Conficker Summary and Review

David Piscitello
ICANN Sr. Security Technologist

What is Conficker?

- An Internet worm
  - Self-replicating malicious code
  - Uses a network for distribution
- A blended threat
  - Uses various methods to spread the infection (network file shares, map drives removable media)
- A Dynamic Link Library
  - Conficker is not an executable but **additional code**
  - An executable already on a computer loads conficker

ICANN sydney No.35 21 - 26 JUNE 2009

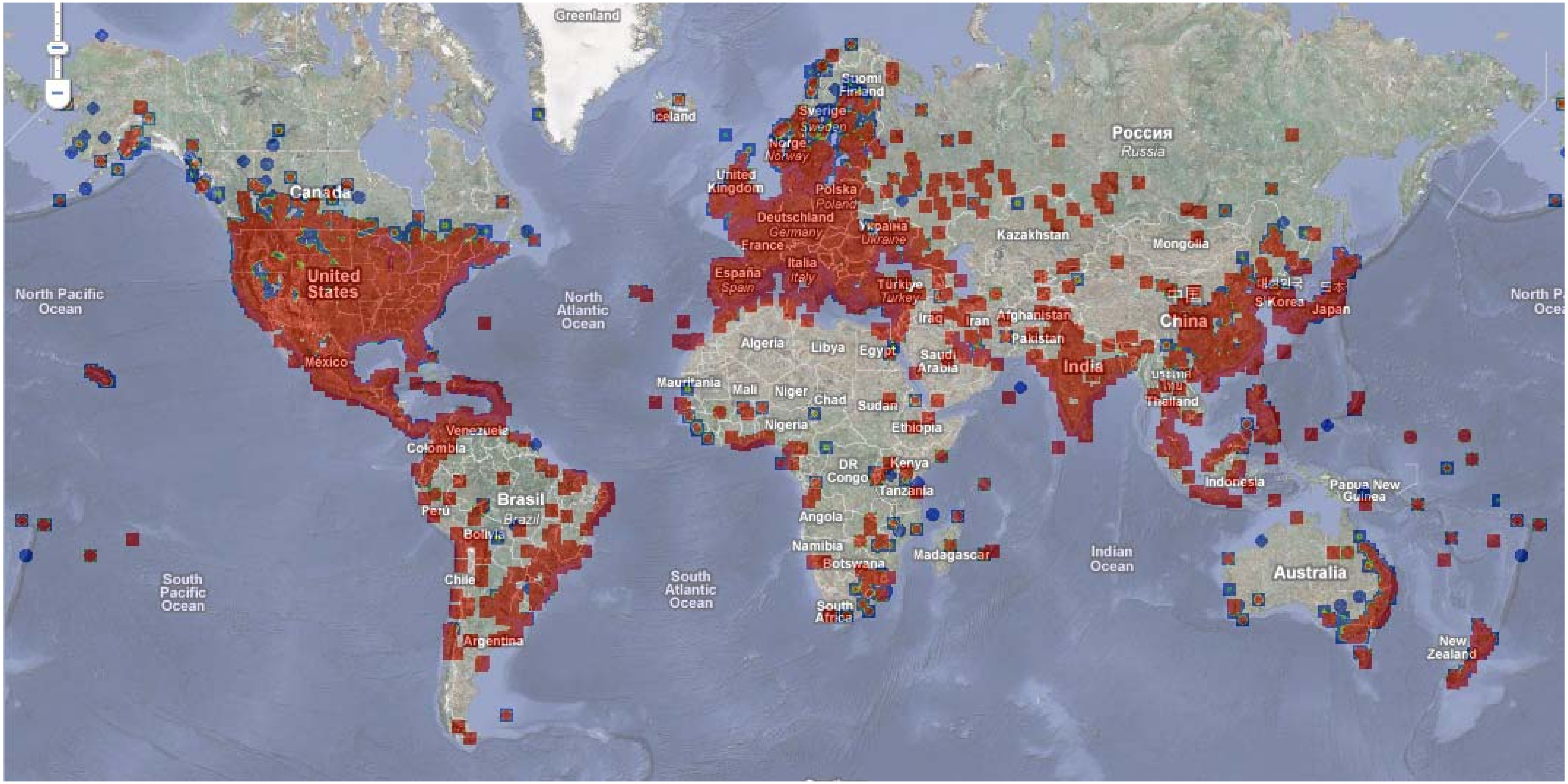
What does Conficker do?

- Sends an Remote Procedure Call request to a target system to cause a buffer overflow
- RPC request exploits a vulnerability in Windows Server service (MS08-67)
- Conficker code is *injected* into Windows Server Service
  - Variants disable security measures
  - Provides the attacker with remote control, execution privileges, and ability to download more malware
- Enlists the infected computer into a botnet
  - Conficker bots query rendezvous points for additional malware or instructions for already present malware

What is the Conficker botnet?

