Iran's nuclear negotiator says U.S. involved in cyberattack

NBC News

updated 1/17/2011 6:42:31 PM

TEHRAN, Iran — Telegraphing Iran's negotiating stance entering key talks about its nuclear program in Turkey later this week, Tehran's chief negotiator is charging that the United States was involved in a cyberattack that he said disrupted a peaceful .program aimed at creating nuclear energy, not weapons
In an exclusive interview with Richard Engel, chief foreign correspondent for NBC News, this week in Tehran, Saed Jalilli said that Iran's investigation has determined that the U.S. was involved in the cyberattack using the Stuxnet computer worm, a virus which targeted centrifuges used to enrich uranium as part of Iran's nuclear .program

I have witnessed some documents that show ... their satisfaction in that (the U.S. was " .involved)," he said

Jalilli indicated, however, that the cyberattack was not as successful as some media .accounts have portrayed it

Those who have done that could see now that they were not successful in that and we " are following our success," he said. He added that Iran is not the only country vulnerable to cyberattacks, as evidenced by the WikiLeaks release of U.S. diplomatic cables. "They are also weak and vulnerable," he said of the United States.

http://www.msnbc.msn.com/id/41121090/ns/world_news-mideastn_africa/

The Limits of Stuxnet

A neat computer trick won't stop Iran from getting the bomb.

By BRET STEPHENS JANUARY 18, 2011

Long before there was the Stuxnet computer worm there was the "Farewell" spy dossier.

In 1980, a KGB officer named Vladimir Vetrov began passing secrets to French intelligence. Vetrov was in a position to know the names of a network of Soviet agents (known as Line X) involved in pilfering capitalist technologies, which is how Moscow managed to stay nearly competitive with the West.

Col. Vetrov's Farewell dossier, as the French code-named it, eventually arrived at the desk of an American National Security Council official named Gus Weiss. It was Weiss who suggested to then-CIA director Bill Casey that the West not roll up the spy network right away, but rather that it be played for greater stakes.

"I proposed using the Farewell material to feed or play back the products sought by Line X," he later wrote in an unclassified CIA history, "but these would come from our own sources and would have been 'improved'. . . . Contrived computer chips found their way into Soviet military equipment, flawed turbines were installed on a gas pipeline. . . . The Pentagon introduced misleading information pertinent to stealth aircraft, space defense, and tactical aircraft. The Soviet Space Shuttle was a rejected NASA design."

How well did the plan work? In June 1982, one of Casey's "improved" computer control systems, containing a Trojan horse in its software, caused the trans-Siberian gas pipeline to explode. U.S. spy satellites captured images of what was described by former Air Force Secretary Thomas Reed as "the most monumental non-nuclear explosion and fire ever seen from space."

Thus did the Soviet Union end up on the ash-heap of history.

Well, not really. But the story of the Farewell dossier is worth recalling amid the hoopla connected to Stuxnet, the ingenious computer worm, likely of U.S.-Israeli design, that seems to have hobbled the Iranian nuclear program. Meir Dagan, the outgoing head of Israel's Mossad, said recently that Iran would not be able to produce a bomb until 2015, a date much further off than the 12 to 18 month timeframe Israeli officials were offering as recently as last year. U.N. nuclear inspectors confirm that Iran has been forced to de-activate 984 uranium-spinning centrifuges. Even Mahmoud Ahmadinejad says Stuxnet has caused "minor problems"—a major admission.

All of this is terrific news and a credit to Stuxnet's authors. It seems to have stopped the further expansion of Iran's enrichment activities. It will also likely require Iran to replace its Western-made computer control systems even as the international sanctions regime makes them increasingly difficult to acquire.

And yet the Iranian nuclear program carries on. Stuxnet appears to have hit Iran sometime in 2009. As of last November, U.N. inspectors reported that Iran continued to enrich uranium in as many as 4,816 centrifuges, and that it had produced more than three tons of reactor-grade uranium. That stockpile already suffices, with further enrichment, for two or possibly three bombs worth of fissile material.

