Notes from the Board of ISSA-COS

In this installment of the ISSA-COS newsletter we’ll cover some of the basics of:

- Getting your next job,
- What you should do,
- What to look at when scanning your resume and why.

If you are right now looking at the job market – and you want to get feedback on your resume – please see the end of this article for that support from ISSA-COS. Yes, we will help you with your job search.

Let’s start off by looking at least 10 things to consider when you are getting yourself ready for your next job search:

#1 Dust off your resume. Look at it carefully. Look at the Job Description. Be precise in the way you show the prospective employer how YOU map yourself and your skills directly to their needs. Make sure that you can specify in no uncertain terms EXACTLY how YOU are the BEST MATCH for the position from among the competition. Make sure you stand out.

#2 ANYTHING you say in your resume can and will be used against you by the HR department. Do not inflate anything, do not exaggerate or make any statements that cannot be verified. Believe in yourself and remember that your resume is an important reflection of who you are and what you stand for – also keep in mind that your next job depends on it.

#3 DO Reconnect with former classmates, mentors and co-workers. Part of the answer to your job search is networking. Do not discount anyone – you need to cast a wide net to find opportunities. The world of work is a big place. Also – know that at ISSA Colorado Springs – you have a built-in network of nearly 400 technical and management professionals who each know their share of other professionals. They are much more likely to hear about a job opening than you looking for one in a newspaper. Consider talking about your job search at the next luncheon, event, or get together.

#4 Become very humble. Ask for help. Do not try to do the job search alone. Keep in mind that some folks are new to the game and have only a basic understanding of your value proposition. Learn to sell – not tell. Explain your value by letting others know how you solve problems, how you can help them – listen to their issues and challenges. In the (Continued on page 5)
The Pentagon is accelerating efforts to develop a new generation of cyber-weapons capable of disrupting enemy military networks even when those networks are not connected to the Internet, according to current and former U.S. officials.

The possibility of a confrontation with Iran or Syria has highlighted for American military planners the value of cyberweapons that can be used against an enemy whose most important targets, such as air defense systems, do not rely on Internet-based networks. But adapting such cyberweapons can take months or even years of arduous technical work.

When U.S. military planners were looking for ways to disable Libya’s air defense system before NATO’s aerial attacks last year, they discussed using cybertechnology. But the idea was quickly dismissed because no effective option was available, said current and former U.S. officials.

They estimated that crafting a cyber-weapon would have taken about a year, including the time needed to assess the target system for vulnerabilities.

“We weren’t ready to do that in Libya,” said a former U.S. official, who spoke on the condition of anonymity because of the sensitivity of the discussions. “We’re not ready to do that now, either.”

Last year, to speed up the development of cyberweapons, as well as defensive technology, then-Deputy Defense Secretary William J. Lynn III and Marine Corps Gen. James Cartwright, then vice chairman of the Joint Chiefs of Staff, placed $500 million over five years into the budget of the Defense Advanced Research Projects Agency, one of the Defense Department’s premier research organizations.

The agency also has launched new cyber-development initiatives, including a “fast-track” program.

“We need cyber options that can be executed at the speed, scale and pace” of other military weapons, Kaigham J. Gabriel, DARPA deputy director, said in testimony last month to Congress.

Pentagon officials, meanwhile, are developing a congressionally mandated strategy for the rapid acquisition of cyber-weapons that can keep pace with threats and technology.

Officials are researching cyber-weapons that can target “offline” military systems in part by harnessing emerging technology that uses radio signals to insert computer coding into networks remotely.

“To affect a system, you have to have access to it, and we have not perfected the capability of reaching out and accessing a system at will that is not connected to the Internet,” said Joel Harding, an independent consultant who is a former military officer and former director of the Information Operations Institute.

Even if an operator gains access, he said, “unless you already have custom-written code for a system, chances are we don’t have a weapon for that because each system has different software and updates.”

In some cases, as with command-and-control systems, military assets rely on Internet connections, making them theoretically easier to target.

