WHY DOES DUQU MATTER?

The short answer is that if your PC got infected by Stuxnet last year, you were just collateral damage, unless you were operating a very specific set of uranium enrichment centrifuges. If you get Duqu this year, your network is under attack from a CIA/Mossad operation. They might seem a little outrageous, but bear with me while we get into the weeds of what Duqu is all about. I will lay out a set of assertions that lead to the conclusion that Duqu really is the "precursor to the next Stuxnet" as Symantec say in their whitepaper.

1. Stuxnet was created by the CIA and the Mossad

Although no one has officially claimed responsiblity for Stuxnet, both the U.S. and Israeli governments have done everything but take offical responsibility. Neither government has ever denied responsibilty, even when directly asked. In fact, officials in both governments have been reported as breaking out in big smiles when the subject comes up.

2. Duqu is from the same team that created Stuxnet.

The first clue that Duqu is from the Stuxnet team is the similarities between the rootkit components in both pieces of malware. The folks who have studied the two most closely are sure that Duqu is based on the Stuxnet component's source code. Despite what you may have read on the internet, the actual source code to Stuxnet is not publicly available. Some folks have reverse-engineered some of the Stuxnet source code from the binaries that are available, for various technical reasons, I'm sure that these don't serve as the basis for Duqu.

Duqu even has a fix for a bug in Stuxnet. Also, the only two pieces of malware in history to install themselves with as Windows device drivers with legitimate, but stolen, digital

certificates are Stuxnet and Duqu. Both Stuxnet and Duqu were active in the wild and managed to evade detection for many months. While that's not unheard of for malware, it is another point of similarity.

Stuxnet targeted a specific industrial control system (ICS) installation (the Siemens PLCs that were used to control the centrifuges at Natanz). Here's the lastest on what Duqu targets:

> Some of the companies affected or targeted by Duqu include the actual equipment that an ICS would control such as motors, pipes, valves and switches. To date, the vendors that make the PLC, controllers and systems/applications found in control centers are not yet affected, although this information could change as more variants are identified and these vendors look more closely at their systems.

There are no other instances of computer malware that target these sorts of installations.

3. Stuxnet was a worm, Duqu is not.

Stuxnet was a very aggressive computer worm. It had to be to jump the "air gap" that protects a secure ICS such as the system that ran the Natanz installation. When Stuxnet was discovered, the A-V vendors quickly discovered millions of computers had been (benignly) infected with Stuxnet. Duqu, on the other hand, has been found on only a handful of computers. Interestingly, no one has yet discovered the dropper, that is, the program used to place the Duqu rootkit on the infected machines. This is almost certainly because Duqu is being placed on these machines via a spear phishing attack. In spear phishing, specific targets are chosen and the attack is customized to the target.

4. Duqu is being used to download a RAT (Remote Access Trojan)

The rootkit component was used to download a standalone program designed to steal information from the computer that it has infected (including screenshots, keystrokes, lists of files on all drives, and names of open windows). Duqu is doing computer network reconnaissance. The information gathered by Duqu is very useful for planning future attacks. Before the command and control server was taken off-line, Symantec observed Duqu downloading three additional files to an infected machine. The first was a module that could be injected into other processes running on the machine to gather some process-specific information as well as the computer's local and system times (including time zone and daylight savings time bias). Another downloaded module was used to extend the normal 36-day limitation on Duqu installations. The last downloaded module was a stripped down version of the standalone RAT, lacking the key logging and file exploration functionality.

5. Put it all together and it adds up to a well-executed, highly targeted covert operation

For the last ten months, Duqu has been quietly stalking a small number of industrial manufacturers. No one even noticed before early September and it wasn't until last week that the nature of the threat was clear to anyone. Duqu is spying on a handful of companies, gathering data that will be used for the design and development of the true Stuxnet 2.0. One thing we don't know is who the target of Stuxnet 2.0 will be. But I have a suspicion. Nothing indicates that the ultimate target (i.e., Iran) of the Stuxnet team has changed. In August of this year, Iran announced that it had activated its first pre-production set of his newer IR-2m and IR-4 centrifuges. These are the successors to the centrifuges that Stuxnet attacked. If you wanted to do these centrifuges what Stuxnet did to the earlier IR-1 centrifuges, you would need a lot of specific data about the safe operating specs of the various components that go into making advanced centrifuges. If you knew or suspected who was

supplying Iran with these components, you might want to gather some data from the internal networks of those suppliers. That’s what I think the point of Duqu really is.