DNS Abuse:

The fight against digital crime

Richard Domingues Boscovich
Sr. Attorney
Microsoft Digital Crimes Unit

MICROSOFT
DIGITAL
CRIMES
UNIT

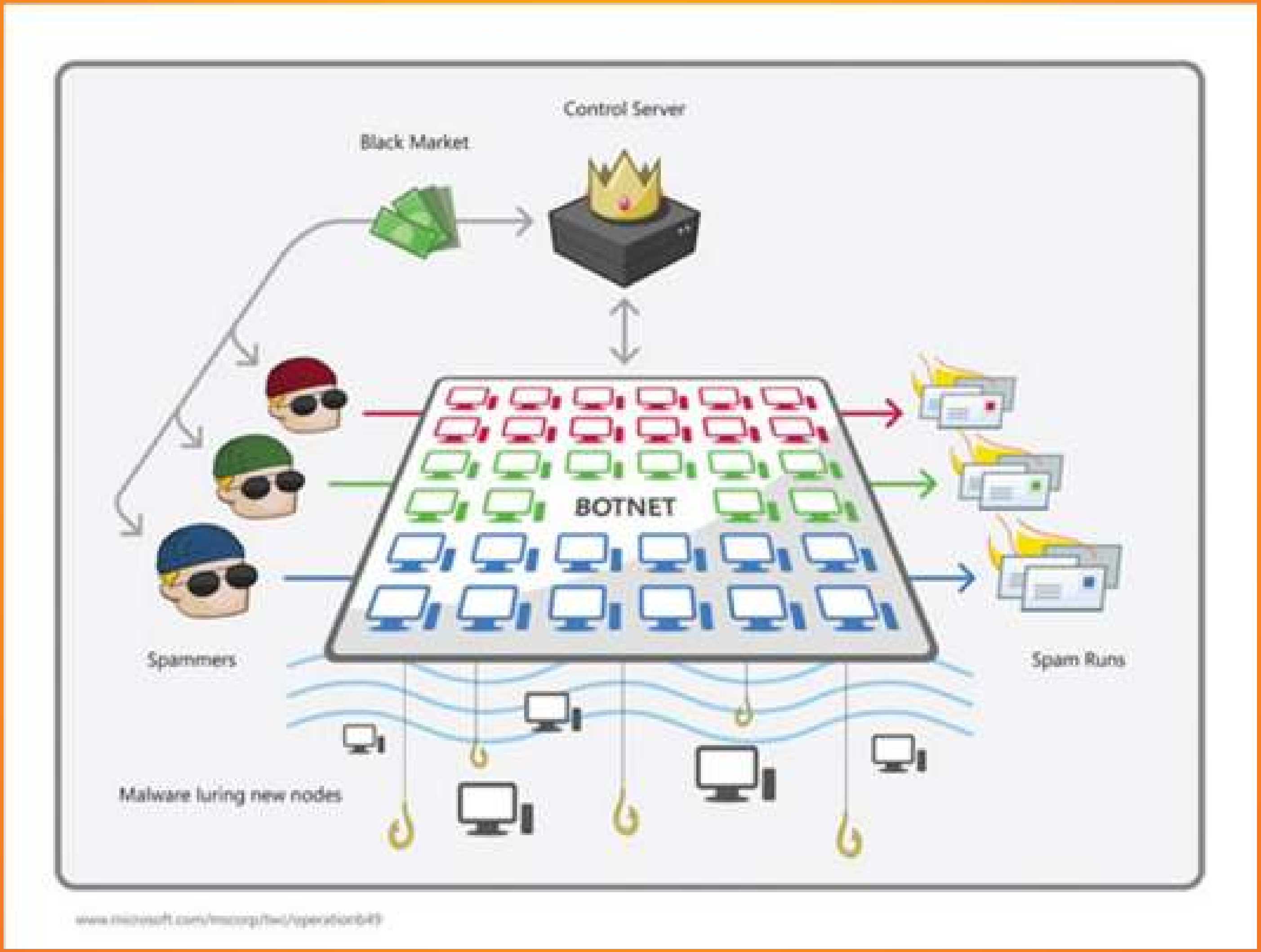
Microsoft Digital Crimes Unit

A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is **to make the Internet safer and more secure** through strong enforcement, global partnerships, policy and technology solutions that help:

- Promote a secure Internet
- Defend against fraud and other threats to online safety
- Protect children from technology-facilitated crimes
- Champion a healthy Internet marketplace for advertisers and businesses

MICROSOFT DCU

Going after the criminals' own infrastructure…"Botnets"



Going after the criminals' own infrastructure…"Botnets"

– Operation b49: The Waledac botnet takedown
  – On October 27 2010, Microsoft secured a default order and took possession of 277 domains used as C& C's for the Waledac botnet
  – Operation b49 effectively severed between 70,000 and 90,000 computers from the botnet
  – B49 was the first initiative in Microsoft's Project MARS, a broad effort to annihilate botnets

Operation b49

Novel Legal Theory Supporting Defensive DNS

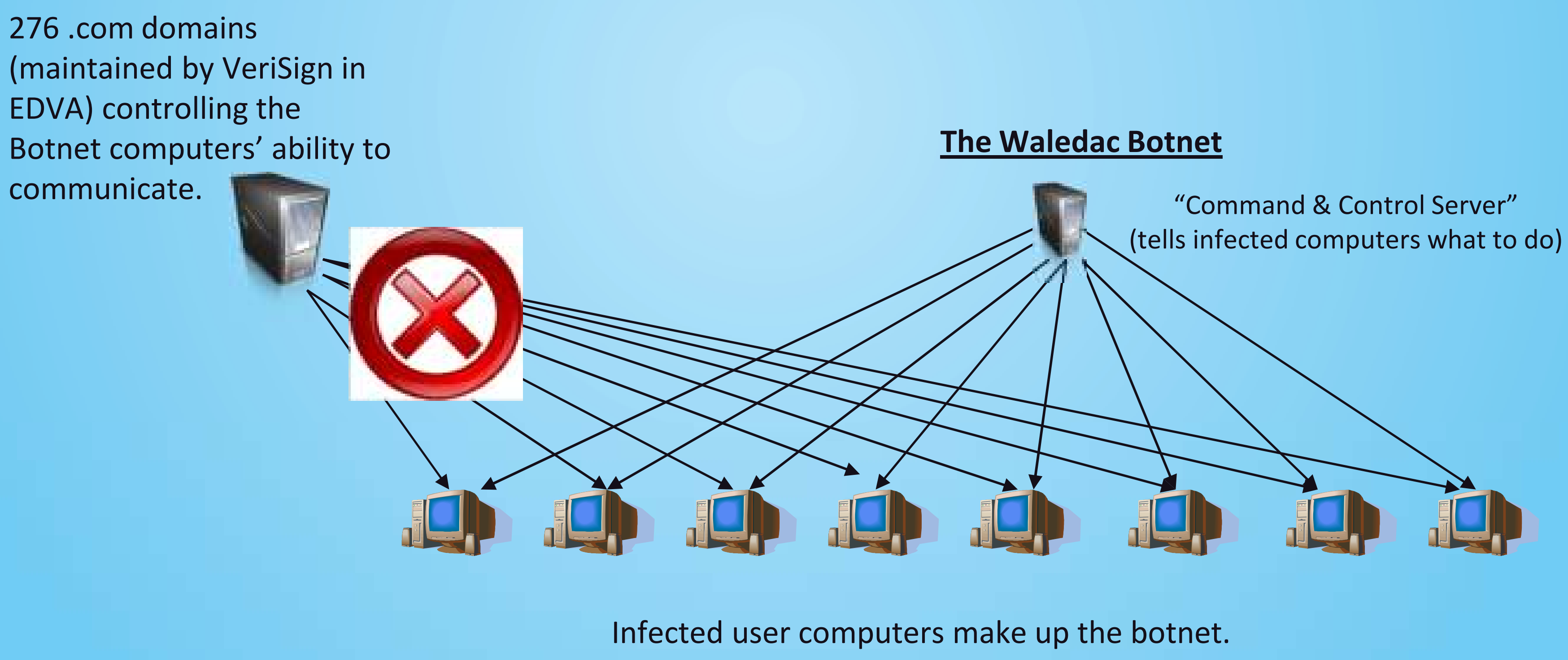
– The Legal Obstacle to Taking Down a BotNet
  - Due Process Rights: Parties have a right to receive notice
  - However, notice to botnet defendants allows them to move the botnet, destroy evidence, and avoid prosecution.

