CipherTrust®

Peace of Mind in Messaging™

Mapping the E-mail Universe

Dmitri Alperovitch

Principal Research Engineer

CipherTrust Highlights

The Leader in Messaging Security

- IDC: CipherTrust is bigger than the next 4 competitors combined
- 1/3 of Fortune 500 count on CipherTrust
- Global presence with customers in 40+ countries

One of the Fastest Growing Tech Company

- Among top 50 fastest growing companies: Red Herring, AlwaysOn, Catalyst and others.
- Profitable for consecutive 12 quarters

Pioneered E-mail Security Gateway

- Best-of-breed yet Integrated – inbound & outbound
- Global intelligence (TrustedSource) for proactive threat prevention
- 11 patents pending/awarded

#1 in All Categories by Leading Reviewers & Analysts

Leader's Quadrant

#1 in Market Share

Best All-around Solution

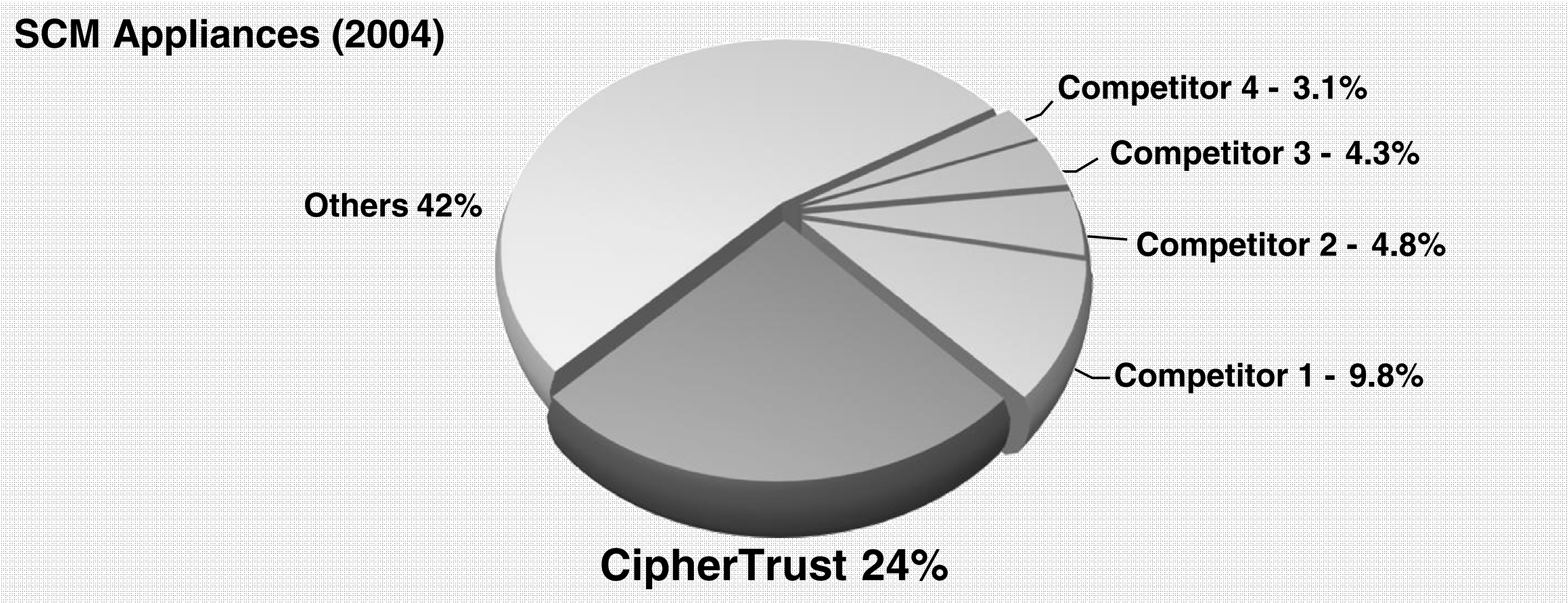
Best Buy Award

Editor's Choice

Pioneering Email Security Appliance

Enterprise Leadership Leads to Market Dominance

CipherTrust's market share equals the 4 closest competitors combined.



Source: IDC 2005

History of Messaging Attacks

- **E-mail**
- May 3, 1978:
  - 1st E-mail Spam (DEC)
- January 1996:
  - 1st Major Phishing Scam (AOL)
- February 26, 1997:
  - 1st E-mail Virus (ShareFun)
- March 26, 1999:
  - 1st Major E-mail Virus (Melissa)
- November 1, 1999:
  - 1st Automated E-mail Worm (Bubble Boy)
- January 13, 2003:
  - 1st E-mail Virus Connected to Spammers (Sobig)

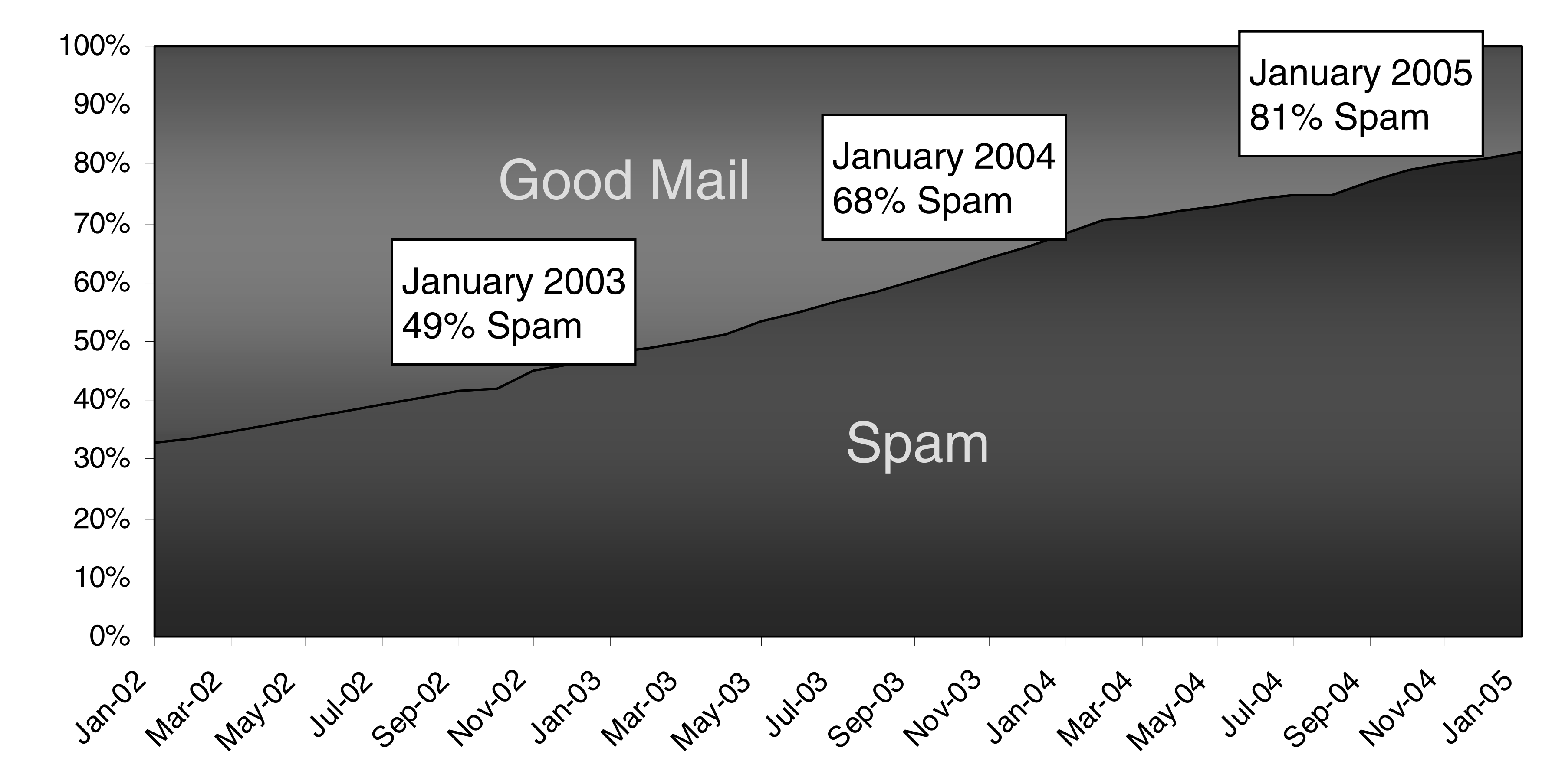
- **Instant Messaging**
- Late 1997:
  - 1st IM spam
- April 25, 2001
  - 1st worm to use IM for propagation. (FunnyFiles)
- February 24, 2004
  - 1st mass-spreading IM worm. (Bizex)

