“I am walking through a city made of glass and I have a bag full of rocks”

(Dispelling the myths and discussing the facts of Global Cyber-Warfare)

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent “break-ins” that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

“The criminals who knocked out those three major online businesses are the least of our worries,” Yabenson told *Weekly World News*.

“There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

“It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

“As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers.”

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

“As dangerous as this technology is right now, it's going to get much scarier,” Yabenson said.

“Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

“Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

“And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

“That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be

Sickos can wreak death and destruction from thousands of miles away!

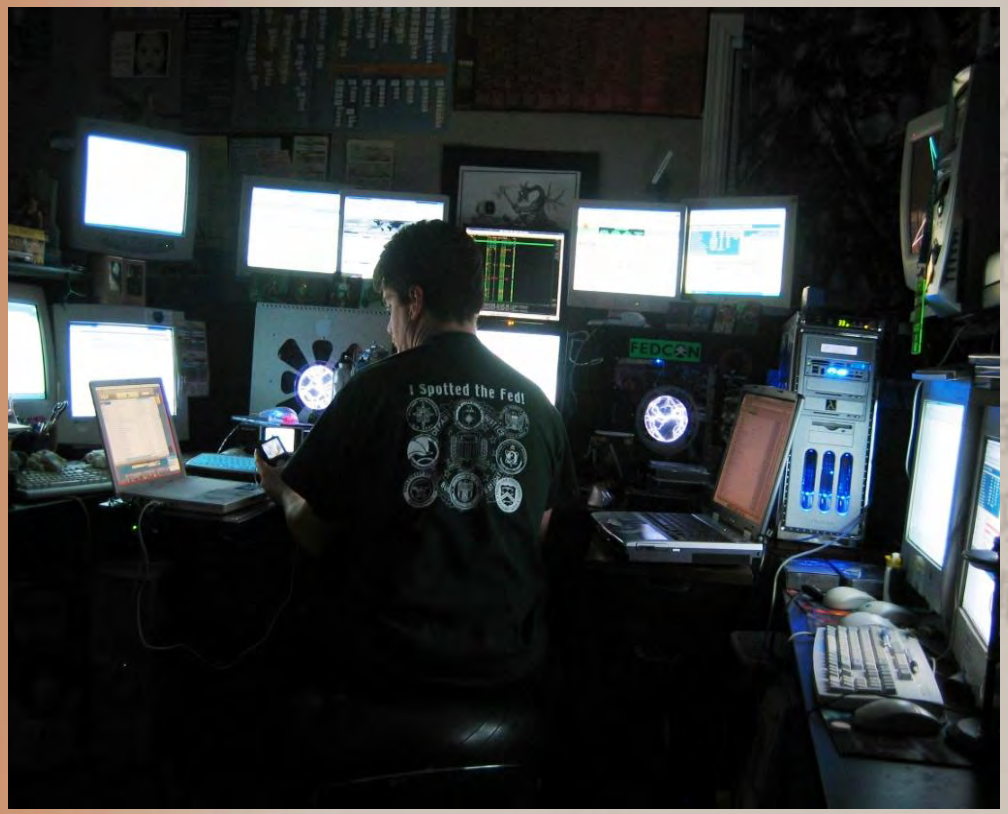
Arnold Yabenson.

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Jayson E. Street,
CISSP, GSEC, GCIH, GCFA,
IEM, IAM, ETC…

Let go of my EGO

- Lets start out with a little about yours truly.

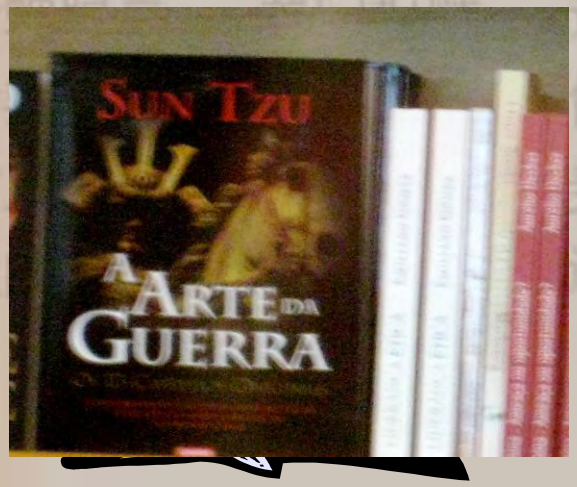


- Defcon17@F0rb1dd3n.com
http://F0rb1dd3n.com

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Yes Sun Tzu was a hacker!

