Anti-Phishing Working Group

www.antiphishing.org

Phishing - Current Status and Mitigation Advice

Presentation for ccNSO Meeting

ICANN - Los Angeles
October 31, 2007

Rod Rasmussen
Co-Chair DNSPWG of the APWG

Agenda

- Overview of APWG
- Current Phishing Issues
- Implications for ccTLD operators
- Mitigation Techniques and Suggestions
- Q&A

Anti-Phishing Working Group

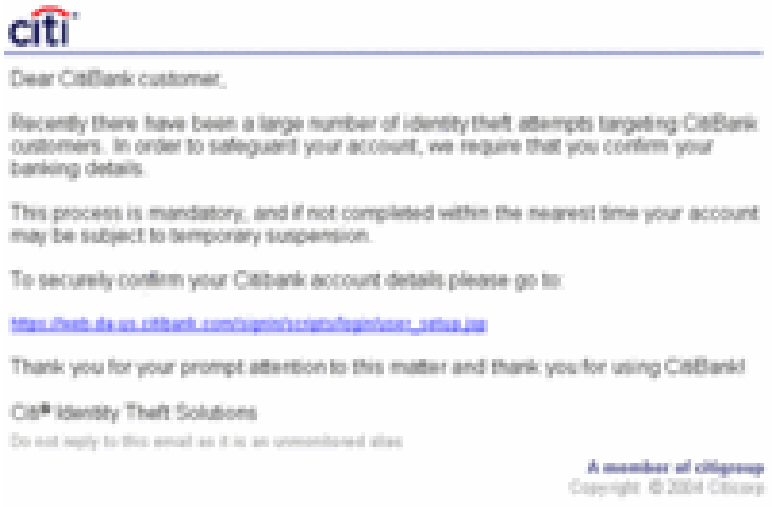
- Launched in 2003
- 2600+ members
  - 1600+ companies and agencies (worldwide)
  - e-Commerce, financial, telecomm, ISP's, solution vendors, law enforcement, academics, national CERTs, etc.

- Focus: Eliminating fraud and identity theft that result from phishing, pharming, crimeware and email spoofing of all types

Phishing Review

In General:

Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and/or financial account credentials.


citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

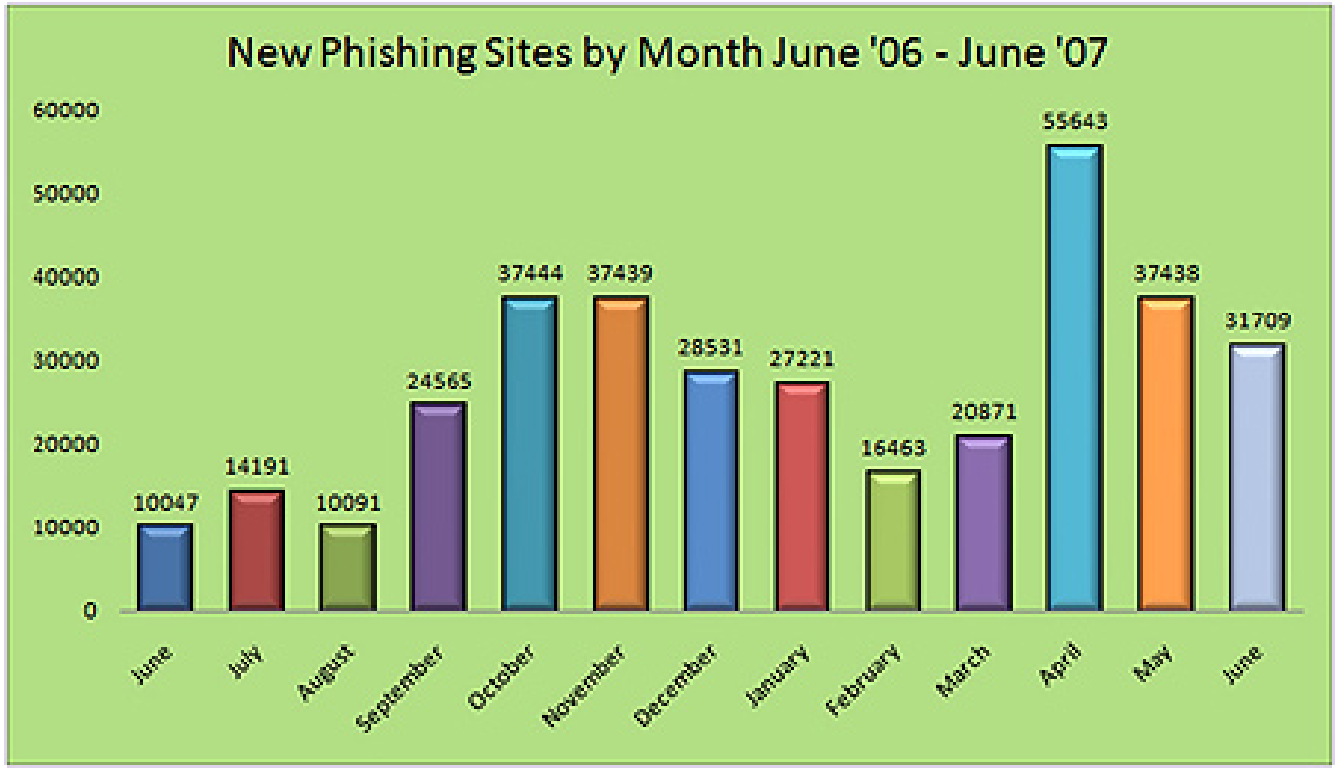
Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

The Overall Phishing System

- Lure to Potential Victims
  - Mainly email, but VOIP, IM, phone, letter are used
  - Malware (keystroke logger, worm) attached (growing)
- Web Interface to User/Victim
  - 'Personal' web pages, hacked servers, phish domains
  - Multiple DNS Servers, fast flux, all the good network engineering practices
- Collection Point
  - Server of some type, sometimes via e-mail drop-box
- Database

Phishing sites continue to proliferate



Methodologies of phishers changing - affecting reported site data - driven by:

- The success of browser blocking in IE and Firefox
- RockPhish
- Reports handling catching up with these changes

Phishing is a Global Problem

Top countries for hosting phish sites in July 2007

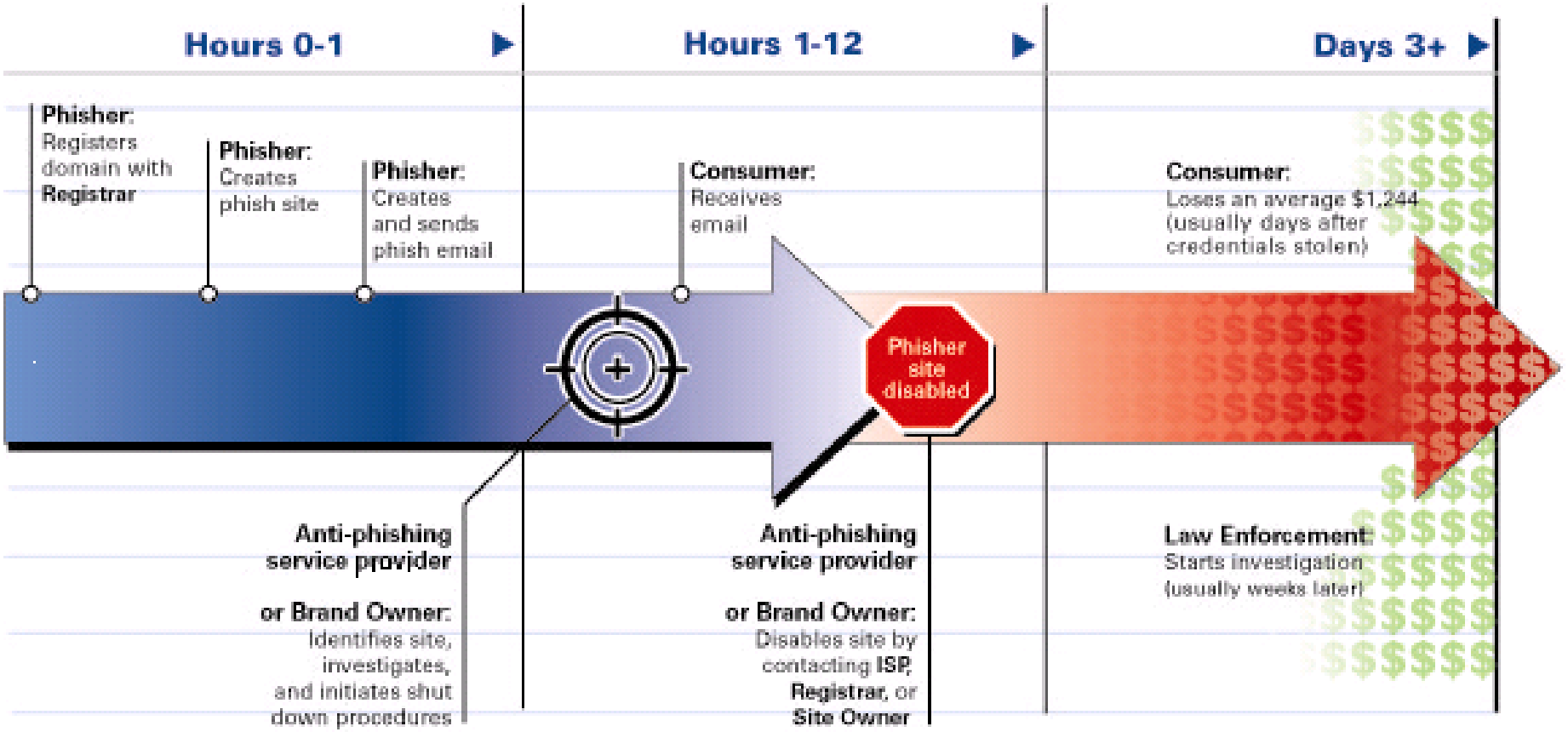
China and US in dead heat

First time ever US NOT #1

Impact of the Problem

- Organized International Criminal Activity
- $182 million **reported** losses in 2005 (FBI IC3)
- $105 billion estimated cybercrime impact in 2004 (US Treasury Department)
- Anecdotal evidence indicates a multi-billion $ problem
- Credential theft leading to other exploits on a large scale

