

Stuxnet: From Iran to Your Organization?

Iranian nuclear facilities, zero-day exploits, secret operatives, and nation-state government involvement sounds more like a spy novel rather than the elements involved in a piece of malware. Stuxnet, the most researched and analyzed malware ever, is still being studied and discussed in security circles around the world even though it was discovered more than a year ago.

You most likely don't operate a nuclear facility, so why should you even care about a piece of software that targeted specific centrifuge models in specific nuclear plants in another part of the world? Simply put, Stuxnet made cyber-dreams reality and changed the security world forever.

Stuxnet was a targeted attack on five different organizations in June 2009, July 2009, March 2010, April 2010, and May 2010; all the targeted organizations have a presence in Iran. The targeting of

specific organizations is what sets Stuxnet apart from the traditional definition of an advanced persistent threat (APT).

What we generally think of as APT, notably the 2010 attacks on Google, Adobe, Juniper, Rackspace and others exploited the same zero-day IE vulnerability, employing the same techniques against multiple organizations in an attempt to steal their source code. The attacks were relatively broad-based and were duplicated against a number of targets.



Continued on page 2

The LastPass Breach: A very valuable cookie jar



AAbout 4 hours before this newsletter went to print, LastPass, the online password management company, announced they had seen anomalous network traffic coming from some of their servers and suspect they are the victim of a data breach. Marketed as the "last password you'll ever need", LastPass stores millions of passwords in the cloud and encrypts those passwords with a master password. The passwords LastPass protects include small business bank account logins. LastPass is requesting all users to reset their master password.

While this type of breach normally would fly under the radar as no credit cards are involved, no identity theft, and doesn't involve a big name brand like Sony, I think this attack could be even more important than the Sony breach in April 2011 which may effect 25 million people. Lastpass is the simplest form of multi-tenant cloud architecture. Multi-tenant means different types of users data is stored in the same location; although, the users cannot access each other's data. Multi-tenant architectures enable high maintenance services for a low cost.

The LastPass process is simple. Create a blob of data, store passwords and usernames within the blob, and encrypt the blob so that only the master password can access it. Not even Lastpass support can access the blob since they don't know the master password.

So, if Lastpass couldn't get the most simplistic cloud architecture secured properly, what hope do other cloud vendors have? All cloud vendors have to centralize their data for cost and management reasons but centralization creates additional risk which requires additional controls above and beyond what would be required if only one set of data was being stored. It appears LastPass may not have these additional controls.

For example, let's look at tokenization, the concept of replacing a credit card number with a unique randomly generated string that has no value – a token. When a retailer like Starbucks needs to store a credit card number, the retailer instead stores the token so that only the merchant

continued on page 2

Inside this Issue

Stuxnet: From Iran to Your Organization — 1

The LastPass Breach: A very valuable cookie jar — 1

The CEO Corner — 2
Michael Davis shares his thoughts

Safety & Security — **Insert**
for the Business Professional Traveling Abroad.

Monthly Special — 3
FREE Executive Briefing

Top 12 Graduation Gift Ideas — 3

Events — 3

Stuxnet: From Iran to Your Organization.

continued from page 1

Stuxnet, on the other hand, was a highly sophisticated, well-financed custom-designed attack created, apparently, for the single purpose of disrupting the production of enriched uranium in Iran. Think of traditional APT as a machine gun, which is aimed at multiple targets within a certain field of fire, vs. Stuxnet, a heat-seeking GPS-guided missile.

Stuxnet used a variety of innovative methods to infect, propagate, and hide itself. For a full analysis of Stuxnet, request our recent report "Stuxnet Reality-Check : A Practical Guide to a Unique Attack Tool", by contacting us and learn exactly how the innovative methods worked.

The real question in the end though is simple: Did it work? Public data that is available about Iran's nuclear program such as the amount of uranium enriched shows that Stuxnet was not very effective in slowing down Iran's uranium enrichment operations. The International Atomic Energy Agency findings show that the groups of centrifuges, called "cascades", that were operational, enriching uranium, for periods in 2009 and 2010 were normal and no excessive downtime was identified; but Iran did publicly state some software caused problems in their Nuclear facilities.