Nor can it be much comfort that even as Stuxnet hit Iran, North Korea began enriching uranium in a state-of-the-art facility, likely with Chinese help. Pyongyang has already demonstrated its willingness to build a secret reactor for Syria. So why not export enriched uranium to Iran, a country with which it already does a thriving trade in WMD-related technologies and to which it is deeply in debt? Merely stamp the words "Handle With Care" on the crate, and the flight from Pyongyang to Tehran takes maybe 10 hours.

Iran is also not likely to be fooled again this way, making Stuxnet, or some variant of it, its own kind of one-hit wonder. Qualified nuclear engineers may be hard to come by, but computer forensics experts

aren't, even for a country like Iran. The next time Israel or the U.S. tries to stop Iran's nuclear advances, the means aren't likely to be as targeted, or as bloodless.

Which brings us back to the Farewell dossier. Despite the CIA's sabotage, the trans-Siberian pipeline was commissioned just two years later. A bigger hit to Moscow was the expulsion of 200 Line X officers from the West, which the Soviets avenged by executing Vetrov in 1983.

But as Weiss noted in his hitory, the real hammer blows came in the form of Reagan's "evil empire" speech and the SDI initiative, which caused the Soviet military to demand budgets the system couldn't afford. Paul Volcker's tight money policies, which "led to a fall in gold and primary product prices, sources of Soviet foreign exchange," also played a key role.

And so Iran has fallen for a neat computer trick. That may be a source of satisfaction in Jerusalem, Washington and even Riyadh. But it cannot be a cause for complacency. Wars are never won by covert means alone. That's as true for Iran today as it was in Cold War days of yore.

http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html

The New York Times

January 15, 2011

Israeli Test on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER

*This article is by **William J. Broad**, **John Markoff** and **David E. Sanger**.*

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms.

“To check out the worm, you have to know the machines,” said an American expert on nuclear intelligence. “The reason the worm has been effective is that the Israelis tried it out.”

Though American and Israeli officials refuse to talk publicly about what goes on at Dimona, the operations there, as well as related efforts in the United States, are among the newest and strongest clues suggesting that the virus was designed as an American-Israeli project to sabotage the Iranian program.

In recent days, the retiring chief of Israel’s Mossad intelligence agency, Meir Dagan, and Secretary of State Hillary Rodham Clinton separately announced that they believed Iran’s efforts had been set back by several years. Mrs. Clinton cited American-led sanctions, which have hurt Iran’s ability to buy components and do business around the world.

The gruff Mr. Dagan, whose organization has been accused by Iran of being behind the deaths of several Iranian scientists, told the Israeli Knesset in recent days that Iran had run into technological difficulties that could delay a bomb until 2015. That represented a sharp reversal from Israel’s long-held argument that Iran was on the cusp of success.

The biggest single factor in putting time on the nuclear clock appears to be Stuxnet, the most sophisticated cyberweapon ever deployed.

In interviews over the past three months in the United States and Europe, 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.

Many mysteries remain, chief among them, exactly who constructed a computer worm that appears to have several authors on several continents. But the digital trail is littered with intriguing bits of evidence.

In early 2008 the German company Siemens cooperated with one of the United States’ premier national laboratories, in Idaho, to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world — and that American intelligence agencies have identified as key equipment in Iran’s enrichment facilities.

Seimens says that program was part of routine efforts to secure its products against cyberattacks. Nonetheless, it gave the Idaho National Laboratory — which is part of the Energy Department, responsible for America’s nuclear arms — the chance to identify well-hidden holes in the Siemens systems that were exploited the next year by Stuxnet.

The worm itself now appears to have included two major components. One was designed to send Iran’s nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played

those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.

"It's like a playbook," said Ralph Langner, an independent computer security expert in Hamburg, Germany, who was among the first to decode Stuxnet. "Anyone who looks at it carefully can build something like it." Mr. Langner is among the experts who expressed fear that the attack had legitimized a new form of industrial warfare, one to which the United States is also highly vulnerable.

Officially, neither American nor Israeli officials will even utter the name of the malicious computer program, much less describe any role in designing it.

