78 Psyme.nc malware

Silkut, Mon 01 Jun 2009

Psyme.nc malware

By Silkut

Foreword

To retain people's privacy I anonymized some names, which shouldn't make it more difficult to understand what follows:

- The website I am talking about is pointed out as http://website.com
- The forum is pointed out as website.com/forum/
- Its redirection is pointed out as http://redirection.com
- The first "iframed" website is pointed out as http://foo.address1.com/bar/
- The malicious file is pointed out as http://address2.com/tXlwpKDL/uCfIXrUcVpycMkVj.qtl

Intro

I discovered this malware on a reversing/cracking forum I used to go to. At this time, a freshly created thread by Guetta caught my eye. It was titled that his antivirus software (Kaspersky) detected a kind of Trojan downloader on a script while accessing the website using its redirection address.

Other people already started posting because while trying to catch it, it simply led to a 404 error (file not found). So I gave it a try.

I launched Firefox and Opera, deactivated JS, looked into the sourcecode, caught the url and gave it a shot. I got the same 404 error as everybody using Firefox, but not with Opera: I started from there.

Digging

From the source code of the redirected main page I noticed two JScript files. The first one, called "wbicm.js" (see .[0x01]), is obviously a fake, a modified version of the redirecting script.

Somehow the server hosting the script got hacked (sniffers, web vulnerabilities leading to shell upload etc...), after which this script was added a link to another JScript called "bskrf.js" (see .[0x02]).

The code is pretty short, but here starts the real deal: encrypted parts, some obscure variable name (vxnhnuse instantly caught my eyes).

Code

We got 3 escaped variables: SB, MR2 and MU2. All of them are obfuscated using the escape function. The role of the obfuscation is not to fool AVs, which are nowadays hopefully handling this little riddle, but to fool the reader if he doesn't pay enough attention to the code.

The first variable contains a link that was leading to http://foo.address1.com/bar/, now giving a 404 error by Apache (Web server). Notice the famous Iframe usage here, certainly malicious (see .[0x03]).

It also contains some escaped stuff carried by a variable named "PayLoadCode" (see .[0x04]), unquestionably a part of the exploit.

MR2 is the most interesting part of the code. It does some operations to properly store the payload using a stealthy way (memory rearrangment, zipped archive, randomized name, registry key to infect at startup).

It also connects to a website http://address2.com/tXlwpKDL/uCfIXrUcVpycMkVj.qtl, to download the file named "uCfIXrUcVpycMkVj.qtl". After that it runs a shell and eventually executes the randomly named binary file (see .[0x04] and .0x05).

To conclude, MU2 tries its way through the WScript system, an XML document and an ADODB stream object.

Vulnerabilities

The QTL file obviously contains some harmful code, which is now unavailable. At the time this trojan downloader was caught, Trojan downloader authors were fond of QuickTime vulnerabilities.

The QTL is a media file with the MIME types application/x-quicktimeplayer and video/x-quicktimeplayer. A quick search pulled out this: http://projects.info-pull.com/moab/MOAB-01-01-2007.html which let us know about its behaviour: "an attacker could overflow a stack-based buffer [...] leading to an exploitable remote arbitrary code execution condition."

Conclusion

This was my first paper about this kind of malware, but something tells me this is not the last case I stumble upon...

Thanks

Greetings to Guetta who spotted this shit, additional hellos to DiamonDie.

Silkut