The dark side of Web 2.0

How the drive to extend e-commerce has come to threaten privacy and security

By Byron Acohido
May 7, 2008
1999 an Age of Innocence
Hacking for bragging rights

Smith, 30
Melissa email virus

De Guzman, 22
ILoveYou bug

Mafiaboy, 16
dDOS pioneer
Hacktivism

“The liability should lie in the hands of the software developers who come out with programs that are defective.”

--Onel deGuzman, author ILOVEYOU virus
Profit motive emerges

July 2001:
- **Code Red** *ISS worm*

Jan. 2003:
- **Slammer** *SQL worm*

Jan.-Aug. 2003:
- **SoBig A-F** *email virus R&D*

Aug. 2003:
- **MsBlast** *RPC-DCOM worm*
MSBlaster copycat

- 48,000 PCs infected
- $12 million damage
- 18-month jail term

Jeffrey Lee Parson, 19, at his sentencing
MSBlast’s deeper impact

- 25 million PCs infected
  - Open backdoor for bot implantation
billy gates why do you make this possible? Stop making money and fix your software!!

--MSBlast virus writer
Profits become predominant

- Jan.-April 2004:
  - **Virus war** MyDoom/Bagel vs. NetSky
- May 2004:
  - **Sasser** LSASS worm
- Aug. 2005:
  - **Zotob** plug-and-play worm

Sven Jaschan, 17
Antivirus vigilante, author Netsky, Sasser
MyDoom/Bagel vs. Netsky

Hey, NetSky, ---- ---- you ------, don’t ruine our business, wanna start a war?

This is the W32. Skynet. AnTiViRuS - we want to kill malware writers!
“He didn’t realize what he was doing was bad.”

[Diabl0] wht u think about this new worm? :o

[Taylor] it is pretty good...i would imagine you will get a lot of bots

[Diabl0] that worm spread only for money :p

Farid Essebar, 19
aka: Diabl0,
author Zotob
Web 2.0:
The dawn of cloud computing
Financial services go digital

Banks:
- Bank of America
- Citigroup

Credit card cos:
- MasterCard
- VISA
- Discover

Credit bureaus:
- Experian
- TransUnion
- Equifax
“Creative marketing”

**Wholly owned sites:**
- CreditReporting.com
- Eloan.com
- LendingTree.com
- FreebieCreditReport.com
- moving-links.com

**Affiliated sites:**
- PrivacyMatters.com
- free-credit-reports.com
- Credit.com
- Free8BureauCreditReport.com
- FreeCreditReportsInstantly.com
- speedycreditreports.com
- spendonlife.com

**Source:** Experian, Equifax, TransUnion, Consumer Reports WebWatch
“Spontaneous collusion”

Open network  
+ anonymity  
+ poor data handling  
+ high system speed  
__________________________________  
= criminal opportunity
Stolen data and a shopping spree

Irving Escobar allegedly purchased at least $225,000 in electronics goods and jewelry at Sam’s Club stores throughout Florida with gift cards. The cards were bought with stolen credit card numbers hacked from retailer TJX in the nation’s largest reported computer data breach, says a criminal complaint from the Florida Department of Law Enforcement. A recap of Escobar and his family’s shopping spree, which may have included more purchases:

First, in North Florida
Gift cards purchased at Wal-Mart with counterfeit credit cards:
- Oct. 25 Jacksonville Beach $35,252
- Oct. 28 Jacksonville $41,200
- Oct. 28 Jacksonville $34,000
- Oct. 31 Holly Hill $18,400
- Nov. 1 Gainesville $18,000
- Nov. 1 Gainesville $24,000
- Nov. 2 Starke $32,800
Source: Florida Department of Law Enforcement