Wireless Messaging

June 14, 2004

1st cell phone virus (Cabir)

Spam Growth Rate



January 2003
49% Spam

January 2004
68% Spam

January 2005
81% Spam

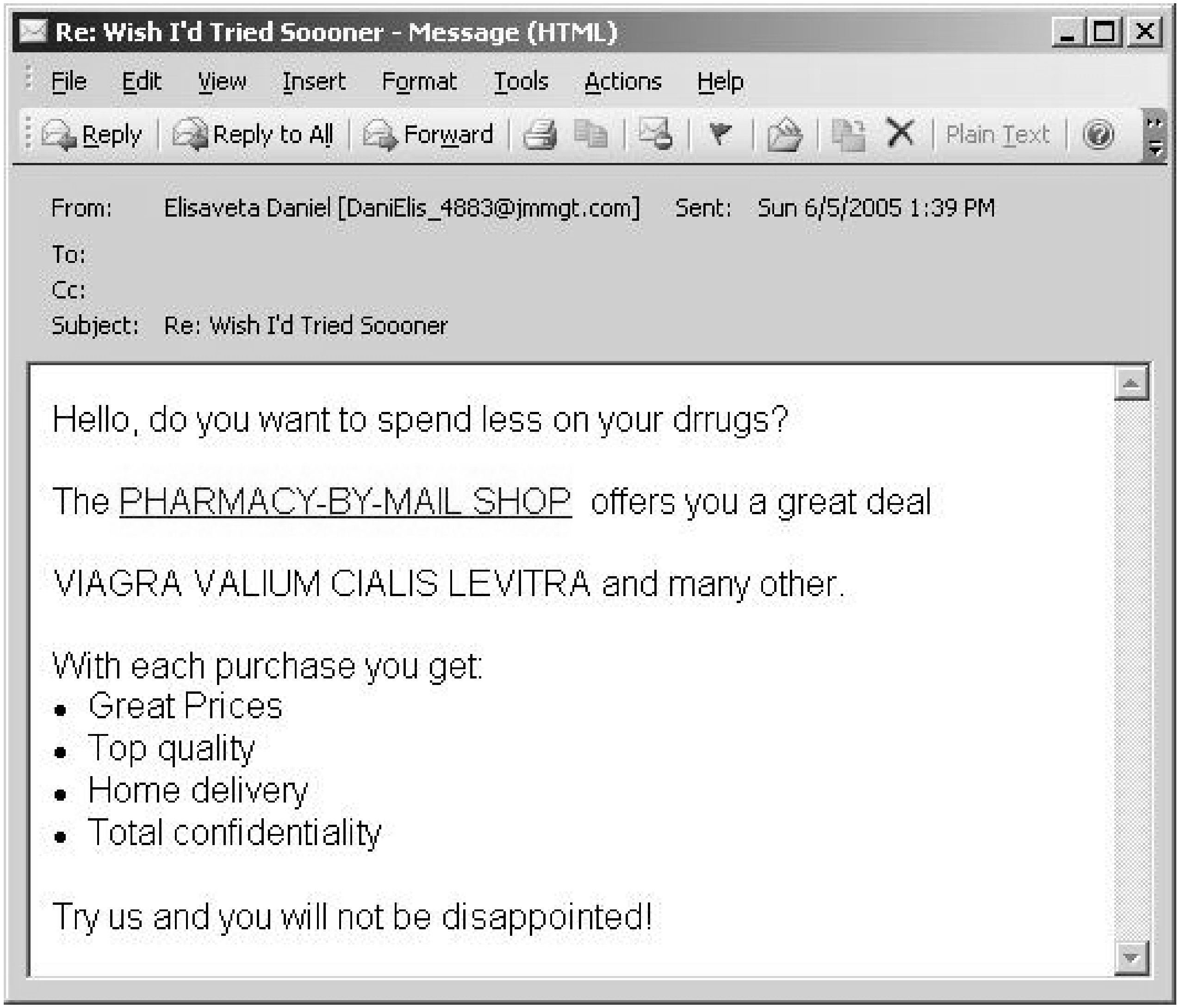
Fighting Spam

- Two main approaches to filter spam:
  - Examine the content of the message
    - Machine-learning techniques (Bayesian, SVM)
    - Signature-based pattern matching techniques
  - Examine the sender of the message
    - Whitelists/Blacklists
    - Challenge Response Systems
    - Reputation Systems

Content-Filtering Challenges

- Never-ending cat & mouse game against spammer randomizations
- Most solutions fail miserably against spam in Asian character sets (many Asian languages have no whitespace separation between words)
- Machine-learning techniques that require training generally are less effective in gateway / organization-wide deployments

Simple Drug Spam


Re: Wish I'd Tried Soooner - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward Plain Text

From: Elisaveta Daniel [DaniElis_4883@jmmgt.com] Sent: Sun 6/5/2005 1:39 PM

To:

Cc:

Subject: Re: Wish I'd Tried Soooner

Hello, do you want to spend less on your drrugs?

The PHARMACY-BY-MAIL SHOP offers you a great deal

VIAGRA VALIUM CIALIS LEVITRA and many other.

With each purchase you get:

- Great Prices
- Top quality
- Home delivery
- Total confidentiality

Try us and you will not be disappointed!

