

VERMONT INFRAGARD ORGANIZATIONAL MEETING

Norwich University Visitors' Center
Northfield, VT
2001-04-26

1 Participants

Tom Aldrich, taldrich@norwich.edu
George Bakos, alpinista@bigfoot.com
Scott Burleson, sburleson@raircityis.com
Randy Hannett, rhannett@symquest.com
Peter Hartshorn, phartshorn@st-vt.com
Bill Holden, bholden3877@yahoo.com
Lisa Holmes, lholfmesvfk@cs.com
Rick Jean, rjean@uhfa.org
Mich Kabay, mkabay@compuserve.com
Gary Kessler, kumquat@sover.net
Shane Kraus, gunner94@mindless.com
Bill Kuhns, wkuhns@vmec.org
Thomas Leene, tleene@leo.gov
Paul Love, epl@internet2.edu
Chris MacAskill, cmacaskill@uhfa.org
Mike Maxwell, mmaxwell@gmavt.net
CJ Moses, cmoses@leo.gov
Richard Moss, rmoss@rsmcpa.com
Wes Parker, wparker@gmavt.net
Tom Paulger, tpaulger@dps.state.vt.us
Marc Reynolds, ptrust01@together.net
Bill Scherr, bscherr@ampeisch.com
John Sennett, jsennett@leo.gov
Joshua Silman, gnome@sover.net
Randy Spooner, rgs@netserve.uvm.edu
Mike Stridsberg, stridsberg@idx.com
Jeff Tarte, jtarte@chittenden.com
Mike Vance, mjvance@gmavt.net
Eric Whyne, root@erudite-aegis.org

2 Greetings and Welcome

- 2.1 Participant sign-in and introductions
- 2.2 Introductions & Guests
 - 2.2.1 Gary Kessler
 - Thanks to Tom Aldrich and Norwich University for the invitation to use the facilities.
 - Appreciate help from NIPC and Albany FBI.
 - Need to work out organizational details
 - 2.2.2 Tom Aldrich, Norwich University
 - 2.2.3 Beth Maher & John Sennet, FBI, Albany
 - 2.2.4 Katherine Bursese, RPI, Albany InfraGard
 - 2.2.5 CJ Moses, FBI, Washington, D.C.

3 Carl J. “CJ” Moses < cmoses@leo.gov >:

Supervisory Special Agent
Chief, Inter-Agency Coordination Cell
National Infrastructure Protection Center
FBI
935 Pennsylvania Ave NW
Washington DC 20535

"The State of the Hack"

- 3.1 Primary duties at NIPC: coordinate counter-intelligence and counter-terrorism programs
- 3.2 Significant changes since end of Cold War
 - Solar Sunrise investigated penetration of military computers — worried about international threat; but showed Cloverdale, CA teenagers guided by Ehud Tenenbaum of Israel (“Analyzer”)
 - New risks and threats coming from global interconnection of infrastructural systems and potential attackers
 - Asymmetric warfare: tools easily available & do not require high expertise
- 3.3 Threats and vulnerabilities
 - Electronic vulnerabilities not generally known; e.g., protect wallets and homes with locks but fail to protect Internet connections
 - Criminal hackers
 - Organized crime (e.g., CitiBank attack by Vladimir Levin et al.)
 - Electronic terrorism (e.g., infrastructure attacks) — and does the bloodless nature encourage terrorism?
 - Hacktivists
 - Trans-national Hacktivism (e.g., Balkans, China/Japan, China/Taiwan, China/US)
 - Hate groups (e.g., holocaust revisionists)
 - Terrorist groups (e.g., Tamil Tigers)
 - Industrial espionage
 - Foreign intelligence services (e.g., France, Russia, China)

- 3.4 Information warfare
 - Video clip from 60 Minutes discusses 100 govts capable of interfering with US infrastrucrure
 - Infrastructure damage and espionage have been shown to win wars in the past
 - Gas & oil storage and delivery
 - Water supply system
 - Banking and finance
 - Transport
 - Electricity
 - Transport
 - Health care
 - Government services
- 3.5 Civilian/law-enforcement cooperation: Computer crime marks probably the larges field of crime where non law-enforcement personnel can play a critical role in investigation and prosecution
- 3.6 Computer security integrates all security disciplines
 - OPSEC
 - Physical security
 - COMSEC
 - Personnel security – the foundation of all the other disciplines
- 3.7 Goals
 - Anticipate the evolution of computer crime by understanding the goal of the perpetrators
 - Know the opposition's playbook
- 3.8 Hacker goals:
 - Avoid monitoring
 - Avoid detection
 - Theft & fraud
 - Espionage
 - Vandalism
 - Hacktivism
 - Plausible deniability
- 3.9 Recent hacker methods
 - 3.9.1 DDoS – e.g., “NetJam” in Feb 2000
 - 3.9.2 New versions of DDoS tools attack domestic (home) computers on DSL or cable connections – extremely difficult to counter DDoS
 - 3.9.3 HTTP Tunneling
 - Pirate client inserted into client system inside the firewall
 - Client automatically launched at specific time
 - Hacker runs server that passes commands to client
 - Data transfers passed in clear via cookies
 - 3.9.4 ICMP and UDP Cover Channeling
 - Loki – tool capitalizes on lack of firewall screening for ICMP
 - ICMP packets then used as covert channel
 - Loki client software uses echo requests and echo reply packets to transfer data outside

3.9.5 Windows DLL hacks

- IE4 and IE5 allow plugins as DLLs for automatic background execution
- Plugins can run when any function is hooked; e.g., “open document”
- App_dll Key is a blank dll that waits for input

3.9.6 Knark

- Kernel-Based Rootkit for Linux 2.2
- Knark.e is linux loadable kernel module
- Can alter system calls to point to unauthorized functions
- Variants have allowed keystroke capture, hiding files and directories, adding new features to the operating system
- Example: can hide promiscuous mode by hiding the “promise” flag; hide files; hide processes; redirect commands to alternative commands or scripts; get root
- Still not widely used, but very dangerous and will likely become a tool of choice for attackers

3.10 Concluding remarks

- Need partnership between technical community and law enforcement
- Specific countries will openly become enemies
- National security requires infrastructure protection
- If we leave our electronic control and communications systems wide open, we will become increasingly vulnerable

3.11 A note about Carnivore

3.12 Discussion

3.12.1 Q: What’s the hangup in working with ISPs to stop DDoS? A: We have a small staff but are getting collaboration from the backbone providers. Q: However, in our experience, the backbone providers have failed to provide concrete measures for blocking broadcast storms.

- Will the list we have established provide technical information for us? A: Well, we have to decide if our list should duplicate the material available from public sources such as CERT-CC.
- We find that ISPs respond with a security focus when a big client threatens not to sign a contract without proper security measures in place.
- Legal issues — some ISP lawyers have argued that users could become liable for downstream damage

3.13 Real problem – Gary Kessler discussed case of teenager who installed Sub7 onto friend’s home machine – tried extortion – no idea of moral or legal issues

3.14 ANSIR alerts from FBI

- one-way transfer of information from LE to government agencies and private industry
- DoD used to give employee-awareness training about foreign threat
- Now FBI covers foreign government intelligence efforts and other threats
- Can receive information automatically by e-mail
- To subscribe, send request with your name, e-mail address, organization to <jsennett@leo.gov >

4 A brief overview of InfraGard

4.1 Beth Maher: The Albany FBI Chapter perspective

4.1.1 Benefits

- Speakers
- Networking sessions immensely valuable
- Different sectors exchange info — much overlap, commonality

4.1.2 Example of interesting cases

- Repeated probes don't usually get followed up through investigation and prosecutions
- But some attacks have resulted in initiation of cases and eventual prosecutions
- One member (NY State agency) reported repeated hits on 3 different agencies; forwarded info to Beth. Working group tied the origin to a foreign country (Asian); sent info to NIPC. Advantage for NIPC is that they can correlate separate info streams, resulting in a NIPC Advisory that helps everyone about the problem.

4.1.3 Fundamental goal: protect everyone's systems to reduce need for investigations and prosecutions

4.1.4 Recent news reports (e.g., Wired) suggest plans for coordinated attacks by Chinese hackers at the start of May.

4.1.5 The application

- Can call Tom Leene, but perhaps we can avoid having him answer repeat questions
- Lowest level of application is simple contact sheet. Paragraph asks whether company or entity wants to be protected — i.e., confidentiality requirement to prevent disclosure of identity and details of cooperation. Most people check YES to preclude public visibility of name and organization.
- Page 8 of 8: InfraGard Member is the organization you work for, not the individual person. Designated rep: your name; will receive communications, software, passwords. This level of participation grants access to a secure Web page (which is not available if you sign only the first page). There is a minor background investigation involving DMV records and the like.
- It is possible to have multiple representatives from an organization; just fill out an application for each contact.
- Need an authorized signer from the employer plus a witness to the signature (anyone).
- Next: page 1 of 1 — your name as rep plus signature, residence, place of birth, Social Security Number.
- In Albany, the chapter charges for meetings to pay for lunch; have a corporate sponsor who pays for speakers, brochures etc.

4.1.6 How we organized

- Steering committee organized first meeting
- Asked for volunteers to get started
- Had first election in January 2001 for Board of Directors
- Active chapter; lots of response. Next meeting May 2 (all invited) at MetLife; already 60 people reserved places
- Meetings monthly or every two months

- Membership is to the overall organization, so it is possible to affiliate with any chapter (rep easily transferred to another chapter when moving to another location)
- 4.1.7 FOIA
- Some concern about whether Freedom of Information Act could force disclosure of confidential information from members
 - But FBI is NOT the organizing body, nor are FBI agents allowed to be members
 - Therefore FOIA, which applies only to government agencies, cannot apply to our discussions
- 4.1.8 Web site: < <http://albanyinfragard.logical.net> >
- 4.1.9 Discussion
- About the Albany chapter: do you maintain a pool of expertise on which members can draw? What if we had an incident and needed help with a technology we don't know about — can you tell us who would be a good resource for us? A: Beth sanitized the message and sent it out to everyone — got an answer quickly.
 - This organization can be an information coordination center so we can share information confidentially. The amazing thing about this process is that INFOSEC professionals are crawling out of the woodwork.
 - List coordinator can anonymize requests for help as requested and either have answers broadcast to list or sent directly to requester.
 - I-4 from AtomicTangerine charges \$25,000 for similar networking — and has been very successful and valuable.
 - What if someone has an answer and wants to charge for the answer — is that consistent with the InfraGard approach? NO. Nothing wrong with networking and discussing business, but not trolling for contracts and sales.
 - If an incident warrants prosecution, the information is considered confidential. If law enforcement express interest in a case, the victim has the right to agree or refuse such contact (except for mandated reporting such as child abuse, child pornography). As far as we know (as non-lawyers), there is no protection for members and coordinators that would obviate their responsibilities under the law to report specific kinds of crime.
- 4.2 A user perspective: Katherine Bursese, Rensselaer Polytechnic Institute < bursek@rpi.edu >
- 4.2.1 How I got involved
- 5.5 years ago was a UNIX programmer; had an FBI agent appear at her door
 - student at RPI had launched 2-day DoS attack on a Texas ISP via a Rutgers computer
 - terms of service were out of date
 - didn't know how to help FBI
 - called Dean of Students, who sent her to RPI legal — who said, “I dunno, what do you think?”
 - Took 8 people a week to figure out what to do — InfraGard would have been a great help.
- 4.2.2 Current situation
- We have a security team
 - Beth came to give a talk on espionage; mentioned InfraGard chapter
 - Saw value of having relationship with LE before there's a crisis
 - Have staff aware of LE issues

- Some concerns about Big Brother
 - RPI Legal looked at agreement
 - Started forming chapter
 - The networking, education, information disovulation ☺ that is really valuable
 - The wider the group of people communicating, the more tools you'll have for your work
 - SANS GIAC thinks so highly of InfraGard that they give Members a 30% discount on all their certifications (and these have been the most valuable and cost-effective training she's seen)
 - As a university security officer, she constantly runs into DoS (e.g., attack on White House gateway), vandalism, theft of intellectual property
 - University also contributes to InfraGard because of the knowledgeable students
- 4.2.3 Legal issues
- CIO looked at the agreement and asked her opinion
 - Saw nothing that would force disclosure of confidential information
 - RPI Legal asked a few questions
 - Took only (!) a month to work through the process
 - RPI even hosted the first meeting.
- 4.3 The Burlington FBI office perspective (Tom Leene) < tleene@leo.gov >
- He is our liaison for setting this program
 - Convinced that InfraGard will help the members as well as law enforcement
 - Fundamental focus is infrastructure protection; each sector in the group might fruitfully share specific information
 - We are just the beginning group — should be able to engage others in the state as we progress

5 Next steps for Vermont (Gary Kessler)

- 5.1 We're set to go
- We have the mailing list...
 - We have a Web site...
 - We can change the domain name!!
 - We have the interest...
 - We have the need...
- 5.2 Steering Committee
- Gary Kessler
 - Mich Kabay (recording secretary)
 - Bill Kuhns
 - Tom Aldrich
 - Joshua Silman
 - Bill Holden
 - Randy Hannett
 - Peter Hartshorn
 - Bill Scherr
- 5.3 People should sign the membership agreement to get us started
- Tom Leene will hold the list

- As far as we know, the Member has to be an employee of a formal entity (including a sole proprietorship)
 - Students cannot be members
- 5.4 Do we need a charter and registration?
- No, we're not handling money
 - Don't have to register with Secretary of State
 - Albany doesn't have a charter — keeping it simple
 - Albany had an organizational meeting to vote on a Board of Directors which started off as the Steering Committee.
 - Organizing group will nonetheless devise simple statement of purpose and ground-rules for participants (e.g., respecting confidentiality, avoiding rampant pre-sales. . . .)
- 5.5 What about criminal hackers?
- Should discuss our stance if known criminal hackers demand to attend the meetings
 - One approach is to allow them in and work on their moral development: “It is better to have them on the inside pissing out than on the outside pissing in.”
 - Another approach is to define access rules for participation
- 5.6 Meetings
- Start with quarterly meetings
 - Anyone can come to the meetings — don't put barriers up
 - Champlain College ready to volunteer facilities during summer term
 - Usually have speakers at meetings
 - Can talk about specific problems or can review new threats and vulnerabilities or any topic that is valuable to us
 - Meetings can start with an open session and then have a part restricted to Members only
 - Always set the dates for next meeting and for Board meeting.
- 5.7 Confidentiality
- Non-members may not have signed confidentiality agreements
 - Suggestion: don't give out anything that you want to be confidential
 - Or send anonymized info to list moderator (Gary) to post on the list
- 5.8 Check on registering VT-INFAGARD.ORG in the DNS