ControlGlobal.com
PROMOTING EXCELLENCE IN PROCESS AUTOMATION

A Scary Piece of Malware Named Stuxnet Is in Town. Remember Its Name. Its Arrival May Make You Want to Change the Way You Think About Control System Security

09/24/2010

By Nancy Bartels

We can't say we weren't warned. For years, the doubters and naysayers have been warning us that maybe all this PC-based computing and connectivity on the factory floor was a bad idea.

Security was always one of the main concerns. But the warnings were drowned out in the noise of the inexorable march to PCs on the plant floor and Internet connectivity.

Meanwhile, control engineers were used to working with closed systems that were pretty well blocked from outside mischief makers, and IT people, who did have a grasp of cyber security issues, were clueless about control systems and their unique security problems. So we've limped along with a few folks from both disciplines doing their best to bridge the gap, struggling to overcome institutional inertia, preaching cyber security best practices, training people to think differently and hoping for the best.

As of July 14, that strategy is no longer good enough.

On that day, Siemens was notified of a security breach within Windows, which could potentially affect its Simatic WinCC SCADA software and the PCS7 DCS, which uses WinCC as its HMI, and the S7 controller. First to discover the worm in June of this year was the Belarus-based maker of the VirusBlokAda anti-virus product. In July, Byres Security's (www.tofinosecurity.com) chief technology officer, Eric Byres, confirmed that Siemens and its users were experiencing "a zero-day exploit against all versions of Windows including Windows XP SP3, Windows Server 2003 SP 2, Windows Vista SP1 and SP2, Windows Server 2008 and Windows 7." Later, it was reported that older versions of Windows, which Microsoft no longer supports, were vulnerable as well.

For the uninitiated, a "zero-day" exploit is one that uses a previously unidentified security breach that only becomes apparent because of and at the same time as the original attack, and leaves all other users of the same system or systems at risk until such time as the vulnerability is eliminated.

According to Nicolas Falliere of security vendor Symantec (www.symantec.com), "Stuxnet can steal code and design projects and also hide itself using a classic Windows rootkit, but unfortunately it can also do much more. It has the ability to take advantage of the programming software to also upload its own code to a PLC typically monitored by SCADA systems. Stuxnet then hides these code blocks, so when programmers using an infected machine try to view all of the code blocks on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC."

Falliere adds, "In particular, Stuxnet hooks the programming software, which means that when someone uses the software to view code blocks on the PLC, the injected blocks are nowhere to be found. This is done by hooking enumeration, read and write functions, so that you can't accidentally overwrite the hidden blocks as well. Stuxnet contains 70 encrypted code blocks that appear to replace some ‘foundation routines' that take care of simple, yet very common tasks, such as comparing file times, and others that are custom code and data blocks. By writing code to the PLC, Stuxnet can potentially control or alter how the system operates."

Byres adds that Stuxnet "uses the Siemens default password of the MSSQL account WinCCConnect to log into the PCS7/WinCC database and extract process data and possibly HMI screens," which it then attempts to export via an Internet connection to a remote server."

Furthermore, says John Cusimano, director of security services at security services and certification vendor exida (www.exida.com), that while this virus seems to have been coded specifically for Siemens products, other products could be just as vulnerable. "WinCC is by far the largest SCADA HMI package. It's embedded into everything. Whether you know you're buying it or not, it may be embedded [in your system]. That's probably why it was the target."

