



MUTE

Malware URL Tracking and Exchange

:-X

Costin Raiu – Kaspersky

Jong Purisima – GFI

Nick Bilogorskiy – Facebook

Philipp Wolf – Avira

Tony Lee – Microsoft



Agenda

- Overview
- Technical works and demo
- Conclusion



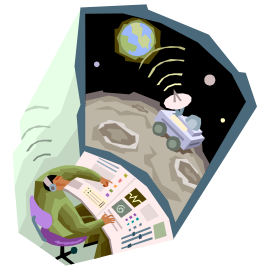
History



Hey, how about URL Sharing?



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

Organization



- Communication Medium
 - Discussion List
 - Exchange System
- Members
 - 25 members, 13 companies
 - Membership via nomination and vote
- Advisory Board
 - Founding members
 - Re-elected annually



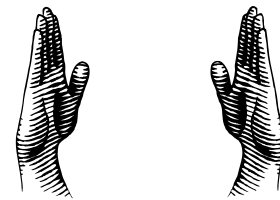
Sharing Principles

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

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
 - Manage feeds at different update frequency
- Managing new relationships



Files vs URLs

	Files	URLs
Threat object potency	As long as the OS or App	Couple of hours / days
Average Size	450KB/sample	< 1KB/sample
Transport requirements	PGP, archive w/password	HxxP / H__P
Storage Persistence	Yes	Not necessarily (TTL)
Most Used Sharing Scheme	1:n	
Best Sharing Scheme	Norman Sharing Framework	?

Why Centralization?

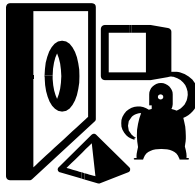
- All the information in one place
 - Easy fetch at own pace
 - Single interface
 - Larger set of statistics
- No need for a participant to setup and host a server.
- Get all the feeds
- Why not?

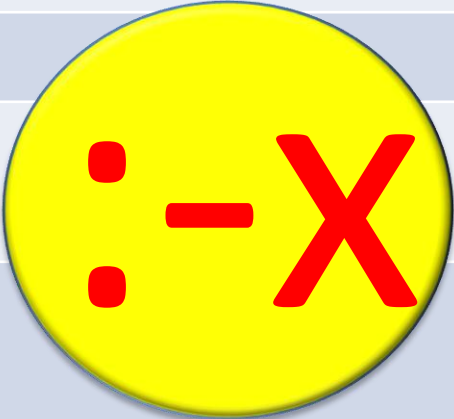
Centralization Challenges



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

Addressing the Non-Technical

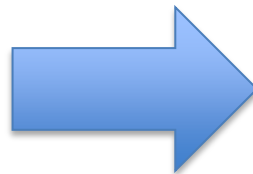


Non-Technical	Solution
Who will build and maintain the system?	Trusted member
Who will host the system?	Trusted member
“I don’t share with everyone”	
“I share differently depending on the sharing partner”	
“No one should have all that control”	

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.

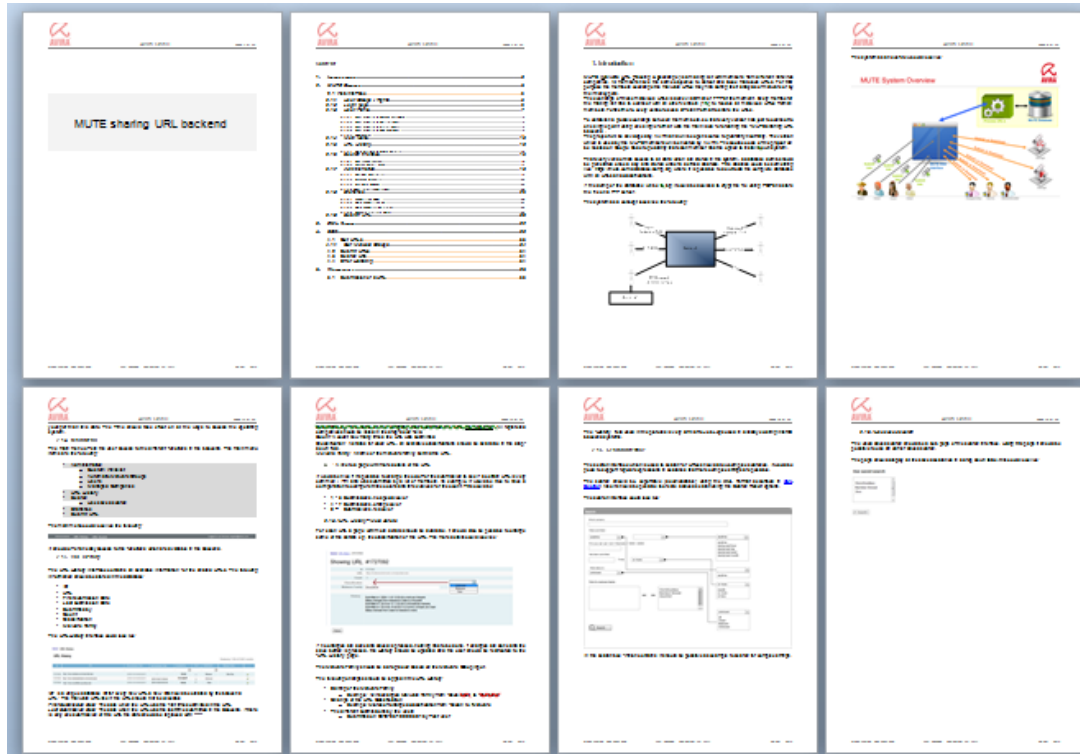
Requirements

The slide contains four panels:

- MUTE sharing URL backend:** A simple interface with a central text box.
- Configuration:** A list of system parameters and their values, such as 'MUTE_BACKEND', 'MUTE_FRONTEND', and 'MUTE_DATABASE'.
- Introduction:** A text block explaining the system's purpose and architecture, accompanied by a small diagram of a server and client.
- MUTE System Overview:** A diagram showing the system's components, including a central server, a database, and various client devices.



Requirements V0.2



+



Requirements V0.7

The grid contains 14 screenshots from a requirements document, organized into two rows of seven. The top row includes:

- 1. MUTE sharing URL backend: A table listing various URLs and their purposes.
- 2. MUTE System Overview: A diagram showing the system architecture with a central server and multiple client devices.
- 3. MUTE Kasten: A hierarchical tree diagram representing the system's structure.
- 4. MUTE Logging: A screenshot of a logging interface with a table of log entries.
- 5. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 6. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 7. MUTE System Overview (continued): A screenshot of a system overview page with a table.

 The bottom row includes:

- 8. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 9. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 10. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 11. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 12. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 13. MUTE System Overview (continued): A screenshot of a system overview page with a table.
- 14. MUTE System Overview (continued): A screenshot of a system overview page with a table.



+



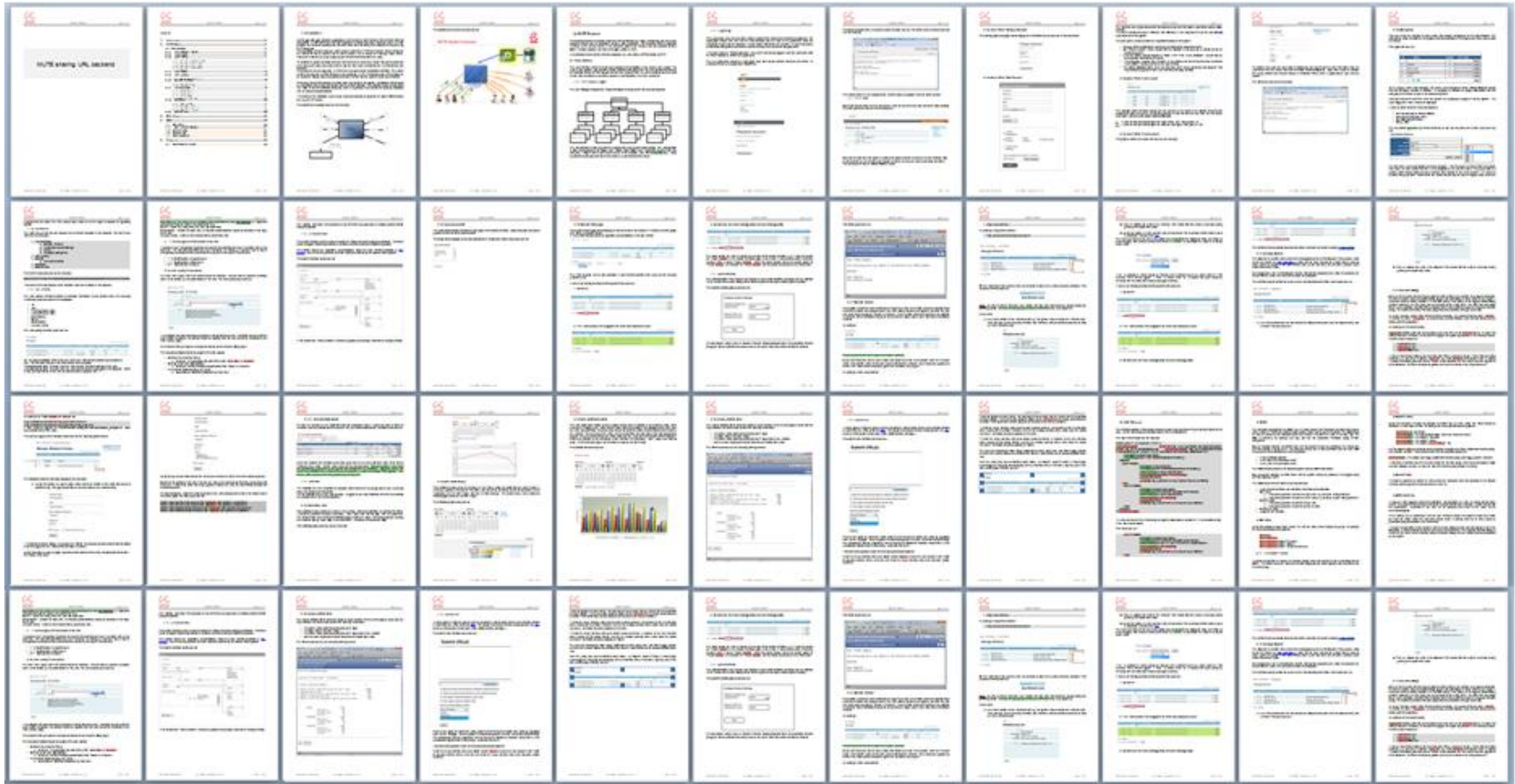
+



+



Requirements final(ly)



+



+



+



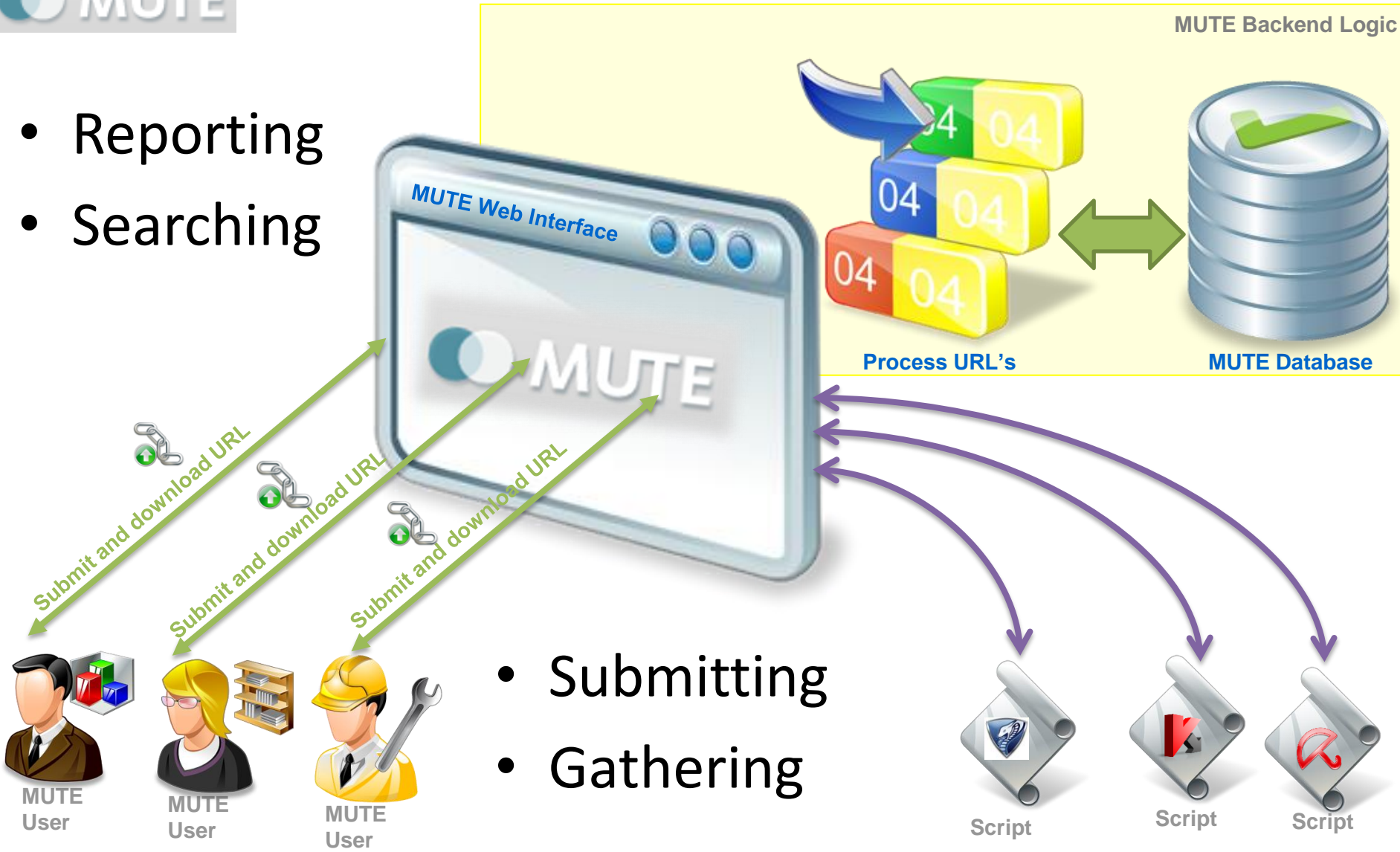
+



Development



- Reporting
- Searching



- Submitting
- Gathering

Submit URLs: using web interface

Submit URL(s)

New SubmissionMy SubmissionsAll 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

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

Classification

Malware Family



Submit URLs: using API

```

Administrator: C:\Windows\System32\cmd.exe

C:\malware"urls>mutec1 --operation=submit --url=https://mute.avira.com --user=
    @avira.com --pass=avira --file=submit.txt
0      Submission ok!
C:\malware"urls>_
    
```

```

malwareURLs.txt - Editor
Datei Bearbeiten Format Ansicht ?
http://www.luis-corrans-naked.com/who_wants_to_see_that.exe
http://dmitry.didnt-pay-the-bar-bill.com/file123.exe

http://74.91.22.206:88/tt/5.exe
http://hn.yigeyuming.com:82/hn.gif?t=.8638422
http://74.91.22.206:88/tt/35.exe
http://tabernaculodafedf.org.br/usuario/amxx.exe

Zelle 4, Spalte 32
    
```

