



Cisco Expo
2007

Internet Criminals Why? How to fight them



Henrik Davidsson
Nordic Territory Manager
IronPort, A Cisco Business Unit



Pop quiz

1978

First spam

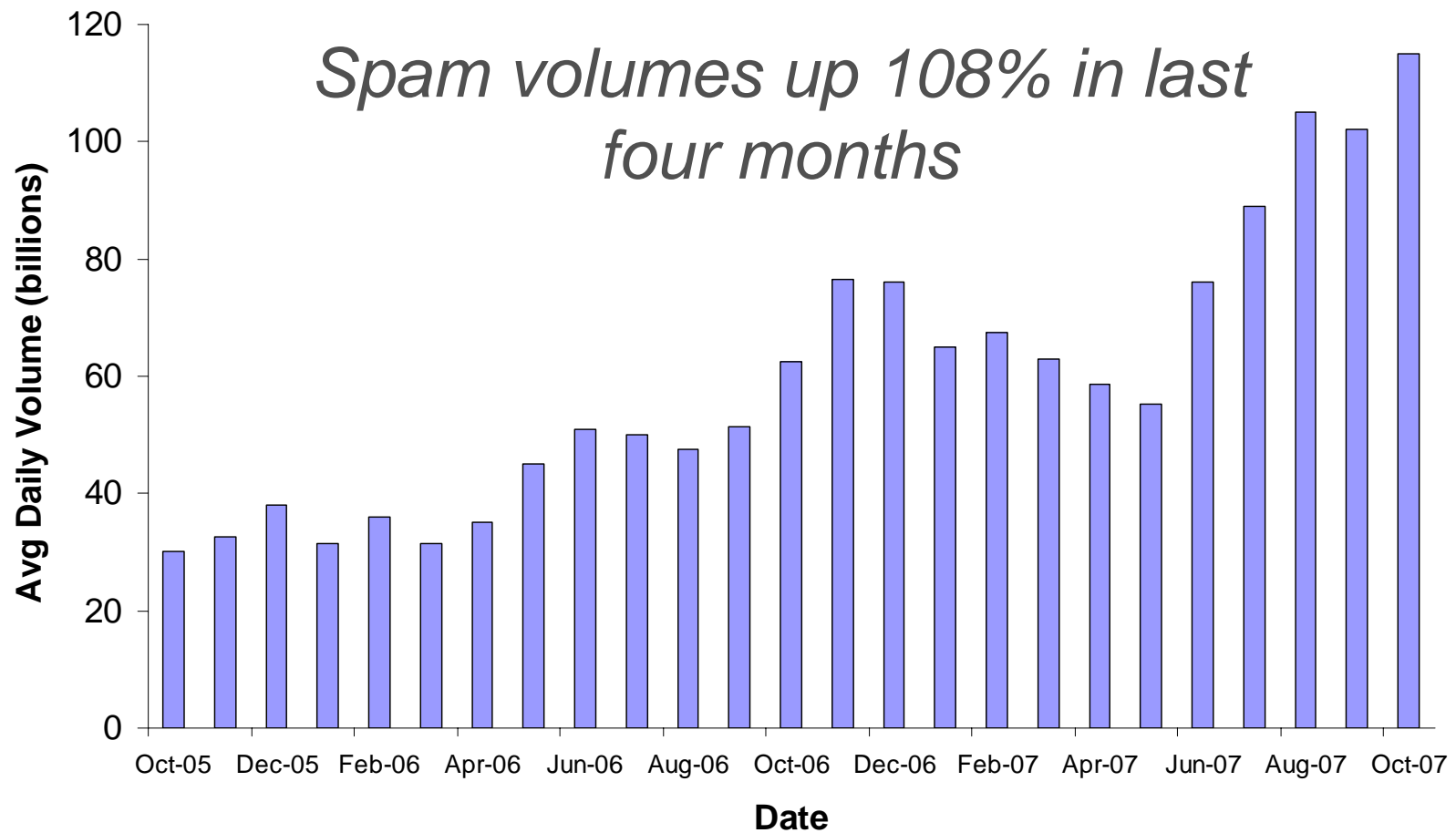
(Digital marketing rep send email to every ARPANET address)

Why?

Payment for period from Jun 24th 2004 to Jun 30th 2004	\$13,371.30
Payment for period from Jul 1st 2004 to Jul 7th 2004	\$15,941.00
Payment for period from Jul 8th 2004 to Jul 14th 2004	\$17,455.50
Payment for period from Jul 15th 2004 to Jul 21st 2004	\$2,027.70
Payment for period from Jul 22nd 2004 to Jul 28th 2004	\$5,147.50
Payment for period from Jul 29th 2004 to Aug 4th 2004	\$11,085.00
Payment for period from Aug 5th 2004 to Aug 11th 2004	\$14,369.00
Payment for period from Aug 12th 2004 to Aug 18th 2004	\$10,029.60
Payment for period from Aug 19th 2004 to Aug 25th 2004	\$12,235.00
Payment for period from Aug 26th 2004 to Sep 1st 2004	\$10,888.20
Payment for period from Sep 2nd 2004 to Sep 8th 2004	\$4,989.80
Payment for period from Sep 9th 2004 to Sep 15th 2004	\$11,461.75
Payment for period from Sep 16th 2004 to Sep 22nd 2004	\$19,422.25
Payment for period from Sep 23rd 2004 to Sep 29th 2004	\$14,033.55
Payment for period from Sep 30th 2004 to Oct 6th 2004	\$16,855.40

Spam Trends

Through October, 2007





Global outbreak of MP3 spam begins

by [Matthew](#) posted on October 22, 2007 1:39 pm

Excel Latest Vehicle for 'Pump-and-Dump' Spam

DATE: 24-JUL-2007

By [Brian Prince](#)

Next Menace: PDF Spam

As image spam declines, a new type of pest takes its place.

