Internet2 Member Meeting Security BoF

Internet2 Spring Member Meeting, Arlington VA
7:30-8:30 April 25th, 2012, Salon K

Joe St Sauver, Ph.D. (joe@uoregon.edu , joe@internet2.edu)
Internet2 Nationwide Security Programs Manager and
InCommon SSL/PKI Certificate Programs Manager

http://pages.uoregon.edu/joe/i2mm-secbof-2012/

New Two Factor Auth Offerings From Net+/InCommon

Duo Security

- http://www.incommon.org/duo/index.html
- Signed literally just this past Friday, anticipate readiness to have subscribers mid-May
- Offers a variety of approaches including Duo Push (Smart phone: y/n) and Duo Mobile (soft OTP), also supports telephony and SMS based auth, and hard tokens
- Site License model priced according to school size (hospital coverage separate, based on bed count); price list available soon.

SafeNet PKI Hard Tokens

- http://www.incommon.org/safenet/index.html
- Also just signed
- Products offered include both selected SafeNet smart cards and selected USB-format hard tokens for storing client certificates.
- Deep discounts, flat rate pricing, 200 unit minimum order.

Some Technical/Policy Topics We Might Want to Discuss

Flashback/Flashfake Trojan

- "Flashback Trojan Hits 600,000 Macs and Counting," http://apple.slashdot.org/story/12/04/05/139243/flashback-trojan-hits-600000-macs-and-counting (April 5th, 2012)
- More Mac malware will likely be on the way
- What should you/your users do?
- Make sure your Mac's software is fully up to date, and consider using a Mac anti-virus product
- Disable Java if you're on 10.5.8 or earlier (but you really should be on a currently supported version of Mac OS X); see http://support.apple.com/kb/HT5244
- Some terrific Flashback/Flashfake analyses/resources at the Kaspersky web site, http://www.securelist.com/

Windows XP End-of-Extended Support

- Many Internet2 schools still have *extensive* deployments of Windows XP, even though Windows XP went end-of-mainstream support April 14th, 2009.

- **Windows XP is going <u>end-of-*extended* support</u> April 8th, 2014** (see http://windows.microsoft.com/en-us/windows/products/lifecycle)

- What are your plans for getting your remaining Windows XP users and getting them to something current, like Windows 7?

DNS Changer

- If you've been getting DNS Changer warnings from the REN-ISAC about hosts on your campus (or seeing recursive DNS traffic going to odd servers), please deal with those potentially compromised hosts before 9 July.

- On 9 July, the replacement servers established by law enforcement will go away, and any users that are continuing to try to use those servers won't be able to visit most web sites. See for example:
  "DNS Changer: FBI Updates Net Access Shutoff Plans -- The FBI called: Your malware-infected PC or router needs to get clean, or lose Internet access."
  http://www.informationweek.com/news/security/government/232900868

OpenFlow/Software Defined Networks

- We've been hearing an awful lot about ***OpenFlow/ Software Defined Networks*** during this week's sessions but I'm **not** hearing a lot about **OpenFlow/SDN security** (yet). This is an area that needs consideration by the community.

- One report: "Startup Tackles OpenFlow Security," http://www.lightreading.com/document.asp?doc_id=219752

Security Implications of 100Gbps

- We run the risk of "driving beyond our headlights" or "driving blind" if we don't **effectively instrument our networks at 100Gbps.** We need a community-wide commitment to making 100Gbps network instrumentation a priority.

- Some boxes are beginning to become available:
  -- **Procera PL20000**
  www.proceranetworks.com/plr-packetlogic-real-time-enforcement/pl20000.html
  -- **EndaceExtreme**
  www.endace.com/endaceextreme.html

CISPA

- "Cyber Intelligence Sharing and Protection Act" (http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523:)
- About sharing cyber security data from the Federal government to the private sector, and vice versa (on a voluntary basis)
- Coming up for a vote on this Friday
- There have been a variety of concerns about the bill, and an attempt to analogize it to SOPA/PIPA, but see "CISPA Isn't 'Son of SOPA'," Kaminsky & Baker, 4/24/2012, http://www.politico.com/news/stories/0412/75546.html

Are Internet Connected TVs and BluRay Players The Next Hacker/Cracker Target?