Then, in South Florida
Merchandise purchased at Sam’s Club with gift cards:
- Nov. 1-30 Miami $112,000
- Nov. 7-30 Miramar $20,000
- Nov. 10-15 Orlando $46,673
- Nov. 17-27 Sunrise $10,500
- Nov. 19 Miramar $450
- Dec. 1-30 Miami $17,539
- Dec. 1-30 Miami $11,000
- Dec. 3-5 Miramar $4,600
- Dec. 7, 9 Miami $500
- Dec. 7 Miami $3,790
- Jan. 2-3 Miramar $3,700
- Jan. 2-21 Miami $1,000
- Jan. 2-18 Miami $4,600
Source: Florida Department of Law Enforcement

Brugueras in Miami and Fort Lauderdale had agreements. So Brugueras at the Embassy Banks, with the Florida Department of Law Enforcement.

The information from the device entered Brugueras in that was being someone new.

According to police, Brugueras in Miami and Fort Lauderdale had agreements. So Brugueras at the Embassy Banks, with the Florida Department of Law Enforcement.

More crime
Wal-Mart investigated the investigation. Though it says it is not a known scheme to spend the funds of others.

“Visa authorized transaction”
Dark side of cloud computing
Key cloud players

- aQuantive
- DoubleClick
- America Online
- Microsoft
- Google
- Y!
- Facebook
- YouTube
- myspace
“…the whole future of media and advertising will move to the Internet.”

Steve Ballmer
CEO Microsoft
Two criminal markets

- Stealing data
- Using stolen data
Three attack vectors

- Insider theft
- Port 25
- Port 80
Variations on a theme

- Social engineering
- Pharm spam
- Stock spam
- Spear phishing
- Drive by downloads
- Web spam
- Banking trojans
- Cross site scripting
- SQL injections
- Zero day exploits
- Tainted banner ads
- Denial of service
- Cross-platform attacks
- Vishing
- Poly-morphic scripts
Spam’s chokehold

Source: Symantec

Feb. 2008: 80%

Mar. 2007: 70%

Source: Symantec
Pervasive phishing

Hijacked Brands by Month Dec. '06 - Dec. '07

Source: Anti-Phishing Working Group
Malware’s surge

2007: 5,490,960

2005: 333,425

Source: AV-Test Labs
Top Web-based malware

- Mal/Iframe 53.3%
- Mal/ObfJS 9.8%
- Troj/Decdec 6.6%
- Troj/Psyme 6.2%
- Troj/Fujif 5.8%
- JS/EnclFra 3.9%
- Troj/Ifradv 2.4%
- Mal/Packer 1.2%
- Troj/Unif 1.0%
- VBS/RedIof 0.8%
- Other 9.0%

Source: Sophos
Top web site flaws

Likelihood that a website has a vulnerability, by Class

Source: White Hat Security
Every major bank has been hit by banking trojans.

--Mikko Hypponen

Source: F-secure

Number of Banking trojan detections
2005-2008

2006: 3,342

2008: 16,755
Global botnet activity

2008-02-20 01:00

Source: Damballa
40% of hosts carry botnet data exchanges

Source: Support Intelligence
1 pixel = 250 hosts
red = bot

Source: Support Intelligence
Average daily botnet communiqués

Jan. 2007: 7,303,148

Aug. 2006: 333,025

Source: Damballa
Single Most Important Security Management Issues...top 5

- Keeping virus definitions up to date: 16% (2008), 16% (2007), 17% (2006)
- Secure file transfer: 12% (2008), 9% (2007), 4% (2006)
- Patching systems: 8% (2008), 12% (2007), 25% (2006)

5th Annual Survey:
Network and System Administrators
April 2008
Copyright VanDyke Software
Courtesy of Amplitude Research, Inc.
Business data in digital format

2006: 161 exabytes*

2010: 988 exabytes

*Exabyte = billion gigabytes

Source: IDC
Prepare for a siege

- Think of data as a valuable asset
- Make data privacy and security a core competency
http://zerodaythreat.com

The Shocking Truth of How Banks & Credit Bureaus Help Cyber Crooks Steal Your Money and Identity

BYRON ACOHIDO AND JON SWARTZ