CS294 Lecture Notes: Botnets
November 13, 2009

Professor: Vern Paxson
Scribe: Emil Stefanov

Botnets / The Modern Threat Labdscape

- 1990's – early 2000's
    - IRC Wars
    - IRC based botnets
    - Vandals -> Cybercrime
- Example: MIPS router infection

    - Hard to defend against – no antivirus is installed on the router to detect it and help clean it up.
- Commercial off the shelf (COTS) software for crooks
    - Can then be used by other actors, such as spies
- GhostNet cyber spying operation

- Infected embassies, NATO, the Dalai Lama, and many more computer systems of political entities.

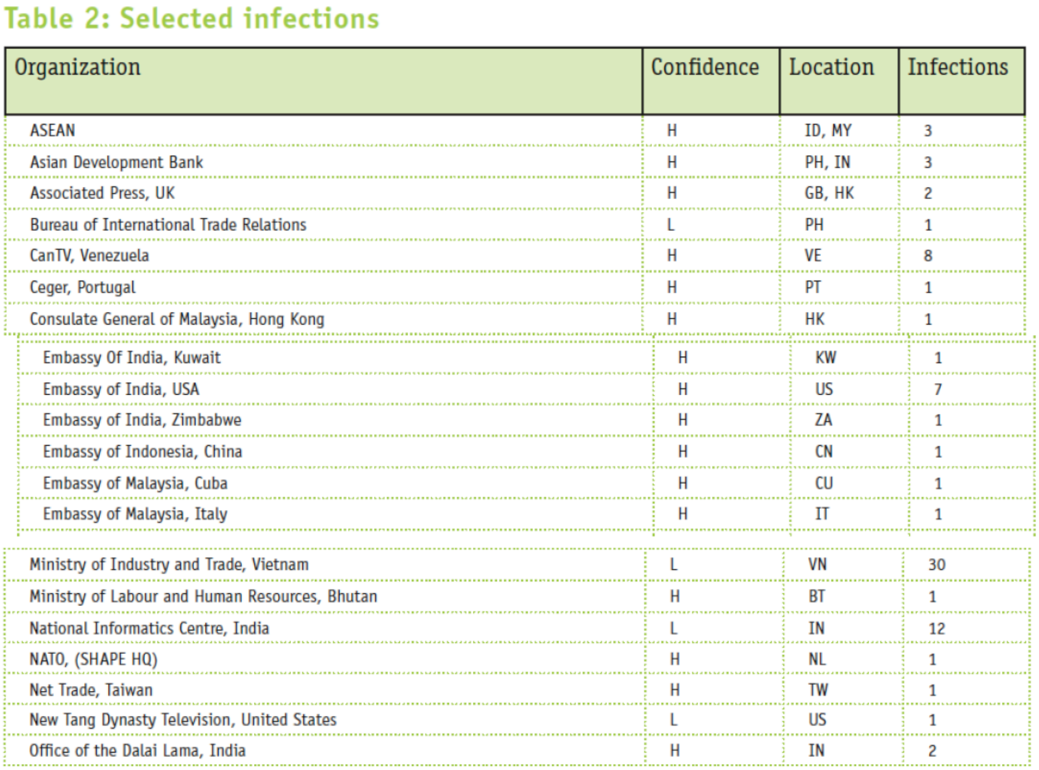
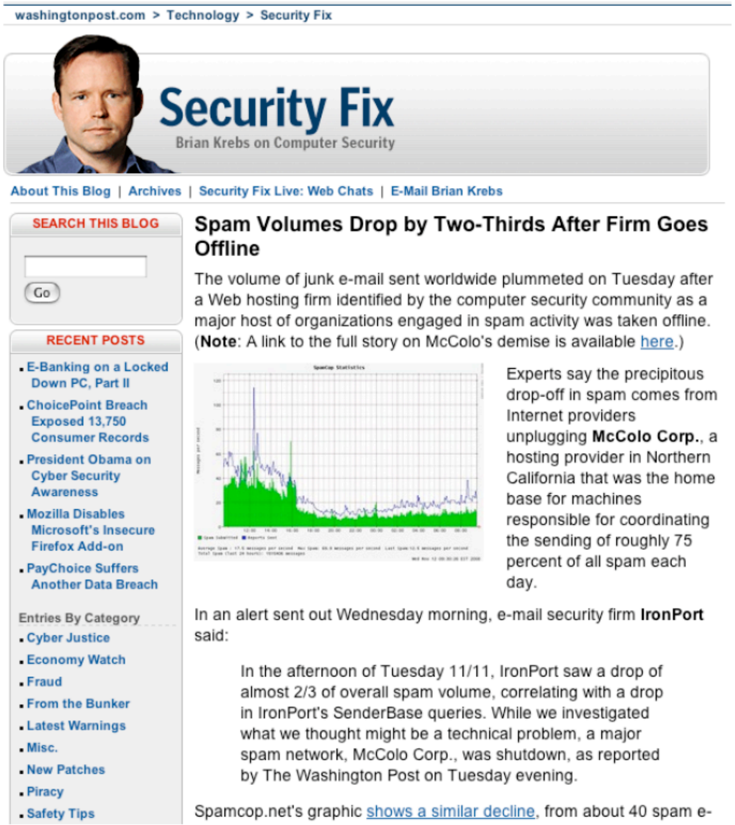


Table 2: Selected infections

Organization	Confidence	Location	Infections
ASEAN	H	ID, MY	3
Asian Development Bank	H	PH, IN	3
Associated Press, UK	H	GB, HK	2
Bureau of International Trade Relations	L	PH	1
CanTV, Venezuela	H	VE	8
Ceger, Portugal	H	PT	1
Consulate General of Malaysia, Hong Kong	H	HK	1
Embassy Of India, Kuwait	H	KW	1
Embassy of India, USA	H	US	7
Embassy of India, Zimbabwe	H	ZA	1
Embassy of Indonesia, China	H	CN	1
Embassy of Malaysia, Cuba	H	CU	1
Embassy of Malaysia, Italy	H	IT	1
Ministry of Industry and Trade, Vietnam	L	VN	30
Ministry of Labour and Human Resources, Bhutan	H	BT	1
National Informatics Centre, India	L	IN	12
NATO, (SHAPE HQ)	H	NL	1
Net Trade, Taiwan	H	TW	1
New Tang Dynasty Television, United States	L	US	1
Office of the Dalai Lama, India	H	IN	2

- Trail points strongly to Chinese origin
- Can send email w/ poisoned attachments from infected machine to contacts for spearphishing

- McColo shutdown (a “bulletproof hosting service” – resists take-down)



washingtonpost.com > Technology > Security Fix

Security Fix
Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

SEARCH THIS BLOG

Go

RECENT POSTS

- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

Entries By Category

- Cyber Justice
- Economy Watch
- Fraud
- From the Bunker
- Latest Warnings
- Misc.
- New Patches
- Piracy
- Safety Tips

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)

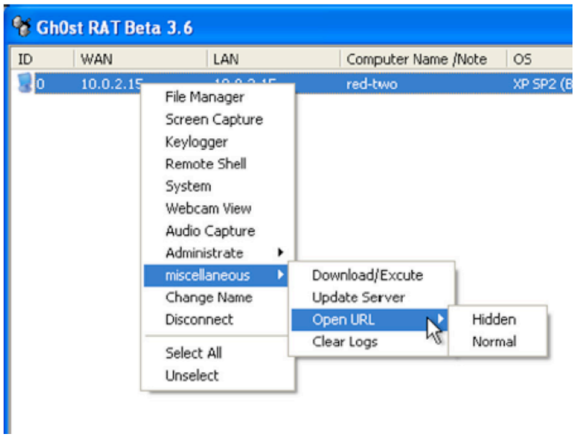
Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

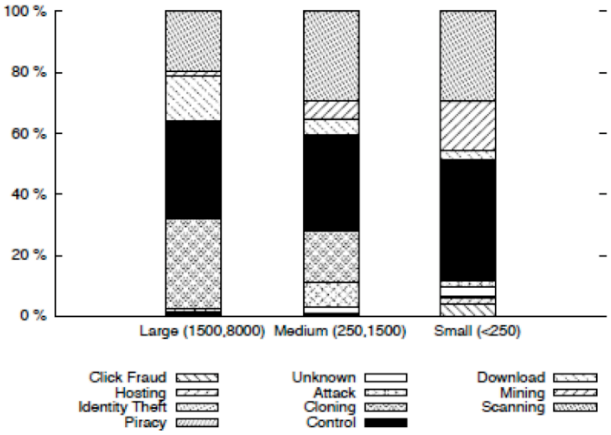
In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

> In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

    - Effective: 2/3 reduction in spam
    - Short-lived
- Botnets adapted. Now they don’t use centralized C&C servers. They have a list. If the list is exhausted then it connects to a new automatically generated DNS name every day.
- We can use DNS cache testing to find out if botnet C&C servers have been looked up.
    - 95% of Chinese servers showed such lookups.
- It seems that Botnets do a lot of different things.





Botlab

- It used the UW Spam feed.
- A Problem: Can have benign URL in spam.
    - Following links can have bad effects on real messages
        - Example: signing up people to review papers.
- How is it that Rustok sends so much less spam but causes about the same amount of incoming UW spam?
- Ethics
    - Could increase somone's spam
    - Prudence
    - Prosecutorial discretion
        - The notion that if something is illegal, it still may prove okay in practice if no reasonable prosecutor is going to go after you for it
- Containment when studying malware
    - Rate limit outbound output
    - Signature check
- Wrong conclusion: 1 IP address = 1 host for 1 day
    - Recent studies show that's not a good assumption, aliasing happens more frequently.

Ethics + Disruption

- Can shut it down, but should you?
    - Not obligated.
    - There can be greater long term good if you can study it
    - Nasty damage if you take it down
    - It may be illegal to shut it down
- MegaD shutdown by FireEye
    - Only received praise
    - They hijacked the C&C server and did nothing (didn't send any commands)
        - Limits the amount of potential damage that could have resulted in trying to remove it rather than silently disable it.

THE IMAGES IN THIS DOCUMENT WERE COPIED FROM VERN PAXSON'S LECTURE NOTES OF THE CORRESPONDING BOTNETS LECTURE.