Without that connectivity, an attacker would have to rely on other means — for instance, physically inserting into those systems portable devices such as thumb drives or computer components that have been altered.

Read More:
http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html?hpid=z1
Has the ‘Cyber Pearl Harbor’ already happened?

By Philip Ewing Monday, March 26th, 2012 10:54 am
Posted in Cyber Security

The Russians are picking our pockets, the Chinese are stealing our most vital secrets, and there’s nothing we can do about it – and it’s all going to get worse.

That was the basic conclusion after Friday’s Air Force Association cyber-conference, where speaker after speaker drove home the utter futility and helplessness of today’s cyber climate, all the while warning that the problem will only grow.

Richard Bejtlich, chief security officer for the infosec firm Mandiant, said 100 percent of the high-profile intrusions his company tracks were done with “valid credentials” – meaning the cyber bad-guys had been able to steal a real user’s login and password, obviating the need for more complex attacks.

The typical time between an intrusion and its discovery is 416 days, he said – down from two or three years – and the way most companies find out about them is when they get a visit from the FBI.

The publicly available malware in the so-called “cyber underground” is now so good that you can do a lot of damage without a dedicated team of code-writers coming up with their own stuff, speakers said. In fact, the much-discussed cyber attack against Georgia was carried out mostly with publicly known tools – “there was nothing sacred here,” said National Defense University iCollege chancellor Robert Childs.

Cyber-intrusions and compromise are so endemic, Bejtlich said, that many attackers don’t even bother with the wholesale vacuuming of information that used to characterize cyber-snooping. Now hackers go after very specific pieces of information, often data that is useless on its own, he said.

He described how a company had approached Mandiant befuddled that someone would want to steal a certain proprietary device, because it only worked in combination with a specific chemical formula owned by another company. Naturally, it wasn’t long before the second company discovered it was compromised, and also befuddled because its chemical formula would only be useful to someone who had information about the device manufactured by the first.

Online miscreants are also becoming more sophisticated at a strategic level, Bejtlich said: He described how they might target small companies that were merging with larger ones, to avoid trying to attack the bigger firm’s online security. Instead, by compromising a small company’s computer networks, the bad guys can then get into the new common network after a merger.

This can have profound financial as well as security implications, Bejtlich said – if you’re an aerospace giant and you want to acquire a small firm because its widget is worth $10 million, but then you discover it’s been cyber-stolen and no longer proprietary, the technology might only be worth $10,000, and that could put your shareholders and Wall Street in a bad mood.

Read the rest: http://www.dodbuzz.com/2012/03/26/has-the-cyber-pearl-harbor-already-happened/

Growing unease over illegal cell phone jammers

For less than $40 nearly anyone can purchase a cell phone jamming device to prevent those nearby from making calls, which has law enforcement officials uneasy.

“The general public doesn’t realize what they’re jamming if they were to start using these things,” Richard Mislan, an assistant professor of computer and information technology at Rutgers University, told KXLY in Spokane, Washington. “What’s not obvious is all the wireless connectivity systems that are in the background and maintaining data communications in our daily lives.”

Read more: http://www.homelandsecuritynewswire.com/dr20120313-growing-unease-over-illegal-cell-phone-jammers
News Ripped From the Headlines

March 28, CNET News - (International) **China nabbing 'great deal' of U.S. military secrets.** Testifying before the U.S. Senate Armed Services Committee March 27, the head of the National Security Agency (NSA) and Cyber Command said China is stealing a “great deal” of the U.S. military's intellectual property, adding that the NSA sees “thefts from defense industrial base companies.” He confirmed speculation that China was behind 2011’s attacks on RSA. Those attacks proved extremely troublesome for U.S. defense contractors. In 2011, Chinese hackers allegedly stole data related to RSA’s SecurID two-factor authentication devices. Soon after, that information was used to break through security safeguards at defense contractors Lockheed Martin, L-3 Communications, and Northrop Grumman. Source:


