Reflow JavaScript Backdoor

kahusecurity.com/posts/reflow_javascript_backdoor.html

A script was left behind on a compromised machine. This led to the discovery of a Windows backdoor written in JavaScript and the C&C backend scripts. Unfortunately I can't post too much details because the victim's organization name is present in the files.

The backdoor script is less than 2KB and the only indication of its presence on a compromised PC is a running process called "wscript.exe", which is a legitimate Windows program. The main part of the script contains an endless do-loop awaiting commands after passing the query string "reflow" to the C&C else it sleeps for 4 hours.

The callback to the C&C looks like this:

I wanted to find out more so I searched for code snippets in various search engines and VirusTotal but that led me nowhere. I turned to Recorded Future and found exactly what I was looking for. In case you don't know Recorded Future (https://www.recordedfuture.com) helps to enrich your raw data with useful contextualized and correlated threat intelligence. What I like best is its ability to find things that search engines can't because it's been removed from paste sites or posted to a private forum, as examples.

The results I got show three hits to matching files that were deleted back in December 2017. The cached data and link back to the original source helped me recover a compressed file with the C&C package.

There are four main scripts (3 PHP and 1 JavaScript files) in the package that are copied to a web server. The web server may be attacker-controlled or compromised by some means. The main script, index.php, contains an SVG animation that looks like this when a visitor happens to visit the page.

This script shows that when "reflow" is passed to the page, contents of a malicious JavaScript file (renamed as a PNG file) is sent to the victim PC and eval'd by the backdoor script. The malicious script uses WMI to obtain the system Information then sends that info back as part of its authentication method.

Here you can see the malicious script running an endless loop waiting for commands such as upload, download, and execute.

The "mAuth" function generates short random strings, concatenates them along with the system info and passes that to the C&C in a cookie after Base64-encoding it. These random strings are important as they are used as markers to identify instructions contained between them.

Data is transmitted back to the C&C using AJAX. There's a function called "FillHeader" that populates the HTTP header.

Again, this is what the HTTP request looks like when the victim PC checks in:

Performing a Base64-decode on the cookie value results in the 2nd line. Repeating the Base64-decode on the string after the second caret reveals the system info.

One of the PHP scripts appears to be a template which is modified with HTML code to make the page look legitimate (e.g. it contain parts of an organization's actual webpage). The script is renamed and referenced by the index.php script. This script has all the functions responsible for uploading and downloading files as well as creating activity logs. Among the log files are victim's IP addresses, what files have been uploaded and downloaded, session information, etc.

The "Authentication" function reads in the cookie value from victims and parses out the system info, and defines variables used to create the log filenames. The victim's username and computer name are MD5-hashed and used as part of the log filenames. When a victim PC connects to the C&C, three files are created on the C&C server:

The last PHP script in their package is used to interact with and send commands to the victim PCs. Note the timezone and interesting login method.

The available commands are quite limited but is more than enough to upload additional, more powerful tools to the victim PC and gain further access into their network. And finally, if the attackers sense they are about to be discovered, they can delete all the important log files with another set of commands built into this script.

I don't have any attribution information on these scripts but it doesn't seem to be related to your-typical-crime-gang. It appears that this campaign is still ongoing as other files show updated timestamps.

Posted on: 03/30/2018