[Cara Garretson](#), NetworkWorld

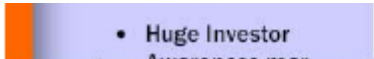
Thursday, July 12, 2007 6:00 AM PDT

PDF spam

```
>DIA'A ^ [DIT@IEJ1' O~:80*ac~D UAO~D
YDDVDw""iá×D_i+simT××8D'iýÏ,,36ÈD)Ù `zZÐÈB×æ×8D.íéáµ cg|[,Yá:v9SG<ÖTyíãBÐ`Áái)áoI`Dí++×1D^tuP»^DÖ4*÷¿*V'
DpÓÈ`fxDDN`¿òÈX»
DÁ-(ÉúçTÄ7;GJ-^`ÁReæ5^: `Á)Üi`"æèD×DÇ£,W&eDóó'YíuÔDÚ^ `D^`FCâÖµ<) "°D
êçây56NQ»DÈÈ`û41...1!s~,,D9Ö@DÖPzmGDÐDL...D4+wÈ7£|f}â' &-qPÝ£BèiDØ2ySÜ,D
)
%DA^PÐD-^ñÁúh~ydøD[ `DD

b vÍ!à...QD,Xé5q,,VàµD2...š
ÙN£^>D-D`D`D6; >`YünD`iDnYðíóD#ÁEÓDz-Ú>DÛÉ3D;YZiúíDdø`ÈSsq·ìPÿ-ÀDñ;+d^á+D€-³Cš:,ÊKZP±>NÀ      äk»,, 'št8U..ÁDDžÁ:
³ÉÉD-D±æYGn$Ö²4"DÈm%3wR~ `Öž+ì

Á(èw^-`ãDriñ«æ'è;ÖPuÈ@s YDÁ{:%Dí!`°S-,^`D×%]Á@·8cÓ-8,áÈ`8áðçDòD      5µH-±òÑ«»DD·Á?"EèàÖŠ<`#ŠÒ-ED_ =ÁÛ3@IÖ+ì,³
gòäNÐYD 3¿...?DN1"ó(š1@È<G $DÄjý_x^ÁDóó@XD
á`Ô`sq,a `»Ú µM±D-FI@Oz·ÁB$×ç+,   DÍSD(iDá`WÖ|úžùž;PY€DÛD.ñÝ<D Dòø%Î-D|P£·á+ÍDlÁÚbDß=»öý Ó«L"o×D(w#ÈØlèeá7'
YiD×V¿±Á!t,,CDuèÄ%çYKDDÀNDð;E`H×6ðS(zD...  ×š¿šHÄ]uc;D
Hh&' $Ø/;Dfñá0¿3^DÁD-È1Y^0E+*Yc      D)P²óDf3MìDDÙ/O%rDfi4Ö(%•D
tDÈ"€D["Y;Dá`DÍ,,`d;^"DD(`T` `c$Vc%Ye-J6^ò
D;)+ñD...DTONDMR&YW DjDfT%òÜ`Dæc×DíD/fq;úÄ8ÇÈw;D; ;ò>Á`DDIæCHtš»DØ,äòq¿$ðDwDJD!"F)D
-×æñ%à`%D>ÀcQé` `!ää@iDèòðDZÖP^D3v D'RRS-ðLO-ìiòÍ`QW÷ÍD
HDDx-D`ÌT-m$ E ñúDDu/{Öá=c£'t,`DÇ·Ö1Ñ-kø_@wÖ
AqIXDù-
EC/DU,ò#X(ÍjD"+,àçóDæúYÁÖŠ;ìDMDò<ÉDÝTS»£ÀTð+çBbÄDKE`š9T:ß"³DDÛtè` )O`Ä...5[|;qqDU>`@qDæD...%
@Kµ+èDD%#G"„AzètæDCCÜ;D9A`q`ø#Ý>D10pqDtd&(E)gsÛgÇ]µj[yÄ°",DDüoD `ÈD
endstream
endobj
```



