The status of SP Security

Steinthor Bjarnason

Security Consulting Engineer, Cisco Europe

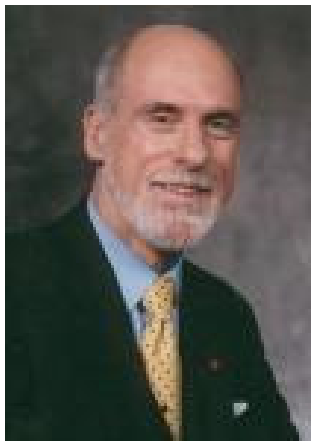
sbjarnas@cisco.com

SITREP
Security Threat Landscape & Drivers

1

“The wonderful thing about the Internet is that you’re connected to everyone else. The terrible thing about the Internet is that you’re connected to everyone else.”

Vint Cerf
Inventor



The Security Trap

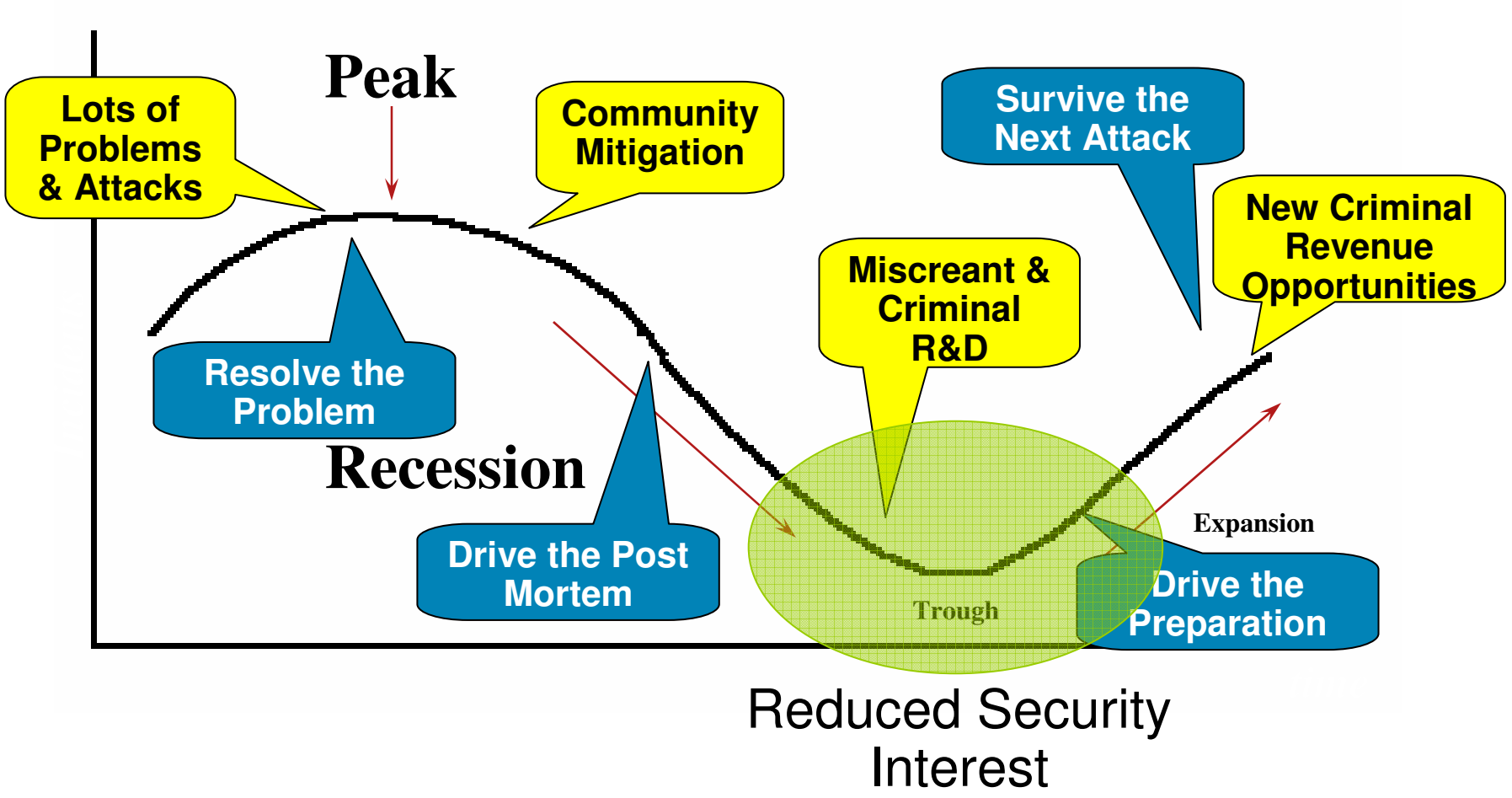
- If you do your Security Job well ….

  "What are you doing and why am I spending all the money on security?"

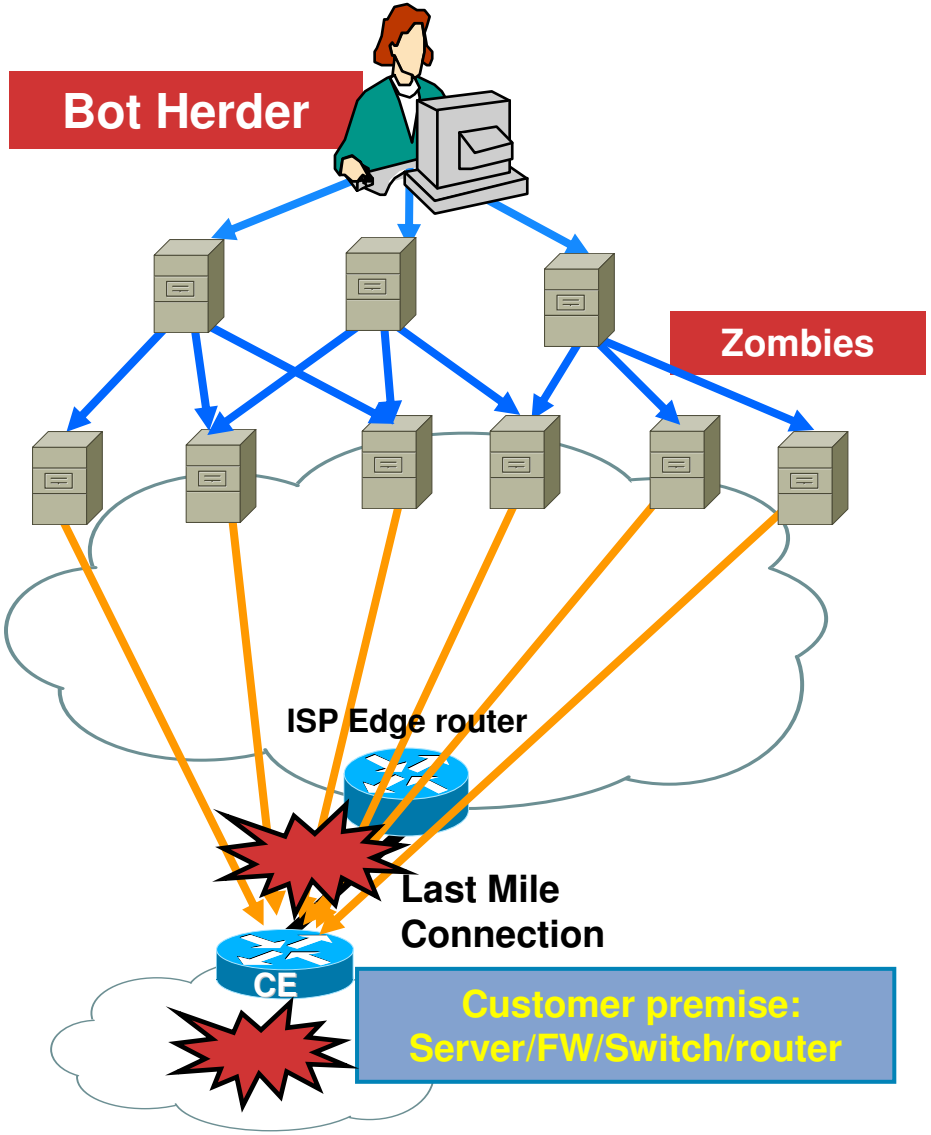
- If you do not do you Security Job well …

