

# Case studies in global criminal attacks: McColo & CheckFreea

Rod Rasmussen, President & CTO Internet Identity, APWG Industry Liaison

E-Crime and Abuse of the DNS Forum:

Session 2. Criminal Attacks & Abuse Response Today

March 4, 2009



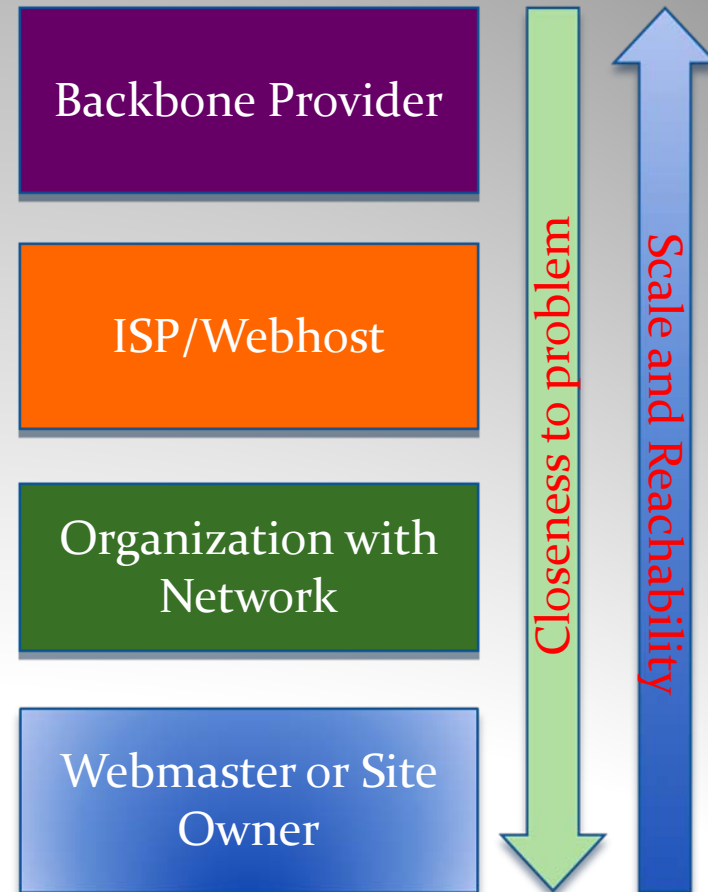
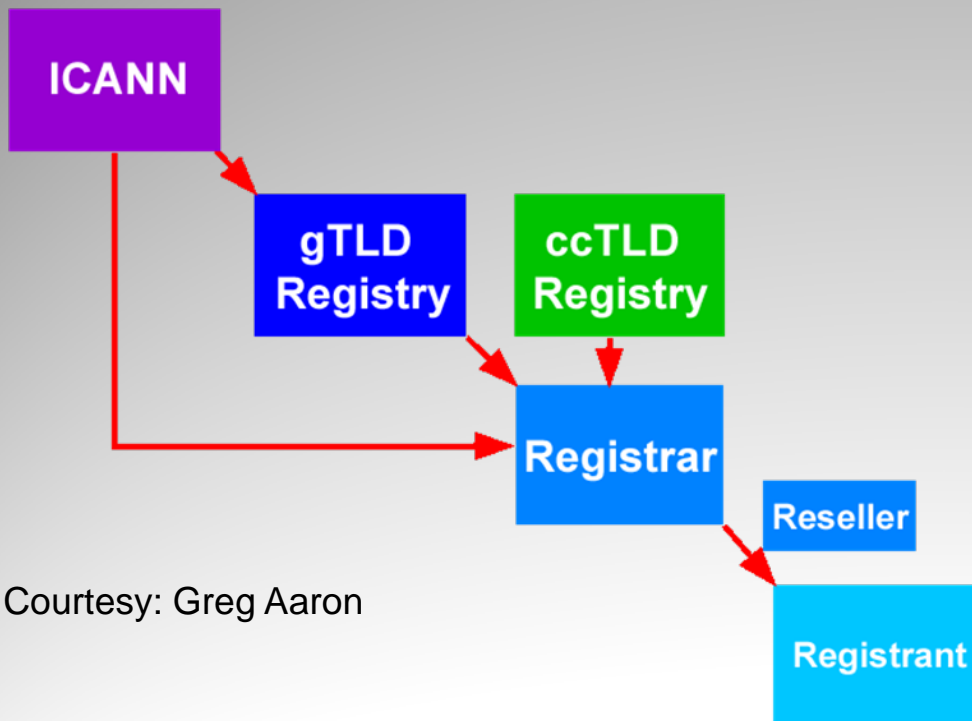
# Overview

- Intro
- Summary of CheckFree attack
- Analysis of CheckFree attack
- History of McColo and its demise
- Battling the Srizbi botnet

# First Responder Viewpoint

- My company provides mitigation services for organizations victimized by on-line fraud and e-crime
- This is largely a private sector activity – law enforcement does not shutter abuse directly as a rule
- Must work with community and find the right people to shut down criminal websites/domains/e-mail/bots
- Must determine type of fraud site
  - Hacked machine
  - Bogus webhosting account (stolen credit card used)
  - Bogus domain registered to use botnet