Most Phish Sites Disabled within Hours
Usually NOT by law enforcement



APWG Successes

- Public Awareness and Education
- Facilitating collaboration and communication
- Phish Site URL Repository
  - Up several years; Everybody loves the statistics ☺
  - Submit URLs and a confidence factor to APWG
    - Every 5 minutes a new list of URLS to block is generated
    - Most big ISPs/Tools pull list to use in filters/blocking
    - Now includes DOMAIN NAMES registered for fraud

DNS Policy Working Group

- 45 members
- Participants include registries, registrars, CERTs, solution providers, ISPs, researchers, financial institutions, etc.
- Goal: Ensure that anti-phishing concerns are represented during the creation or modification of Internet policies
- Approach: collaborative and non-confrontational - deliver actionable data and constructive prescriptive advice to the communities that can best utilize it to improve our overall response to phishing

Initiatives of the DNS Policy Working Group

- Accelerated Domain Suspension by Registries
- ICANN WHOIS issues
- Registrar Best Practices
- Domain Tasting in Phishing
- “What to do if your site has been hacked by phishers”
- Collaboration with ICANN constituencies and SSAC

Accelerated Domain Suspension Plan for Registries: Key Points

- Some registries are considering adopting such a Plan
- APWG will create a Committee (or outsource a provider) that will accredit entities to submit Suspension Requests – upon approval from the APWG Steering Committee
- Helps mitigates risk to users from prolonged phish site uptime
- Hacked domains, and shared hosting environments are not eligible for suspension

Accelerated Domain Suspension Plan for Registries: Overview

To be defined by the APWG committee and Registry(s)

- Accredited interveners
- Authenticated communication
- Investigation & domain eligibility criteria
- Suspension request mechanism to registry
- Notice timeframe and requirements to registrar and ISPs
- Timeframe of registry suspension of DNS to eligible domain
- Appeal process
- Penalties for erroneous requests

Registrar Best Practices

- Goal: Provide **recommendations** to registrars to help them assist the anti-phishing community and make the Internet safer for all of us
- Focus:
  - Evidence preservation (help LE catch the criminals)
    - What is useful? How to preserve? Who to provide to?
  - Registrant screening tips to identify fraudsters proactively
  - Phishing domain takedown assistance

Registrar Best Practices (cont.)

- Understand the operational realities of the registrar business
- Can help registrars REDUCE costs:
  - Reduce fraudulent domain purchases/chargebacks
  - Reduce load on abuse departments
  - Limit potential legal liability
- Provide resources to help identify malicious activity

“What to do if your website has been hacked by phishers”

- Intended to be a quick reference guide
- Supported by resources on the APWG website
- Includes feedback from the wider APWG group
- Sample recommendations include:
  - Identification: notify your ISP
  - Containment: remove the unauthorized content
  - Recovery: restore your site from backup
  - Reporting: inform law enforcement
  - If you only do one thing: Ensure your applications are all up to date with the most recent patches and use hard to guess passwords

Current Phishing/Criminal Trends

- Global Impact - Statistics
- Fast Flux and ROCK phish
- Phishing targeting registrars
- Phishing targeting social networks and other non-financials
- Malware proliferation: keyloggers, address book heists, automated social engineering (STORM)
- Targeting of companies for customer intel

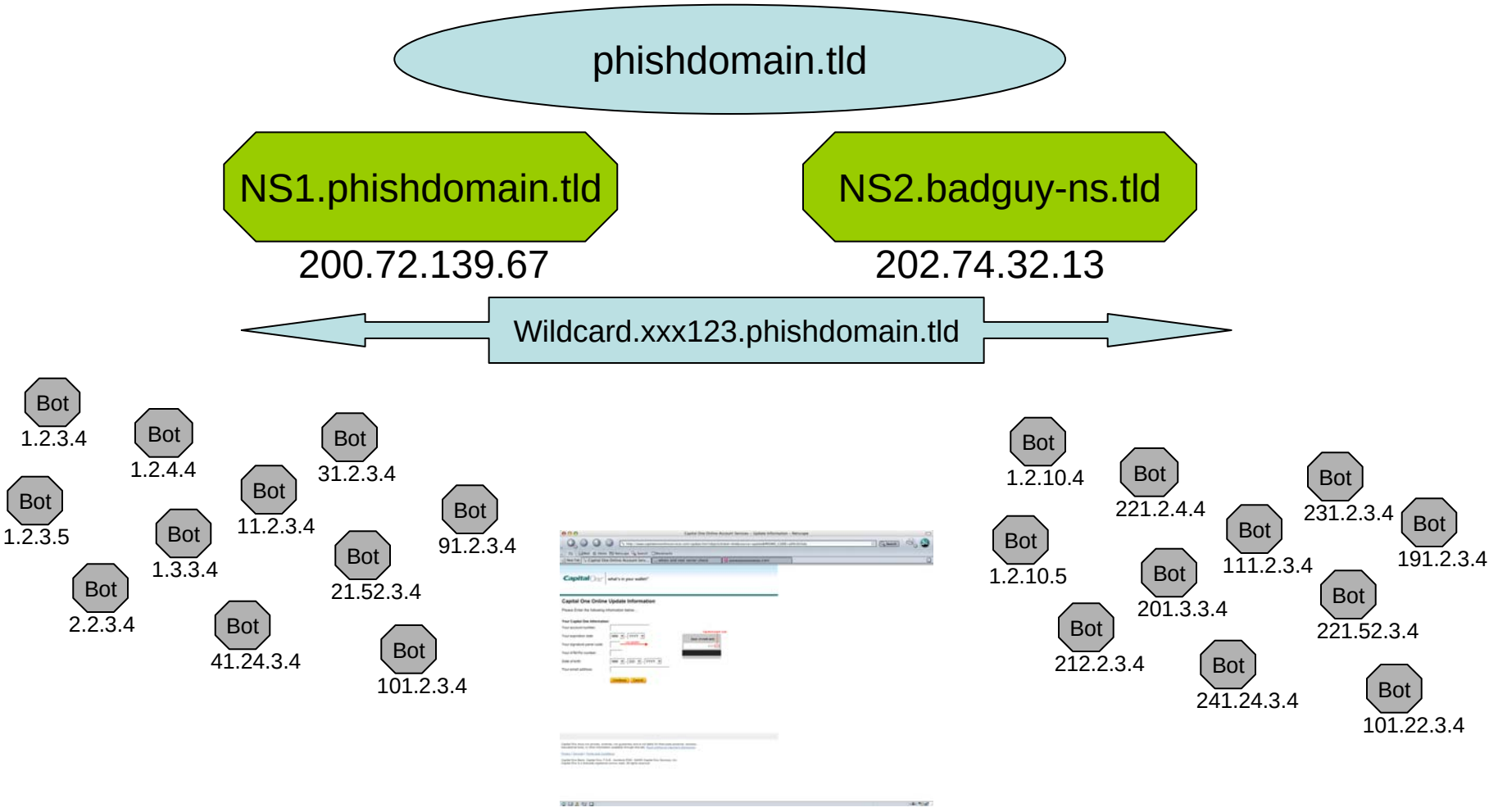
Implications for ccTLD Operators

- Large-scale abuse: effects on TLD reputation
- Credit Card Processing (direct sales model)
- Need for evidence preservation in all attacks
  - Especially against registry/registrars
- Integrity of user account credentials
- Targeting of your own executives and personnel

