**Malicious JavaScript Analysis**

<http://virusshare.com/download.4n6?sample=6949636511564320bf80ce9cbc3bfbf26ef15cc70732f3ac7311c1203a6ec573>

-Analyzed, Malicious iframe

Description: The HTML file does not contain any JavaScript however it does contain an iframe that is loaded when the page is loaded. The size of the iframe is 1 pixel wide by 1 pixel high which is a good indicator that the user is not supposed to see it when the page is actually loaded. The iframe contains a URL of the page it is attempting to load and sure enough, after checking the site on VirusTotal and wepawet, the website is marked as malicious.

<http://virusshare.com/download.4n6?sample=4a86bb004b73aefef5c326e58bef862c87ef3bed9a1e84cae5a0a1223bebdffb>

-Analyzed, Malicious iframe

Description: The HTML file contains some JavaScript that loads up an iframe. The iframe is loaded inside of a heading tag which is kind of odd and may be there to hide its presence. The iframe contains a URL of the page it is attempting to load. After checking the site on VirusTotal and wepawet, the website is marked as malicious.

<http://virusshare.com/download.4n6?sample=8bb716c726527f901b9e6755a2c496fbaf47c573edde2cc775bcab33d09bf8f8>

-Analyzed, Malicious iframe

Description: The HTML file does contain some JavaScript however the malicious code is not in the JavaScript. The malicious code is in an iframe that is loaded when the page is loaded. The size of the iframe is 1 pixel wide by 1 pixel high which is a good indicator that the user is not supposed to see it when the page is actually loaded. The iframe contains a URL of the page it is attempting to load and sure enough, after checking the site on VirusTotal and wepawet, the website is marked as malicious.

<http://virusshare.com/download.4n6?sample=061b192b8486ab665230ed3a5a16ad390e8625ec7ea6bfad8ca62b5ff76b05b3>

-Analyzed, Malicious iframe

Description: The HTML file contains just Javascript code.  There are two different sections found, the first one is simply opening an iFrame on the page to a website (which was found to be malicious by using VirusTotal).  The second script tag is using a mild obfuscation technique in order to hide it’s purpose.  A bunch of seemingly random strings are being created and then appended together to be used as the source of a script being written onto the page.  Using simple re-formatting of the strings, it was discovered that the Javascript was adding a Russian JS script onto the page, which was also found to be malicious.

<http://virusshare.com/download.4n6?sample=60296e3740a93f5428c3fc9666c8ca8c423969da786492ea2c67b67caa33d224>

-Analyzed, Malicious iframe

Description: This HTML page belongs to that of a Flash application, as is evident by the HTML and JS code.  A self invoking anonymous function is placed in the Javascript, meaning it will automatically call itself.  This function works by creating a new iframe, setting its source to a Russian php script, and then placing it in the top left corner of the screen with a width and length of both 1px(making it invisible to the user on the page).  This script is most likely performing some malicious actions once it’s loaded onto the page, such as downloading malware or redirecting the user to some malicious website.

<http://virusshare.com/download.4n6?sample=283663cfa93948cd1730c2bf2b9bd25813c52ae57806c69b7cf691aa0c5050db>

-Analyzed, Redirection

Description: The Javascript in this HTML file is executing once the HTML page loads for the client.  It modifies the window.location property, meaning it redirects the client to another page.  To do its redirection, the Javascript uses the encodeuri and encodeuricomponent functions.  This modifies the strings being concatenated together so that any special characters inside of them(/, @, =) so that they are encoded using their hex value.  Finally, the resulting url that the client is being redirected to is a function of the URL that client was at before they arrived at this HTML page, along with the current url of the HTML page.

<http://virusshare.com/download.4n6?sample=b7f0456b5f81bc5f7ca87ed8fda91f162b2dfc80b636c5744c80cedaa2c66544>

-Analyzed, Malicious iframe

Description: The HTML content on this page suggests that it’s either an ad, or some legitimate page about a restaurant infected with malicious Javascript.  The Javascript on the page is mildly obfuscated, but is done using a scheme that is easily readable with some simple formatting of the code.  Upon closer inspection, the code is declaring many different variables which are simply strings of seemingly random characters.  Further down, the code is concatenating some of them together, and using the resulting strings to add/modify elements on the HTML page.  Simple re-formatting of the strings was done in order to discover the true functionality.  The script was found to be creating two iframes, setting their sources to different malicious sites, changing their width and length to both 1px(making it invisible on the page), and adding them to the HTML page.  The most reasonable guess of these unknown sites is that they both download malware on the victim’s machine after opening the iframes.

<http://virusshare.com/download.4n6?sample=3869da2843c0848d2d3e50e01742774334f382a3158400fdeeb66cbf7a725c46>

-Analyzed

Description: This HTML page is from a Russian site containing a lot of images and links to other sites.  Embedded in the page is a block of Javascript code, some of which is obfuscated.  The obfuscated code contains a large string that is being evaluated by a later function call. The string contains many hexadecimal values separated by the ! character.  Analyzing the code further, it was discovered that each hexadecimal value is being converted to its integer value, having 5 subtracted from it, and then converting to a char.  These chars were concatenated together to form the resulting Javascript.  Using a python script, the obfuscated code was de-obfuscated by reversing the method using to encode.  It was discovered that the obfuscated script being evaluated was creating an iframe on the page, setting it’s src to a Russian php script, and inserting it inside the document.