- Sun Wu (Tzu) “Ping-fa”(The Art of War)
- “Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement!”



Contents

- INTRO
- Caveats
- History & Geography lessons
- Players and Haters
- You’re involved? YES!!
- Discussion

I read it on the Internets

- Report VS. Investigate

Facets of Perspective

VS.

Meet your new neighbors (and they hate you)

- This war is not dictated by boundaries just bandwidth.

- War is God's way of teaching Americans geography.

Ambrose Bierce

The Roster for the B1G Game

- China
- Russia
- Jihadist
- More players
- USA (and friends)

CHINA
(The Terrell Owens of cyber-war)

- **Definition of Red Hacker Alliance:**
- **A Chinese nationalist hacker network, made up of many independent web sites directly linked to one another in which individual sites educate their members on computer attack and intrusion techniques. The group is characterized by launching coordinated attacks against foreign governments and entities to protest actual and perceived injustices done to their nation. There is a growing trend that suggests monetary motivations are becoming as important as patriotic passion.**

They started without us

- 1997 Formation of the Green Army Founded by GoodWell (China)
- 1998 Anti-Chinese riots in Indonesia provide the catalyst for the creation of the Red Hacker Alliance.
- 2000 *Honker Union of China founded by Lion China Eagle Union founded by Wan Tao Javaphile founded by Coolswallow and Blhuang*
- *2001* Sino-US cyber conflict *1000 web defacement protesting death of Chinese pilot.*

73% of all statistics are made up. (But still OUCH)

- Visiting each of the 90 sites that kept statistics (out of 250 sites looked at) and then adding up the total number of registered members showed a total of 1,197,769 participants.
- The range therefore would be from a minimum of 24,000 to a maximum of around 1.2 million.
- It is probable that during times of political strife, these numbers rise dramatically higher and move closer to the upper ranges.

Locked and Loaded

- One of the sites directly linked to the Red Hacker Alliance and operating out of the Green Power Bar is the *Friendly Download Site (http://www.xxijj.com). It claims to have 69,951 downloads available, many of which are Trojan horses and attack tools. The Friendly Download Site also has the newest 2005 version of the Gray Pigeon Trojan. This is an updated version of the same Gray Pigeon Trojan that was discussed in Chapter One and used during the 1999 Cyber Conflict with Taiwan. Its design is based on the Glacier Trojan and is an indigenously produced product.*
- In June of 2005, the National Infrastructure Security Co-ordination Centre (NISCC)108 released a report detailing Trojan e-mail attacks targeting United Kingdom “government and companies.” The briefing noted that the attacks were coming from the “Far-East” and Trojans used in the attack included Gray Pigeon and Nethief.109 Chinese hackers have taken credit for the creation of both of these two Trojan programs.

Citizen S0ld13r

- The central problem with our initial inquiry and the thinking behind it is that we are viewing the situation from a US paradigm and applying cultural bias. In Chinese society, independence from government direction and control does not carry with it the idea of separation from the state. The PRC government views its citizenry as an integral part of Comprehensive National Power and a vital component to national security.

- From a Western perspective, the idea of active espionage against another nation requires government initiative, involvement, and direction. It is hard for us to conceive of links being formed between state authorities and quasi-freelance intelligence operations, simply because it does not fit our preconceived notion of the proper relationship. When in fact, there is a very good chance this is exactly the type of association that is taking place between the central government and the Red Hacker Alliance.

It’s all about the Mao’s (yuan) baby

- An interview with a Chinese hacker from Beijing provides an excellent example of this “nontraditional” relationship:
- *“One Beijing hacker says two Chinese officials approached him a couple of years ago requesting ‘help in obtaining classified information’ from foreign governments. He says he refused the ‘assignment,’ but admits he perused a top US general's personal documents once while scanning for weaknesses in Pentagon information systems ‘for fun.’ The hacker, who requested anonymity to avoid detection, acknowledges that Chinese companies now hire people like him to conduct industrial espionage. ‘It used to be that hackers wouldn't do that because we all had a sense of social responsibility,’ says the well-groomed thirty something, ‘but now people do anything for money.’”158*

From Russia with ….