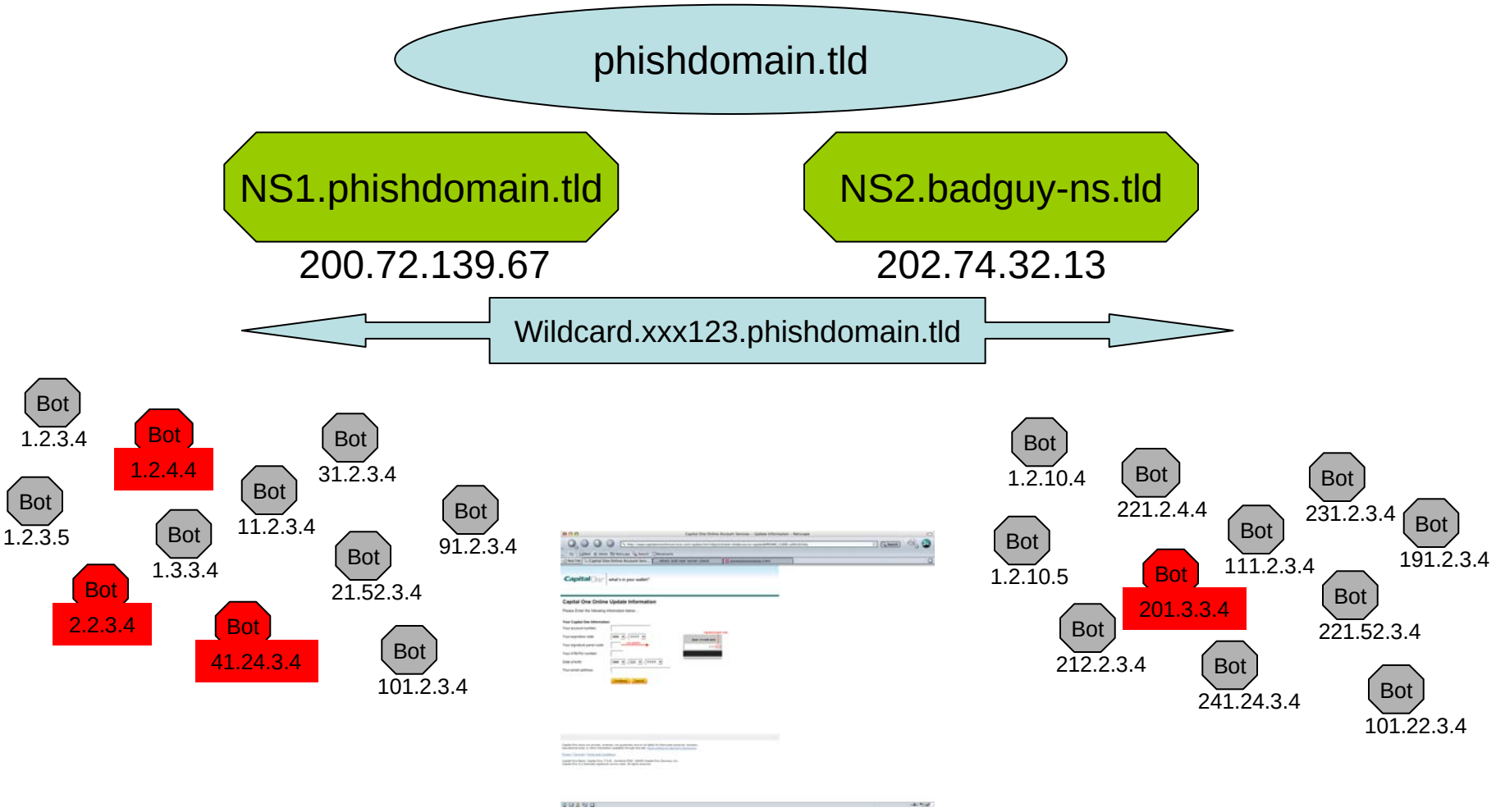
Fast-Flux and ROCK

- ROCK phish continues to be prolific (20-40% of lures)
  - Refining methods, constantly testing
  - Targeting wider - GoDaddy, Lexis/Nexis, Equifax
  - 20-40 domains per day - all registries - a dozen targets each
- Fast-Flux phishing rising rapidly
  - Large-scale use of botnets with rapidly changing IP addresses for site resolution
  - Systems are automated and resilient to loss of nodes
  - Domain shut-down only viable option
  - “Double Flux” being seen - rotating nameserver IPs
- Relatively easy for registries to detect
  - Processes needed for taking actual mitigation action
  - Sharing of data across registries/cc registries/ registrars?
    - Seems like a good idea - we’d be happy to help facilitate it!