• Huge Investor

campaign starting next week, we are expecting our German

media before making any investment decisions. We feel

this one - **DON'T LET IT PASS YOU BY!**

Excel Spam

July 21st, 2007

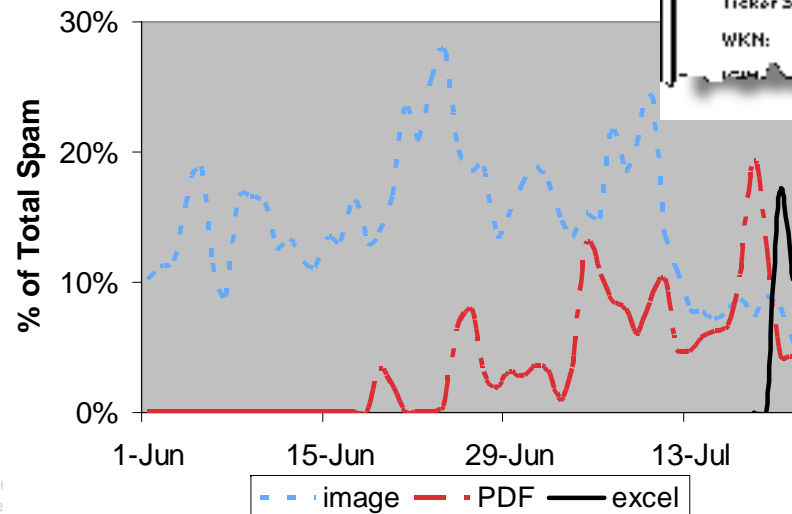
OUTBREAK DESCRIPTION

- Spam sent as text inside excel file
- First appeared July 21st, 2007
- Within hours, represented 17% of spam volumes

EXCEL SPAM EXAMPLE



SPAM VOLUMES BY TYPE



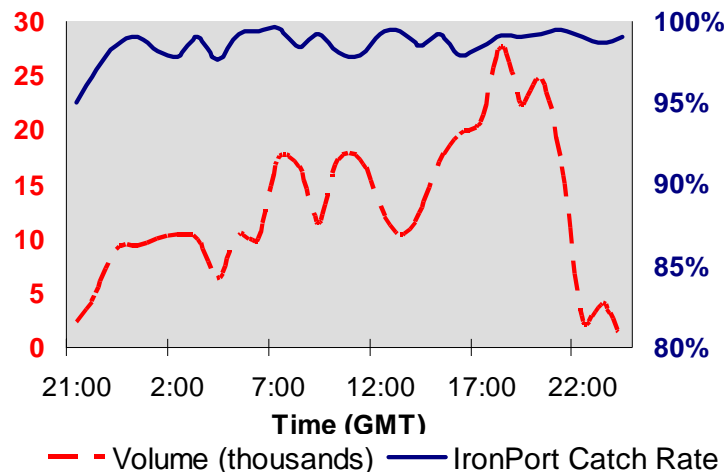
MP3 Spam Outbreak

October 17th, 2007

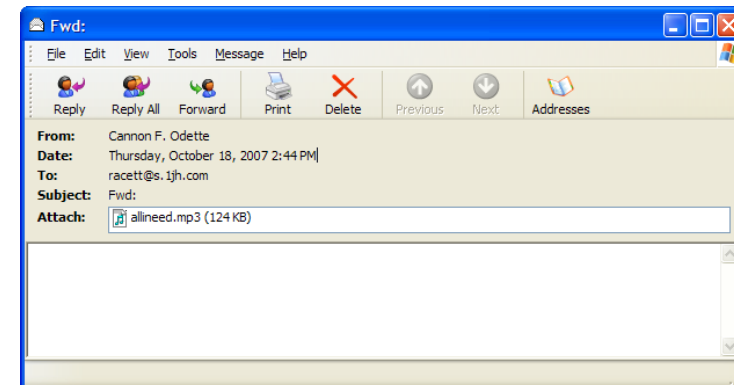
Outbreak Description

- Spam sent as MP3 audio files
- files named after popular songs / musicians to fool recipients
- files randomized by changing audio speed and content
- represented 1% of spam volumes on day of outbreak

Volume & Catch Rate



MP3 Spam Example



IronPort Protection

- Stopped MP3 spam within minutes through combination of several technologies
- **Reputation Filters:** proactively blocked majority of MP3 spam by identifying bots sending spam
- **IronPort Anti-Spam:** issued rules based on file type, file content, message size and other information to catch remaining spam

Storm worm

- ~30% spam 3 weeks ago
- Responsible for one of largest Web-based malware attacks

this is not good. If this video gets to her husband your both dead
<http://www.youtube.com/watch?v=cXJn6wLPOr7>

- Storm worm every 30 minutes
- Est ~10-50 million infections worldwide

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

Messages Maillists Rotation Settings Proxies Advanced Test

SpecialOffer ID: ombt1115 New Save Delete

FROM Emails: FROM Aliases: TO Aliases: Attachments:

webmaster@indatate Webmaster
 testdirectv@yahoo.co Postmaster
 johntacker@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.

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

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.

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

Botnet Command & Control Page

Go to botnet controller Compress logger.txt to logger.gz

Remark: displayed only online socks (socks that was in online in last 20 minutes)
 Remark: to copy IP or ID to clipboard press button "copy IP" or "copy ID"