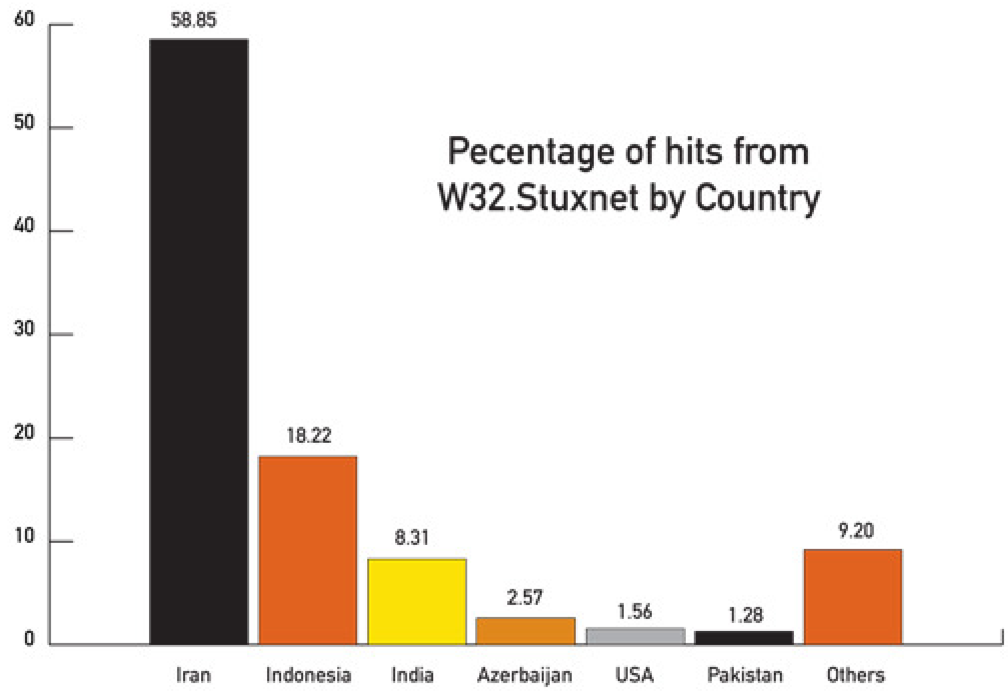
The situation gets even scarier. After Stuxnet was created—and Symantec says that initial versions were circulating as early June of last year—its developers created a second, much more powerful iteration that allowed it to spread among USB devices with virtually no intervention by the victim. They also got their hands on encryption keys belonging to chip companies Realtek and JMicron and digitally signed the malware, so antivirus scanners would have a harder time detecting it. This has allowed Stuxnet to defeat multiple factor authentication.

Not Just a Prank

Stuxnet is not some prank cooked up by a kid with more cyber smarts than sense. The sophistication of the attack and the kind of money that must have been spent on it suggest the perpetrators have a more serious agenda. What that might be is open to speculation. Intellectual property theft is one likely possibility, but other, even more disturbing ideas come to mind as well—state sponsored espionage, nationalistic, political or religious groups "sending a message" or even terrorism.

Joe Weiss, author of ControlGlobal.com's "Unfettered" blog and principal at Applied Control Solutions (ACS, http://realtimeacs.com) says, "Many people think of Stuxnet as a data exfiltration issue. This does not seem credible to me for at least two reasons. First and foremost, why go to a controller unless you want to take control? If you want economic data, go to an archival database. Secondly, zero-day Microsoft vulnerabilities and counterfeit digital signatures are extremely expensive. I find it very unlikely that a cost-benefit can be made for this kind of investment if the sole purpose was economic espionage. It is not clear yet what Stuxnet has been programmed to do or when it will be activated, but it certainly has something to do with control. Although Stuxnet could have been used by a counterfeiter to steal industrial secrets, Kaspersky Lab's (http://usa.kaspersky.com/) Roel Schouwenberg suspects a nation-state was behind the attacks."

The fact that, according to Symantec, most of the attacks seem to have been directed at Iran, India and Indonesia (Figure 1) lends credibility to this kind of thinking.



Iran's the Biggest Victim

Figure 1. Most Stuxnet hits have been found in Iran.

Courtesy of Symantec.

As of Sept. 17, Hamburg, Germany-based security expert Ralph Langner (www.langner.com/en/index.htm) offers a suspected victim, the Bushehr nuclear site in Iran, as well as a possible source of the virus, a Russian systems integrator. Note that none of this is proven yet, but Langner makes an interesting case for it.

Industrial espionage. Nuclear facilities. Nation-states. Terrorism. Now we're getting into Tom Clancy territory. Interesting speculation, but not necessarily helpful.

Let's get back to what we really know now as I am writing this story. Within days of the virus' discovery, both Siemens and Microsoft issued patches to close the holes that Stuxnet used to get into systems. As of now, Michael Krampe, director of media relations for Siemens (www.siemens.com), says that "We have identified 15 customers where the virus has been identified on their systems. We have been able to isolate it, detect it and remove it from those systems without damage to operations."

Another way to get perspective on the issue is by seeing what has not happened. No major process event has happened that can be attributed to the Stuxnet virus. Furthermore, no entity has come forward to say it is the perpetrator or demanded money or issued threats. Why that is the case is open to interpretation, but the fact is, at the moment, in spite of its disturbing potential, Stuxnet seems not to have done much harm.

No Harm, No Foul?

