New Duqu virus linked to Microsoft Word Documents

November 4 2011, by Bob Yirka

I new virus has cropped up in various countries across the world and its target appears to be corporate networks. The Duqu virus, first noted last month by a laboratory at Budapest University, has now been spotted in several other countries and appears to be sent via Microsoft Word documents attached as emails. Microsoft has announced that it is working on a fix.

The point of the new virus seems to be to gather corporate information and then send it to some as yet unknown site. Thus, it's a form of corporate espionage. Chillingly, researchers at Symantec, the giant antivirus company, say it looks like some of the code in the virus is the same as was found in the Stuxnet virus that wreaked havoc on Iran's

nuclear program, indicating that the perpetuators were either able to obtain the code from that virus, or, are the same people.

The virus is activated when a person to whom an infected Word document was sent, opens it. The virus infects that computer then seeks out other computers through the corporate network. As it goes, it collects data and then apparently, seeks a path out to the Internet where it can send the data it's collected to a predefined destination. Thus far it has relied on a so-named zero day exploit to take advantage of a previously unknown weakness in the Windows kernel, which means getting in and doing its dirty work before victims have a chance to come up with a means of defense against it.

Thus far, it appears that the virus has been targeted at specific types of companies, as the data- collecting part of the virus seems to seek out information pertaining to industrial control-systems. So it's likely that whoever unleashed the virus, did so in hopes of gaining information on how companies are designing and manufacturing their products; not something the average person would need to worry about, but still enough to cause concern about the growing sophistication of computer viruses.

So far, instances of the virus have been seen in Iran, India, France, Ukraine, the UK and at least eight other countries that have not been specifically identified.