Panel: The Continuing Evolution of the Zombie Threat

MAAWG Fifth General Meeting

Montreal, Quebec

5-6 PM, Wednesday, 9 Nov 2005

Zombies: Updates, Data and Perspectives from Six Panelists

- Aaron Kornblum, Microsoft
- Alan Murphy, Spamhaus
- Chris Lewis, Nortel
- Dave Dagon, Georgia Tech
- Rob Fleischman, Simplicita
- Suresh Ramasubramanian, Outblaze

“What Is A Spam Zombie…?”

- A spam zombie is an insecure broadband-connected Windows PC which has been intentionally compromised by malware, malware which converts that system into a remotely-controlled anonymous proxy server without the assent of the system’s owner. Spammers then shovel spam through those machines.
- By some estimates, up to 80% of all spam today is delivered via spam zombies.

“Why Do Spammers Love Spam Zombies?”

- Spam zombies give spammers access to IP address space which hasn’t been DNSBL’d
- Spam zombies allow spammers to “smear” traffic across multiple IP addresses, thereby avoiding per-dotted-quad traffic limits
- Use of spam zombies complicates spam backtracking and attribution, making some spammers believe that if the use spam zombies, they’re “untraceable.”

“Look Upstream”

- At the March 2005 San Diego MAAWG meeting, I presented a talk explaining how providers can deal with spam zombies in a scalable way…
  -- recognize that spam zombies are spam **pipelines**, not spam factories; what goes out equals what came in -- so **look upstream**
  -- “looking upstream” means routinely collecting Netflow data (or SYNs) for inbound flows
  -- receive complaints? retrospectively review the **inbound** flows seen to the zombied customer
  -- block that inbound traffic src or report to taste

What's New With Spam Zombies Since That Time?

- Are providers, anti-spammers, researchers and vendors coping with the challenge spam zombies represent, or are spammers continuing to exploit spam zombies with impunity?
- What are the new challenges we collectively face in the area of spam zombies?