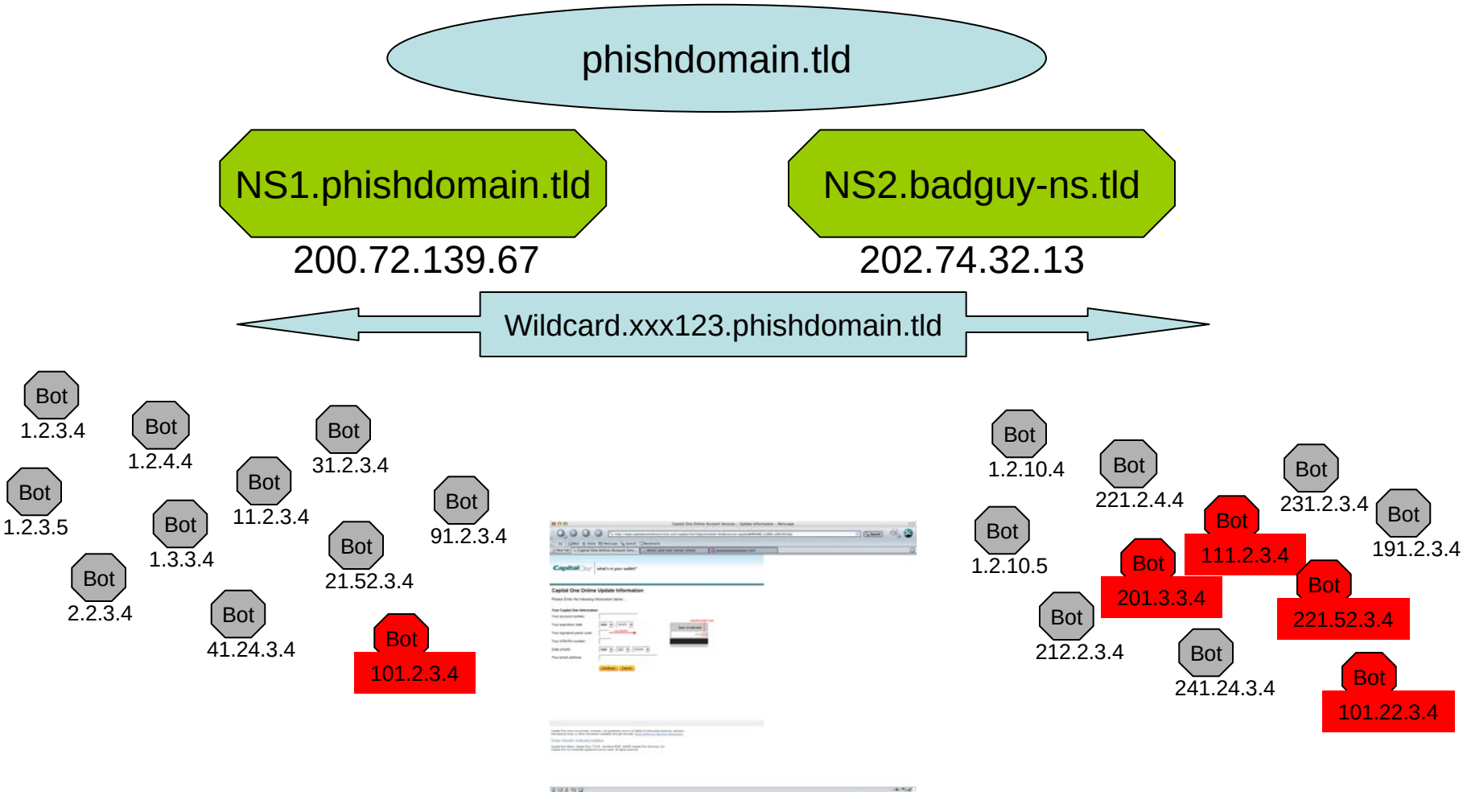
How Fast Flux Works



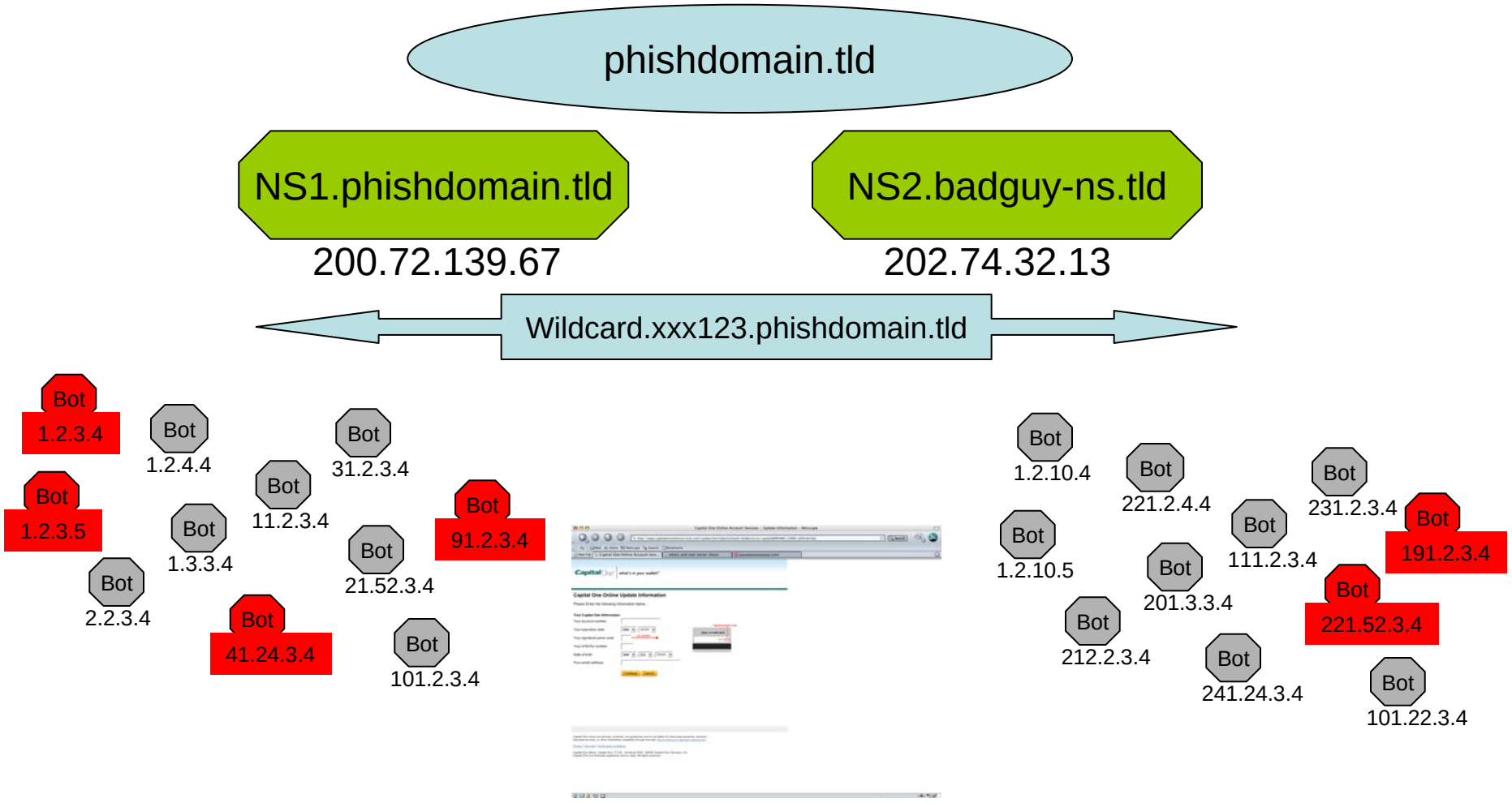
Fast Flux Example + 10min



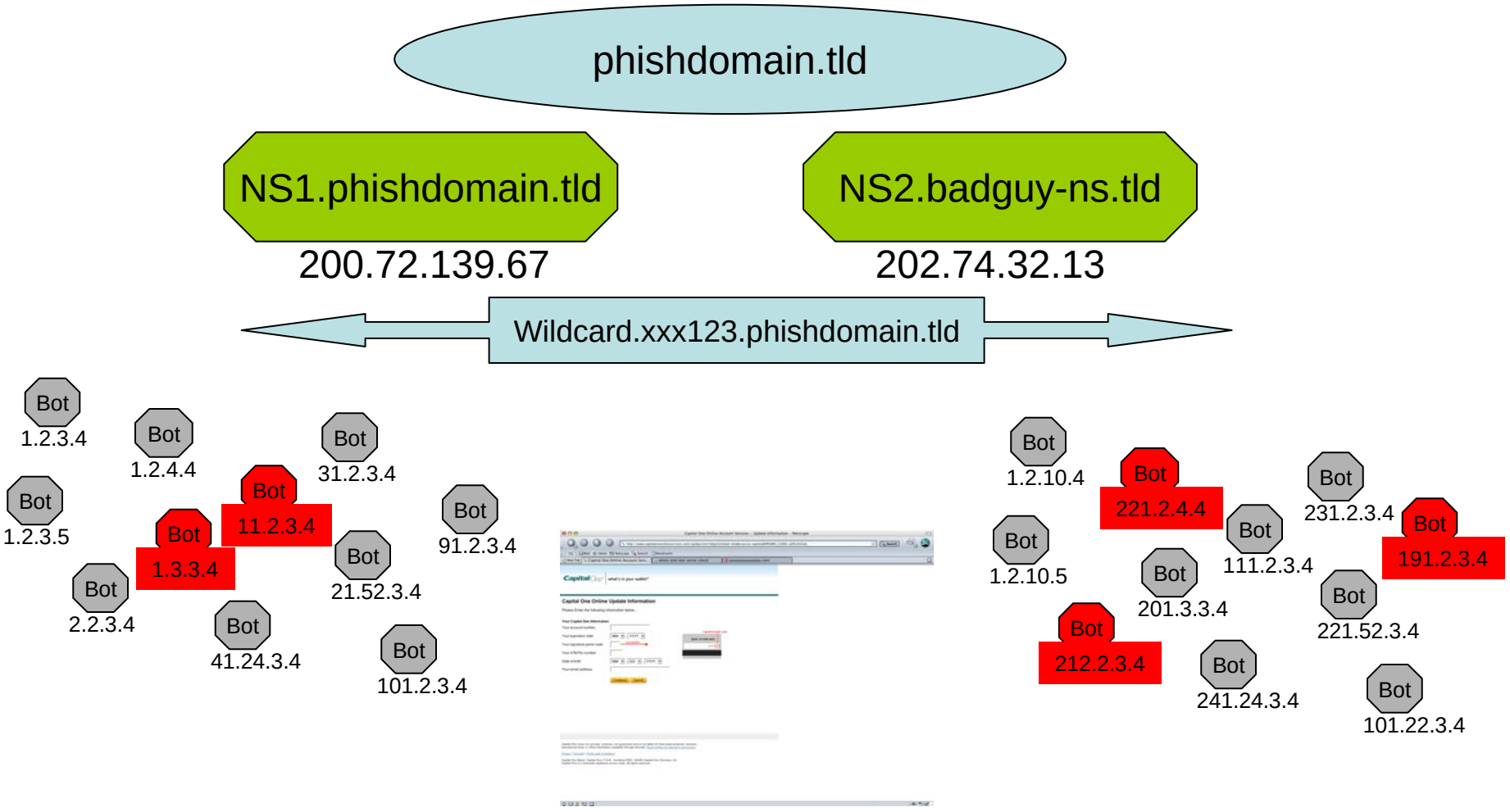
Fast Flux Example + 20min



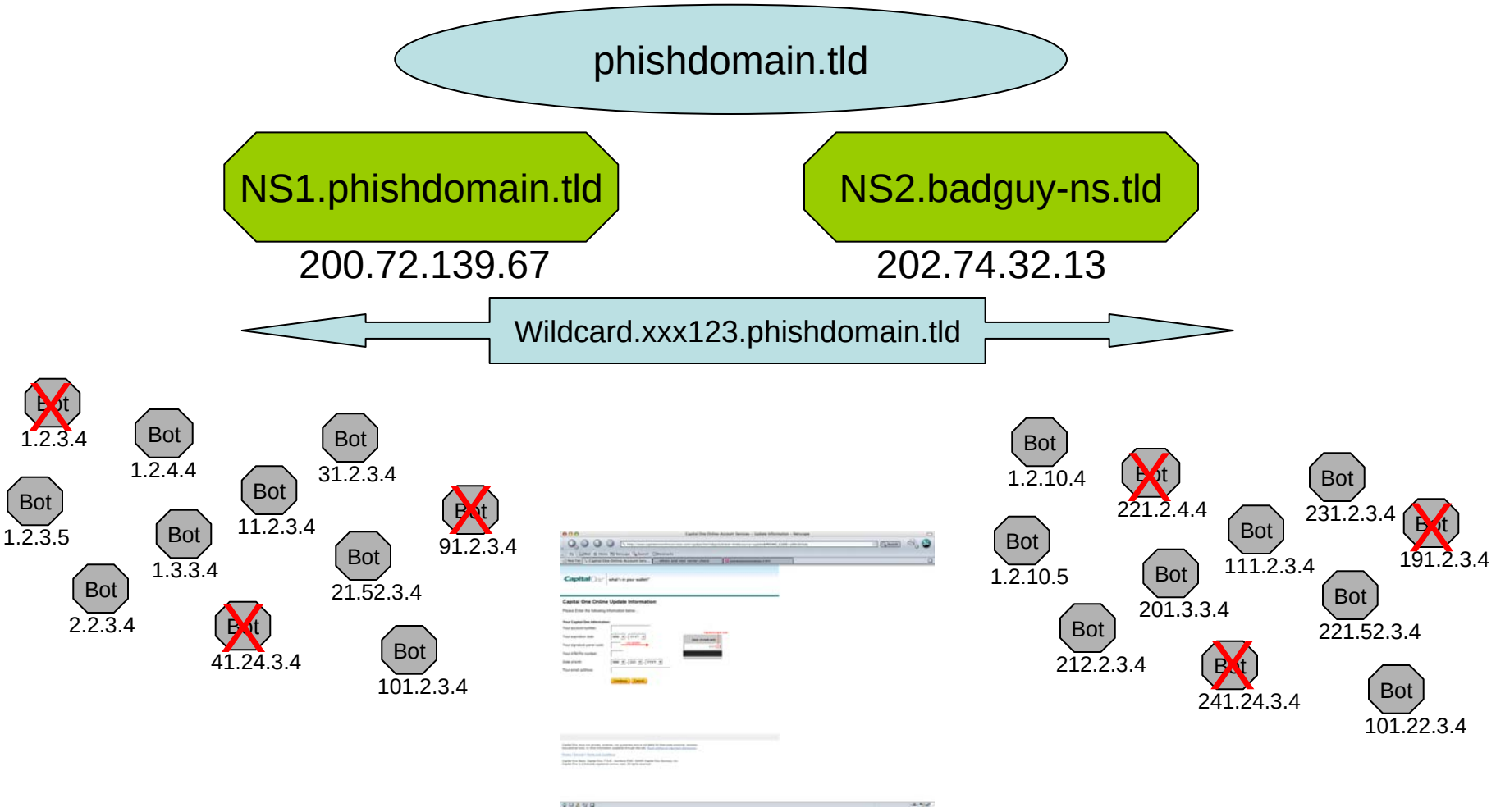
Fast Flux Example + 30min



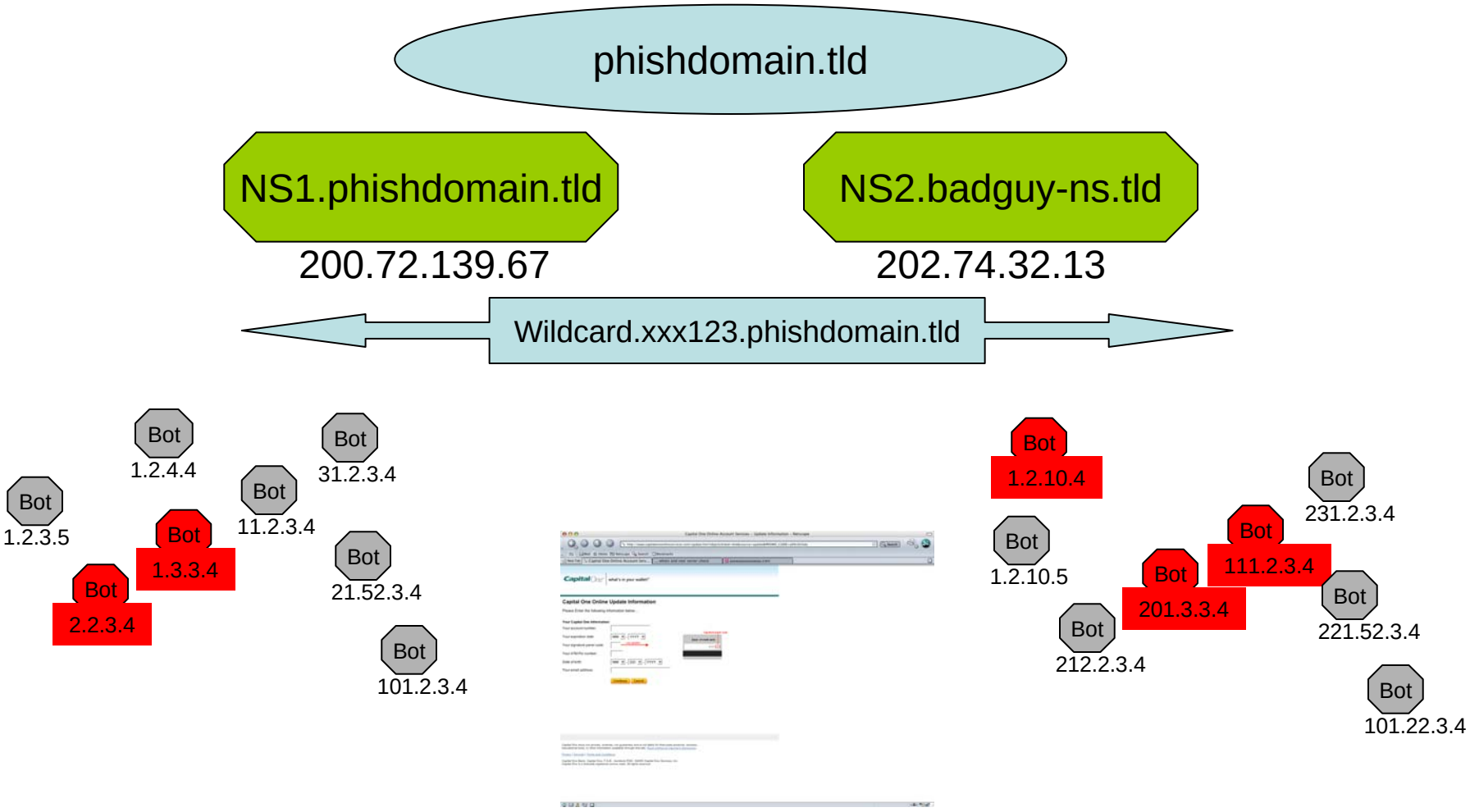
Fast Flux Example + 40min