- An army that can be directed at will by rendezvous points to support a wide range of malicious, criminal or terrorist activities *for as long as the computer remains infected and as long as the bots can remotely communicate with the rendezvous point(s)*

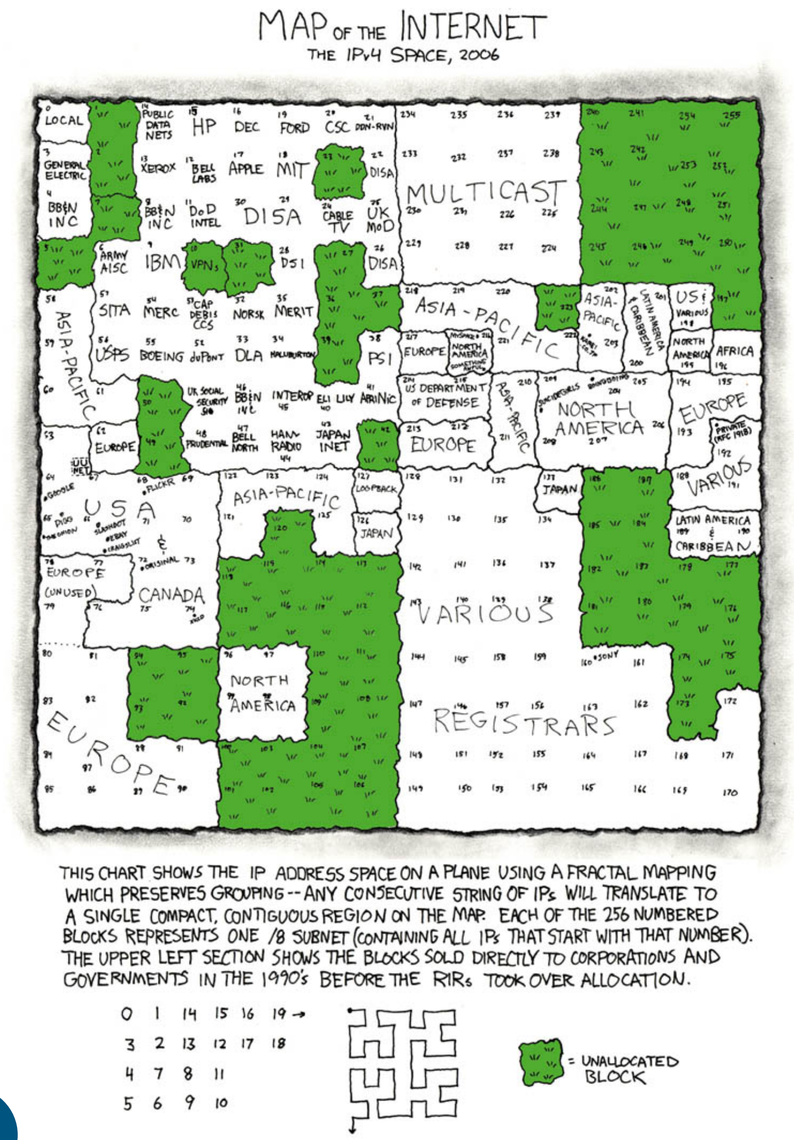
Infection Map (World)