C client

API available for **all languages**

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

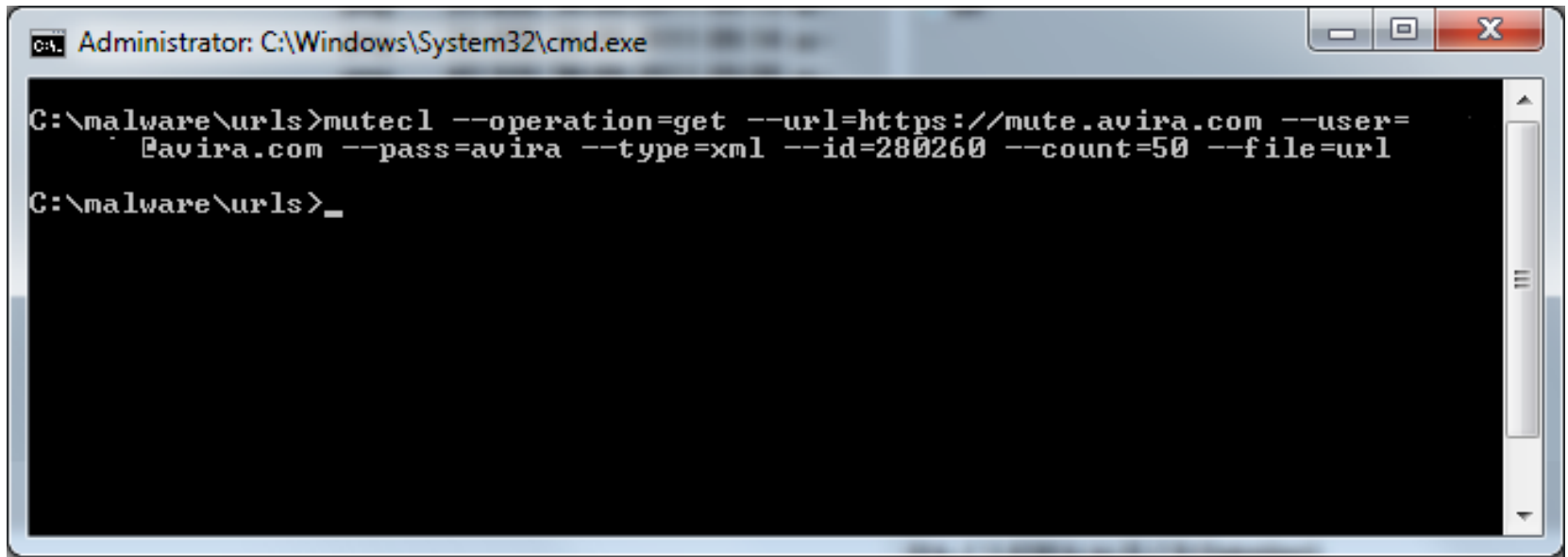
[← Back to list](#)

Submission Log

Displaying 21-40 of 509 result(s).

Id	Url	Status	New
279643	http://vwyjkeaqcfdj.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/pornorolik7.avi.exe	ok	-
279646	http://beautyxvidseff.tk/new/dog-doing-girl.avi.exe	ok	-
279647	http://bestdvddownload.com/New-Video-Addon.48563.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://bghhdjjedfwsfg.cz.cc/forum.php?tp=ba2f32cb3a6cd876	ok	✓
279651	http://freesexpornonew.info/1/video/pornorolik1.avi.exe	ok	-
-----	http://freesexpornonew.info/2/video/porno-	.	

Download URLs: using API



```
Administrator: C:\Windows\System32\cmd.exe
C:\malware\urls>mutec1 --operation=get --url=https://mute.avira.com --user=
Pavira.com --pass=avira --type=xml --id=280260 --count=50 --file=url
C:\malware\urls>_
```





```
<?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-alcapas.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>
```

Search for URLs

Url Search

[Search](#) [Load Last Results](#) [Url History](#)

 [Reload Last Search](#)  [Load Search](#)

Url Contains

Classification

Id

Belongs to any of the following malware families

- Koobface
- Zbot

Were Submitted

Count

Limit

 [Belongs to any malware family](#)

[Search](#)





Search for URLs

Search results:

[Search](#) [Load Last Results](#) [Url History](#)

[← Back to search](#) [NEW New search](#) [Save search](#)

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

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


View History for each URL





[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



Whitelist

Manage Whitelist Entries

Switch to Blacklist Add a new entry

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

Id	Url	Comment	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/> 2	avira.com/	AVIRA Antivirus	
<input type="checkbox"/> 4	microsoft.com/	Microsoft	
<input type="checkbox"/> 5	google.de/	Google Search Engine	

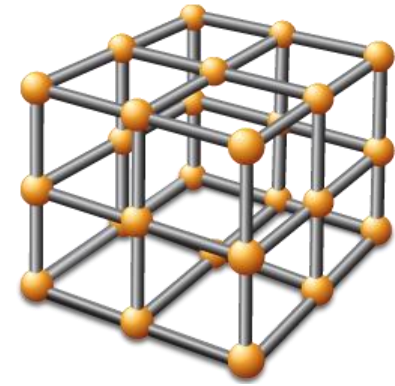
Select: all none

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>
```

Malware Families





MUTE Submit URLs Search Statistics Administration My Profile Logout

Manage Malware Families Users Companies Lists **Malware Families**

[+ Add a new malware family](#)

Displaying 1-2 of 2 result(s).

Id	Family Name	Automatic	URL Pattern	Enabled
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
1	Koobface	✓	<i>/.sys/?getexe=</i>	✓ 
2	Zbot	✓	<i>.bot.exe</i>	✓ 

RegEx