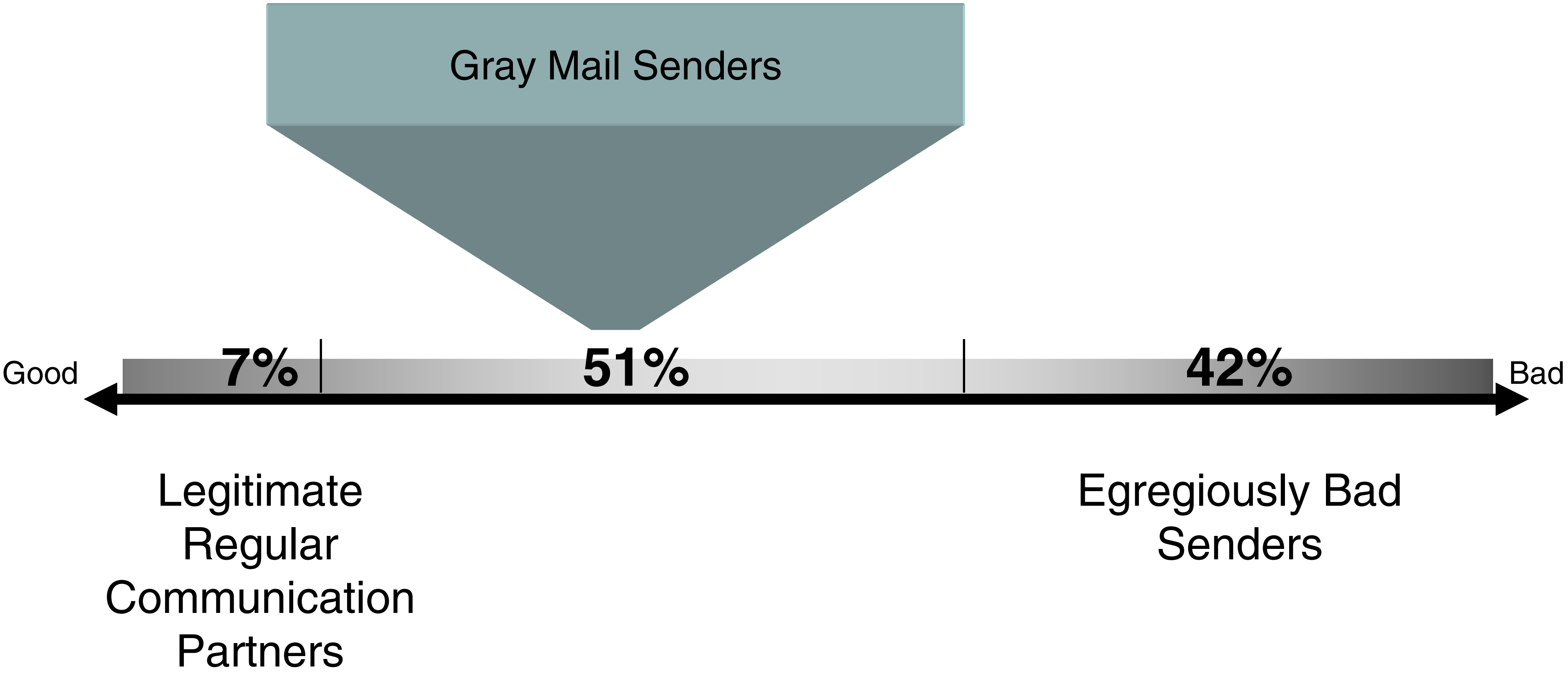
Not so simple…

Message Source:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>

<META content="MSHTML 6.00.2800.1106" name=GENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=#ffffff>
<DIV><FONT face=Arial>Hello, do you want to spend less<SPAN style="DISPLAY: none">sailed
    along o' Bishop.  But Bishop didn't trust us.  He knew too</SPAN> on your
    drrugs?</FONT></DIV>
<DIV><FONT face=Arial></FONT>&nbsp;</DIV>
<DIV><FONT face=Arial>The <A href="http://www.jptl.requiyot.com">PHAR<SPAN style="DISPLAY:
    none">long, inactive waiting was straining the nerves of both Lord</SPAN>MACY-BY-MAIL
    SHOP</A>&nbsp; offer<SPAN style="DISPLAY: none">level of the negroes who sometimes
    toiled beside him.  The man,</SPAN>s you&nbsp;a great deal</FONT></DIV>
<DIV><FONT face=Arial></FONT><FONT face=Arial></FONT>&nbsp;</DIV>
<DIV><FONT face=Arial>VIA<SPAN style="DISPLAY: none">would be placed if you had direct word
    from him of what has happened.</SPAN>GRA VA<SPAN style="DISPLAY: none">level of the
    calves of his fine boots of Spanish leather, Captain</SPAN>LIUM CIAL<SPAN style="DISPLAY:
    none">and in the latitude into which Lord Julian had strayed this was a</SPAN>IS LEV<SPAN
    style="DISPLAY: none">all resolved upon joining the great Brotherhood of the Coast,
    as</SPAN>ITRA and many other.</FONT></DIV>
<DIV>&nbsp;</DIV>
```

E-mail Sender IP Universe



Gray Mail Senders

Good

7%

51%

42%

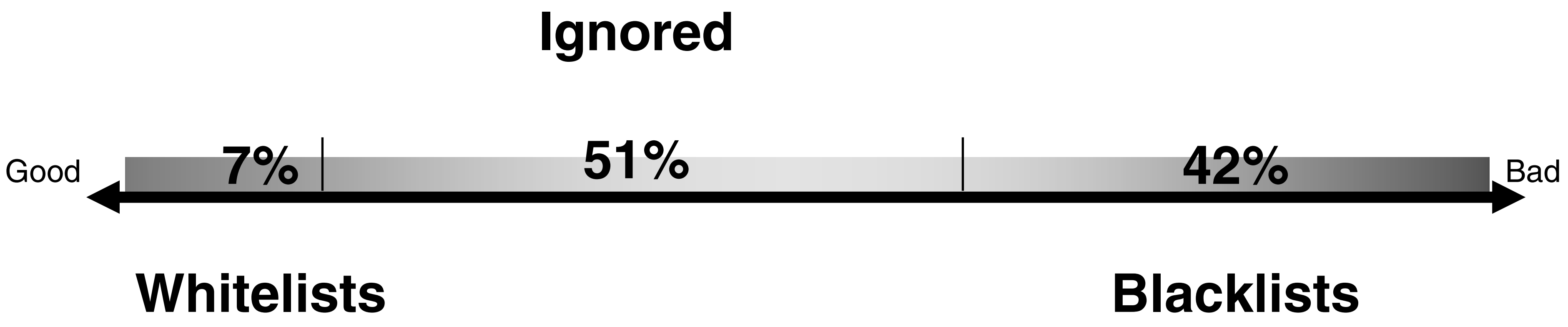
Bad

Legitimate
Regular
Communication
Partners

Egregiously Bad
Senders

CipherTrust

Traditional Approach

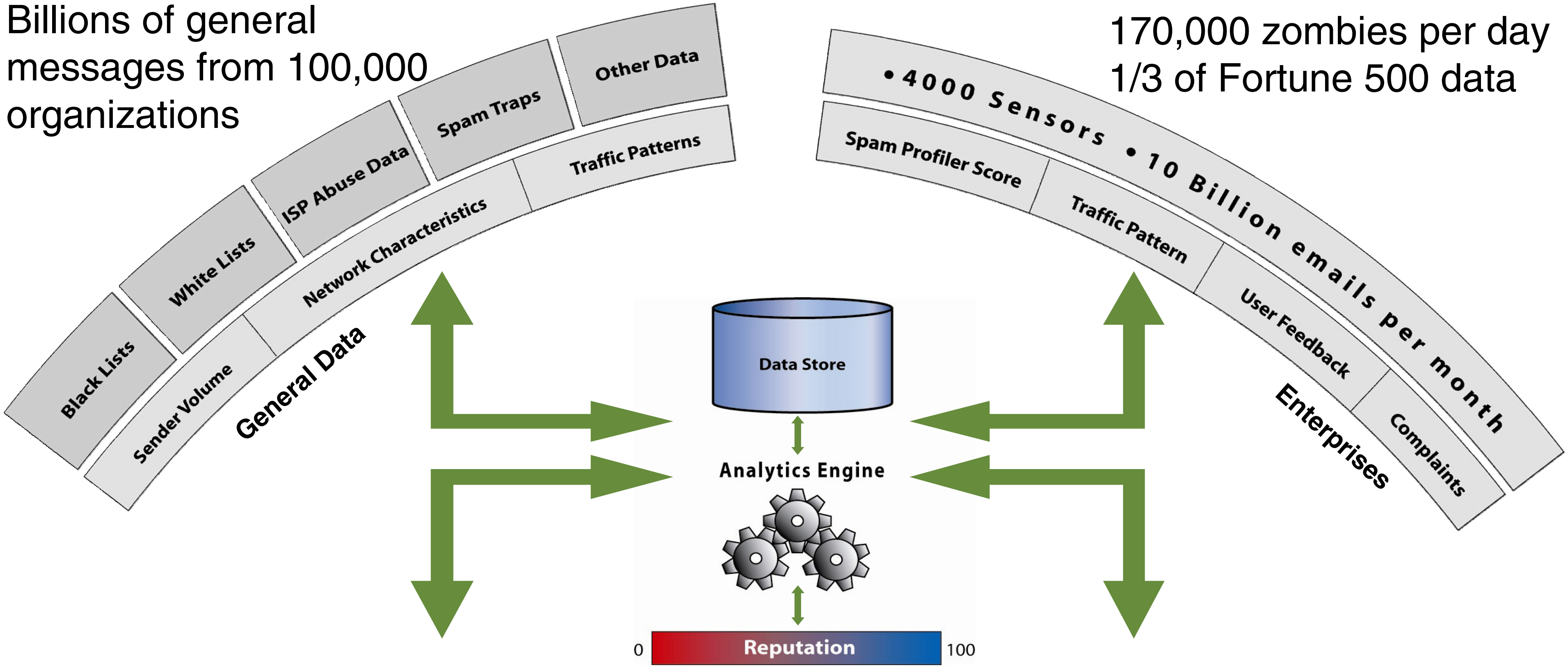


TrustedSource Architecture

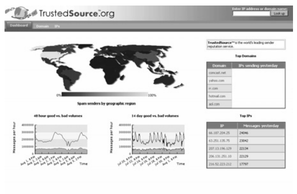
Share global intelligence with local behavior

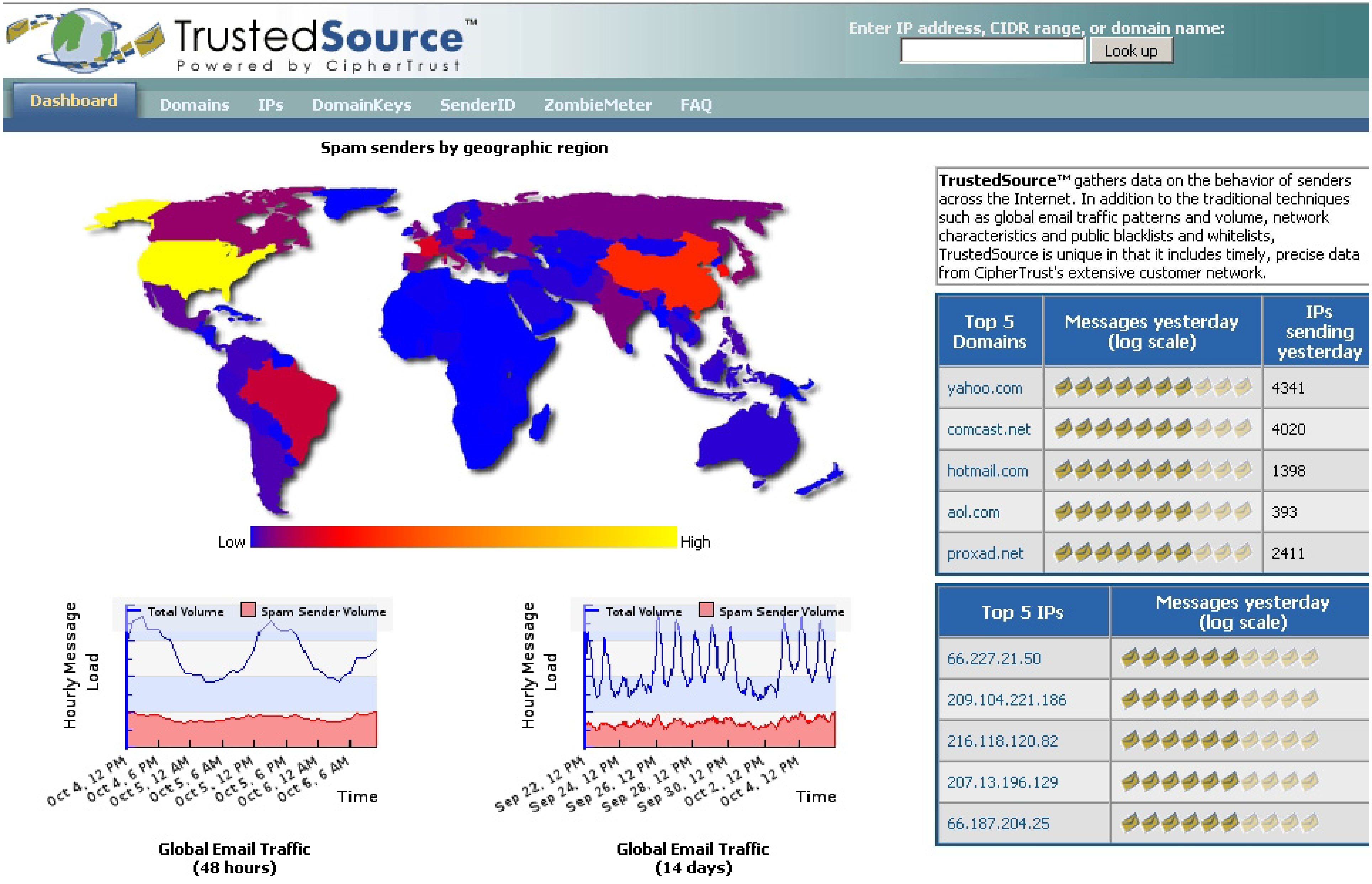
