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

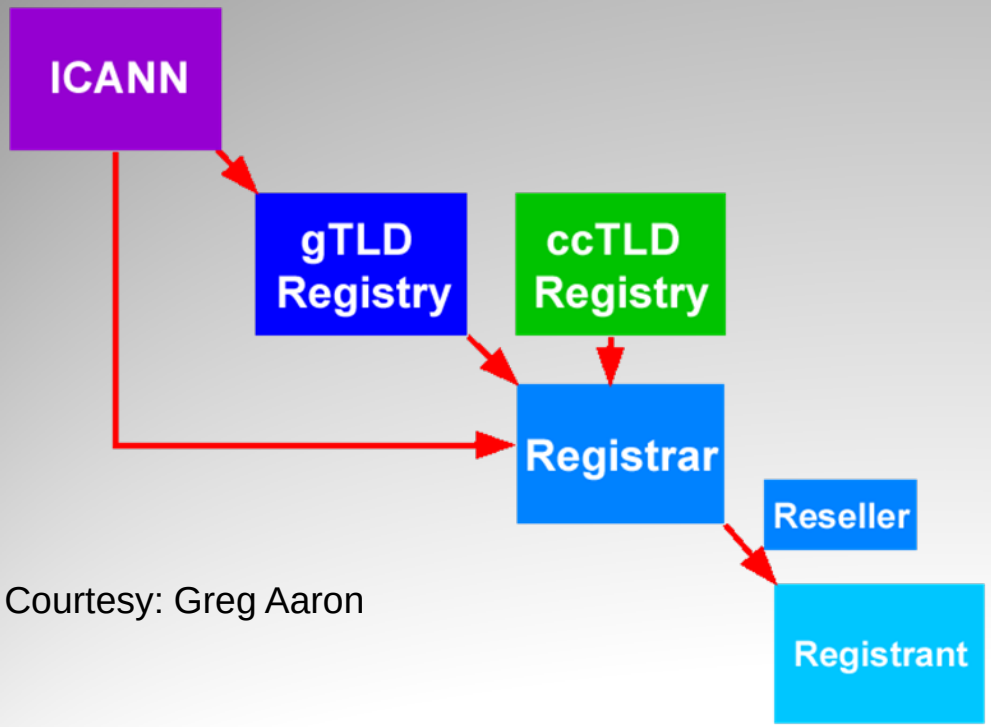
Overview

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

