Didier Stevens

Monday 16 March 2015

Quickpost: Metasploit User Agent Strings

Filed under: Quickpost — Didier Stevens @ 0:00

I searched through the Metasploit source code for User Agent Strings (starting with Mozilla/).

This is what I found:

```
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0; SIMBAR={7DB0F6DE-8DE7-4841-9084-28FA914B0F2E}; SLCC1; .N
Mozilla/4.0 (compatible; Metasploit RSPEC)
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/4.0.221.6 Safari/525.13
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
```

Quickpost info

Share this:

Facebook X

Related

Detecting Network Traffic from Metasploit's Meterpreter Reverse HTTP Module
Monday 11 May 2015
In "Networking"

Sampling a Malicious Site
Sunday 10 August 2008
In "Malware"

Quickpost: Retrieving Malware Via Tor On Windows
Sunday 21 January 2018
In "Malware"

Comments (7)

7 Comments »

1. Are lines 5 and 7 truncated?

   Comment by Drew Hunt — Monday 16 March 2015 @ 14:11

2. Here are my finds for comparison:

   Mozilla/4.0 (compatible)
   Mozilla/4.0 (compatible; BullsEye; Windows 95)
   Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
   Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\
   Mozilla/5.0
   Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
   Mozilla/5.0 (compatible; MSIE 10.6; Windows NT 6.1; Trident/5.0; InfoPath.2; SLCC1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 2.0.50727) 3gpp-gba UNTRUSTED/1.0
   Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
   Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
   Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3
   Mozilla/5.0 (iPhone; CPU iPhone OS 614 like Mac OS X) AppleWebKit/536.26 (KHTML like Gecko) Version/6.0 Mobile/10B350 Safari/8536.25
   Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.3 Safari/534.53.10
   Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.75 Safari/537.1\

Pages

- About
- Didier Stevens Suite
- Links
- My Python Templates
- My Software
- Professional
- Programs
  - Ariad
  - Authenticode Tools
  - Binary Tools
  - CASToggle
  - Cobalt Strike Tools
  - Disitool
  - EICARgen
  - ExtractScripts
  - FileGen
  - FileScanner
  - HeapLocker
  - MyJSON Tools
  - Network Appliance Forensic Toolkit
  - Nokia Time Lapse Photography
  - oledump.py
  - OllyStepNSearch
  - PDF Tools
  - Shellcode
  - SpiderMonkey
  - Translate
  - USBVirusScan
  - UserAssist
  - VirusTotal Tools
  - XORSearch & XORStrings
  - YARA Rules
  - ZIPEncryptFTP
- Public Drafts
  - Cisco Tricks
- Screencasts & Videos

Search

Top Posts

- PDF Tools
- oledump.py
- My Software
- Didier Stevens Suite
- Test File: PDF With Embedded DOC Dropping EICAR

Categories

- .NET
- 010 Editor
- Announcement
- Arduino
- Bash Bunny
- Beta
- bpmtk
- Certification
- Didier Stevens Labs
- Eee PC
- Elec

Comment Subscribe •••

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:15.0) Gecko/20100101 Firefox/15.0\
Mozilla/5.0 (Macintosh; Intel Mac OS X 1084) AppleWebKit/536.30.1 (KHTML like Gecko) Version/6.0.5 Safari/536.30.1
Mozilla/5.0 (Macintosh; Intel Mac OS X 1084) AppleWebKit/537.22 (KHTML like Gecko) Chrome/25.0.1364.99 Safari/537.22
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.99 Safari/533.4
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:23.0) Gecko/20131011 Firefox/23.0
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0\
Mozilla/5.0 (X11; U; Linux i686; pl-PL; rv:1.9.0.2) Gecko/20121223 Ubuntu/9.25 (jaunty) Firefox/3.8

Comment by Drew Hunt — Monday 16 March 2015 @ 14:30

3. @Drew No, these lines are not truncated. This is what I found in the source code:

   OptString.new(‘UserAgent’, [true, “The HTTP User-Agent sent in the request”, ‘Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0; SIMBAR={7DB0F6DE-8DE7-4841-9084-28FA914B0F2E}; SLCC1; .N’])

   header = { ‘User-Agent’ => “Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/4.0.221.6 Safari/525.13”}

   Comment by Didier Stevens — Monday 16 March 2015 @ 14:43

4. @Drew There are many User Agent Strings found in the comments of the Metasploit source code. I did not include these, and that explains why you find so many.
   I used the following regex: ([“‘])Mozilla/.+\1

   Comment by Didier Stevens — Monday 16 March 2015 @ 14:45

5. Interesting. I’m not able to find the ‘SIMBAR’ UAS to validate. What module is it from?. It looks to be a cut-off .NET string. That would be an intersting anomaly to search for.

