Confluence INVESTMENT MANAGEMENT

# Weekly Geopolitical Report

*By Bill O'Grady*

*October 4, 2010*

## The Stuxnet Virus

Over the past two weeks, reports began to surface that unusual malware was striking industrial facilities across Asia and the Middle East. As details emerged, the virus, named Stuxnet, appears to be unusually dangerous and remarkably sophisticated. In fact, this virus is being considered by some to be the first example of a state-to-state cyberweapon.

In this report, we will detail what is known about the Stuxnet virus. We will discuss the likelihood of this virus being a weapon, where it was deployed, the damage it may have caused and who might have created it. We will examine the geopolitical ramifications of the malware and wrap up with how it may affect financial and commodity markets.

### The Stuxnet Virus

In mid-June, an obscure security firm named VirusBlockAda, based in Belarus, reported a rather sophisticated malware was targeting "supervisory control and data acquisition" (SCADA) control systems of Siemens-built installations. A month later, Microsoft confirmed that this virus, technically a "worm," was targeting Windows PCs that were used in managing industrial units that used Siemens software. SCADA is used to operate industrial operations, including pipelines, refineries, power plants, etc.

As security analysts examined Stuxnet further, a number of disturbing characteristics emerged. First, the worm could exploit four "zero-day" vulnerabilities in Windows software. A zero-day vulnerability is a previously unknown portal that will give a hacker access to a Windows operated computer. The typical virus will only employ one of these zero-day portals as they are very valuable. Usually when a hacker discovers one, he will use it quickly (because it will be patched soon after discovery) or he will sell it to virus creators. A virus developer willing to sacrifice four zero-day portals clearly wanted to ensure that his target was hit and that the malware would have multiple areas of access. In addition, employing four suggests a creator with ample monetary resources.

Second, the virus was first planted into computers by flash drive instead of the internet. This suggests, at least at inception, this was an inside job by someone who would have access to target computers. Third, the virus was ingenious in its structure. It searched for a unique software "fingerprint" that would allow it to infect a specific industrial process. Until it found this fingerprint, it would quietly wait in the background, hidden, avoiding exposure by standard anti-virus software. Fourth, the virus included two authentic signed digital licenses that were apparently stolen from two different Taiwanese technology firms, which added to the overall cost.

### Is it a weapon?

Analysts who have examined the malware note that this software is so sophisticated that no single person could have constructed it. The malware shows a deep knowledge of Siemens software which is not widely used outside of industrial facilities. In fact, the

code only attacks two models of Siemens programmable logic controllers, the S7 300 and the S7 400. These were apparently used in Iran.

To ensure success, whoever built the virus would have needed access to physical hardware to test it before its launch. The malware has the ability to spread into other systems using one of the four portals (zero-day vulnerabilities) including a printer spooler. Thus, once inside a facility, it would proliferate rapidly.

Once the virus found the correct fingerprint, it would commandeer the SCADA software, using the stolen authenticated certificates to take control. It would then have the capability to disrupt an autonomic process, usually a process that occurs several times a minute (e.g., an instruction to lubricate a critical machine). The effect was that a critical process that is not directly controlled by an operator would begin to malfunction but not be detected by monitoring equipment. The Stuxnet virus could cause severe damage to the infected facility.

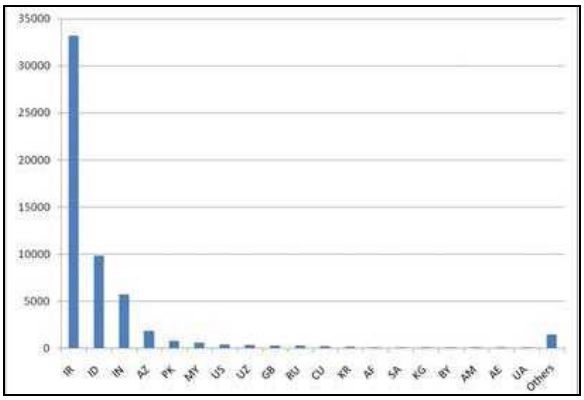
Although there is some dispute about the creator of the Stuxnet malware, the preponderance of opinion suggests that it most likely required the resources of a nation-state and was probably not the work of a private hacker. It appears that this is the first malware that specifically targeted industrial facilities with the goal of creating a dangerous malfunction. Private hackers usually create viruses to capture information or to steal funds. A private group creating something this dangerous would usually be looking for ransom; to date, no group has come forward to claim responsibility or offer a way to eradicate the virus for a fee. In fact, recent reports suggest that efforts to remove the virus have caused it to spread further.