Select by country: All countries

Select by state: all








IP of infected computer connected to C&C node - Real-time list

Current country selected: all
 Current state selected: all

List							
IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION	
Copy IP 70.178.130.171	57253	Copy ID XPCNZBSCWZLCZTZCXFLKHVDJQXPVKO				1	
Copy IP 72.153.6.139	39112	Copy ID NMAWFUNDOTCUJFLZUQUPSCLMFMUATC				1	
Copy IP 86.138.210.148	31295	Copy ID KQAPBQXEYGHBJTYURAHGQUHSPGAPEUR				0	
Copy IP 70.229.125.18	32924	Copy ID DWYFSDPYDIORNSFYXIOSUOAFMDBGHTC				1	
Copy IP 84.9.86.199	51169	Copy ID BSYOUMQEPSSERBFTBIRFOHCKSHJUWKA				1	
Copy IP 68.96.235.136	21535	Copy ID KPNZBYSPUPZENYWEQNFUAUWFLFMSRBY	United States	Atlanta	GA	1	
Copy IP 70.232.92.129	17167	Copy ID USPVOTVLNTDYFLAZTNJSSUELRFKOPW				1	
Copy IP 87.74.45.27	40415	Copy ID CJKIXMIRLOZTFLSTLQSUZUPUWMJSGOM				1	
Copy IP 24.186.245.152	55147	Copy ID ATOTJDEXFOIDCNDJPALJRXKABULYKEU	United States	Lynbrook	NY	1	
						Total: 10	

What's stored on the C&C node?

Index of /uk

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	03-Aug-2006 13:12	-	
 check.php	12-May-2006 18:43	1k	
 dupes.php	12-May-2006 18:43	1k	
 logger.php	12-May-2006 19:00	1k	
 logger.txt	10-Aug-2006 18:37	211M	
 socks.txt	10-Aug-2006 18:38	1k	
 socks/	25-May-2006 09:55	-	

Apache/1.3.34 Server at www.yops.biz Port 80

211 MB file...

Excerpt from
211 MB file

Malware
uploads
keystrokes
to C&C
node

```
botnet controller excerpt - Notepad
File Edit Format View Help
-----
REMOTE ADDRESS: 172.189.109.174
ID: BPAQZLZBBLUWRYGVXOTJHALUVNRBXS
TIMESTAMP: 25\5 14:0:51
Copyright By Smash and SARS
From: MATTHEW

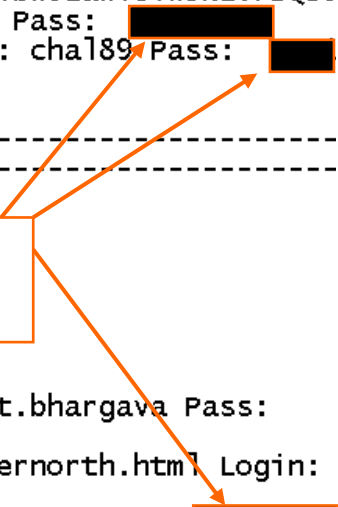
Windows XP
Internet Explorer 6.0.2900.2180

*****
MAIL: POP383EE26C0
Cha189
PAUL
10.0.0.4
http://petiteteeniemia.join4free.com/_B64S_bm9kZwQvNjYvbw92awVsYw5kL0FBQS9
TMxNDk30TQ2L2ZBdi5UZGY5SEJscUU=_E/ Login: cha189@aol.com Pass: [REDACTED]
10.0.0.4 http://sib1.od2.com/common/Framework.aspx Login: cha189 Pass: [REDACTED]
10.0.0.4 http://uk.mcafee.com/root/login.asp
*** Protected Storage Data ends ***
-----

REMOTE ADDRESS: 125.23.22.246
ID: KOBERVBOUKQIPXGITBBFSQWSGXJFUMO
TIMESTAMP: 31\12 19:47:37
|
.....

*****
192.168.1.2 http://in.rediff.com/index.html Login: puneet.bhargava Pass:
*****
192.168.1.2 http://north.airtel-broadband.com/touchtelusernorth.html Login:
*****
192.168.1.2 http://sv2.freewh.com/index.php Login: udit_2001 Pass: [REDACTED]
*****
192.168.1.2 http://www.airtelworld.com/ Login: udit_2001 Pass: [REDACTED]
*****
192.168.1.2 http://www.airtelworld.com Login: 01152458021 Pass: [REDACTED] i
*****
192.168.1.2 http://www.cooltoad.com/go/login Login: udit_2001 Pass: [REDACTED]
*****
192.168.1.2 http://www.cooltoad.com/go/setup Login: udit_2001 Pass: [REDACTED]
*****
192.168.1.2 http://www.indianmoviesclub.com/board/forumdisplay.php Login: ud
*****
```

Website
passwords



Crimeware

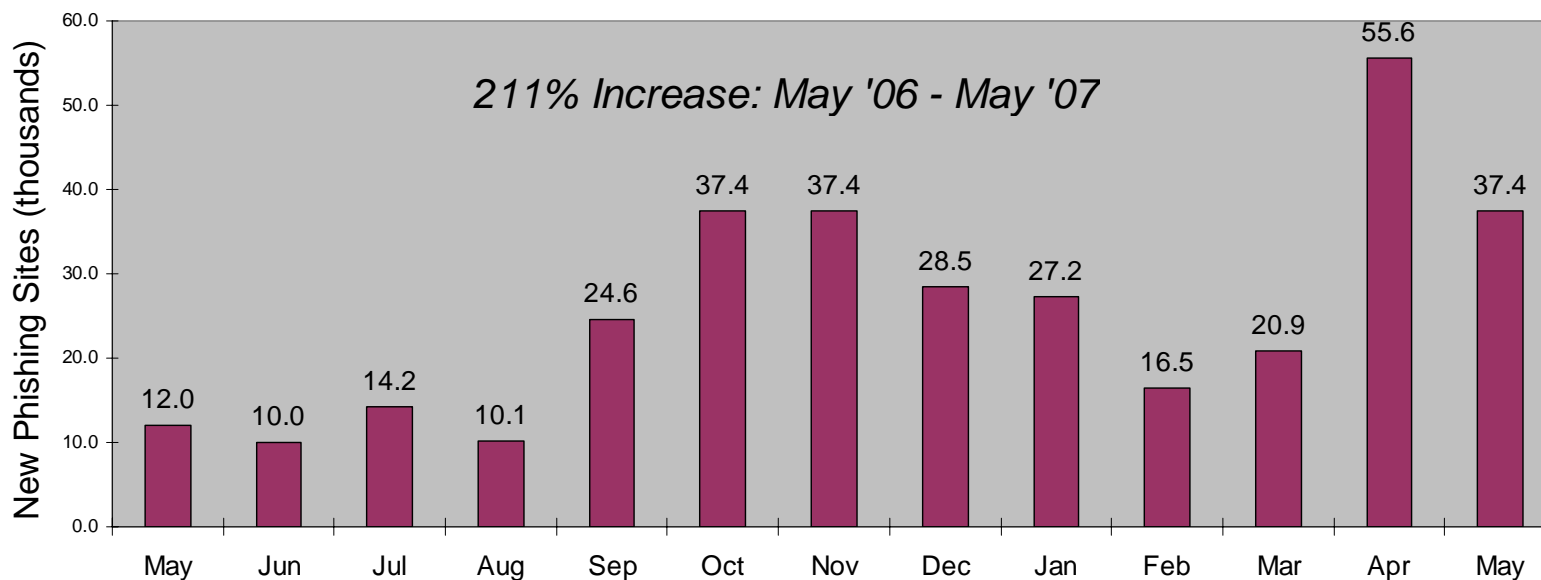
What is Phishing?

“Use of 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.”

- Anti-Phishing Working Group (apwg.org)

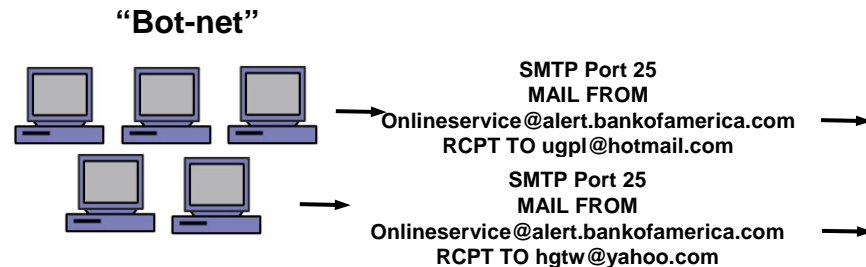
Facts & Trends

- 97% of phish attacks target at financial sector brands
- 33% of phish sites host malware
- Phish sites online on average of 3.8 days
- US business estimate loss at \$2bn per year

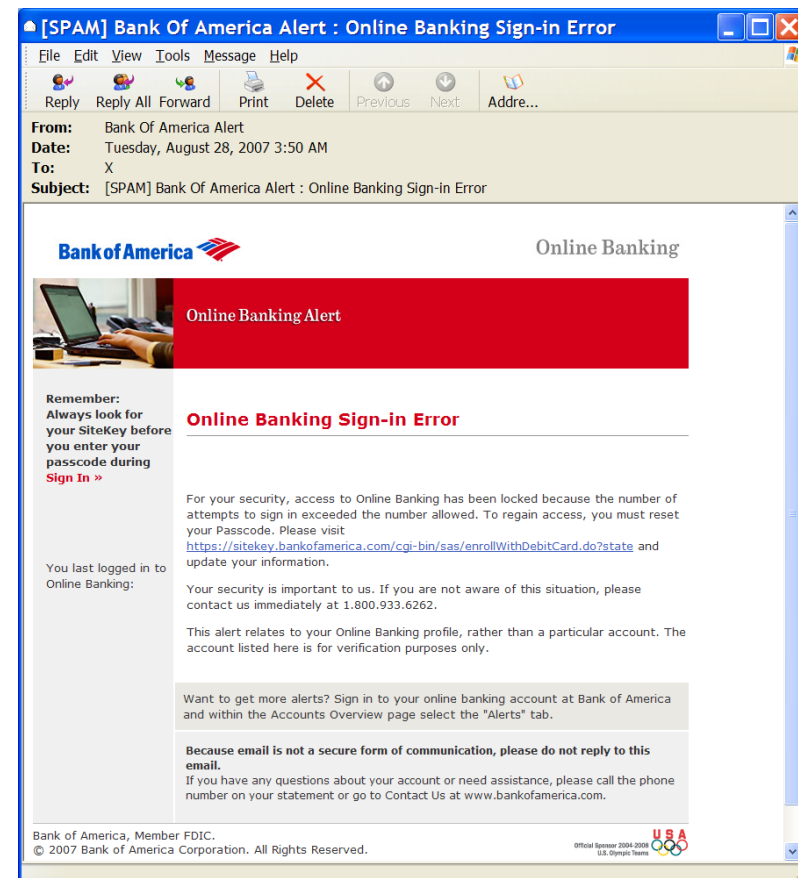


Typical Phishing attack

- 1 Obtain mailing list (hack/buy)
- 2 Build website & register domain
- 3 Send millions of phish mails to list