# Internet Ecosystem



Courtesy: Greg Aaron

# Who is CheckFree?

- Largest provider of on-line billpay services in the U.S.
  - 1.4 billion transactions handled annually (160K/hr)
  - Process over 75% of all ACH transactions in U.S.
- Serve 22 of top 25 U.S. Financial Institutions
- Direct integration with thousands of payment websites
  - Banks, CU's, utilities, e-commerce companies

# Attack Summary

- What the attacker did:
  - took control of several CheckFree domain names via their domain management account
  - changed authoritative DNS for domains
  - pointed all hostnames to malware server in Ukraine

# Attack Summary

- Result:
  - CheckFree visitors redirected to malware site
    - All visitors to CheckFree domain names
    - Billpay customers of client FI's (from THEIR sites)
  - Some customers directly infected
  - Most customers blocked from using billpay services

# Attack Summary

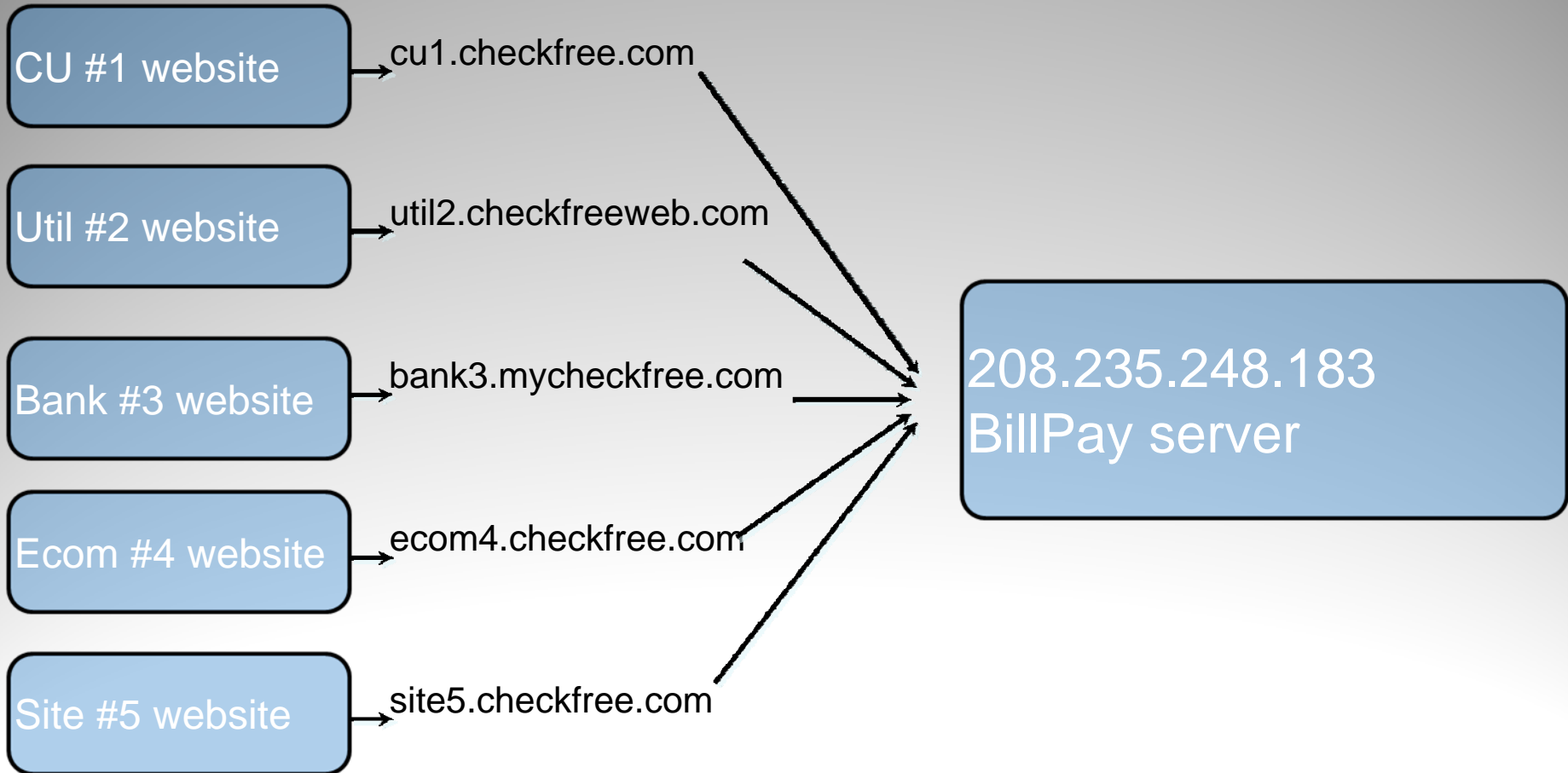
- CheckFree regained control of domains after about 8 hours
- Persistent nature of DNS caused attack effects to linger for 48 hours longer
- Impact was far reaching
  - Numerous Credit Unions and banks shut down Bill Pay services for a day or longer
  - Tens of thousands of individuals exposed to potential malware infection



# The CheckFree Infrastructure

- Uses Domain Name Service (DNS) to its advantage
  - Sample paradigm: FI\_NAME.checkfree.com
    - Strength: Easy to set up new customers
    - Strength: Can load balance and rearrange IP addresses without customers needing to know
    - Weakness: DNS must remain reliably controlled

