Hal Berghel

# CYBERWARFARE 2011: LET THE STUXNET GAMES BEGIN

Stuxnet has proven that we live in interesting times.

For those of you new to Stuxnet, its 2011's biggest gift to cyberwarfare. At this writing, we're pretty confident that we understand what it does/did. As to who did it, not so much.

## The Evolution of Stuxnet

Stuxnet is basically an enhanced "worm" that begins life on a removable storage device. Stuxnet has an interesting, albeit complicated, genesis. According to the Symantec W32.Stuxnet Dossier (www.symantec.com/connect/blogs/w32stuxnet-dossier), "Stuxnet is one of the most complex threats we [Symantec] have analyzed.... Stuxnet is a large, complex piece of malware with many different components and functionalities." Although the Stuxnet package was discovered in late 2010, many of its components were derived from well-known malware dating back to 2005.

From an evolutionary point of view, Stuxnet's DNA derives from several sources, including:

- The Trojan.Zlob (2005) trojan horse backdoor
- A Windows Shell vulnerability (Microsoft Security Advisory 2286198) that allows remote code execution
- A Windows Print Spooler vulnerability (MSA 2347290)
- A Windows "LNK" vulnerability (MSA 2286198) that allows malware to automatically spawn on Windows XP, Vista and W7 computer when the host USB device is connected and accessed through Windows Explorer

Several of these vulnerabilities were exploited and the drivers registered with Verisign under a variety of legitimate corporation's certificates. The parent Stuxnet encrypted DLL files are embedded in a self-executable wrapper program that acts as the "dropper." On execution, the wrapper extracts the DLLs and support utilities, loads them into a computer's memory, and calls the export routines for further propagation. The business part of Stuxnet is a