- 4 Wait for account/password details & remove money



IKEA

Subject: Ihre IKEA Rechnung
Date: 2007-02-19 10:33:21

IKEA® DEUTSCHLAND
Ihre detaillierte IKEA Rechnung

Rechnungsnummer 656 975 488 7945
Kundennummer 888 516 2132
Datum 10 Februar 2006

Sehr geehrter IKEA Kunde,

die Gesamtsumme für Ihre Rechnung beträgt: **287,81** Euro.
Anbei erhalten Sie den detaillierten Rechnung sowie die alle anderen wichtigen Unterlagen zu Ihrem Bestellung im beigefügter ZIP Datei.

Kopie dieses Schreibens wird Ihnen gleichzeitig auch per Post zugeschickt.
Die Unterlassung rechtzeitiger Einwände gilt als Genehmigung. Weitere Informationen zum Widerspruch finden ebenfalls im beigefügten Dokument.

Gemäß der erteilten Einzugsermächtigung werden wir den Rechnungsbetrag in den nächsten Tagen von Ihrem Konto einziehen.
Ihre Rechnung ist im PDF-Format erstellt und mit einer "Digitalen Signatur" unterzeichnet worden. Den entsprechenden Verifikationsbericht finden Sie im Anhang dieser E-Mail.
Durch die "Digitale Signatur" wird Ihre Rechnung nach dem Signatur-Gesetz (SigG) anerkannt.

Um sich die Rechnung anschauen und die Signatur prüfen zu können, benötigen Sie den Adobe Reader, Version 7.0 (oder höher).
Sollten Sie keinen Adobe Reader besitzen, können Sie diesen kostenfrei auf der Homepage von Adobe downloaden: <http://www.adobe.de/products/acrobat/readstep2.html>

Targeted & Blended Attack #1

Purported email from US IRS



The screenshot shows the CNET News.com website interface. At the top left is the CNET NEWS.com logo. To the right is a search bar with the text "Search:". Below the logo and search bar is a navigation menu with buttons for "Today on CNET", "Reviews", "News", "Downloads", "Tips & Tricks", "CNET TV", "Compare Prices", and "Blogs". Below this is a secondary navigation menu with links for "Business Tech", "Cutting Edge", "Access", "Threats", "Media 2.0", "Markets", "Personal Tech", "Blogs", "Video", and "Ext". The main headline is "Top executives face personalized e-mail attacks" in large, bold black text. Below the headline, it says "By Tom Espiner" and "Special to CNET News.com". The publication date is "Published: July 2, 2007, 6:29 AM PDT". A yellow highlighted box contains the following text: "Complaint Made by Consumer Mrs. Marcia E. Worthington", "Complaint Registered Against: Scott Banister of IronPort", and "Date: 05/09/2007/".

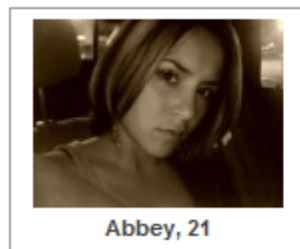
Complaint Made by Consumer Mrs. Marcia E. Worthington
Complaint Registered Against: Scott Banister of IronPort
Date: 05/09/2007/

Scam Phishing Trojan

- **BBB Phishing Trojan**
- Highly-targeted attack – aimed at specific executive-level company managers
- Steals **all** interactive data sent from victim's IE browser to remote websites
- Uses browser helper object to access form data before it is SSL-encrypted
- One stolen data repository located. As of Friday, May 25, there were **1, 500 victims and >150 MB of data** in the repository. Approx 70 megabytes of data is being collected daily

Blended Threat #3 :Social networking

- Profiles attract requests



You have a new comment!

Abbey says: hey, i swear i know ...

[View Comment](#)



You have a new friend request!

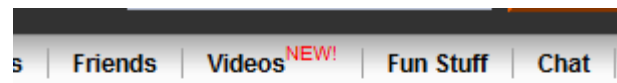
Please accept or reject by clicking below...

[Click here](#)

Page shows personal details to contact

Site contains malware

- 2 weeks later



This account is no longer available !

Phishing

- Large rise in phishing attacks in 2007
- 1/3 phish sites now host malware cocktail
- “Single use” Phishing URLs. Redirect after first page visit.
- “Rock Phish” Kit
- Fast flux dns
- Rock Phish Example

Host mqsul.cd configured for phishing attack. (CD is Congo TLD, server in China).

Single server hosts 10 attacks:

Key Bank: <http://accounts.key.com.startsession.mqsul.cd/sc/info.asp/>
Bank of America: <http://ba-ca.onlinebanking.com.de.mqsul.cd/i/a/index.html>
E*Trade: <http://global.etrade.com.memberdirectory.mqsul.cd/member.do/>
National Bank: <http://ib.national.com.au.confirmationpage.mqsul.cd/sc/isap/custcare/index.asp.htm>
German Bank: <http://meine.deutsche-bank.de.webxobjects.mqsul.cd/dbpbc.woa/>
German Bank: <http://sparkasse.de.redirector.webservices.mqsul.cd/do.asp/>
German Bank: <http://www.berliner-volksbank.de.navigation.mqsul.cd/i/s>
Barclays: <http://ww4.barclays.co.uk.brcccontrol.taskstart.custbase.mqsul.cd/detailsconfirm/>
Fifth/Third: <http://www.53.com.bankingportal.session.mqsul.cd/sbcbconfirm>

Web site attacks

- Legitimate websites hacked

Superbowl site hacked earlier this year

Bank Of India

The Bill...

