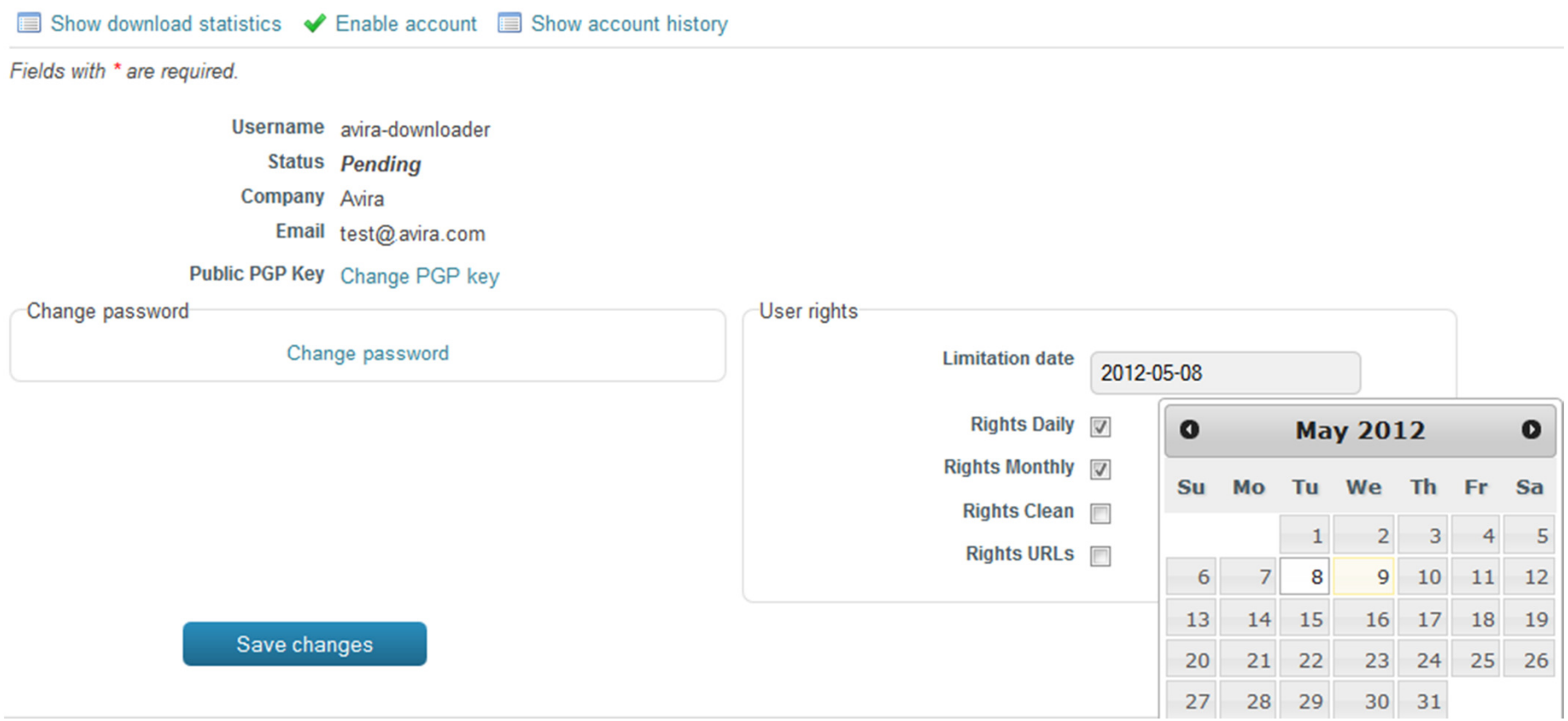
Virex: User management

virus exchange

Backend view

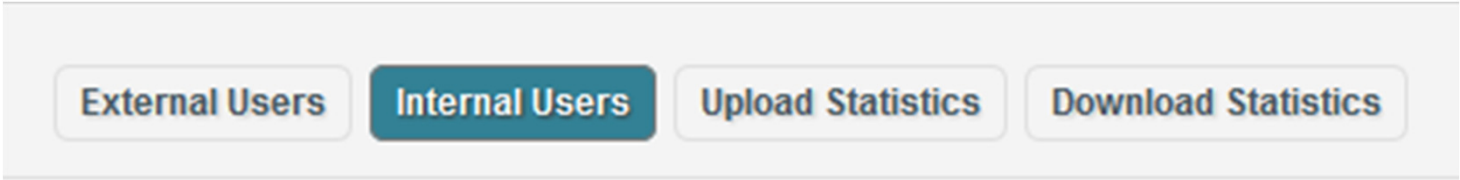


Virex: User management