- An interesting point to keep in mind is that Moscow does the arms business with over 70 countries, including China, Iran, and Venezuela, and in 2006 exported $6 billion worth of arms. Russian intelligence services have a history of employing hackers against the United States. In 1985 the KGB hired Markus Hess, an East German hacker, to attack U.S. defense agencies in the infamous case of the “Cuckoo's Egg”.

- The following is an estimate of Russia's cyber capabilities.
- Russia's 5th-Dimension Cyber Army:
- Military Budget: $40 Billion USD
- Global Rating in Cyber Capabilities: Tied at Number 4
- Cyber Warfare Budget: $127 Million USD Offensive Cyber Capabilities: 4.1 (1 = Low, 3 = Moderate and 5 = Significant)

As of May 27, 2008

From Russia with …(cont.)

Cyber Weapons Arsenal in Order of Threat:

- Large, advanced BotNet for DDoS and espionage
- Electromagnetic pulse weapons (non-nuclear)
- Compromised counterfeit computer software
- Advanced dynamic exploitation capabilities
- Wireless data communications jammers
- Cyber Logic Bombs Computer viruses and worms
- Cyber data collection exploits Computer and networks reconnaissance tools
- Embedded Trojan time bombs (suspected)

- Cyber Weapons Capabilities Rating: Advanced
- Cyber force Size: 7,300 +
- Reserves and Militia: None
- Broadband Connections: 23.8 Million +

Russia VS. Estonia (or just getting warmed up)

- Cyberattacks on Estonia (also known as the Estonian Cyberwar) refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's row with Russia about relocation of a Soviet-era memorial to fallen soldiers, as well as war graves in Tallinn.[1] Most of the attacks that had any influence on general public were distributed denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.[2]

Russia VS. Georgia

(Military precision or an excuse for poor infrastructure?)

- The stories are still coming in and still changing or evolving depending if you listen to n3td3v or not.
- Meanwhile, Estonia (once the victim of Russian-based hackers) is now hosting Georgia's Ministry of Foreign Affairs website. And "in a historic first, Estonia is sending cyberdefense advisors to Georgia," Network World observes.
- And, of course, the strikes aren't just made up of ones and zeros. The Russians are reportedly bombing Georgia's telecommunications infrastructure -- including cell towers. "It's still very difficult to get a call anywhere around the country right now," an NPR reporter says.
- When political tensions flared last month between Georgia and its large neighbor to the north, the country was ready to block Internet traffic from Russia, hoping to avoid the denial-of-service attacks that shut down Internet service in Estonia for several days in 2007. Instead, most of the DoS attacks that were directed against Georgia came from an unlikely place: the United States.

Russia VS. ????

- The FSB is the internal counter intelligence agency of the Russian Federation and successor to the Soviet KGB. Russia is often overlooked as a significant player in the global software industry. Russia produces 200,000 scientific and technology graduates each year. This is as many as India, which has five times the population. This is hard to believe since their software industry can be traced back to the 1950s.

- A study by the World Bank stated that more than one million people are involved in software research and development. Russia has the potential to become one of the largest IT markets in Europe. The Russian hacker attack on Estonia in 2007 rang the alarm bell. Nations around the world can no longer ignore the advanced threat that Russia's cyber warfare capabilities have today and the ones they aspire to have in the near future.

- From this information, one can only conclude that Russia has advanced capabilities and the intent and technological capabilities necessary to carry out a cyber attack anywhere in the world at any time.

- Kids or KGB The same still holds true don’t mess with Russia

Russian Business Network (a new definition to risky business)

- Security researchers and anti-spam groups say the St. Petersburg-based RBN caters to the worst of the internet's scammers, renting them servers used for phishing and malware attacks, all the while enjoying the protection of Russian government officials. A report by VeriSign called the business "entirely illegal."