But Israeli officials grin widely when asked about its effects. Mr. Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sidestepped a Stuxnet question at a recent conference about Iran, but added with a smile: "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."

In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported. That may explain why Mrs. Clinton provided her public assessment while traveling in the Middle East last week.

By the accounts of a number of computer scientists, nuclear enrichment experts and former officials, the covert race to create Stuxnet was a joint project between the Americans and the Israelis, with some help, knowing or unknowing, from the Germans and the British.

The project's political origins can be found in the last months of the Bush administration. In January 2009, The New York Times reported that Mr. Bush authorized a covert program to undermine the electrical and computer systems around Natanz, Iran's major enrichment center. President Obama, first briefed on the program even before taking office, sped it up, according to officials familiar with the administration's Iran strategy. So did the Israelis, other officials said. Israel has long been seeking a way to cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in 1981 and Syria in 2007.

Two years ago, when Israel still thought its only solution was a military one and approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its

officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down.

Now, Mr. Dagan's statement suggests that Israel believes it has gained at least that much time, without mounting an attack. So does the Obama administration.

For years, Washington's approach to Tehran's program has been one of attempting "to put time on the clock," a senior administration official said, even while refusing to discuss Stuxnet. "And now, we have a bit more."

Finding Weaknesses

Paranoia helped, as it turns out.

Years before the worm hit Iran, Washington had become deeply worried about the vulnerability of the millions of computers that run everything in the United States from bank transactions to the power grid.

Computers known as controllers run all kinds of industrial machinery. By early 2008, the Department of Homeland Security had teamed up with the Idaho National Laboratory to study a widely used Siemens controller known as P.C.S.-7, for Process Control System 7. Its complex software, called Step 7, can run whole symphonies of industrial instruments, sensors and machines.

The vulnerability of the controller to cyberattack was an open secret. In July 2008, the Idaho lab and Siemens teamed up on a PowerPoint presentation on the controller's vulnerabilities that was made to a conference in Chicago at Navy Pier, a top tourist attraction.

"Goal is for attacker to gain control," the July paper said in describing the many kinds of maneuvers that could exploit system holes. The paper was 62 pages long, including pictures of the controllers as they were examined and tested in Idaho.

In a statement on Friday, the Idaho National Laboratory confirmed that it formed a partnership with Siemens but said it was one of many with manufacturers to identify cybervulnerabilities. It argued that the report did not detail specific flaws that attackers could exploit. But it also said it could not comment on the laboratory's classified missions, leaving unanswered the question of whether it passed what it learned about the Siemens systems to other parts of the nation's intelligence apparatus.

The presentation at the Chicago conference, which recently disappeared from a Siemens Web site, never discussed specific places where the machines were used.

But Washington knew. The controllers were critical to operations at Natanz, a sprawling enrichment site in the desert. "If you look for the weak links in the system," said one former American official, "this one jumps out."

Controllers, and the electrical regulators they run, became a focus of sanctions efforts. The trove of State Department cables made public by WikiLeaks describes urgent efforts in April 2009 to stop a shipment of Siemens controllers, contained in 111 boxes at the port of Dubai, in the United Arab Emirates. They were headed for Iran, one cable said, and were meant to control "uranium enrichment cascades" — the term for groups of spinning centrifuges.

Subsequent cables showed that the United Arab Emirates blocked the transfer of the Siemens computers across the Strait of Hormuz to Bandar Abbas, a major Iranian port.

Only months later, in June, Stuxnet began to pop up around the globe. The Symantec Corporation, a maker of computer security software and services based in Silicon Valley, snared it in a global malware collection system. The worm hit primarily inside Iran, Symantec reported, but also in time appeared in India, Indonesia and other countries.

But unlike most malware, it seemed to be doing little harm. It did not slow computer networks or wreak general havoc.

That deepened the mystery.

A 'Dual Warhead'

No one was more intrigued than Mr. Langner, a former psychologist who runs a small computer security company in a suburb of Hamburg. Eager to design protective software for his clients, he had his five employees focus on picking apart the code and running it on the series of Siemens controllers neatly stacked in racks, their lights blinking.