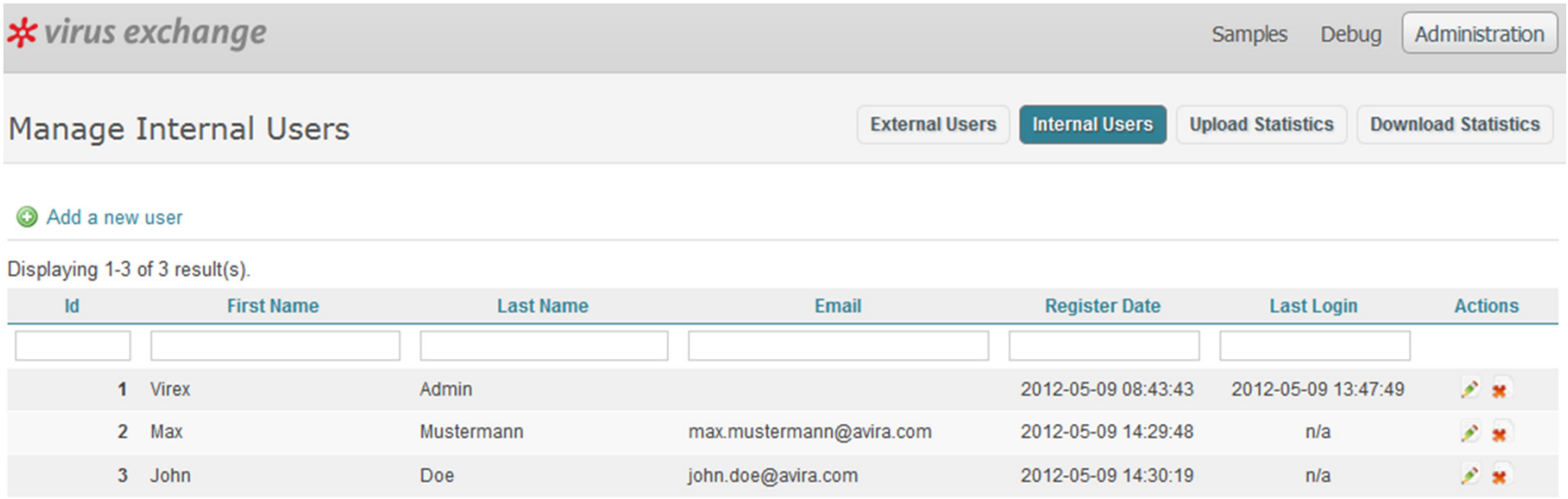
Virex: User management

virus exchange



Virex: User management

virus exchange

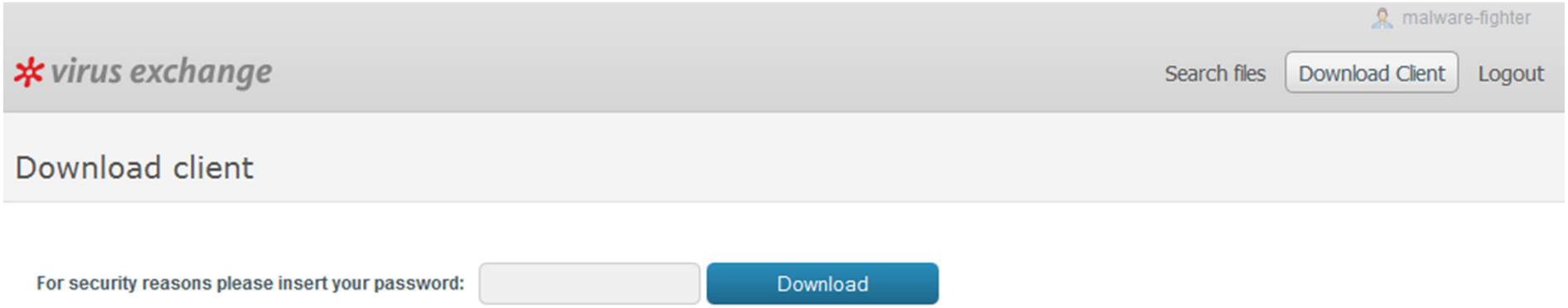