  "Why didn't you do something to keep this from happening!?!"

Criminal - Incident Economic Cycles



Botnets: "The Dawn of the Zombies"



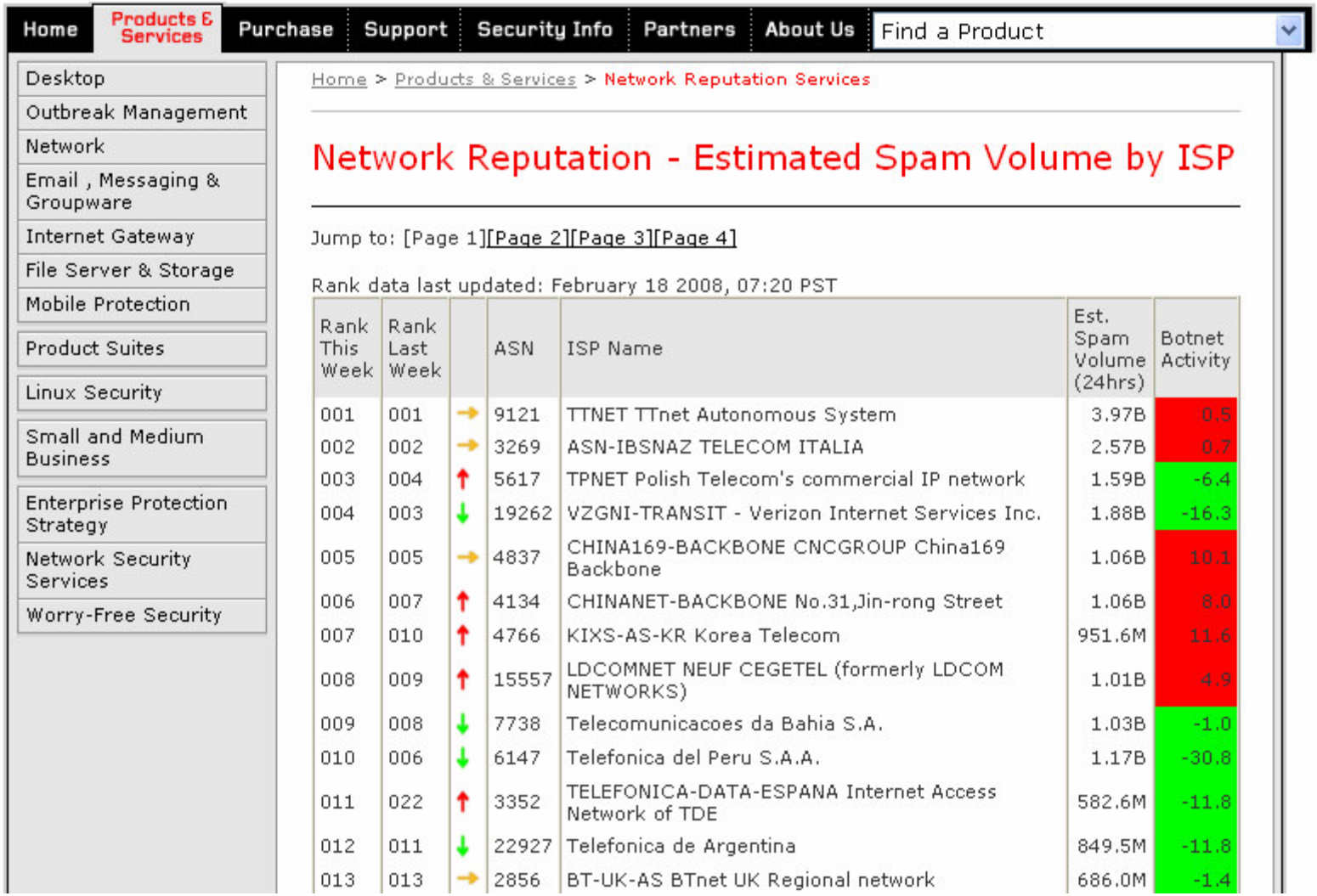
- Botnets for Rent!
- A "Botnet" is a group of compromised computers on which bot herders have installed special programs (zombies) .
- These computers can then be used for almost any activity without the owner knowing what is going on
- Examples are:
  - DoS & DDoS attacks
  - Generate SPAM
  - Phising attacks

Botnets: Why do you care?

- Bots on your PC
  - Capture your bank details, passwords, etc.
  - Clear, right? ;-)
- Bots on your network
  - Can consume bandwidth (spam, dos bots)
  - Can affect the network (collateral damage)
  - Serious operational cost!!!
- Being blackholed / filtered
  - Major spammers, dossers, etc, increasingly often blackholed upstream
  - Sometimes a host, sometimes the whole ISP, …

… oops!