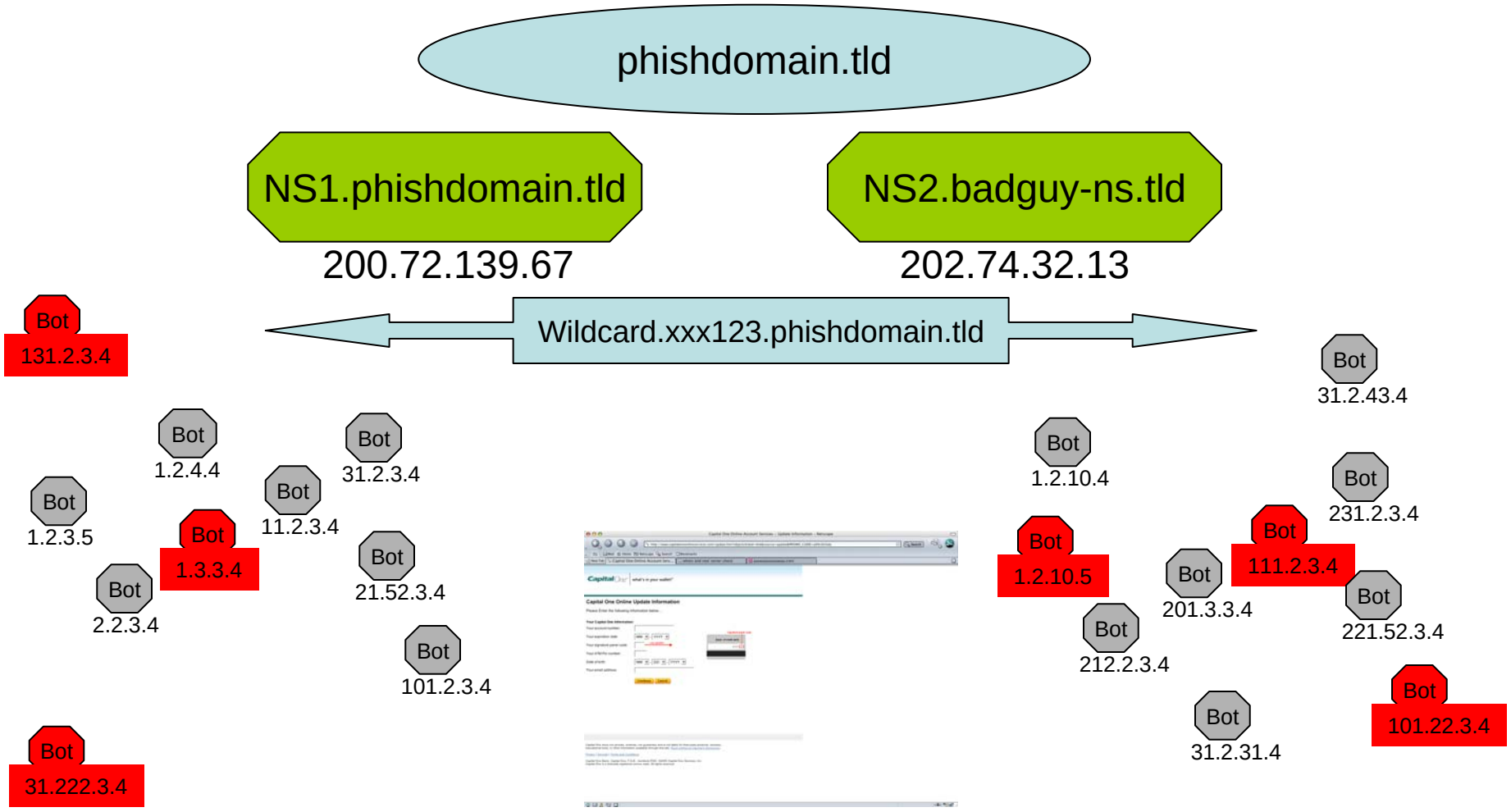
Killing Fast Flux - the WRONG way



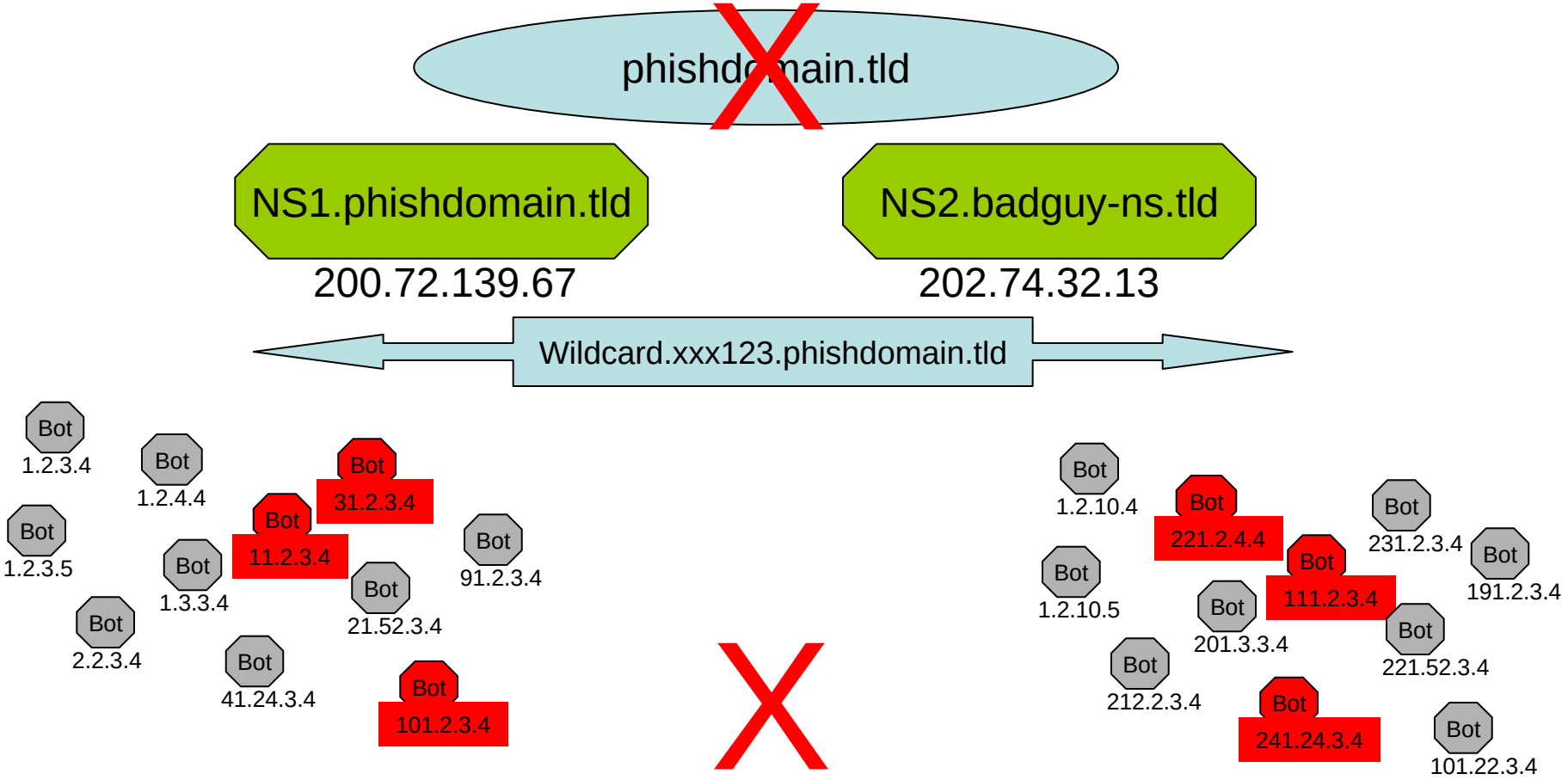
Killing Fast Flux - the WRONG way



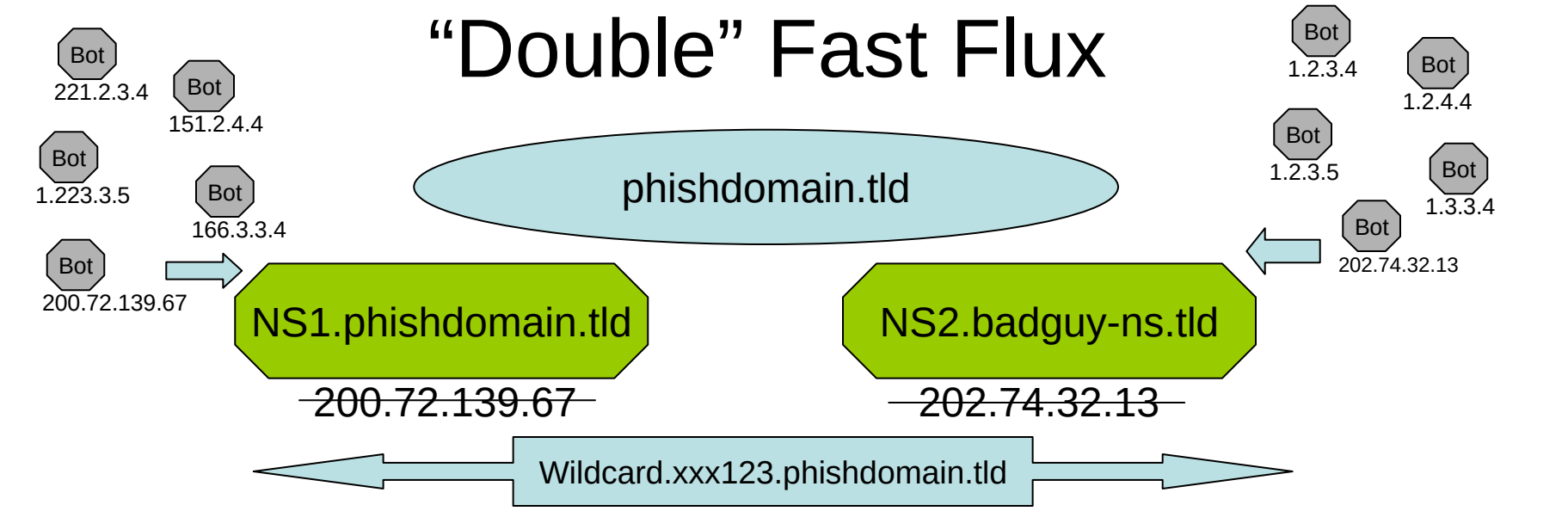
Killing Fast Flux - the WRONG way

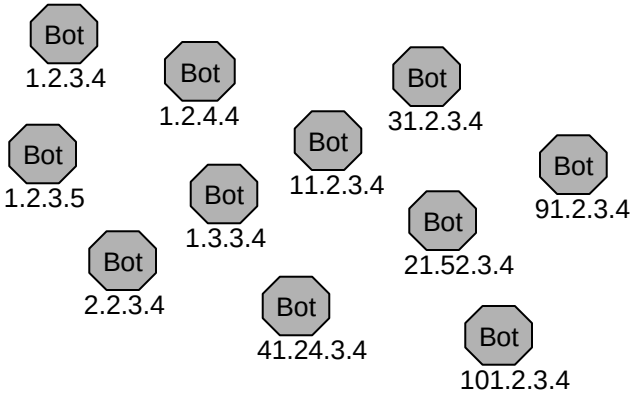


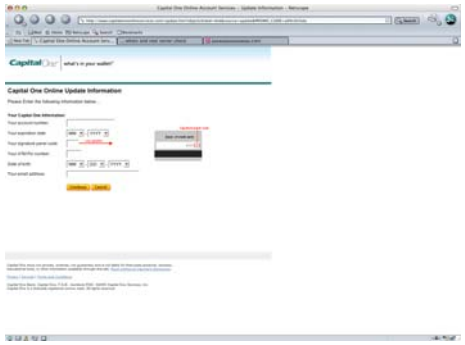
Killing Fast Flux - Permanently

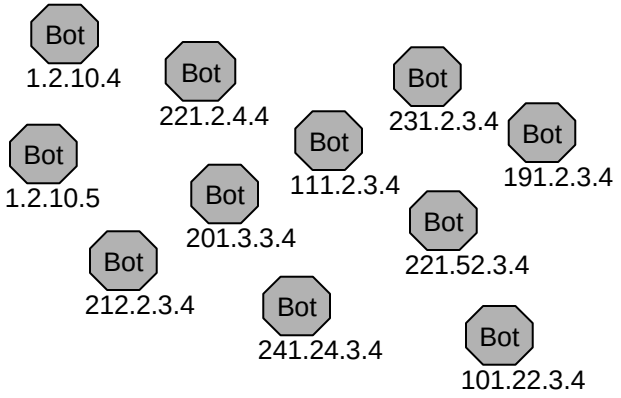


