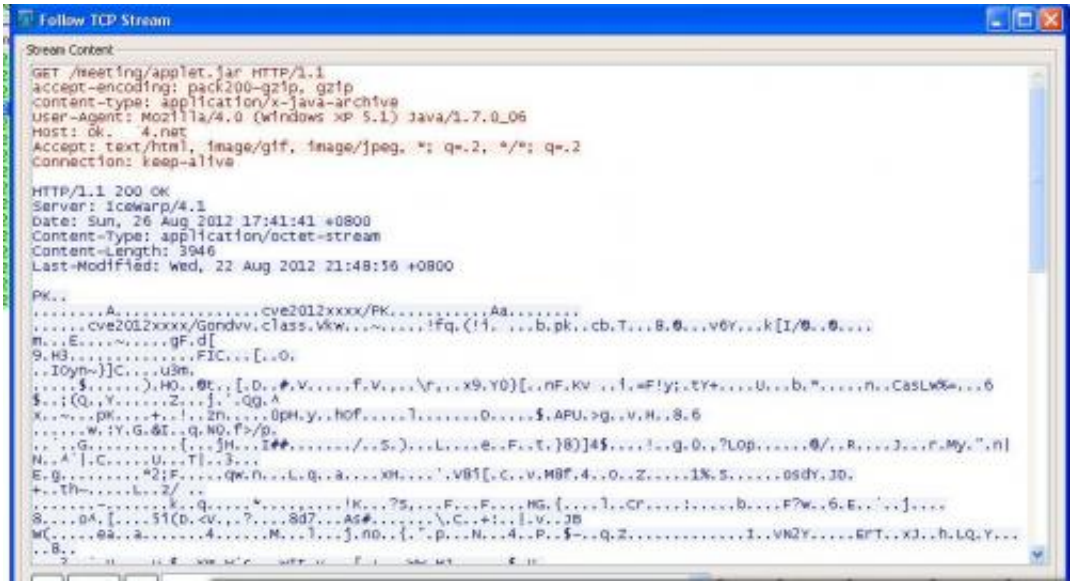
Latest Java poison romps on as ok.XXX4.net

August 28 2012, by Nancy Owano



(Phys.org)—Yet another Java-related computer threat, cross-platform, has been nailed by security researchers. An exploit was seen by FireEye researchers on Sunday, being hosted on a domain ok.XXX4.net. When successful, the exploit downloads and executes a malicious binary, which calls to another IP address/domain. The Java threat was reported by FireEye's security researcher Atif Mushtaq, who said on August 26 that the initial exploit "is hosted on a domain named ok.XXX4.net. Currently this domain is resolving to an IP address in China." Subsequent reports are that it was discovered on a server with a domain name that resolved to an IP address located in China, and that the malware once installed on

systems attempted to connect to a command-and-control server believed to be in Singapore.

Numerous security watchers are calling this a worrying vulnerability in the latest version of Oracle's Java software framework, which could get worse. The attackers have found a way to get at a vulnerability that affects the latest version of Java—Update 6—in order to infect computers with malware. More specifically, the exploit affects Java 1.7 update 6.

Most recent Java run-time environments are vulnerable, added Mushtiuqe. "In my lab environment, I was able to successfully exploit my test machine against latest version of FireFox with JRE version 1.7 update 6 installed," he said.

Security experts warn that the exploit code works on several browsers and computer platforms. Once the initial attack is made, a second piece of software referred to as Poison Ivy is released that lets hackers gain control of the computer.

Numerous computer security firms are telling PC users to disable Java software until a patch is released. As of this writing, there was no patch from Oracle.

Oracle typically patches Java at given points throughout the year. The next patch is scheduled for October. The updates are supposed to be collections of security fixes for Oracle products. Oracle says on its site, however, that "Oracle will issue Security Alerts for vulnerability fixes deemed too critical to wait for distribution in the next Critical Patch Update."

As such, Java is gaining a dubious distinction as being not only globally ever-present but also among the apps most frequently exploited, taking

its place on the throne alongside Adobe Reader and Flash. According to Oracle, 97% of enterprise desktops run Java. Under different circumstances, that factoid would sound far less menacing.

More information: blog.fireeye.com/research/2012 … is-not-over-yet.html