Figure 2 RBN AS

Rbnexploit.blogspot.com

Know your enemy (it is ignorance and fear)

- ISLAM In Arabic, the word means "surrender" or "submission" to the will of God. Most Westerners think of Islam as one of the three ...
- slate.msn.com/id/1008347/

- When the angels said, 'O Mary, ALLAH gives thee glad tidings of a son through a word from HIM; his name shall be the Messiah, Jesus, son of Mary, honoured in this world and in the next, and of those who are granted nearness to God;

- 'And he shall speak to the people in the cradle, and when of middle age, and he shall be of the righteous.

- She said, 'My Lord, how shall I have a son, when no man has touched me? He said, 'Such is the way of ALLAH. HE creates what HE pleases. When HE decrees a thing HE says to it 'Be,' and it is;" -- Qur'an, Surah 3:38-48

When Jihad becomes J1H4D

- Jihad what does the word mean? “Literally 'struggle,' it includes both the inward spiritual struggle against human desires and the outward struggle against injustice, oppression and the rejection of the truth by non-believers, which leads to 'holy war' only when sanctioned by the legitimate political authority.
- www.c-r.org/our-work/accord/sudan/glossary.php”

- “The funny thing is that so many of the real Al Qaeda websites are hosted in the US,” he says. “One simple reason is it’s one of the cheaper places to host. They circulate via mailing lists and these sort of out of bounds methods where they can be found. They’re all in Arabic. Not many westerners know Arabic, and everything’s fine until some journalist figures out where the website is.”

- Posted on Monday, January 21, 2008 “Originally introduced by the Global Islamic Media Front (GIMF), the second version of the Mujahideen Secrets encryption tool was released online approximately two days ago, on behalf of the Al-Ekhlaas Islamic Network. “http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html

You can’t google for new recruits. (Or can you?)

- “Those who think that we can stop online terrorism by removal of websites are either naive or ignorant about cyberspace and its limitations for interference,” says Gabriel Weimann, professor of communication at Haifa University in Israel and author of Terrorism on the Internet (http://bookstore.usip.org/books/BookDetail.aspx?productID=134280).

- “As a short answer, there is a need for strategy and not tactics, there is a need for a multimeasured approach, and not just “Let's kill those websites.’ They reemerge within days or even hours.”

- The teams, and the lone gunmen cyber jihadists in this post are : Osama Bin Laden's Hacking Crew, Ansar AL-Jihad Hackers Team, HaCKErS aLAnSaR, The Designer - Islamic HaCKEr and Alansar Fantom. None of these are known to have any kind of direct relationships with terrorist groups, therefore they should be considered as terrorist sympathizers.

Dealing drugs not for profit but for "The Prophet"

- The U.S. General Accounting Office reports that financing for Al-Qaeda operations come from many sources including subscription/membership fees, false contracts, counterfeiting/forging currency, robbing state banks/bank employee and kidnapping. The Treasury Department has even linked three Yemeni honey companies to Osama bin Laden's terrorism-financing operation.
- Western intelligence agencies believe Khan has become the kingpin of a heroin-trafficking enterprise that is a principal source of funding for the Taliban and al-Qaeda terrorists. A Western law-enforcement official in Kabul who is tracking Khan says agents in Pakistan and Afghanistan, after a tip-off in May, turned up evidence that Khan is employing a fleet of cargo ships to move Afghan heroin out of the Pakistani port of Karachi. The official says at least three vessels on return trips from the Middle East took arms like plastic explosives and antitank mines, which were secretly unloaded in Karachi and shipped overland to al-Qaeda and Taliban fighters.

Terrorize a city been there
Terrorize a country done that
Terrorize the World Wide Web …

- Let's discuss what cyber jihad isn't. Cyber jihad is anything but shutting down the critical infrastructure of a country in question, despite the potential for blockbuster movie scenario here. It's news stories like these, emphasizing on abusing the Internet medium for achieving their objectives in the form of recruitment, research, fund raising, propaganda, training, compared to wanting to shut it down.

From Brazil to Romania. (and all the trouble in between)

- South America = Community based Hacking
- Eastern Europe = A mix between the movies “Hackers” and “Good Fellas”

U. S. of OMGWTFBBQ

This > Than = WTF!!!!