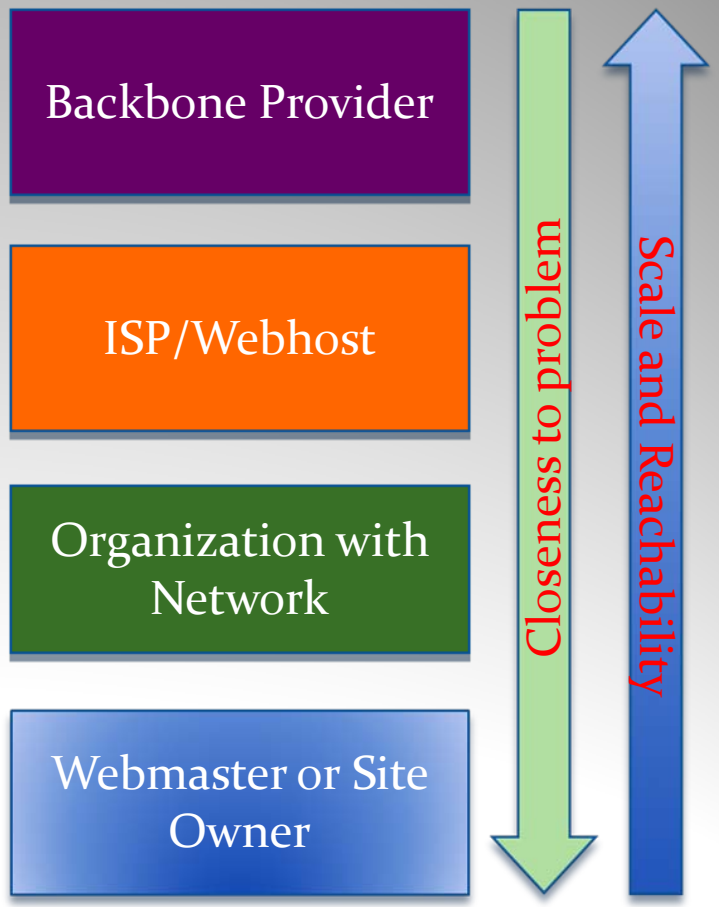
First Responder Viewpoint

- 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

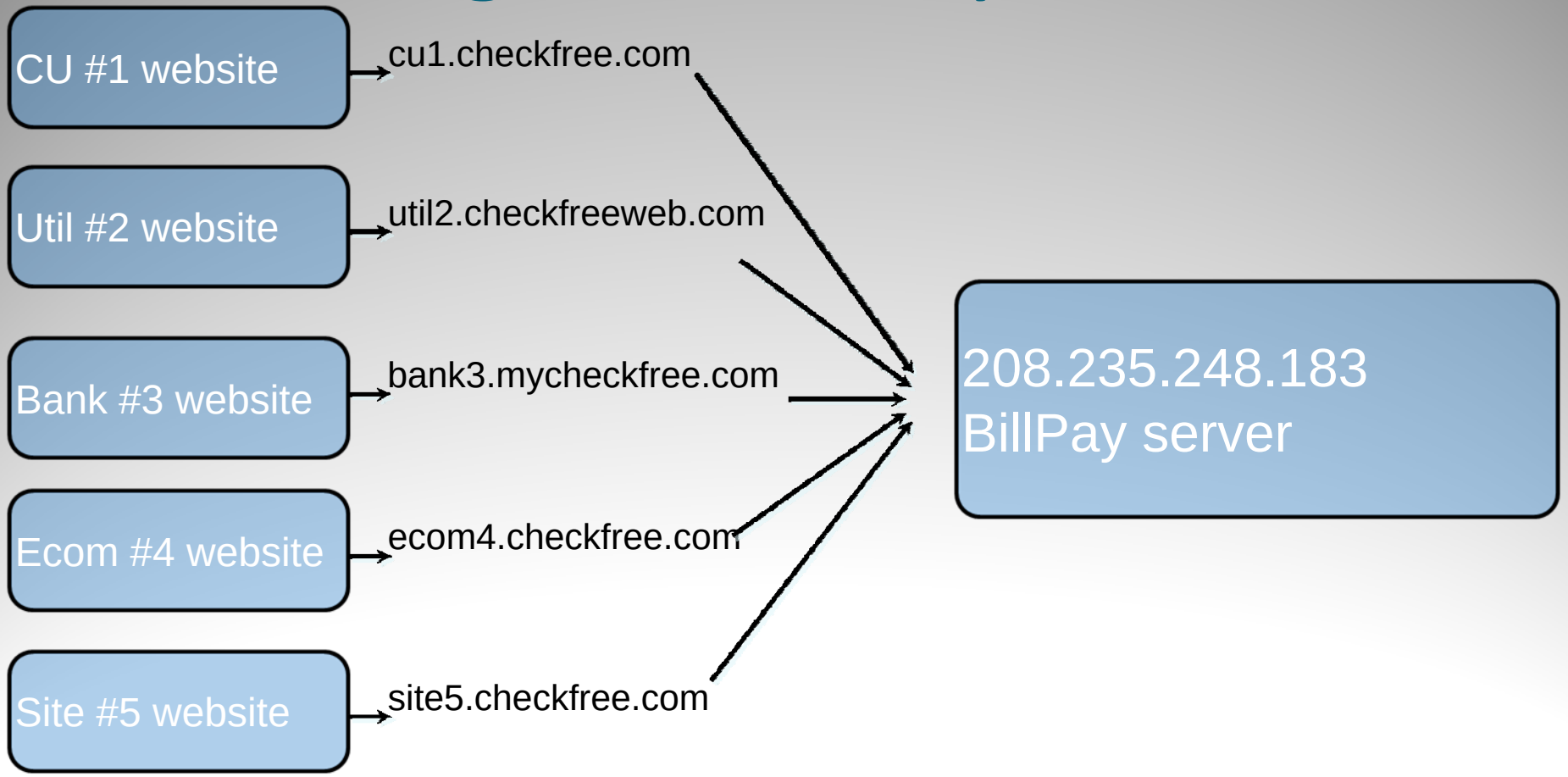