Why do you care? Part 2



Home | Products & Services | Purchase | Support | Security Info | Partners | About Us | Find a Product

- Desktop
- Outbreak Management
- Network
- Email , Messaging & Groupware
- Internet Gateway
- File Server & Storage
- Mobile Protection
- Product Suites
- Linux Security
- Small and Medium Business
- Enterprise Protection Strategy
- Network Security Services
- Worry-Free Security

Home > Products & Services > Network Reputation Services

Network Reputation - Estimated Spam Volume by ISP

Jump to: [Page 1][Page 2][Page 3][Page 4]

Rank data last updated: February 18 2008, 07:20 PST

Rank This Week	Rank Last Week		ASN	ISP Name	Est. Spam Volume (24hrs)	Botnet Activity
001	001	→	9121	TTNET TTnet Autonomous System	3.97B	0.5
002	002	→	3269	ASN-IBSNAZ TELECOM ITALIA	2.57B	0.7
003	004	↑	5617	TPNET Polish Telecom's commercial IP network	1.59B	-6.4
004	003	↓	19262	VZGNI-TRANSIT - Verizon Internet Services Inc.	1.88B	-16.3
005	005	→	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	1.06B	10.1
006	007	↑	4134	CHINANET-BACKBONE No.31,Jin-rong Street	1.06B	8.0
007	010	↑	4766	KIXS-AS-KR Korea Telecom	951.6M	11.6
008	009	↑	15557	LDCOMNET NEUF CEGETEL (formerly LDCOM NETWORKS)	1.01B	4.9
009	008	↓	7738	Telecomunicacoes da Bahia S.A.	1.03B	-1.0
010	006	↓	6147	Telefonica del Peru S.A.A.	1.17B	-30.8
011	022	↑	3352	TELEFONICA-DATA-ESPANA Internet Access Network of TDE	582.6M	-11.8
012	011	↓	22927	Telefonica de Argentina	849.5M	-11.8
013	013	→	2856	BT-UK-AS BTnet UK Regional network	686.0M	-1.4

https://nssg.trendmicro.com/nrs/reports/rank.php?page=1; snapshot from 18th Feb 2009

Why do you care? Part 3

- As an engineer, you want to help making the Internet a more secure place ;-)
- Next question: Does your boss care?

Why are Home PC's getting infected? They have AV don't they?

79% feel their computers are "very safe", or "somewhat safe" from virus infection

81% claim to have anti-virus software installed

61% claim to have anti-spyware software installed

On average, 6.8 virus infections were found per computer

69% of systems were found to have adware or spyware infection

*20% of PCs had been cleaned once before, then reinfected with a different kind of bot

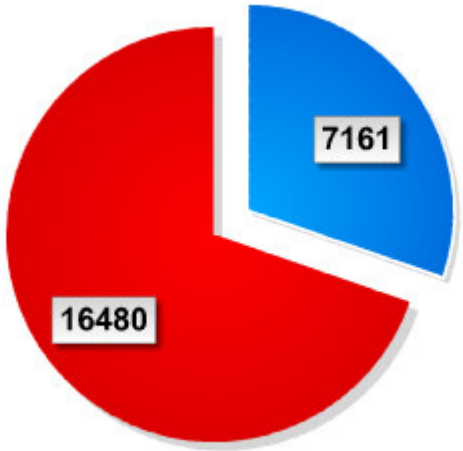
Source: AOL/NCSA Online Safety Study Dec 2005

*Source: Microsoft Jun 2006

How good are today's AV tools?
(or who is winning the arms race?)

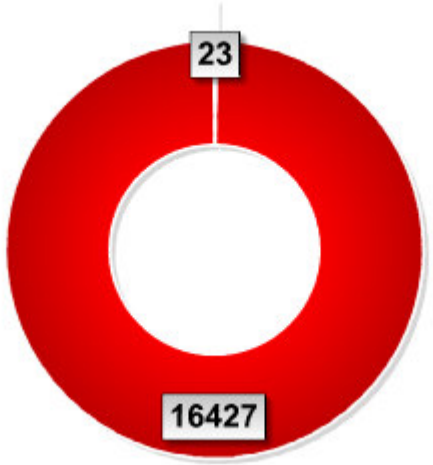
Virustotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines.

Infected / Non Infected (Last 24 Hours)



Red: Infected files
Blue: Non Infected files

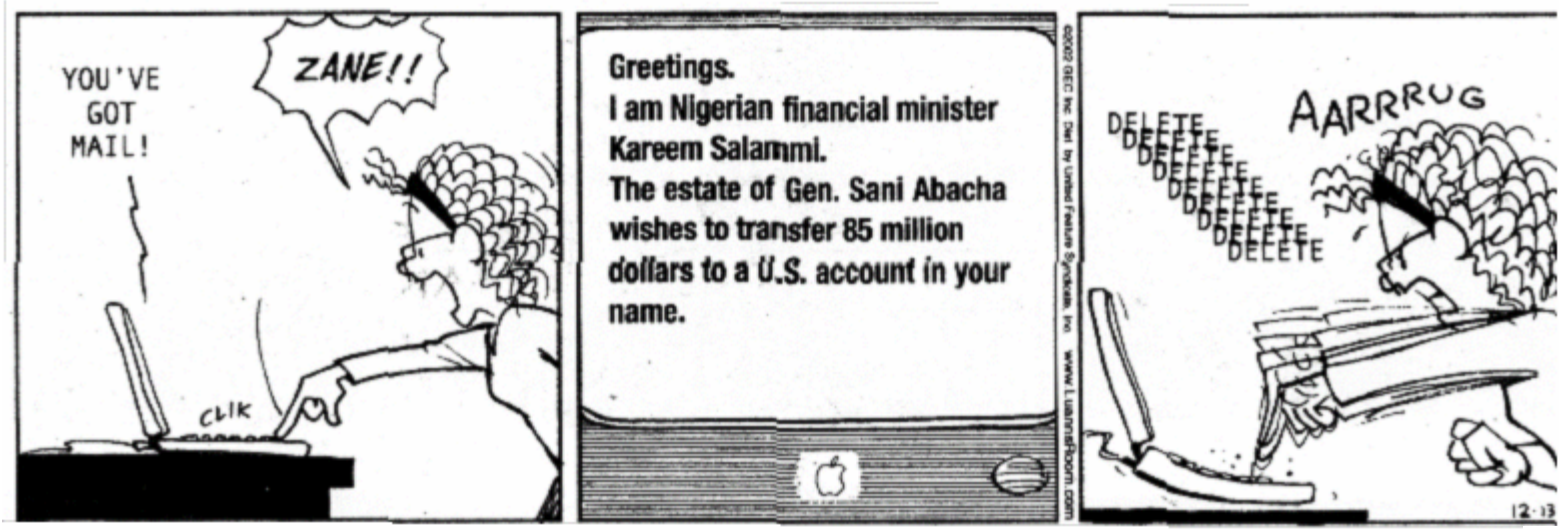
Failures in Detection (Last 24 Hours)



Red: Infected files not detected by at least one antivirus engine.
Blue: Infected files detected by all antivirus engines.

Source: virustotal.com 18th Februar 2008

Social Engineering - Art



- As long as there are people out there who “click here, there will be crime on the Internet.
- The Summer of 2007 saw a polishing of the criminal’s use of professional advertising techniques to get people to “click here.”
- So the Criminal Economy is here to stay.

Storm Worm…catch me if you can!

Why are the miscreant doing this?
The status of the Threat Economy today

Writers | First Stage Abusers | Middle Men | Second Stage Abusers | End Value

$$$ Flow of Money $$$

Under the Threshold

- We've done a good job keeping Networks Up and Running – the Criminals Now know the *pain threshold.*
- Consequence:
  1. Executive Management in SPs are not interested in continued investment
  2. Expertise getting reassigned off SP Security Work
  3. Criminals have bypassed traditional security prevention techniques (anti-virus) and are keeping "under the threshold" of pain.
  4. Vendors are not hearing about "SP Security" from any of their RFP negotiations (i.e. Cisco and Juniper). Vendor Product Management is not making new SP Security innovation a priority.

