Closing Panel:
End Users & Cybercrime

Joe St Sauver, Ph.D. (joe@uoregon.edu)
MAAWG Senior Technical Advisor

Grand Ballroom, 1530-1700 hrs, June 11th, 2009
Grand Hotel Krasnapolsky, Amsterdam

http://www.uoregon.edu/~joe/end-users/

Disclaimer: All opinions expressed
are solely those of the author.

Our Topic Today

"How do we force/encourage/cajole users into cleaning up their systems? What do our users expect from us?"

I'd like to start by sharing a few brief thoughts, or "propositions" if you will…

Proposition #1: "At Root, ISPs *Can* Simply Turn Off Infected Systems, But Customers Have Countervailing Powers of Their Own…"

- Assuming suitable terms of service (TOS) and acceptable use policy (AUP) terms, ISPs come to the table with a huge hammer:

  If you want to be connected via our network, your system cannot misbehave (spamming, scanning, packet flooding, hosting malware, etc.). If your system does do these things, we'll turn off your connection.

- On the other hand, customers are not completely without offsetting substantial powers of their own:

  If you treat me harshly or unfairly, I can and will take my business elsewhere.

- Or at least this is the unspoken underlying ultimatum.

Proposition #2: "If I Tell You That Your System Must Get Cleaned Up, I May Reasonably Be Expected To Help With That Sisyphean Task"

- Online tools and resources may sometimes be enough to help users get cleaned up, but what if more than that's required?
- In highly competitive markets with thin margins, it doesn't take long for intensive customer support costs to eliminate any profitability associated with perpetually-infested customer accounts.
- Are there some perpetually-infested and expensive-to-service customers a smart ISP simply doesn't want to have?

"In your case, we strongly recommend you try our competitors."

Proposition #3: "Even If Users Wanted to Clean Up Their Systems, They Often Can't."

- Most can't self-clean because they lack the requisite **tools and training** to remove all but the most trivial of malware themselves
- Nor **can they hire someone** to clean up their old clunker system, because that may end up costing nearly as much (or more!) than simply buying a new one.
- A new "name brand" desktop with a Core 2 Duo, 3GB, 500 GB disk and a 21.5 LCD=$439; a new "name brand" laptop with a Pentium Dual Core T3400, 3GB, 250 GB disk, 15.6" display, webcam, DVD burner and more=$449 (and let's assume pretty much any running old system can be sold for at least $100).
- Users **can't "nuke-and-pave"** because they have no backups, they can't find their original media for their installed software, they have little hope of recreating all their customizations, etc

Sidenote: So What Does Eventually Happen? Let's Spin The "Wheel of Possibilities"…

- The malware gets silently removed by Microsoft's Malicious Software Removal Tool when it gets downloaded and run each month
- The user's own antivirus software does finally catch up with the infection (once it has bedeviled a large enough number of users)
- Some other bit of malware consolidates its own position by removing "competing malware"
- The user just turns off the infected system
- The user replaces the infected system, potentially selling or "gifting" the still-infected system to some new owner (surprise!)
- **A computer-savy friend or relative get's invited over (but should your core line of business depend on an informal network of amateur clean up specialists having dinner?)**

Proposition #4: "Users May Not Want To Clean Up Their Still-Usable Systems Anyway…

- Historically, users wanted malware off their system because being infested made the system unstable, further-slowed already painfully slow network connections, and generally acted like an ill-behaved uninvited guest. Today, however:

  -- malware "quality control" is improving
  -- end user systems have faster processors (with dual or even quad cores!) plus gigs of memory and fast connections, and
  -- malware has learned to stay low profile.

  Thus malware infections may "fly under the radar" and be less of a concern to the end user. **If end users can't even tell that they have a "problem," how motivated will they be to "fix" it?**

Proposition #5: "<u>Our</u> Users Aren't *Your* <u>Real</u> Problem" (aka "Just Six Countries Account for Half the Spam Zombies on the CBL Blocklist")

- http://cbl.abuseat.org/country.html (Wed, 10 Jun 2009)

Total: 8,758,560 listed compromised hosts

Country	**Count**	**Percent**	**Cum Percent**
Brazil	1,313,360	15.00%	15.00%
India:	880,818	10.06%	25.05%
Turkey:	694,111	7.92%	32.98%
Russia:	684,747	7.82%	40.79%
Poland:	439,928	5.02%	45.82%
Vietnam:	310,939	3.55%	49.37%

Are There Simple Steps We Could Take To Help Address The Problem In Those Countries?

- For example, if I'm one of 1.3 million Brazilians with an infected system, are there Portuguese language versions of the tools I need to clean up those systems, and are there instructions to help walk me through using them? If I'm an Indian and I speak a South Asian language rather than English, are there tools and information resources to help me? What about those sort of resources in Turkish? Russian? Polish? Vietnamese?
- If those sort of resources don't exist, might that not be a simple but important deficiency to attack?
- **There's nothing like a week in a foreign country to remind you just how frustrating it can be to be unable to read signs and warnings and instructions written in another language you never bothered to learn!**

Proposition 6:
"Is The Ultimate "Cure" Really Prevention?"

- Are we tired enough of this problem that we're willing to step up efforts to prevent customers from getting infected in the first place?
- Has the time come for us to candidly advise users to consider alternative operating systems?
- Is this problem serious enough that we're willing to consider discouraging HTML-ified email and the exchange of attachments? Text-based email, after all, has limited infective potential.
- If so, what are we to do about some key web environments which absolutely require Javascript to be enabled, with all the security implications that can have? (And while NoScript may be great, it isn't the solution for less technical users)
- Are we willing to make and live with some hard choices?

Proposition 7: "Does The Government Have A Role As A Provider of Last Resort Assistance?"

- When a problem is of this breadth and magnitude (including international components and potential national security implications), is there a governmental role that should exist as a provider of last resort cyber assistance?
- If so, this **isn't** a law enforcement function, it is more a sort of "cyber welfare," or "national cyber insurance" thing.
- But if we can't afford the costs of real health care or all the other existing people-centered programs out there, can our government afford to take on new cyber-oriented responsibilities?
- **Who/what agency would offer this sort of service?**
- **How would we effectively reach out internationally?**
- **Do we <u>really</u> want to ask our governments to take this on?**
  If not, who will step up to handle it instead?

Thanks For The Chance To Share These Thoughts With You This Afternoon!