Those who disagree with state sponsorship suggest that it would be possible to bring a private group together to create the bug. However, the acquisition of four zero-day portals and authentic (but stolen) certificates suggests that whoever did it was well funded. In addition, it seems rather odd that a private group could get access to a facility using Siemens software to test its malware. Although one cannot completely prove that Stuxnet was built by a government, it appears most likely that this was the source. Overall, the most likely conclusion one can draw is that Stuxnet is a cyberweapon.

**Where is it hitting?**

Although the virus has spread around the world, by far the largest infection rate is in Iran.

**Known Stuxnet Incidents**




(Source: Symantec)

This chart shows the number of known Stuxnet incidents. The bar on the left of the chart represents Iran. We note that recent reports suggest the actual number of inflected PCs in Iran may be up to 45,000. There does appear to be a Stuxnet "Typhoid Mary," namely, the Russian firm AtomStroyExport which worked on the Bushehr nuclear reactor in Iran. This firm apparently has contacts with facilities across Asia and appears likely to be the transmitter of the virus. We doubt the firm was the creator, but it was probably the unwitting

carrier. In addition, the Belarus firm that first reported the virus was working in Iran. Thus, it appears probable that Iran was the target of the attack.

The focus on Siemens equipment is further evidence that Iran was the target. It is well documented that the Bushehr nuclear plant used Siemens systems and last year, officials in Dubai seized a shipment of Siemens Simatic S-7 controllers (mentioned above). The controllers were captured after Western intelligence agencies warned Dubai that the equipment would likely be used in its nuclear program.

**Has Stuxnet already hit its target?**

In July, Wikileaks, the online bulletin board for rumors and leaks, reported that there was a nuclear accident at Iran's uranium enrichment facility at Natanz. There was no further independent confirmation, but the BBC noted that Gholam Reza Aghazadeh, the head of Iran's Atomic Energy Organization, unexpectedly resigned under mysterious circumstances. The IAEA has noted that since May, the number of operating centrifuges at Natanz fell by 23%. There have been numerous reports that Iran was dealing with problems in uranium enrichment, but these issues were generally thought to be due to outdated equipment and inadequate training of staff.

We also note that the Bushehr nuclear reactor was expected to go online by the end of August. Initially, reports indicated that the start was delayed due to "unusually warm temperatures" in the area even though temperatures had been normal. Just this week, Iran's Atomic Energy Agency noted that the reactor would not begin producing power until next year. Iran has admitted that its computers at Bushehr have been attacked by Stuxnet.

There has been a good deal of speculation that either of these facilities was the target for the attack and the continued spread of the virus is simply collateral damage. Reports indicate that Iran has been unable to eradicate Stuxnet. In fact, Iran has stopped using the patch created by Siemens to remove the virus because Iranian advisors either believe it doesn't work or worry it is causing the virus to spread further.

The general consensus of technology analysts is that Stuxnet was created by a nation and is a cyberweapon targeted at Iran's nuclear industry. Although we cannot know for sure, the weight of the evidence would suggest that this assertion is probably true.

**Who created Stuxnet?**

At this point, no one has stepped forward to take responsibility for creating and deploying Stuxnet. Although there are private firms capable of building such a virus, there seems to be little incentive for the private sector to make and deploy Stuxnet.

The most obvious culprit is either the U.S. or Israel. Both nations have the technological prowess to develop this cyberweapon. Israel is considered the most likely nation to deploy the weapon. Israel is clearly threatened by Iran's potential development of nuclear weapons and it faces opposition from the U.S. for military strikes. Developing a weapon that delays Iran's nuclear program without putting its relationship with the U.S. in danger would be an attractive outcome for Israel. Recent media reports indicate that Israel has pushed back the date when it believes Iran will have nuclear weapons, perhaps reflecting the damage caused by Stuxnet.