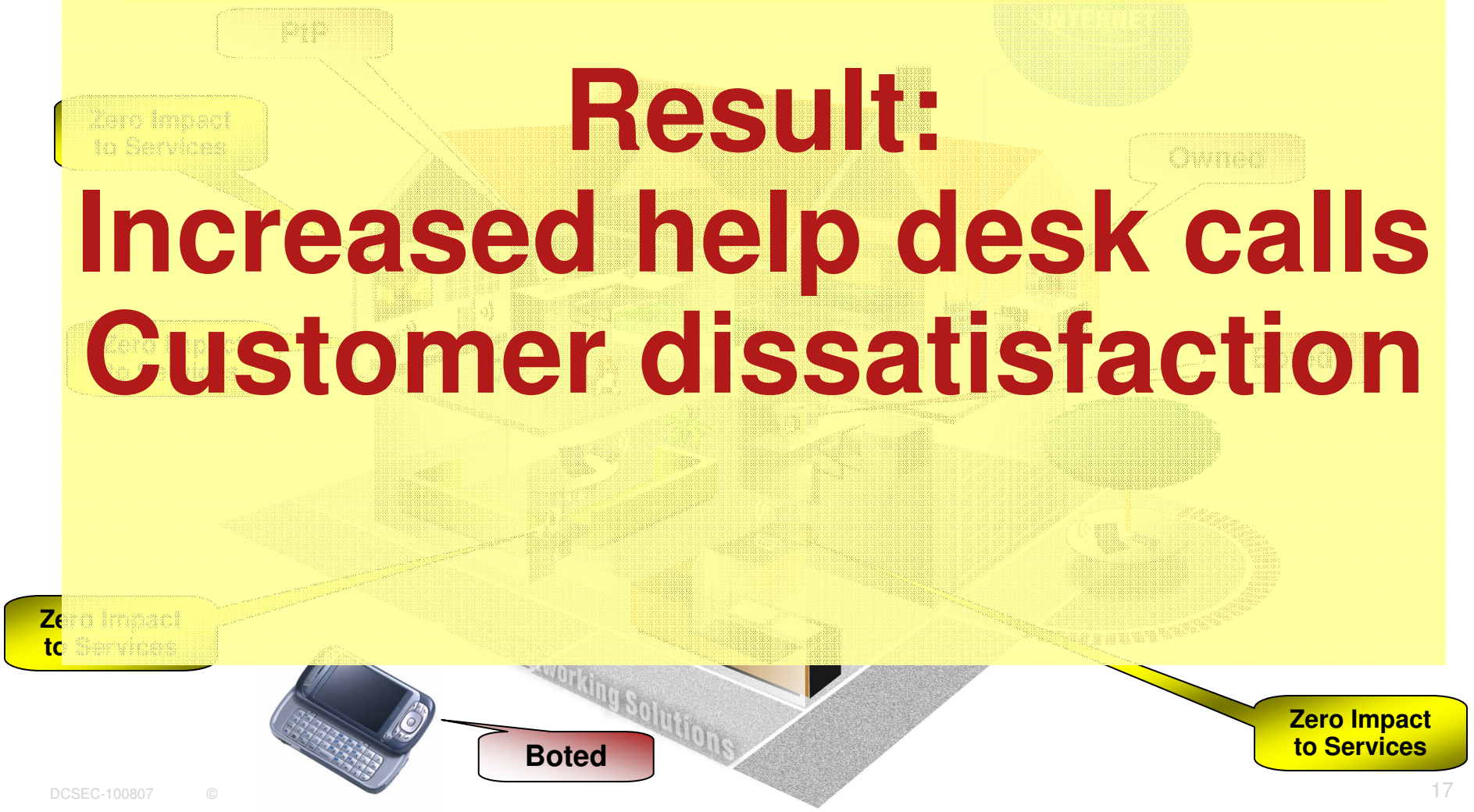
The Principles of the Miscreants

1. Don’t Get Caught
2. Don’t work too hard
3. Follow the money
4. If you cannot take out the target, move the attack to a coupled dependency of the target.
5. Always build cross jurisdictional attack vectors
6. Attack people who will not prosecute
7. Stay below the pain threshold

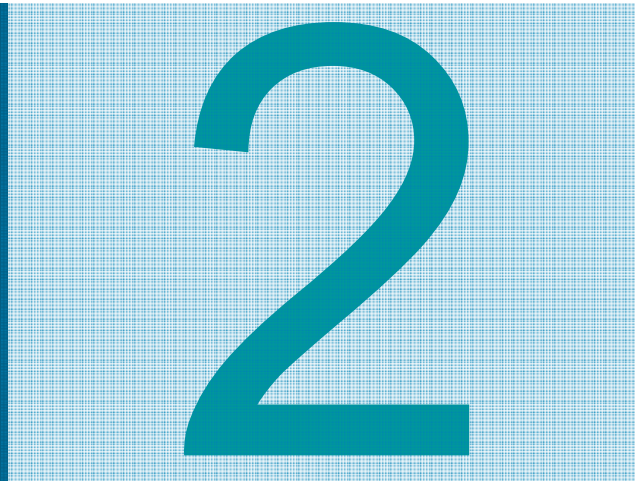
SP point of view:
Offering Services in a Hostile Environment

