Bots, Malware, and What We Need From Uncle Sam

Joe St Sauver, Ph.D. (joe@uoregon.edu)
Senior Technical Advisor
Messaging Anti-Abuse Working Group

MAAWG 14th General Meeting, Ft Lauderdale, Florida
September 22nd-24th, 2008
http://www.uoregon.edu/~joe/unclesam/

Deja Vu: APWG E-Crime Summit, SFO, May '07

- A year ago May, the Anti-Phishing Working Group (APWG) had an E-Crime Summit in San Francisco, and some of my APWG colleagues invited me to participate in a panel on botnets. As part of that meeting I presented a brief talk entitled, "We Need a Cyber CDC or Cyber World Health Organization,"
- I'm a pretty shy guy and try to avoid speaking at events that get media coverage, but I failed to notice Ryan Singel from *Wired* at the APWG Summit. The result? *Wired* published an article, "Desperate Botnet Battlers Call for an Internet Driver's License," www.wired.com/politics/security/news/2007/06/bot_strategy (complete with a picture of me). Let me state for the record that while my picture was featured with that article, ***I*** was NOT advocating for net driver's licenses, one of my co-panelists was.
- I mention that meeting/talk here because much of what I'll share with you here today was originally presented at that earlier event.

There Are Currently Millions of Compromised Consumer PCs

- See, for example, the roughly five million hosts listed on the CBL DNS blocklist (as used by the Spamhaus XBL), all listed for having sent spam
- While spam is unquestionably annoying (and an insidious drain on business productivity and email usability), those same compromised systems could just as easily be used for a host of other far more nefarious purposes including:
  -- hosting phishing sites, malware, pirated software or child porn
  -- scanning the network to find other vulnerable hosts
  -- sniffing traffic on the wire to compromise passwords
  -- DDoS'ing online businesses or even
  -- attacking US government sites or critical online infrastructure.
- Bottom line, those compromised hosts are a significant threat to the Internet as a whole, and to the U.S. in particular.

So Who Will Clean Those Systems Up?

- **Why not the system owner?**
- They bought that system, so they should also be responsible for its upkeep, shouldn't they? Yes, well, but…
  … even when infested, the system will usually still **sort of** work, and even if it is bothering other folks on the Internet, it may **not** be bothering the system owner, so as a result the system owner may not really **care** if their system is infested
  … the user may not have the technical **expertise**, the **software** tools, or the **time** they'd need to clean their system up
  … the user may not be able to **afford** to hire someone to do it for him or her (it may be cheaper to simply buy a new system!)
- Bottom line, even if the system owner is responsible for cleaning up their system, they may not accept that responsibility.
- Is there someone **else** who might also be responsible?

If Not the System Owner, What About Their Internet Service Provider (ISP)?

- If an infested consumer host wasn't connected to the Internet, no one would even care that that that host was infested (without network connectivity, no one else could be attacked by that compromised system). Once an ISP sells Internet connectivity to that person, however, suddenly the picture changes. **With** network connectivity, an infested customer's system can impact other users all around the world.
- In earlier days, sites connecting to the Internet recognized that they were part of a very special community, and accepted that being part of that community meant that they had a responsibility to their fellow users to keep the community healthy. Sites worked hard to deal with any hacked or abusive systems they might connect -- it was simply something which everyone expected and accepted as part and parcel of being a good online neighbor.

The ISP as Common Carrier (Not!)

- About the time the regional telephone companies began selling access to the Internet, that tradition made a sharp turn.
- Unlike the old Internet tradition of doing what was best for the Internet regardless of whether or not there was any formal regulation requiring that action, when the regional telephone companies entered the Internet market they brought along a highly regulated **"common carrier"** mentality -- from their perspective they just sold pipes, and as long as there was no law requiring them to act, they were "powerless" to limit or control how the connections they sold were ultimately used.
- Of course, the claim that ISPs are common carriers fails several key tests that any true common carrier can readily pass (for example, real common carriers tend to be heavily regulated), but the common carrier myth provides a nice excuse for not having to work at cleaning up compromised customer systems.