There have also been references in Stuxnet's code to Myrtus which refers to the biblical Esther. The Book of Esther tells the story of a young Jewish bride (Hadassah, in Hebrew, which means "myrtle" or joy) whose actions prevented the Persians (ancient Iranians) from eradicating the Jews when they were dominated by Persia. And, there is a date in the code of May 9, 1979, the day when Jewish Iranian businessman Habib Elghanian was executed by the revolutionary government. Elghanian was instrumental in bringing Western technology to Iran during the Shah's reign.

These references could be Israeli "calling cards" to let Iran know who is attacking them and why. Or, it could simply be a clever "red herring." In any case, these hints raise speculation that Israel deployed the weapon.

The U.S. would have an interest in using such a weapon as well. The U.S. does not want Iran to develop nuclear weapons but loathes starting another war. If a bit of cyber derring-do delays and, perhaps, prevents Iran from developing nuclear materials, it would be a welcome development. In addition, media reports suggest that the U.S. is trying to open backchannels for negotiations with Iran. The U.S. bargaining position would improve if the Obama administration knew that the nuclear program had hit major snags.

However, there might be others that would favor the disruption of Iran's nuclear program and have either the U.S. or Israel blamed for the attack. Russia especially would benefit from a "false flag" operation. It has little interest in Iran developing nuclear weapons but would like to have good relations with the country. Russia delayed fueling the Bushehr reactor for years, and we note that it was a Russian firm that is thought to be responsible for "injecting" the virus into Iran. Thus, acting as if it is supporting Iran and yet, at the same time, using a cyberweapon to thwart those aims and place responsibility on the U.S. or Israel is a great outcome for Russia. Iran would likely retaliate against the U.S. and prevent the U.S. from withdrawing from Afghanistan and Iraq. Russia wants to keep the U.S. bogged down in the Middle East and this cyberweapon might just do that. China would have similar sentiments.

**How does Iran retaliate?**

Iran has a long history of retaliating against covert attacks. The problem Iran faces is that it doesn't have any real evidence to point to the perpetrator of Stuxnet. If Iran attacks Israel, it will need to retaliate with some semblance of proportionality. Simply kidnapping or killing some Israeli soldiers won't replicate the potential damage brought to its nuclear program.

It would be tempting to Iran to attack an Israeli industrial or military site that is roughly equivalent Bushehr or Natanz. However such a strike, which would be overt, could trigger a massive military retaliation that would appear justified. On the other hand, it is unlikely that Iran has the technological skills to retaliate in a similar fashion to Stuxnet.

Iran tends to prefer attacks that will give it plausible deniability (which is what the Stuxnet attack has given Israel or the U.S. if they were indeed the perpetrators). Thus, we would expect retaliation to come from one of its proxies, Hamas or Hezbollah. However, in the current environment, it may be difficult for Iran to prevent an escalation of hostilities. The key issue for Iran is whether or not it is prepared for war.

**Ramifications**

At first glance, one could argue that the Stuxnet attack lowers the odds of military action in the Middle East. After all, a major goal of the U.S. and Israel is to delay Iran's nuclear program either by diplomatic or military means. The cyberstrike may have accomplished that goal; although admittedly one of the problems with such attacks is that reconnaissance is very limited, so it is difficult to know the true impact the cyberstrike really had.

Complicating matters is the Iranian response. If Iran avoids an overt response that would trigger Israeli and Western military action, the need for airstrikes against Iran is lessened. However, Iran does not have a plethora of responses that can offer proportionality and not trigger a military response.

The most likely response would be attacks against U.S. targets in Iraq and Afghanistan. If Iran decides that Israel is the target, it could strike via its proxies, Hezbollah or Hamas. However, either could trigger a counterstrike that could potentially bring broader military action.

The other issue with Stuxnet is that it opens the "Pandora's Box" of cyberwarfare. It reminds one of the first deployment of poison gas or atomic weapons. The initial use of the weapon gives the aggressor great power but invites an equivalent response. Unfortunately, the U.S. is vulnerable to such attacks given our dependence on technology. The apparent success of Stuxnet will encourage other nations to develop similar weapons and potentially create an arms race in cyberspace. Assuming that this was not a "false flag" operation, whoever decided to deploy this weapon had to be aware of the longer term ramifications and decided that the target was important enough to warrant the risks.

In the short run, the Stuxnet worm will probably postpone airstrikes against Iran. However, that assumption depends on the Iranian retaliatory response. Until we feel confident about the nature of that response, we will maintain our overweight positions in energy.

Bill O'Grady
October 4, 2010