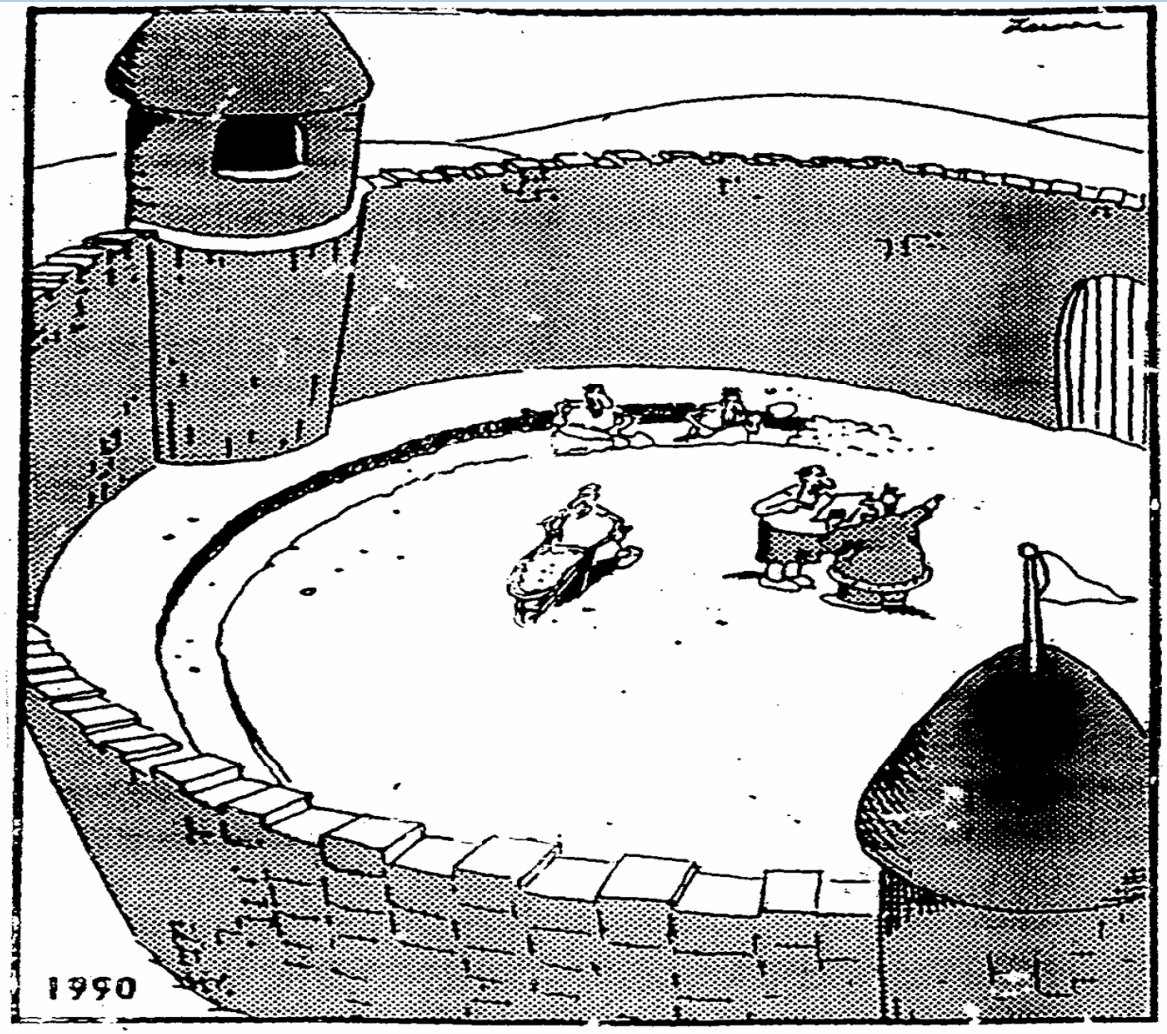
Goal: Service work - No Help Desk Calls!

Result:
Increased help desk calls
Customer dissatisfaction



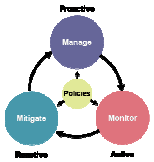
What can we do about this?





Suddenly, a heated exchange took place between the king and the moat contractor.

Cisco Security Framework
Phased Approach



Regulate and Harden

Add Monitoring Tools

Add Mitigation Tools

Add Service Assurance

Today

- Static access lists
- Layer 3/4 firewalls
- Device hardening
- Secure passwords
- Authentication
- Authorization

Static

Phase 1

- User awareness
- Data mining
- Resource monitoring
- Event correlation
- Lawful interception

Phase 2

- Per service policy control
- Per user policy control
- Content filtering
- Dos protection
- Virus prevention
- Worm detection
- Attack mitigation
- Self-defending

Dynamic

- High availability
- High resiliency
- Guaranteed QoS
- SLA assurance
- New services

Increased Profitability

Security Solutions Can Be Deployed in Phases to Achieve Increased Visibility, Control and Profitability

The Importance of Detection and Classification

- In order to operate and ensure availability of the network, we must have the ability to detect undesirable network traffic and to classify it appropriately
- We cannot contain/mitigate what we cannot detect

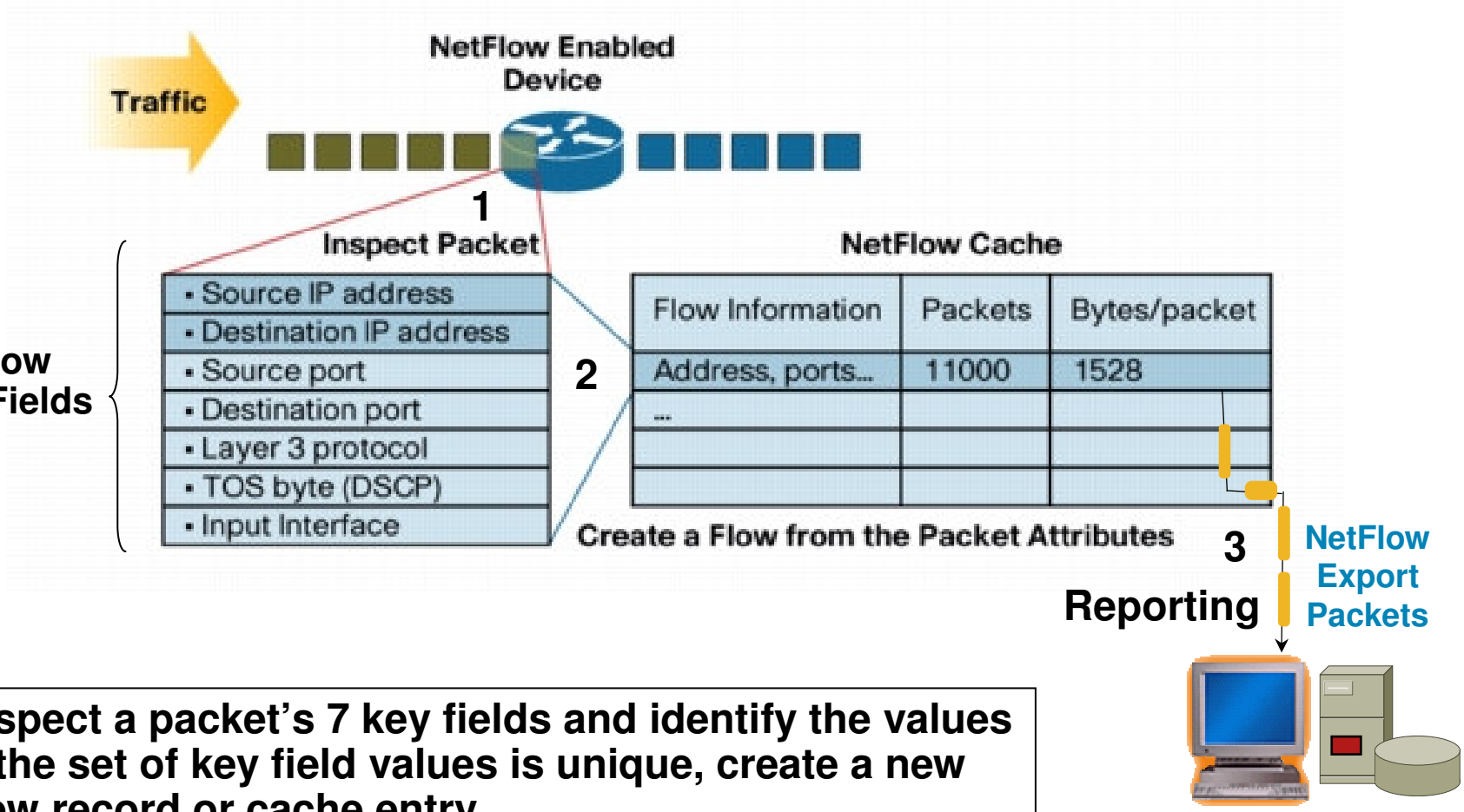
  All the mitigation technology in the world isn't helpful if we've no visibility into threats to network availability