He quickly discovered that the worm only kicked into gear when it detected the presence of a specific configuration of controllers, running a set of processes that appear to exist only in a centrifuge plant. "The attackers took great care to make sure that only their designated targets were hit," he said. "It was a marksman's job."

For example, one small section of the code appears designed to send commands to 984 machines linked together.

Curiously, when international inspectors visited Natanz in late 2009, they found that the Iranians had taken out of service a total of exactly 984 machines that had been running the previous summer.

But as Mr. Langner kept peeling back the layers, he found more — what he calls the "dual warhead." One part of the program is designed to lie dormant for long periods, then speed up the machines so that the spinning rotors in the centrifuges wobble and then destroy themselves. Another part, called a "man in the middle" in the computer world, sends out those false sensor signals to make the system believe

everything is running smoothly. That prevents a safety system from kicking in, which would shut down the plant before it could self-destruct.

“Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept,” Mr. Langner later wrote. “It is about destroying its targets with utmost determination in military style.”

This was not the work of hackers, he quickly concluded. It had to be the work of someone who knew his way around the specific quirks of the Siemens controllers and had an intimate understanding of exactly how the Iranians had designed their enrichment operations.

In fact, the Americans and the Israelis had a pretty good idea.

Testing the Worm

Perhaps the most secretive part of the Stuxnet story centers on how the theory of cyberdestruction was tested on enrichment machines to make sure the malicious software did its intended job.

The account starts in the Netherlands. In the 1970s, the Dutch designed a tall, thin machine for enriching uranium. As is well known, A. Q. Khan, a Pakistani metallurgist working for the Dutch, stole the design and in 1976 fled to Pakistan.

The resulting machine, known as the P-1, for Pakistan’s first-generation centrifuge, helped the country get the bomb. And when Dr. Khan later founded an atomic black market, he illegally sold P-1’s to Iran, Libya, and North Korea.

The P-1 is more than six feet tall. Inside, a rotor of aluminum spins uranium gas to blinding speeds, slowly concentrating the rare part of the uranium that can fuel reactors and bombs.

How and when Israel obtained this kind of first-generation centrifuge remains unclear, whether from Europe, or the Khan network, or by other means. But nuclear experts agree that Dimona came to hold row upon row of spinning centrifuges.

“They’ve long been an important part of the complex,” said Avner Cohen, author of “The Worst-Kept Secret” (2010), a book about the Israeli bomb program, and a senior fellow at the Monterey Institute of International Studies. He added that Israeli intelligence had asked retired senior Dimona personnel to help on the Iranian issue, and that some apparently came from the enrichment program.

“I have no specific knowledge,” Dr. Cohen said of Israel and the Stuxnet worm. “But I see a strong Israeli signature and think that the centrifuge knowledge was critical.”

Another clue involves the United States. It obtained a cache of P-1's after Libya gave up its nuclear program in late 2003, and the machines were sent to the Oak Ridge National Laboratory in Tennessee, another arm of the Energy Department.

By early 2004, a variety of federal and private nuclear experts assembled by the Central Intelligence Agency were calling for the United States to build a secret plant where scientists could set up the P-1's and study their vulnerabilities. "The notion of a test bed was really pushed," a participant at the C.I.A. meeting recalled.

The resulting plant, nuclear experts said last week, may also have played a role in Stuxnet testing.

But the United States and its allies ran into the same problem the Iranians have grappled with: the P-1 is a balky, badly designed machine. When the Tennessee laboratory shipped some of its P-1's to England, in hopes of working with the British on a program of general P-1 testing, they stumbled, according to nuclear experts.

"They failed hopelessly," one recalled, saying that the machines proved too crude and temperamental to spin properly.

Dr. Cohen said his sources told him that Israel succeeded — with great difficulty — in mastering the centrifuge technology. And the American expert in nuclear intelligence, who spoke on the condition of anonymity, said the Israelis used machines of the P-1 style to test the effectiveness of Stuxnet.

The expert added that Israel worked in collaboration with the United States in targeting Iran, but that Washington was eager for "plausible deniability."