March 8, Softpedia – (International) **Scareware demands ransom after making files and folders invisible.** Bitdefender came across a piece of scareware that makes victims believe something may have happened to all the files and folders stored on their computers. The user is then requested to pay $80 for a tool that allegedly addresses the problem. Identified as Trojan.HiddenFilesFraud.A, the rogue disk repair utility starts operating by informing the user of certain issues that affect the computer. Since many users are accustomed to fake antivirus, this malicious application is programmed to make everything look more realistic. It changes the attributes of all files and folders, setting them as Hidden, so the user may believe everything was deleted from the hard drive. Certain key shortcuts are also disabled to induce more panic. Also, the worm that downloads HiddenFilesFraud.A, Win32.Brontok.AP@mm, ensures the files’ attributes cannot be modified from Windows Explorer back to their original state. After displaying the numerous —errors— that affect the system, the scareware advertises a repair utility that costs $80. However, the so-called utility does absolutely nothing. Brontok.AP@mm, the element responsible for installing Trojan.HiddenFilesFraud.A, quickly copies itself on removable media drives to ensure it spreads without difficulty from one computer to another. Source: http://news.softpedia.com/news/Scareware-Demands-Ransom-After-Making-Files-and-Folders-Invisible-257383.shtml

March 13, Dark Reading – (International) **Malicious proxies may become standard fare.** A number of security-as-a-service applications — from Postini to OpenDNS to Zscaler — reroute domain-name system (DNS) requests through centralized servers or proxies to detect security threats and sanitize traffic before it reaches the client network. Yet proxies are not just used by security companies, but by criminals as well. DNSChanger, which authorities shut down November 2011, used just such a strategy to reroute victims to custom advertisements and malicious installers. When the program compromised a system, it would replace the list of valid DNS servers with entries that pointed to servers controlled by the criminal operators. After displaying the numerous —errors— that affect the system, the scareware advertises a repair utility that costs $80. However, the so-called utility does absolutely nothing. Brontok.AP@mm, the element responsible for installing Trojan.HiddenFilesFraud.A, quickly copies itself on removable media drives to ensure it spreads without difficulty from one computer to another. Source: http://news.softpedia.com/news/Scareware-Demands-Ransom-After-Making-Files-and-Folders-Invisible-257383.shtml

March 15, IDG News Service – (International) **Digitally signed malware is increasingly prevalent, researchers say.** Security companies recently identified multiple malware threats that use stolen digital certificates to sign their components in an attempt to avoid detection and bypass Windows defenses, IDG News Service reported March 15. When it was discovered in 2010, the Stuxnet industrial sabotage worm surprised the security industry with its use of rootkit components that were digitally signed with certificates stolen from semiconductor manufacturers Realtek and JMicron. Security experts predicted at the time that other malware creators would adopt the technique to bypass the driver signature enforcement in 64-bit versions of Windows Vista and 7. Given recent developments it appears they were right. A backdoor discovered by Symantec in December 2011 installed a rootkit driver signed with a digital certificate stolen from an undisclosed company. The certificate was revoked by VeriSign at the owner’s request 9 days later. However, the time window available for the malware to remain undetected was larger than that, because Windows operating systems rarely check certificate revocation lists, or do not check them at all, Symantec’s principal software engineer said March 15. Source:

http://www.computerworld.com/s/article/9225237/Digitally_signed_malware_is_increasingly_prevalent_researchers_say?taxonomyId=17
job search you are essentially selling a product and THAT PRODUCT IS YOU. Oh, did I mention that you MUST learn intense listening skills?

#5 Make personal connections and lots of them. Be ready to help others on this journey. This might sound repetitious but it is true. When you help others – your value comes through loud and clear. They understand you and your value and can better help find you a job that matches your skills and abilities. Do not be shy – when someone is having difficulties – ask them how you can help.

#6 Keep a positive attitude throughout your search. Never bad mouth a previous job or employer for any reason. This is the golden rule, and it really applies to everything in life. If you are upset – keep it to yourself. Telling a prospective employer that XYZ was a terrible company to work for lets the HR team know that you are likely to badmouth them.

