MUTE

Malware URL Tracking and Exchange

:-x

Costin Raiu – Kaspersky

Jong Purisima – GFI

Nick Bilogorskiy – Facebook

Philipp Wolf – Avira

Tony Lee – Microsoft

MUTE

Agenda

- Non-technical stuff
- Technical stuff
- Followed by non-technical stuff
- Live demo = 10 min of your lunch break

MUTE

History

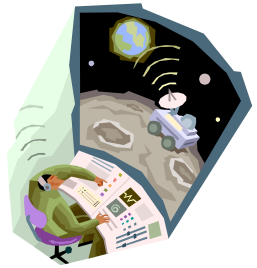
vb 2009 GENEVA

Hey, how about URL Sharing?

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Charter



- Mission:
  - is to minimize the exposure of end users from computing threats through timely tracking and exchanging of URLs (malicious, grey & clean).
- Objectives:
  - Share quality URLs faster
  - Simplify the exchange process
  - Combine all data for better reporting

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

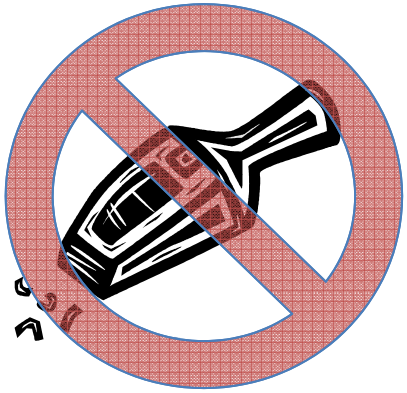
Organization

- Communication Medium
  - Discussion List
  - Exchange List (or system)
  - Board List
- Members
  - 17 members, 11 companies
- Advisory Board
  - Founding members

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Sharing Principles

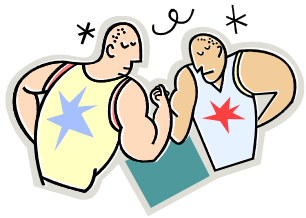


- NO Leechers!
- Main metrics:
  - Share often (Frequency)
  - Share only the “good” stuff (Quality)
  - Share as many as you can (Quantity)
- No re-share
- No re-sell

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

URL Sharing Challenges



- URL Time-To-Live (TTL) is short and critical.
- Costly to set-up exchange
  - Set-up outgoing servers
  - Different formats for incoming shares

    (Email, FTP, HTTPS, hxxp, h__p, etc)
  - Set-up incoming shares' access and parsers
- Managing new relationships (!=File-based shares)

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Files vs URLs

MUTE

Why Centralization?

- All the information in one place
  - Easy one-time fetch
  - Single interface
  - Larger set of statistics
- No need for a participant to setup and host a server.
- Why not?

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

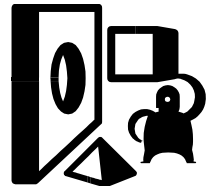
Centralization Challenges

Non-Technical	Technical
Who will build and maintain the system?	Requirements and Features
Who will host the system?	Architecture and Infrastructure
Who will pay for Server/System/Bandwidth Costs?	Development Language to use
“I don’t share with everyone”	Development/Maintenance effort
“I share differently depending on the sharing partner”	Testing
“No one should have all that control”	Release Lifecycle

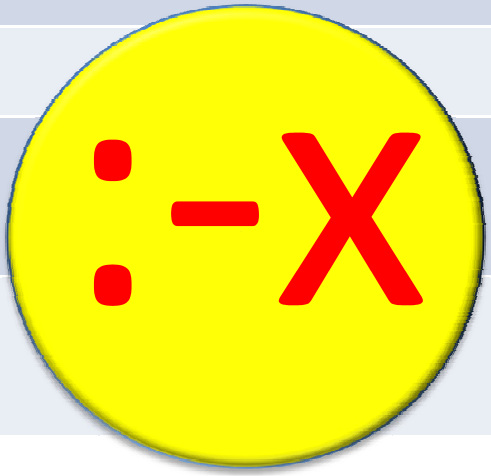
AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Addressing the Non-Technical



Non-Technical	Solution
Who will build and maintain the system?	Shared by each member
Who will host the system?	3rd Party or neutral group
Who will pay for Server/System/Bandwidth Costs?	Shared by each member
“I don’t share with everyone”	
“I share differently depending on the sharing partner”	
“No one should have all that control”	

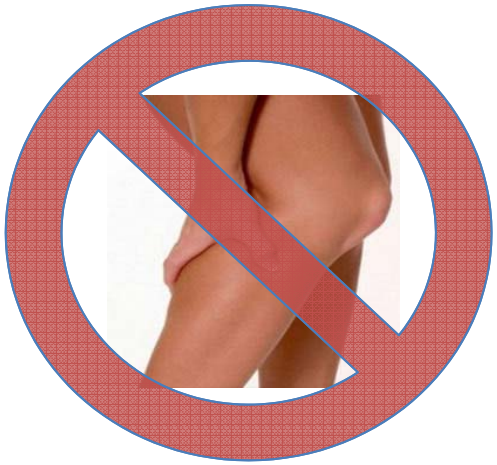


AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Solve the Technical issues first 

