



www.fidelissecurity.com  
www.threatgeek.com  
@FidSecSys  
+1 800.652.4020

Fidelis Threat Advisory #1004

## USERAGENT STRINGS

September 30, 2011

Document Status: FINAL  
Last Revised: 2011-09-30

### Executive Summary

User-Agent (UA) strings are used in HTTP(S) sessions to identify the capabilities of the client to a web server. Normally this string identifies the browser version, operating system and applicable plugins such as Adobe Flash or Java. However, some types of malware use the UA string as a covert channel for command and control (C&C). Anomalous UA strings can thus be a post-infection indicator. As the use of the UA string requires no protocol malformations and as there is no formal standard for the content or format of a UA string, its use as a C&C channel is difficult to detect and thus bypasses most security devices.

### Threat Overview

The normal purpose of the UA string is to identify the capabilities of a web client to a web server. This typically includes details of the browser's rendering engine, the user's operating system and any applicable plugins such as the .NET Framework, Adobe Flash, Silverlight or Java. This information can be used by web servers to tailor content for a specific client. For example, if a web server detects that a browser is not Internet Explorer then it knows that ActiveX controls will not function and can provide a page free of ActiveX (or tell the client that it does not meet the requirements to view the page). Certain varieties of malware, such as the GRUM spam bot or the FunWebProducts adware toolbar modify the UA string on hosts they infect. In the case of GRUM, it uses the UA string as a covert channel for outbound C&C activity. Since most users don't know what a UA string is, and since it's transmitted to web servers unbeknownst to them, and since most security devices do not inspect the UA string, this type of malicious activity can often fly under the radar.

### Risk Assessment

The use of UA strings for C&C is indicative of an infection already present within an enterprise network. The risk is therefore equivalent to that posed by any form of covert C&C. It indicates that malware might be spreading throughout the network or that data exfiltration might be in progress.

Users are granted permission to copy and/or distribute this document in its original electronic form and print copies for personal use. This document cannot be modified or converted to any other electronic or machine-readable form in whole or in part without prior written approval of Fidelis Security Systems, Inc.

While we have done our best to ensure that the material found in this document is accurate, Fidelis Security Systems, Inc. makes no guarantee that the information contained herein is error free.



www.fidelissecurity.com  
www.threatgeek.com  
@FidSecSys  
+1 800.652.4020

The GRUM spam bot is a well-known malware that uses UA strings for C&C. Its presence could mean that enterprise mail servers are being used to deliver spam, which could lead to blacklisting, having important outbound emails being blocked by spam filters, and/or loss of reputation.

### **Indicators & Mitigation Strategies**

Most enterprises have a standard desktop image for their non-privileged users with the same operating system, browser and versions of .NET, Flash and Java. This means that across an entire enterprise the number of unique UA strings should be manageable. Any client that does not match one of the approved UA strings constitutes an anomaly worthy of investigation: the host might be infected with a particular malware or adware or may be using a version of software that is not approved. Privileged users such as IT or software developers tend to use a wider array of software and thus UA profiling might be more difficult for them, but anomalous elements such as names of adware toolbars or C&C commands will still stand out. For a list of common UA strings, consult the “Further Reading” section.

### **The Fidelis Take**

Fidelis XPS sensors can inspect UA strings on all outbound HTTP traffic, or—with the use of Fidelis SSL Inspector—all HTTPS traffic as well. Sensors have built-in rules to look for certain anomalous characters in UA strings and it is easy to import a whitelist of acceptable UAs and look for deviations.

### **Further Reading**

- Intrepidus Group, “Identifying Malware via User-Agent Headers”, Benn, 6/16/10. <http://goo.gl/YtSib>
- List of User-Agents, <http://www.user-agents.org/>
- Fidelis Security Systems, “Fidelis XPS Policy Pack (July 2011).” <http://fidelissecurity.com/support>