For the most part, other than Siemens, major automation vendors at first treated Stuxnet as just another security vulnerability. "How we treat Stuxnet is pretty much how we view every vulnerability for control systems. It's not the first, and it won't be the last," says Ernie Rakaczky, program manager for control systems cybersecurity, Invensys Operations Management (http://iom.invensys.com).

Vendors also reported that only a few of their customers seemed especially concerned, even after news of Stuxnet was released.

In part, this is no doubt due to the fact that not every control system is architected the same way, and the techniques deployed by Stuxnet's inventors would not necessarily work on other systems. Furthermore, every major vendor has systems in place for managing security and notifying users of vulnerabilities.

"We have formalized a whole set of practices to address cyber security—basic stuff—design, validation of code, training, information exchange with customers, monthly patch updates," says Rakaczky, naming a laundry list that would apply to most vendors.

So what's the big deal? Just another virus. Not exactly.

"This is a defining moment for the industry." says Doug Wylie, business development manager for networks and security at Rockwell Automation (www.rockwellautomation.com) "This was intentional, focused on industrial applications. The intent has caused a number of customers and the entire industry to say, 'Yes, this is real.' There are parties not just looking for information, but wanting to take control of systems,"

Roy Tanner, of Strategic Marketing, Industries at ABB (www.us.abb.com), adds, "While this was a focused attack on a particular control system, it is also a clear sign that control systems are being specifically targeted. This must be considered in all phases of control system product development, but also in how control systems are installed, operated and maintained."

"They could have done it to anyone's system," says Bob Huba, product manager and security architect for Emerson Process Management (www2.emersonprocess.com). "[Stuxnet] will certainly accelerate security awareness a bit."

Kevin Staggs, engineering fellow at Honeywell Process Solutions (http://hpsweb.honeywell.com), adds that, "Although Stuxnet may have targeted specific systems, it serves as a reminder of the responsibility of keeping the malware protection software current on all control systems and following the best security practices. "

Brian Owen of OSIsoft (www.osisoft.com) adds, "This was very targeted, and if anyone thinks they can hide when they're targeted, they're wrong."

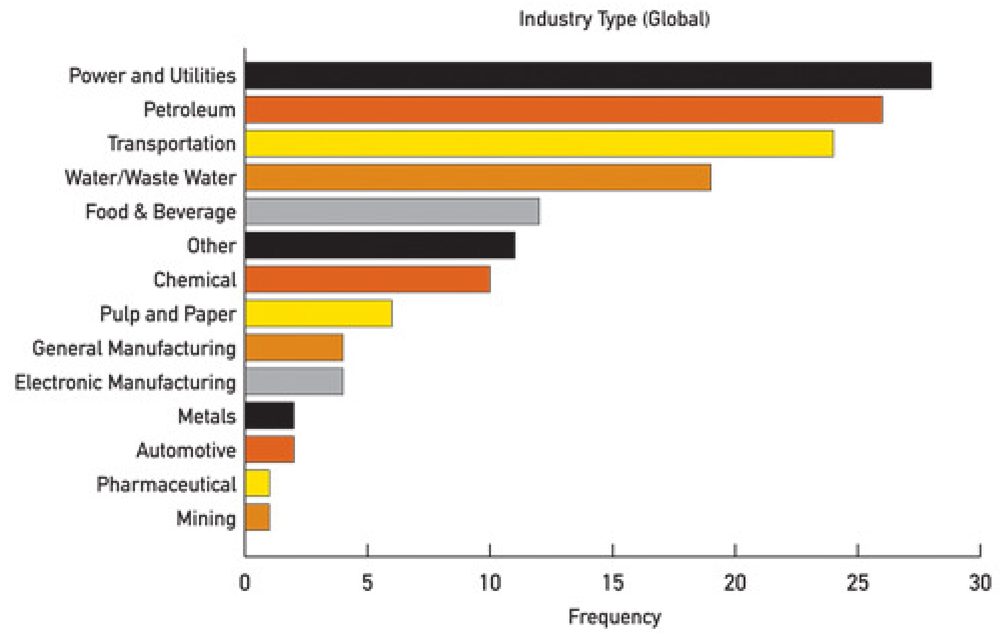
A Change to the Systems?

"One effect of the Stuxnet virus is that there will be a change in the way systems are built," says Cusimano. "The trend has been around for awhile, but this will kick it into high gear. Users have been pressuring vendors to build security into systems.