  To detect the abnormal, and possibly malicious, we have to know what's normal—we must establish a baseline of network activity, traffic patterns, etc.
- Classification is key—it provides the context for further action

Detection and Classification

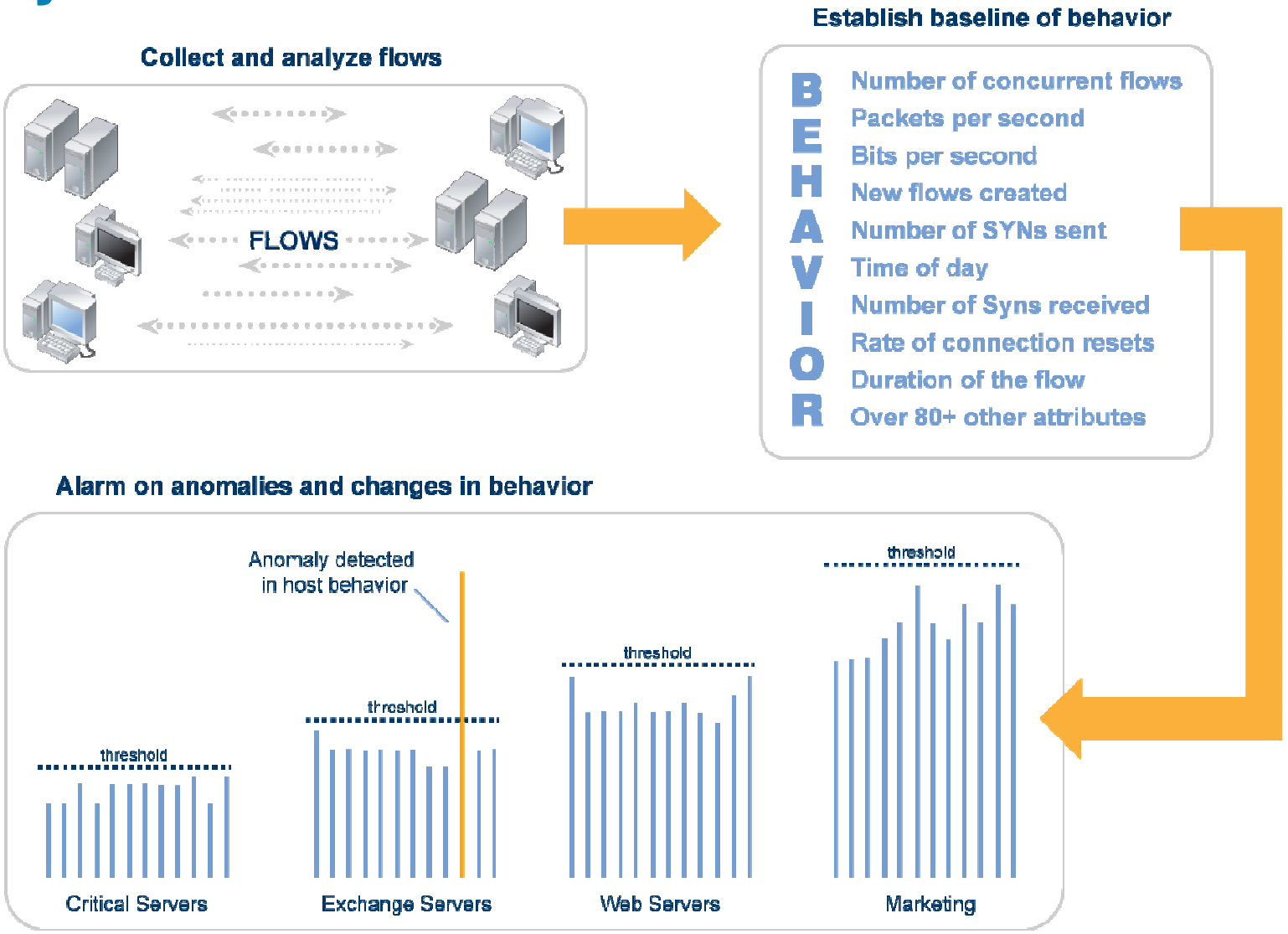
- There are a number of tools & technologies which can be used to get a better view of what is going on
  - –**Netflow** for analyzing traffic patterns
  - –**In-line devices** to control end-users
  - –**Reputation** to validate external sources
  - –**Analysis** of messages/transactions

Netflow:
What Constitutes a Flow?



1. Inspect a packet's 7 key fields and identify the values
2. If the set of key field values is unique, create a new flow record or cache entry
3. When the flow terminates, export the flow to the collection/analysis system

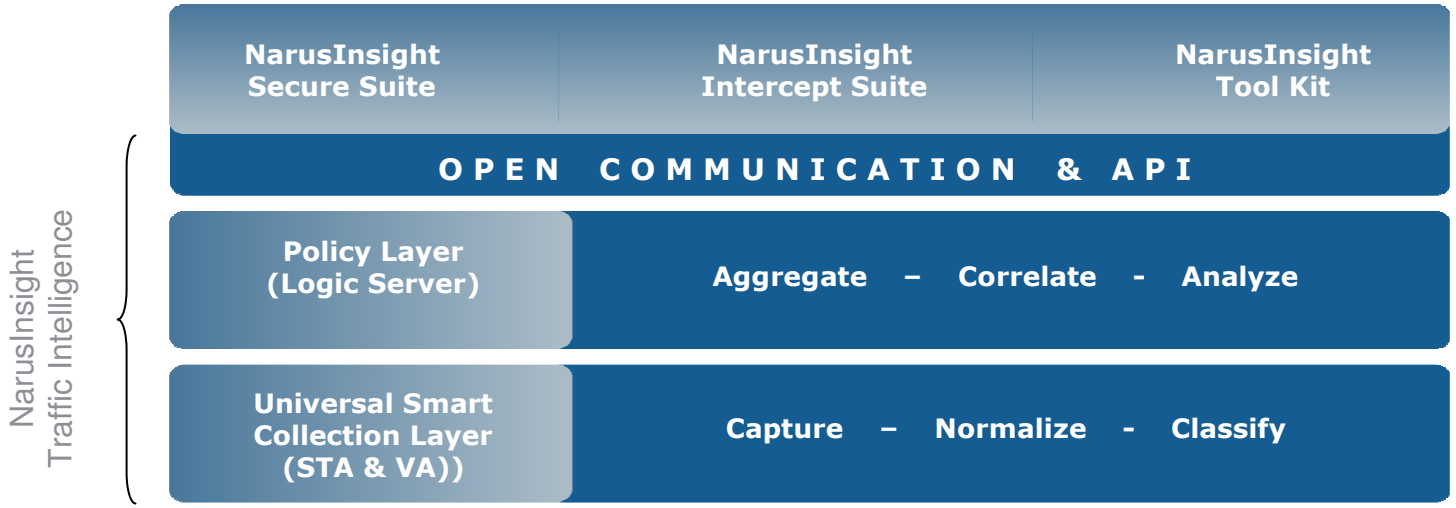
NetFlow Threat Detection: Behavior-based Analysis

