Botnets, the FCC CSRIC Botnet Working Group, and Opportunities for Internet2 Industry Partners and Researchers

Internet2 Spring Member Meeting, Arlington VA
Combined Industry and Research Constituency Meeting
8:30-10:15AM April 24th, 2012, Salon B

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-csric-wg7/

Introduction

- I'd like to begin by thanking Bob Brammer for the opportunity to visit with you this morning.
- We have multiple presenters, so I'll just take fifteen minutes to brief you about one security activity I've been involved with over the last year or so, and that's the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) III's Working Group 7, and its anti-botnet efforts.
- I hope that by the time we're done, you'll agree that this topic fits the industry-plus-researcher constituency of this morning's session quite well.
- FWIW, I know that if you're like many folks, you may never have heard much about bots or the FCC CSRIC activity, so let's begin with a little background info.

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)

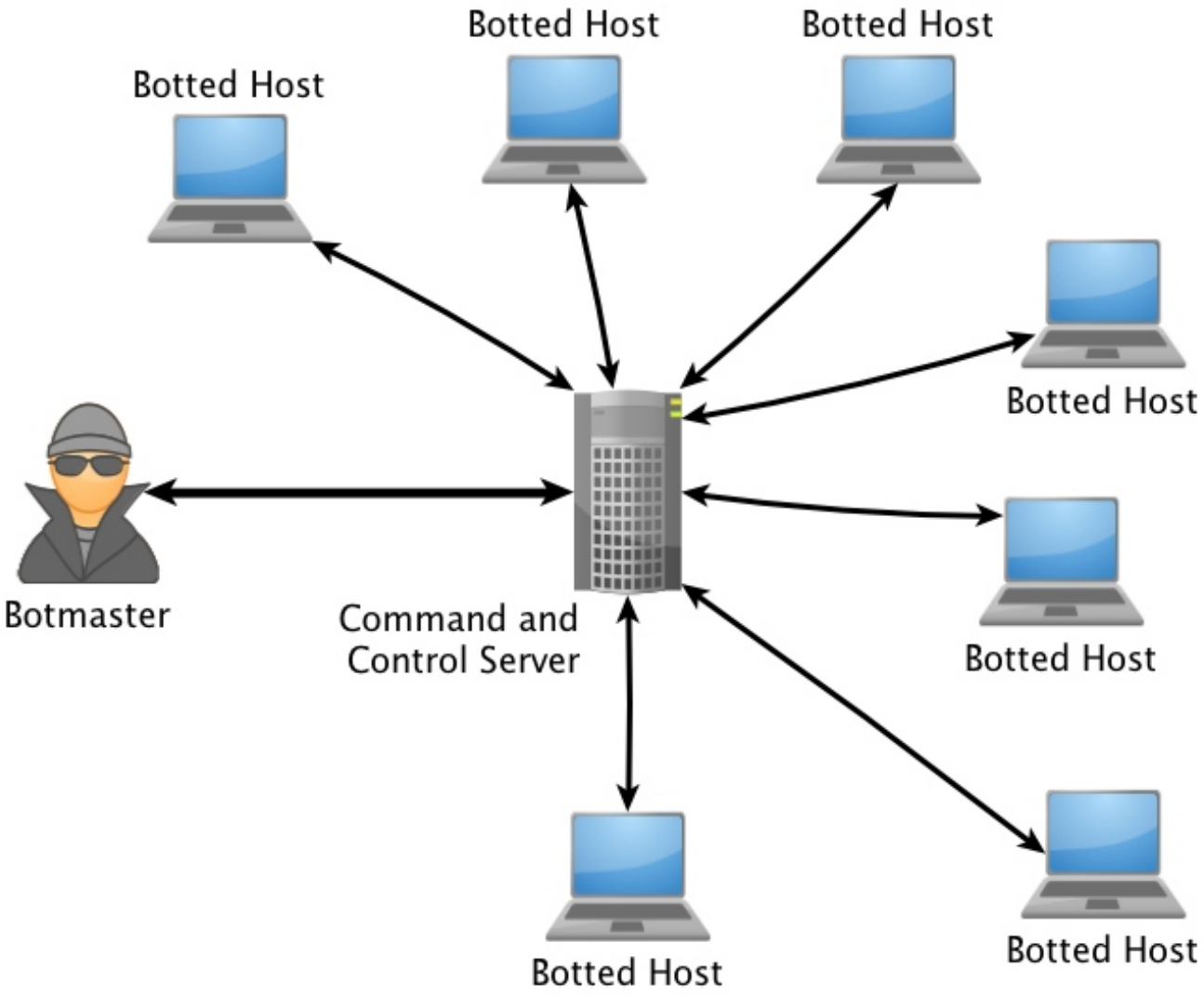
Disclaimers

- Although I work for Internet2 under contract through the University of Oregon, my affiliations are mentioned in the WG7 context purely for identification purposes.
- I'm also involved with a number of other organizations participating in the WG7 effort, including participating with MAAWG as a senior technical advisor, with OTA as a strategic advisor, with the REN-ISAC as a member (and as a member of the REN-ISAC TAG), and with CAUCE as a member of the CAUCE board of directors. Again, I mention those affiliations here in the spirit of full disclosure, but I'm not representing any of those groups.
- Finally, although I'm part of WG7, today's remarks also do not necessarily represent the positions of the FCC, CSRIC, or WG7. Put simply: "any opinions expressed are my own."