   WRT searching, I believe the bulk of the UAS I located were in the included Ruby libraries, not Metasploit itself.

```
root@host1:/opt/metasploit# cat /tmp/ua1 | awk -F: ‘{print $1}’ | sort | uniq -c | sort -nr
8 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-1.1.1/spec/lib/secure_headers_spec.rb
5 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-
1.1.1/spec/lib/secure_headers/headers/content_security_policy_spec.rb
4 apps/pro/ui/db/runners/se_reporting_seed_objects.rb
2 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-
1.1.1/fixtures/rails_3_2_12/spec/controllers/things_controller_spec.rb
2 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-
1.1.1/fixtures/rails_3_2_12/spec/controllers/other_things_controller_spec.rb
2 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-
1.1.1/fixtures/rails_3_2_12_no_init/spec/controllers/things_controller_spec.rb
2 apps/pro/vendor/bundle/ruby/1.9.1/gems/secure_headers-
1.1.1/fixtures/rails_3_2_12_no_init/spec/controllers/other_things_controller_spec.rb
2 apps/pro/vendor/bundle/ruby/1.9.1/gems/rack-1.4.5/test/spec_request.rb
1 apps/pro/vendor/bundle/ruby/1.9.1/gems/robots-0.10.1/test/fixtures/eventbrite.txt
1 apps/pro/ui/app/models/websploit_task.rb
1 apps/pro/ui/app/models/webscan_task.rb
1 apps/pro/ui/app/models/webaudit_task.rb
1 apps/pro/ui/app/models/social_engineering/web_page.rb
1 apps/pro/ui/app/models/scan_task.rb
1 apps/pro/ui/app/models/exploit_task.rb
1 apps/pro/engine/spec/modules/auxiliary/pro/social_engineering/web_phish_spec.rb
1 apps/pro/engine/lib/pro/dynamic_stagers/templates/reverse_http_svc.c.template
1 apps/pro/engine/lib/pro/dynamic_stagers/templates/reverse_http.c.template
```

   Eliminating the Ruby spec strings, the list is reduced, but still not matched to yours. Then again, I’m searching the Kali packaged installation and not the source code.

```
root@host1:/opt/metasploit# fgrep -r Mozilla/ * | fgrep -v access.log | fgrep -v “vendor/bundle” | tee
/tmp/ua1.1 | perl -pe ‘s/^(.*)\”(Mozilla\/[^\”]+)\”(.*)$/$2/;’ | perl -pe
“s/^(.*)\'(Mozilla\/[^\’]+)\'(.*)$/$2/;” | perl -pe ‘s/^(.*)\s(Mozilla\/.*)$/$2/;’ | perl -pe ‘s/^\s*$//’|
sort | uniq | tee /tmp/ua2.1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\
Mozilla/5.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
```

- Fellow Bloggers
- Forensics
- Hacking
- Hardware
- maldoc
- Malware
- My Software
- N800
- Networking
- Nonsense
- nslu2
- OSX
- PDF
- Personal
- Physical Security
- Poll
- Puzzle
- Quickpost
- Release
- Reverse Engineering
- RFID
- Shellcode
- smart card
- Spam
- technology
- UltraEdit
- Uncategorized
- Update
- video
- Vulnerabilities
- WiFi
- Windows 7
- Windows 8
- Windows Vista
- Wireshark

Blog Stats

- 7,687,892 hits

Twitter @DidierStevens

Posts from @DidierStevens

Nothing to see here - yet

When they post, their posts will show up here.

View on X

Archives

- October 2024
- September 2024
- August 2024

Comment Subscribe •••

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.75 Safari/537.1\
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:15.0) Gecko/20100101 Firefox/15.0\
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0\

Interesting findings. Thanks for the post!

Comment by Drew Hunt — Monday 16 March 2015 @ 15:08

6. @Drew Indeed, it is a truncated .NET CLR string, and makes it easy to spot. I found it here: metasploit-framework-master\modules\exploits\windows\http\hp_nnm_ovas.rb line 90.

   Comment by Didier Stevens — Monday 16 March 2015 @ 15:26

7. […] on the Metasploit User Agent Strings I published a couple of months ago, I made these Snort […]

   Pingback by Detecting Network Traffic from Metasploit’s Meterpreter Reverse HTTP Module | Didier Stevens — Monday 11 May 2015 @ 5:52

RSS feed for comments on this post. TrackBack URI

Leave a Reply (comments are moderated)

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Blog at WordPress.com.

- May 2024
- April 2024
- March 2024
- December 2023
- November 2023
- October 2023
- September 2023
- August 2023
- July 2023
- June 2023
- May 2023
- April 2023
- March 2023
- February 2023
- January 2023
- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- November 2021
- October 2021
- September 2021
- August 2021
- July 2021
- June 2021
- May 2021
- April 2021
- March 2021
- February 2021
- January 2021
- December 2020
- November 2020
- October 2020
- September 2020
- August 2020
- July 2020
- June 2020
- May 2020
- April 2020
- March 2020
- February 2020
- January 2020
- December 2019
- November 2019
- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019
- March 2019
- February 2019
- January 2019
- December 2018
- November 2018
- October 2018
- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018
- February 2018
- January 2018
- December 2017

Comment Subscribe •••

- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016
- May 2016
- April 2016
- March 2016
- February 2016
- January 2016
- December 2015
- November 2015
- October 2015
- September 2015
- August 2015
- July 2015
- June 2015
- May 2015
- April 2015
- March 2015
- February 2015
- January 2015
- December 2014
- November 2014
- October 2014
- September 2014
- August 2014
- July 2014
- June 2014
- May 2014
- April 2014
- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013
- July 2013
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011

Comment Subscribe •••

- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009
- December 2008
- November 2008
- October 2008
- September 2008
- August 2008
- July 2008
- June 2008
- May 2008
- April 2008
- March 2008
- February 2008
- January 2008
- December 2007
- November 2007
- October 2007
- September 2007
- August 2007
- July 2007
- June 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007
- December 2006
- November 2006
- October 2006
- September 2006
- August 2006
- July 2006
- June 2006

March 2015

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

« Feb Apr »

Comment Subscribe •••