What Is ROI for Attackers

- Researchers subverted a botnet's command and control infrastructure (proxy bots)
  - Modified its spam messages to point to the Web server under researcher control
- That server mimicked the original Web page from the spam emails
  - A pharmacy site
  - A greeting card download site

"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

What Is ROI for Attackers

- How many spam emails reach recipients: open a few email accounts themselves and append them to email delivery lists in spam messages
- How many emails result in Web page visits
  - Must filter out defense accesses
- How many users actually buy advertised products or download software
  - No "sale" is finalized
- Ethical issues abound

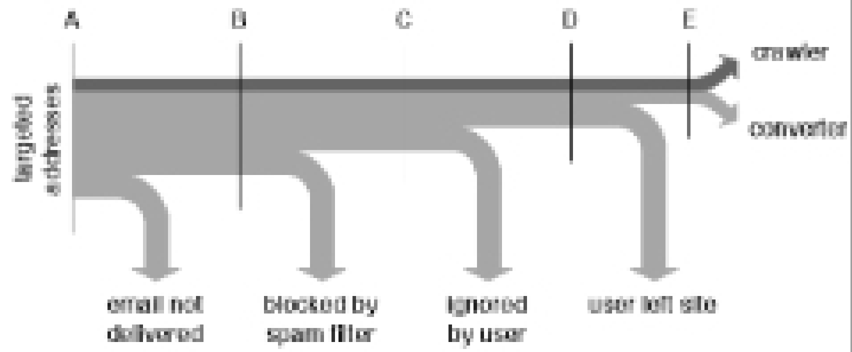
"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

Most-targeted E-mail Domains

Domain	Freq.
hotmail.com	8.47%
yahoo.com	5.05%
gmail.com	3.17%
aol.com	2.37%
yahoo.co.in	1.13%
sbcglobal.net	0.93%
mail.ru	0.86%
shaw.ca	0.61%
wanadoo.fr	0.61%
msn.com	0.58%
Total	23.79%

"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

Spam Conversion Pipeline



"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

Spam Conversion Pipeline

Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
C – Inbox Delivery	—	—	—	—	—	—
D – User Site Visits	10,522	0.00303%	3,827	0.00457%	2,721	0.00678%
E – User Conversions	28	0.0000081%	316	0.000378%	225	0.000561%

"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

Spam Filter Misses

Spam Filter	Pharmacy	Postcard	April Fool
Gmail	0.00683%	0.00176%	0.00226%
Yahoo	0.00173%	0.000542%	none
Hotmail	none	none	none
Barracuda	0.131%	N/A	0.00826%

"Spamalytics: An Empirical Analysis of Spam Marketing Conversion" C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage, ACM CCS 200

For More on Botnets

http://www.shadowserver.org
http://www.honeynet.org/papers/bots/
http://www.honeynet.org/papers/ff

Trusted Computing

What Problem Are We Solving?

- Can't protect applications from within themselves
  - Exploits can turn off defenses
- Can't protect the OS from within itself
  - Exploits can turn off defenses
  - Rootkits can hide any sabotage from users
- May not be able to trust users
  - They may be uninformed
  - They may be malicious – OK for their computer but risk for the others they communicate with
  - Digital right management issues

What is Trusted Computing

- Attestation
  - Means of ensuring someone (user, remote computer) of the system's trustworthy status
    - Usually means authentic/approved apps
  - Root of trust needed to store keys
  - Trusted path (allows user to have confidence in the system)
  - Chain of trust (like for certificate authorities)
- Separation
  - Secure storage (data/keys)
  - Protection of processes
- The rest is policy
  - That's the hard and controversial part

Trusted Path

- We need a "trusted path"
  - For user to communicate with a domain that is trustworthy.
    - Usually initiated by escape sequence that application can not intercept: e.g. CTL-ALT-DEL
  - Could be direct interface to trusted device:
    - Display and keypad on smartcard

Communicated Assurance

- We need a "trusted path" across the network.
- Provides authentication of the software components with which one communicates

What Can We Do with TC?

- Clearer delineation of security domains
  - We can run untrusted programs safely
    - Run in domain with no access to sensitive resources
    - Such as most of your filesystem
    - Requests to resources require mediation by TCB (trusted computing base), with possible queries to the user through trusted path.

Mediating Programs Today

- Why are we so vulnerable to malicious code today?
  - Running programs have full access to system files
  - Why? NTFS and XP provide separation
    - But many applications won't install, or even run, unless users have administrator access
  - So we run in "System High"

Corporate IT Departments' Solution

- Users don't have administrator access even on their own laptops
  - This keeps end users from installing their own software, and keeps IT staff in control
  - IT staff select only software for end users that will run without administrator privilages
  - But systems still vulnerable to exploits in programs that cause access to private data
  - Effects of "Plugins" can persist across sessions

The Next Step

- But, what if programs were accompanied by third party certificates that said what they should be able to access?
  - IT department can issue the certificates for new applications
  - Access beyond what is expected results in system dialogue with user over the trusted path

Red / Green Networks

- Butler Lampson of Microsoft and MIT suggests we need two computers (or two domains within our computers)
  - Red network provides for open interaction with anyone, and low confidence in who we talk with
  - We are prepared to reload from scratch and lose our state in the red system

Red / Green Networks

- The Green system is the one where we store our important information, and from which we communicate to our banks, and perform other sensitive functions
  - The Green network provides high accountability, no anonymity, and we are safe because of the accountability
  - But this green system requires professional administration
  - A breach anywhere destroys the accountability for all