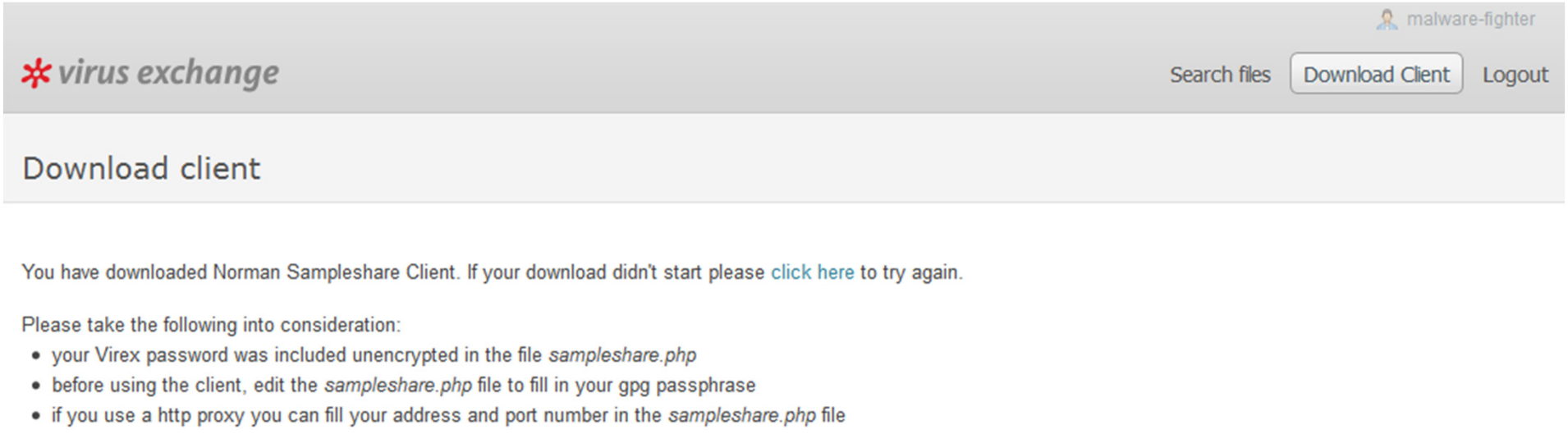
Virex: External view

virus exchange

Virex: External view

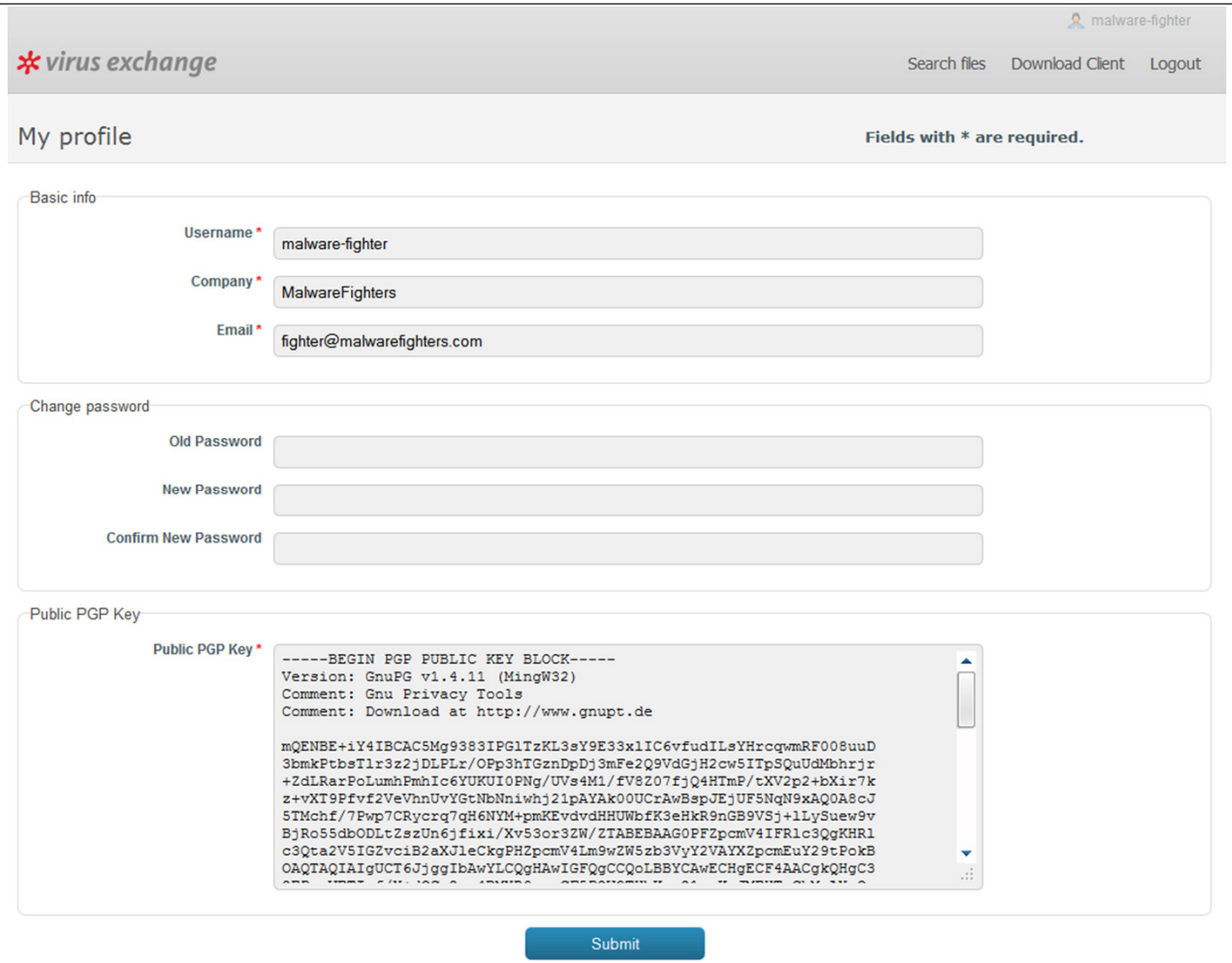
virus exchange