#7 When you get to an interview – be ready. Prepare 7 to 10 word answers to the most critical questions. Know your history and know something about the position and about the company. Know WHY you want to work there. Know what to ask when you are asked if you would like to ask them anything. Be ready to give examples of your skills like leadership and motivation, teamwork etc... One example is the great volunteer work you are doing for ISSA, RIGHT?

#8 Think of an interview as a sales call – when you get there - you are really selling yourself. So you got to the interview because you sold yourself in your resume. GREAT! Now you get another shot at selling yourself and make it right. KNOW why you are the best fit for the job. KNOW why you want the challenge of a specific position.

#9 During the interview - be fully ready to discuss your failures and challenges. Tell how you solved problems. If you have failed (and we ALL have) be ready to use this type of question as a turnaround so that you show you learned from your failures.

#10 Next time a potential employer asks you to email your resume, ask when you can bring one in person.

Now – let's talk about how I am about to ask you to open your mind to the exciting possibilities that the new economy is providing us with – understand that while the employers are holding off and not doing their own hiring (outsourcing and such) – this leads to changes in the workforce and to the speed with which employers are moving to hire new personnel.

There isn’t likely going to be any sustained corporate hiring of consultants or researchers until consistent economic data positive results are shown. This is to say that in the short term you will see fewer high paying jobs – Information Assurance, computer and network security, forensics, ethical hacking and industrial security are slightly lower than a few years ago. The good news is that all of those jobs are around and plentiful, AND all of those translate to a requirement for new full time staff at good salaries. Just don’t be surprised at slightly lower dollar amounts – and – don’t expect to see the really big bucks at least right away.

So - you want to get a job? Your first task is to figure out what kind of job you want, where you want it, what type of position is the employee classification such as Temp, regular full time, part-time, and so forth. You’ll also have to figure out which status is applicable such as: non-exempt, salary, hourly, or commission basis. You’ll need to know these items of information along with having a good idea about what the company wants in the position it is hiring for, what the company does, what it stands for, and what business target (customer) the company wants – all this before you go to any interview.

In short – know where you want to go and why - and know where the company stands, and where it wants to go. Ask yourself - are you in alignment with the company? Do you match the company goals and objectives? These are important considerations before you embark on the job search. If you are searching because you are already out of work – take heart – most people don’t do their homework so you’ll have a real advantage if you do the research and use your built-in network at ISSA-COS.

Now that we’ve talked about the first part – let’s look at the question - what do I need to do to get the job? Have you really looked at the job description? No – I mean have you “REALLY” looked at the job description? Is your skill level, experience, education, and outlook a good match for the position and the company.

Have you written a convincing cover letter for each different position applied to? There are several types of cover letters but generally speaking – the purpose of the cover letter is to map your case for exactly why your experiences are the right fit. This letter gives you the power to explain your interest in the company, your fit with their mission and values and the cover letter lets you identify your experiences in terms of the company’s self-interests. That’s right – think about the other side and make your case to show not HOW you are going to do something but WHAT you are going to do and WHY you are relevant. If you don’t have a seriously high level of interest and knowledge about the position – what can you hope to do for the company?
A hiring manager will not entertain the resume of a plumber’s apprentice for the job of executive administrative assistant and vice versa. Unless you have done a superb job at mapping the experiences you have that tie directly to the job description – you will fail at convincing you are the right person for the job. That’s right – you MUST show the company that you are applying for a position that is a direct match to the experiences you have. The company has plenty of applicants, and they want to find the one “best match” for the job. So – why hire you? Show them why in writing.

LET’S CREATE THE RESUME

When you are creating your resume use a standard format and standard terms for your industry. Use small words with big picture ideas. Skip the details. A hiring manager does not want to know how many times you swept the floor – he or she wants to know how YOU can deliver the cleanest floors on the planet for the least cost. He or she wants to know how you have been successful – how did you add value?