Attack Summary

- 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

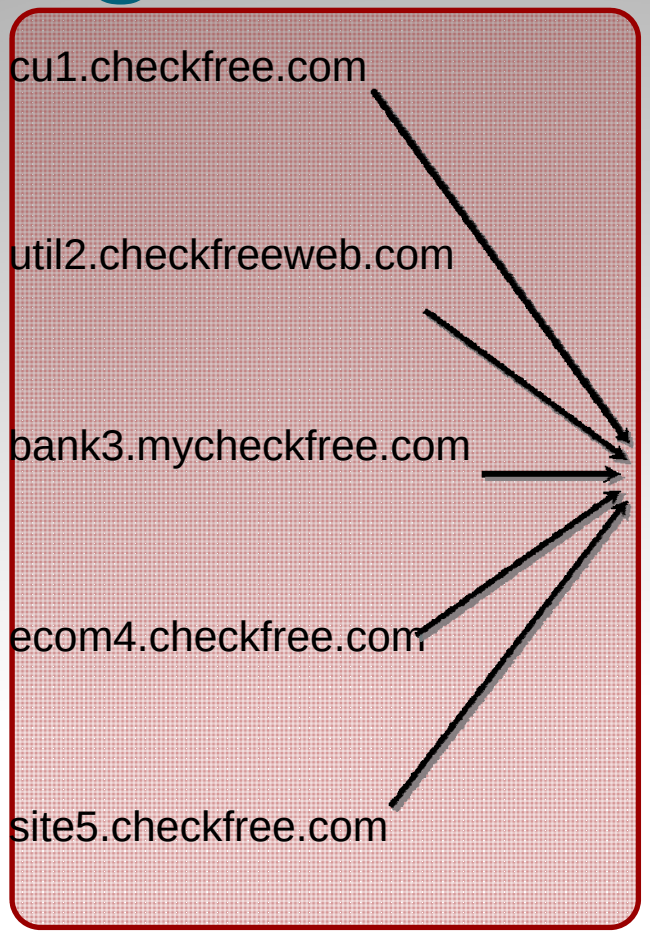
CU #1 website

Util #2 website

Bank #3 website