Source:
http://www.confickerworkinggroup.org

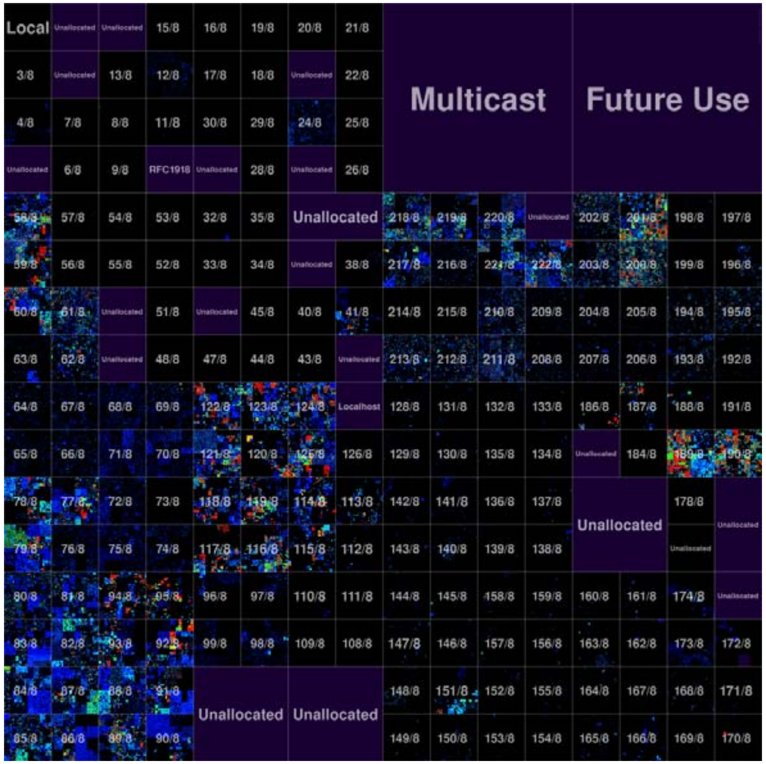
ICANN sydney No.35 21 - 26 JUNE 2009

Infection (IP network blocks)



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

Map of the Infected 'net
The Ipv4 Space, 2009



Sources:
http://imgs.xkcd.com/comics/map_of_the_internet.jpg
http://www.confickerworkinggroup.org

Why is Conficker remediation hard?

- Security community cannot hope to remove malware from millions of computers
  - Patch for MS08-067 vulnerability in October 2008
  - 30% of Windows systems still vulnerable January 2009 (Source: Qualys)
  - Unlicensed copies of Windows OSs cannot be patched
- Malware writers are strongly incented to adapt quickly to detection and removal methods
  - Variants of malware “released” to resist known methods for detection and removal by disabling security software
  - Conficker variants also adapted the way bots contact rendezvous points in response to actions taken by security and DNS community

Variant & date	Bot Evolution	DNS/Domain Abuse
Conficker.A 2008-11-21	• Infects via MS08-67 exploit, anonymous shares • Resets system restore point • Contacts C&C for updates	250 pseudo-randomly generated domains registered in 5 TLDs
Conficker.B 2008-12-29	• Infects via MS08-67 exploit, anonymous and weakly passworded shares, map drives, removable media • Resets system restore point • Updates the domain name generation algorithm • Disables security software and security updates	250 pseudo-randomly generated domains registered in 8 TLDs
SRI Conficker.C a.k.a. Conficker.D 2009-02-20	• Infects via MS08-67 exploit, spreads via anonymous shares, shares with weak passwords, map drives • Resets system restore point • Disables security software and security updates • Changes from C&C model to P2P • Set 1 April 2009 date for D/E update	Tens of thousands of pseudo-randomly generated domains registered in 100+ TLDs
Conficker.E	•Infects via MS08-67 exploit, updates earlier variants •Resets system restore point •Changes from C&C model to P2P •Disables security software and security updates • Self-destructs on 3 May 2009 • Possible connection to Waledac	

ICANN sydney No.35 21 - 26 JUNE 2009

Containing Conficker:
Learning from McColo Takedown, Srizbi botnet

- McColo takedown (November 2008)
  - ISPs stopped routing traffic to hosting provider
  - Srizbi bots could not reach C&Cs at McColo
  - AV companies reported (temporary) 60-75% drop in spam
- Malware writers value resilient networking
  - Srizbi bots attempted to contact C&Cs at pseudo-randomly generated domain names when hard-coded IP addresses became unreachable
- Reverse engineering of Srizbi payload reveals algorithm
  - Security community preemptively blocked registrations
  - Similar strategy proved effective in containing Conficker