CARO2010 HELSINKI

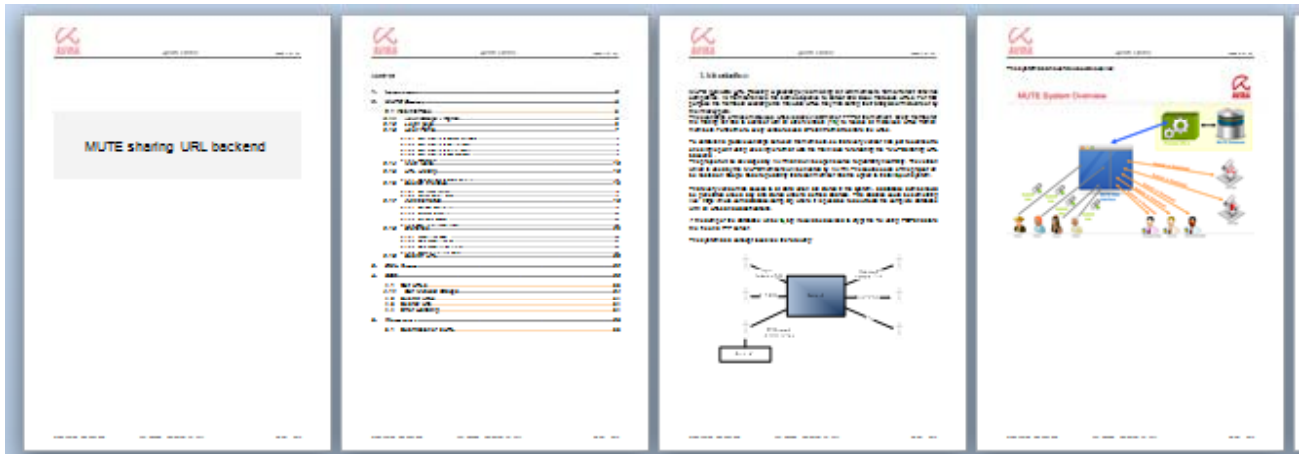


- Avira offered their Web Dev guys for dev
- Use Open Source so can still be hosted and maintained by other members in the future, if necessary.