# Accessing the BillPay Server



# Accessing the BillPay Server

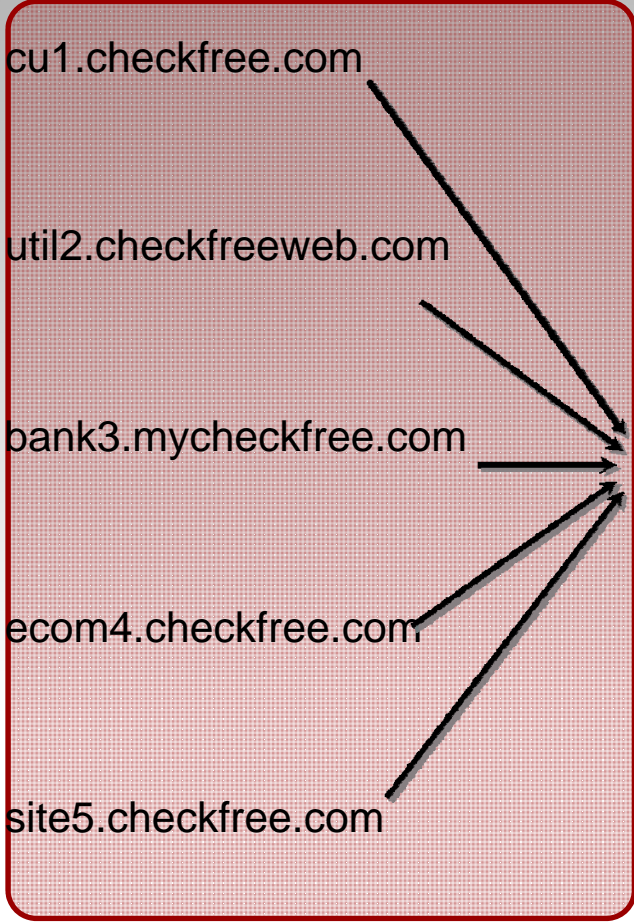
CU #1 website

Util #2 website

Bank #3 website

Ecom #4 website

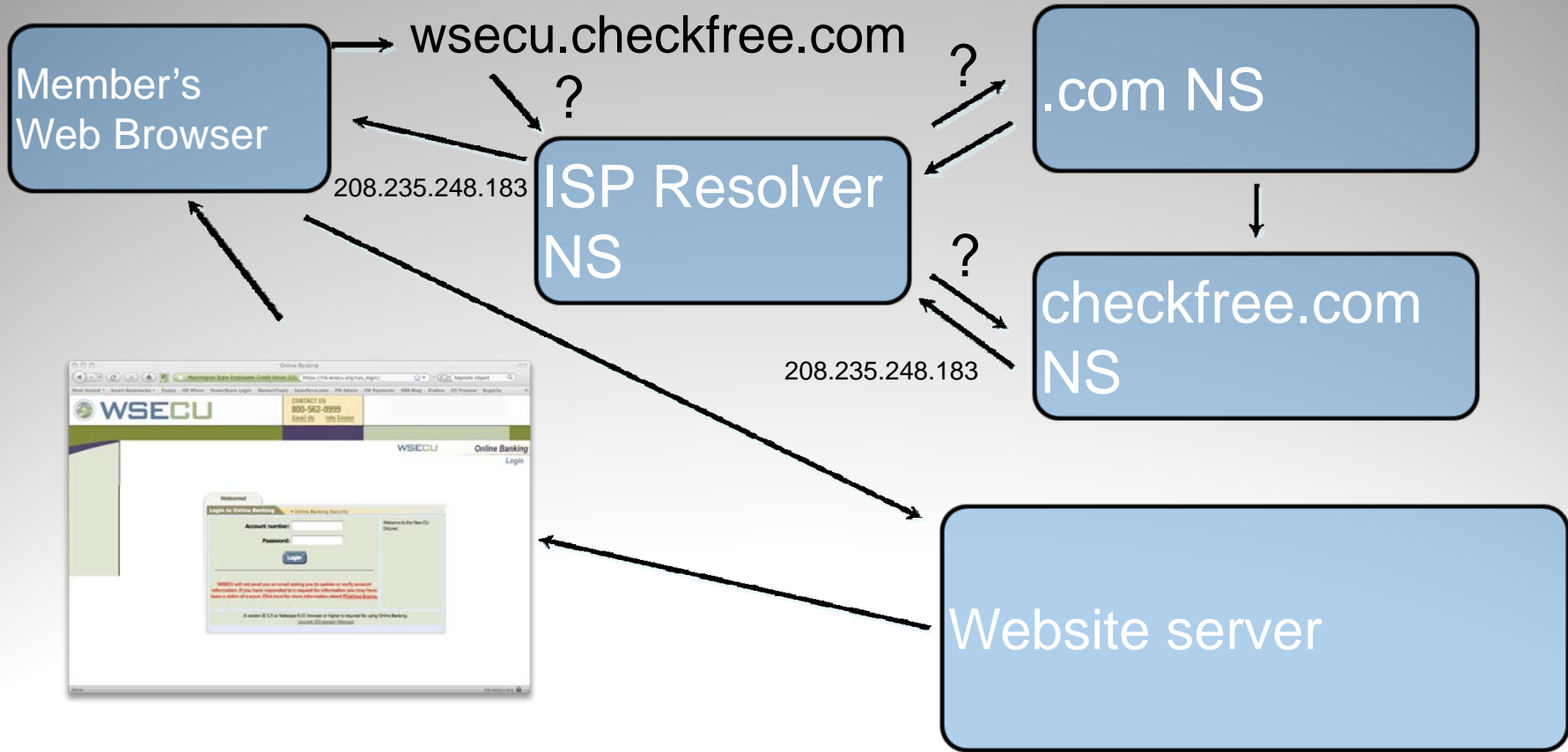
Site #5 website



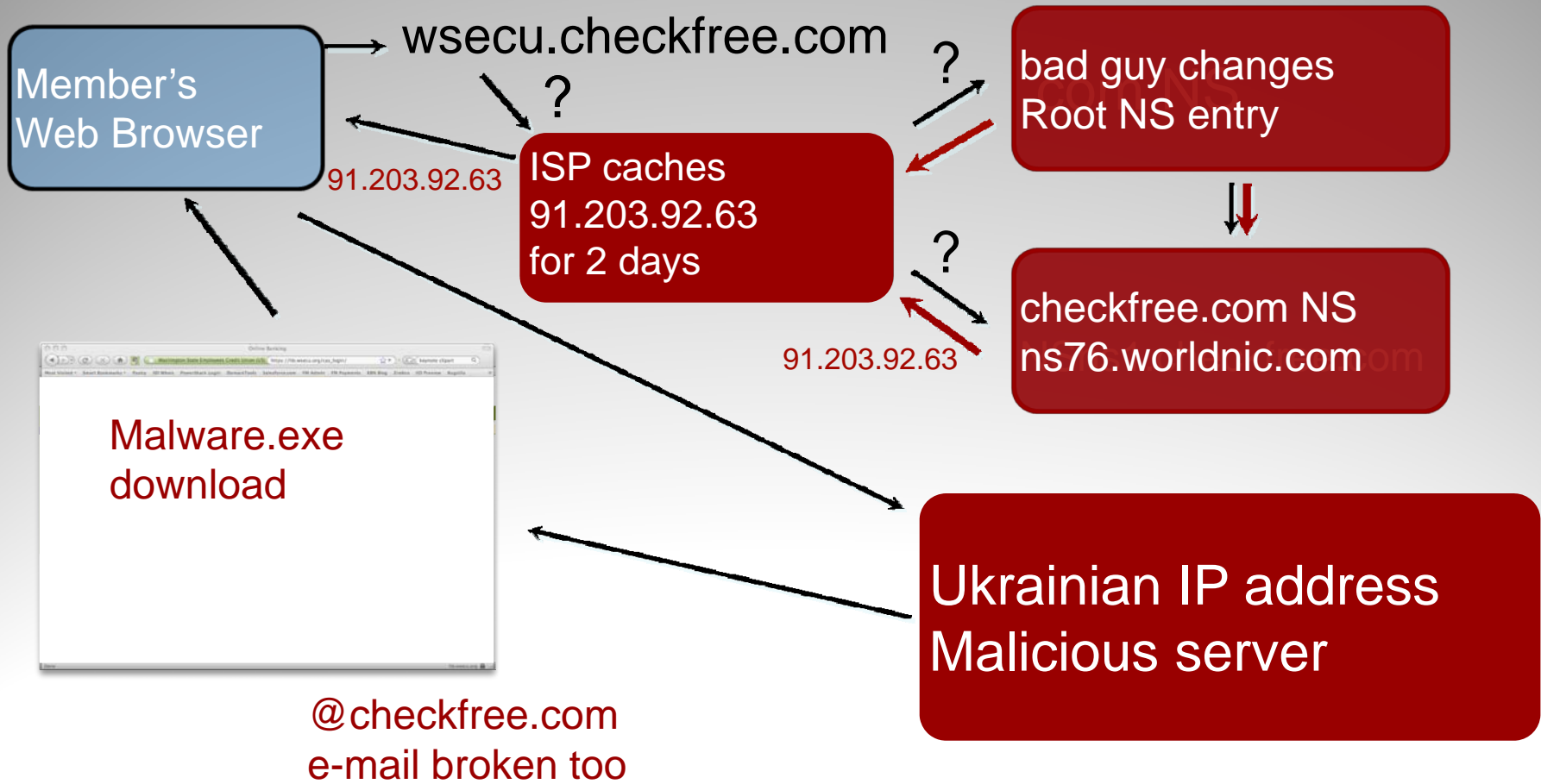
Weakness: Reliance on accurate DNS records

208.235.248.183  
BillPay server

# Normal DNS Resolution



# CheckFree attack attack



# Attack Summary - Step 1

- Attacker took control of several CheckFree domains
  - by breaking into the password protected domain management account at Network Solutions
  - obtained the password by phishing or malware
    - Network Solutions customers phished 6 weeks before
    - keylogger software could easily steal this info

# Attack Summary - Steps 2 & 3

- Attacker changed authoritative DNS for domains
  - Name servers changed to Network Solutions' free Name Server service on ns##.worldnic.com
- Attacker pointed "A" records for all hostnames to malware server in Ukraine
  - Used Network Solutions' free DNS tools



