



E-Telligence

2009 Calendar of Events

- March 3-4, 2009
CyberSecurity Applications and Technology Conference
Washington, DC, USA
[Click here](#)
- March 29-April 1, 2009
Cambridge University Internet Intelligence Conference
Cambridge, UK
[Click here](#)
- April 13-16, 2009
APWG Spring Counter-eCrime Operations Summit
Barcelona, Spain
[Click here](#)
- April 20-24, 2009
18th Annual International World Wide Web Conference
Madrid, Spain
[Click here](#)
- April 27-29, 2009
Critical Infrastructure and Security Risk Vulnerability Workshop
Vancouver, BC, Canada
[Click here](#)
- May 12-14, 2009
APWG Spring Counter-eCrime Operations Summit
Barcelona, Spain
[Click here](#)
- June 9-11, 2009
Kestenberg Siegal Lipkus LLP Anti-Counterfeiting Training Conference
Vancouver, BC Canada
[Click here](#)
- June 18-19, 2009
Tri-Lateral Security Conference
Calgary, AB, Canada
[Click here](#)
- July 10-12, 2009
Video Game Cultures and Future of Interactive Entertainment Conference
Mansfield College, Oxford, UK
[Click here](#)

HEADLINE NEWS — February 18, 2009

What's New on the Frontline!

Self-Professed Geek Wows Security Community

By *Kathy Macdonald*

Dr. Phyllis Schneck, vice-president of cyber intelligence and critical infrastructure protection for McAfee Inc., recently spoke in Calgary, to a packed room of members from the Security Professionals Information Exchange (SPIE). Local member Troy Davidson, an incident response analyst with the Energy Resource Conservation Board, worked diligently to coordinate Phyllis's whirlwind trip from a mild Atlanta to a chilly Calgary. The weather almost forced Phyllis to wear the elbow-length, reinforced, ultra-warm snowmobile gloves she had packed, just in case, in her briefcase.

The audience listened intently as Phyllis spoke enthusiastically about the value of information sharing and reaching out to the grass roots, small and medium-sized companies. "Build it and they will come applies in the situation," said Phyllis. After all, this is how InfraGard got started back in 1996, when business members from Cleveland cooperated with the FBI on a cyber threat case. The FBI then realized the value of attracting companies to help solve crime. This idea has now grown to include almost 30,000 members from across the U.S. and it also began a lengthy career for Phyllis, culminating in her position as chair on the National Executive Board of InfraGard and the founding president of InfraGard Atlanta. Today, she is now a chairman emeritus.

InfraGard, a U.S.-based organization, is a partnership between the FBI and the private sector. This includes thousands of FBI agents as well as thousands of representatives from 350 of the top Fortune 500 companies in the United States. Their website indicates that members also represent academic institutions, state and local law enforcement agencies — all dedicated to sharing information concerning various terrorism, intelligence, criminal, and security matters. In exchange, members gain access to information that enables them to protect their corporate assets more effectively.

Phyllis was mostly responsible for the strategic growth and vision of the private sector side of the InfraGard Program. She has also been recognized for expanding the relationship between InfraGard and the Department of Homeland Security. Phyllis spoke candidly about her time with InfraGard and the importance of building partnerships to collaborate, exchange ideas and, most importantly, to understand, "who to talk to in time of a crisis." Engaging members as a resource, Phyllis said, helped InfraGard use the community for preparing, planning, information gathering and building trust, and it also helped in "humanizing the FBI." Phyllis made the audience laugh when she told a story about flying with about 80 FBI agents on an assignment.

After inspecting the same identification from all of these FBI agents, her turn came up to produce her credentials. It was at this point, the airline employee looked at Phyllis and then turned to FBI agent standing next to her and asked, "and who is your prisoner?" As a patent holder, advisor, author, thought leader and a person voted as one of Information Security Magazine's Top 20 Women Leaders in Information Security, she is also genuinely warm and engaging. As a self-professed geek, Dr. Schneck continues her work in the area of cyber security and, today, she holds a distinguished presence in the security and infrastructure protection community.

Phyllis knows who to talk to in time of a crisis, and now, so do we.

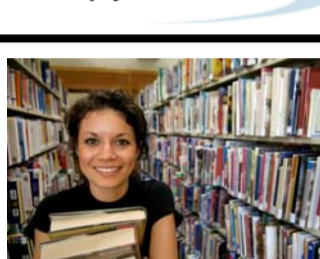


Welcome to E-Telligence

Twice a month, we'll be profiling guest writers, cyber crime news and important events to keep you informed.

Part 2: Using the Internet as an Investigative Research and Open Source Intelligence (OSINT) Tool

By *David Toddington, Founder and President, Toddington International Inc.*
The following is part two in a two-part series. Part one can be found at www.gcsc.org.



The Deep Web and User Generated Content

While the basic search engines represent an invaluable resource to the online investigator, there are many other specialized search and reference sites that should be explored and exploited to fully take advantage of the Internet as an investigative research and intelligence tool.

While knowing how to effectively query a search engine's database is an important step in becoming a good Internet investigator, consider the importance of knowing *where* to ask the question. It is now deep web and web 2.0 sites that hold the largest share of information available on the web.

Deep web fee-for-service sites such as Lexis-Nexis, Dunn and Bradstreet, Researcha and Equifax can provide essential data on a person or company's credit history among other things. While fee-for-service deep web sites can often be expensive to use, in today's world of increasingly restricted budgets, it is important to note that some 95 per cent of deep web sites are not subject to charges or subscriptions.

In the social networking strata of web 2.0, Facebook, MySpace and Friends Reunited, these sites have proven invaluable in locating persons based on a database in which users voluntarily submit personal details.

And it is not just the information people leave about themselves on social networking sites that may be of value to you; consider the worth of what the associates of the primary subject of your investigation may be saying about them. Second party "chatter" on web logs (or blogs) and social network sites about the prime subject of an investigation has proven invaluable time and time again in successfully concluding operational files.

Deep Web Resources

An excellent starting point for finding a number of useful deep web sites is Complete Planet at www.completeplanet.com. Compiled by a team of human editors, this well organized site provides links to and ratings for many specialized, searchable databases.

The number of law enforcement specific deep web sites available to the general public may surprise some online investigators. The Canadian Police Information Centre website at www.cpic-cipc.ca allows members of the general public to conduct their own checks for stolen vehicles and property based on vehicle identification number, license plate or other serial number. While the CPIC website will not provide the detailed results available to an authorized police user, it will indicate to a member of the public whether an item is on file as being stolen along with an advisement to contact local police.

A site that has proven very useful in a number of investigations that demand the location of old or unavailable web documents is the Wayback Machine operated by the Internet Archive at www.archive.org. Founded in 1996, the San Francisco-based Internet Archive was created in order to build a digital library, offering permanent and free access to researchers, historians, scholars, and the general public. The archive currently holds a collection of well over 85 billion archived web pages dating back 12 years.

Targeted to US based private investigators, the Black Book Online at www.blackbookonline.info provides links to numerous law enforcement related resources including sex offender registries, inmate locators and aircraft/vessel databases. Two outstanding people search sites are located at www.zoominfo.com and www.zabasearch.com.

Challenges and Dangers

As the web continues to grow at an increasing pace, key challenges will continue to face online investigators. Language will pose a significant problem for many. English continues to decline as the primary language spoken by Internet users globally (29 per cent of online users as of December 2008) as Chinese, Spanish and Japanese language populations proportionally increase. Arabic is currently the fastest growing online language population with a 1,576 per cent increase in users between 2000 and 2007.

Changing language demographics mean that, particularly within the web 2.0 sphere, the information an investigator may be looking for could well be available in a language not spoken by them – search queries need to be translated and conducted in a foreign language.

By identifying the unique Internet protocol address used by a web investigator to access the Internet, it may be possible for the target web site administrator to make specific assumptions about where an investigator is and what agency they represent during a visit to that site. As a complex issue that cannot be adequately covered in this article, investigators should be very cautious when viewing sensitive web sites via a network that could be identifiable to their agency. Privacy software is strongly recommended for even routine online research either in the form of a web-based proxy server such as the Cloak (www.the-cloak.com) or installed software such as Tor (www.torproject.org).

Investigators must be highly cautious when employing deception to elicit information from other Internet users (for example, by posting to message boards or participating in chat rooms). Legislation, such as the UK Regulation of Investigatory Powers Act and/or agency policy may dictate that specific legal requirements must be met.

Conclusion

Given the anarchic nature of the Internet, online investigators require basic and ongoing training in order to be effective in finding online information and critically evaluating the data found. Dedicated equipment, Internet connectivity and adequate provision for security all play a critical role in effective online investigations. To become and remain effective, unique strategies specific to many different types of investigations will have to be developed.

Today, the Internet is playing an increasing and essential role in both reactive and proactive police operations. Cost effective and of significant value to front line investigators and senior managers alike, the Internet will continue to grow in importance in our day-to-day lives.

David Toddington will be teaching Internet Intelligence for ICC Commercial Services — a three-day course at Cambridge University on How to Use the Internet as an Effective Investigative Research Tool, March 29-April 01, 2009 (please see the link in this newsletter's calendar of events).

Toddington International Inc. provides a variety of specialized classroom and distance learning online investigative and research training programs to both the public and private sector and is a supplier to a number of police and government agencies in both the UK and Canada.

In partnership with the RCMP Pacific Region Training Centre, the Canadian Police College and the Ontario Police College, TII delivers a number of accredited, comprehensive 5-day classroom based training programs on using the Internet as an effective police research tool.

In partnership with the OPC, TII offer an in-depth distance learning program. For more information and to sign up for the free bi-monthly Online Research Newsletter, visit www.toddington.com

Websites you should visit...

- InfraGard
www.infragard.net
- Department of Homeland Security
www.dhs.gov
- SANS Computer Virus Alerts and Warnings
www.incidents.org
- Fourth Annual Tri-Lateral Security Conference in Calgary
<http://www.trilateralcalgary.ca>

If you need to print...



The E-Telligence newsletter is a green document and is not designed to be printed.

If you wish to print an article, just copy and paste the information into a Word document and print in the normal manner. The environment thanks you!

A Report from the SANS SCADA Security Summit



February 2009

Orlando, Florida

What do the movies Die Hard 4, Eagle Eye and this season of the TV series 24 all have as a common theme? The answer — Critical Infrastructure (CI) or more specifically, the ease at which rogue nations and individuals can usurp and take over systems that we depend on to survive in our daily life. It was these systems, their methods of communicating and the interdependence with each other, that was at the heart of discussions at this year's SANS SCADA Security Summit in Orlando, Florida.

What exactly is considered critical infrastructure? Both the United States and Canada have identified the following key sectors to be considered CI: electrical generation/grid, oil and gas pipelines, water works/treatment, food processing, chemical refineries, transportation (highways, airports, and rail lines), telecommunications, government and emergency services. What is not completely understood is that, in many of these sectors the systems that control our dams, runway lights, compressor stations and relief valves that happen to separate sewage from our drinking water and more, are becoming highly vulnerable.

SCADA stands for "Supervisory Control and Data Acquisition" and is the common thread that links together software used to control valves and switches used at industrial centers. Security of these systems was never considered a major concern, especially in the 1980s and 90s, as most SCADA systems were isolated and separated from any other IT or network system. But, in the past decade, a new trend emerged that found these SCADA systems starting to be networked together over phone, satellite and most interestingly, the Internet. Of greater risk was that they were utilizing more open and less proprietary standards. It is because of this progression of being a unique and proprietary environment, to a more open standardized environment, that leads many to question the security of SCADA systems and their vulnerability to cyber-warfare and cyber-terrorism attacks.

There is a fear that a great "cybergeddon" attack could take place which has subsequently raised the level of attention to these networks. In fact, the FBI holds cyber attacks, especially against critical infrastructure and SCADA systems, immediately below nuclear and WMD attacks, as the greatest threat to the United States.

Worryingly, it is believed that this has already happened as reported by a senior CIA analyst, Tom Donahue. "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge," Donahue said at last year's 2008 SANS event. What was further revealed at this year's event was that a U.S. electrical power utility had its control system taken over and held hostage. The intent was to extort money from the company, not unlike what has happened in the past to online casinos. In this case, though, the attackers apparently were successful in taking offline this company's power generators thus cutting the lights out to three geographical areas.

Of additional interest at the conference were presentations highlighting the fact that what was once obscure (SCADA) is now beginning to gain the focus of attention by software security researchers and malicious users. There is clearly an upward trend to more vulnerability alerts of SCADA software being disclosed and corresponding network activity witnessed trying to take advantage of these flaws. Hackers find the ability to turn the lights off to a whole city via a computer system "sexy" and foreign nation states see the effectiveness of high profile attacks such as the cyber conflict between Russia vs. Estonia, a few years back.

The challenges being faced by those of us affected by this new threat are not to be underestimated. All organizations who have substantial SCADA and other industrial process control systems, must deal with the fact that their legacy environment that has been shaded in the dark by its isolation are feeling the pain of the new spotlight shining on them.

Currently, the U.S. government is attempting to get industry to respond to this concern by the introduction of new regulations. The first on the target list was the electrical generation sector, which has had two years to comply with the NERC cyber security regulations. This forces the organizations to ensure that their critical cyber assets are reliable and secure by becoming compliant to a series of nine specific control areas. Several conference attendees feel that it is likely that this framework will be applied to other critical infrastructure sectors.

A refreshing leap forward at the summit was work done by the Idaho National Labs. This organization is trying to research and identify the security risks of industrial control systems apparatus and provide corresponding mitigation approaches. Many of the conference attendees were fortunate to be able to take advantage of a free training course sponsored by the U.S. Government and a half dozen of the National SCADA Test Bed program members from Idaho National Labs. These are the individuals who are attempting to support industry and government to enhance the cyber security of control systems used through the electricity, oil and gas industries. It is not everyday that one would have access to real SCADA equipment, available to hands-on access and run by security tools in real time. This exercise makes one fully understand how easy and fragile these systems really are.

We left this conference realizing that it is only a very thin thread that separates the 21st century luxurious, digital lifestyle from that of the hardworking, 19th century homesteaders. Each time we flip a switch to turn the lights on, or turn the heat up on our natural gas fueled furnace, drink a glass of water from the tap or land a plane on a runway, we need to understand the sheer dependence we have on these potentially vulnerable control systems. Thankfully, critical infrastructure protection is now finally getting the attention it deserves. Let's hold off looking for a horse drawn buggy or an oil lamp...for the time being anyhow.

Lars Maul (CISSP, CISM, CISA, CGEIT, MCSE) is head of information security at Alliance Pipeline, a natural gas transport company. He has over 10 years experience in information security. He is currently the vice-president of the High Tech Crime Investigation Association – Western Canada Chapter.

You'll be Interested in This

Cybersecurity Applications and Technology Conference

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate is pleased to announce their first Cybersecurity Applications and Technology Conference for Homeland Security (CATCH) to be held March 3-4, 2009, at the Washington DC Convention Center. This conference represents the culmination of significant DHS S&T research programs and a progress report on other programs and will showcase the results of many research efforts during both the program and exposition. The goal is to stimulate scientists, developers, and operational customers with research products, experimental results, and capabilities emerging from DHS S&T research to better address operational needs for information security. The hope is that CATCH will provide an opportunity for information and technology exchange between DHS S&T research scientists and practitioners of information security technologies. ([go to web site](#))

Malware Writers Use Multiple Botnets to Spread Valentine's Day Heartache

A successor to the Storm botnet that worried security managers in 2007, the Waledac botnet is believed by experts to be the source of a massive Valentine's Day spam campaign. Researchers at Marshal8e6, an Internet email and security provider, have discovered at least two other botnets assisting Waledac in the campaign, in addition to numerous spam attacks from other unidentified sources. The Waledac botnet was spotted in late 2008, not long after Microsoft's malicious software removal tool eradicated the Storm botnet in September 2008, says Marshal8e6's Patrick Murray. Like its predecessor, Waledac relies on peer-to-peer connections with fast-flux Domain Name System capabilities and secured communication. Researchers believe Waledac may employ as many as 20,000 bots that could be responsible for as much as 1 percent of all spam volume. ([go to web site](#))

THINK BEFORE YOU POST



New information for kids from the CyberTipline at www.missingkids.com

Webcams, microphones, and digital cameras allow you to post videos, photos, and audio files online and engage in video conversations. Webcam sessions and photos can be easily captured, and users can continue to circulate those images online. In some cases, people believed they were interacting with trusted friends but later found their images were distributed to others or posted on web sites. You may come across offensive or inappropriate images and videos while surfing the web.

Caution

- Use webcams or post photos online only with your parents or guardian's knowledge and supervision.
- Ask yourself if you would be embarrassed if your friends or family saw the pictures or video you post online. If the answer is yes, then you need to stop.
- Be aware of what is in the camera's field of vision and remember to turn the camera off when it is not in use.
- Be careful about posting identity-revealing or sexually provocative photos. Don't post photos of others — even your friends — without permission from your friend's parents or guardians. Remember, once such images are posted you give up control of them and you can never get them back.

What to report

- Anyone you don't know who asks you for personal information, photos or videos.
- Unsolicited obscene material from people or companies you don't know.
- Misleading URLs on the Internet that point you to sites containing harmful materials rather than what you were looking for.
- Anyone who wants to send you photos or videos containing obscene content of individuals 18 and younger. (The possession, manufacturing, and distributing of child pornography is illegal.)
- Online enticement for offline sexual activities. (No one should be making sexual invitations to you adults — and it's an especially serious crime for adults to do it.)