RapidShare.com – The Phishing Begins

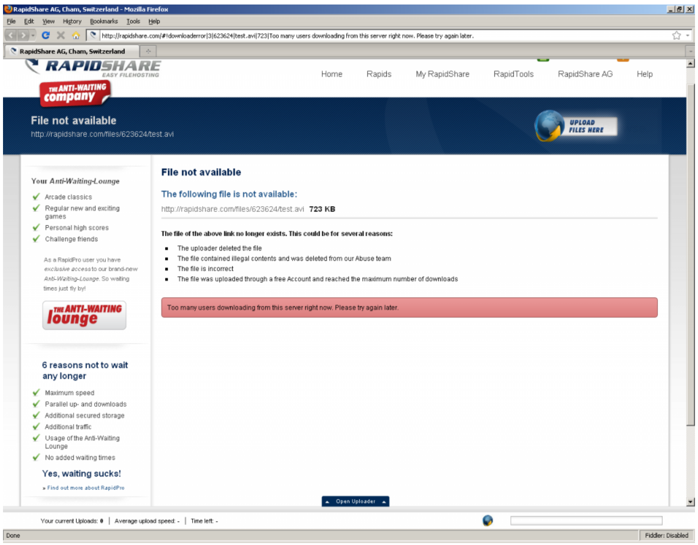
By Yaniv Miron • February 20th, 2011 • Phishing

A few weeks ago, M86 Security Labs discovered how to create a phishing page on RapidShare.com. As most of you probably know, RapidShare is one of the largest file sharing websites, with thousands of users worldwide.

While trying to download a file from RapidShare.com we encountered an error message indicating that the servers were busy.

We decided to test the error message and found that there is an improper input validation vulnerability in the “downloaderror” field.

Below is the original error message from RapidShare:



RapidShare AG, Cham, Switzerland - Mozilla Firefox

http://rapidshare.com/#!downloaderror|3|623624|test.avi|723|Too many users downloading from this server right now. Please try again later.

File not available
http://rapidshare.com/files/623624/test.avi

File not available

The following file is not available:

http://rapidshare.com/files/623624/test.avi 723 KB

The file of the above link no longer exists. This could be for several reasons:

- The uploader deleted the file
- The file contained illegal contents and was deleted from our Abuse team
- The file is incorrect
- The file was uploaded through a free Account and reached the maximum number of downloads

Too many users downloading from this server right now. Please try again later.

Your Anti-Waiting-Lounge
- ✓ Arcade classics
- ✓ Regular new and exciting games
- ✓ Personal high scores
- ✓ Challenge friends

As a RapidPro user you have *exclusive access* to our brand-new *Anti-Waiting-Lounge*. So waiting times just fly by!

6 reasons not to wait any longer
- ✓ Maximum speed
- ✓ Parallel up- and downloads
- ✓ Additional secured storage
- ✓ Additional traffic
- ✓ Usage of the Anti-Waiting Lounge
- ✓ No added waiting times

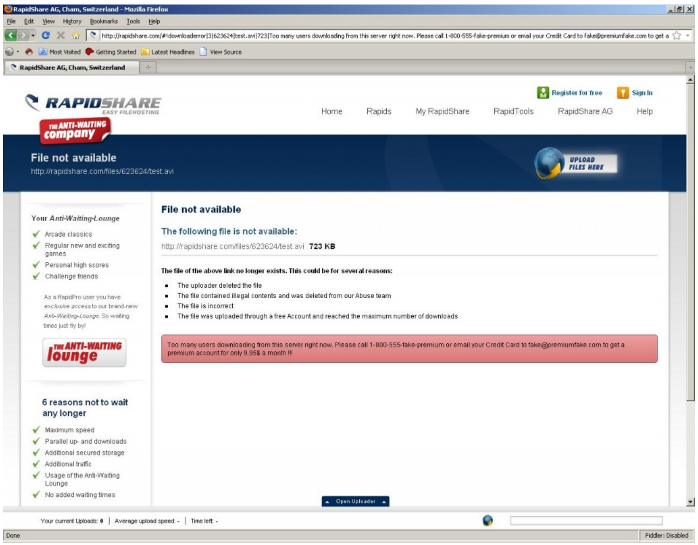
Yes, waiting sucks!