# CheckFree's response

- Actually very good – responsive and thorough
- CheckFree regained control of DNS in about 8 hours
  - Had to work with registrar - CheckWho?
  - process was complicated due to admin e-mail address defined under checkfree.com domain - no verification via e-mail possible
- But...
  - the attacker set the TTL for the bad DNS to 48 hours
  - the bad DNS settings were in use for up to 56 hours depending upon ISP



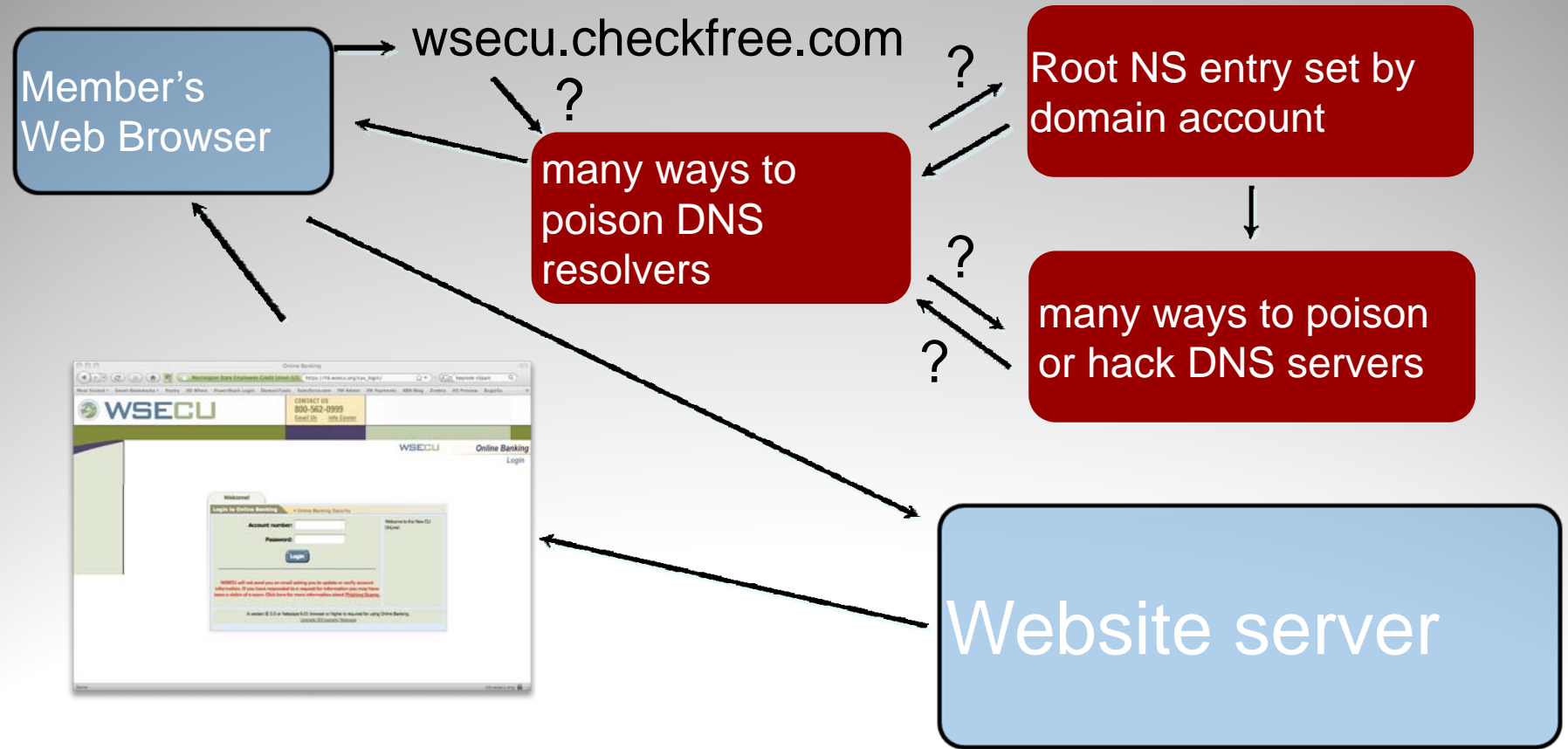
# Attack Motivation

- Attack appeared related to phishing attacks six weeks prior that targeted Network Solutions and eNom
- Dozens of domains from those registrars were also compromised and pointed to the Ukrainian malware server at exact same time
- Motivation appears to have been malware distribution - not disruption of a majority of the U.S. online bill pay systems!

# How TTL prolongs attack

- TTL tells resolving DNS servers how long to keep IP address
- ISPs run these for most users
- Can't update from outside
  - ISP must refresh cache of one or all domains
  - No standard process for doing this available
- By the way, customers' machines cache DNS data too...