Even Irish

Crackers Turn Toward Web Site Attacks

- Current te
realtime

Source: [IT Business Edge](#) | Priority: [Fortifying Network Security](#) | Topic: [Network Security](#)
Date Published: 4/13/2007

With Billy Hoffman, lead researcher, [SPI Dynamics](#). Hoffman spoke at the Shmoocom conference last month in Washington, D.C.

- Web site p
..easy att

Question: How much danger are Web sites facing?

Hoffman: We don't know how often someone gets breached. Some organizations try to track whether there is an increase in attacks, but they don't know. I've heard that 80 percent of attacks go unreported. So we are not dealing with the full picture. It certainly is on the rise.

Cyberterrorism

- Phishing/spam for harvesting credit card details
37,00 cards /\$ 3.5m in fraudulent charges
Launder money through gambling sites
- Trio used stolen credit card accounts to set up a network of communication forums on the net
- Sites hosted with tutorials on computer hacking, bomb-making, videos of beheadings and suicide bombings in Iraq
- Legal team - "The trouble is I don't understand the language. I don't really understand what a Web site is"



Terrorism's Hook Into Your Inbox

U.K. Case Shows Link Between Online Fraud and Jihadist Networks

By [Brian Krebs](#)

washingtonpost.com Staff Writer

Thursday, July 5, 2007; 2:34 PM

The Amateur



Jeanson James Ancheta

\$60K from Adware on 400K PCs



Loudcash (now ZangoCash)

– \$0.40 per install

“Every day, 7,500-10,000 ZangoCash affiliates distribute our software to users who are then connected with more than 6,000 MetricsDirect advertisers.”

The Professional Criminal



Sanford Wallace



Smartbot.Net Malware

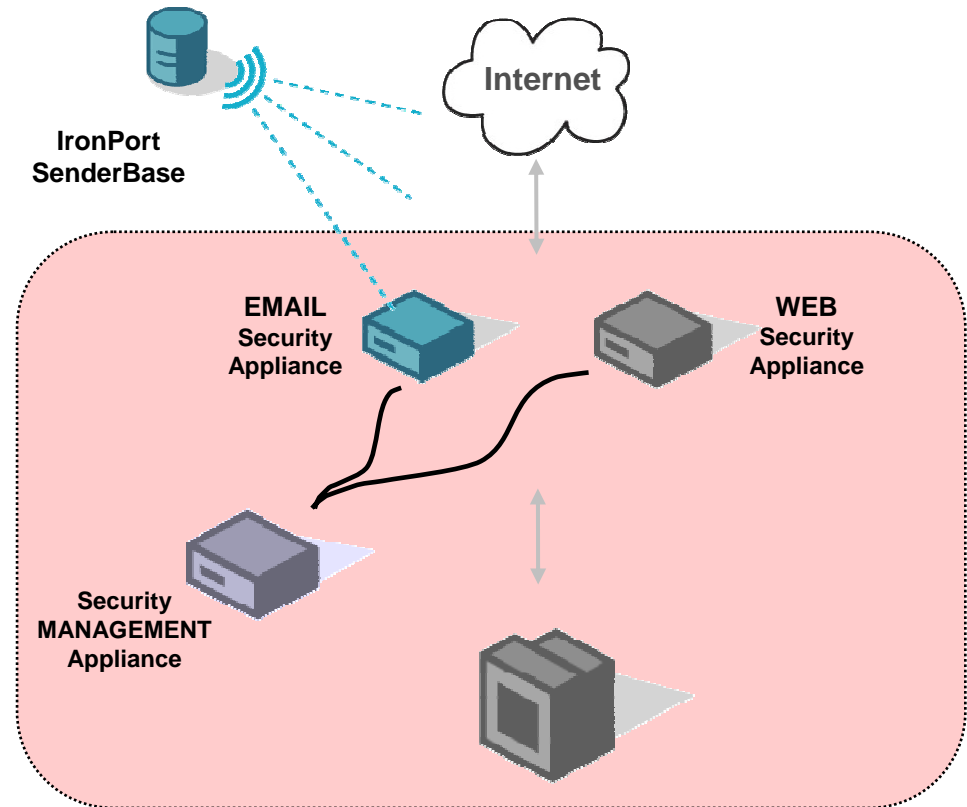
- Opened CD-ROM tray
- *"If your cd-rom drive's open . . . You DESPERATELY NEED to rid your system of spyware pop-ups IMMEDIATELY! Download Spy Wiper NOW!"*
- Spy Wiper and Spy Deleter sold for \$30

\$4M FTC judgment

What is the tool you need?



The IronPort Vision



Web Security

Email Security

Security management

Reactive Security



SenderBase® / Threat Operations Center

SenderBase



TOC



- **Expert** team of skilled analysts
- Staffed **24 x 7 x 365**
- **32 languages** spoken
- **Documented & verified** processes

+ than 90 parameters

- *Data Volume*
- *Message Structure*
- *Complaints*
- *Blacklists, whitelists*
- *Off-line data*

E-Mail Reputation Filters



Reputation Score

+ than 45 parameters

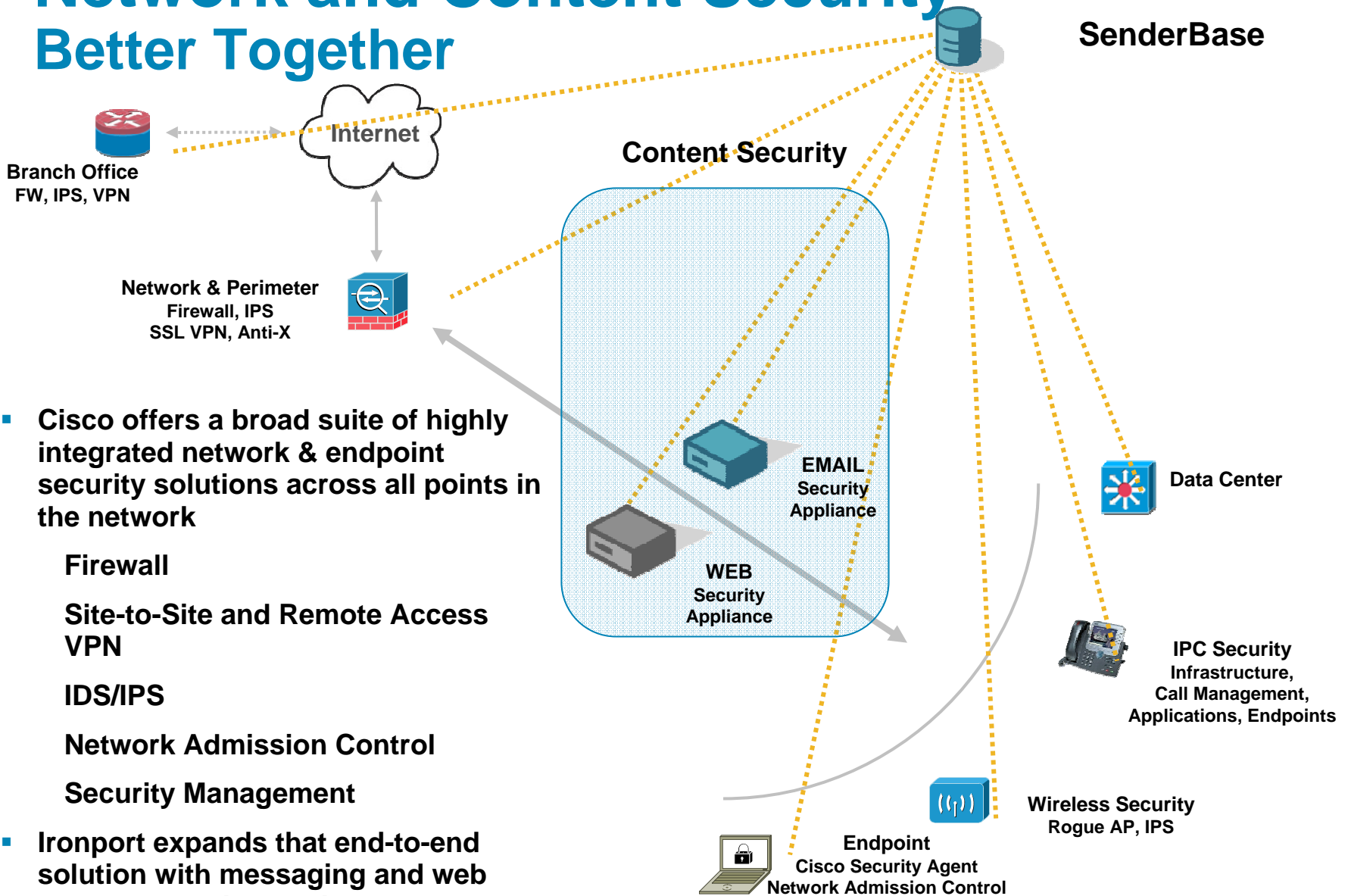
- *URL blacklists & whitelists*
- *HTML Content*
- *Domain Info*
- *Known "bad" URLs*
- *Website history...*

Web Reputation Filters



Reputation Score

Network and Content Security Better Together



- Cisco offers a broad suite of highly integrated network & endpoint security solutions across all points in the network

Firewall
Site-to-Site and Remote Access VPN
IDS/IPS
Network Admission Control
Security Management

- Ironport expands that end-to-end solution with messaging and web content security services

Conclusion

The Criminal Ecosystem is Real

- This analysis is one spam attack over two weeks – a small portion of the real criminal enterprise

The Criminal Ecosystem is Profitable

- Zombies are the enabler to the attack
- Extraordinarily sophisticated and successful spam techniques
- A large, mature business operation supports the spam

A multi-faceted effort is required to solve this problem.



Cisco Expo
2007

Thank you



Henrik Davidsson

henrik@ironport.com

hdavidss@cisco.com

+46 701 90 11 00

**Please Complete Your
Session Evaluation!**