– The Solution, *Ex Parte* Temporary Restraining Order (“TRO”):
  - A very extraordinary remedy
  - Temporarily restrains defendant’s conduct without notice
  - Must show that “immediate irreparable” harm will occur

Operation b49

Novel Legal Theory Supporting Defensive DNS

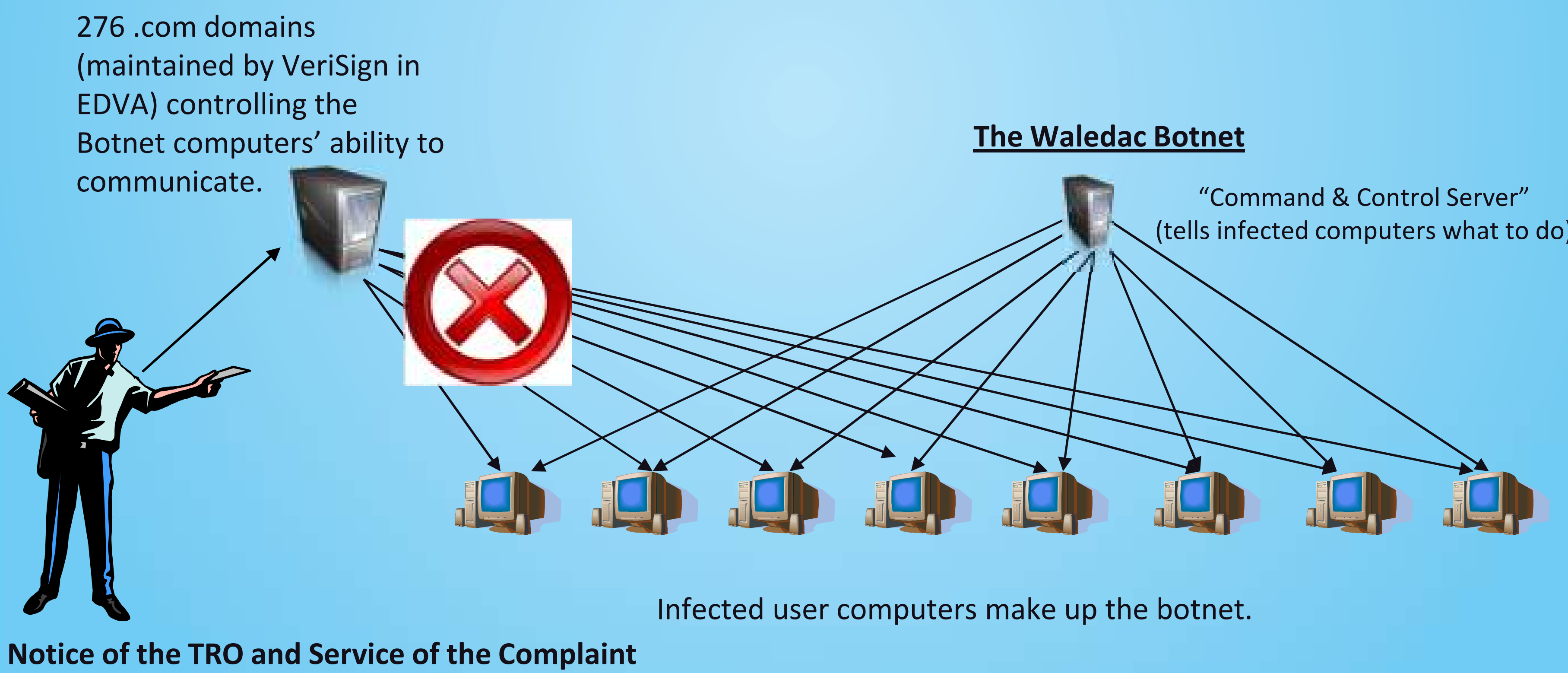
- Once *ex parte* TRO granted, Microsoft had four days to act before giving notice to defendants
- Microsoft coordinated with VeriSign to shut down the 276 domains disseminating malicious botnet code



Operation b49

Novel Legal Theory Supporting Defensive DNS

- Once the immediate harm was stopped, Microsoft had to provide notice to domain registrants by (1) e-mail, (2) personal service, (3) fax, and (4) publication on a website.



