A CYBER FIRST STRIKE

A little town in Massachusetts had a talented engineer / inventor who created a device called PLC. One of the members name was Dick Morley and he is known as the father of the PLC. It filled a need in the auto industry to replace the hardwired relays that were installed by electricians for the auto industry.

The birth of modern day PLC's started in the late 1960's and into 1970's. This burst of innovation was on America's Technology Highway. It preceded the

proliferation of ingenuity in Silicon Valley California.

It has evolved to a sophisticated process logic controller that can run process systems, such as chemical companies, oil companies, contribute to running nuclear power facilities etc.

A computer malware has been in the news lately. The attacks actually started in July and the big guns on the malware front have been attempting to prevent this from spreading. That is the official word.

What makes this malware so unique and powerful is the way it has been put together. Infection is accomplished by inserting a host USB drive into a computer and or through networks.

The code is so intricate and professionally packaged that is compartmentalized
into encrypted sections., and parts of the executables are written in different programming languages.

What this means is that is that it was created, most likely by a team of coding professionals that might be one of our first examples of cyber warfare. Most of the attacks have taken place in Iran.

It's the most advanced piece of malware ever discovered. It originally appeared four months ago. The only serious damage done to servers has been Iran. Now using your imagination do you think this came from China or Russia?

This is not the work of a script kiddie having fun with code, this was done by the pros and the pro's look to be friends of ours. Draw your own conclusions. Even the military silent professionals suspect this to be one of ours.

We have been told that the US has lost talent that the best is found in India, China, and beyond. Not so fast, some of the best remain here and will for the foreseeable future.

What do PLC's have to do with this story? PLC's are what control some of the very large processes at huge chemical and oil companies. They are responsible for opening valves and

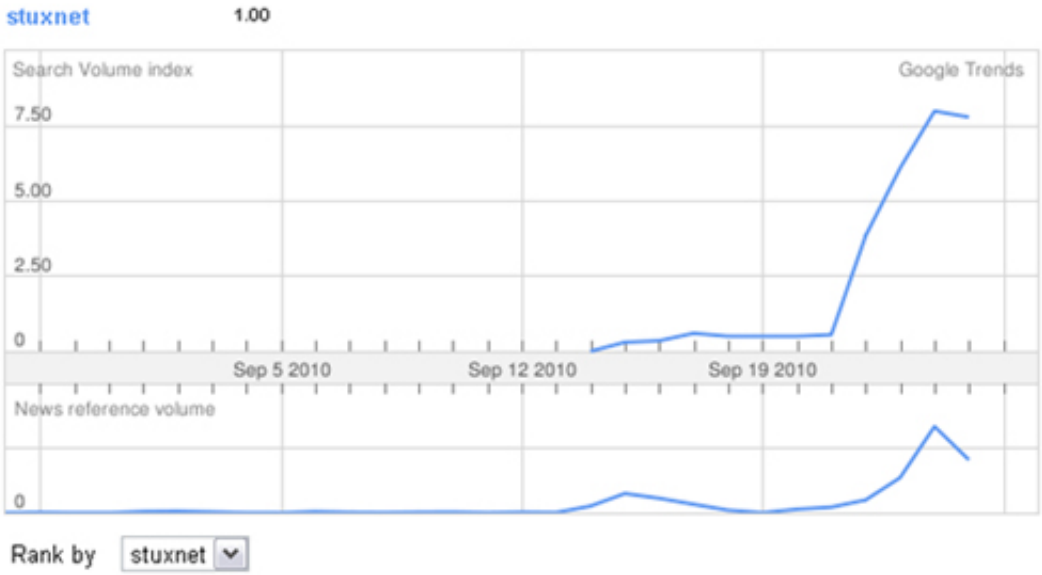
bleeding off high temperatures in piping systems that may carry lethal products used in production.

If you had an executable piece of code that could hide itself and go into a zero day hunt to kill at its predetermined time, then you have a weapon. This weapon does not look like the typical munitions, however it is just as potent.

Some antivirus commercial companies have come up with ways to detect this malware, however it does not look like “here” is the target. If it installs itself as a root-kit and establishes a back door to return later, it could inflict more damage.

The code is still being disassembled. It may have further capabilities that are yet to be discovered. Imagine if after month or two, the original attack spawned a whole new attack, that was not revealed in the first payload.

Below is a Google Trend data chart for Stuxnet:



What has been reported is that a large number of the centrifuges at the Iranian site in Natanz have been compromised and are still not working. This is Iran’s large

nuclear enrichment site.

It is not clear if the other parts Iran’s nuclear program have been affected by this, however it is possible that this is only the beginning.

Think about the politics of this. Iran will now be invited into further discussions to change policies. If stubborn rants of defiance continue, the attacks may well escalate.

It would be naïve for the mullahs to believe that this is all that can be done. Imagine if their financial structure was brought to its knees? Imagine if their meager infrastructure stopped all together?

We have heard many doomsday scenarios regarding our vulnerabilities and it is time for our enemies to understand that the pendulum swings both ways.

The West is not stupid and the large facilities that have been built by oil, power, and chemical companies have redundant systems in place. For one thing their critical controlling PLC's are not accessible via the outside world. These critical process intensive sections of the companies are in a total closed loop, insulated from outside attack vectors and they are guarded as if the plant was filled with gold. (Hopefully this is still true)

I have worked in some of them and the security is impressive. If we are talking nuclear plants then you better have a cloned army of supermen and they still are going to die trying.

Stuxnet was highly efficient and targeted at delivering a direct hit to the SCADA, which literally means (supervisory control and data acquisition) software.

It attacks the Siemens Simatic WinCC and PCS7 software through a poisoned USB key and networks. It is not widely known that many of the default passwords for these systems were never changed.

It is unclear if the above password changes would have totally prevented the attack. It is spread via USB keys and networks, now that changes the attack vector field, doesn't it?

Part of the false authentication process was performed with stolen digital certificates. This just reveals the multiple layers of sophistication that was present in this attack. RSA experts have since revoked the stolen certificates.

So far there are three Siemens companies blessed by Siemens who are McAfee, Trend Micro or Symantec. Microsoft has also released a patch, which can be found here.

Microsoft Critical Security Patch MS10-046

One might also question the logic in Microsoft sharing source code with China and Russia.

Sophos reported that Siemens actually advised power plants and manufacturing facilities not to change the default passwords. This is certainly questionable behavior for Siemens, if true. It was

probably to reduce the tech support needed

for those customers who lost their passwords.

We knew threats like this were coming, new threats are emerging constantly and we must all do our parts to protect our on little domains and home networks.

This means install on a regular basis, security patches for any OS, whether it be MacOSX, Windows, Unix, Linux. That is your first line of defense, do not ignore this.

Marco