Dealing With Zombies and Trojans and Port 25

Joe St Sauver, Ph.D.

(joe@uoregon.edu)

MAAWG Senior Technical Advisor

March 3rd, 2005

http://darkwing.uoregon.edu/~joe/port25.html

Understanding Zombies

- Zombies are spam **pipelines**, not spam **factories**
- What goes out from a spam zombie is (to a first approximation) what came in
- That which is coming in is coming in FROM somewhere… WHERE?
- Spammers usings spam zombies RELY on you NOT bothering to look back upstream

Dealing with Zombies

- **==> LOOK AT THE *INBOUND* FLOWS THAT ARE TOUCHING YOUR ZOMBIED CUSTOMER HOSTS! <==**

  -- The folks abusing your customers are **really** easy to spot **if you just look!**

  -- They're almost always coming from US and Canadian colo facilities; they're **not** proxy chaining nor coming from overseas

  -- At any given time you're only looking at maybe 500-600 upstream source IPs

Network Engineers and Lawyers

- We recognize that many of you are abuse handlers or mail server architects, not network engineers -- you’ll **need** your network engineers to participate if you want to start trying a flow based approach
- You will **also** want to carefully review any proposed flow tracking measures with your lawyers (IANAL, but see 18 U.S.C. 2511(2)(a)(i) and 18 U.S.C. 2511(2)(g)(iv))

The Mechanics of Looking Upstream

- You can capture flow data from your routers using Netflow, or you could instrument your network using passive optical splitters plus something like Endace’s DAG packet capture cards (or Metanetworks Technologies’ cards)
- Yes, you *can* instrument OC192’s or 10gig ethernet links (as well as anything slower)
- Minimize what you collect; SYNs for inbound connections may be enough

Now That I’ve Identified The Upstream Zombie “Drovers…”

- Experiment a little: what happens when you complain to their providers? :-)
- One option is simply to block the zombie drovers /32 by /32 at the network level (or if you notice a pattern, by larger ranges)
- Civil lawsuits are another option
- Criminal prosecution may also be possible
- There are other amusing possibilities :-)

What About Blocking Port 25?

- Treating symptoms rather than underlying illness: blocking port 25 is cough syrup for lung cancer.
- Emitting spam email is really among the LEAST problematic behaviors that compromised customer hosts can exhibit (consider DDoS attacks, sniffing traffic, etc.)
- But what if you **do** decide to block port 25, if only because you’re sick of the coughing?

So You’ve Blocked Port 25…

- Even if you’ve blocked port 25, you still need to limit/track outbound mail via your officially permitted SMTP relays -- scaling?
- Forcing mail to go via official SMTP relays ==> all your users are “sharing fate.” Do you trust your SMTP relays enough to route YOUR outbound corporate email via them? Be willing to eat your own dogfood. :-)
- DNSBLs become less useful when everything goes via central SMTP relays

Details, Details…

- If you block port 25, what about SMTPS (encrypted SMTP) on port 465?
- Do NOT block port 587
- If you block port 25 **outbound**, be sure to also block port 25 **inbound** to prevent asymmetric traffic delivery (spammer with dual attached host: gig E at colo provider with no egress spoofing filters, dialup to you (just to get one of your IP and ACKs from the spoofed colo traffic))

Futures?

- Who knows? A couple of possibilities…
- Removal-resistant malware such as Hacker Defender today… “boobytrapped” “hostageware” tomorrow (try to remove a parasitic infection or just block traffic from a zombied host? ==> The malware may just *kill* that host… Customers/providers will just ***love*** that I’m sure…)
- Interfere with customer’s hosts being used for spamming purposes? Expect to see some “packet love” (spam zombies auto-converting into DDoS agents upon blocking/loss of spammer usability)