Billions of general messages from 100,000 organizations

170,000 zombies per day
1/3 of Fortune 500 data



TrustedSource.org





Spam senders by geographic region

Global Email Traffic
(48 hours)

Global Email Traffic
(14 days)

TrustedSource™ gathers data on the behavior of senders across the Internet. In addition to the traditional techniques such as global email traffic patterns and volume, network characteristics and public blacklists and whitelists, TrustedSource is unique in that it includes timely, precise data from CipherTrust's extensive customer network.

Top 5 Domains	Messages yesterday (log scale)	IPs sending yesterday
yahoo.com	✉✉✉✉✉✉✉	4341
comcast.net	✉✉✉✉✉✉✉	4020
hotmail.com	✉✉✉✉✉✉✉	1398
aol.com	✉✉✉✉✉✉✉	393
proxad.net	✉✉✉✉✉✉✉	2411

Top 5 IPs	Messages yesterday (log scale)
66.227.21.50	✉✉✉✉✉✉
209.104.221.186	✉✉✉✉✉✉
216.118.120.82	✉✉✉✉✉✉
207.13.196.129	✉✉✉✉✉✉
66.187.204.25	✉✉✉✉✉✉

Sender Behavioral Tests

- Spam sender behavior is vastly different from legitimate mailers

- Goal: send quickly as many messages as possible to a wide recipient population (few legitimate senders exhibit those characteristics)

- Sending IPs are predominantly zombies

Zombies: Definition

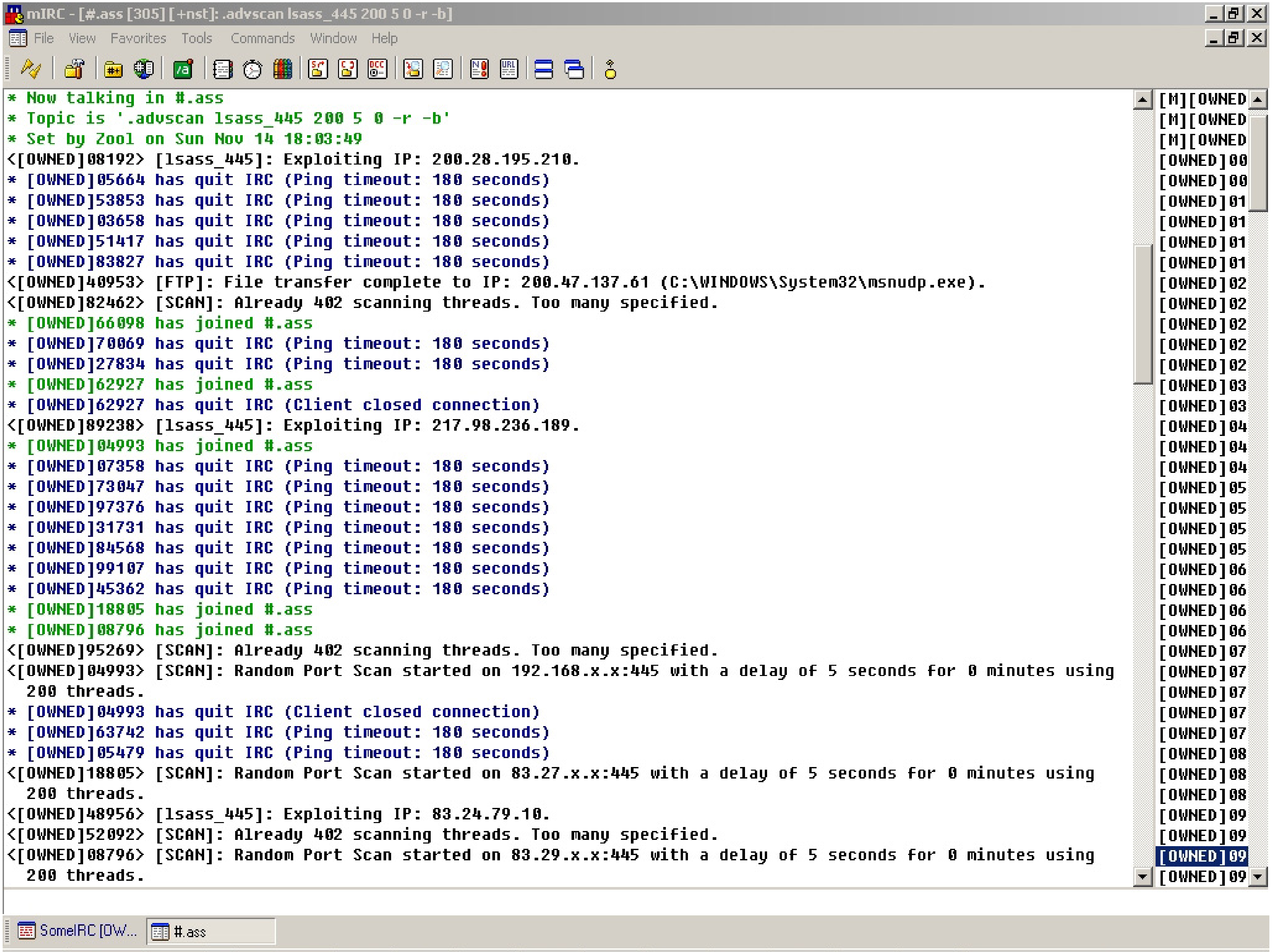
- Zombie: innocent machine infect with a worm/virus that carries (or downloads) a ‘bot’ program as its payload, used as staging ground for attacks

- The ‘bot’ software reports to a controller Internet Relay Chat (IRC) channel/website and downloads and executes instructions from it

- Instructions:
  - Launch DDoS attack
  - Open SOCKS/SMTP relay proxy
  - Harvest passwords/e-mail addresses from infected system
  - Distribution of viruses

•Popular bot software: Mitgleider, rBot, AgoBot

•Largest botnet detected to date: 350,000 zombie IPs