In November, the Iranian president, Mahmoud Ahmadinejad, broke the country's silence about the worm's impact on its enrichment program, saying a cyberattack had caused "minor problems with some of our centrifuges." Fortunately, he added, "our experts discovered it."

The most detailed portrait of the damage comes from the Institute for Science and International Security, a private group in Washington. Last month, it issued a lengthy Stuxnet report that said Iran's P-1 machines at Natanz suffered a series of failures in mid- to late 2009 that culminated in technicians taking 984 machines out of action.

The report called the failures "a major problem" and identified Stuxnet as the likely culprit.

Stuxnet is not the only blow to Iran. Sanctions have hurt its effort to build more advanced (and less temperamental) centrifuges. And last January, and again in November, two scientists who were believed to be central to the nuclear program were killed in Tehran.

The man widely believed to be responsible for much of Iran's program, Mohsen Fakrizadeh, a college professor, has been hidden away by the Iranians, who know he is high on the target list.

Publicly, Israeli officials make no explicit ties between Stuxnet and Iran's problems. But in recent weeks, they have given revised and surprisingly upbeat assessments of Tehran's nuclear status.

"A number of technological challenges and difficulties" have beset Iran's program, Moshe Yaalon, Israel's minister of strategic affairs, told Israeli public radio late last month.

The troubles, he added, "have postponed the timetable."

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Schneier on Security

More Stuxnet News

This long New York Times article includes some interesting revelations. The article claims that Stuxnet was a joint Israeli-American project, and that its effectiveness was tested on live equipment: "Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium."

The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

My two previous Stuxnet posts. And an alternate theory: The Chinese did it.

Stuxnet's Finnish-Chinese Connection

Dec. 14 2010 Posted by Jeffrey Carr

I recently wrote a white paper entitled "Dragons, Tigers, Pearls, and Yellowcake" in which I proposed four alternative scenarios for the Stuxnet worm other than the commonly held assumption that it was Israel or the U.S. targeting Iran's Bushehr or Natanz facilities. During the course of my research for that paper, I uncovered a connection between two of the key players in the Stuxnet drama: Vacon, the Finnish manufacturer of one of two frequency converter drives targeted by this malware; and RealTek, who's digital certificate was stolen and used to smooth the way for the worm to be loaded onto a

Windows host without raising any alarms. A third important piece of the puzzle, which I'll discuss later in this article, directly connects a Chinese antivirus company which writes their own viruses with the Stuxnet worm.

Most people who have followed the Stuxnet investigation know that the international headquarters for Vacon is in Finland, but surprisingly, Finland isn't where Vacon's frequency converter drives are manufactured. Vacon's manufacturing plant is actually located in the Peoples Republic of China (PRC) under the name Vacon Suzhou Drives Co. Ltd., located at 11A, Suchun Industrial Square 428# Xinglong Street, SIP Suzhou 215126 China.

Vacon isn't the only company involved with Stuxnet that has a Chinese connection. The first genuine digital certificate used by Stuxnet developers was from RealTek Semiconductor Corp., a Taiwanese company which has a subsidiary in (of all places) Suzhou under the name Realsil Microelectronics, Inc. (450 Shenhu Road, Suzhou Industrial Park, Suzhou 215021 Jiangsu Province, China).

The question, of course, is what, if anything, does this say about China's possible role as the source of the Stuxnet worm. There are scenarios under which China would benefit such as the rare-earths scenario that I presented in my white paper, however there's a lack of data on mining failures that can be attributed to Stuxnet. The closest that anyone has come to identifying compromised operations is at Natanz however their centrifuge failures go back several years according to this February, 2010 report by ISIS, while the earliest Stuxnet sample seen by Symantec's researchers was June, 2009 and that's before it had signed driver files or exploited the remote code execution vulnerability that appeared in January, 2010 and March, 2010 respectively. Natanz may very well have been the target of an earlier cyber attack, or even multiple attacks, which had nothing to do with Stuxnet.

Does China Benefit By Attacking Natanz?