The Real Reasons ISPs Don't Want To Be Responsible for Cleaning Up Customers

- **What are some real reasons why ISPs don't want to be responsible for cleaning up compromised customer systems?**
- **Cost:** one protracted online customer service call (or one offsite truck roll) made in an effort to help an infested customer get cleaned up can destroy the profitability of that customer for years to come -- maybe forever! ISPs can increase their rates for all customers to cover those additional costs, but if some ISPs do so while others don't, the ones who do so will be at a serious competitive disadvantage relative to those who don't do so.
- **Liability:** after the ISP tries to help the customer get cleaned up, any and all system problems from that point forward may end up getting blamed on the ISP's clean up efforts (and there's always the very real possibility that a technician may end up killing a badly infected system while trying to get it cleaned up).

More Reasons Why ISPs Don't Want To Have to Clean Up Customer Systems

- **The Reinfection Problem:** Another reason why ISPs don't want to have to clean up customer systems is the problem of repeat infections. That is, having cleaned up a customer's system once, how do you keep that customer from quickly becoming reinfected? If you fail to **harden the system** and **train the user to avoid unsafe online behaviors** the ISP will quickly end up recleaning the same system, over, and over, and over, again.
- **Customers with Systems of Dubious Provenance:** While I know that all of you are scrupulous when it comes to only running properly licensed software, some infested users may have systems running pirated software. Most computer professionals refuse to work to help clean up systems running pirated software, and vendors may not make patches available for installation on pirated copies of their products.

Speaking of Software Vendors…

- One could argue that if an operating system or application was properly designed and coded, it would not be broadly vulnerable to infection, and thus the ultimate responsibility for any infestation lies with the maker of the apparently defective operating system (or the maker of a defective application)…
- But, vendors usually license their products "as-is" with extensive disclaimers, thereby doing their legal best to completely eliminate any and all liability they might have had if they'd sold a defective product.
- Moreover, a single system may contain software from dozens (if not hundreds!) of different vendors; how would you know which one of all those was responsible for a system compromise? Is it the application software's fault? The operating system software's fault? Everyone's fault? No one's fault? Who knows?

What About the Bad Guys (or Gals)?

- The system owner, the ISP and the software vendors all share one thing in common: they come forward with (basically) clean hands.
- The bad guys (or bad gals) on the other hand, do not. They either intentionally compromised the end user's system, or they obtained use of the compromised system from someone who did. The bad guys (or gals) are the one who are, or should be, financially responsible for the creation and/or exploitation of those compromised system. If the world was fair, they're the ones who'd bear financial responsibility for cleaning those systems up.
- But, as we all know, the world's not necessarily fair. The person who compromised a given system may ultimately be unknowable, be legally inaccessible (overseas, or a minor), or have no legally attachable financial assets, and the result may be that the bad guy or gal never ends up paying a cent for all the damage they caused.

And Thus We Come to The Government…

- **It <u>shouldn't</u> be the government's responsibility to deal with millions of compromised customer hosts, but <u>if they don't, no one may end up doing so</u>.**
- As someone who is politically and financially conservative, I don't believe in casually establishing new governmental responsibilities -- I believe that generally the best government is the least government. Sometimes, however, there are situations where ONLY the government can address a problem. For example, when it comes to national defense, no one would question that maintenance of our military forces is a task properly done by Washington. Similarly, when it comes to responding to natural disasters such as Hurricane Ike, or responding to an epidemic, those responsibilities lay squarely with the federal government.
- So why do those governmental responsibilities stop at cyberspace?

Time For a National Cyberspace Doctrine

- Just as the government has a responsibility to defend its citizens from conventional military threats or from terrorism, and to respond in case of natural disasters or widespread disease, so, too, the time has come for us to recognize that **the government has a compelling national interest in the protection of its citizens and businesses online, and in the protection of their networks and systems. An attack on US networks and systems, whether blatant or insidious, is an attack on the United States as a whole, and properly deserves national attention and response.** This is not a trivial proposition, and not one that I advance lightly.
- The best way to understand the need a national cyberspace doctrine is to look at the impact on the US if we were to be denied the ability to peacefully exist/work in cyberspace -- what would the impact of that be to our economy & our influence worldwide? **I believe the impact would be huge, and wholey intolerable.**