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Requirements

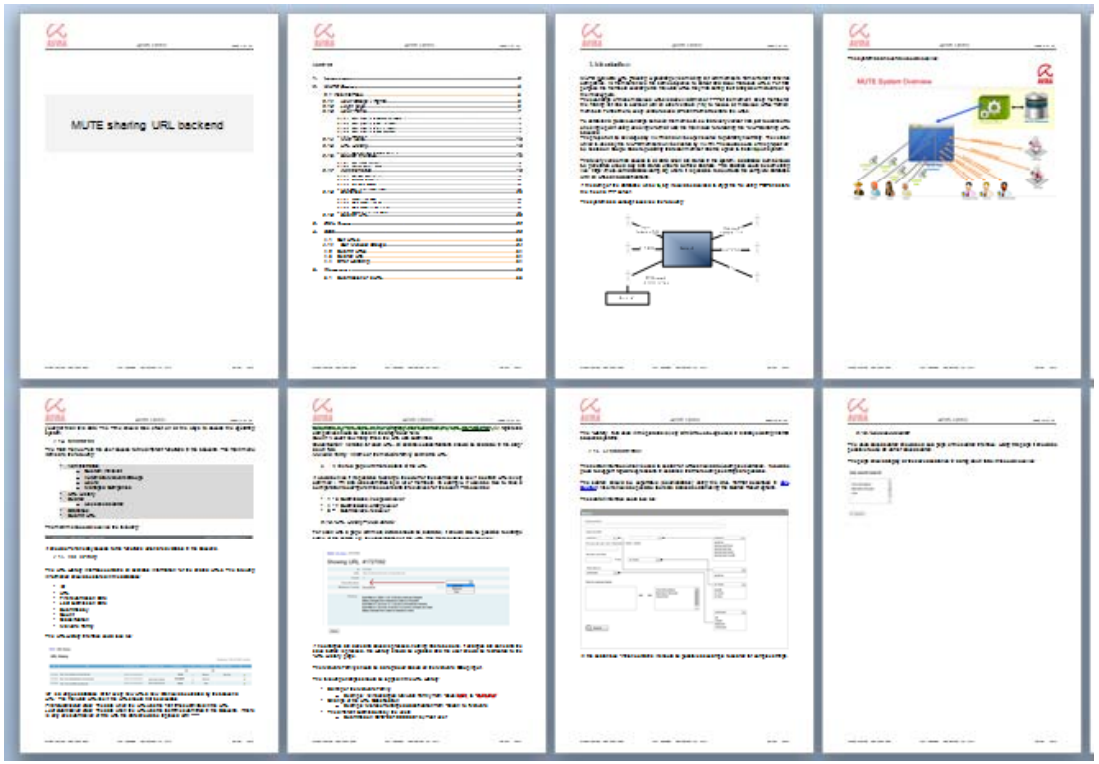


AVIRA

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Requirements V0.2



AVIRA

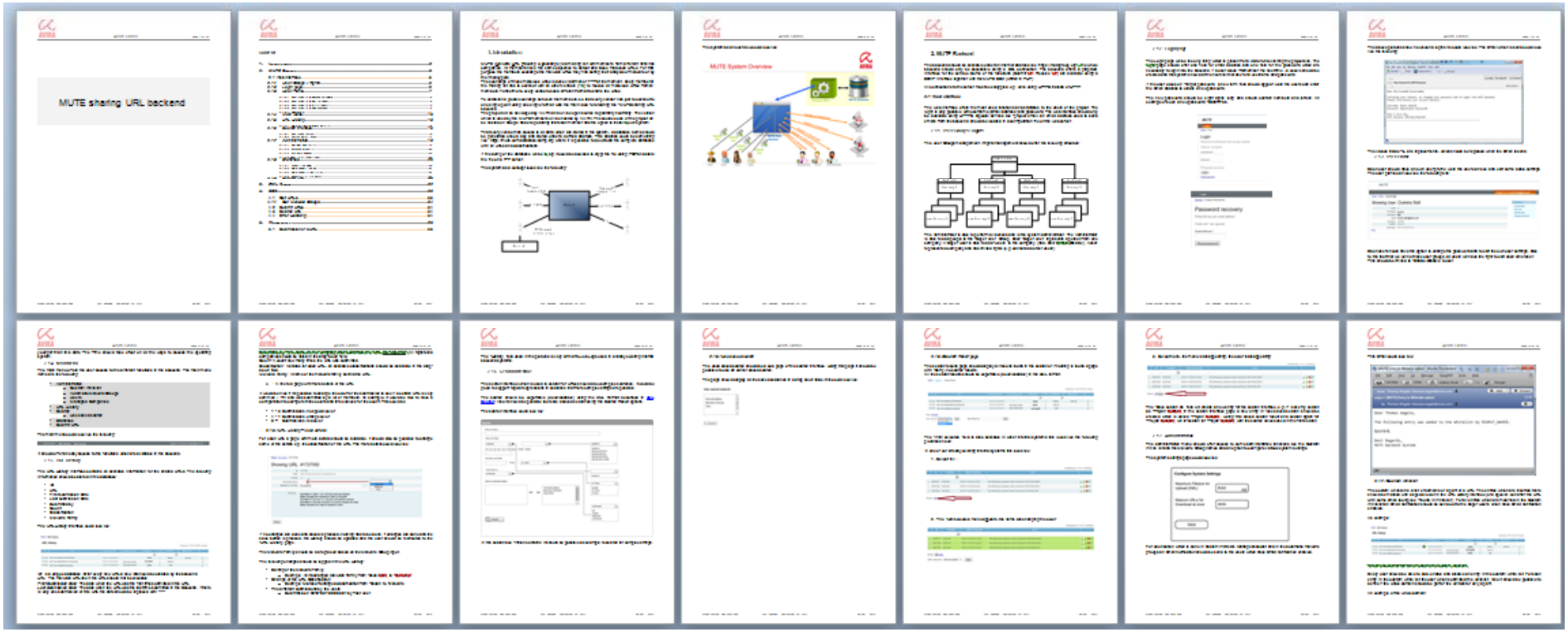
+

KASPERSKY lab

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Requirements V0.7

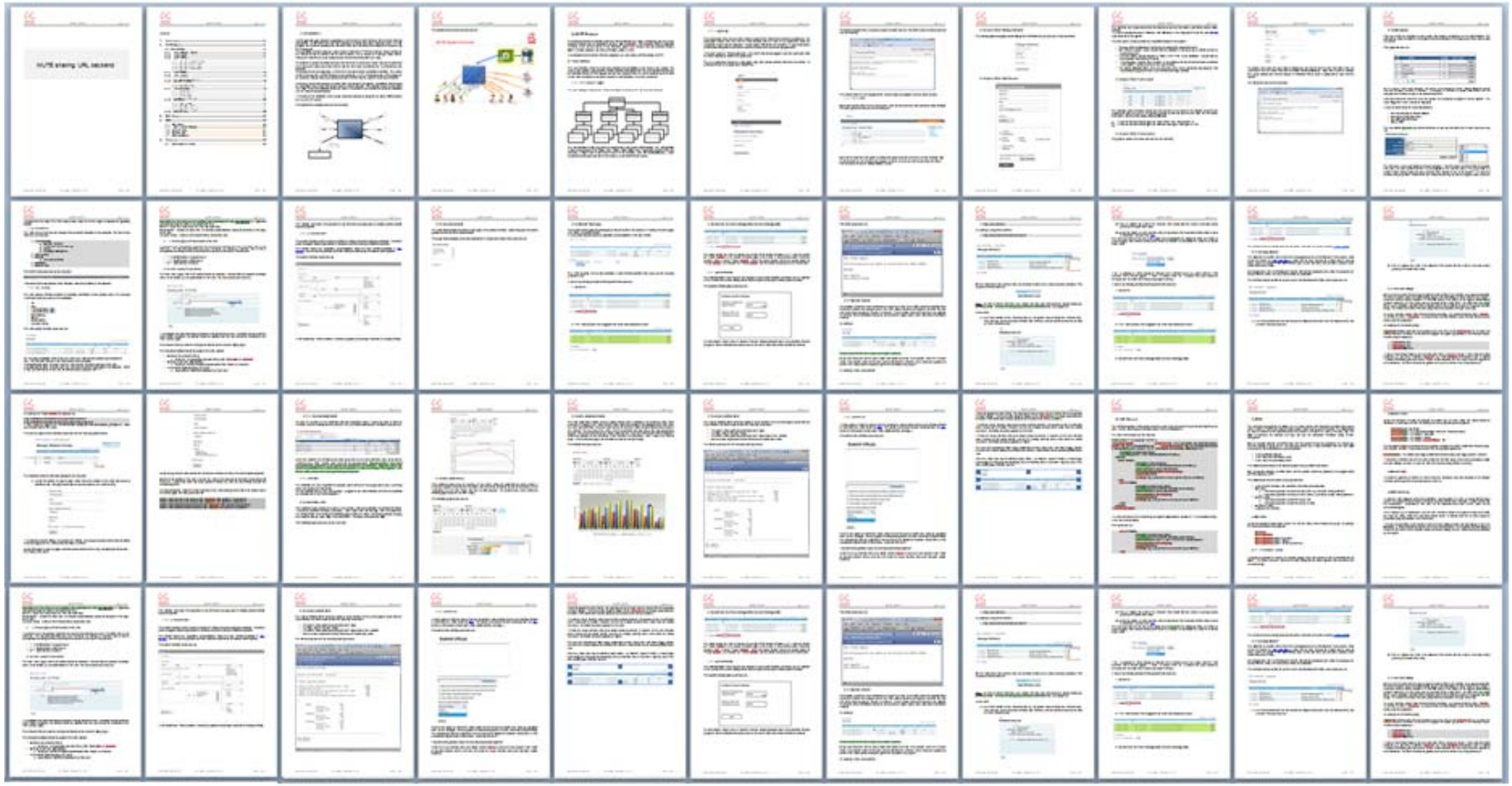


AVIRA + KASPERSKY + facebook + GFI

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Requirements final(ly)