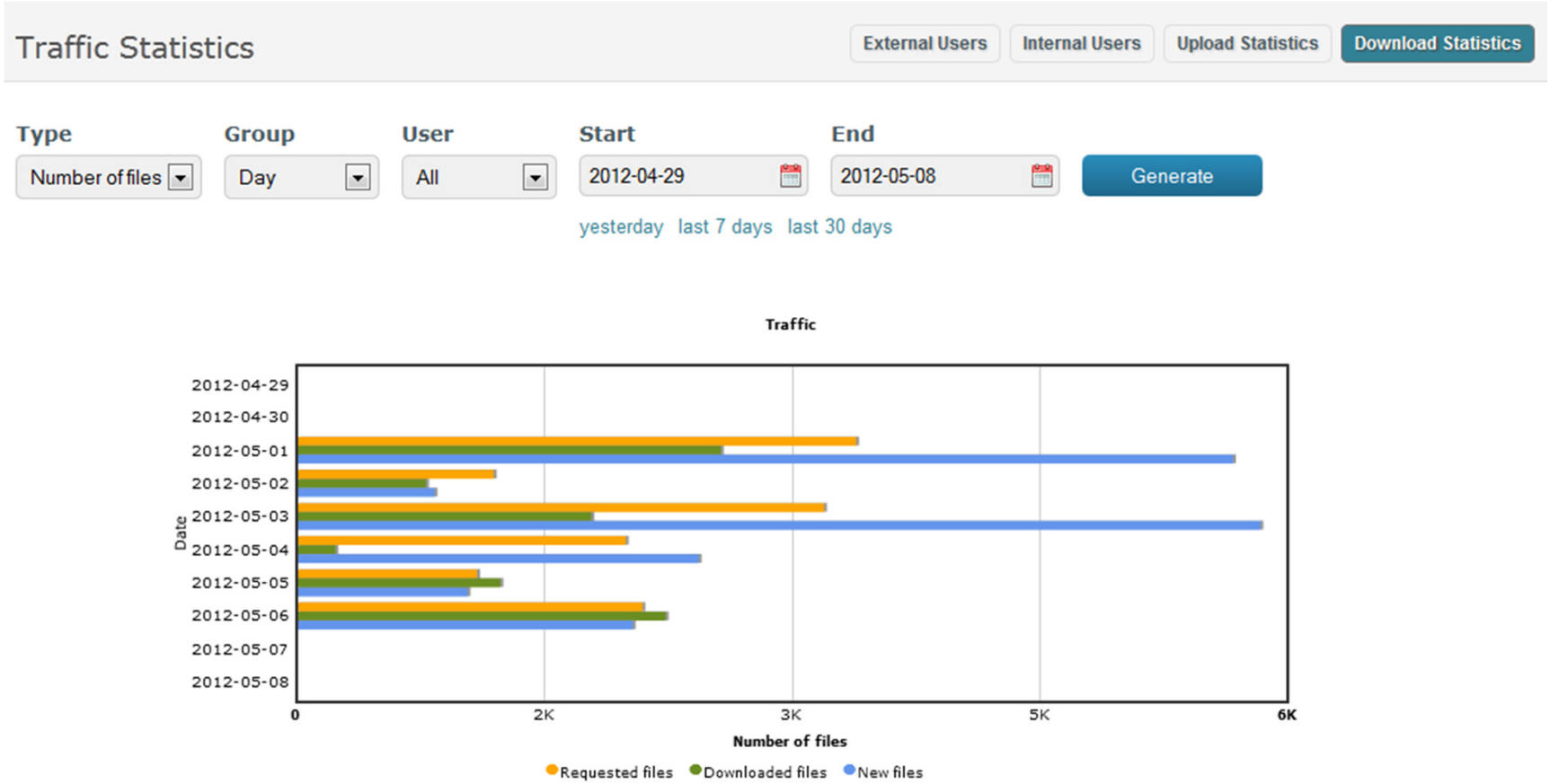
Virex: External view

virus exchange



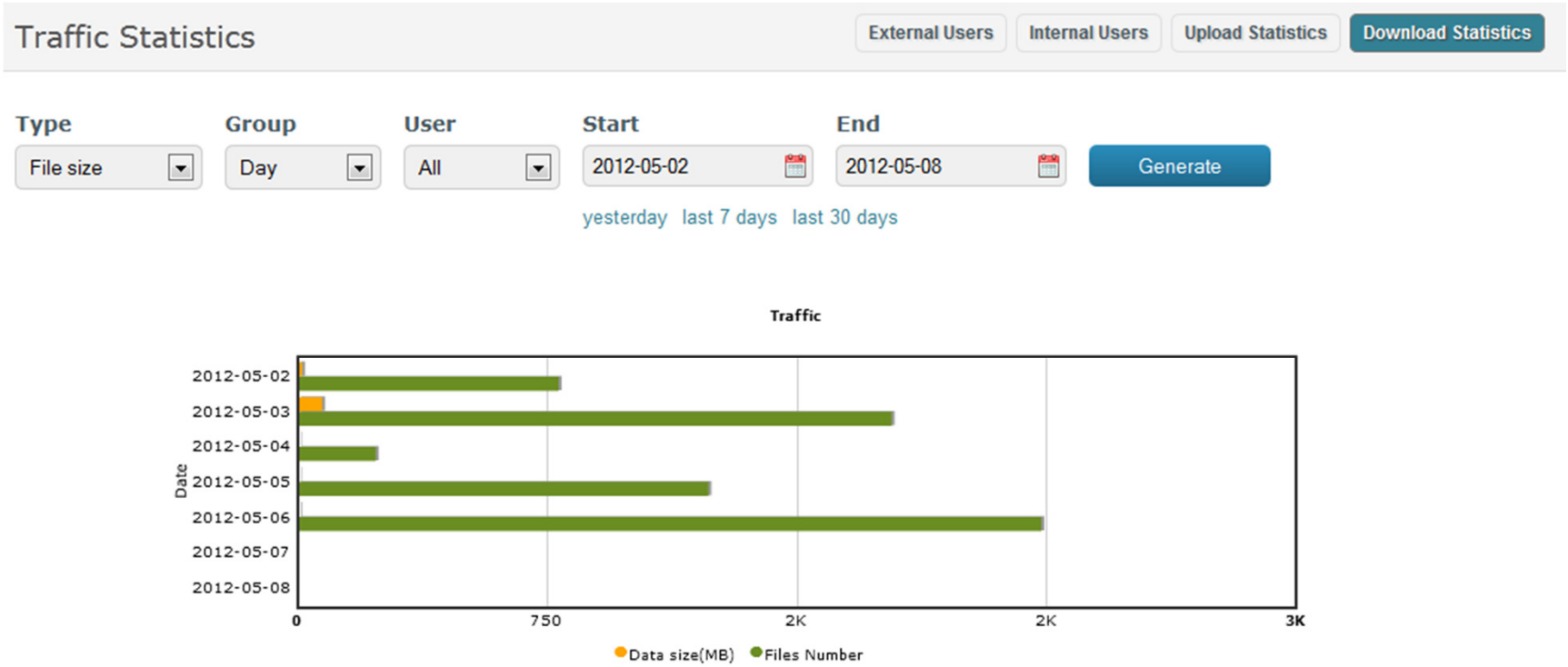
Virex: Statistics

virus exchange