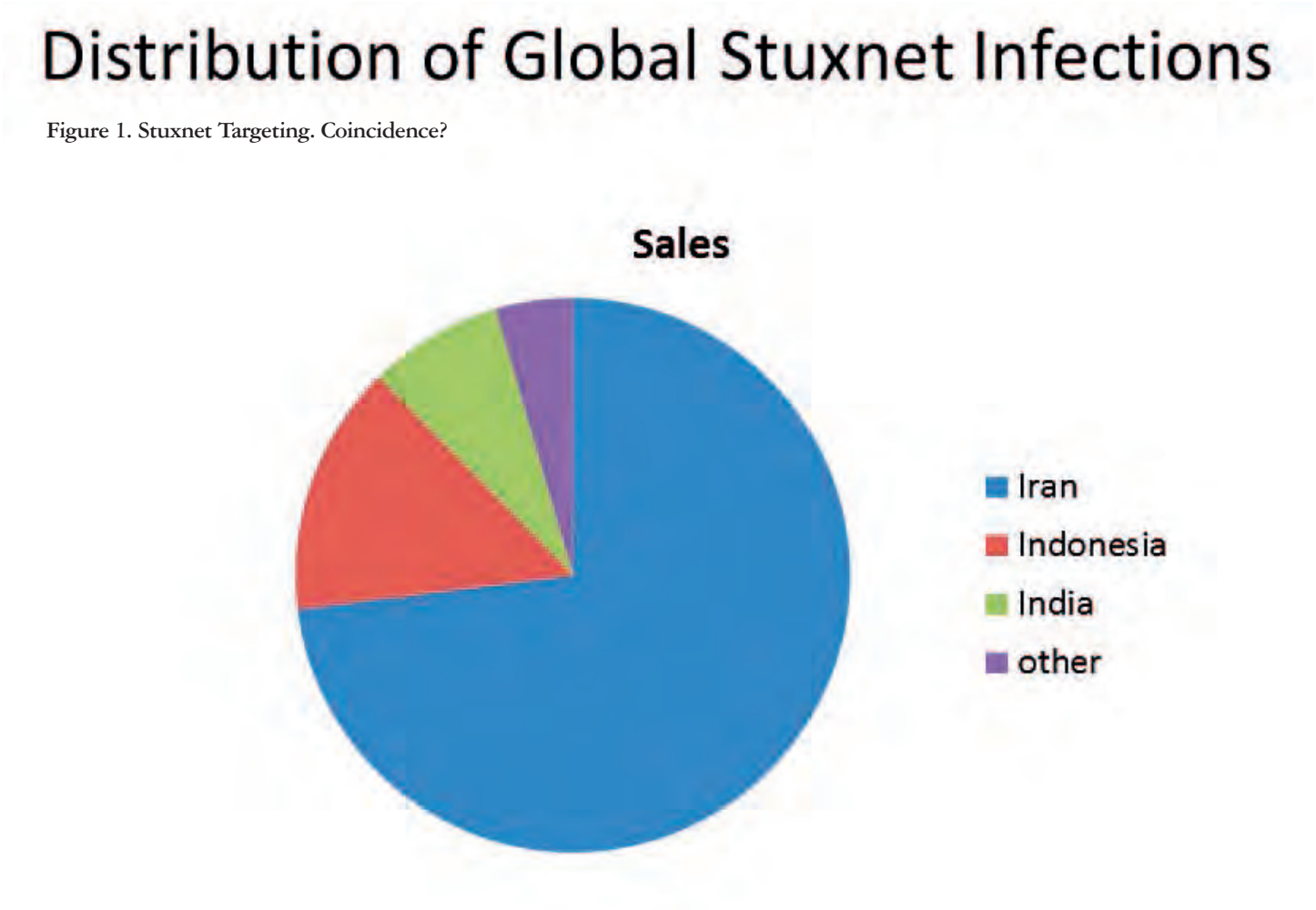


Figure 1. Stuxnet Targeting. Coincidence?

rootket that is optimized for a programmable logic controller (PLC) used in control systems.

## Concentration and Centrifuges

Stuxnet is focused on a particular type of control system developed by Siemens called SCADA (supervisor control and data acquisition systems). It proved especially virulent on the P.C.S.-4 controller that is used to control uranium enrichment with centrifuges. You can probably see where this is headed.

Enter Dr. A.Q. Khan, the Pakistani scientist to whom Western media have attached the sobriquets "Merchant of Menace" for his suspected trafficking of weapons-level nuclear technology. Khan worked in the Netherlands in the 1970's in a laboratory (URENCO) that enriched Uranium for nuclear reactors. His status as senior scientist provided him with privileged access to enrichment technology and IP.
Natural uranium consists of three isotopes: U-238 (>99%), U-235 (.7%) and U-234 (the rest). U-235 is the stuff of which nuclear weapons are made. However, the uranium in a nuclear weapon has to be at least 90% U-235. Anything less won't fizz. The solution is to convert uranium yellow cake into a uranium hexafluoride gas and spin it in a centrifuge. A high speed (~1,500 revolutions per second) centrifuge is ideal for creating a high concentration of U-235. The uranium gas separates with the heavier U-238 driven to the bottom of the containers while U-235 remains at the top. The lighter U-235 is continuously bled off through repeated processing, eventually yielding the infamous "weapons-grade uranium." This process was refined by a fellow named Zippe in the 1950's and 1960's. Zippe centrifuges were deployed in the Dutch lab where Khan worked.

This much is widely agreed upon. After that, Khan's history is subject to debate depending on one's allegiances. According to Western sources, Khan miss-appropriated secret, proprietary IP and technology from the Dutch lab for use in the Pakistani nuclear weapons program. Khan became the head of Pakistan's uranium gas-centrifuge development program which duplicated the Dutch Zippe centrifuge technology. The concentrate was satisfactory, and Pakistan ended up with their nuclear bomb.

Shortly thereafter, the Zippe centrifuge technology shows up in countries with which Khan and his associates had working relationships. In fact, Khan confessed in 2004 to exporting nuclear designs and technology of use in nuclear weapons development to North Korea, Libya, and Iran - although he has since recanted. In any case, all three countries ended up with the same PK-1 gas centrifuges that Khan developed in Pakistan. It turns out that PK-1 gas centrifuges use a version of the Siemen's SCADA controller discussed above. At this point, we've travelled full circle. Sure enough, the PK-1 controllers used the programmable logic controllers developed by Siemens for Step 7 software used to reprogram the PLCs.

According to media reports, the SCADA-controlled Zippe centrifuges remain in use in

North Korea and Iran. Libya apparently decided that nuclear weaponry was dispensable and abandoned its uranium enrichment program. It has been suggested that the Libyan equipment has found its way to labs within the Department of Energy and Unit 8200 on Mt. Avital in the Negev desert.

## Technical Details

The most thorough analysis of Stuxnet that I've seen is Symantec's W32.Stuxnet Dossier (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pd). Though technical, this dossier makes interesting reading for those with a background in computer science or informatics.