Cyber Public Health Differs From Fighting Cyber Crime

- Part of fighting the online threats we face is pursuing cyber criminals, and law enforcement is vigorously doing so, albeit with woefully insufficient resources. I appreciate every cyber prosecution which occurs, and every cyber conviction obtained, and I recognize just how much hard work is involved. **Thank you!**
- But fighting cyber crime does nothing to address our vulnerable infrastructure. Fighting cyber crime does nothing to make online victims of cyber infestation whole and sound again. We're awash with vulnerable and compromised systems, and our government has no systematic plan for helping to **clean up that mess**.
- We need to **continue** to fight cyber crime, but we must **ALSO** begin to practice cyber "public health." **Since no one else will accept responsibility for cleaning up and securing infested systems, the time has come for the government to do so.**

Two Public Health Functions

- We can identify two potential public health functions, both of which are currently missing:
  (1) Dealing with mass scale acute emergencies: this function is analogous to providing emergency assistance following a major natural disaster. For example, in the physical world this might mean passing out MREs and bottled water or providing temporary housing for victims of a major hurricane.
  (2) Correcting chronic health problems: this function, equally as important as dealing with acute emergencies, is similar to public health workers striving to eliminate contaminated water sources, or to eliminate malnutrition, or to get lead paint off the walls, or to vaccinate children against polio or measles.
- We need **BOTH** types of public health functions **online**, too. We need government help to deal with acute cyber emergencies, and we need help dealing with chronic cyber health problems, too.

Root Cause Analysis

- Like a traditional public health agency, the new cyber public health office I envision should also devote energy toward root cause analysis, reporting **in aggregate only** (thereby preserving the privacy of individual clients they may be helping) on how users are getting infested and who's exploiting those infestations.
- That targeted field research will allow the cyber public health agency to better understand and control the infestations they see, while also allowing partner agencies to begin appropriate criminal or civil actions against the bad guys and gals who are ultimately responsible.
- The cyber public health agency should also have the ability to work with vendors and ISPs where appropriate, striving to correct systematic software vulnerabilities and to work to disinfect other infested customers, always striving to preserve victim privacy.

Who Should Deliver These Cyber Public Health Services?

- Cyber public health service can't come from existing law enforcement agencies -- they're already overcommitted and in many cases infested systems may have become infested through what I sometimes refer to as "low grade online illegal behavior."
- For example, we know that a common source of infection is downloading trojan'd software or tainted music files. I don't want a user with an infested system to be reluctant to ask for official help just because they've violated someone's copyright or because they're embarrassed at having become infected while visiting an online illegal gambling site. While no one is saying that it is okay to break the law, the overriding goal in this case is to get infected systems cleaned up, and that can **only** happen if users know that they can safely ask for help **without** risking action by law enforcement. Requests for cyber assistance **must** be privileged.

What Federal Agency Will Do All This?

- It would be convenient if we could just point to an existing federal agency and say, "Ah, this would be a perfect fit for the Department of Justice, or the Federal Trade Commission, or the Federal Communications Commission, or the Department of the Interior or <fill in the blank>" but unfortunately I don't see any agency that's both appropriately focused and eager to take on the massive challenges which will be associated with delivering cyber public health services to our nation. I am therefore left with no option but to suggest that we need a **new cabinet level federal agency** to deal with cyber public health.
- This agency should **NOT** be a **"Department of the Internet!"** Anything that all-encompassing will immediately run into a storm of knee-jerk opposition as everyone worries about what a Department of the Internet might do about network neutrality or whatever may be the Internet policy crisis of the day. We **just** want an agency which can help clean up our cyber mess.

Nationwide Delivery of Cyber Public Health Services

- Just like the delivery of traditional public health services, cyber public health will require the establishment of service providers in close contact with the communities they were created to serve.
- It won't do to just have an agency in Washington DC, or even just a handful of regional offices. Effective delivery of cyber public health is going to require cyber public health offices, and cyber public health officers, in every state and in every county across the country, so that it won't matter where you may be -- there will be a cyber public health office close to you where you can go for help with an infested system.
- Yes, there will also need to be a central agency inside Washington DC and regional offices to help deliver surge capacity when dealing with mass cyber emergencies, but for chronic cyber health problems, we need "boots on the ground" all across America.