"The ISA Security Compliance Institute (www.ISAsecure.org), for example, is a consortium of venders and users, who have written a set of compliance criteria for assessing the level of security embedded in products."

He continues, "There's also stuff going on in terms of best practices and competency of systems integration personnel. Control system security is a narrow field. It requires control system, IT and risk management knowledge. That's a pretty special skill set."

Invensys' Rakaczky says vendors must build more security management tools into their systems. "Tools must have functionality to enable people to use them. We have a lot of good guidance and direction, things to do, etc. in our systems—but customers are still struggling with the fact that that too much of that focuses on more for control engineers to do. Every successful [security] program has a strong management component—keeping logs, changing passwords, etc. The key will be the approach. We need a standard way of managing it, so that it can talk to all vendors' products. It needs to recognize multiple vendor environments. We have an obligation to the community here. We're not so much competing against one another here. At this level, all vendors are in this together."



Who is getting attacked?

Figure 2. Power and utilities, petroleum and transportaion industries experience the majority of cybersecurity incidents

Rockwell's Doug Wylie says, "The sophistication level of Stuxnet is one that customers hadn't anticipated in the past. They're looking to vendors for leadership here. It has provided affirmation to vendor companies putting together control system solutions that investments in incidents response and designing in systems-level security are worthwhile. It helps them justify their investments in these things."

The Buck Stops Here

That brings us to the hard truth that applies to all control system users: Good cyber security begins at home.

What should you be doing in response to Stuxnet? The answer is both simple and not-so-simple. Look to your own security.

Begin by asking how secure you are now. Then talk to your system vendor(s). They've built your systems, after all. Who better understands the best way to secure them?

Look to standards—ISA99, IEC SC65C WG13, NIST and others—for help. If you're in a "critical infrastructure" industry, there are government guidelines. The guidelines for the power industry from the North American Electric Reliability Corp. (NERC), the Dept. of Homeland

Security, and the Chemical Facility Anti-Terrorism Standards (CFAT) provide some regulatory benchmarking.

Don't let the multiplicity of standards confuse you. Most are quite similar. "If I take them all—ISA, NIST, NERC- CIP, etc.—they all have same framework. Use a little bit of all of them," says Invensys' Rakaczky.

Cusimano adds, "Get a copy of ISA99.02.01 (March 2009, 'Establishing a Cyber Security Management System.' It's directed at control system users. It takes a lifecycle approach addressing risk assessment, policy and procedures. It's also industry-independent, but there are good documents from specific industries. They can be cross-referenced. There's no topic in one that is not addressed in the others."

Get outside help if you think you need it. Cyber security firms and consultancies with expertise in control systems can be a real help here.

The not-so-simple part of the answer is that cyber security is not just about Stuxnet.

Cyber security is about culture change—one of the hardest things to pull off in any organization. The CEO or someone on the board is going to have to make cyber security a priority and make it someone's job—complete with accountability—not just another duty tacked on to the control room operator's task list.

Getting the attention of the executive suite on any subject not related to next quarter's profits is a challenge, but Stuxnet's emergence may have made that easier. "One of the main takeaways," says Rockwell's Wylie, "is that there was a risk of loss of control and loss of intellectual property. That's an attention-getter."

Still, selling security is a tough gig. If the system works, you literally have nothing to show for expenditures, because nothing has happened. Says Wylie, "Security conversations are always short: ‘We haven't been attacked yet.'"

He adds that the magic word for selling security to upper management is "uptime." Management wants uptime, availability and reliability in their systems, and they can't have those without security (and safety).

Brad Hegrat adds, "You can't regulate due diligence, but executives do care about uptime. There's the reputation factor as well and the possibility of a loss of public confidence.

Accidents happen, but if I have to explain to the board why a digital security failure happened, the subject of negligence is apt to come up."

Good cyber security means developing a whole way of thinking about behaviours and operations. It means sorting out the knotty issues when IT and control engineering work together. It will take homework, and it will require on-going training and vigilance.

What the Stuxnet affair has taught us, says Hegrat, is that in terms of security, "the entire enterprise [must] be treated collectively. It's going to be a full-on requirement from now on. [With Stuxnet] every last digital protection mechanism that you'd have deployed would have failed because this was a piece of targeted code that required human intervention. What this tells you is that no matter how secure the system is, if you don't have people who are properly trained, etc., you're not secure. On the flip side, a less secure system with properly trained people is better off."

Changing the way your organization thinks about security is a daunting task, but there is a model—safety.

OSIsoft's Owen says, "One of our executive VPs told me that 25 years ago, you'd get safety bulletins in morning meetings about fatalities. News was shared across the plant, and the culture did change slowly. Security is going to be the same kind of thing. These changes are cultural. It does take awhile. I'm looking forward to the time when we're on top of this stuff instead of being reactive."

The question is how much time? Stuxnet suggests that time to let a security culture evolve slowly may be running out.

Nancy Bartels is Control's managing editor.

End of COTS and the USB Stick?

The Stuxnet virus has exploited the vulnerability of using a commercial off-the-shelf (COTS) operating system for control and one of the most convenient, ubiquitous tools available now, the USB stick, in process automation operations. One obvious solution is to go back to using only closed systems and banning USB sticks from the control room. But is either option viable?

John Cusimano, director of security services at security services and certification vendor exida (www.exida.com), doesn't think so. "Momentum for open systems is too great. Going back is almost not an option," he says. "We're far too dependent on being able to move data around throughout the organization so we can make good decisions and optimize processes. It may slow down a bit, but it won't stop. Nor is the drive to invest COTS systems going to stop. The productivity and technical benefits are too great. Except for the most conservative industries, such as nuclear, most will continue to use them."

Brad Hegrat, principal security consultant at Rockwell Automation (www.rockwellautomation.com) predicts that USB sticks still have a lot of life in them as well. "This is not the end of the USB stick because it's so useful, but it might be the end of the USB stick in control systems. A control system-centric security system has a very limited place to integrate the USB into the environment."

He also suggests limiting the use of USB sticks to non-mission-critical systems. If they are to be used in the control room, they should be purchased from a trusted vendor and be clean—that is, have no other files on them.
"You also have to have physical control over them. You should treat them like keys to the building. [Their use] should be regulated and enforced by strict policies in a formalized program."

Securing Your Systems

Jim Toepper, product marketing manager at industrial networking products supplier Moxa (www.moxa.com) offers a number of suggestions for securing your systems from Stunxet and other malware.

- Begin with the understanding that you need to look at three different kinds of security: physical, network and people security. Then, when looking at network security, understand the two aspects—external and internal. They are equally vulnerable.
- Look to your firewall. Is it configured correctly? Don't leave all the settings in default mode. "In my experience, 95% of users don't set their firewalls correctly. It's just a matter of not having enough experience with network and communications," says Toepper.
- Use both router- and firewall-based security.

- Insist on robust passwords. Limit people and bandwidth on your network. No one should be on your control system network who doesn't need to be there.
- Set up redundancy plans—not just redundant devices, but redundant networks. If a failure occurs, you need a backup plan.
- Configure your systems locally. Remote configuration is tempting and convenient, but risky. The most secure way to configure your system is directly from a serial port. The second most secure way is SSH or SSL security. Make sure all data is encrypted and authenticated. "Almost everyone uses Telnet or a browser, and all that info is transmitted in clear text," says Toepper.
- Look to physical security. Physically turn off USB ports and switches. Set up computers so they won't use a USB stick. Few people need physical access to computers themselves. Lock them away in a secure enclosure and use a wireless keyboard and mouse. Use an industrial computer rather than a PC. Put items on a secure network. Another option is to install software to scan USB stick for malware or just eliminate their use. Disallow executables.
- Finally, train, train, train so good security practices become second nature to everyone.

Want to Know More?

The Stuxnet story is an evolving one. As researchers continue to study it, more information will become available. Here are some places to look for updates.

- The Tofino Security blog written by Eric Byres and Scott Howard. www.tofinosecurity.com/blog/
- Symantec security expert blogs. www.symantec.com/connect/symantec-blogs/security-response/11761/all/all/all/all.
- Industrial Defender. www.industrialdefender.com/. Look for white papers and regular updates on Stuxnet.
- The Repository of Security Incidents. www.securityincidents.org/. A regular compilation of security incidents in the process industries.
- Joe Weiss' "Unfettered" blog. http://community.controlglobal.com/unfettered.
- Also check with your control system vendor's website. Most vendors are watching this story and updating information on a regular basis.

PutmanMedia

Contact Us | Advertise | Privacy Policy | Legal Disclaimers, Terms and Conditions

P: 630-467-1300 | 555 West Pierce Rd., Suite 301, Itasca, IL 60143