Operation b49

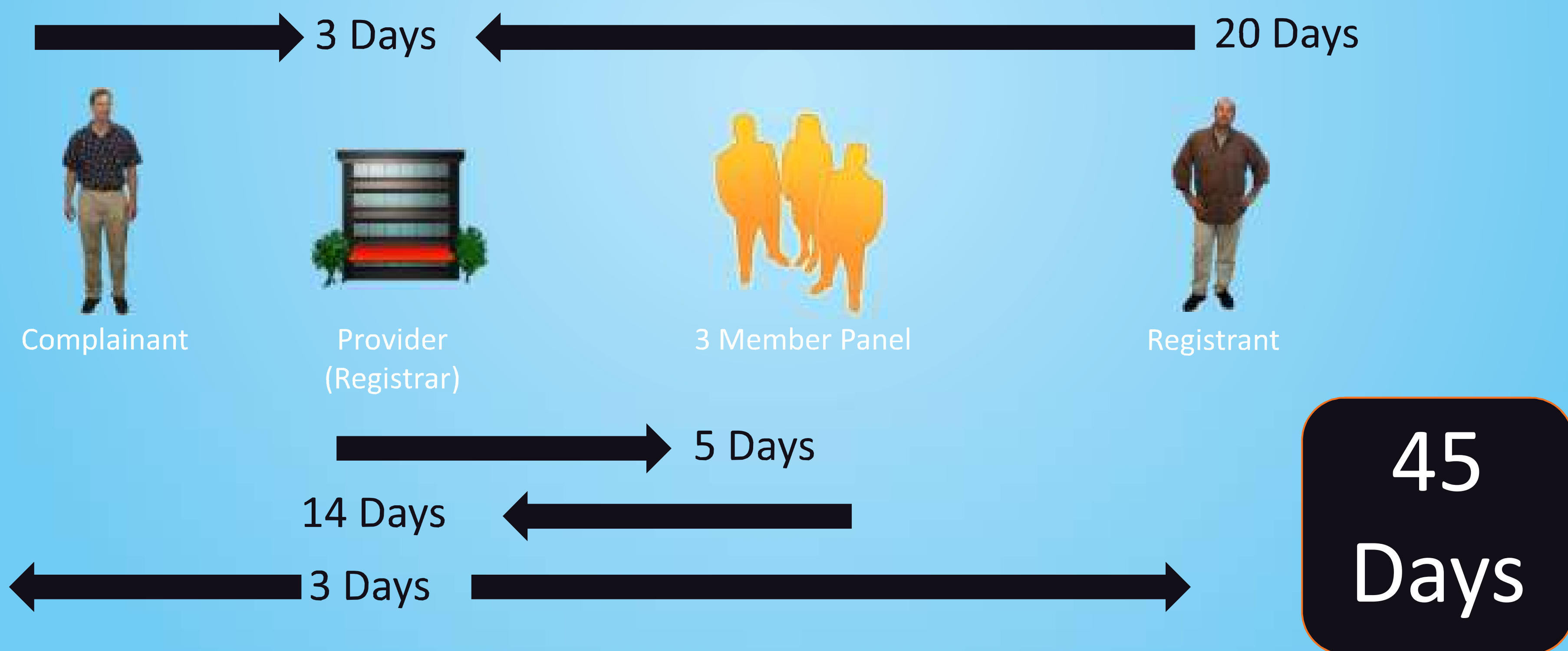
Novel Legal Theory Supporting Defensive DNS