In 2008, China decided to assist the IAEA inspectors after it learned that Iran was in possession of blueprints to shape uranium metal into warheads, according to this article in The Telegraph. That same article discloses that Chinese designs for centrifuges were discovered in Iran, supplied via Pakistan's AQ Khan.

On April 13, 2010, Beijing reiterated its opposition to Iran's goal to develop nuclear weapons capabilities while stating that sanctions against Iran would be counter-productive. In other words, the PRC wanted to support its third largest supplier of oil (after Saudi Arabia and Angola) while at the same time seeking ways to get Iran to stop its uranium fuel enrichment program. What better way to accomplish that goal than by covertly creating a virus that will sabotage Natanz' centrifuges in a way that simulates mechanical failure while overtly supporting the Iranian government by opposing sanctions pushed by the U.S. It's both simple and elegant. Even if the worm was discovered before it accomplished its

mission, who would blame China, Iran's strongest ally, when the most obvious culprits would be Israel and the U.S.?

Reviewing The Evidence

China has an intimate knowledge of Iran's centrifuges since, according to one source quoted above, they're of Chinese design.

China has better access than any other country to manufacturing plans for the Vacon frequency converter drive made by Vacon's Suzhou facility and specifically targeted by the Stuxnet worm (along with an Iranian company's drive). Furthermore, in March 2010, China's Customs ministry started an audit at Vacon's Suzhou facility and took two employees into custody thereby providing further access to Vacon's manufacturing specifications under cover of an active investigation.

China has better access than any other country to RealTek's digital certificates through it's Realsil office in Suzhou and, secondarily, to JMicron's office in Taiwan.

China has direct access to Windows source code, which would explain how a malware team could create 4 key zero day vulnerabilities for Windows when most hackers find it challenging to develop even one.

There were no instances of Stuxnet infections in the PRC until very late which never made sense to me, particularly when Siemens software is pervasive throughout China's power installations. Then, almost as an after-thought and over three months from the time the virus was first discovered, Chinese media reported one million infections, and here's where the evidence becomes really interesting.

That report originated with a Chinese antivirus company called Rising International, who we now know colluded with an official in Beijing's Public Security Bureau to make announcements encouraging Chinese citizens to download AV software from Rising International (RI) to fight a new virus that RI had secretly created in its own lab. Considering this new information, RI's Stuxnet announcement sounds more like a CYA strategy from the worm's originators than anything else.

In Summary

The conventional wisdom on which nation state was responsible for the Stuxnet worm has relentlessly pointed the finger at Israel or the United States almost from day one of the worm's discovery. No other scenarios were discussed or even considered with the exception of my own conjecture about India's INSAT-4b satellite failure and Britain's Heysham 1 nuclear plant shutdown, and then my white paper proposing 4 additional alternative scenarios; all of which were my way of trying (and failing) to expand the discussion beyond Israel and Iran. The appeal of a U.S. or Israeli cyber attack against first Bushehr, then Natanz, was just too good to pass up even though there was no hard evidence and very slim circumstantial evidence to support a case for either country. The best that Ralph Langner, CEO of

Langner Communications (and the leading evangelist for this scenario) could point to was an obscure Hebrew word for Myrtus and a biblical reference for a date found in the malware that pertained to Persia; both of which could have been explained in a half dozen alternate ways having nothing to do with either Israel or the U.S.

As far as China goes, I've identified 5 distinct ties to Stuxnet that are unique to China as well as provided a rationale for the attack which fits China's unique role as Iran's ally and customer, while opposing Iran's fuel enrichment plans. There's still a distinct lack of information on any other facilities that suffered damage, and no good explanations for why there was such massive collateral damage across dozens of countries if only one or two facilities in one nation state were the targets however based solely on the known facts, I consider China to be the most likely candidate for Stuxnet's origin.

http://blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

October 7, 2010

Stuxnet

Computer security experts are often surprised at which stories get picked up by the mainstream media. Sometimes it makes no sense. Why this particular data breach, vulnerability, or worm and not others? Sometimes it's obvious. In the case of Stuxnet, there's a great story.