```

<?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>://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>

```



Statistics

Url Statistics

Statistic Type

New Urls Per Company

Group By

Day

Filter Providers

all

Start Date

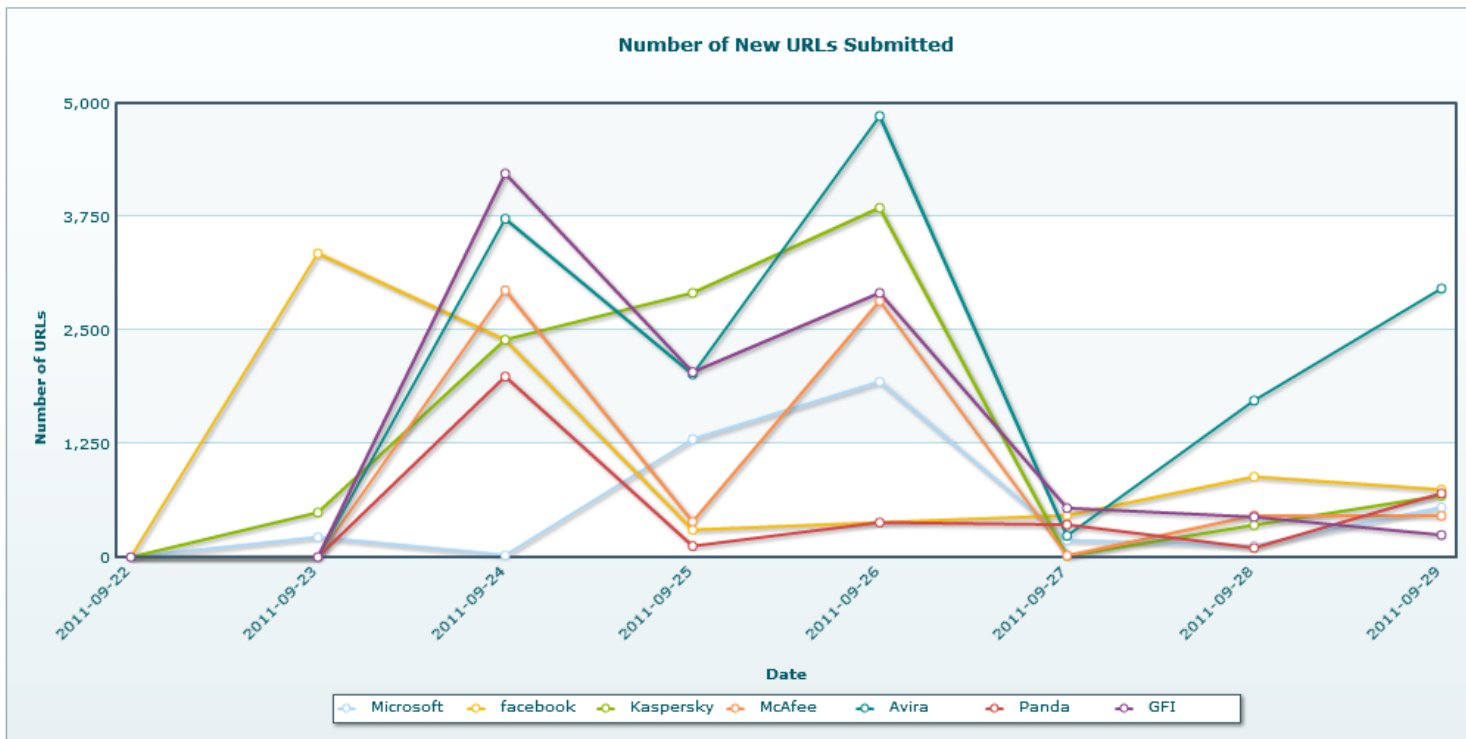
2011-09-22

yesterday last 7 days last 30 days

End Date

2011-09-29

Generate



Live Demo

Future Considerations



- Mute System
 - Get out of Beta in Jan. (launched Nov 1st, 2011)
 - Full IEEE data schema compatibility
 - Sharing meta-data such as clean file data
- Organization
 - Accept new members in Jan.
 - Release of organization charter and procedure.

Questions?

Malware URL Tracking and Exchange



One Beer – One Answer