Internet Corporation for Assigned Names and Numbers

Operation b49

Novel Legal Theory Supporting Defensive DNS

Uniform Domain Name Dispute Resolution Policy - UDRP



Operation b49

Novel Legal Theory Supporting Defensive DNS

ICANN

Internet Corporation for Assigned Names and Numbers

Operation b49

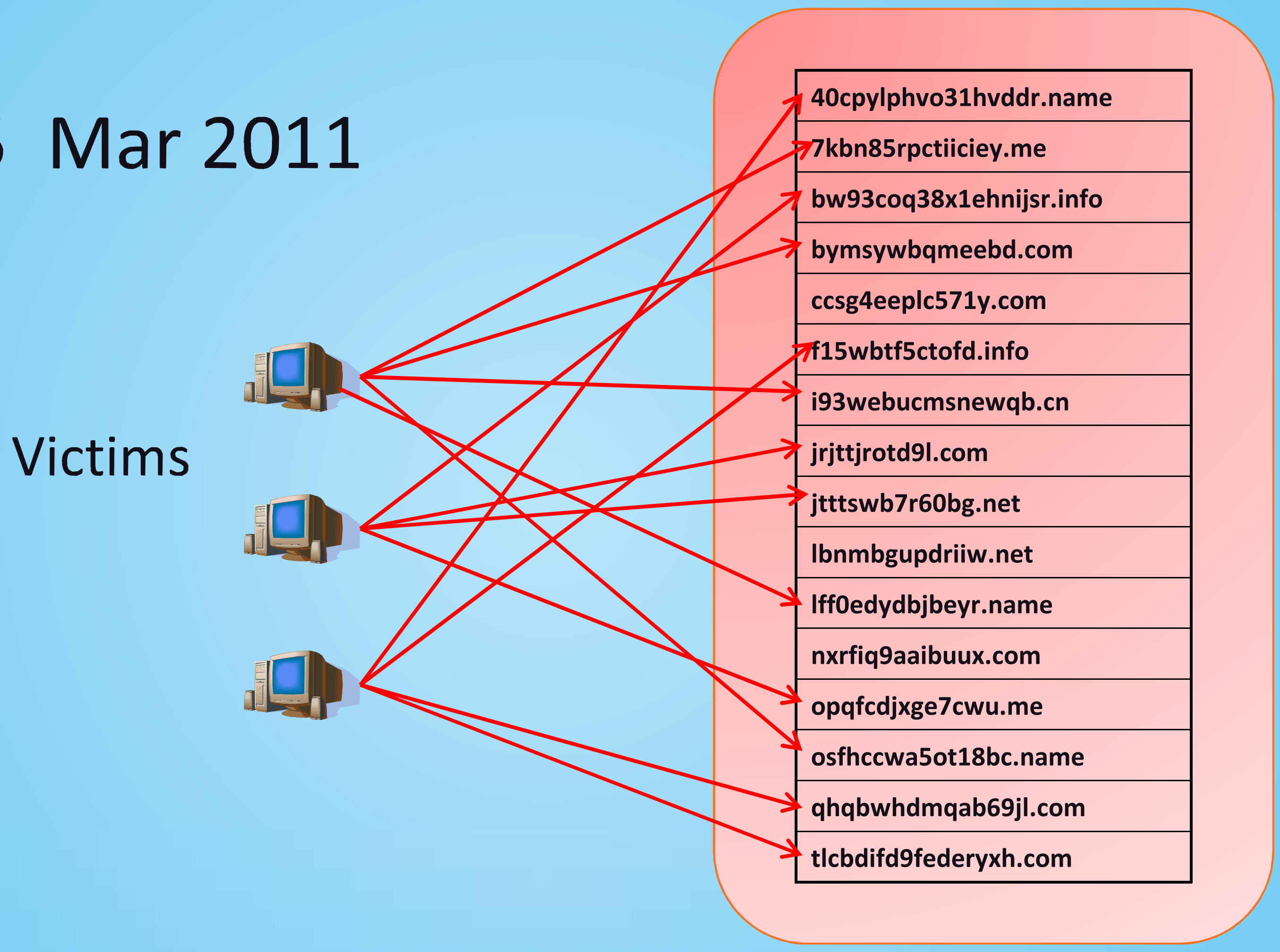
Novel Legal Theory Supporting Defensive DNS

- Obstacles to Effecting Service and Notice Abroad

  - Almost all domains were registered through China domain registrars
  - Identifying and locating registrants abroad is difficult
  - Working through international treaties to effect personal service is complex and slow
  - Ensuring registrant's U.S. due process rights are preserved abroad requires creative forms of notice

