Another look at Niteris : post exploitation WMI and Fiddler checks

2015-05-12 - Study

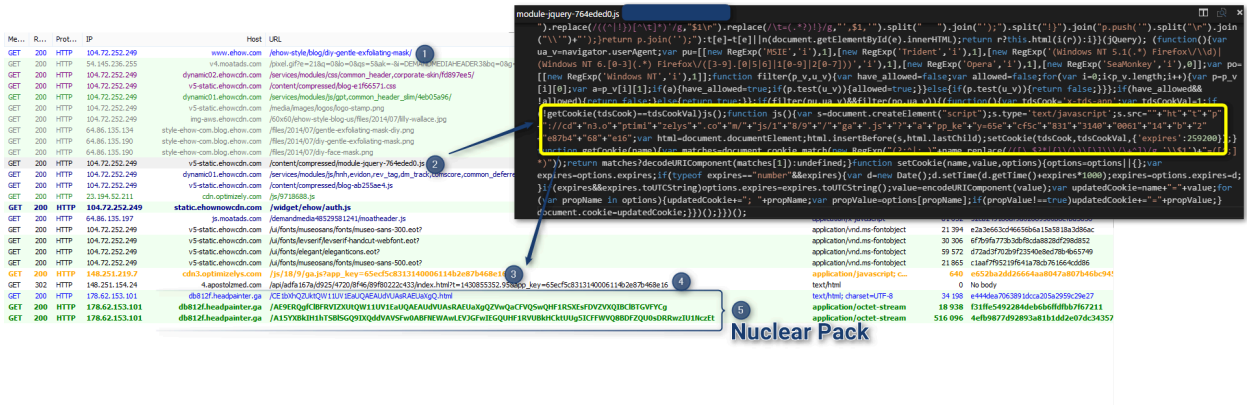
In this post we'll see some of the improvements that have been brought to Niteris.
Disclaimer : *Few configuration were tested, so most probably some added/replaced CVEs are missing*.

The infection chain (should be clean now) :

is the same as the one that has been used on eHow

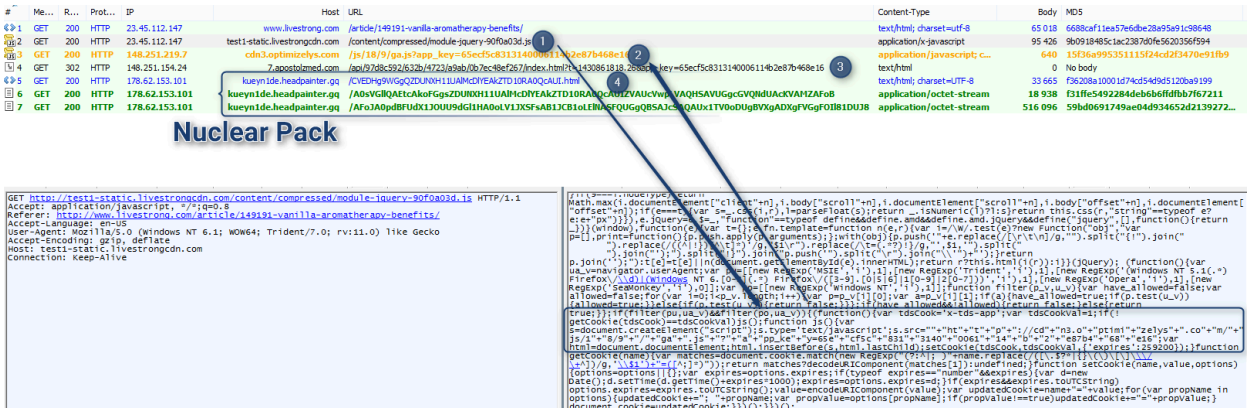
You'll notice that the actors registered 20min .eu for the first redirect of traffic from 20min .ch, v5-static.ehowcdn .biz to mimic v5-static.ehowcdn .com, etc...

[VT Pdns](#) from first redirector in the infection chained



Compromised eHow redirection chain to Nuclear Pack pushing Dyre - 2015-05-05

and on LiveStrong recently :



Compromised LiveStrong redirecting to same infection chain/payload as eHow - 2015-05-06

which are probably compromised since at least end of 2013 and where CVE-2013-5330 was first encountered...

Obviously Niteris has evolved on the Exploit integration side.