Ecom #4 website

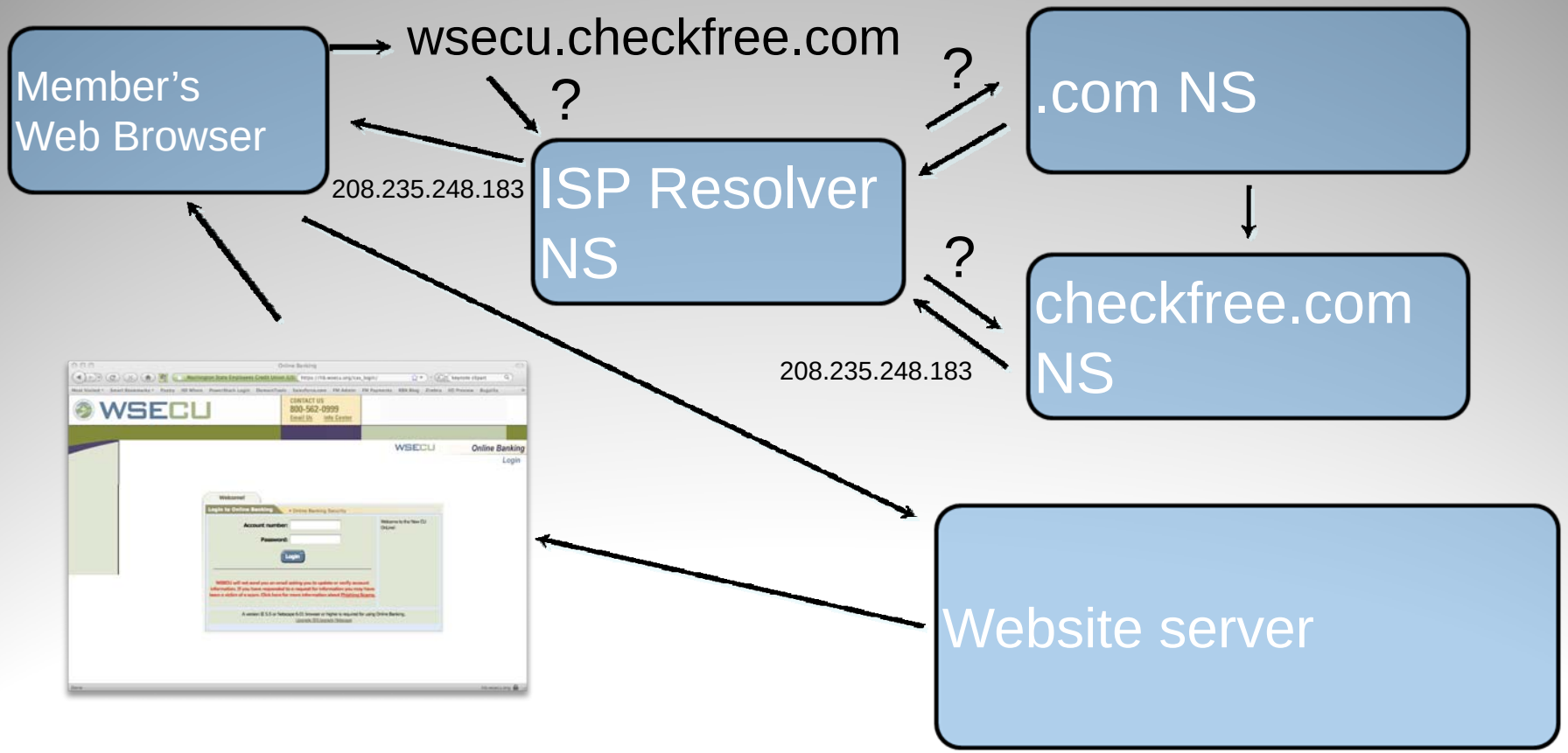
Site #5 website



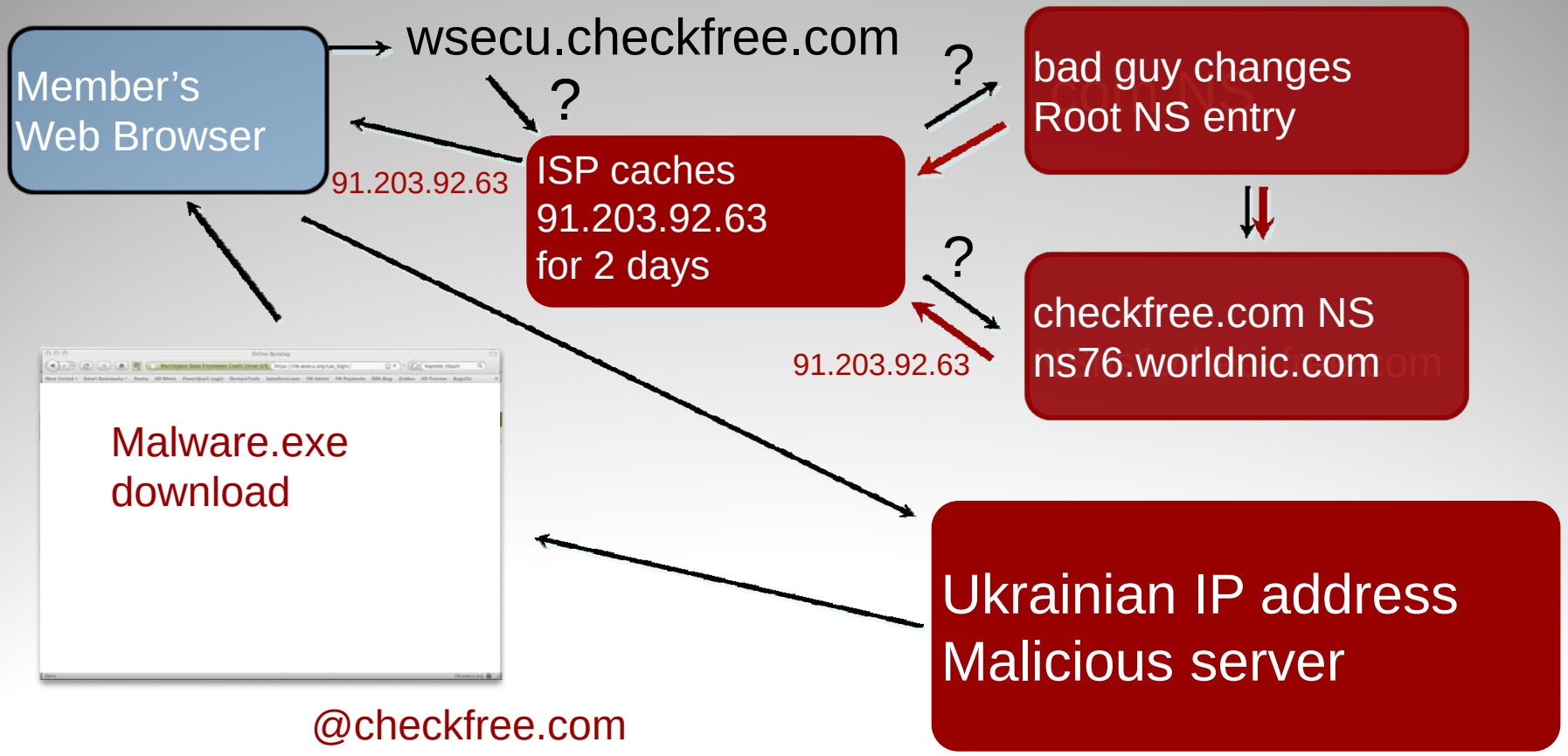
Weakness: Reliance on accurate DNS records