"The authors point to a 2004 Pentagon statement on military doctrine, indicating that the United States might respond to a cyberattack with the military use of nuclear weapons in certain cases. "For example," the Pentagon National Military Strategy statement says, "cyberattacks on U.S. commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent." "

http://www.nytimes.com/2009/04/30/science/30cyber.html

USA home of the free (and land of the Hacked.)

- Organized Chaos = Chaos
- Working for the “Man” a lot different than fighting for fellow man.

All the cool kids are doing it!

South Korea, Japan, Germany, UK, Israel (yeah I said Israel), ETC…

We must not only learn but adapt!

- *"The smallest detail, taken from an actual incident in war, is more instructive for me, a soldier, than all the Theirs, and Jominis in the world. They speak, no doubt, for the heads of states and armies but they never show me what I wish to know – a battalion, a company, a squad, in action." -Col. Charles Ardant du Picq*
- Battle Studies: Ancient and Modern Battle from Russel A. Gugeler, Combat Actions in Korea, *US Government Printing Office, 1970 revised edition, p. iii*

Okay now what can we do?

- Without understanding where the opponent's weaknesses are you cannot borrow their strength to use against them. (Cheng Man Ching)

- http://jayson-street.tumblr.com/
- http://stratagem-one.com
- http://f0rb1dd3n.com
- http://www.security-twits.com/
- http://OSVDB.org
- http://isc.sans.org

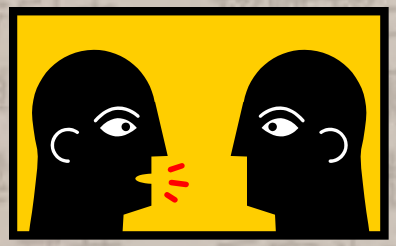
- My presentation located here
- http://F0rb1dd3n.com/s1s/**WP**/

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Now let's learn from others

- Discussion and Questions????

- Or several minutes of uncomfortable silence it is your choice.



- This concludes my presentation Thank You

The Links

- No order here they are.

- http://ddanchev.blogspot.com/2007/10/russian-business-network.html
- http://www.defensetech.org/archives/004200.html
- http://dsonline.computer.org
- http://www.time.com/time/magazine/article/0,9171,1101040809-674777,00.html
- http://news.cnet.com/8301-1009_3-10049008-83.html
- http://www.thedarkvisitor.com/

- I am sure I missed some though not on purpose. If you do not find a proper source in this list but mentioned in the presentation please contact me and I will correct it.

All those other links in no order

- http://intelfusion.net/wordpress/?p=432
- http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Storage+Security&articleId=9134010&taxonomyId=153&pageNumber=2
- http://bostonreview.net/BR34.4/morozov.php
- http://www.csoonline.com/article/495520/Cyberwar_Is_Offense_the_New_Defense_
- http://www.itar-tass.com/eng/level2.html?NewsID=14070168&PageNum=0
- http://www.google.com/hostednews/afp/article/ALeqM5geMDsdejQoeSn8FQseQHZKeTe50A
- www.heritage.org/research/asiaandthepacific/upload/wm_1735.pdf
- http://www.nap.edu/nap-cgi/report.cgi?record_id=12651&type=pdfxsum
- http://news.bbc.co.uk/2/hi/uk_news/politics/8118729.stm
- http://en.wikipedia.org/wiki/Honker_Union
- http://blog.security4all.be/
- http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2
- http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=3&hp
- http://www.foxnews.com/story/0,2933,464264,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,448626,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,403161,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,370243,00.html?sPage=fnc/scitech/cybersecurity
- http://www.spiegel.de/international/germany/0,1518,606987,00.html
- http://threatchaos.com/
- http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome
- http://shanghaiist.com/2009/06/08/how_to_make_money_as_a_hacker.php

All those other links (cont.)

- http://www.socialsignal.com/blog/rob-cottingham/censorship-isnt-only-problem-with-chinas-new-internet-blocking-software
- http://www.nytimes.com/2009/04/30/science/30cyber.html?_r=1
- http://www.thetrumpet.com/?q=5940.4309.0.0

- I LOL'ed http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps