http://www.worldsecuritynetwork.com/showArticle3.cfm?Article_ID=18540

Stuxnet - The Trojan Horse. A Noble Weapon?
written by: PJ Wilcox,
20-Feb-11

Stuxnet worm's true origins are exposed

- Virus intended as "weapon of peace"

- Origins date back over 30 years, not 2009 as estimated

- U.S., KGB, Israel, Canada, Australia and others have all had earlier versions

- Proliferation may continue undetectable with experts only having solved "false flags"

- Changes landscape of modern warfare as we know it

PJ Wilcox, author of the World Security Network:*"The malware worm may have started out as a logistical program, Promis. Then it morphed into an "Enhanced Promis" for intelligence work. It was subsequently altered for specific situations, given different names and sold to perhaps a dozen countries, worming its way around the world. In the process, rather than burrowing, the worm became like a centipede with hundreds of legs regenerating in different sizes and shapes, taking direction from its owners regarding objectives."*

It's breaking dawn by a beachside command center for Hezbollah. But already, the commander has been up for hours in anticipation of the day's work – the simultaneous annihilation of revered European cultural sites and the inner border of Israel. The former attack sites have been indiscriminately chosen to garner world attention. The latter would be retribution for, well, for just being. All the commander needs to do now is give the word.

He picks up the receiver of his impenetrable, mega-million-dollar communications system installed to withstand all but a nuclear war. But the receiver is silent, no dial tone. Dead. Impatient but unperturbed, he turns to his cell phone. No service. By now, he is on a rampage, waking up the entire installation with shouts of ineptitude. Others come to his aide, aimed at restoring lines. But they too encounter silence. No phones, no fax, no Internet. Back to the Middle Ages. There will be no war today. No missiles fired. Without communication, there is no relaying of orders. The best laid plans of sabotage gone astray.

An event like this did happen this past fall in the Mid-East, according to two deep, inside sources of mine. Except that there were actually five command centers, and all five went down simultaneously. There was still worse chaos, 40 minutes later, explosions ratcheting the air like a blitzkrieg, underground weapons caches exploding in place. The command centers knew the explosions were close, but with no communications, knew not where – they couldn't relay offensive orders, deploy defensive actions, or even discern what was going down.

A neighboring nation came to the rescue, their radar detecting enemy jets over Lebanon skies and scrambling its fighter jets. Except in truth, there were no enemy jets to be found, just sunny, cloudless skies. Much like communications at the command center, that neighboring air force's radar had been manipulated.

Off in a different country, in the land of an enemy combatant, there were wry smiles among those in the know. This had all been a long time coming. Not just years, but decades. Because they knew survival might come down to just such a day. And so they had planned well for their Trojan horse, the smallest, most microscopic of masquerades. The malware worm, Stuxnet.

Nineteen hours later, all communications order was miraculously restored in Beirut and radar resumed working. But there was then another type of silence at command and air control centers because one player in this game of chess had showed that it could start and stop all communications at the drop of a hat, and turn them back on at whim. A message that to others might be subtle is not subtle to a trained eye in war.

As they might say in War College, "We choose the time, the place, and the element." The element, in this case, was the worm, Stuxnet. And the message was clear: Any time, any place. Our choosing.

To some, the worm is a noble weapon, to the recipient, ignoble.

Some might find a noble weapon an oxymoron. But let me relay comments of Geir Lundestad, Secretary of the Norwegian Nobel Committee at an Oslo presentation attended by an associate of mine. Lundestad said the esteemed Nobel Peace Prize is sometimes awarded not for accomplishments toward peace, but as a deterrent to war. "The prize can actually influence outside events," he said. Lech Walesa said that he would not have achieved Solidarity's victory in Poland in 1989, had he not earlier received the Nobel Peace Prize. Likewise, East Timor winners said their prize in 1996 helped that country become independent. Lundestad said the Committee had "adapted the definition of peace. The Nobel Peace Prize is also a protective device." He said Committee members ask themselves, "What can we actually do for peace?"

And so now we have the worm opening undetectable doors not visible to the naked eye. But like the Nobel Peace Prize, the doors opened are with the ultimate goal being to deter war and maintain peace. The goal is to fight and win a war with no bloodshed, with few if any human casualties.

The worm, Stuxnet, is a Trojan horse said to have disabled Iran's nuclear weapons program. The New York Times said late last year, "Meanwhile, the search for other clues in the Stuxnet program continues — and so do the theories about its origins."

The Times updated their take on January 15, 2011 calling Stuxnet, "the most sophisticated cyberweapon ever deployed…experts who have picked apart the computer worm describe it as far more complex — and ingenious — than anything they had imagined when it began circulating around the world, unexplained, in mid-2009."

Other major news outlets report it as an attack that was the perfect storm leaving no fingerprints, or that it should have won "Person of the Year" for its impact on world events. Still others at first tried to decipher cryptic language within the worm, supposedly tied to this or that chapter of the bible. In other words, no one has much clue as to the true Stuxnet origin. That's because no one has been looking back far enough. As Santayana said, "Those who cannot remember the past are doomed to repeat it."

No one is looking back to a time in the mid-70s, when an obscure program called Promis first reared its head. Promis, according to sources, is at the root of Stuxnet. Promis was a computer program that promised to help US prosecutors track criminals and legal maneuverings through the system, "Prosecutor's Management Information System." The people-tracking software was later marketed by a firm named Inslaw, under the auspices of William Hamilton, a former NSA officer who still markets a version of the product today.

The Department of Justice became intrigued by Promis, seeing its potential for exorbitant legal case-management and provided funding for improvements. As Promis morphed, its capabilities refined, its natural alternative applications became self-evident: the worlds of intelligence, terrorists and targets.

Rafi Eitan, head of the Israeli Defense Ministry's Lekem in the early 1980s, a clandestine, scientific and technological intelligence unit, attended a presentation of Promis under an assumed name. He was so impressed with it that he obtained a copy – how, and whether legally, is another story. Suffice it to say that he especially saw its potential for tracking the spidery web of PLO installations around the world, at the time under Yasser Arafat, as well as tracking the leader himself. Eitan, however, wanted a "trapdoor", a built-in chip so that if Promis was later sold to other organizations, Israeli intelligence could track the information for which those entities might search. Big brother tracking little brother, or intelligence tracking of intelligence.

Boldly, Eitan then arranged for Arafat himself to buy the Promis program for his security needs, this according to author Gordon Thomas. But the trapdoor instead allowed Israeli intelligence to follow Arafat's aliases on the lam. You can run, but you can't hide from Promis. And here's where it gets really interesting.

By the late 1980s, Promis programs had been sold to Britain, Australia, South Korea and Canada. Allies harmless enough, right?

But then up next was the KGB. There are multiple claims as to who sold Promis to the Russians. Several, including a source of mine, said it was newspaper mogul Robert Maxwell in assistance to Israel. Another acquaintance, former double agent David Dastych (Polish intell working for the CIA during the Cold War) said that an American intelligence officer admitted to him, "Yes, we gave Promis to the Russians and Chinese to back door their intel. Worked like a charm." Both claims may overlap.

In fact, the KGB is said to have used Promis for over 15 years. At first, there was nothing to suspect since malicious malware had not really been coined. Few back then understood the power of the computer, and so the Trojan horse entered the realms of international espionage, the microscopic spy.

As former US Attorney General Elliot Richardson later said on Australia's TV show, A Current Affair, in 1990 regarding Promis, "The US Government had through clandestine means planted software on foreign intelligence agencies so the US would be better able, the phrase goes, to read their mail."

The only problem was the "blowback", David Dastych reported. "As we gave it to our enemies in order to back door them through the trap door in Promis, we left 64 federal agencies open in the US Government who also used Promis."

That's a big, "Whooops." An intelligence contact I know recently noted, "We opened all the cans of worms rather than just the *right* can of worms."

At least according to Dastych about that not-slight mishap, the information obtained far outweighed the damage done.The importance of the program's role was also pointed out in a WIRED expose in the '90s. It quoted an ex-Israeli spy, Ari Ben Menashe, as saying "PROMIS was a very big thing for us guys, a very, very big thing….The whole form of intelligence collection changed."

"This is a big worry for the future," warns Scott Borg, Director and Chief Economist of U.S. Cyber Consequences Unit, an independent, non-profit research institute. "We are entering a completely new defense era. If you have the tools like Stuxnet, why would you bother with missiles? Why bother invading with an army? The whole relationship between the military and society is going to have to be re-thought."

So you ask, what does all of this twisted espionage in the 1980s have to do with today's malware worm called Stuxnet? It is said of some nations and their causes that they do not plan for this generation or the next, but for hundreds of years, especially true if they are fighting for existentialism. Stuxnet is just such a case.

The malware worm may have started out as a logistical program, Promis. Then it morphed into an "Enhanced Promis" for intelligence work. It was subsequently altered for specific situations, given different names and sold to perhaps a dozen countries, worming its way around the world. In the process, rather than burrowing, the worm became like a centipede with hundreds of legs regenerating in different sizes and shapes, taking direction from its owners regarding objectives.

At issue, however, is who that current "owner" might be. Most fingers point to nations intent on halting Iran's nuclear weapons facilities, the US and Israel. But there is no dearth of suspects given the program's piracy over the years.

Both Russia and China have sold high-tech systems and weapons to Iran for years, and could have unwittingly been modern-day Typhoid Mary's carrying the worm to their recipients. In a game of highly sophisticated Clue, for example, Israel might

have sold Promis to the KGB; the KGB or its successors later sold critical systems to Iran; and then Iran built operations with a Trojan horse in place. Likewise, Chinese scientists tapped by Iran could have brought that country Promis, the gift that keeps giving.

It's a scintillating game of Clue with no sure culpability, no one to shoot, a war with no casualties. Nobel Peace Prize potential. Half of the world's computer security experts are still scratching their heads opining on this new worm, not realizing that Stuxnet is not "new" at all.

Said one publication, it was "like the arrival of an F-35 into a World War I battlefield." Another, "The timing is intriguing because a time stamp found in the Stuxnet program says it was created in January [2010], suggesting that any digital attack took place long before it was identified and began to attract global attention." Long before is an understatement.

One man who spends his days worrying about such worms is Scott Borg, Director and Chief Economist of U.S. Cyber Consequences Unit, an independent, non-profit research institute that assesses cyber attacks and counter-measures. He says that the phrase "worms" is grossly outdated.

"We're so far beyond worms," says Borg. "We're into big, complicated creatures."

He likens Stuxnet to the Velociraptor dinosaurs from Jurassic Park, intelligent, cunning, capable of hunting in groups till they find their prey. "Modern malware -- like Stuxnet -- will use any channel available to spread and search out its prey. If the target system isn't connected to the internet, the malware will migrate from device to device until it reaches the system it is looking for."

Once planted, the Stuxnet bosses never have to talk to it again; it operates totally on its own. Somewhere, someone just watches and waits. And, in the case of Iran, Stuxnet's target was very precise -- automation control facilities. Not just any control systems, but nuclear. So Stuxnet wormed its way around the world until as Borg says, "When it finds the system it meant to destroy, it *will* destroy it."

Some think Stuxnet was spread by international contractors moving between facilities. But they don't know about Promis.

What's odd to Borg, for example, is that Stuxnet included some features to help it avoid being detected, but not others. Stuxnet was designed to erase itself after each copy made four additional copies on different devices. In effect, Stuxnet was designed to have a limited number of children and to kill itself after its quota of kids. This would eliminate copies that had reproduced, but hadn't reached their target so that Stuxnet's trail would be minimized. But there was no limit on later descendants, so Stuxnet would eventually spread and almost certainly be detected. Why didn't its creators make Stuxnet eventually die, so it could covertly be used again in a different situation?

Borg offers some theories: the "attacker" was fairly desperate to reach the intended target; could not release Stuxnet very close to its intended target, hence the extra

children produced; had resources to burn; and, didn't care if Stuxnet were detected and received a great deal of attention.