Use only 3 to 4 bullets that show how your work at that previous employer made a difference.

<table>
<thead>
<tr>
<th>Month/Year to Date</th>
<th>Company Name</th>
<th>Location, State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- How many $ did you save the company?
- How many # of Employees did you manage and at what level?
- What % of improvement was recognized because of the job you did?
- How did you personally help the bottom line?

Why should these specifics be important? Everyone wants to do a good job, right? Well, employers want to be certain that you are the one “right fit” for the job and their culture. If you don’t understand the job or the culture you are simply – NOT THE SINGLE BEST FIT or worse – you are NOT A FIT. If you did good things at your previous jobs but are simply along for the ride and did not make a difference – then why should any new company want you over the hundred or so other applicants? How many original ideas have you given the company to improve its market position? How many patents? How many published white papers, books, or seminars taught, etc…. ?

One note here (and often overlooked by job searchers) is that your prior success is the single most important factor / indicator of future success. Look at this as if your next job depends on it – because it does.

CAN YOU DO THE JOB? WILL YOU FIT IN? Are you certain that you are the “BEST FIT”?

Put “BEST FIT” into perspective: What if you had some type of critical medical life event that required the services of a “doctor”? Doctor X just graduated with the doctorate last week and while that might seem vague – it really does concern you. Let’s assume that you are a patient in a clinic – what about the specifics of that degree the doctor just received? A doctor could have a degree in computer science, law, philosophy, or veterinary medicine – among others.

Would any of these “doctors” be the first choice and best “fit” for your critical and potentially life-changing MEDICAL event? I think not. Companies look at their positions and desire the person to fix their pain. Tell them how you can do that in the cover letter and resume. Show them your repeated success.

Within the group called medical doctors some have many years of experience and yet their quality will fluctuate from doctor to doctor. Some have specific specialties. Ask yourself - do you have relevant, qualitative skills? Are you the one best fit? You must be very specific and show how you are that best fit.

Next on the list of items to look at are your qualifications. To a company that is working on Government contracts – there are requirements that must be met. That means that if a job requires a specific level of education or degree then you must have earned that degree to get that job. That will be true in nearly every case. If the qualifications call out 10 years of experience but you have 2 – then you are not likely a strong match. And don’t forget any required security clearances. You will not likely be considered unless there are no other candidates or, depending on the terms of the contract, you may not be considered at all.

Now that we’ve discussed the resume a bit – let’s be candid – the resume is only one thing that the company sees and the purpose of the resume is to get you into the interview.

WHAT CAN YOU DO TO GET YOURSELF IN THE RIGHT FRAME OF MIND FOR THE INTERVIEW?

So let’s assume you get the interview or two or three. Interviews are as unique as the interviewers themselves. Each company and each position will have specific matches so be prepared by studying the types of questions that can be asked and be prepared to remain calm throughout an interview or two. Here are some typical questions (and answers) to consider before going into your next interview. During the interview keep each of your answers to a maximum length (7 to 10 words) and let the interviewer drive the
Let the interviewer do most of the talking. Answer the questions and then be quiet. If the interviewer wants more information – let him or her ask. You will hear open ended questions like:

- Tell me about yourself.
- Explain what special strengths you bring to this position.
- What is your greatest weakness, and what have you done to correct it?

Watch out for open ended questions. Keep your answers short and to the point. Keep the focus on the job and the tasks that were within the job. Keep it impersonal. Talk about your job skills and not about your personal interests. The interviewer really does not care that you can hang 10 on your new 72.766 inch surfboard with sex wax that is ½ inch deep.

The interview is the time to turn your weaknesses into strengths. You could mention that people tell you that you work too much, but you typically get interested and excited in the work itself. Remember that the interviewer has likely heard a lot of answers so you’ll need to get some coaching if you haven’t done an interview in a while. Use what is called the behavioral interview format and sit with someone you don’t know to walk through questions in rapid succession. Make sure you know how to answer everything that is thrown at you.