Voluntary Participation at No Cost

- The cyber public health service I envision would be a **voluntary** one delivered at **no cost to those who elect to participate**.
- A cyber public health program cannot include federally coerced participation, because trying to force that sort of thing would quickly kill popular willingness to cooperate. Users should be free to take advantage of a federal cyber health program or not, as they may prefer, although I will admit that it is not inconceivable that at least some ISPs might insist that infested customers either visit with a private cyber specialist or see a federal cyber public health office as a condition of reconnection post-infection.
- I also wouldn't want an inability to pay to be a reason why someone might be turned away and not helped by a federal cyber public health system-- the cost of getting a system cleaned up is trivial in comparison to the amount of damage that even a low-end infested system can cause, and should be centrally funded.

International Efforts

- Because we have no cyber borders, and currently lack the public will to set up any sort of national perimeter, we also need to work **internationally** to improve cyber health. Infested systems in Zambia and infested systems in Albania can attack United States citizens' systems and networks just as easily as compromised systems here at home can. If we focus only on cleaning up infested American systems, we'll end up no better than we are now because there will still be millions of compromised and exploitable systems overseas. A global effort is needed, and America needs to exert international leadership when it comes to dealing with cyber health, or we'll just replace domestic attack traffic with foreign attack traffic, effectively gaining little or no ground. We recognize this in the real world, and that's why the UN has the World Health Organization for physical diseases, but **where's the UN's world <u>cyber</u> health organization?**

Two More Reasons Why the Federal Government Should Be Paying Attention

- Bots (and the spam they enable) cost the American economy a ***lot*** of money
- We're also starting to recognize that some of our historical enemies may be waging a clever and inexpensive sort of online "open source war" against us, simply by tolerating externally focused online criminals (such as spammers!)

The Cost of Spam Is Too Huge To Disregard

- We periodically see estimates of the cost of spam -- for example, Ferris Research has quoted the cost of spam to corporate customers at $140 billion worldwide, and $42 billion in the US.*
- That may seem like a laughably big number, but if you were to spread that over the entire population (checking the Census Bureau,** they say we're around 305,210,497 people in the US, and 6,724,925,242 worldwide), that's only:
  *140,000,000,000/6,724,925,242/365=**$0.057/person/day globally***
  *42,000,000,000/305,210,497/365=**$0.377/person/day in the US***
- I think that estimate is **way, way too low**. So why isn't anyone noticing billion dollar hits on our economy? Answer: that money's being taken from us in tiny little slices a billion times a day, so we simply don't perceive it. But what a whack against our economy!

---

* http://www.newswiretoday.com/news/32531/

** http://www.census.gov/main/www/popclock.html

For Comparison, Some Other Recent Costs

- "Hurricane Katrina cost insurers an inflation-adjusted $43 billion," http://money.cnn.com/2008/09/13/news/economy/ike_effect/
- "The attack on the World Trade Center will cost New York City $83 billion to $95 billion," http://query.nytimes.com/gst/fullpage.html?res=940DE3DF143EF936A3575AC0A9649C8B63
- "In February 2008, the Congressional Budget Office projected that additional war costs from FY2009 through FY2018 could range from $440 billion, if troop levels fell to 30,000 by 2010, to $1.0 trillion, if troop levels fell to 75,000 by about 2013. Under these scenarios, CBO projects that funding for Iraq, Afghanistan and the GWOT could reach from about $1.1 trillion to about $1.7 trillion for FY2001-FY2018."
  The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11, Updated July 14, 2008, CRS Report RL33110, page 2.

A Final Reason Why Congress Should Be Paying Attention to Bots and Spam

- Consider John Robb's 15 Aug 2008 posting "Open Source Warfare: Cyberwar," (http://globalguerrillas.typepad.com/globalguerrillas/2008/08/open-source-war.html):

In contrast to failed US efforts, both China and Russia have adopted the OSW [Open Source Warfare] approach to cyberwarfare. How did they do it? Simply:

** Engage, co-opt, and protect cybercriminals. Essentially, use this influence to deter domestic commercial attacks and encourage an external focus. This keeps the skills sharp and the powder dry.*

** Seed the movement. Once the decision to launch a cyberattack is made, start it off right. Purchase botnets covertly from criminal networks to launch attacks, feed 'patriotic' blogs to incite attacks and list targets, etc.*

** Get out of the way. Don't interfere. Don't prosecute participants. Take notes.*

Thanks For The Chance to Speak Today!

- Are there any questions?