# DNS Vulnerabilities



# Lessons learned

- Entire online infrastructures rely on the DNS to work
  - and the DNS is vulnerable to attack
- Domain name registrations are vulnerable
  - DNS can be compromised via the registrar account
- System-to-system hand-offs should be verified every time
  - just in case a rogue system has taken over

# McColo & Srizbi

Many thanks to Brian Krebs ([washingtonpost.com](http://washingtonpost.com))

Alex Lanstein@ ([fireeye.com](http://fireeye.com))

A host of security researchers everywhere

# What is (was) McColo?

- Mid-level size webhosting provider
- US Based (San Jose, California)
- Offered typical range of hosting services
- Looked pretty normal at first glance
- However...
- A favorite haunt of ESTDomains
- IPs on lots of black lists
- A top area of “study” for security researchers



# McColo: E-crime Central

Ambien-plus.com Canadianpharmacorp1.com  
 Canadianpharmacorp10.com Canadianpharmacorp2.com  
 Canadianpharmacorp3.com Canadianpharmacorp4.com  
 Canadianpharmacorp5.com Canadianpharmacorp6.com  
 Canadianpharmacorp7.com Canadianpharmacorp8.com  
 Canadianpharmacorp9.com Onlinepharmacysolutions-a.com  
 Onlinepharmacysolutions-b.com Onlinepharmacysolutions-c.com  
 Onlinepharmacysolutions-d.com Rxclubdiscount.net Rxclubdiscount.org  
 Valium-plus.com Xanax-plus.com 5-easysteps.com Ambienplus.com  
 Onlinepharmacyltd-a.com Onlinepharmacyltd-c.com  
 Onlinepharmacyltd-n.com Onlinepharmacyltd-q.com  
 Onlinepharmacyltd-x.com Onlinepharmacyltd-y.com  
 Onlinepharmacyltd-z.com Rx-club.biz Rxclub.biz Rxdiscountcenter.biz  
 Valiumplus.com Vanebol.com Cam2girl.net My-support-area.com  
 My-support-central.com My-support-city.com My-support-clients.com  
 My-support-home.com My-support-house.com My-support-manager.com  
 My-support-page.com My-support-pharmacy.com My-support-place.com  
 My-support-system.com My-support-ticket.com P0llko.com  
 High-quality-viagra.com Online-pills-shop.com Belovedpills.com  
 Choiceforonline.com Desiredmeds.com Easilygenerics.com  
 Easilymeds2.com Mybestdrug.com Openpills.com Pay4pills.com  
 Pills-pay.com Pills24.biz Rxmania.biz Rxmania.com Topqualitymeds.com

### Pharna Domains

→ **McColo, AS26780**

208.72.169.100 defendyourpc .com  
 mycupupdate .com  
 secureupdatecenter .com  
 secureupdateserver .com  
 webscannertools .com  
 secureyourpayments .com

### Rogue Security Software

208.72.168.84  
 ietoolsupdate .com  
 iexplorefile .com

208.72.169.56 Control server for Torpig/Sinowal Rootkit/Keylogger  
 Responsible for stealing 500k bank, credit accounts over 2.5 years

### Child Pornography Web sites

### Botnet Controllers

- Srizbi
  - 208.66.195.172
  - 208.72.168.144
  - 208.72.169.110
  - 208.72.169.2
  - 208.72.168.85
  - 208.72.169.212
- Rustock
  - 208.72.169.54
  - 208.72.169.55
  - 208.66.194.2
  - 208.66.194.14
- Mega-D/Ozdock 208.69.32.132
- Pushdo/Cutwail
  - 208.66.194.232
  - 208.66.194.240
  - 208.66.195.15
  - 208.66.195.71
- Warezov 208.72.169.2
- Asprox 208.69.32.132
  - tray62 .tw
  - encode1 .name
  - 4client .mobi
  - 4client .jp

### Pharmacy Payment Sites

- GSpay.com (Pharmacy)
- Avalonpay.com
- Pills-pay.com
- Pay4pills.com

### Proxy/Anonymization Services

- proxy.fraudcrew.com
- fastsox.biz

# McColo gets attention

- Security researchers and spam hunters deal with McColo “support” for many months (years)
- Open discussions within community on veracity of provider, getting LE action, best approach
- Increasing direct pressure
- Brian Krebs calls upstream providers to interview on story and provides wealth of evidence
  - Other researchers report concurrently
  - Hurricane Electric, Global Crossing
- Providers de-peer McColo, isolating from Internet



# Nov 12, McColo Knocked Offline



Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [XML RSS Feed](#) ([What's RSS?](#))

## Major Source of Online Scams and Spams Knocked Offline

A U.S. based Web hosting firm that security experts say was responsible for facilitating more than 75 percent of the junk e-mail blasted out each day globally has been knocked offline following reports from **Security Fix** on evidence gathered about suspicious activity emanating from the network.

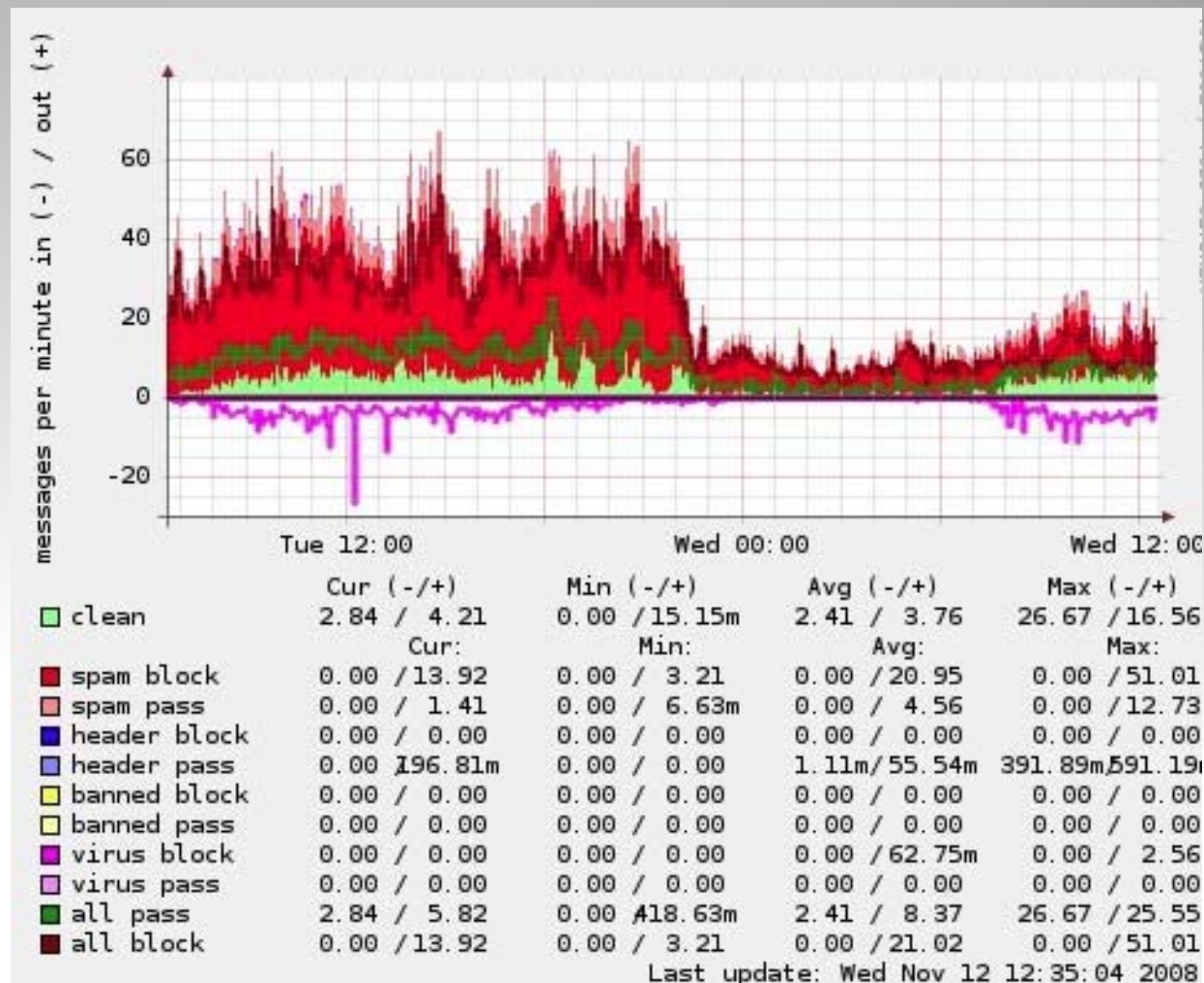
For the past four months, Security Fix has been gathering data from the security industry about **McColo Corp.**, a San Jose, Calif., based Web hosting service whose client list experts say includes some of the most disreputable cyber-criminal gangs in business today.

On Monday, Security Fix contacted the Internet providers that manage more than 90 percent of the company's connection to the larger Internet, sending them information about badness at McColo as documented by the security industry.

On Tuesday afternoon, I heard back from **Global Crossing**, one of McColo's major Internet providers. Their spokesman declined to discuss

# Spam Drops 50-75% Overnight

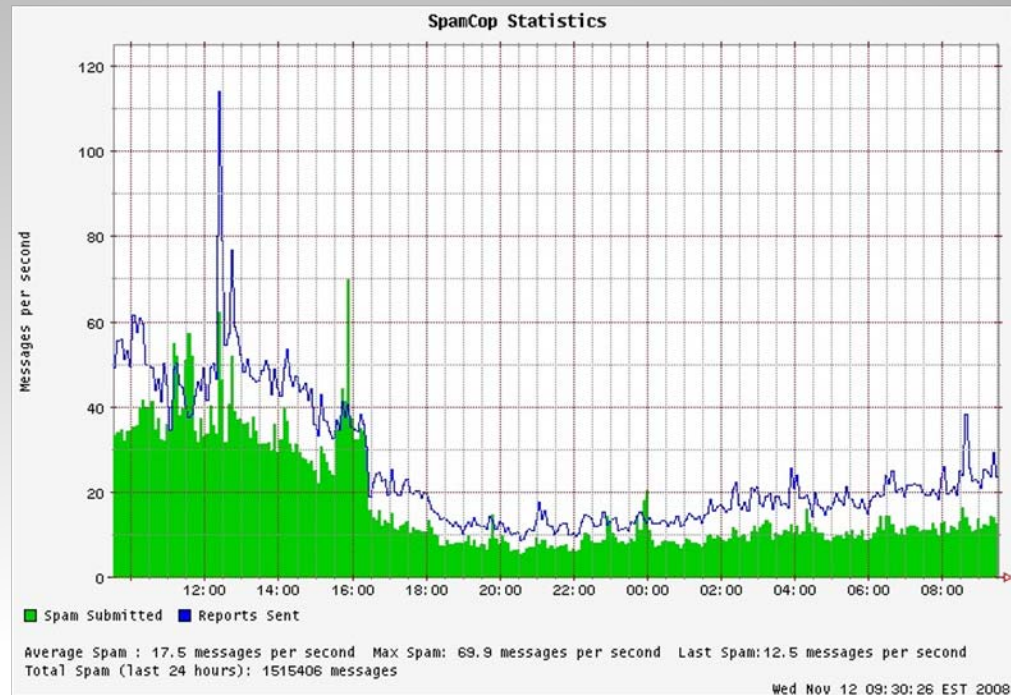
- SpamHaus





# Spam Drops 50-75% Overnight

- SpamCop



# Retail Fraud Rates Plummet

- ◆ “Ori Eisen, founder of [41st Parameter](#), said close to a quarter of a million dollars worth of fraudulent charges that his customers battle every day came to a halt. “It stopped completely that night,” Eisen said, referring to a drop in fraudulent activity linked to purchases of high-value merchandise with stolen credit and debit cards on Nov. 11, the day McColo was shut down.” – Brian Krebs





NO. 34

Ciudad de

México

1-6 march 2009

# Source of Fraud Proxies



## Proxy Socks Service

© Fraud Crew



|         |        |            |        |        |                  |        |
|---------|--------|------------|--------|--------|------------------|--------|
| Правила | Прокси | Логи входа | Отзывы | Оплата | История платежей | Пароль |
|---------|--------|------------|--------|--------|------------------|--------|

|  |                   |
|--|-------------------|
|  | Дней до закрытия: |
|  | Дневной лимит:    |
|  | Месячный лимит:   |
|  | Сегодня:          |

| IP         | Host Name | Online   | Flags | Country       | State          | Town    |
|------------|-----------|----------|-------|---------------|----------------|---------|
| 66.57.*.*  | *****     | 00:56:57 |       | United States | South Carolina | Colum   |
| 72.229.*.* | *****     | 03:06:19 |       | United States | New York       | Ridgew  |
| 71.140.*.* | *****     | 03:11:25 |       | United States | California     | Westmi  |
| 65.188.*.* | *****     | 79:47:51 |       | United States | South Carolina | New Or  |
| 70.23.*.*  | *****     | 00:42:37 |       | United States | New York       | Brook   |
| 72.209.*.* | *****     | 02:35:26 |       | United States | Rhode Island   | Woonso  |
| 76.182.*.* | *****     | 09:46:23 |       | United States | North Carolina | Car     |
| 66.19.*.*  | *****     | 00:10:36 |       | United States | Illinois       | Plainf  |
| 66.229.*.* | *****     | 02:59:33 |       | United States | California     | Murri   |
| 24.189.*.* | *****     | 00:48:03 |       | United States | New York       | Stony B |
| 72.231.*.* | *****     | 05:31:38 |       | United States | New York       | Roche   |
| 75.215.*.* | *****     | 01:08:17 |       | United States | New Jersey     | Living  |
| 64.10.*.*  | *****     | 00:00:00 |       | United States | West Vir       | Clark   |

# E-Mail Address Harvesting

- *...statistics from Project Honey Pot suggest that crawler bots hosted at McColo are responsible for more than 30 million spam messages sent to the project's e-mail traps since June 2006.*
- *...The project estimates that each e-mail address harvested by bots at McColo could expect to receive an additional 2,000 junk e-mail messages a year as a result. Such activity could have major implications for businesses that list large numbers of employee e-mail addresses on their Web sites.*

# Botnet owners respond

- Pre-arranged emergency peering via “shell” organization allows brief re-peering of McColo
- Many botnets re-establish control of their bots and update the IPs of C&C servers to new ones
  - Primarily offshore netblocks
  - Operations hampered (not full update) but not knocked out due to “back door” access
- “Biggest” spamming botnet not updated “Srizbi”
  - Estimates this network responsible for 30-50% of all spam at the time

# The Srizbi Domain Gambit

- FireEye had reverse engineered Srizbi code
- Had normal C&C hardcoded to IPs at McColo
- Backup mechanism was to look for instructions on servers hosted on one of several domains
  - Set of 40 or so domains
  - Rotated every 3 days, for total set of approx. 120
  - FireEye cracked the algorithm for which backup domains would be queried
  - Domains were NOT registered already!



# Keeping Srizbi down

- FireEye starts registering all upcoming domains for Srizbi backup access to keep bad guys away
- Successful for several weeks but getting expensive!
- Able to research size of botnet, exposures and report
- Arrangement made to permanently rotate out Srizbi domains via domain registration community
- Unfortunate gap occurs – bad guys register some domains and update large swath of the botnet
  - Good news, still not re-using

# Srizbi is not the only one...

- Botnet “herders” have incorporated this technique
- Conficker
  - 250 domains per day – 2 variants = 500 per day
  - Some legitimate domains come up in algorithm
  - Big effort launched to block with Microsoft working with several registries and registrars
- What next and how do we deal with this from a policy and operational context?

# Some take-aways

- Criminals can be very smart
- Use the DNS system to their advantage
- Are exploiting several “weak points” in the systems
- DNS was not designed for security/authentication on its own
- Everyone is involved in some way

**Thank You!**

# Case studies in global criminal attacks: McColo & CheckFree

Rod Rasmussen, President & CTO Internet Identity,  
APWG Industry Liason  
[rod.rasmussen <at> internetidentity.com](mailto:rod.rasmussen@internetidentity.com)

E-Crime and Abuse of the DNS Forum:  
Session 2. Criminal Attacks & Abuse Response Today  
March 4, 2009