“Double” Fast Flux

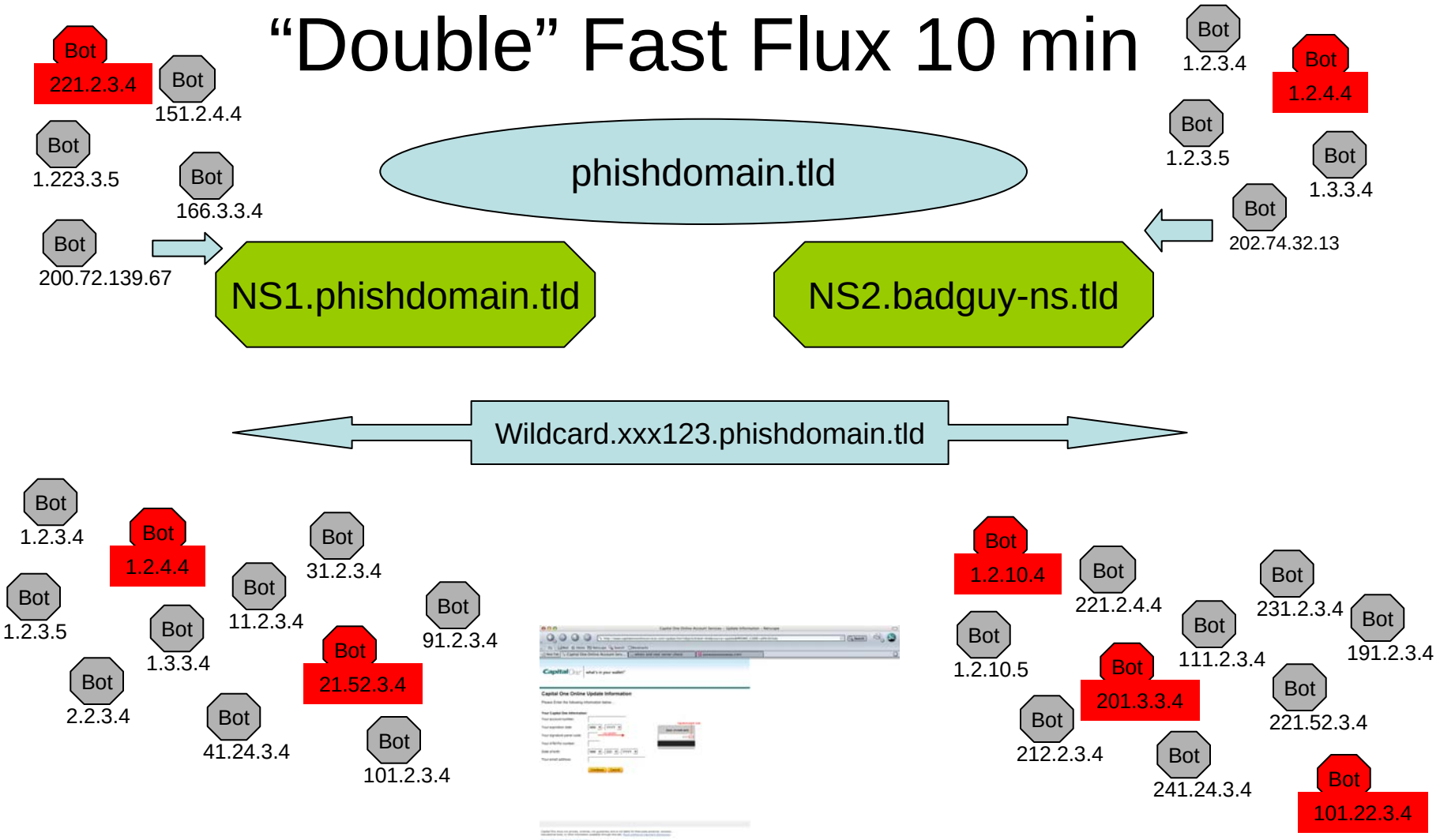




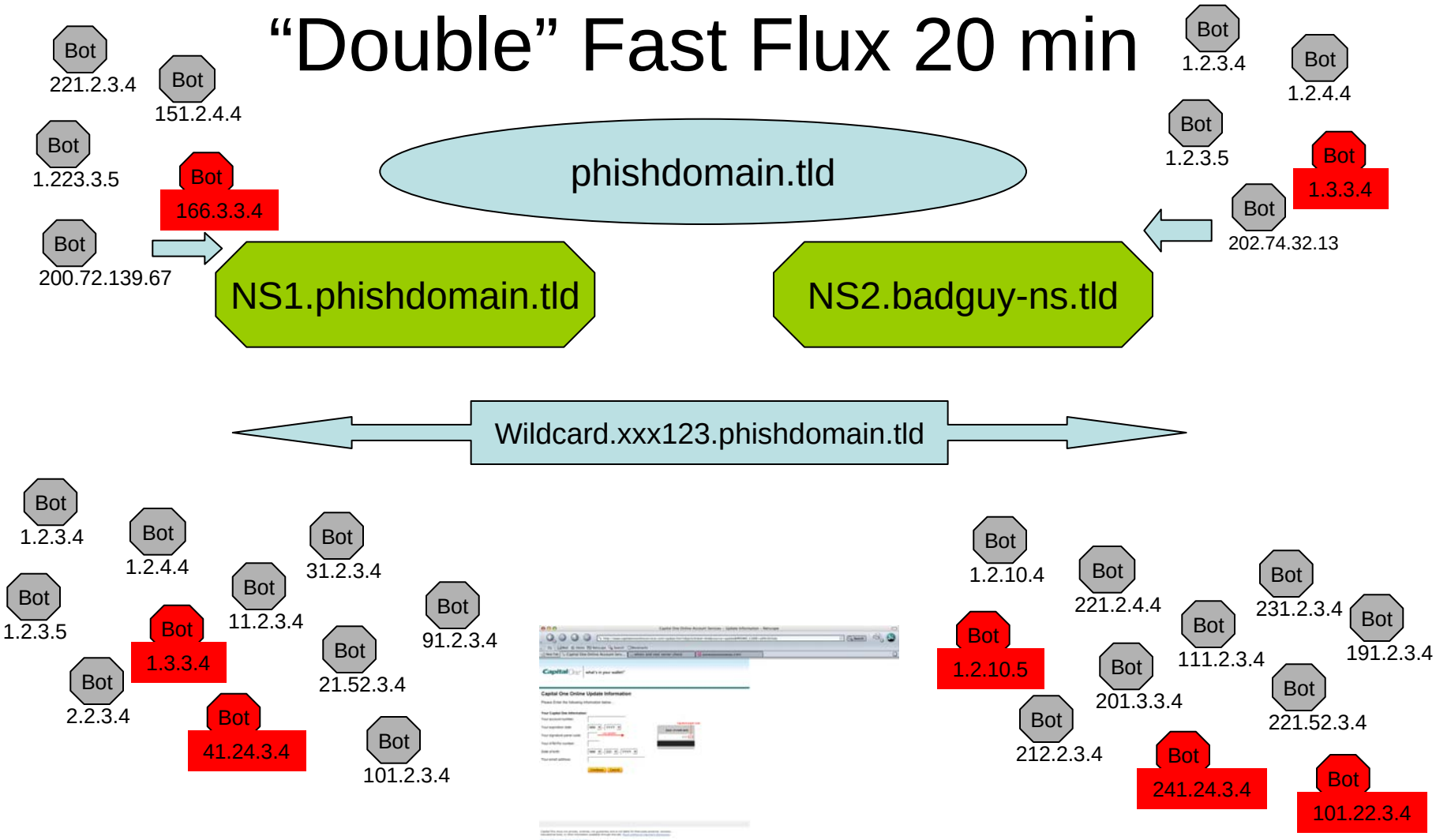




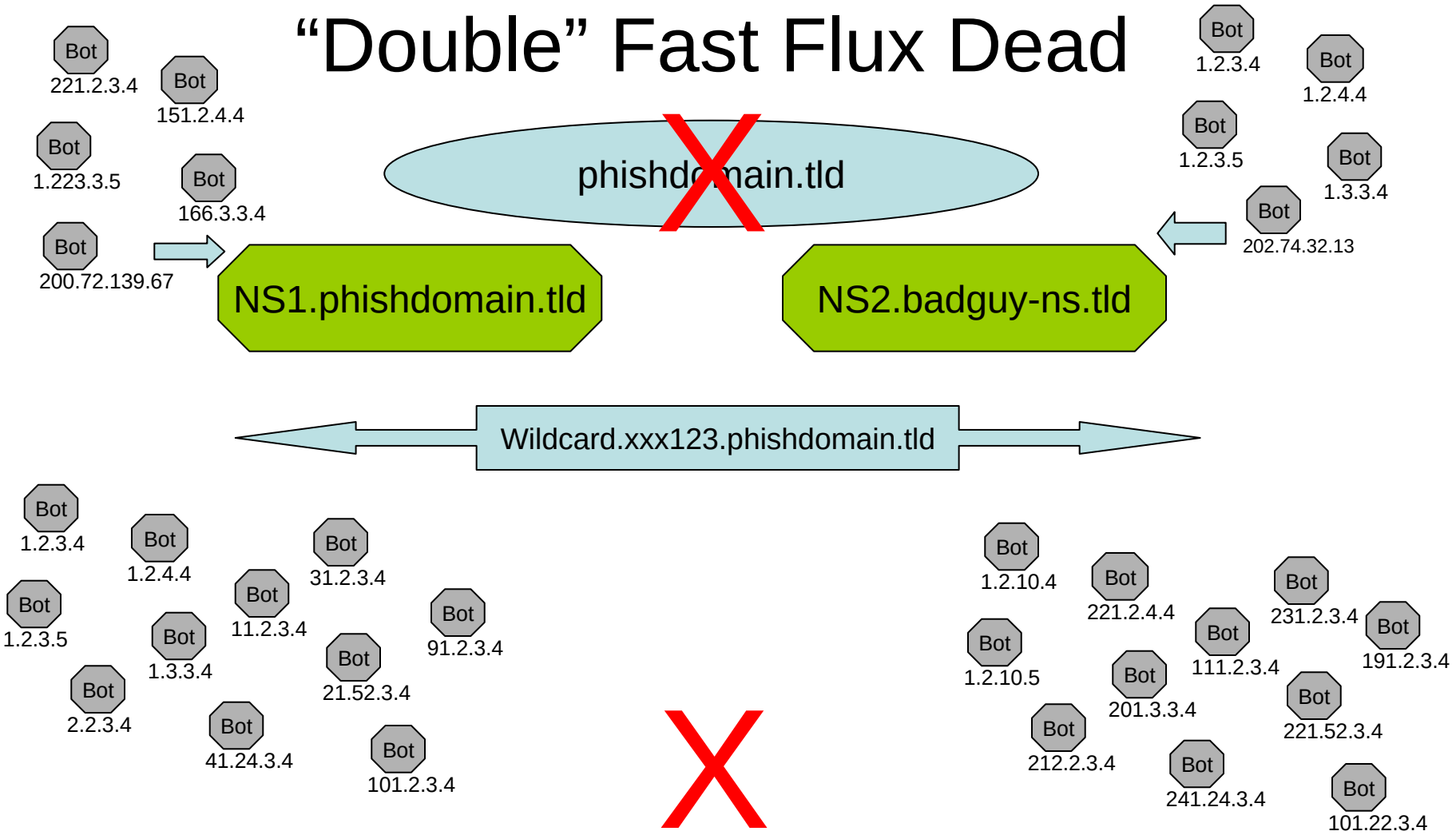
“Double” Fast Flux 10 min



“Double” Fast Flux 20 min



“Double” Fast Flux Dead



Detecting, Killing, Preventing

- DNS set-up the key
  - Nameservers
    - New nameservers on unusual domains/TLDs
    - DNS servers located on consumer netblocks
    - Flux changes to nameservers (double FastFlux)
  - Domain A Records
    - Fast Flux
    - Located on consumer netblocks
      - Move daily from one to another - around the glove
      - Multiple entries - worldwide
      - Can compare to known bad actors
    - Wildcard - all hosts resolve