» Find out more about RapidPro

Your current Uploads: 0 | Average upload speed: - | Time left: -

RapidShare.com Error message – Too many users downloading…

In the following screen, we see a fake phishing message that offers users the opportunity to buy a premium account for RapidShare:



RapidShare AG, Cham, Switzerland - Mozilla Firefox

http://rapidshare.com/#!downloaderror|3|623624|test.avi|723|Too many users downloading from this server right now. Please call 1-800-555-fake-premium or email your Credit Card to fake@premiumfake.com to get a

File not available
http://rapidshare.com/files/623624/test.avi

File not available

The following file is not available:

http://rapidshare.com/files/623624/test.avi 723 KB

The file of the above link no longer exists. This could be for several reasons:

- The uploader deleted the file
- The file contained illegal contents and was deleted from our Abuse team
- The file is incorrect
- The file was uploaded through a free Account and reached the maximum number of downloads

Too many users downloading from this server right now. Please call 1-800-555-fake-premium or email your Credit Card to fake@premiumfake.com to get a premium account for only 9.95$ a month !!!

Your Anti-Waiting-Lounge
- ✓ Arcade classics
- ✓ Regular new and exciting games
- ✓ Personal high scores
- ✓ Challenge friends

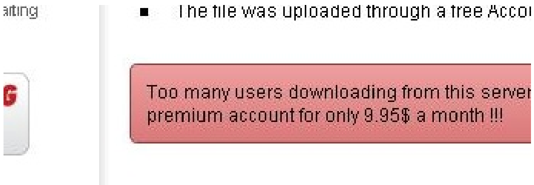
As a RapidPro user you have *exclusive access* to our brand-new *Anti-Waiting-Lounge*. So waiting times just fly by!

6 reasons not to wait any longer
- ✓ Maximum speed
- ✓ Parallel up- and downloads
- ✓ Additional secured storage
- ✓ Additional traffic
- ✓ Usage of the Anti-Waiting Lounge
- ✓ No added waiting times

Your current Uploads: 0 | Average upload speed: - | Time left: -

RapidShare.com Fake Error message

A closer look:



aiting

- The file was uploaded through a free Accou

Too many users downloading from this server
premium account for only 9.95$ a month !!!

Latest Blogs

M86 Security Labs now part of Trustwave’s SpiderLabs

The Cridex Trojan Targets 137 Financial Organizations in One Go

Cutwail Drives Spike in Malicious HTML Attachment Spam

M86 Security Threat Report for the Second Half of 2011 is Now Available

MIDI Files – Mid-Way to Infection

Categories

Botnets
Cybercrime
General
Malware
Phishing
Reports
Social Networking
Spam
Vulnerabilities

Archives

2012
2011
2010
2009
2008
2007
2006

For further information, see this demo link:

http://rapidshare.com/#!downloaderror|3|623624|test.avi|723|Too%20many%20users%20downloading%20from%20this%20server%20right%20now.%20Please%20call%201-800-555-fake-premium%20or%20email%20your%20Credit%20Card%20to%20fake@premiumfake.com%20to%20get%20a%20premium%20account%20for%20only%209.95$%20a%20month%20!!!

In addition, we can control all of the “downloaderror” fields. For example, the file folder (623624), the file name (test.avi), and of course the error message.

This type of improper input validation can help malicious attackers create phishing pages within RapidShare.com. A user that receives an email or a link to the malicious phishing page could unknowingly give away credit card information to the malicious attacker either by email or by a phone call.

We contacted RapidShare.com regarding this subject and received a response from the RapidShare Abuse team assuring us that they have fixed the issue.

Tags: Featured | Phishing | RapidShare | Social Engineering | Vulnerabilities

One Response to “RapidShare.com - The Phishing Begins”

Tweets that mention RapidShare.com, The phishing begins… « M86 Security Labs Blog -- Topsy.com says:
February 20, 2011 at 11:36 am

[…] This post was mentioned on Twitter by Fakhri Me and Christiaan Rakowski, joviann . joviann said: RapidShare.com, The phishing begins… http://bit.ly/hBXOLt | M86 Security Blog […]

Entries (RSS)