AVIRA + KASPERSKY + facebook + GFI + Malware Protection Center Threat Research and Response

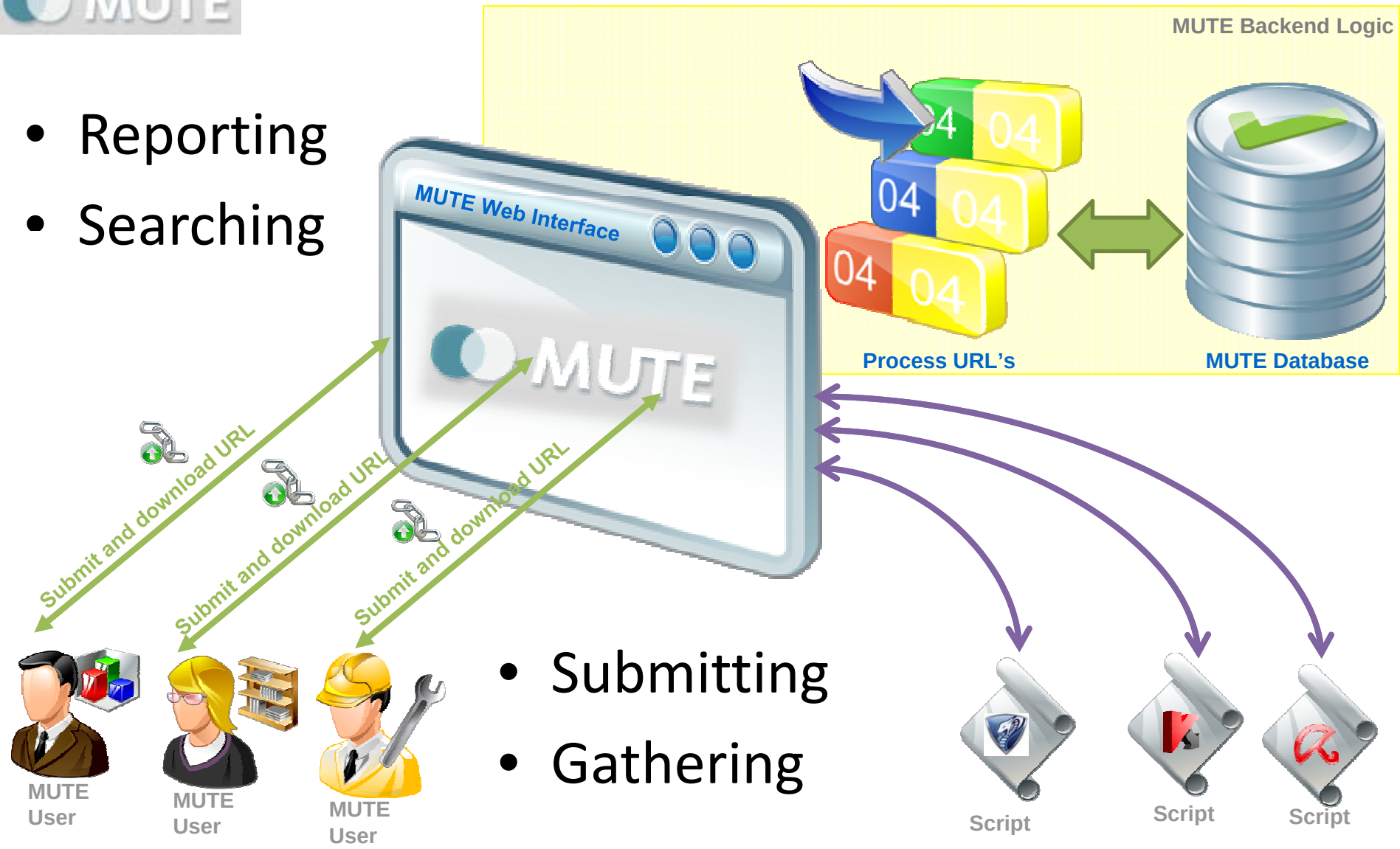
MUTE

Development

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

- Reporting
- Searching



- Submitting
- Gathering

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

Submit URLs: using web interface

MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Submit URL(s)

New Submission | My Submissions | All Submissions

Enter URL(s)

```
http://tendeki.tk/c99.txt??
http://bjminmao.com/images/facebook-pic000934519.exe
http://pastebin.com/raw.php?i=6CK5RBQW
http://hackforums.ru/bot.exe
http://tendeki.tk/rfiid.txt
http://tendeki.tk/sprd.txt
http://which-solar.co.uk/wp-content/themes/twentyten/izle.exe
```

Maximum number of lines is 50.000

Or upload a file with URLs

Durchsuchen...