As the story goes, the Stuxnet worm was designed and released by a government--the U.S. and Israel are the most common suspects--specifically to attack the Bushehr nuclear power plant in Iran. How could anyone not report that? It combines computer attacks, nuclear power, spy agencies and a country that's a pariah to much of the world. The only problem with the story is that it's almost entirely speculation.

Here's what we do know: Stuxnet is an Internet worm that infects Windows computers. It primarily spreads via USB sticks, which allows it to get into computers and networks not normally connected to the Internet. Once inside a network, it uses a variety of mechanisms to propagate to other machines within that network and gain privilege once it has infected those machines. These mechanisms include both known and patched vulnerabilities, and four "zero-day exploits": vulnerabilities that were unknown and unpatched when the worm was released. (All the infection vulnerabilities have since been patched.)

Stuxnet doesn't actually do anything on those infected Windows computers, because they're not the real target. What Stuxnet looks for is a particular model of Programmable Logic Controller (PLC) made by Siemens (the press often refers to these as SCADA systems, which is technically incorrect). These are small embedded industrial control systems that run all sorts of automated processes: on factory floors, in chemical plants, in oil refineries, at pipelines--and, yes, in nuclear power plants. These PLCs are often controlled by computers, and Stuxnet looks for Siemens SIMATIC WinCC/Step 7 controller software.

If it doesn't find one, it does nothing. If it does, it infects it using yet another unknown and unpatched vulnerability, this one in the controller software. Then it reads and changes particular bits of data in the controlled PLCs. It's impossible to predict the effects of this without knowing what the PLC is doing and how it is programmed, and that programming can be unique based on the application. But the changes are very specific, leading many to believe that Stuxnet is targeting a specific PLC, or a specific group of PLCs, performing a specific function in a specific location--and that Stuxnet's authors knew exactly what they were targeting.

It's already infected more than 50,000 Windows computers, and Siemens has reported 14 infected control systems, many in Germany. (These numbers were certainly out of date as soon as I typed them.) We don't know of any physical damage Stuxnet has caused, although there are rumors that it was responsible for the failure of India's INSAT-4B satellite in July. We believe that it did infect the Bushehr plant.

All the anti-virus programs detect and remove Stuxnet from Windows systems.

Stuxnet was first discovered in late June, although there's speculation that it was released a year earlier. As worms go, it's very complex and got more complex over time. In addition to the multiple vulnerabilities that it exploits, it installs its own driver into Windows. These have to be signed, of course, but Stuxnet used a stolen legitimate certificate. Interestingly, the stolen certificate was revoked on July 16, and a Stuxnet variant with a different stolen certificate was discovered on July 17.

Over time the attackers swapped out modules that didn't work and replaced them with new ones--perhaps as Stuxnet made its way to its intended target. Those certificates first appeared in January. USB propagation, in March.

Stuxnet has two ways to update itself. It checks back to two control servers, one in Malaysia and the other in Denmark, but also uses a peer-to-peer update system: When two Stuxnet infections encounter each other, they compare versions and make sure they both have the most recent one. It also has a kill date of June 24, 2012. On that date, the worm will stop spreading and delete itself.

We don't know who wrote Stuxnet. We don't know why. We don't know what the target is, or if Stuxnet reached it. But you can see why there is so much speculation that it was created by a government.

Stuxnet doesn't act like a criminal worm. It doesn't spread indiscriminately. It doesn't steal credit card information or account login credentials. It doesn't herd infected computers into a botnet. It uses multiple zero-day vulnerabilities. A criminal group would be smarter to create different worm variants and use one in each. Stuxnet performs sabotage. It doesn't threaten sabotage, like a criminal organization intent on extortion might.

Stuxnet was expensive to create. Estimates are that it took 8 to 10 people six months to write. There's also the lab setup--surely any organization that goes to all this trouble would test the thing before releasing it--and the intelligence gathering to know exactly how to target it. Additionally, zero-day exploits are valuable. They're hard to find, and they can only be used once. Whoever wrote Stuxnet was willing to spend a lot of money to ensure that whatever job it was intended to do would be done.