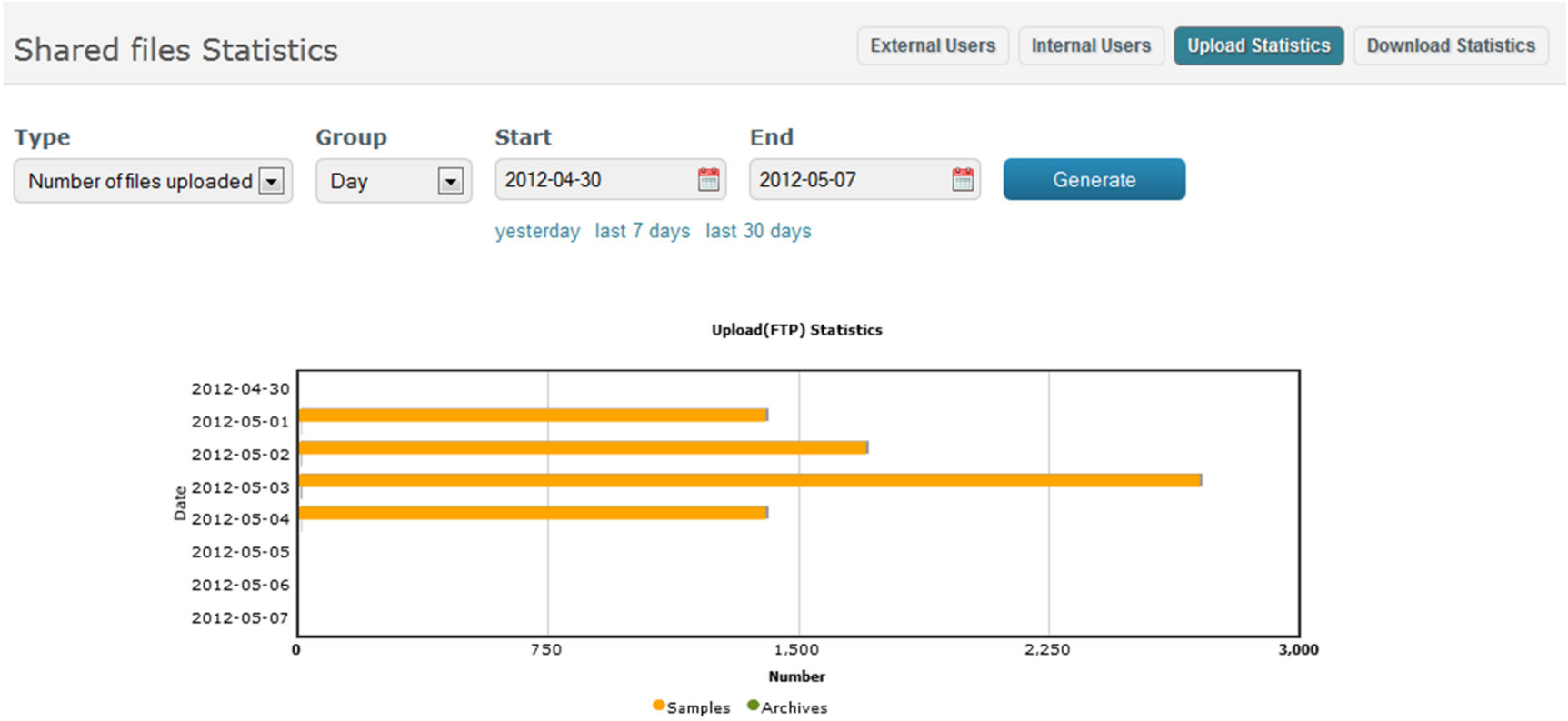
Virex: Statistics

virus exchange



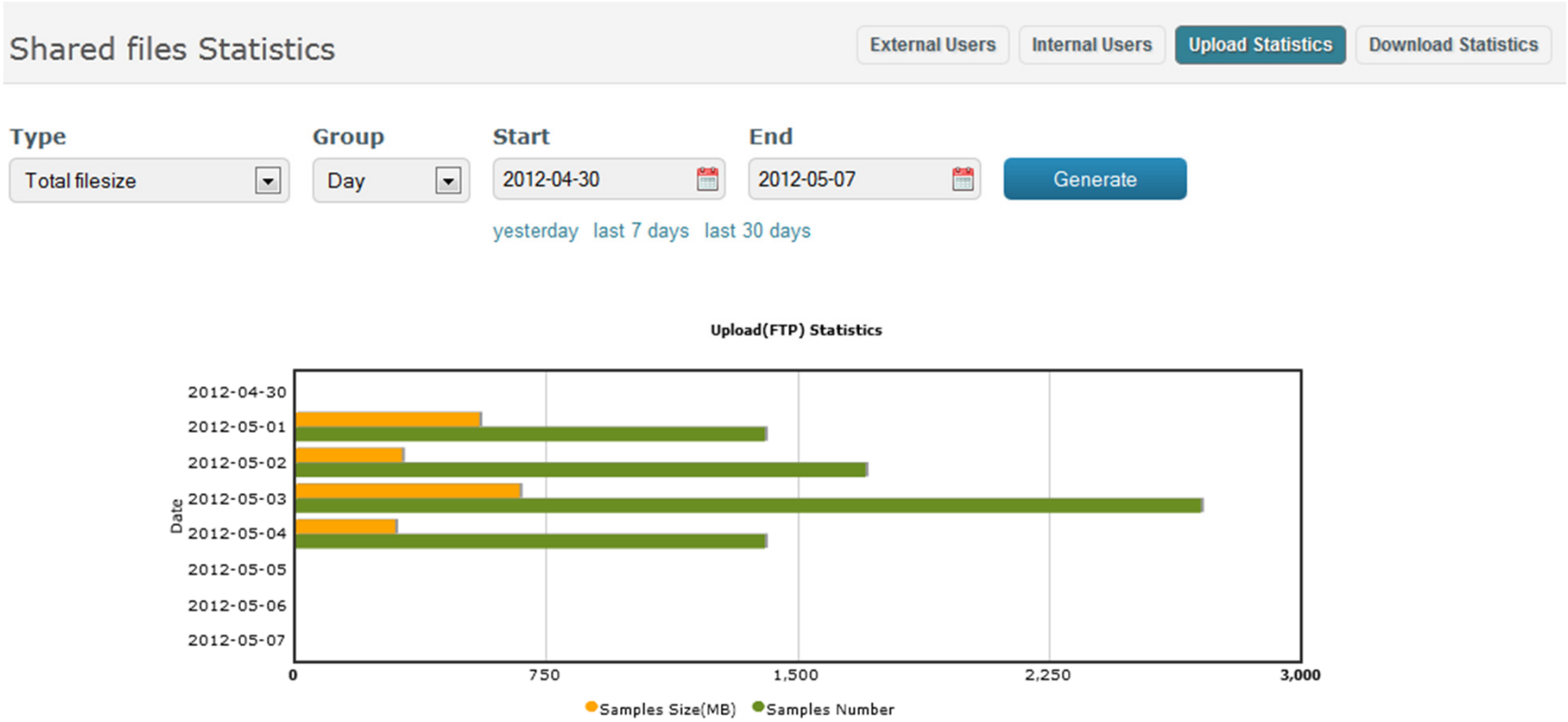
Virex: Statistics

virus exchange