```
* Now talking in #.ass
* Topic is '.advscan lsass_445 200 5 0 -r -b'
* Set by Zool on Sun Nov 14 18:03:49
<[OWNED]08192> [lsass_445]: Exploiting IP: 200.28.195.210.
* [OWNED]05664 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]53853 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]03658 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]51417 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]83827 has quit IRC (Ping timeout: 180 seconds)
<[OWNED]40953> [FTP]: File transfer complete to IP: 200.47.137.61 (C:\WINDOWS\System32\msnudp.exe).
<[OWNED]82462> [SCAN]: Already 402 scanning threads. Too many specified.
* [OWNED]66098 has joined #.ass
* [OWNED]70069 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]27834 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]62927 has joined #.ass
* [OWNED]62927 has quit IRC (Client closed connection)
<[OWNED]89238> [lsass_445]: Exploiting IP: 217.98.236.189.
* [OWNED]04993 has joined #.ass
* [OWNED]07358 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]73047 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]97376 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]31731 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]84568 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]99107 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]45362 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]18805 has joined #.ass
* [OWNED]08796 has joined #.ass
<[OWNED]95269> [SCAN]: Already 402 scanning threads. Too many specified.
<[OWNED]04993> [SCAN]: Random Port Scan started on 192.168.x.x:445 with a delay of 5 seconds for 0 minutes using
  200 threads.
* [OWNED]04993 has quit IRC (Client closed connection)
* [OWNED]63742 has quit IRC (Ping timeout: 180 seconds)
* [OWNED]05479 has quit IRC (Ping timeout: 180 seconds)
<[OWNED]18805> [SCAN]: Random Port Scan started on 83.27.x.x:445 with a delay of 5 seconds for 0 minutes using
  200 threads.
<[OWNED]48956> [lsass_445]: Exploiting IP: 83.24.79.10.
<[OWNED]52092> [SCAN]: Already 402 scanning threads. Too many specified.