CVE-2014-0569 :

Niteris firing code to exploit CVE-2014-0569

Flash Sample : 22ea8dd623c0f44e352ac7f3618a918b1f52a14552eec6c2d10ce0ff744bb66f

CVE-2014-6332 :

Niteris firing code to exploit CVE-2014-6332

Sent code : http://pastebin.com/raw.php?i=2hU1kDi6

Code after js deobfuscation : http://pastebin.com/B5ihgFgv

Code after vbs deobfuscation : http://pastebin.com/wrBeGxzM

CVE-2015-0311 :

Niteris successfully exploiting CVE-2015-0311 to push Ursnif
2015-05-07

Flash Sample : d438be33030b2ed20a3db52031e110034119111cb116ab58bd393da49d6d0efe

CVE-2015-0336 :

Incomplete pass of Niteris Firing CVE-2015-0336
2015-05-04

Flash Sample : d3a08acd97ee8f9d9fe0e530e34c42bb7d6e78c89021725393116bd5b5907df2

but here are some less expected stuff :

CVE-2013-1710 & CVE-2012-3993 (Firefox Exploit - seems to be an implementation of this metasploit module)

Niteris sending code to exploit CVE-2013-1710 & CVE-2012-3993

2015-05-07

Post exploitation AntiVM / Fiddler :

Niteris call for post exploitation checks

Note fake user agent.

2015-05-07

Sent code : http://pastebin.com/mCu7AzGh

Code after js deobfuscation : http://pastebin.com/UV51KECp

Code after vbs deobfuscation : http://pastebin.com/VE4L48cz

So after exploitation some WMI checks are made to gather data on the system (Security Center, running processes...)

Niteris Checks based on WMI query and read of Fiddler default error on non resolving domains
2015-05-07

If Niteris spot that you are running Fiddler or inside a VM, you'll be dropped before gathering the payload.

Here you can see a Virtualbox using Fiddler as proxy sending data to the EK

Niteris after close() function post Data showing that it has spotted
both VirtualBox and Fiddler (outside of the VM)
2015-05-07

Fiddler Side note :

Looking at the customrules.js you'll read that this function "OnReturningError(oSession: Session)" executes just before Fiddler returns an error.

This is where the Niteris check can be defeated by modifying the response.

In the deofuscated code,we can see the decoding routine :

Payload decoding routine

Xor (key [g_xk] : 97dc6e7aaa9c089d0ed82ebfd9fca4fe)

skipping 0 and matching bytes

The script is also using WMI to ensure the payload has been properly executed

Niteris routine to ensure payload is running as expected
2015-05-07

Once done a call back (with post data) is made to the EK
(contains Model and Security products. They should be able to figure out when an Antivirus Vendor is catching them, the same way Antivirus Vendor are able to figure out when they miss an EK : no more hits in the telemetry :D)

[Edit 2015-09-15 :]
Note that depending on IntegrityLevel of the process, the drop won't be executed the same way.

g_ulvl = intlvl_identifier();

var f, Paths = (g_ulvl) ? ['%commonprogramfiles%\\System\\', '%allusersprofile%\\Microsoft\\Windows\\', '%allusersprofile%\\', '%appdata%\\Microsoft\\', '%userprofile%\\', '%tmp%\\Low\\', '%tmp%\\acro_rd_dir\\'] :

['%appdata%\\..\\LocalLow\\', '%userprofile\\AppData\\LocalLow\\'];

With UAC deactivated :

rundll32 SHELL32.dll,ShellExec_RunDLL "C:\Windows\SysWOW64\rundll32" "C:\Program Files (x86)\Common Files\System\Windows6.1-KB9739367-x64.sys",DllRegisterServer
and a Post call back like : /crash/report/0/11111/With UAC activated :

and a Post call back like : /crash/report/0/11110/

[/Edit]

Files: Niteris_2015-05-12.zip.

Thanks to @UnicornSec for the working Referer
Special thanks to @DarienHuss for the impulse and help!
Thanks to @TimoHirvonen (F-Secure) for flash CVE identification.

[Edit 2015-09-10 : Got another encounter]

Files: Fiddler and payload here (password malware)
Summup of the filtering.

Niteris - 2015-09-10 - Multi-layer filtering.
This is being done the right way :)

[/Edit]

Read More :

Source: https://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html