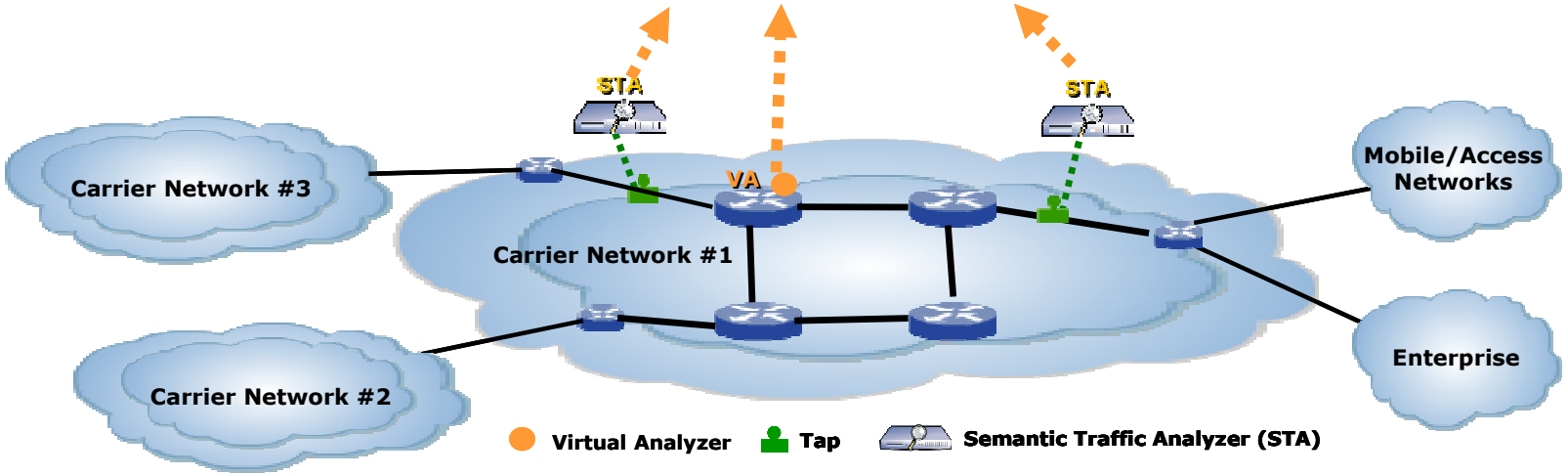


Lancope.
Optimizing Security and Network Operations

Netflow: Total Network View Enabling Total Network Control

NARUS®





Controlling the end-users: Where Is The Root Of The Problem?

- Insecure PCs
  - OS vulnerabilities allow malware to enter
  - Browsers: Either not secure enough or not functional. Hmmm…
  - No clear solution in sight
- Naïve users
  - Run *any* script, *any* program, from *anywhere*??
  - (You can't "patch" silly users)

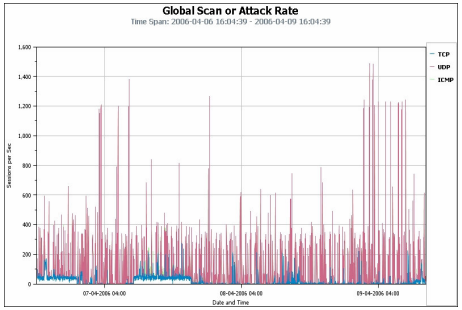
Controlling the end-users: Anomaly Detection with SCE….

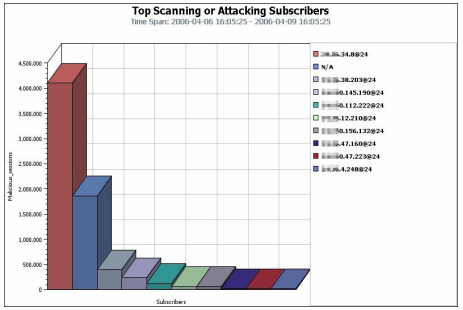
- **SCE anomaly detectors. e.g.:-**

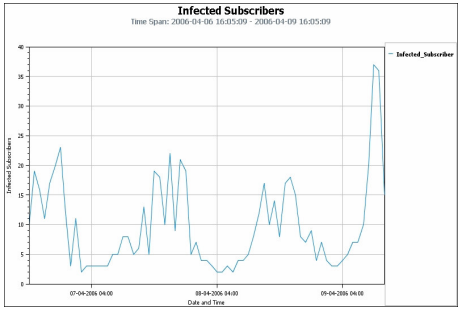
Classify traffic as suspected DDoS once the rate of connections TO a subscriber side IP address exceeds 100 connections/sec of which more than 50% are unidirectional. Disregard IP protocol, port

Classify traffic on UDP port 445 as suspected worm once the rate of connections from a subscriber side IP address exceeds 250 connections/sec