By no means should Stuxnet be top of mind in your security program however. Chances are your mind is focused on the things that most of our clients are concerned about: negligent insiders, insecure applications and malware/attackers.

But, if you want to take away some additional defenses you could use to help protect against a Stuxnet like threat, here are two tips from our security team:

Use 64-bit Operations Systems

We are not necessarily advocating a wholesale switch to 64-bit operating systems but, for the short-term foreseeable future, you can reduce your risk by using 64-bit operating systems and disabling the capability of running 32-bit applications because most exploits and malware only run in 32-bit environments. This may not be practical for most workstations but it is most definitely practical for servers.

Host Based Firewalls Work

Stuxnet relied upon network exploits to propagate. This type of propagation requires peer-to-peer communication between workstations. Restrict the communication of workstations to only those ports that are commonly used by specific applications to and from your server network can also reduce the risk of this type of vulnerability. For example, most workstations only talk with the server network in a restricted

environment using a certain set of protocols, so why should they ever be able to talk RPC with a workstation on the same subnet?

Most organizations, whether it's an SMB or even a larger enterprise, should not worry about Stuxnet-like attacks. Cyber-criminals and unscrupulous competitors have neither the resources nor the incentive to execute this kind of assault (Remember, they attack you for Money, not to damage your nuclear plants). And whatever your circumstance, stay focused on your vulnerabilities, not the threats that change every day around you. Enjoy the spy novel-like reading Stuxnet provides but stay focused on your risks.

FREE Report on Stuxnet



"Stuxnet Reality-Check: A Practical Guide to a Unique Attack Tool"

Email us at: info@avidtech.com to receive your free copy

The LastPass Breach: A very valuable cookie jar

continued from page 1

processor has the real credit card number. The end result? The merchant is the only spot with credit card numbers. We have just gone from a large number of decentralized retailers with say a couple thousand credit cards numbers to a few merchants with hundreds of millions in the data bases. If the attackers steal a hundred million credit cards they would have to break into thousands of companies. Now, they can target less than 20.

Is that the same risk? Of course not, yet most of the security controls put in place by organizations such as LastPass are the same as those used within decentralized organizations that have less data. If data was a chocolate chip cookie (my favorite), cloud vendors are analogues to a big glowing cookie jar sitting in the middle of a kindergarten class. Every kid will be tempted and will try to steal a cookie from the cookie jar but most importantly if just one kid gets into the jar just once all the cookies will be spilled on the floor.

The point here is you must analyze the security of any outsourced vendor to ensure they are implementing security better than you are on your data; otherwise, when you move your data you may be increasing your risk more than you realize. Have a structured checklist that compares their policy and procedures to yours and ask for details. Abstract documents like SAS-70 Type II and security marketing documents only go so far. Don't let your cookies be stolen from a vendor's cookie jar.

CEO Corner



Whenever we discuss cyber security breaches, the biggest risk is normally protecting against identity theft. We do not want our employees or family members' identity or credit cards stolen. No doubt, this risk is definitely the most prevalent but this month I wanted to discuss another type of risk that will grow in the next few years: Health Identity Theft. Once an attacker has

the identity of someone and they are able to buy or steal the person's health records it enables the attacker to receive fraudulent health care such as prescriptions (which can be sold on the black market), medical treatment and even transplants.

Two weeks ago, the Ponemon Institute, released their second annual National Study on Medical Identity Theft. The study concluded that roughly 1.5 million Americans are victims of medical identity theft and the average cost to resolve a case of medical identity theft is \$20,663, much higher than traditional identity theft. If you are the victim of identity theft, think beyond your credit cards to your health insurance card and make sure you contact your health insurance provider.

