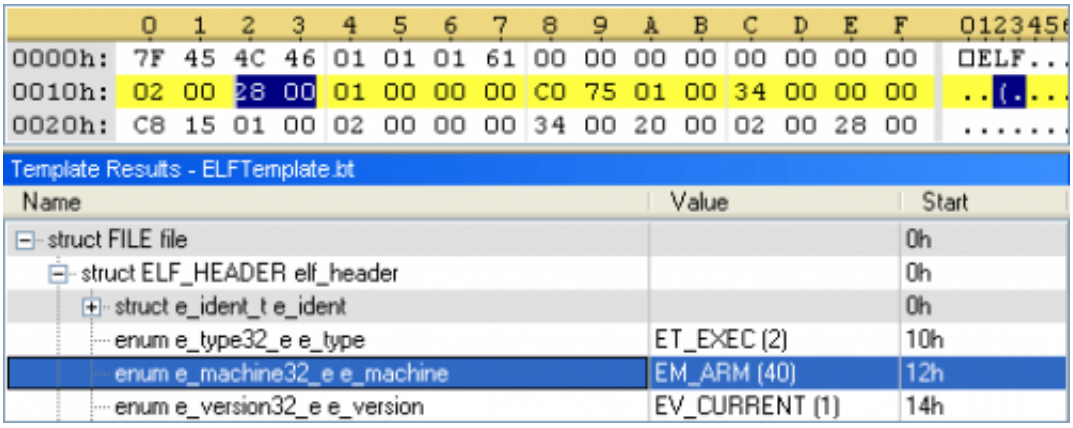
Symantec discovers worm that targets systems running Linux—threat to other devices

December 2 2013, by Bob Yirka



(Phys.org) —Antivirus company Symantec has announced that it has discovered a new worm on the loose—one that attacks vulnerabilities in computer systems running Linux. Thus far, they report, the threat is minimal due to the worm only operating on x86 type computers. It could grow much worse, however, as the worm appears to be easily changed to allow for exploiting other types of hardware running Linux such as home routers, smart TVs or security cameras.

Symantec has named the worm Linux.Darlloz and reports that its main abilities at this time appear to be one of replication by taking advantage

of a PHP vulnerability in systems running older versions of Linux. When it executes, it creates random IP addresses and attempts to locate pathways to other devices on the network. Those devices that aren't protected become infected as well, which in turn serve as aids in propagating the worm.

Linux is an open source operating system that is similar in many respects to Unix and has been widely used as both a learning and research tool. More recently, those making hardware devices have begun using it because no licensing fee is required. The down side is that because it's open source, many versions lack the security features of more robust operating systems such as (Unix based OS X) or Windows.

The fear with the new worm is that it appears it could be easily adapted to run on virtually any platform, and perhaps other operating systems—also, there is the problem of a sometimes lackadaisical approach to security by some device makers. A worm that infects a home router or TV isn't a big problem by itself—it's what it represents—an opportunity to infect an entire home or business network—that makes it a cause for alarm.

Symantec suggests that consumers consider only purchasing devices that can have their software upgraded and to choose hard-to-break passwords when configuring them, and of course, to make sure password entry is required. They also suggest consumers take advantage of the fact that most devices also come with console software that allows for verification as well as a means for blocking incoming PHP post requests.