"Sometimes we know who carried out an attack," adds Borg, "but it's usually from other intelligence."

One highly placed intelligence source I know, says we've hardly seen the last of Stuxnet, i.e. Promis. Sure, computer security experts found its vulnerabilities and have supposedly closed those exposures. But posed this source, "How do you know Stuxnet didn't show those vulnerabilities on purpose, a 'false flag', so everyone would go 'solve' those problems while Stuxnet moved on?" That source winked, *Gotcha.* Maybe in fact, Stuxnet's grandchildren are roaming the streets of the information superhighway as I write, ready to pounce on their next prey.

Dr. Peter Vincent Pry, a former CIA officer, now President of EMPACT America, a non-profit focused on electromagnetic pulse threats (EMPs) which have the potential to down power grids, thinks cyber threats are overblown at the risk of more probable, and more damaging, EMPs. Simply put, EMPs create a radio-frequency shockwave that zaps electronic fields of energy, burning out electrical systems such as computers, power grids, weaponry and communications. There's been some tug-of-war going on in Washington as to which threat is worse, EMPs or "cybergeddon".

Russia, for one, addressed significant cyber-risk by throwing out Promis with the bath water, choosing to re-construct their computer systems from scratch a decade or so ago, I'm told, rather than worry about generous gifts that keep giving.

But Stuxnet has also shown the civilized world the dangers of copycats. With the attention now drawn to the "good" that can be done by the likes of a Stuxnet, come the possibilities of future versions that might harm. The enormous physical power harnessed by some industrial facilities, for example, if unleashed in the wrong way by a worm could be astounding. Think of the dangers of opening a dam that should have been shut, or an oil pipeline backwashed into the sea. Nuclear reactors are just the half of it.

"There's no reason to keep the secret from the American people, or our own allies, because the bad guys are on to it. This is a big worry for the future," warns Borg. "We are entering a completely new defense era. If you have the tools like Stuxnet, why would you bother with missiles? Why bother invading with an army? The whole relationship between the military and society is going to have to be re-thought."

Without a doubt, it is a new day of warfare. And cybergeddon aside, Stuxnet remains at the forefront, one of the most amazingly sophisticated pieces of malware ever publicly recognized; it always did have promise.

So do we have to worry about world powers attacking each other's power grids with Stuxnet tools any time soon? Hardly, says Borg. "The last thing China or Russia wants is for our economy to take another dive. No one wants destabilization. But that doesn't mean they haven't planted malware programs for possible use at a future date."

And that's exactly what was done several decades ago with a promising new people-tracking program intended to stave off war, not start it. That brings us back to this weapon of peace, ever the more important as the Mid-East cracks at the seams. It also brings us back full circle to Beirut last October. Promis aka Stuxnet was at the core of the communications shutdown at command centers in Lebanon that day. This, confirmed by two extremely reliable, unrelated sources.

But Stuxnet only cleared the way in Beirut. The blasting of underground weapons caches that followed were achieved through electromagnetic pulses. The radar that went on the blink? Also electromagnetic pulses. So Stuxnet's purpose was like clearing obstructive land mines before doing battle.

A Tehran journal a decade ago put it this way, "…today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country." Sounds like wording for a Stuxnet how-to-manual.

Regardless, Stuxnet and EMPs make it exceedingly clear that in any future major war, there may be no images of Patton charging across Europe in tanks, no massive armies forging rivers. The war will be fought below the radar, both literally and figuratively, with a new era of weapons.

As for Stuxnet, the "newest" weapon in that arsenal -- or oldest depending how much you know – right now it could be on its way to a target near you. Jeffrey Carr, author of Inside Cyber Warfare acquiesces that possibility. "*No one* has a product that would have stopped the Stuxnet worm."

On that, Carr is undoubtedly correct. Because in one of the greatest whodunits in modern history, I know all the sleuths are looking in the wrong places. Rather than looking at where Stuxnet visited, they should be looking at where it came from, Promis. I just hope that the people that have Stuxnet are reasonable, either that, or they're our friends.