None of this points to the Bushehr nuclear power plant in Iran, though. Best I can tell, this rumor was started by Ralph Langner, a security researcher from Germany. He labeled his theory "highly speculative," and based it primarily on the facts that Iran had an unusually high number of infections (the rumor that it had the most infections of any country seems not to be true), that the Bushehr nuclear plant is a juicy target, and that some of the other countries with high infection rates--India, Indonesia, and Pakistan--are countries where the same Russian contractor involved in Bushehr is also involved. This rumor moved into the computer press and then into the mainstream press, where it became the accepted story, without any of the original caveats.

Once a theory takes hold, though, it's easy to find more evidence. The word "myrtus" appears in the worm: an artifact that the compiler left, possibly by accident. That's the myrtle plant. Of course, that doesn't mean that druids wrote Stuxnet. According to the story, it refers to Queen Esther, also known as Hadassah; she saved the Persian Jews from genocide in the 4th century B.C. "Hadassah" means "myrtle" in Hebrew.

Stuxnet also sets a registry value of "19790509" to alert new copies of Stuxnet that the computer has already been infected. It's rather obviously a date, but instead of looking at the gazillion things--large and small--that happened on that the date, the story insists it refers to the date Persian Jew Habib Elghanain was executed in Tehran for spying for Israel.

Sure, these markers could point to Israel as the author. On the other hand, Stuxnet's authors were uncommonly thorough about not leaving clues in their code; the markers could have been deliberately planted by someone who wanted to frame Israel. Or they could have been deliberately planted by Israel, who wanted us to think they were planted by someone who wanted to frame Israel. Once you start walking down this road, it's impossible to know when to stop.

Another number found in Stuxnet is 0xDEADF007. Perhaps that means "Dead Fool" or "Dead Foot," a term that refers to an airplane engine failure. Perhaps this means Stuxnet is trying to cause the targeted system to fail. Or perhaps not. Still, a targeted worm designed to cause a specific sabotage seems to be the most likely explanation.

If that's the case, why is Stuxnet so sloppily targeted? Why doesn't Stuxnet erase itself when it realizes it's not in the targeted network? When it infects a network via USB stick, it's supposed to only spread to three additional computers and to erase itself after 21 days--but it doesn't do that. A mistake in

programming, or a feature in the code not enabled? Maybe we're not supposed to reverse engineer the target. By allowing Stuxnet to spread globally, its authors committed collateral damage worldwide. From a foreign policy perspective, that seems dumb. But maybe Stuxnet's authors didn't care.

My guess is that Stuxnet's authors, and its target, will forever remain a mystery.

This essay originally appeared *on Forbes.com*.

My alternate explanations for Stuxnet were cut from the essay. Here they are:

A research project that got out of control. Researchers have accidentally released worms before. But given the press, and the fact that any researcher working on something like this would be talking to friends, colleagues, and his advisor, I would expect someone to have outed him by now, especially if it was done by a team.

A criminal worm designed to demonstrate a capability. Sure, that's possible. Stuxnet could be a prelude to extortion. But I think a cheaper demonstration would be just as effective. Then again, maybe not.

A message. It's hard to speculate any further, because we don't know who the message is for, or its context. Presumably the intended recipient would know. Maybe it's a "look what we can do" message. Or an "if you don't listen to us, we'll do worse next time" message. Again, it's a very expensive message, but maybe one of the pieces of the message is "we have so many resources that we can burn four or five man-years of effort and four zero-day vulnerabilities just for the fun of it." If that message were for me, I'd be impressed.

A worm released by the U.S. military to scare the government into giving it more budget and power over cybersecurity. Nah, that sort of conspiracy is much more common in fiction than in real life.

Note that some of these alternate explanations overlap.

EDITED TO ADD (10/7): Symantec published a very detailed analysis. It seems like one of the zero-day vulnerabilities wasn't a zero-day after all. Good CNet article. More speculation, without any evidence. Decent debunking. Alternate theory, that the target was the uranium centrifuges in Natanz, Iran.

Posted on October 7, 2010 at 9:56 AM • 145 Comments

http://www.schneier.com/blog/archives/2010/10/stuxnet.html