Java-based malware driving DDoS botnet infects Windows, Mac, Linux devices

By *Rianne Schestowitz*
Created *29/01/2014 - 4:43pm*
Submitted by Rianne Schestowitz on Wednesday 29th of January 2014 04:43:48 PM Filed under Software [1] Security [2]

The cross-platform HEUR:Backdoor.Java.Agent.a, as reported in a blog post published Tuesday by Kaspersky Lab, takes hold of computers by exploiting CVE-2013-2465, a critical Java vulnerability that Oracle patched in June. The security bug is present on Java 7 u21 and earlier. Once the bot has infected a computer, it copies itself to the autostart directory of its respective platform to ensure it runs whenever the machine is turned on. Compromised computers then report to an Internet relay chat channel that acts as a command and control server.

Read more [3]

Software Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/38
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] http://arstechnica.com/security/2014/01/java-based-malware-driving-ddos-botnet-infects-windows-mac-linux-devices/