The interviewer might ask: “Well what do you do for fun?” Remember - the company does not care that you are an ATARI 2600 gamer unless that is the job requirement or unless you are spending 16 hours a day as a gamer and only working 6 hours a day with 2 hours of sleep.

Your answers during an interview should contain much more about your job skills than your personal interests – keep answers short, positive and use the interview time to tell the interviewer why you seek this job and what you can do for the company. You will also hear questions that deal with your character:

- How important is punctuality?
- How are you with deadlines?
- How are you at multi-tasking?

These last three questions are saying that the company has URGENT needs to be ON-TIME with HIGH PRESSURE assignments in quick sequence. Are you up for that? Pay attention to the questions you are asked. Make a mental note of the expectations of the company as well as your expectations to check and see if they match. Another type of question will focus on your interpersonal skills:

- Describe a situation where you were able to use persuasion.
- Describe a situation where you had to think on your feet.
- Describe a situation where you had to use incomplete information and come to a decision …

These questions are about how you think and act on your thoughts. Are you a quick thinker? Can you relate times when you had to think quickly and deliver before you were ready? Were you successful? Are you ready in 7 to 10 words to show success? Another type of question deals with integrity, teamwork and championing issues:

- Give me an example of a time when you worked with a colleague who was not completing his or her share of the work. Who, if anyone, did you tell or talk to about it?
- Did the manager take any steps to correct your colleague?
- Did you agree or disagree with the managers actions?

Here the questions are about how you fit with the team. Are you a contrarian? Do you try to fit or fight the situation? Do you work well with others? Do you voice your opinion? Do you do what is right even in the case where you might be seen negatively? How strong are your values and how strong are the company values? What does the company think about integrity, voicing opinions and so on? Don’t know how the company culture acts and reacts – that’s what the ISSA Colorado Springs can bring to the table. With nearly 400 peer professionals you are sure to find someone who works at the company, has worked for the company, or knows someone …. YOUR NETWORK – USE IT.

These are only a few examples of what can be asked during an interview. Many interviewers will spend the most time asking about your failures and how you handled them because they want to know what you have learned and whether you could apply those solutions in their setting and culture. Other interviewers will ask about successes and what you could have done differently or better. Again – keep your answers brief – give the interviewer your confident and brief answers and no more.
DO YOU HAVE ANY QUESTIONS ABOUT OUR COMPANY?

If you have read this article – and you have done your homework about the prospective company you seek to work for – you will know plenty BEFORE the interview starts. Usually you are asked near the end of any interview if there is anything you would like to know about the company or the job. Most candidates either say that they can’t think of anything or simply answer “no” – which will send the wrong message to the interviewer. Saying “no” means you are not interested and your job during the interview is to show that you are interested. Do so by asking questions about the challenges that the company faces, the new markets that the company seeks to enter, the number of people you can expect to work with or supervise, education program, opportunity for advancement, the specifics of the working relationships (who would I report to), and the amount of travel and so forth. Please keep questions about vacation, salary, and work hours until after you have a job offer.

IS THERE ANYTHING YOU WOULD LIKE TO ASK US or ADD?

BY all means have a few questions ready to ask the company. Ask about the position, additional details about how the tasks are done, how learning is carried out, what the training program is like and so forth. Remember also, this is your opportunity to discuss your unique skills, abilities, or qualities that might interest the interviewer. Have you told the interviewer your secondary or alternative selling points? Here you could tell about a language you know that is applicable to the company’s operation in that country.

Also, consider this question another opportunity to correct a previously given answer that you thought didn’t come out right, or that you might not have liked when you gave. Oh – WHY ARE YOU THE BEST CANDIDATE FOR THIS JOB? TELL THE INTERVIEWER.

If you are applying for a new job and would like a review of your resume, please send your resume with a copy of the job description to Tim Hoffman, Executive Vice President, ISSA-COS, at:

tim.hoffman@alidaconnection.net.

Part II of this article will be in next month's issue.