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

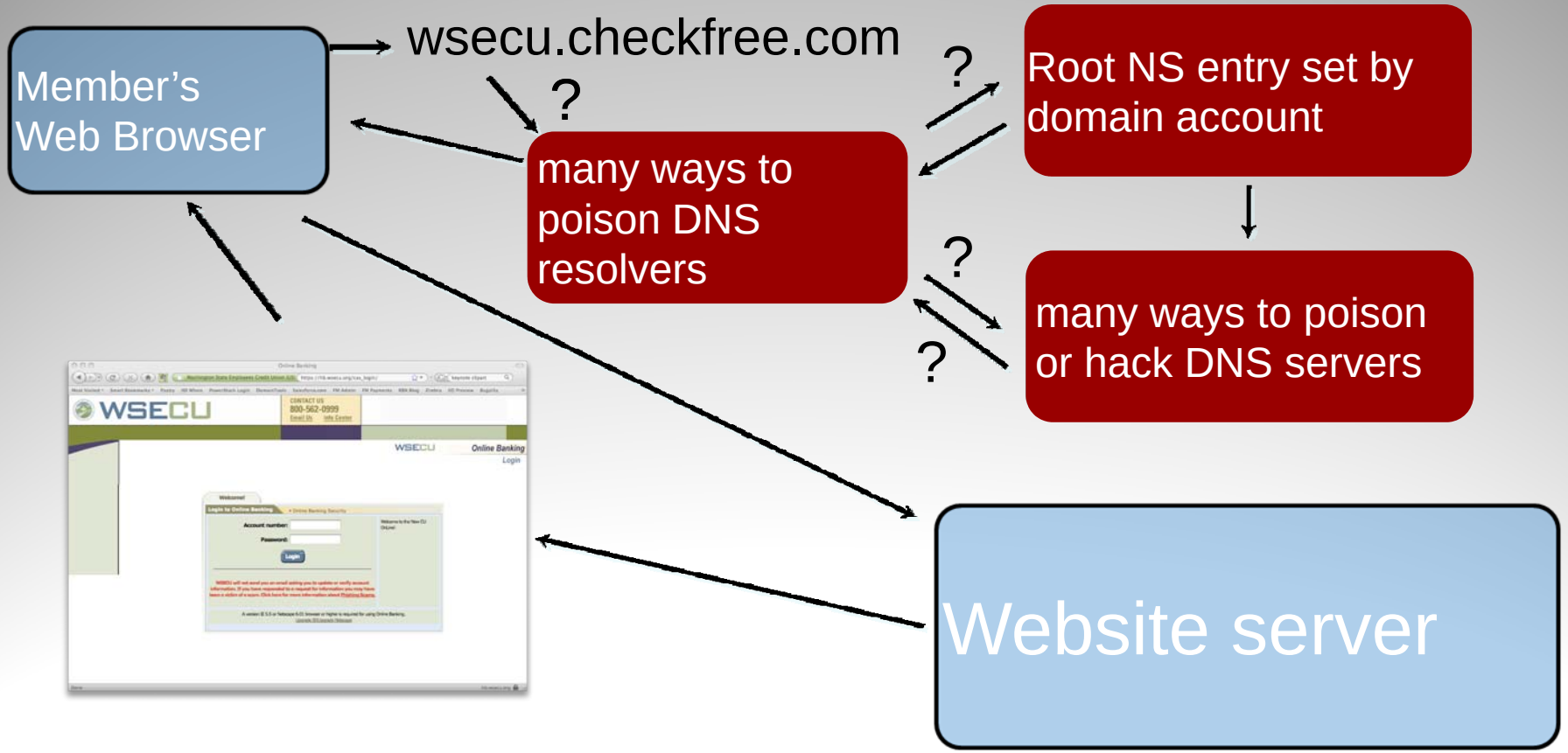
Attack Motivation