Since This *Isn't* A Security-Focused Audience, "What's A Bot?" [from the WG7 Report]

- A malicious (or potentially malicious) "bot" [...] refers to a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator (often referred to as a "bot master" or "bot herder.")
- Computer systems and other end-user devices that have been "botted" are also often known as "zombies".
- Malicious bots are normally installed surreptitiously, without the user's consent, or without the user's full understanding of what the user's system might do once the bot has been installed.
- Bots are often used to send unwanted electronic email ("spam"), to reconnoiter or attack other systems, to eavesdrop upon network traffic, or to host illegal content such as pirated software, child exploitation materials, etc.
- Many jurisdictions consider the involuntary infection of end-user hosts to be an example of an unlawful computer intrusion.

A Small "Traditional" Botnet



Some Of The Special Properties of Bots

- Bots allow a botmaster to hijack and use *your* gear (for free!) instead of having to buy systems and network connectivity on their own dime.
- Bots generally anonymize traffic passed through them (the traffic appears as if it is coming from the botted host itself, not from the botmaster). This helps the botmaster avoid prosecution, hindering backtracking and attribution.
- Botnets can be very resilient and tricky to take down.
- Bots are very versatile – they're like potato: they can be seasoned/adapted to meet changing needs. (Send spam today, do DDoS tomorrow & click fraud work next week)
- Bots can act as "amplifiers" – a small amount of initial traffic can be replicated & resent from thousands of bots, collectively representing a huge amount of total capacity.

A Concrete Example of Why Bots Are Bad That Any User Should Be Able To Relate To

- Some bots (so-called "Banker Trojans) are deployed for the purpose of stealing banking/brokerage credentials. The banker trojan lurks in the background, waiting patiently for the user of the system to login to his or her bank or brokerage. When the user does so, the trojan then grabs the username and password and sends it off to the cyber criminal for them to use. (This sort of crimeware-based attack is becoming more popular with cyber criminals as traditional phishing has come to work less well over time)
- Once the botmaster has your bank or brokerage credentials, they can then steal assets from your online accounts simply by logging in using your password.
- Even if you eventually get "made whole" by your bank or brokerage, this sort of theft is hugely disruptive, time consuming, and a big pain.

Law Enforcement IS Tackling These (Coreflood)

Department of Justice Takes Action to Disable International Botnet

More Than Two Million Computers Infected with Keylogging Software as Part of Massive Fraud Scheme

---

U.S. Department of Justice
April 13, 2011

Office of Public Affairs
(202) 514-2007/TDD (202) 514-1888

WASHINGTON—Today, the Department of Justice and FBI announced the filing of a civil complaint, the execution of criminal seizure warrants, and the issuance of a temporary restraining order as part of the most complete and comprehensive enforcement action ever taken by U.S authorities to disable an international botnet.

Related Court Documents
Order to Show Cause
Complaint
Seizure Warrant

Another LE Example… DNSChanger

Update on March 12, 2012: To assist victims affected by the DNSChanger malicious software, the FBI obtained a court order authorizing the Internet Systems Consortium (ISC) to deploy and maintain temporary clean DNS servers. This solution is temporary, providing additional time for victims to clean affected computers and restore their normal DNS settings. The clean DNS servers will be turned off on July 9, 2012, and computers still impacted by DNSChanger may lose Internet connectivity at that time.

Operation Ghost Click

International Cyber Ring That Infected Millions of Computers Dismantled

11/09/11

Six Estonian nationals have been arrested and charged with running a sophisticated Internet fraud ring that infected millions of computers worldwide with a virus and enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry. Users of infected machines were unaware that their computers had been compromised—or that the malicious software rendered their machines vulnerable to a host of other viruses.

Details of the two-year FBI investigation called Operation Ghost Click were announced today in New York when a federal indictment was unsealed. Officials also described their efforts to make sure infected users' Internet access would not be disrupted as a result of the operation.

The indictment, said Janice Fedarcyk, assistant director in

FBI Statement:

But, There's A Limit to What LE Can Do

- While bots can be used for many different undesirable activities (including things such as sending spam or stealing credentials), the most serious bot-related problem may be their use for DDoS (distributed denial of service) attacks, particularly against critical infrastructure.
- When a site is DDoS'd, it may be flooded with so much bogus traffic that there's no residual capacity left to service legitimate users of that site.
- Depending on where the "weak link in the chain" may be, a DDoS may involve saturating a site's network connections, overwhelming the servers used by the site, or something else (and if you fix a issue, you may just shift the bottleneck from one choke point to another one).
- For background, Arbor Networks offers a nice annual DDoS report, see http://ddos.arbornetworks.com/report/

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

And Bots Are *Not* Just A MS Windows Issue. Macs, Mobile Devices, etc., Can Also Be Botted

- "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)
- "Millions Caught Up In Android Botnet," http://www.zdnet.com/blog/hardware/millions-caught-up-in-android-botnet/17891 (January 28th, 2012)
- *Everyone*, on *every* platform, needs to be made aware of the botnet problem and *everyone* needs to harden their systems and networks.
- And all the currently botted hosts need to get cleaned and hardened.
- But who's going to take that on?

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 Already 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 real 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.

Bots and You, As Internet2 Industry Members

- **If you're a service provider, encourage your company to voluntarily embrace the Anti-Botnet Code of Conduct!**
- **If you offer security products or services**:
  -- Learn about the anti-botnet code and help spread the word to customers who may not have heard about it yet
  -- Does your company offer products or services that might help meet the needs of providers working to deploy the anti-botnet code? If not, *should* you think about it? (Remember, we're talking about MILLIONS of botted users...) For example, maybe you have botnet detection products you've been working on, or maybe you offer a cleanup and hardening service that might be able to help?
  -- Share info about any botted hosts you may discover!
  -- Think globally! Many of the botted hosts that are attacking us are located abroad. So what's your strategy for engaging with customers in, say, India?

What About Researchers and Internet2?

- Researchers also have a critical role to play in the war on bots. While bots are critically important, they often don't receive nearly the research attention they deserve.

- For example, consider the seemingly simple question of "How many systems are currently botted?" In truth, we don't know with any reasonable degree of precision, even though we should.

- If we can't measure the botnet problem repeatedly and consistently over time, it will be hard for us to tell if the anti-botnet code is succeeding or a dismal failure.

- Many of the most interesting aspects may be overseas...

CBL-Listed Hosts by Country

- http://cbl.abuseat.org lists botted hosts that have been observed spamming. It breaks those listings down in various ways, including country by country. The US is *not* the most botted country in the world, believe it or not.

Country	Count	%	Cum %	Rank	% Infected
Total	8,055,665				
IN	1,566,453	19.45	19.45	1	3.739%
VN	633,385	7.86	27.31	2	3.302%
RU	544,291	6.76	34.06	3	0.934%
BR	543,552	6.75	40.81	4	0.781%
PK	527,122	6.54	47.36	5	7.151%
CN	317,133	3.94	51.29	6	0.064%
IR	247,860	3.08	54.37	7	2.006%
TH	182,178	2.26	56.63	8	1.185%
KZ	167,523	2.08	58.71	9	3.309%
BY	159,801	1.98	60.69	10	5.645%
[…]					
US	*70,215*	*0.87*	*84.98*	*28*	*0.004%*

Some Measurement Complications

- We often identify bots by their output (such as spam emitted directly from botted hosts). But now, imagine that many ISPs are blocking direct-to-MX spam. Unfortunately, even if bots can't spam, that doesn't mean that they've been totally defanged. Those bots *could* still be used for other evil purposes.
- NAT can also make it hard to get accurate counts. If we see unwanted traffic from an IP, is that from *one* botted system behind a home gateway/firewall, or are there *several* botted systems there? It's easy to undercount...
- DHCP can also be problematic. One infected host may show up on half a dozen different IPs over several days as one user ends up using multiple different IPs.
- And what if a system's botted by multiple bots at once? How should that be counted?
- And of course, UDP and ICMP traffic can be spoofed...

Not All Bots Are Simple, Either

- While I showed a diagram of a conceptually very simple bot earlier in this talk, many bots aren't simple at all. Consider, for example:
  -- hierarchical/multi-tier bots with extensive redundancy
  -- use of peer-to-peer architectures for botnet C&C
  -- use of domain name generation in an effort to hinder botnet monitoring and frustrate C&C take downs
  -- botnets with active defenses (trying to inject into a bot but get detected? you may get DDoS'd), or botnets which employ evasion and deception as survival strategies (don't assume that you'll get the same response that someone else might receive)
  -- bots working in emerging environments (such as IPv6)
- Truly, bots can be a fascinating area for potential research, and deserve more research attention.

Security Areas Other Than Bots

Only 15 Minutes...

- Given that we only had 15 minutes, we didn't really have time to cover all the other potentially interesting security areas that industrial members or researchers might like to be thinking about, but I'll mention two more in closing:

  -- ***OpenFlow/Software Defined Networks:*** During this week's sessions you'll be hearing a LOT about OpenFlow/ SDN, but I'm **not** hearing a lot about **OpenFlow/SDN security** (yet). This is an area that needs work.
  -- ***Security Implications of 100 Gbps:*** We run the risk of "driving beyond our headlights" or "driving blind" if we don't **effectively instrument our networks at 100Gbps.** Some 100Gbps products are begining to appear (such as the EndaceExtreme), but we need a community-wide commitment to making 100Gbps instrumentation a priority.

Thanks for The Chance To Talk Today!

- Are there any questions?