DID DUQU FIX THE BUG THAT REVEALED STUXNET?

Duqu isn't Christopher Lee in *Attack of the Clones*, but it is the newest computer malware to hit mainstream consciousness. It's attracting attention mainly because it is based on the same software source code base as the Windows portion of Stuxnet. If you haven't heard about Duqu, check out the Wired article that first alerted me to its existence. If you are interested in the technical details, you need to read the excellent write-up by Symantec (pdf link).

Unfortunately, the twitterverse, blogosphere, and the computer security profession all seem to be caught up in a hype/debunking/speculation cycle that is spreading more heat than light. The primary significance of Duqu is what it tells us about the operation behind Stuxnet and Duqu, i.e. that it is an on-going enterprise conducting computer espionage and sabotage around the world. The fact that it is rather obviously (though not publicly) run by the U.S. intelligence community should concern everyone. I'll put up a more extensive post later (including a timeline!) detailing what the Duqu phase of the Stuxnet operation tells us about the cyberwarfare strategy of the U.S. and how it is endangering the safety and security of the U.S. and the whole industrialized world. But first, I want to remind everyone how Stuxnet was originally discovered:

> … the VirusBlokAda security firm in Minsk, received what seemed to be a relatively mundane email on June 17, 2010. An Iranian firm was complaining that its computers were behaving strangely, shutting themselves down and then rebooting. Ulasen and a colleague spent a week examining the machines.

> Then they found Stuxnet. VirusBlokAda notified other companies in the industry, including Symantec.

This incident became curiouser and curiouser as Symantec, Langner, and others took apart Stuxnet. There wasn't any obvious reason that Stuxnet would have caused that sort of behavior on an infected computer. I even wondered at the time whether or not Stuxnet's cover was blown intentionally since the perpetrators moved quickly to call further attention to themselves. But, thanks to the good work of the Symantec team, we can surmise something quite revealing about the initial discovery of Stuxnet.

The rootkit component of Duqu is quite similar to, but not exactly the same as, the one in Stuxnet. In both cases, if the infected computer gets rebooted while it is infected, the rootkit wants to make sure that it is running before the operating system is fully loaded. That's why this rootkit (both flavors, Stuxnet and Duqu) is packaged as a hardware device driver. Here's a feature of Duqu's driver that wasn't present in Stuxnet (as described by Symantec on page 4 of the pdf linked above):

> The driver then registers a DriverReinitializationRoutine and calls itself (up to 200 times) until it is able to detect the presence of the HAL.DLL file. This ensures the system has been initialized to a point where it can begin injecting the main DLL.

The bolded portion is the new functionality that wasn't present in Stuxnet. As a software developer, this detail tells me a lot. The driver is checking to make sure that the hardware abstraction layer (HAL.DLL) of Windows is loaded before it proceeds with the re-infection routine. The HAL is a portion of the Windows OS that really needs to be loaded before

device drivers can function properly. Between the time that Stuxnet was deployed and this later version was compiled, the Stuxnet team identified a problem (a race condition) with their software being loaded before the HAL, probably only under the rarest of circumstances. So they modified their program to take this possible condition into account.
As I thought about this, I realized that the likely impact of the Stuxnet device driver being loaded before the HAL was properly initialized would almost certainly be that the machine would continuously crash and reboot. Look again at how Stuxnet was first discovered (remember it was in the wild for at least a full year before it was noticed by any anti-virus vendor):

> … the VirusBlokAda security firm in Minsk, received what seemed to be a relatively mundane email on June 17, 2010. An Iranian firm was complaining that its computers were behaving strangely, shutting themselves down and then rebooting. Ulasen and a colleague spent a week examining the machines. Then they found Stuxnet. VirusBlokAda notified other companies in the industry, including Symantec.

By November 3, 2010 (the compile date of the Duqu component), the Stuxnet team had fixed the bug that led to the discovery of Stuxnet last year. And then went almost another full year without being discovered by the anti-virus vendors. It is likely to be a lot harder to reconstruct what the Stuxnet team has been up to this time around, but it is clear that the operation is on-going and we can assume (unless specific information turns up pointing in a different direction) that the primary target is still the Iranian nuclear program.