- 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)

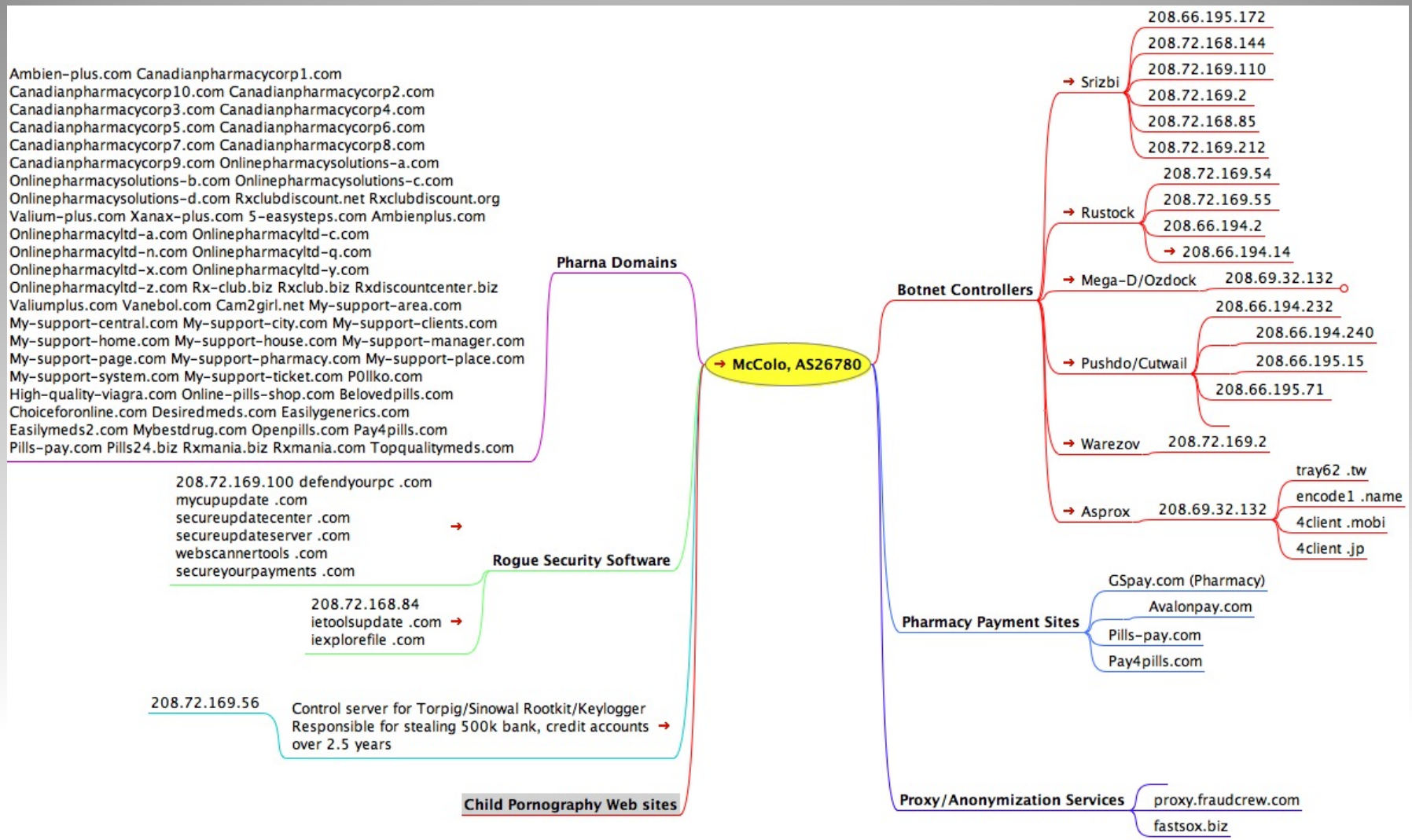
Alex Lanstein@ (fireeye.com)

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



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

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.

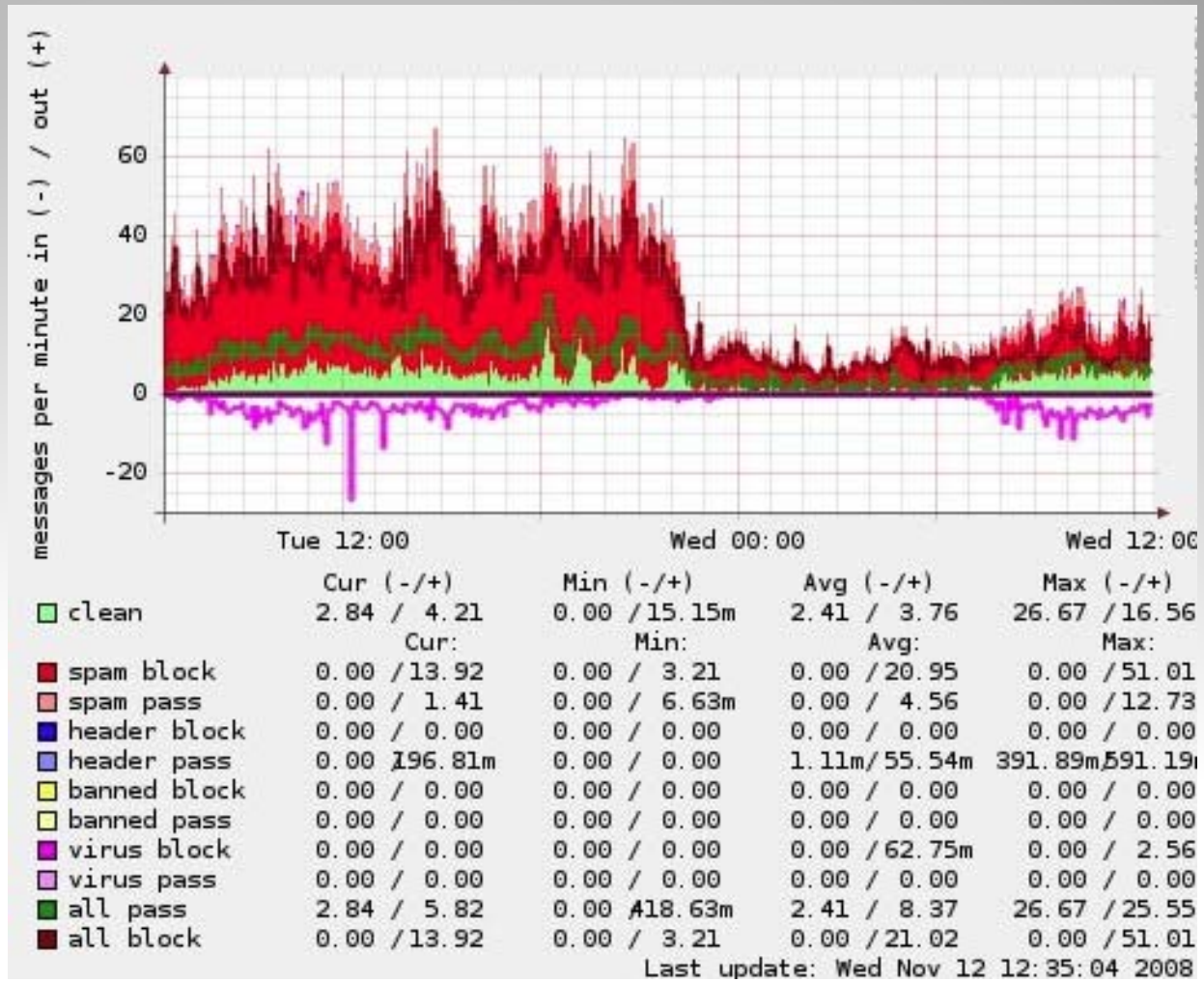
For the past four months, Security Fix has been gathering data from the security industry about **McColo Corp.**, a San Jose, Calif., based Web hosting service whose client list experts say includes some of the most disreputable cyber-criminal gangs in business today.

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

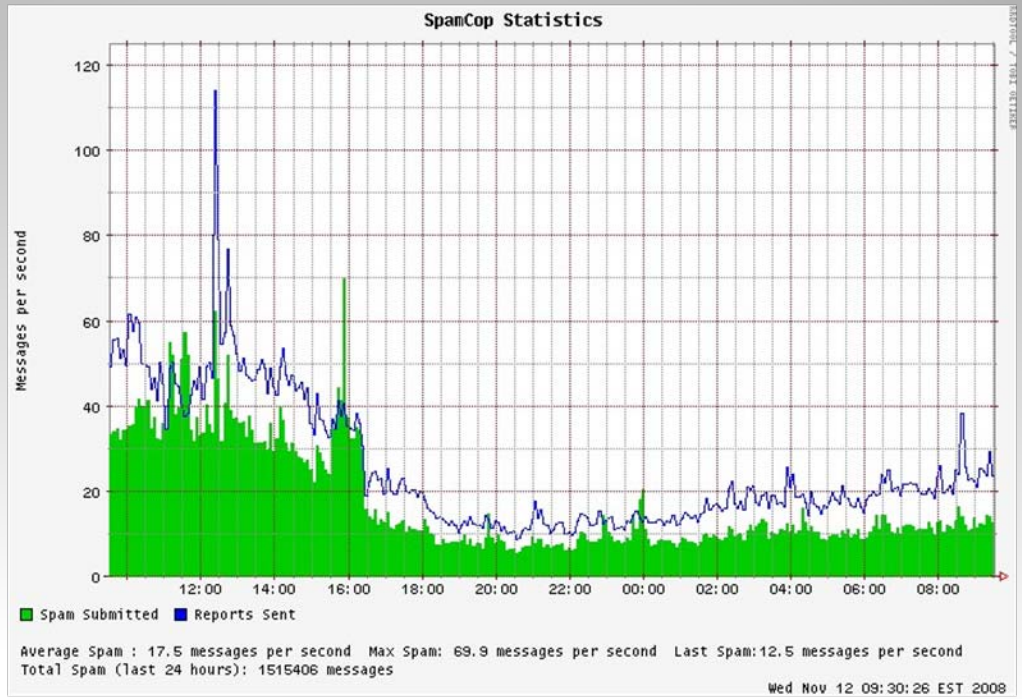
Spam Drops 50-75% Overnight

- 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

Source of Fraud Proxies

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

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