<[OWNED]08796> [SCAN]: Random Port Scan started on 83.29.x.x:445 with a delay of 5 seconds for 0 minutes using
  200 threads.
```

Zombies: Location

- Average of 170,000 never before seen zombies each day

1	United States	19.08%
2	China	14.56%
3	South Korea	9.61%
4	Germany	5.99%
5	France	5.69%
6	Brazil	5.56%
7	Japan	3.70%
8	United Kingdom	3.13%
9	Spain	2.96%
10	Taiwan	2.31%

•~1500 new zombies seen each hour are located in US

Top 10 Networks:

1.	AS 4134:	ChinaNet Backbone
2.	AS 4766:	Korea Telecom
3.	AS 3320:	Deutsche Telekom
4.	AS 4837:	China169 Backbone
5.	AS 3215:	France Telecom
6.	AS 9318:	Hanaro Telecom (Korea)
7.	AS 3462:	Chunghwa Telecom (Taiwan)
8.	AS 19262:	Verizon Global Networks
9.	AS 7738:	Telecomunicacoes da Bahia (Brazil)
10.	AS 4812:	China Telecom

Top 5 Networks in US:

1. AS 19262: Verizon Global Networks
2. AS 3356: Level 3 Communications
3. AS 6198: BellSouth Network Solutions
4. AS 7132: SBC Internet Services
5. AS 7018: AT&T WorldNet Services

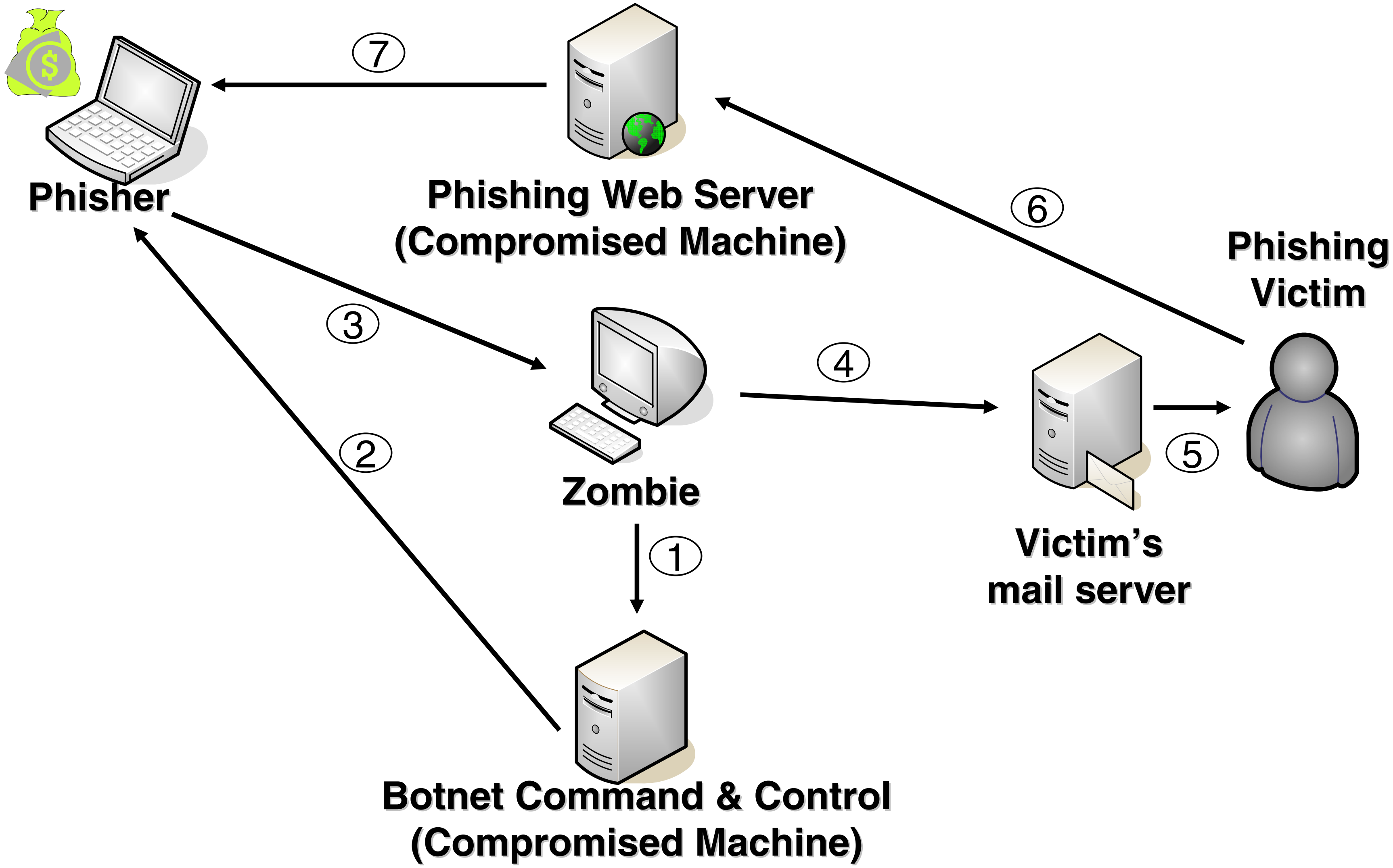
Zombies: Source of Phishing

- Once a zombie is told to run a SOCKS/SMTP proxy, it is resold to spammer/phisher who proceeds to relay e-mails directly through it

- Get control of the zombie machine while it is relaying the e-mails from the phisher and you have a great chance of catching them!

•Virtually all phishing is sent through zombies

Phishing Cycle



Phisher

Phishing Web Server
(Compromised Machine)

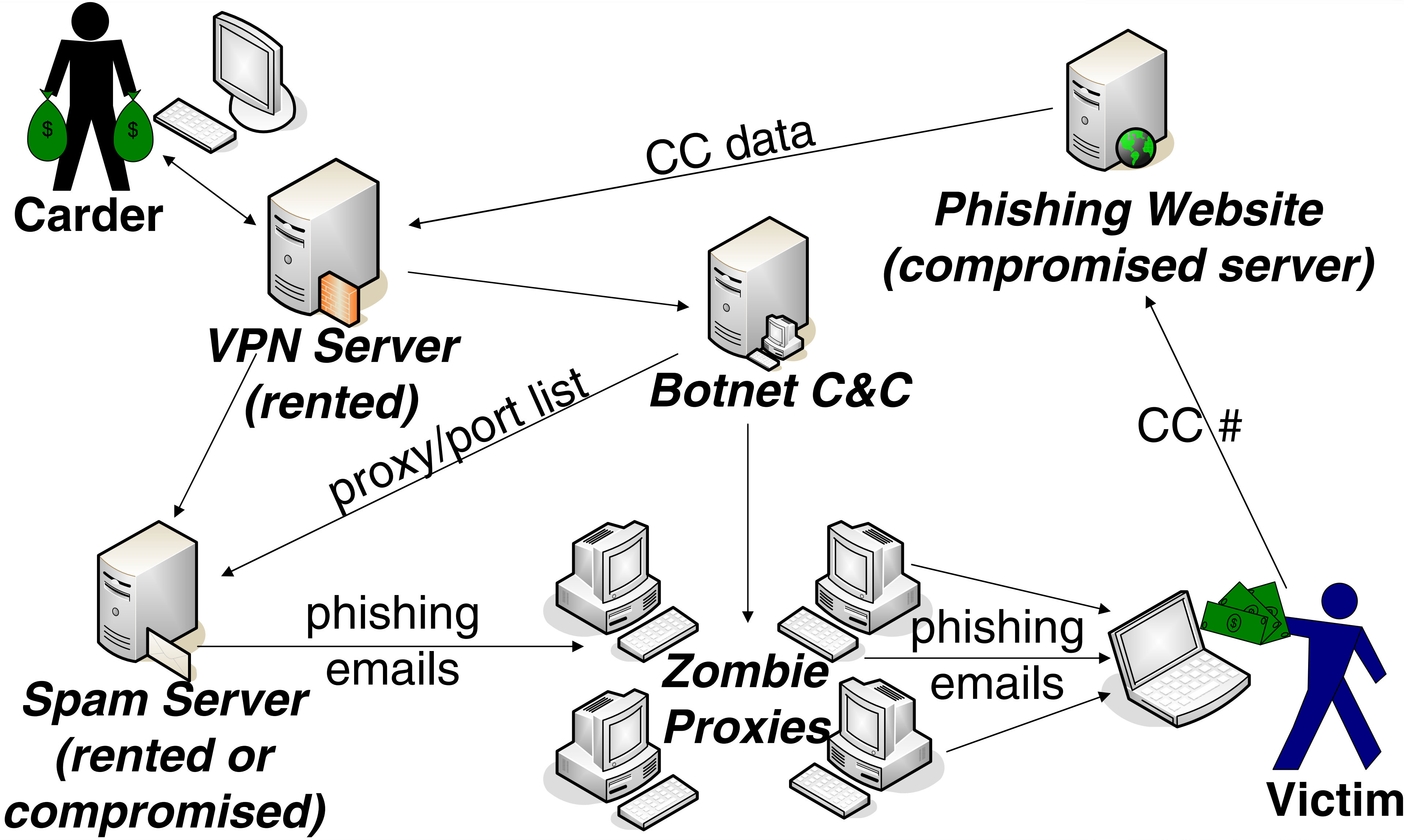
Zombie

Botnet Command & Control
(Compromised Machine)

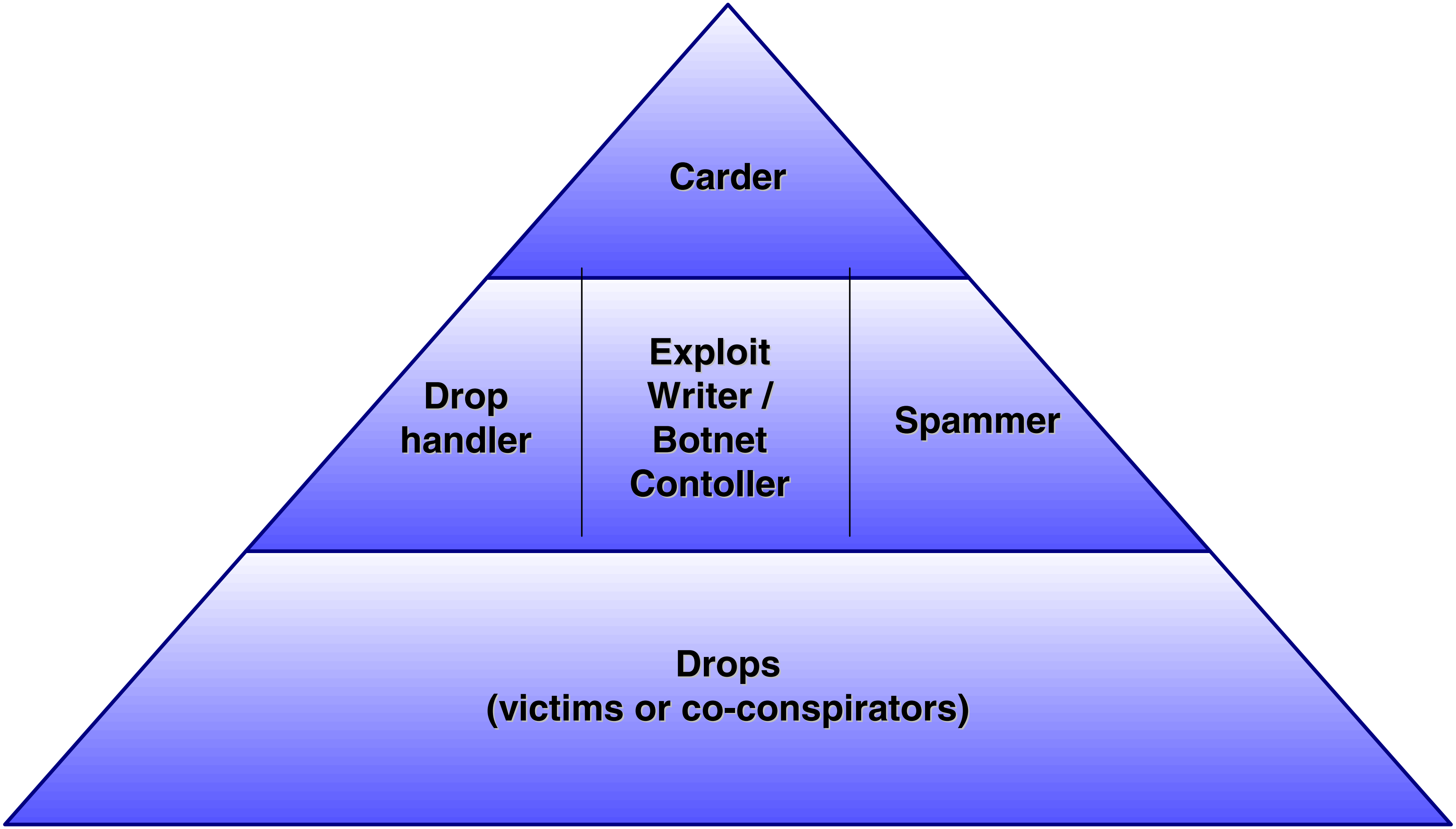
Victim’s
mail server

Phishing
Victim

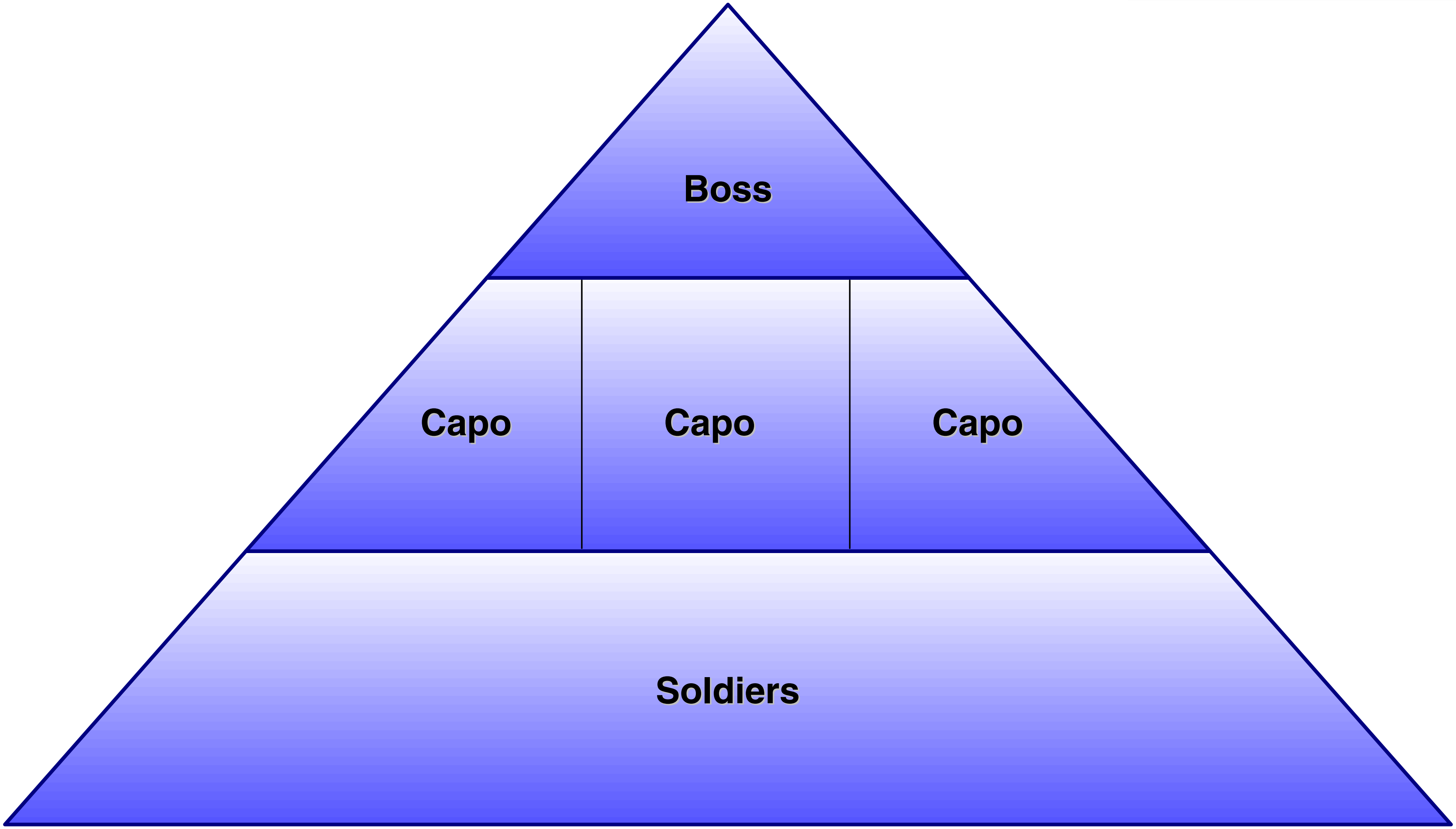
Operational security



Phishing: Organizational Structure


Carder
Drop handler
Exploit Writer / Botnet Contoller
Spammer
Drops
(victims or co-conspirators)

Mafia: Organizational Structure



Types of Phishing

1. **Website Phishing**

   Victim conned into visiting to fraud website

2. **Trojan Phishing**

   Trojan steals data directly off victim’s machine or modifies OS/browser settings to unwittingly redirect them to fraud website