Top 12 Graduation Gift Ideas



1. iHome iP1 Studio Series Audio Systems for iPod/iPhone:

This award-winning studio series delivers big sound and clear audio, charges and plays your iPhone or iPod, and has a innovative and stylish design (Gifts.com \$299)

2. Multiple Gadget Charging Station:

A convenient one stop shop to charge all your electronic gadgets, smartphones, and iPods all at the same time (Amazon \$70)

3. Guitar Hero: Warriors of Rock:

With over 90 tracks, a redesigned rock inspired guitar controller, and new game play features, your graduate will become a living room legend to all! (Best Buy \$50)

4. Handheld GPS:

Whether in the car, on a walk, or going for a bike ride, this small and sleek GPS will keep anyone on track and never have to ask for directions (Sharper Image \$80)

5. Wireless indoor/outdoor speaker:

This tiny speaker with remote delivers a big sound with its powerful 2.4 GHz technology for your iPod, iPhone, computer, stereo, MP3 player, and other audio output devices (Sharper Image \$129)

6. Mini Digital Video Camera:

Capture life on the move with full color AVI video files and a 720 x 480 resolution. It's tiny and makes it easy to transfer files and recharge battery with the USB cable (Sharper Image \$99)

7. EconoDriver Fuel Efficiency Monitor:

These days, we could all use to save on fuel. This mileage computer scores your driving and gives you the tools to save money (FindGift.com \$50)

8. Digital Video Converter:

This converter can rip home movies and DVD's to digital files... without a computer! (Brookstone \$80)

9. Car Speaker with Headset:

Keep hand on the wheel with this hands free speaker for your car. No batteries or cables required, and the speaker is high power with adjustable volume and clear sound (Sharper Image \$50)

10. iPod Case with Built in Bottle Opener:

This hard shell slider case with soft touch finish and built-in bottle opener combines two of a graduate's favorite things for a Friday nights. (uncommongoods.com \$20)

11. Wireless key finder:

No more misplaced keys. This wireless key finder locates keys with one press of a button up to 60 feet away (Brookstone \$50)

12. Digital Golf Scorecard:

A convenient way to keep score, featuring 4 player score tracker, clock, and hole tracker (HansonEllis \$36)



Monthly Events

May 8th - 12th, Interop, Las Vegas

Attending Interop this year? Catch Michael Davis speaking on the 12th on "Making the Consumerization of IT Work for You" and on "How IT Makes a Difference to the Midmarket Company: Mobility & Security".

May 11th - 13th, MISTI Super Strategies

Stop by our booth and sign up to win fun gadgets and a chance to win a 3G Kindle. Join us at the Sheraton Chicago. Hotel & Towers

May 13th @ 10:00am, Savid Cloud Webinar

Get valuable information on the Cloud and how it can benefit your business.

June 9th @ 9:00am -5:00pm, CAMP IT-Enterprise Risk/Security Management

If attending this event stop by our table to win fun gadgets, and big prizes. Join us at the Donald E. Stephens Convention Center Rosemont, IL (O'Hare)

June, CIO Executive Breakfast

Enjoy complimentary breakfast with high level discussions on data management and compliance being held in June. Look for more details in our next issue.

For more information and to register for these events go to:

<http://www.savidtech.com/events>

Get Out From in Front of the Train



FREE Executive Briefing

Michael Davis will review his 2011 Security Report discussing the results of a year long study of over 1,300 security professionals in the US. demonstrating how organizations approach security strategically, and how you can learn from the mistakes of others.

Contact us at 877-307-0444
or info@savidtech.com to schedule
Executive Briefing today!



savidtechnologies

18470 Thompson Ct. Ste. 2B
Tinley Park, IL 60477

Comprehensive Knowledge. Delivered.

Take a Break!



Monthly Trivia

Be the first to email us the correct answer and win a **\$20 Starbucks Gift Card!**

Which is the word in English that has nine letters, and remains a word at each step even when you remove one letter from it, right up to a single letter remaining. List each letter as you remove them, along with the resulting word at each step.

Email your answer to: info@savidtech.com and look for the winner listed in next months newsletter
Congratulations to last months trivia winner Greg Bee!

Joke of the Month

What did the general do when he learned via Twitter that the battle was going badly?
He Retweeted.

Got a funny joke? Send it to us at info@savidtech.com and we may include it in an upcoming issue.

Ask the Readers

We want to here from You!

Topics, questions, ideas?
Give us your comments to help us provide the best *Insight* to our readers!
Call 877-307-0444 or visit us at: <http://www.savidtech.com/contact-us>

Want More?

Contact us to receive more information on these articles.
Find out how Savid Technologies can help your business. Give us a call at 877-307-0444 or Email: info@savidtech.com.