- Increasingly popular to have an Internet-connected smart TV or BluRay player
- iPad/iPhone remotes available for selected Samsung products (sure beats the limited keypad on the remote), but now see http://aluigi.org/adv/samsux_1-adv.txt
- Other interesting technology, e.g., Flingo for Vizio TVs to fling video from a website to a TV ("Flingo enables a website to discover a device in the user's network and bidirectionally communicate arbitrary messages with that device.", see http://flingo.org)
- My spidey sense is tingling.
- Are you guys/gals paying attention to this one?

FCC CSRIC WG7
Anti-Botnet Code of Conduct

(What The Heck Is A CSRIC?)

FCC CSRIC

- "The Communications Security, Reliability and Interoperability Council's (CSRIC) mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety." (http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii)
- CSRICs run for two year terms. We're currently on CSRIC III, chartered to run from 3/19/2011-3/18/2013.
- CSRIC work gets done via working groups focused on particular topics. For example, WG5 is focused on DNSSEC Implementation Practices for ISPs, WG6 is focused on Secure BGP Deployment, and WG7 is focused on Botnet Remediation. I participate on WG7.

WG7 – Botnet Remediation

- "**Description:** This Working Group will review the efforts undertaken within the international community, such as the Australian Internet Industry Code of Practice, and among domestic stakeholder groups, such as IETF and the Messaging Anti-Abuse Working Group, for applicability to U.S. ISPs. Building on the work of CSRIC II Working Group 8 ISP Network Protection Practices, the Botnet Remediation Working Group shall propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to op-into the framework proposed by the Working Group. *[this part's done]*

- "The Working Group will also identify potential ISP implementation obstacles to the newly drafted Botnet Remediation business practices and identify steps the FCC can take that may help overcome these obstacles. *[in progress]*

- "Finally, the Working Group shall identify performance metrics to evaluate the effectiveness of the ISP Botnet Remediation Business Practices at curbing the spread of botnet infections." *[in progress]*

http://www.fcc.gov/pshs/advisory/csric3/wg-descriptions_2-28-12.pdf

WG7 Participants

- WG7 is chaired by Mike O'Reirdan of the Messaging Anti-Abuse Working Group; Vice Chair is Pete Fonash of DHS.
- Representatives of many major US ISPs participated including AT&T, CenturyLink, Comcast, Cox, Microsoft, Sprint, T-Mobile, Time Warner, Verizon and USTelecom.
- Federal participation includes folks from DHS, FCC & NIST.
- Other participants include Bell Labs, BOA, CAUCE (Coalition Against Unsolicited Commercial Email), Damballa, EMC, IID (Internet Identity), Intersections, ISC (Internet Systems Consortium), OTA (Online Trust Alliance), PayPal, SANS Institute, SourceFire, Stop Badware, and Verisign.
- Higher ed (HE) participation? Me (Internet2 and UO), plus Gabe Iovinio of the REN-ISAC (Research & Education Network Information Sharing and Analysis Center, at IU). (Why HE? Many universities run large ISP-like networks)

Significant Sites Have Been Successfully DDoS'd By Just A Few *Thousand* Users, But *Millions* of Bots Exist In The Wild

- Immediately following the takedown of Megaupload, less than 6,000 people reportedly used a DDoS tool known as "LOIC" to DDoS the Dept of Justice and other sites.*
- There were ~81.6 million US households with broadband connectivity as of 10/2010.** It is estimated that roughly 1-in-5 such households has one or more botted hosts.***
- Given that less than 6,000 bots were enough to take down the DOJ, a population of (.2*81.6 million)=**16 million+** bots, in the US **ALONE**, bots obviously represent a huge problem

* http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm

** http://www.census.gov/compendia/statab/cats/information_communications/internet_publishing_and_broadcasting_and_internet_usage.html (table 1155)

*** http://blog.damballa.com/?p=1549

SOMEONE Must Be Responsible For Cleanup?