3. **Phone Phishing**

   Traditional phone scamming (now with a VoIP twist)

4. **E-commerce Store Phishing**

   Fake online store is setup to harvest credit cards

Phishing: What is involved?

1. **Website Phishing**
   - Scam e-mail writer (English-competence required)
   - Fraud website developer
   - Bulk domain registrant for fraud site
   - Web hosting provider for fraud site
   - Professional spammer

•Typical phishing response: 15-20 legitimate replies on 1 million sent e-mails

Phishing: What is involved?

2. **Trojan Phishing**
   - Trojan developer
   - Web hosting provider for fraud site

3. **Phone Phishing**
   - English speaker
   - Equipment
     - IVR (Interactive Voice Response) System
     - Phone dialing system (ex. BigInform)
     - Analog Phone Gateway (ex. Cisco VG224)

•Proliferation of VoIP technology likely to soon result in increase in Phone Phishing

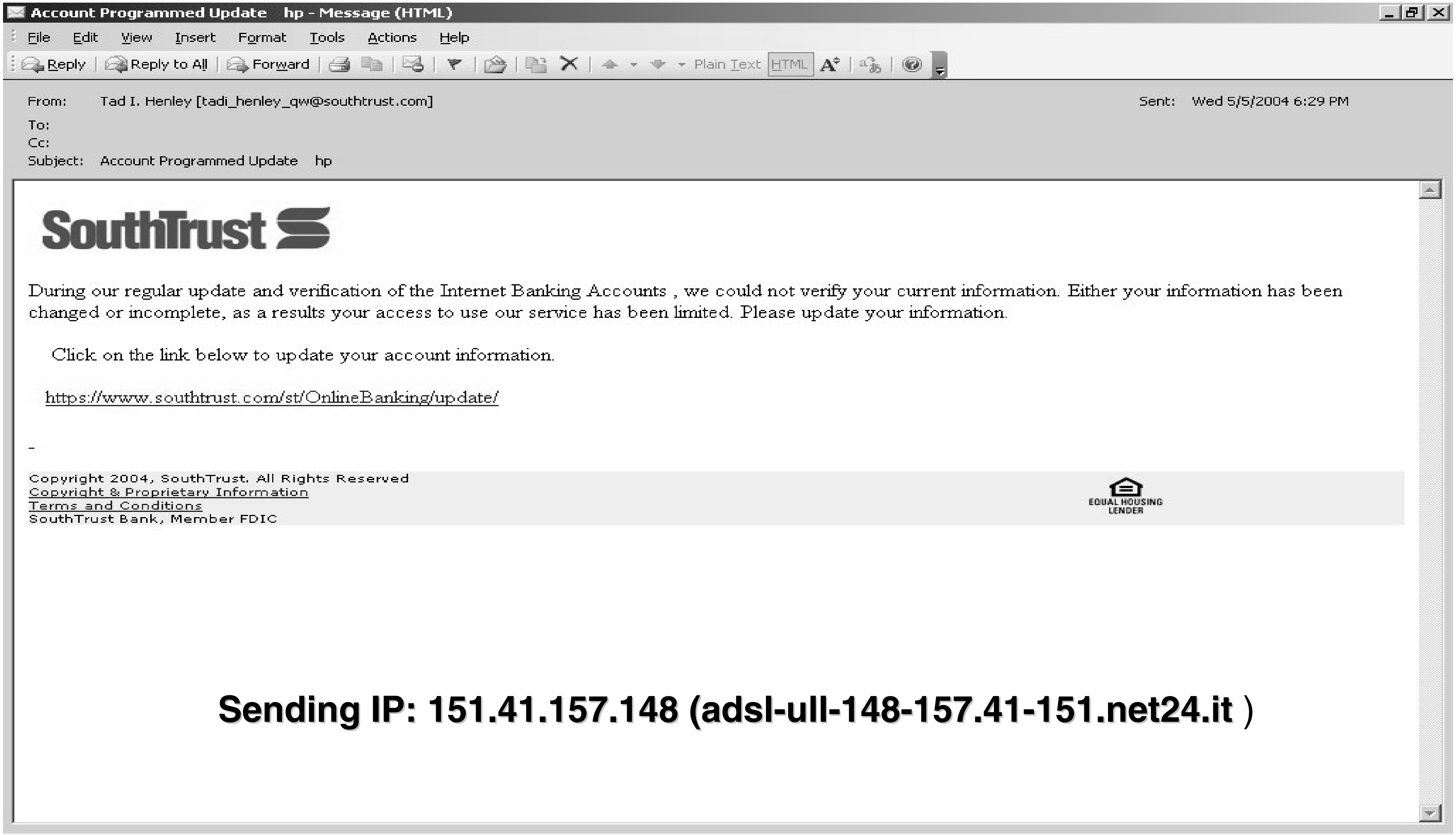
Phishing: What is involved?

4. E-Commerce Store Phishing

- Website developer
- Web hosting provider

- Typically each of these services purchased from multiple verified ‘vendors’ advertised on Carder Forums

Phishing Zombie Analysis


Account Programmed Update hp - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward Plain Text HTML

From: Tad I. Henley [tadi_henley_qw@southtrust.com]

Sent: Wed 5/5/2004 6:29 PM

To:

Cc:

Subject: Account Programmed Update hp

SouthTrust

During our regular update and verification of the Internet Banking Accounts , we could not verify your current information. Either your information has been changed or incomplete, as a results your access to use our service has been limited. Please update your information.

Click on the link below to update your account information.

https://www.southtrust.com/st/OnlineBanking/update/

-

Copyright 2004, SouthTrust. All Rights Reserved
Copyright & Proprietary Information
Terms and Conditions
SouthTrust Bank, Member FDIC

EQUAL HOUSING LENDER

Sending IP: 151.41.157.148 (adsl-ull-148-157.41-151.net24.it)

Time is of the essence

- **151.41.157.148** global sending history:

  2005-05-06 10:23:51 EST
  2005-05-06 10:23:51 EST
  2005-05-06 10:35:58 EST
  ....
  2005-05-06 14:29:35 EST
  2005-05-06 14:29:45 EST
  2005-05-06 14:31:22 EST

  4 hour activity window

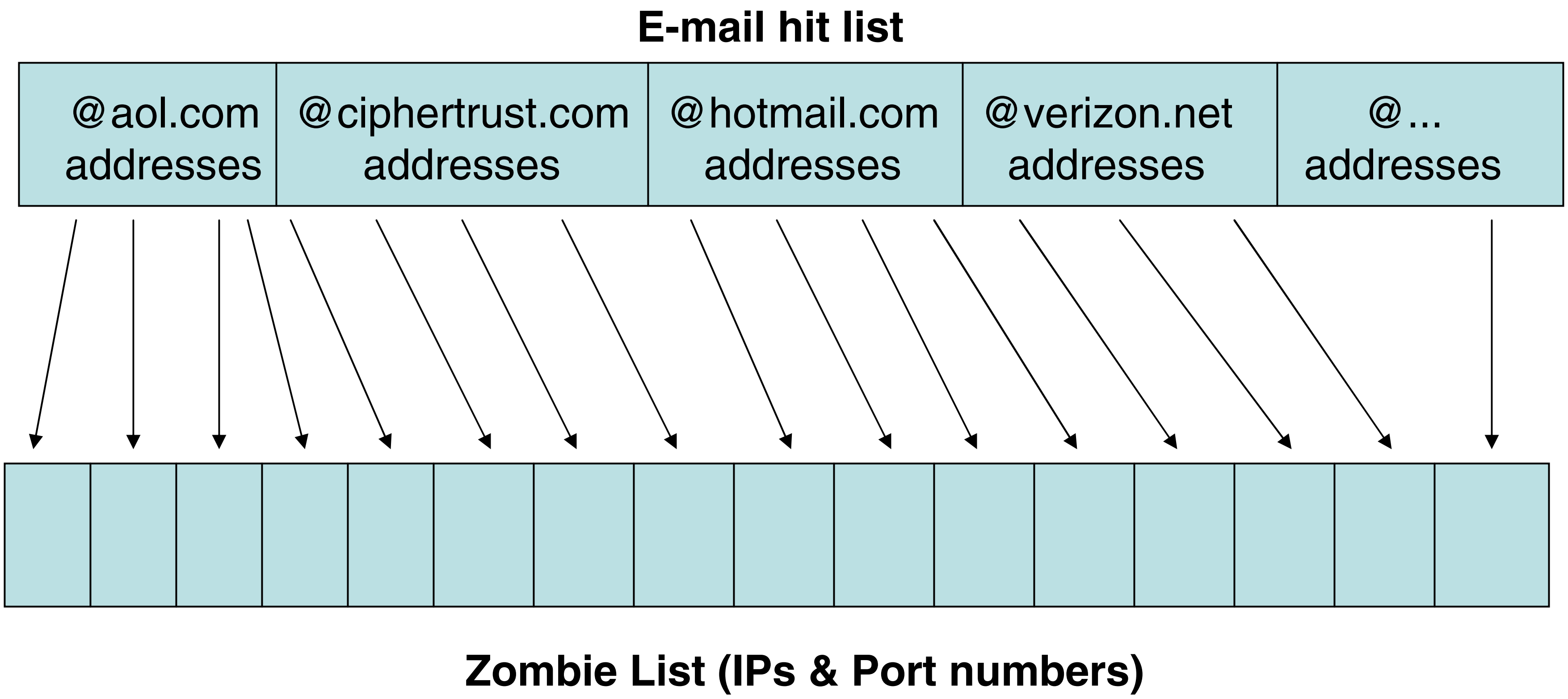
- Hit ~8% of large U.S. enterprises
- Hasn't been heard from since

•Average uptime for a phishing zombie: 8 hours

Phishing Zombies

- Reasons:
  - Phishers and Spammers use e-mail ‘hit’ lists, addresses of all the people they send a particular e-mail campaign to
  - Phishing lists are typically smaller and more targeted in nature
  - The hit list is usually sorted and divided between all the zombies that are used in a campaign to optimize for speed and minimize chances of spamtrap detection

Phishing: Distribution Patterns



E-mail hit list

@aol.com addresses

@ciphertrust.com addresses

@hotmail.com addresses

@verizon.net addresses

@... addresses

Zombie List (IPs & Port numbers)

Zombie goes silent once it is done with its portion of the list: often does not come back for months

Sender Authentication

- 3 Industry Evolving Standards:
  - Sender Policy Framework (SPF)
  - SenderID
  - DomainKeys Identified Mail (DKIM)

- Goal: Verify that the sending IP is permitted to send mail on behalf of the domain it claims to come from

Sender Authentication Standards

- SPF: Authenticates IP based on connection-level data (RFC 821 MAIL FROM)
- SenderID: Authenticates IP based on message header data (RFC 822 Purported Responsible Address)
- DKIM: Cryptographically authenticates message based on message header data (RFC 822 From)

Anti-Spam Application

- Message Authenticity != Message Reputation
- Spammers have learned to register SPF/DomainKeys DNS records
  - 20% of spam with SPF records passes SenderID
  - 6% of spam with SPF records fails SenderID
- Need for reputation systems to make into an effective anti-spam tool

- Thank you.
- Questions?

Dmitri Alperovitch
Principal Research Engineer
dmitri@ciphertrust.com
(678) 904-9235