We'll leave the technical issues to the reader. In broad terms, Stuxnet is a worm whose primary method of propagation is removable USB storage devices. It resembles a commercial-grade application in function. It has:

- An executable "wrapper" that installs an umbrella .dll file
- The main .dll file contains specific .dll files for individual resources
- Windows CAB files with self-contained executables for injection of the malware into trusted processes (either Windows (lsass.exe, svchost.exe) or anti-virus/security processes (Symantec's Common Client))
- A utility to monitor Stuxnet behavior
- A system resource analyzer that looks for installed antivirus and intrusion protection utilities
- A configuration utility that controls Stuxnet behavior
- Two zero-day elevation of privilege attacks to obtain Administrative rights, one for W2k and XP, and the other for the newer versions of Windows
- Support for HTTP communication with hostile servers for command and control
- Support for P2P communication between compromised computers
- A set of HKLM registry entries
- A rootkit
- An internal log file
- An expiration datestamp of June 24, 2012 that causes Stuxnet to uninstall itself.
- And, of course, a decryption engine - the malware is encrypted.

This is just a partial list of Stuxnet features. One of the interesting characteristics of Stuxnet is the fact that the HTTP packet payload used for command and control is this system information XORed with FF. I mention this because this is a pretty primitive encoding technique to obscure the payload. Some commentators cite this as evidence that at least the command and control programmers were not the sharpest knives in the drawer.

Stuxnet will run on virtually any recent Windows operating system - Win2k, XP, 2003 Server, Vista, 2008 Server, and Windows 7.

## The Rest of the Story

What makes Stuxnet interesting to the security community is its complexity and effectiveness. It is this complexity that suggests multiple teams of hackers and 10+ individuals were involved in its development. Its effectiveness suggests that the development was very focused on industrial controllers that use the Siemens Step7 PLCs -- like those used by Iran at its uranium enrichment centrifuge installation at Natanz. Figure 1 emphasizes this point.

What was the effect of the Stuxnet attack? It depends upon who you listen to.

"...virtually all the centrifuge arrays used in the Iranian uranium enrichment program have been temporarily shut down." - RichardSilverstein.com

"The Stuxnet virus that has infected Iran's nuclear installations may have been behind the decommissioning of 1,000 centrifuges at the Natanz uranium enrichment facility." - Jerusalem Post

"Stuxnet "sabotages the system by slowing down or speeding up the motor to different rates at different times," including sending it up to 1410 Hz, well beyond its intended maximum speed." - Christian Science Monitor

"Rapid changes in the spinning speed of the thousands of centrifuges enriching uranium to weapons-grade can cause them to blow apart suddenly without the monitors detecting any malfunction. The Iranian operators first tried replacing the P1 and P2 centrifuges used at Natanz with the more advanced IR1 type, but got the same effect. They finally decided to shut the plant down until computer security experts purged it of the malworm. But then, when work was resumed Monday, about 5,000 of the 8,000 machines were found to be out of commission and the remaining 2,500-3,000 partially on the blink." - DEBKAfile

"...Ahmadinejad announced in November that unspecified malicious software sent by western enemies had affected Iran's centrifuges at its Natanz plant and "succeeded in creating problems for a limited number of our centrifuges." - Wired

We may never know. However, Tom Parker of Securicon offers some refined speculation in his recent BlackHat D.C. presentation (1/18/11). To paraphrase Parker, if this is state-sponsored, it's probably a smaller state with limited resources because the code isn't as good as we would expect of a super-power. Whoever it was had access to Siemens' controllers to practice on. It was likely that the code was developed by at least five people comprising at least two teams of varying skill levels, the command and control team being the weakest.

All things considered, some level of U.S./Israel involvement should not be ruled out at this point. If no state-sponsored, perhaps state-aware?

In any case, Stuxnet definitely raises the bar for future Cyberwarfare.

***Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.***


# Leveraging Strong Experience with the Best Industry and Security Standards

- Security and Compliance Assessment & GAP Analysis
- Governance, Risk Management
- Policy and Procedure Development
- Technical Control & Architecture Review
- Risk Assessment
- Security Architecture & Design
- Compliance Program Development
- IGT Support
- Infinium Back Office Support
- Project Management
- Network and Help Desk Support
- Systems Integration

Link Technologies helps to ensure compliance of IT and data security requirements such as Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX) and Nevada Gaming Board Minimum Internal Control Standards (MICS). Link Technologies is an approved QSA company with certified staff. So we have proven to successfully help our clients meet the requirements set out by the PCI DSS mandates or other compliance requirements while helping them manage their security risks. Our expert consultants look to fully understand the clients business first and then determine the risks and appropriate mitigation.

LINK TECHNOLOGIES

Las Vegas Office
9500 Hillwood Drive Suite 112
Las Vegas, Nevada 89134
Phone: (702) 233-8703

Reno Office
995 Forest Street
Reno, Nevada 89509
Phone: (775) 824-4545

Additional locations in:
Philadelphia
Washington D.C.
Los Angeles

Visit us online to learn more about what we can do for you!

www.LinkTechConsulting.com