  Monitor at DNS level

  Suspension plan when match found

  Verify issue and alert registrar

Reputation IS being used against specific TLDs - Today

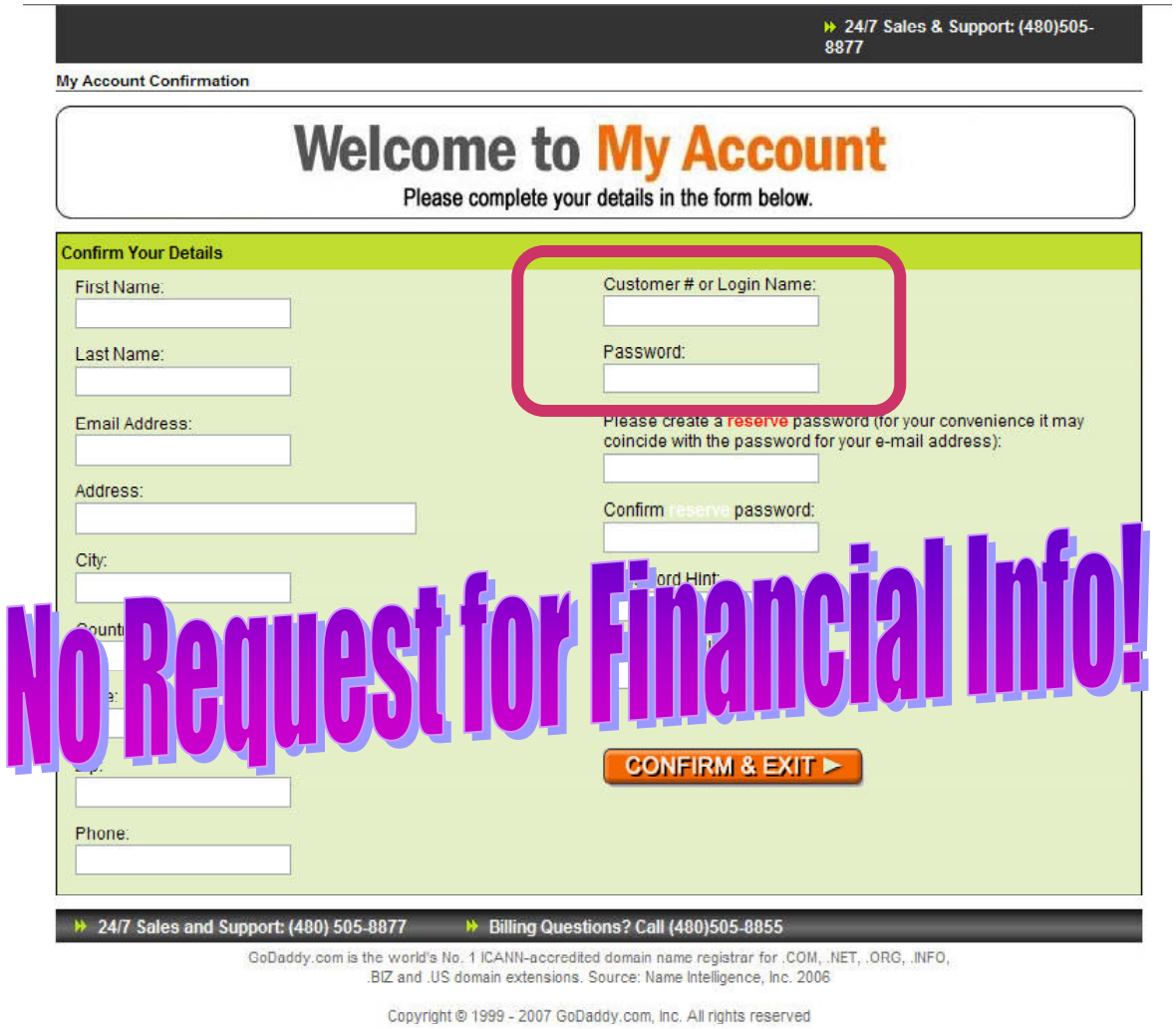
- Phishing and Malware the main issue
  - Overall spam load also a major factor
- Easy to track abuse issues by TLD
- Assumption - bad hygiene is TLD specific
- Directed actions (e.g. Spamhaus, IM services)
- Automated scoring systems
  - Anti-Spam systems vendors
  - A/V software
  - ISPs
  - Hosting providers

Further impacts of these trends

- Credit Card merchant fees raised
- Support impact
  - Complaint handling
    - General public - large numbers of random e-mails
    - Anti-phishing/anti-abuse SIRTs
  - Dealing with fraud domains in the DNS
  - Handling bogus nameservers - not even on radar
- Law enforcement involvement in your business
  - Dealing with subpeonas and legal process
  - Evidence preservation requirements

Phishing of Registrars/Registries

- August 2007: Rock Phish Gang attacked GoDaddy
  - NO attempt to get financial details, this was strictly an attack to get account access by targeting customers
  - Spam volumes show both “mass” attack and targeted attacks
    - Possible use of some whois information to target phishing
    - Possible use of “smart” targeting within domains (e.g. domain.admin@domain, support@domain, admin@domain)
- So far, no overt activity, but there are many important implications for operators of domain registration systems
- Many details are too sensitive for public meetings
  - We are happy to provide private briefings to registry operators
  - Consider yourselves a target of organized crime - update your procedures, systems and security accordingly


24/7 Sales & Support: (480)505-8877
My Account Confirmation
Welcome to My Account
Please complete your details in the form below.
Confirm Your Details
First Name:
Last Name:
Email Address:
Address:
City:
Phone:
Customer # or Login Name:
Password:
Please create a reserve password (for your convenience it may coincide with the password for your e-mail address):
Confirm reserve password:
CONFIRM & EXIT
No Request for Financial Info!
24/7 Sales and Support: (480) 505-8877
Billing Questions? Call (480)505-8855
GoDaddy.com is the world's No. 1 ICANN-accredited domain name registrar for .COM, .NET, .ORG, .INFO, .BIZ and .US domain extensions. Source: Name Intelligence, Inc. 2006
Copyright © 1999 - 2007 GoDaddy.com, Inc. All rights reserved

Phishing Hitting Social Networks

- MySpace example
  - One year ago - Zero phish
  - More than 2,000 since then
  - Currently over 5 per day
- Capturing login credentials and associations to other people/affinities/companies
  - Use for spamming/spear phishing
  - Logins can be re-used by many for other services
    - People are generally poor with password practices
- Implication for registrars/registries
  - You need to assume that the USER/PASSWORDs for many of your customers (registrants) are COMPROMISED!

Malware proliferation

- Change in emphasis - now Crimeware
  - Organized crime with specialists creating sophisticated attacks
  - Open up computers to become zombies
  - Install keyloggers and scans for user/pass information
  - Capturing and using address books
    - Direct targets for sophisticated social engineering
    - Going after “whales” - people with high-value assets
- Implication for registrars/registries
  - You need to assume that the USER/PASSWORDs for many of your customers (registrants) are COMPROMISED!
  - What about compromises of your registrars or their resellers?
  - High compromise value individuals (e.g. domain administrators) may be targeted in particular

Targeting of Businesses for Data

- Major phishing and malware gangs now targeting companies with vast stores of sensitive information
  - Attacks are looking for database access credentials
  - NOT targeting financial institutions
  - Particularly looking for executive staff data and HR access
- Rapidly growing phishing activity over past 6 months
  - Business data: Lexis/Nexis, Salesforce.com
  - Employment data (HR acct): Monster.com, CareerBuilder.com
  - Credit Bureaus (business access): Equifax
- Wide swath of major financials also targeted directly
  - Malware and/or phish targeted to executives
  - Disguised as important agencies (IRS, FTC, BBB, EEOC)
- Registry and Registrar staff are potential targets

Mitigation Suggestions

- Know your customers and what they're doing!
  - Front-end security on transactions
    - CC companies will help you - they are targets too
  - Thorough vetting of applications (registrar and registrant)
  - Do you know who the Russian Business Network is?
    - http://en.wikipedia.org/wiki/Russian_Business_Network
    - http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html
- Watch for suspicious behavior
  - Fast flux, odd-ball nameservers
  - Flag, investigate, process suspensions direct or via registrars
- Be prepared to react
  - Have staffing or partner on-hand 24X7
  - Preserve evidence
  - Update your agreements to allow flexibility for shut-down, registrar requirements for abuse handling

Primary Take-Aways

- Bad guys know how to use DNS and domains
  - Sophisticated campaigns to find “weakest link”
  - Will abuse your systems relentlessly until you respond
- Unchecked abuse will hurt TLD reputation and (for some) CC processing fees - YOUR bottom line
- You must assume a significant portion of your customers’ accounts will be compromised
- Quick reaction and intel are necessary - organized crime is behind a lot of these trends
- Evidence preservation important to implement

APWG Contacts

- Website: http://www.antiphishing.org
- Phish Site Reporting: reportphishing@antiphishing.org
- Membership: membership@antiphishing.org

Thank You!

Anti-Phishing Working Group

www.antiphishing.org

Phishing - Current Status and Mitigation Advice

Presentation for ccNSO Meeting

ICANN - Los Angeles
October 31, 2007

Rod Rasmussen
Rod.Rasmussen@internetidentity.com
+1.253-590-4100