- But who?
- ***The end user?*** If a botmaster is careful, users whose systems are being exploited may never directly notice that their systems have been botted and are being abused, and if they don't notice, users may often wonder why should they care (with the exception of things like the Banker Trojans previously mentioned)
- ***What about the manufacturer of the operating system?*** Well, they certainly also have a potential role, and some already do try quite hard to help. For example, Microsoft removes an awful lot of bots via their Malicious Software Removal Tool (you run MSRT in every time you do your monthly updates). Unfortunately, some users don't update their computers very often, if at all.

- What about ***the government?*** Beyond law enforcement, surely there must be *some* government agency that could provide cyber assistance to individuals with botted hosts, much as the Centers for Disease Control, or Federal Emergency Management Agency helps with pandemics or national disasters, isn't there? No. No agency or bureau is clamoring to take on the thankless task of cleaning up the world's botted consumer hosts.
- ***So, we're left with ISPs.*** ISPs end up "holding the bag" for bot cleanup for multiple reasons, including:
  -- ISPs are the only ones who can map unwanted network traffic to customer "meat space" identities
  -- If ISPs don't take care of their compromised customers it's the ISP's address space that will get blackholed
  -- ***ISPs are also potentially subject to government regulation. ISPs try hard to avoid <u>that.</u>***

Some ISPs Have <u>Already</u> Begun To Tackle Bots

- Comcast, the largest broadband provider in the US, and an entity that's been very active in helping to lead MAAWG, went from being one of the (self-admitted) most botnet-infested ISPs in the world to having only a miniscule level of infection today. They're a <u>real</u> success story!
- Comcast even went so far as to *document* how they achieved that miraculous turn around, see Livingood and O'Reirdan, "Recommendations for the Remediation of Bots in ISP Networks," 3/2012, http://tools.ietf.org/html/rfc6561
- "For his sins", Mike O'Rierdan, one of the co-authors of RFC6561 and the head of MAAWG, was asked by the FCC to lead CSRIC WG7, the anti-botnet working group.
- The Working Group has been doing a tremendous job, and working group deliverables are already beginning to appear.

The First Deliverable from FCC CSRIC WG7

- "Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), A Voluntary Code," March 2012, 26 pages, available to download via a link http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii
- Let me emphasize: this is a **VOLUNTARY** code of conduct
- It does **NOT** attempt to dictate technical approaches
- Participants need to take meaningful anti-bot action in five areas:
  1) Education
  2) Detection
  3) Notification
  4) Remediation
  5) Collaboration

- **Education** - an activity intended to help increase end-user education and awareness of botnet issues and how to help prevent bot infections;
- **Detection** - an activity intended to identify botnet activity in the ISP's network, obtain information on botnet activity in the ISP's network, or enable end-users to self-determine potential bot infections on their end-user devices;
- **Notification** - an activity intended to notify customers of suspected bot infections or enable customers to determine if they may be infected by a bot;
- **Remediation** - an activity intended to provide information to end-users about how they can remediate bot infections, or to assist end-users in remediating bot infections.
- **Collaboration** - an activity to share with other ISPs feedback and experience learned from the participating ISP's Code activities.

A Few (of Many Possible Ways) That An ISP Might Approach Those Activities

- **Education:** create a web site describing bots, why they're a problem, and what users can do to avoid getting botted; include a bot awareness brochure in customer mailings
- **Detection:** accept abuse reports from credible third party reporters who've identified botted customers; monitor network traffic (and/or recursive DNS traffic) for signs of contact with known botnet command and control hosts
- **Notification:** do in-browser notifications of infections to customers; send customers notifications by email or snail mail
- **Remediation:** refer customers to a third party service provider for cleanup; provide anti-virus software that can be used by customers who want to try self-cleanup
- **Collaboration:** share experiences and lessons learned via industry fora such as MAAWG, APWG, RSA, NANOG, etc.

The ABCs for ISPs and YOU

- Your school should consider adopting the Anti-Botnet Code of Conduct – in most cases, you're *already* doing all this stuff, so why not get recognized for those efforts?

- Consider this an opportunity to show the world that higher ed *does* "get it" and *is* a "good neighbor" when it comes to dealing with botted hosts.