Tim Hoffman
ISSA-COS
Executive Vice President

Tim is a well-known consultant, trainer, former radio show host, and co-author of four technical books published by Prentice Hall PTR. He has extensive experience with security of wired and wireless networks, and computers and telecommunications that dates from 1969. He has worked with Fortune 1000 to small businesses, helped start small businesses of his own, and is currently the President and Owner of the Alida Connection, a VA Approved Veteran Owned Small Business that provides computer security consulting and technical training. Tim holds an MS, CISSP, GCIH, ISP, C|EH, Expert Rating PmP, CTT+, Security+ and Network+ and a range of other certifications. He consults, teaches and writes about computer and network security, TCP/IP, CISCO and most other vendor BackOffice technologies.
Failed Attack Leaves Clues to Anonymous Activities

New evidence from a failed attack on the Vatican provides insight on how the hacker group Anonymous operates.

The attack on the Vatican was a 25 day siege designed to disrupt the visit of the Pope to Madrid for World Youth Day.

Computer forensics show that a small group of individuals, who are probably skilled hackers, spent 19 of the 25 days searching the site for any holes that could be exploited to break into the system. Only when this strategy failed did Anonymous progress with the Distributed Denial of Service (DDoS) attack against the Vatican, meaning that all those DDoS attacks we’ve seen are probably just because Anonymous couldn’t get in to steal information.


How hackers are caught out by law enforcers

The internet has gained a reputation as somewhere you can say and do anything with impunity, primarily because it is easy to disguise your identity.

This feature has proved particularly helpful to hackers, many of whom have developed a feeling of invulnerability, and even boast that they will never be caught.

However, the arrests of members of the hacker group Lulzsec this week, and some other recent but less high-profile arrests, show that the authorities are not quite as impotent as many would have you believe.

Increasingly, hackers' boasts are followed shortly afterwards by a surprise visit from the local police. So, how do these investigators catch these new-age criminals?

Source: http://www.bbc.co.uk/news/technology-17302656

Anonymous members tricked into giving up bank details

Members of Anonymous regularly band together to take down websites owned by those they don’t like, but security firm Symantec reports that a recent attack could actually have backfired, putting amateur hacktavists’ bank accounts at risk.

Anonymous uses tools such as the Low Orbit Ion Cannon or Slowloris to perform distributed denial-of-service (DDoS) attacks against its targets, with sympathetic Anons downloading the software to become part of a voluntary botnet.

In January the group decided to hit the websites of the US Department of Justice and various media companies in response to the takedown of file storage site Megaupload, providing a guide on Pastebin for those who wished to take part in the attacks. Symantec says that an attacker appears to have copied that guide and inserted their own version of the Slowloris software containing a secret Trojan that downloaded a copy of Zeus, a piece of malware often used to take control of an infected computer.

Computers infected with the malware still took part in the Anonymous DDoS attacks, but were also secretly sending online bank account and webmail logins back to the attacker. Anonymous members have tweeted links to this fake guide nearly 500 times, referring to it as "Tools of the DDos trade" and "Idiot's Guide to Be Anonymous."

"Not only will supporters be breaking the law by participating in DDoS attacks on Anonymous hacktivism targets, but may also be at risk of having their online banking and email credentials stolen," says Symantec. "The joining of malicious financial and identity fraud malware, Anonymous hacktivism objectives, and Anonymous supporter deception is a dangerous development for the online world."

Source: http://www.newscientist.com/blogs/onepercent/2012/03/anonymous-members-tricked-into.html
China Has A Scary Plan

by James Dunnigan, March 17, 2012

March 1, 2012: The U.S. Department of Defense believes that China's military strategy relies heavily on over a decade of penetrating American government, military and commercial computer networks. These penetrations, many of them never discovered, were mainly to steal technical data for commercial products. But a lot of military, diplomatic and weapons data was obtained as well. The Department of Defense has been pleading with Congress for help in this area, but Cyber War defense is not sexy, so American defenses remain weak, and the Chinese keep at it.