Maximum file size is 8M. Maximum number of lines is 50.000

Classification

Malware

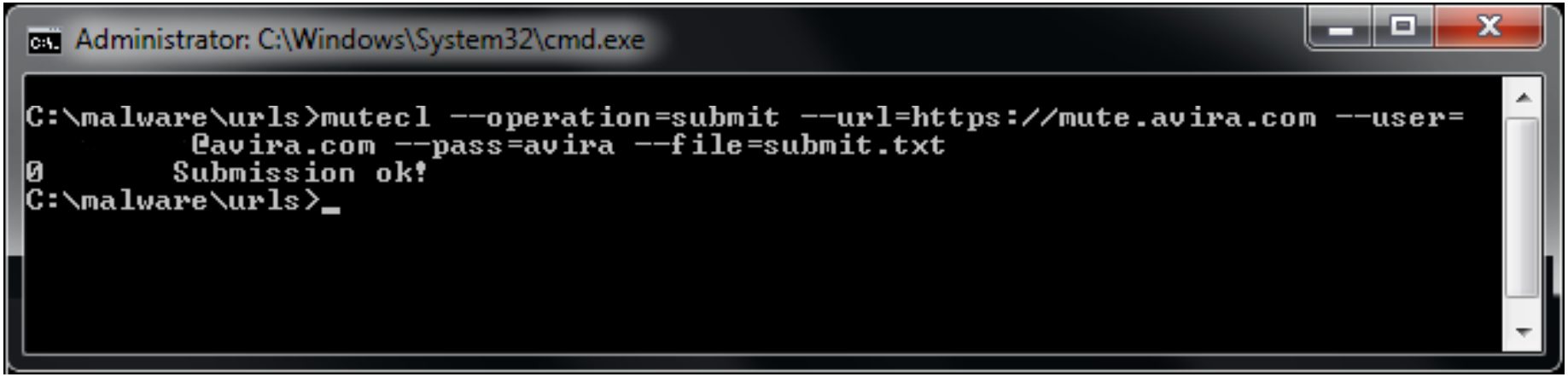
Malware Family

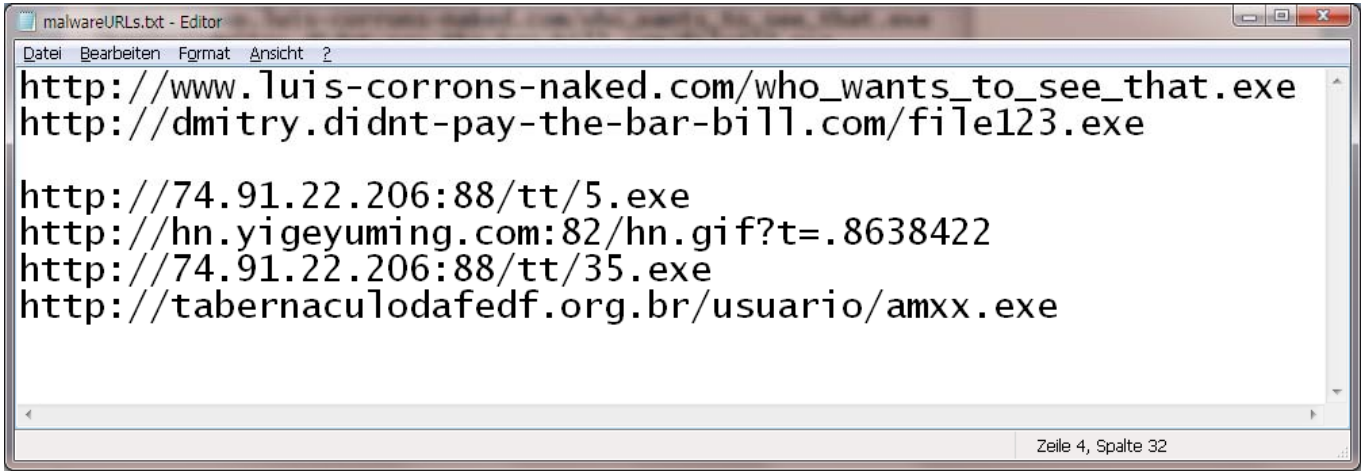
AUTO

Submit

MUTE

Submit URLs: using API





C client

API available for all languages

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Review your submission(s)

Showing URL Submission #47

New Submission | My Submissions | All Submissions

Submission Details

Submitted By	
Status	Done
Filename	form_input
Filesize	25.44 KB
Time Submitted	2011-07-07 09:29:45
Time Processed	2011-07-07 09:29:47 (in 1.7024s)
Classification	malware
Malware Family	automatic

⇐ Back to list

Submission Log

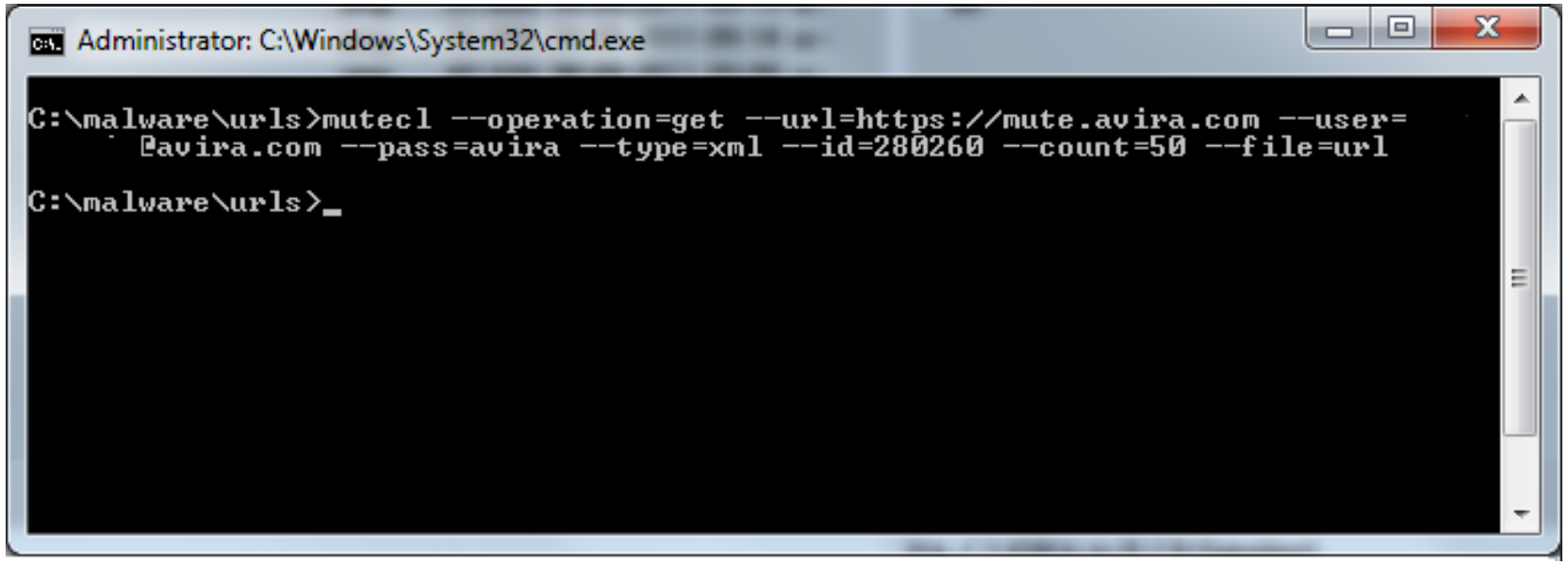
Displaying 21-40 of 509 result(s).

Id	Url	Status	New
279643	http://vwyjkeaqcfhdj.cz.cc/games/2fdp.php?f=43	ok	✔
279644	http://beautyxvidseff.tk/new/animal-porn-movie.avi.exe	ok	✔
279645	http://freesexpornonew.info/7/video/porno-rolik7.avi.exe	ok	-
279646	http://beautyxvidseff.tk/new/dog-doing-girl.avi.exe	ok	-
279647	http://bestdvddownload.com/New-Video-Addon.40563.exe	ok	✔
279648	http://bestdvddownload.com /SOTI.Pocket.Controller.Pro.6.0...	ok	✔
279649	http://eileen-shark-1.co.tv/counter1/574a353789f /lastrger...	ok	-
279650	http://bghhdjjedfwdsfg.cz.cc /forum.php?tp=ba2f32cb3a6cd876	ok	✔
279651	http://freesexpornonew.info/1/video/porno-rolik1.avi.exe	ok	-
------	http://freesexpornonew.info/2/video/porno-		

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Download URLs: using API



AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

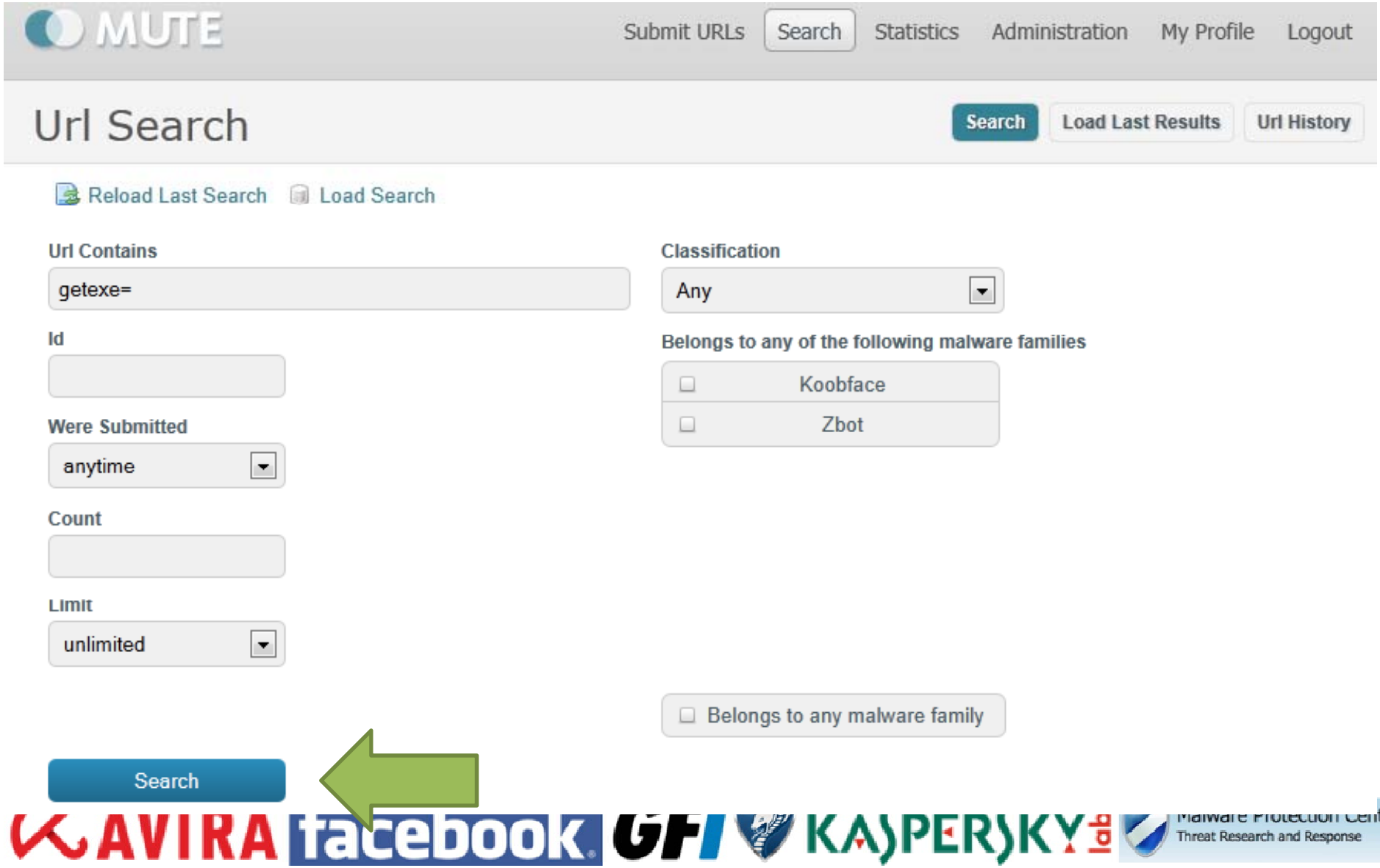
MUTE


```
<?xml version="1.0" encoding="UTF-8"?>
- <urls>
  - <url id="3494">
      <company>Avira</company>
      <last_time>2011-04-27 15:45:33</last_time>
      <count>1</count>
      <classification/>
      <whitelisted>0</whitelisted>
      <malwarefamily/>
      <urlstring>http://nvranch-alpacas.com/.yf4wq/?getexe=d.exe</urlstring>
    </url>
  - <url id="4337">
      <company>Avira</company>
      <last_time>2011-04-27 15:45:36</last_time>
      <count>1</count>
      <classification/>
      <whitelisted>0</whitelisted>
      <malwarefamily/>
      <urlstring>http://www.afadjapo.org/.8u4yf52/?getexe=aolblog.exe</urlstring>
    </url>
```

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Search for URLs



MUTE

Search for URLs

MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Search results:

Search | Load Last Results | Url History

Back to search | New search | Save search

Displaying 1-5 of 953 result(s). 5 items

Id	Url	Last Submitted	Submitted by	Count	Classification	Malware Family
3494	http://nvranch-alpacas.com/.yf4wq /?getexe=d.exe	2011-04-27 15:45:33	Avira	1		
4337	http://www.afadjapo.org/.8u4yf52 /?getexe=aolblog.exe	2011-04-27 15:45:36	Avira	1		
5831	http://www.longting.nl/.rqtsoj1 /?getexe=v2captcha21.exe	2011-04-27 15:45:41	Avira	1		
5832	http://vakre-hjem.com/.t2ac /?getexe=loader.exe	2011-04-27 15:45:41	Avira	1		
5833	http://www.longting.nl/.rqtsoj1 /?getexe=manyblogs.exe	2011-04-27 15:45:41	Avira	1		

Select: all none Selected 5 across page. Click here to select all 953! Go to page: < Previous 1 2 3 4 5 6 7 8 9 10 Next >

With selected: choose action Go!

choose action
download xml
download csv

download your search result in XML

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

View History for each URL

MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Showing URL #153172

Edit URL classification and malware family

URL Details

Id	153172
Url	hxxp://symposium.israimplant.com /.sys.php?getexe=fcblog.3.exe
Md5	3187595EBC9CF721F2F77195C128B068
First Submitted	2011-09-29 15:15:00
Last Submitted	2011-09-29 15:15:00
Count	1
Classification	Malware
Malware Family	*Koobface*
Submitted by	Avira

History

2011-09-29 16:28:27 Updated by Avira: added "malware" Classification, added "Koobface" Malware Family

2011-09-29 16:28:22 Updated by Avira: removed Classification

2011-09-29 16:28:19 Updated by Avira: Classification from "malware" to "clean", removed Malware Family

2011-09-29 16:28:16 Updated by Avira: Malware Family from "Koobface" to "Zbot"

2011-09-29 16:28:12 Updated by Avira: added "malware" Classification, added "Koobface" Malware Family

2011-09-29 15:15:00 Submitted by Avira

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Whitelist

MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Manage Whitelist Entries

Users | Companies | Lists | Malware Families

Switch to Blacklist | Add a new entry

Displaying 1-3 of 3 result(s). 25 items

Id	Url	Comment
2	avira.com/	AVIRA Antivirus
4	microsoft.com/	Microsoft
5	google.de/	Google Search Engine

Select: all none

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

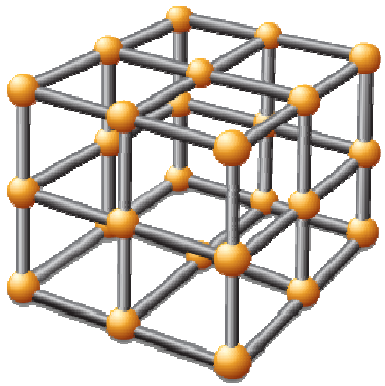
Whitelist

```
<?xml version="1.0" encoding="UTF-8"?>
<urls>
    <url id="5">
        <company>Avira</company>
        <last_time>2011-04-27 13:02:46</last_time>
        <count>1</count>
        <classification/>
        <whitelisted>1</whitelisted>
        <malwarefamily/>
        <urlstring>http://www.avira.com</urlstring>
    </url>
</urls>
```

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Malware Families



MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Manage Malware Families

Users | Companies | Lists | Malware Families

RegEx

Add a new malware family

Displaying 1-2 of 2 result(s).

Id	Family Name	Automatic	URL Pattern	Enabled
1	Koobface	✔	/.sys/?getexe=	✔
2	Zbot	✔	.bot.exe	✔

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

```
<?xml version="1.0" encoding="UTF-8"?>
- <urls>
  - <url id="4337">
      <company>Avira</company>
      <last_time>2011-04-27 15:45:36</last_time>
      <count>1</count>
      <classification/>
      <whitelisted>0</whitelisted>
      <malwarefamily/>
      <urlstring>http://www.afadjapo.org/.8u4yf52/?getexe=aolblog.exe</urlstring>
    </url>
  - <url id="5831">
      <company>Avira</company>
      <last_time>2011-04-27 15:45:41</last_time>
      <count>1</count>
      <classification/>
      <whitelisted>0</whitelisted>
      <malwarefamily>Koobface</malwarefamily>
      <urlstring>http://www.longting.nl/.rqtsoj1/?getexe=v2captcha21.exe</urlstring>
    </url>
</urls>
```

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

Statistics

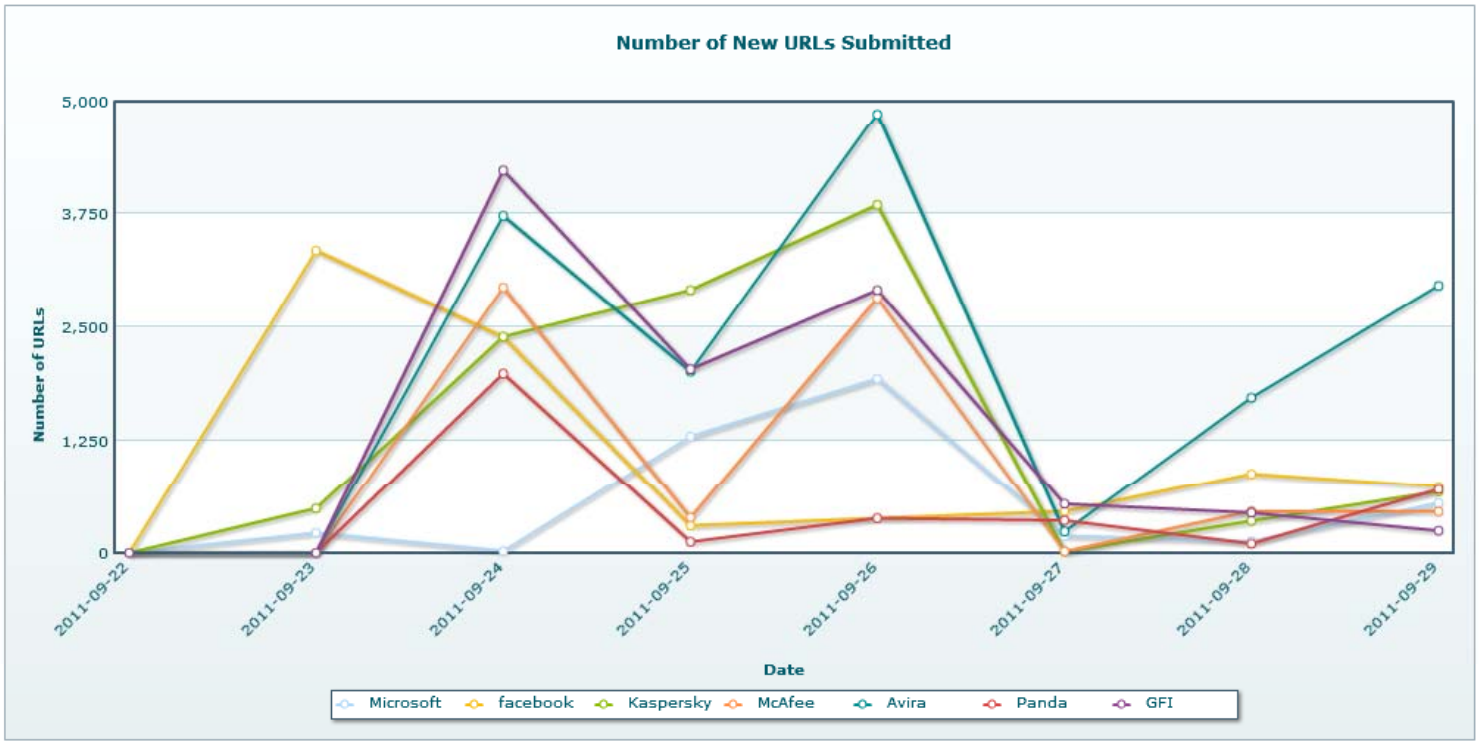
MUTE

Submit URLs | Search | Statistics | Administration | My Profile | Logout

Url Statistics

Statistic Type: New Urls Per Company | **Group By**: Day | **Filter Providers**: all | **Start Date**: 2011-09-22 | **End Date**: 2011-09-29 | Generate

yesterday last 7 days last 30 days



AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Future Considerations

- Mute System
  - Auto Monitoring – kicks out bad users.
  - Get out of Beta – Launching MUTE
- Organization
  - Prepare for a bigger membership
  - Board needs to be refreshed regularly

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

MUTE

Questions?

Malware URL Tracking and Exchange

One Beer – One Answer

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response

END

MUTE

Backup-Memberships

- Founders as initial members
- Added a few more for the discussion list
- Individual Membership
- Affiliations can be declared
- Must be nominated by a member
- Member nomination, Zero ‘NO’ vote to get in
- Expenses are shared by all members equally

AVIRA facebook GFI KASPERSKY lab Malware Protection Center Threat Research and Response