Missed one of our webinars go to: <http://www.savidtech.com/resources>

Follow Us On:



<https://www.facebook.com/savidtech>



<http://twitter.com/savidtech>



<http://www.savidtech.com/blog>

During Your Stay



Beware that your conversations may not be private or secure. Unlike the United States, most other countries do not have legal restrictions against technical surveillance. Most foreign security services have various means of screening incoming visitors to identify persons of potential intelligence interest.

They also have well established contacts with hotels and common hosts that can assist in various forms of monitoring you. Electronic eavesdropping has been reported on airlines, in hotel rooms, taxis, and meeting rooms.

Business and government travelers have reported their hotel rooms and belongings were searched while they were away. Sometimes there was no effort to conceal the search.

Do not leave electronic devices unattended. Do not transport them (or anything valuable) in your checked baggage. Shield passwords from view. Avoid Wi-Fi networks if you can. In some countries they are controlled by security services; in all cases they are insecure.

Clear your Internet browser after each use: delete history files, caches, cookies, and temporary internet files.

If your phone or laptop is stolen, report it immediately to the local US Embassy or Consulate.

Do not use non-company computers to log into your company's network. Always consider any information conveyed through a non-company computer to be compromised, even if encrypted.

Cyber criminals from numerous countries buy and sell stolen financial information including credit card data and login credentials (user names and passwords).

Do not allow foreign electronic storage devices to be connected to your computer or phone. They may contain malware or automatically copy your stored electronic data. Do not use thumb drives given to you – they may be compromised.

In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. All information you send electronically can be intercepted, especially wireless communications. If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.

During the Beijing Olympics, hotels were required to install software so law enforcement could monitor the Internet activity of hotel guests.

Beware of "phishing." Foreign security services and criminals are adept at pretending to be someone you trust in order to obtain personal or sensitive information.

Upon Your Return

Review your system access with your company's Information Security Officer. Access that is not accounted for should be investigated.

It is not uncommon for foreigners to contact you after your return. The FBI may be able to help you determine if these contacts pose any risk to you or your company.

Change all your passwords including your voicemail and check electronic devices for malware.

Report any unusual circumstances or noteworthy incidents to your security officer and to the FBI. Notifying the FBI will help ensure that future travel advisories take into consideration the circumstances and incidents you encountered.

Additional travel security tips and country threat assessments are available from the FBI upon request.

Your local FBI office #: _____



www.fbi.gov

Overseas Security Advisory Council: www.osac.gov

U.S. Department of Justice
Federal Bureau of Investigation



"The willingness of US scientists and scholars to engage in academic exchange make US travelers particularly vulnerable not only to standard electronic monitoring devices—installed in hotel rooms or conference centers—but also to simple approaches by foreigners trained to ask the right questions." –ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2003.

SAFETY AND SECURITY for the Business Professional Traveling Abroad

You or your firm may be a target of a foreign country's efforts to obtain information or technologies in order to increase their market share, build their economies, or modernize their militaries. Targeting methods include luggage searches, extensive questioning, and unnecessary inspection and downloading of information from laptop computers.



Business travelers should take measures to ensure not only the safety and security of themselves but also their business information while traveling outside the United States.



Good security habits will help protect you and your company.

Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. In many countries, domestic corporations collect competitive intelligence with the help and support of their government. To mitigate this risk, your organization's critical information and technologies should not reside on any hard copy or electronic device you take unless it is absolutely necessary, and if so, then you must safeguard the physical access to the information by using encryption and keeping the material on your person at all times. Hotel safes are not adequate protection.

Critical business information may include:

- Customer data
- Employee data
- Vendor information
- Pricing strategies
- Proprietary formulas and processes
- Technical components and plans
- Corporate strategies
- Corporate financial data
- Phone directories
- Computer access protocols
- Computer network design
- Acquisition strategies
- Marketing strategies
- Investment data
- Negotiation strategies
- Passwords (computer, phone, accounts)

Before You Go

Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.



Plan your wardrobe so that it does not offend the locals, nor draw unwanted attention to yourself. Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.

Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Keep one copy at home; carry a second copy with you but separate from the originals. This will help speed the replacement process if they are lost or stolen.

Do not take unnecessary identification or credit cards in case they are stolen. Take only what is necessary. Obtain traveler's checks if needed.

Establish points of contact for your family to contact and for your foreign hosts to contact in the event of an emergency. Register your trip with the State Department. Obtain the phone number and address for the US Embassy or Consulate in the country(s) you plan to visit.

Take any necessary medications with you in their original containers and keep them in your carry-on luggage (not checked baggage) during the flight. Verify you have adequate medical insurance.

Obtain specific pre-travel country risk assessments for the country(s) you plan to visit from your security officer, the State Department, and/or the FBI. There may be specific issues you should be aware of and prepare for that will ensure your safety and peace of mind.

Visit www.osac.gov for security news and reports for the country(s) you plan to visit.



Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Back-up all information you take and leave that at home. If feasible, use a "clean" laptop, phone and a new email account while traveling. **Or If you can do without the device, Do Not Take It!**

Cell phones can be hacked to steal contact lists, usernames, passwords, and browser history.

Use up-to-date protections for antivirus, spyware, security patches, and firewalls.

Clean out your voice mail. When you access your messages, the pass code may become compromised and others may then retrieve your messages.

During Your Stay

Protect your passport! Theft of American tourist passports is on the rise. It is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes, and that it remain with you at all times. Some hotels require you to leave it at the desk during your stay and they may use it to register you with the local police--a routine policy. Ask for a receipt and be sure to retrieve your passport before continuing your trip. If your passport is lost or stolen, report the situation immediately to the nearest US Embassy or Consulate.

Be courteous and cooperative when processing through customs. Do not leave your bags unattended. Stay alert.

Use authorized taxis. You could be overcharged, robbed or kidnapped when using "gypsy" taxis.

Do not invite strangers into your room.

Avoid traveling alone, especially after dark. Be conscious of your surroundings and avoid areas you believe may put your personal safety at risk. Be wary of street vendors and innocent-looking youngsters. While one person has your attention, another might be picking your pocket.



Do not carry large amounts of cash. Always deal with reputable currency exchange officials or you run the risk of receiving counterfeit currency. Keep a record of your financial transactions.

Beware that theft from sleeping compartments on trains is common.

Do not leave drinks unattended -- someone could slip a drug into it that causes amnesia and sleep.

Avoid long waits in lobbies and terminals, if possible. These areas may harbor pickpockets, thieves, and violent offenders. Laptop theft is especially common in airports.

At the airport, a thief preceded a traveler through a security checkpoint. After the traveler placed his laptop computer on the x-ray machine conveyer belt, a second thief set off the metal detector causing a delay. The first thief then stole the traveler's laptop after it passed through the x-ray machine.

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate.

Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.

Avoid civil disturbances and obey local laws. If you come upon a demonstration or rally, be careful; in the confusion you could be arrested or detained even though you are a bystander. Be mindful that in many countries, it is prohibited to speak derogatorily of the government and its leaders. It may be illegal to take photographs of train stations, government buildings, religious symbols, and military installations.

Avoid any actions that are illegal, improper or indiscreet. Avoid offers of sexual companionship; it may lead to a room raid, photography, and blackmail. Do not attempt to keep up with your hosts in social drinking. Do not engage in black market activities. Do not sell your possessions. Do not bring in or purchase illegal drugs or pornography. Do not seek out political or religious dissidents. Do not accept packages or letters for delivery to another location.

An American was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening national security officers visited the American and admonished him for taking the letter.

Keep a low profile and shun publicity. Do not discuss personal or business information with local news media and be careful what type of information you share with foreigners. They may have been directed to obtain information in order to exploit you or your company. Politely redirect the topic. The FBI can provide tips on how to recognize deceitful elicitation.

Evade criminals and terrorists by being aware of your surroundings and alert to the possibility of surveillance. Take mental notes of anyone following you and promptly report it to the appropriate security officials and/or the US Embassy or Consulate. In general, criminals will strike when their target seems most lax about his/her security. If anyone grabs you, make a scene--yell, kick and try to get away! If you are kidnapped, remain alert and establish a program of mental and physical activity for yourself; try to remain calm and non-threatening.

Do not gossip about character flaws, financial problems, emotional relationships, or other difficulties of your fellow Americans or yourself. This information is eagerly sought by those who want to exploit you or your fellow travelers.