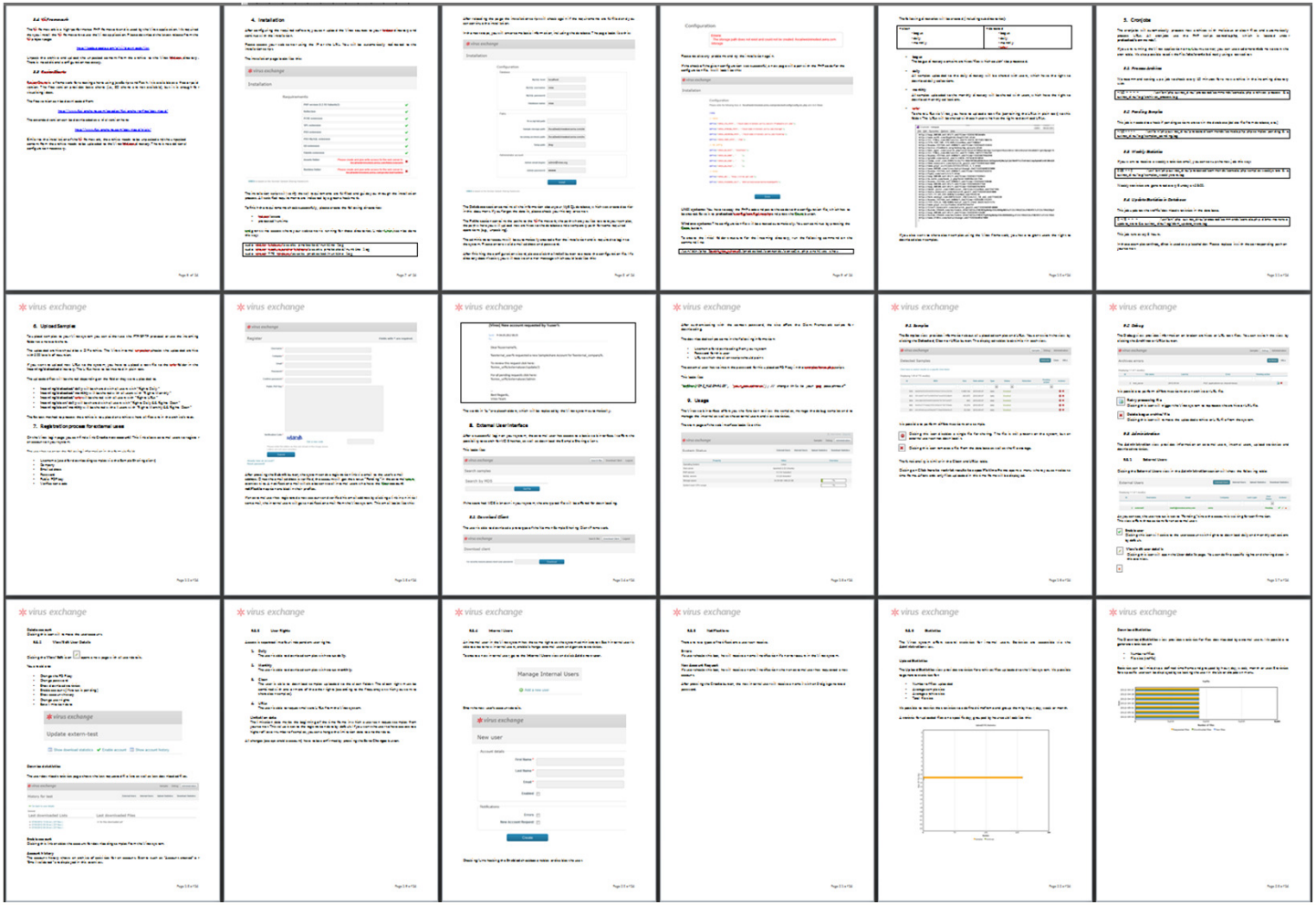
Virex: Statistics

virus exchange



Virex: Help document

virus exchange



Virex: Live demo

virus exchange

Virex: notes

virus exchange

- The application is published under the “new BSD license”
- The project is hosted on Google Code http://code.google.com/p/virex
- Reporting issues is possible on the project site
- Submitting code is possible using GIT repository on Google Code

Questions? Questions!

Philipp Wolf
Director Protection Labs

www.avira.com