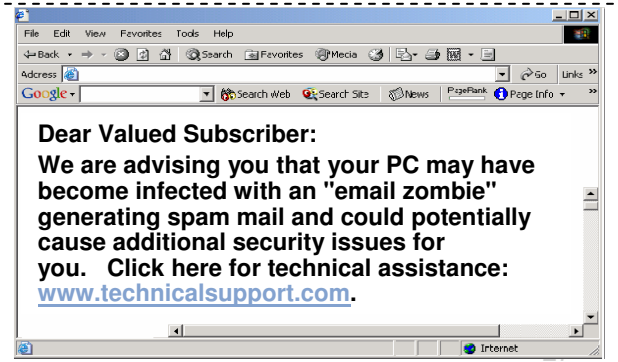
- **Generate reports or SNMP traps:**



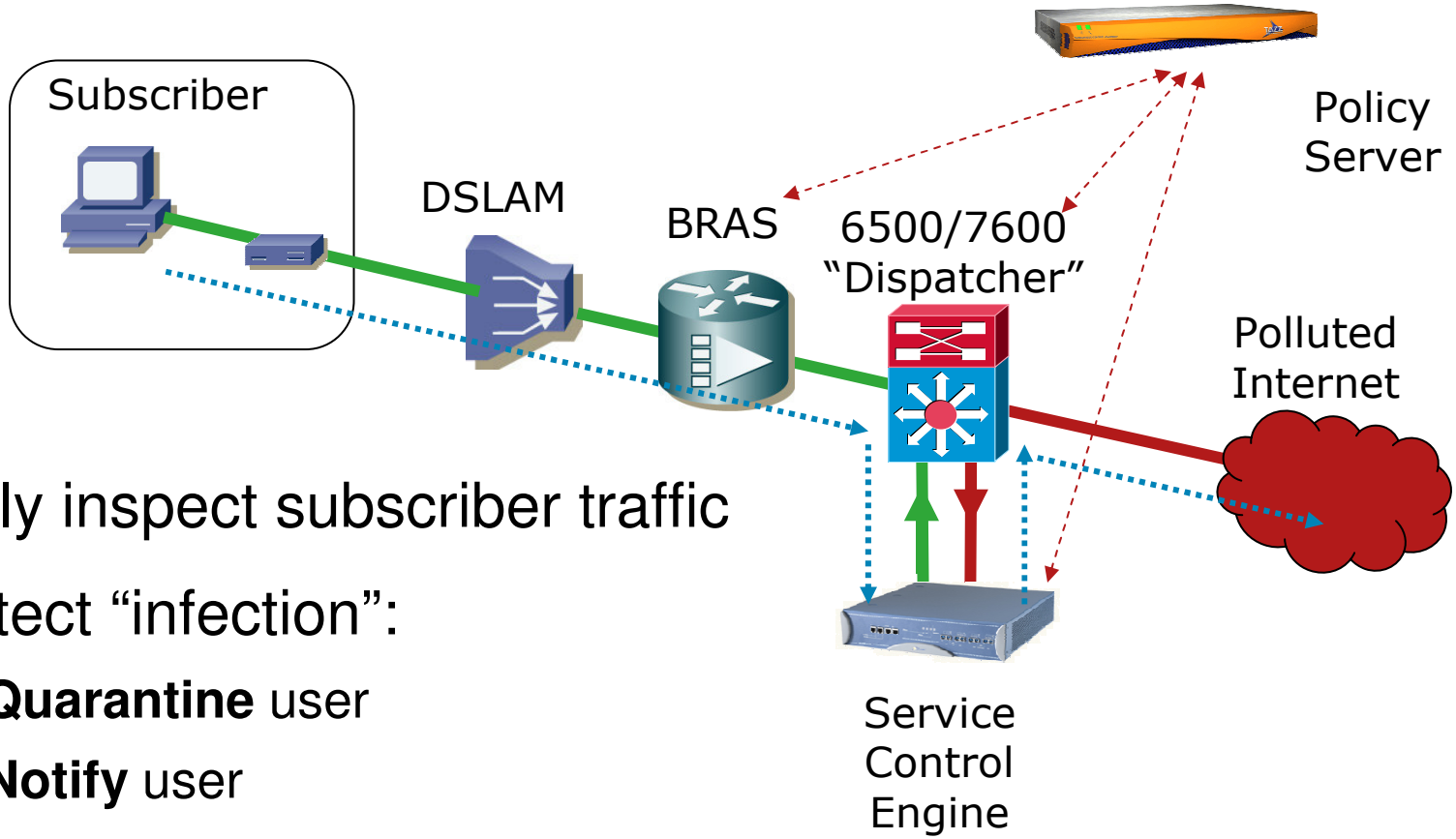




- **Block traffic and/or redirect user for notification**



Controlling the end-users: Subscriber Control



- Fully inspect subscriber traffic
- Detect "infection":
  - **Quarantine** user
  - **Notify** user
  - (**Block** user)
- Not a simple solution

Reputation:
IronPort SenderBase® Network

REPUTATION!

The Dominant Force in Global Email and Web Traffic Monitoring…

- **5B+** queries daily
- **150+** Email and Web parameters
- **25%** of the World's Email Traffic

…Results in Accuracy and Advanced Protection

Spam Caught by Reputation

Ironport	**80%**
CipherTrust	50%
BorderWare	40%

Network Reach (Contributing Networks)

Ironport	**120,000**
CipherTrust	4,000
BorderWare	8,000

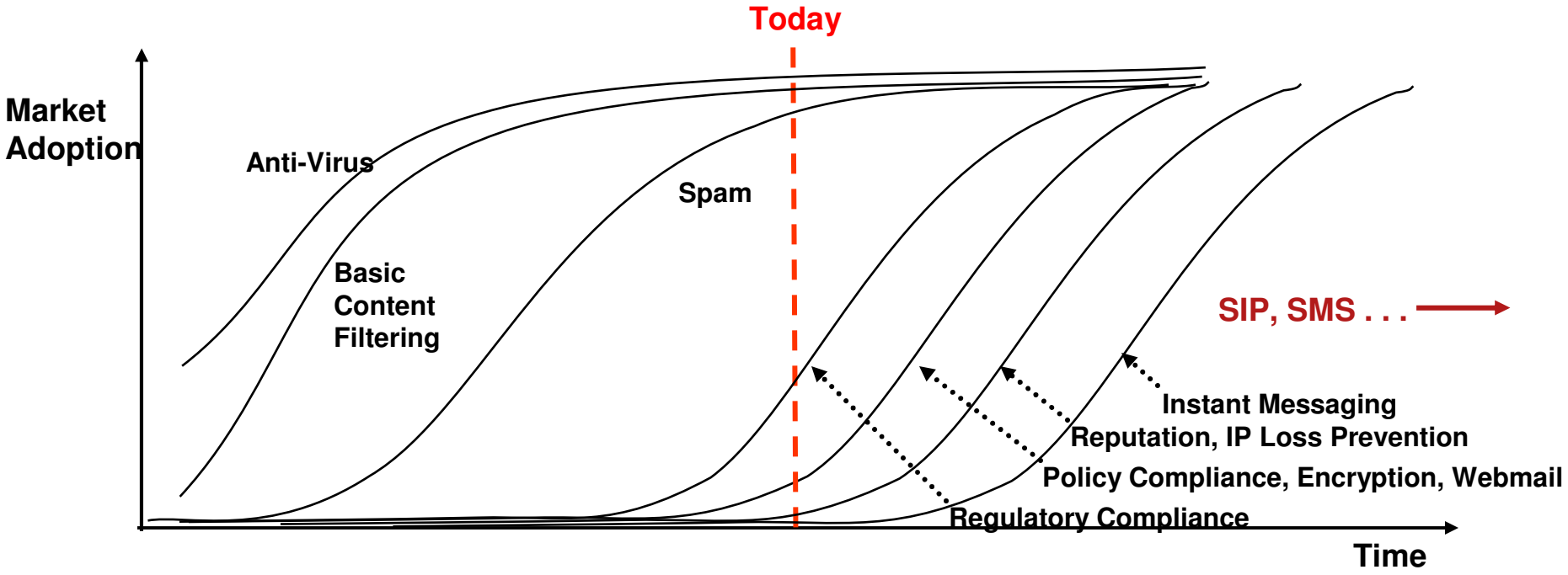
Virus Protection Lead

Ironport	**13 hours***
McAfee, Trend, Symantec, Sophos, CA, F-Secure	

** 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.*

Source: www.ciphertrust.com and www.borderware.com, August 6, 2006

Messaging Security: Rapidly Evolving



- **Messaging represents a large opportunity with new emerging technologies applied across multiple protocols with common management**
  - **Compliance and "data leakage" solutions are in their infancy as are cross protocol solutions**
  - **Reputational technologies such as SenderBase, yield strong synergies with the network**
- **Primary in-bound eMail technologies are mature**
  - **Significant opportunity remains for consolidation of fragmented solutions and replacement of existing Sendmail MTA infrastructure with converged platform → TCO advantages**

Infrastructure availability: