**List of Uploaded Malicious Files with IP Address on October 29, 2017**

91.200.12.22 - - [29/Oct/2017:09:29:35 -0400] "GET /wp-login.php HTTP/1.1" 200 3017 friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:36 -0400] "GET /wp-login.php HTTP/1.1" 200 3017 friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:37 -0400] "POST /wp-login.php HTTP/1.1" 302 - www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:38 -0400] "GET /wp-admin/ HTTP/1.1" 200 59095 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:39 -0400] "GET /wp-admin/ HTTP/1.1" 200 59095 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:40 -0400] "GET /wp-admin/theme-editor.php HTTP/1.1" 200 55923 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:41 -0400] "GET /wp-admin/theme-editor.php?file=cache%2Fb12193cc54edf932e43f04db1a287d04.php&theme=Minimal HTTP/1.1" 200 35649 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:42 -0400] "POST /wp-admin/theme-editor.php HTTP/1.1" 500 3305 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:43 -0400] "POST /wp-content/themes/Minimal/cache/b12193cc54edf932e43f04db1a287d04.php HTTP/1.1" 200 1510 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:44 -0400] "GET /wp-content/themes/Minimal/m0d.php HTTP/1.1" 404 24741 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:45 -0400] "GET /wp-admin/theme-editor.php HTTP/1.1" 200 55923 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:46 -0400] "GET /wp-admin/theme-editor.php?file=cache%2Fb12193cc54edf932e43f04db1a287d04.php&theme=Minimal HTTP/1.1" 200 35649 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:47 -0400] "POST /wp-admin/theme-editor.php HTTP/1.1" 302 - www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:47 -0400] "GET /theme-editor.php?file=cache/b12193cc54edf932e43f04db1a287d04.php&theme=Minimal&scrollto=0&updated=true HTTP/1.1" 404 24822 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:48 -0400] "POST /wp-content/themes// HTTP/1.1" 200 - www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:48 -0400] "GET /wp-content/themes//m0d.php HTTP/1.1" 301 - www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:49 -0400] "GET /wp-content/themes/m0d.php HTTP/1.1" 404 24731 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:50 -0400] "GET /wp-admin/plugin-install.php?tab=upload HTTP/1.1" 200 28782 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:51 -0400] "POST /wp-admin/update.php?action=upload-plugin HTTP/1.1" 200 23477 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:53 -0400] "GET /wp-content/uploads/2017/10/maink.php HTTP/1.1" 200 114 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:53 -0400] "POST /wp-content/uploads/2017/10/maink.php HTTP/1.1" 200 8488 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:54 -0400] "POST /wp-content/uploads/2017/10/maink.php HTTP/1.1" 200 16351 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:55 -0400] "POST /wp-content/uploads/2017/10/maink.php HTTP/1.1" 200 17030 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

91.200.12.22 - - [29/Oct/2017:09:29:56 -0400] "GET /wp-content/uploads/m0d.php HTTP/1.1" 200 120 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:15.0) Gecko/20121011 Firefox/15.0.1" "-"

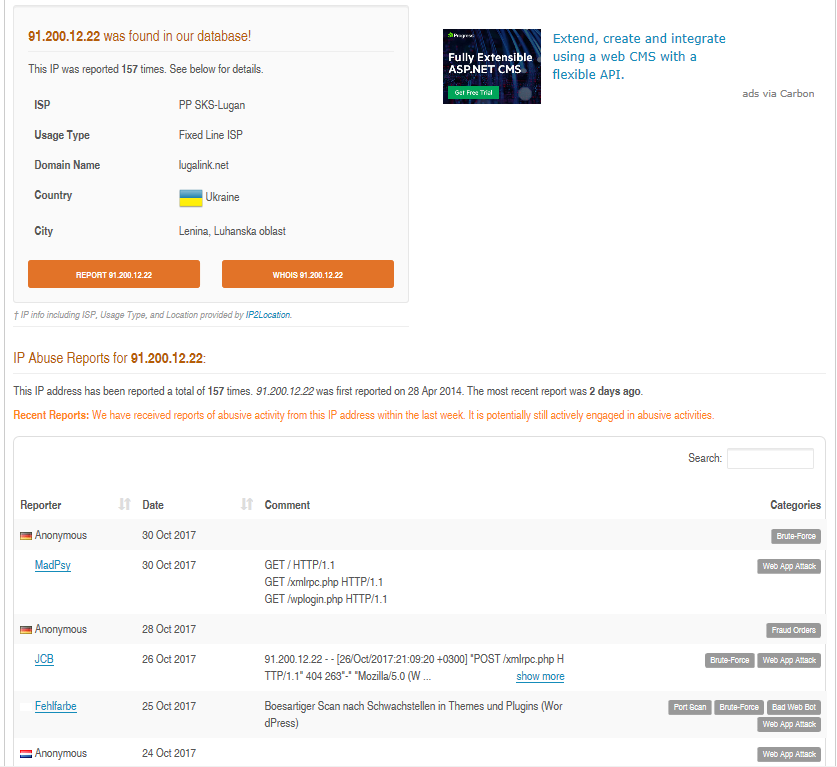
217.23.9.143 - - [29/Oct/2017:09:45:31 -0400] "POST /wp-content/uploads/m0d.php HTTP/1.1" 403 15 www.friendsofsmithgallwoods.org "http://www.friendsofsmithgallwoods.org/wp-content/uploads/m0d.php" "Opera/9.80 (Windows NT 6.1) Presto/2.12.388 Version/12.17 support.wordpress.com" "-"

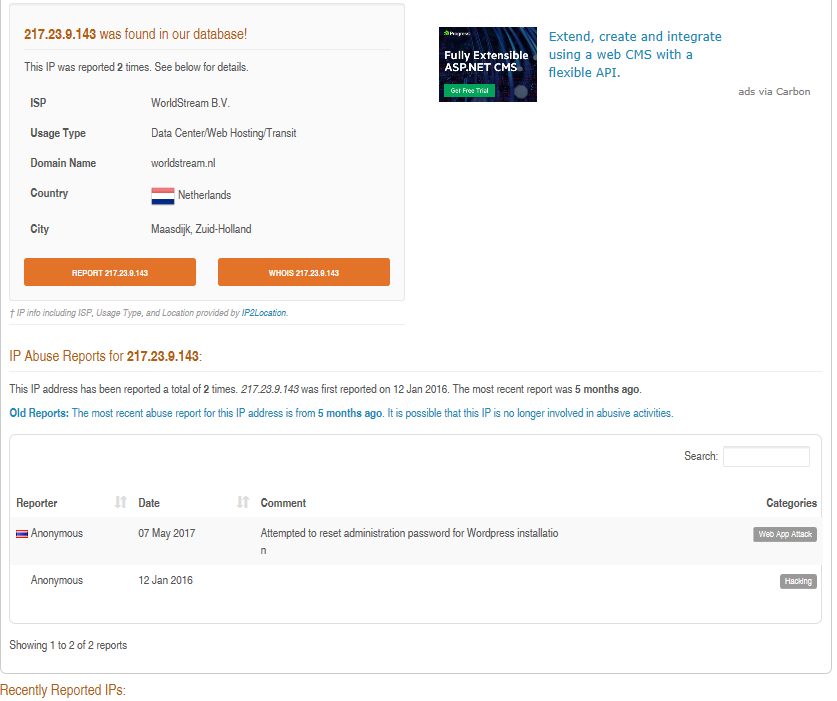
217.23.9.143 - - [29/Oct/2017:09:50:56 -0400] "GET /wp-content/uploads/m0d.php HTTP/1.1" 403 15 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0" "-"

217.23.9.143 - - [29/Oct/2017:09:50:56 -0400] "GET /favicon.ico HTTP/1.1" 200 4286 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0" "-"

217.23.9.143 - - [29/Oct/2017:09:50:56 -0400] "GET /favicon.ico HTTP/1.1" 200 4286 www.friendsofsmithgallwoods.org "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0" "-"

**More info on IP Addresses below……………**





**Code Inside Compromised Files**

Two existing files, wp-login.php and theme-editor.php, were changed.

In wp-login.php, line 784 was changed from this:

$user = wp\_signon( '', $secure\_cookie );

To this:

$user = wp\_signon( array(), $secure\_cookie );

In theme-editor.php, lines 159 through 162 were changed from this:

$description = get\_file\_description( $relative\_file );

$file\_show = array\_search( $file, array\_filter( $allowed\_files ) );

if ( $description != $file\_show )

$description .= ' <span>(' . $file\_show . ')</span>';

To this:

$file\_description = get\_file\_description( $relative\_file );

$file\_show = array\_search( $file, array\_filter( $allowed\_files ) );

$description = esc\_html( $file\_description );

if ( $file\_description != $file\_show ) {

$description .= ' <span>(' . esc\_html( $file\_show ) . ')</span>';

It appears that these changes allowed strings passed by the malicious code to be used to login and upload the b12193cc54edf932e43f04db1a287d04.php file to the Themes folder in the Friends web server, and then other files from there.