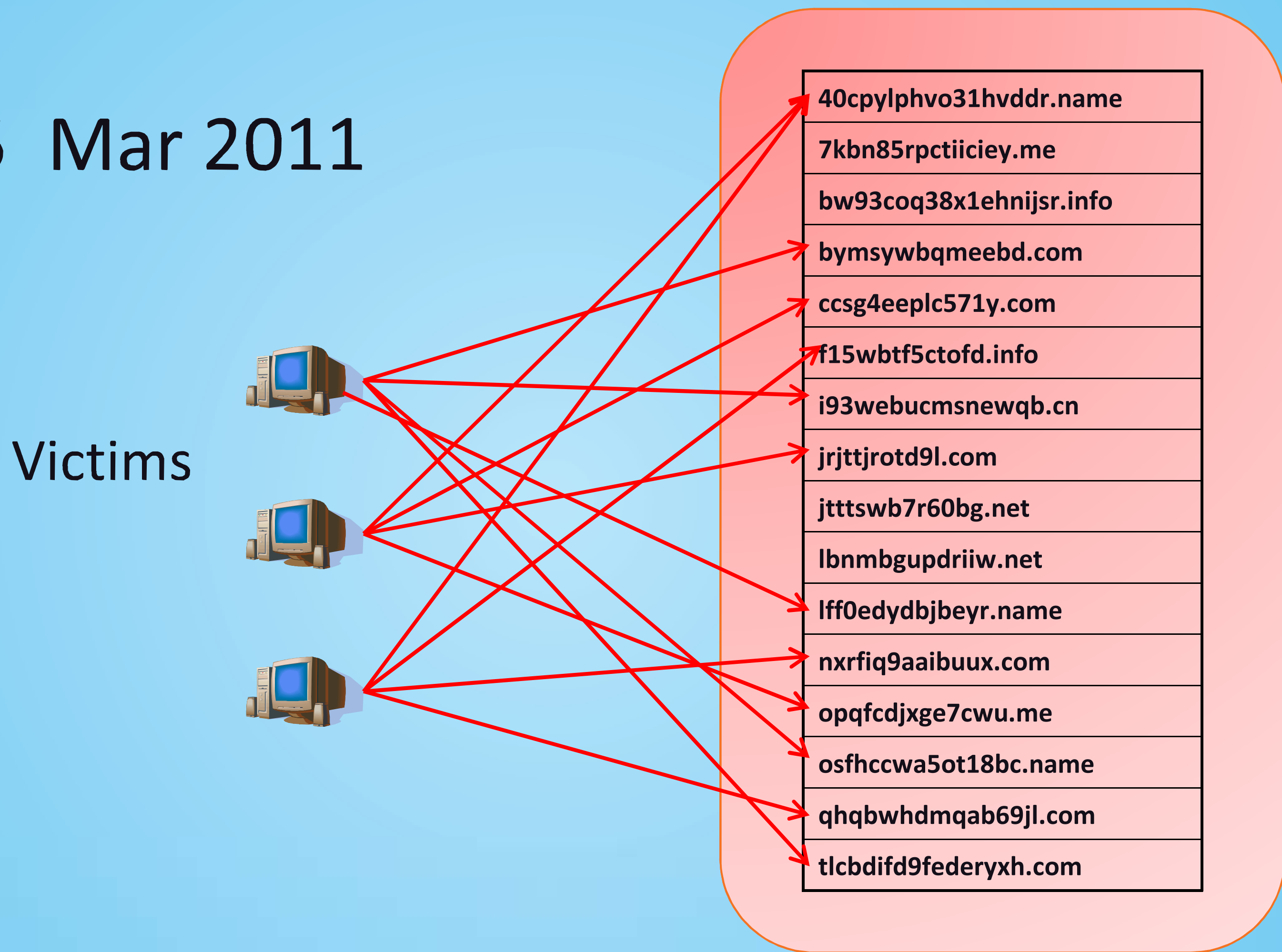
Domain Name Generation Algorithm/Hardcoded

15 Mar 2011



Domain abuse

15 Mar 2011



Follow us on

Facebook and Twitter!

facebook.com/MicrosoftDCU
twitter.com/MicrosoftDCU

MICROSOFT DIGITAL CRIMES UNIT