China uses all this Internet based theft to improve Chinese military capabilities, and weaken American ones. Department of Defense officials also see China's ambitious space program as another component of Chinese military strategy. By combining the ability to knock down American military satellites, while at the same time launching Internet based attacks at American military, government and commercial Internet activities, China believes it could make up for a lot of current American military superiority. At the very least, the Chinese believe that all this stolen (via the Internet) data and damage to American space satellites would cripple American military power aimed at China.

This is all consistent with Chinese strategic thinking. Chinese leaders are very much aware of historical lessons, and the writing of the ancient Chinese military writer Sun Tzu. This sage was a big proponent of the indirect approach, and winning wars without much fighting. The Chinese particularly admire the American ability to fight so often, but suffer such low casualties, and seek to do that against the American. Not all of Sun Tzu's advice is still applicable, but he was a big believer in doing what the enemy did not expect, and exploiting enemy weaknesses. Sun Tzu lived 2,500 years ago, in a world that could not conceive of something like the Internet, or space satellites. But Sun Tzu understood the value of information, communications and secrets. That's what China is concentrating on now, and it has the Department of Defense nervous.

http://www.strategypage.com/htmw/htiw/articles/20120301.aspx

Occupying the High Ground

Bill Gertz - March 8, 2012 8:17 am

China's military has developed highly sophisticated cyber warfare capabilities that would be used to cripple computer networks at the U.S. Pacific Command and U.S. Transportation Command that would direct American forces to defend Taiwan in a future conflict, according to a congressional report.

The cyber attacks would begin weeks before actual hostilities, as cyber warriors associated with two units of the People's Liberation Army secretly penetrate networks and plant sleeper software that can destroy both hardware and software needed for moving and commanding troops and forces across the Pacific, according to a new report by the congressional U.S.-China Economic and Security Review Commission.

"Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict," the report states.

The 136-page report, “Occupying the Information High Ground,” (found here: http://web.docuticker.com/go/docubase/68226) was produced by Northrop Grumman for the commission. It ... is based on Chinese military writings, Chinese government statements, and public analysis of recent Chinese intrusions into public and private computer systems.

China Commission Chairman Dennis Shea said in releasing the report that the United States has been a victim of continuous cyber operations “sanctioned or tolerated by the Chinese government.”

“Our nation's national and economic security are threatened, and as the Chinese government funds research to improve its advanced cyber capabilities these threats will continue to grow,” Shea said.

Said commission member Michael Wessel: “It's getting harder and harder for China's leaders to claim ignorance and innocence as to the massive electronic reconnaissance and cyber intrusions activities directed by Chinese interests at the U.S. government and our private sector.”

Read the rest at: http://freebeacon.com/the-coming-china-cyberwar/
## Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 18</td>
<td>11:00 to 1:00</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121</td>
</tr>
<tr>
<td>May 23</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jun 20</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jul 18</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Aug 15</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 19</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 17</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec TBD</td>
<td>11:00 to 1:00</td>
<td>Carrabba's North</td>
</tr>
</tbody>
</table>

## Training

**DISSA/Navy security tools class...** 14 April, 28 April and 5 May

**Security+...** June 9, and September 8

**CISSP...** June 2, 16, and 30; July 14 and 28

**(ISC)2 Exam...** 18 August

**Learning Strategies Course** (Tentative)... April/May timeframe; details being worked out

## Upcoming ISSA Events

- **May 16-17**, Wednesday and Thursday, CISO Conference (Denver)
- **Aug 1-2**, Wednesday and Thursday, Crowne Plaza Hotel (CSTC)
- **Oct 24-26**, Wednesday through Friday, Disney Hotel, Anaheim, ISSA Annual Conference
- **Nov Conference**, **Friday, Nov 16, Crowne Plaza Hotel**, 7:30 – 5:00
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at doncreamer@q.com or william.creamer.ctr@us.af.mil

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

The Little White Box That Can Hack Your Network