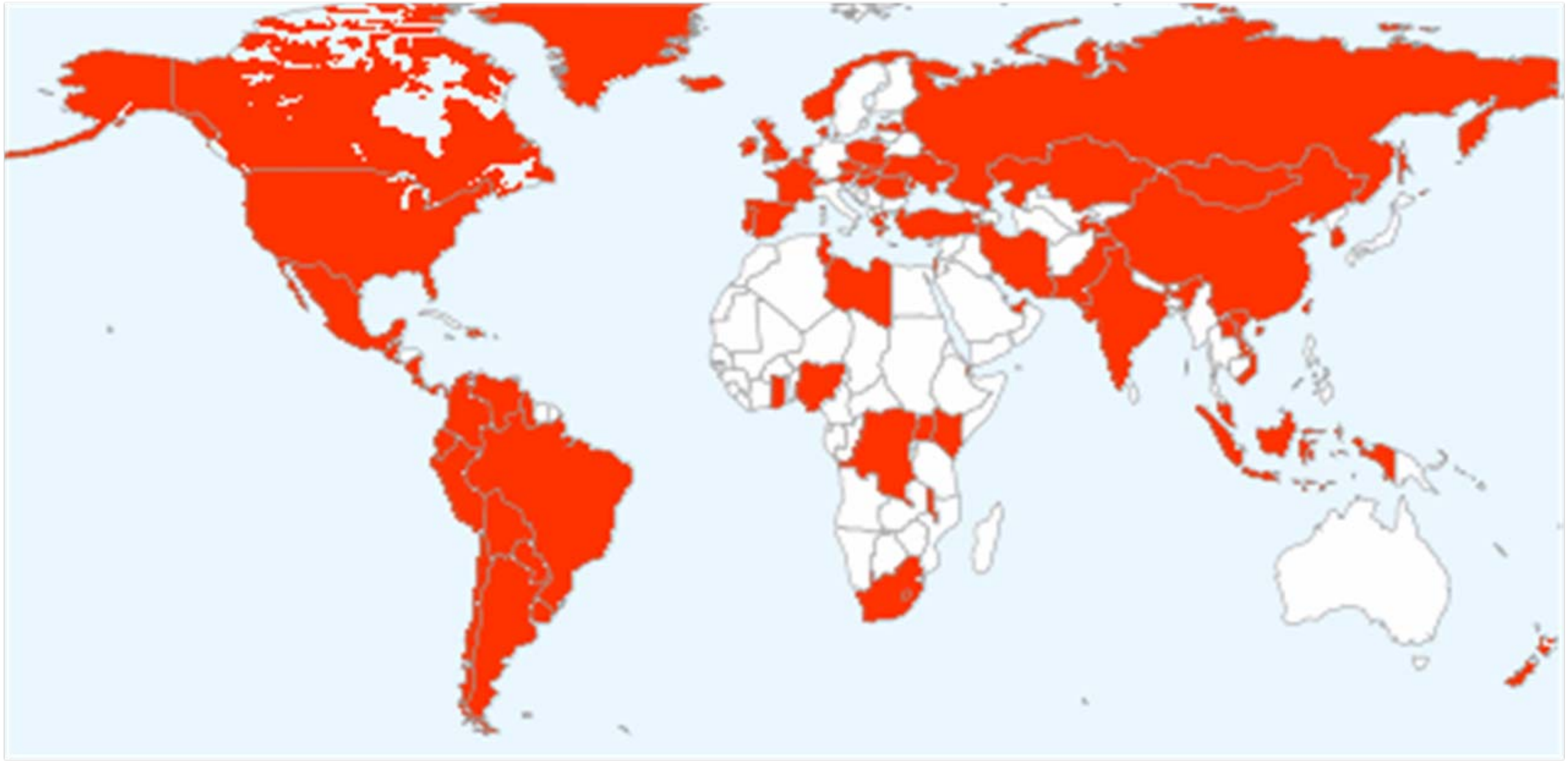
Conficker Chronology of Events

- November 2008 – 1 January 2009
  - Security community identify Conficker.A
  - Researchers preemptively register domains to contain botnet
- 2 January – 3 February 2009
  - Conficker name algorithm uses more names, more TLDs
  - Security community asks DNS community for help in containing Conficker
  - DNS community joins ad hoc partnership, blocks Conficker domains at registry
- 12 February 2009
  - First public announcement of collaborative operational response
  - Microsoft offers $250,000 reward

Conficker Chronology of Events (Cont'd)

- 19 February 2009 – 31 March 2009
  - Conficker.C/D identified, more aggressive in domain registrations, begins using P2P
  - DNS community continues to block domains, Security community releases Conficker scanners
- 1 April 2009
  - Conficker.E variant activated on previously infected hosts
- 3 May 2009 - present
  - Conficker.E variant removes itself but leaves DLL and P2P network in place
  - Security community continues to monitor activities, studying relationship with Waledac worm

Affected Country Code TLDs



Positive Lessons learned

- Security and DNS communities can work effectively together, at an operational level, to contain global security threats
  - Trust was a critical element in ad hoc partnership
- Communications channels are essential in coordinating operational response
  - ICANN's role in enabling communications and staff participation in ad hoc partnership was appreciated
- Security and DNS communities need each other
  - Leverage competencies rather than duplicate them
  - Collective, global expertise is essential for effective response

Problems not yet solved

- Collaborative response forced botnet operators out of comfort zone but not out of business
- Botnet writers are agile and elusive
  - Cannot put them out of business without adopting a similarly agile model for response
- Communications channels are difficult to sustain
  - Numerous and complex, harder to build and maintain fragile than botnets
- The risk-reward table favors our adversary
  - Low risk, low cost, high reward for bad actors
  - High risk, high cost, modest reward for good actors

Way forward

- Efforts to effectively block Conficker use of the DNS should be sustained
  - Must address challenges of long-term engagement
- Broader collaborative efforts within both the security and DNS communities should be considered
  - Security community dialogue about future collaboration models on-going
- In the DNS community, key players have continued to discuss how to organize effectively
  - ICANN plans for active participation in these efforts