··II··II·· CISCO





Hrvoje Dogan

IronPort Systems Engineer, Emerging Markets Cisco IronPort Systems, LLC

Agenda

- 1. Recent Stories
 - **USAid Website Hacked**
 - Digg.com Serving Malicious Codecs
 - Conficker/Downadup Worm
 - Scareware Spyware
- 2. Threat Landscape
- 3. Web #1 Threat Vector
- 4. A Bit of Good News

Recent Stories

azerbaijan.usaid.gov



- The Azerbaijan section at the US Agency for International Development (azerbaijan.usaid.gov) became another well-known legitimate web site compromised. (usaid.gov has approx 86K visitors a month*)
- 2. The Website was embedded with **malware and exploits serving scripts** sometime around the 1st of March.
- **3**. Upon successful exploitation a Trojan Downloader was installed on the user's computer (Windows only).

Multiple Malicious Redirections

The malware infection showed three malicious redirections;

cs.ucsb.edu.4afad2ceace1e653.should-be.cn/jan10.cn

2

3

orderasia.cn/index.php

orderasia.cn/iepdf.php?f=old



- fileuploader.cn/check/check.php
- The malware's phone home location is a domain that was exclusively used by the Russian Business Network (RBN) back in January, 2008.



Digg.com Serving Malicious Codec's



- 1. On February 11, a surge of false stories with popular social news subject lines were created by malware writers as an attempt to bait users into clicking links which lead to malware.
- 2. Users prompted to install an Fake Codec, which is actually **malware.**
- 3. Once the malware is installed, it can **grab sensitive data** off the users PC, like credit card numbers

Conficker/Downadup Worm

- 1. Microsoft MS08-067 out of band security update on Oct 23, 2008
- MS08-067 is a 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
- 3. 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

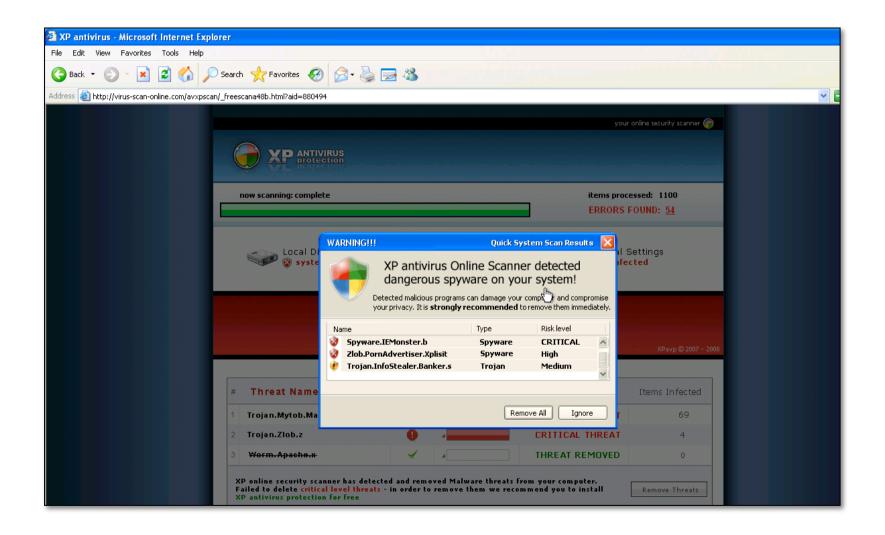
- 4. Disables DNS lookups to security sites
- 5. Generates 250 domain names via algorithm daily and connects via HTTP
- 6. Estimate approximately 9M infected PCs (F-Secure) Only 1% in US while China, Russia and Brazil account for 41%

Scareware Spyware

- 1. Malware that scares users into purchasing fake antivirus protection
- Greatly increases consumer-based revenue per infection from pennies to ~\$1
- Infects via (at least) socially-engineered AV sites, email blended threats and compromised legitimate websites
- 4. Affiliate program run by bakasoftware.com

One affiliate earned \$147k in 10 days based on 155k infects generating 2772 purchases at \$50 each → \$5M per year

Current Scareware Spyware Attacks



Click Yes to Remove 2794 virii ③

File Edit View Help REGISTER								TIY De	efore buy
🚏 Windows processes 🔀 Remove 🛛 🕉 Quarantine	🧭 Google 🛛 🧭 <u>B</u>	luy Now							
Name	Rating CPU	-				Туре	Title, Description		Manu
pphcgt1j0ep37.exe	72	2 % 3.4 M	B C:\WINDOWS\sys	tem32\pphcgt1j0ep37.exe	P	rogram		_	•
AVXP2008install[1].exe	1						×		•
🕼 rholt1j0ep37.exe					- N				•
lphogt1j0ep37.exe Virtual Machine Additions								tive) Continue (0042ED01.1D00	- •
Virtual Machine Additions	An An	htivirus	XP 2008					Services - {0843FD01-1D28 ces - {42F5296B-4A0D-4731	. Microso . Microso
Virtual Machine Additions					Desistantias		Current	r Sharing Service	Microso
CTF Loader					Registration		Support	I Shaling Service	Microso
LSA Shell (Export Version)	Scan	Scan							Microso
Generic Host Process for Win32 Services									Micros
Generic Host Process for Win32 Services	System Status	s s	tart Scan	Stop Scan		Re	move Viruses		Micros
Generic Host Process for Win32 Services	Options								Micros
Generic Host Process for Win32 Services	Optiona	_		Alert ! Your syste	m is infected!				Micros
Application Layer Gateway Service	Update					Infect	ed: 2794		Micros
Windows NT Session Manager	About	Antivirus)	KP 2008			×			Micros
Client Server Runtime Process	About	1					Status 🔺		Microso
Windows NT Logon Application	Realtime Protection	Antivirus X	P 2008 has found 279	94 threats. It is recommende	d to proceed with remov		Infected!		Microso
Services and Controller app		•				tedium			Micros
Generic Host Process for Win32 Services	Known viruses : 1025	5		Yes No		ligh ligh	Infected! Infected!		Micros
Spooler SubSystem App			/in32/IRCBot.AAH	The IRCBot.AAH malware	family is a group of bot		Infected		Micros Micros
System System idle			/in32/IRCBot AAH	The IRCBot AAH malware		High	Infected!	ess	Micros
🕉 Windows Messenger			/in32/IRCBot AAH	The IRCBot AAH malware		-	Infected!	Windows Messenger - Not	Microso
Security Task Manager			irus Win.CIH	Dangerous virus. It destruc		-	Infected!	er	A. & M.
Windows Security Center Notification App		🧕 🔬 🗤	/in32/Adware.Sear	Program is used to direct a		-	Infected!	rts	Microso
Automatic Updates		🧕 🔬 🗤	/in32/IRCBot.AAH	The IRCBot.AAH malware	family is a group of bot	High	Infected	up to date.	Microso
😇 Internet Explorer		🗕 🙆 w	/in32/Adwre.Virtum	Virus applications used to	deliver advertisements t.,	Low	Infected!	ft Internet Explorer	Micros
💡 Windows Explorer	Get Maximal		/in32/Toolbar.Myw	Toolbar which includes a s	earch function that dire		Infected! 🖵	lume	Micros
	Realtime Protection	- 1					[` -[
<	with Antivirus XP								
🗊 Security Task Manage	2008								
 A high rating does not necessarily mean that a prog only that it has characteristics typically found in source 	ram is a threat								
only that it has characteristics typically found in spy	Mare								

Security Threat Landscape

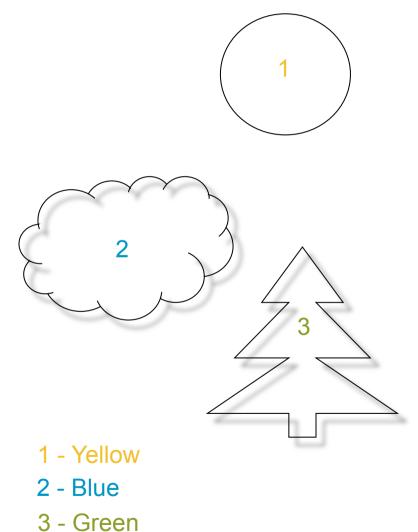
Security Threat Landscape

- 1. Profits, collaboration, innovation
- 2. Attack in depth numerous attack methods to ensure any weaknesses will be exploited
- 3. Rising number of vulnerabilities & weaponization of vulnerabilities
- 4. Malware and theft is covert
- 5. Data loss & Virtual Banks
- 6. Web vector is weakest link

Web is #1

1. What's on that Web Page Web pages are like paint by numbers

- Web pages return html which indicates objects to fetch
- 2. Objects are fetched from specified location
- 3. Objects can be images, executables, javascript...
- 4. Visiting a web page can cause content to be fetched from anywhere the web pages says



2. Web Browser Ecosystem Vulnerable

SANS Top 20 2007 Security Risks http://www.sans.org/top20/#c1

1.IE and Firefox vulnerable

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

2.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.

Mpack: Infection rates per country

Country	Traff	Loads	Efficiency
👤 JP - Japan	93635	19875	21.23
E - Germany	18702	4625	24.73
💶 ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1089	294	27

3. Malware Defeats Anti-Virus Signatures Race to Zero at DefCon Conference

- 1. Criminals have developed tools to mutate malware to defect signature-based detection
- 2. At DefCon teams of researchers proved their success yet again
- 3. Seven viruses and two exploits, all wellknown, were mutated to defeat anti-virus engines
- 4. Winning time: 2 hours, 25 minutes

4. Web Servers Vulnerable

4. 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."

minnesotahomefinance.com web site

	🕲 Credit : minnesotahomefinance.com - Mozilla Firefox						
	Eile Edit View History Bookmarks ScrapBook Iools Help		$\langle \Diamond \rangle$				
	< C 📀 🏠 📄 http://minnesotahomefinance.com/?cat=23	🛛 🔹 🕨 💽 🖌 Google 🔤 🔍	- 52				
	minnesotahomefinance.com						
	Blog						
	Housing Slump Hurts Freddie Mac Profit	Recently Written					
	Freddie Mac, the second-largest U.S. home-mortgage financier, posted a 45% drop in	Agreement on Auto Deal - Sighs of Reliet alround	f				
	second-quarter net income as it set aside \$320 million for losses, and said it expects credit losses to continue to rise as the housing slump persists.	NY Times to Drop Fees for Online Version					
	The McLean, Va., company predicted that credit-market turmoil would force it to mark down this quarter the value []	401 Plans Retirement plans not quite what they were thought					
		3 Core Principals for the maintenance of mature and successful growth					
		Housing, Credit Worries Hurt Stocks					
	Stocks Rise on Techs, Fed Letter	Nasdaq Soars on Rate-Cut Hopes	~				
			>				
Loading	\mathbb{S} Scripts Partially Allowed, 1/3 (googlesyndication.com) <script>: 5 <OBJECT>: 1</td><td>Options</td><td></td></tr><tr><td>aarmrgdxrv.com</td><td>http://aarmrgdxrv.com/dl/adv448.php</td><td>artially Allowed <SCRIPT>: 5 <OBJECT>: 1</td><td>0 .::</td></tr></tbody></table></script>						

What's really happening

- 1. Minnesotahomefinance.com registered at Godaddy june, 2005
- 2. 209.51.132.218, Global Net Access in NY, with 312 domains



- Browser fetches IFRAME & loads PHP from aarmrgdxrv.com
- 85.255.121.195, Ukrtelegroup Ltd in Ukraine, with 15 domains
- Ukrtelegroup is part of RBN (Russian Business Network)
 Other domains match the pattern; e.g. adtctqypoa.com...
- aarmrgdxrv.com registered at BIZCN.COM, INC.
 - Spamvertized domain ranking: #18 by volume, #11 by % bad

Some Good News

Some 2008 Good News

1. Intercage, a US hosting provider associated with the Russian Business Network, was taken offline

Operated in US for years from San Francisco supporting all types of criminal activity

2. McColo also taken offline

Supported command and control for Srizbi, largest spamming botnet of 2008, and other criminal activity

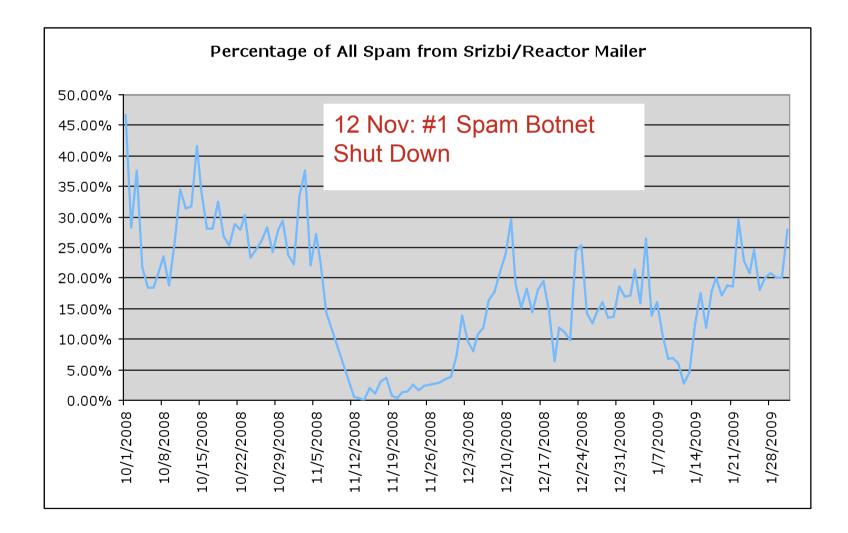
3. EstDomains de-accredited by ICANN

Criminal domain registrar purporting to be US company, controlled by Russian criminals

4. SanCash/GenBucks spam affiliate program shut down

Prosecuted by US and New Zealand law enforcement Botnet affiliates spammed numerous "enhancement" products

Impact of McColo Shut Down

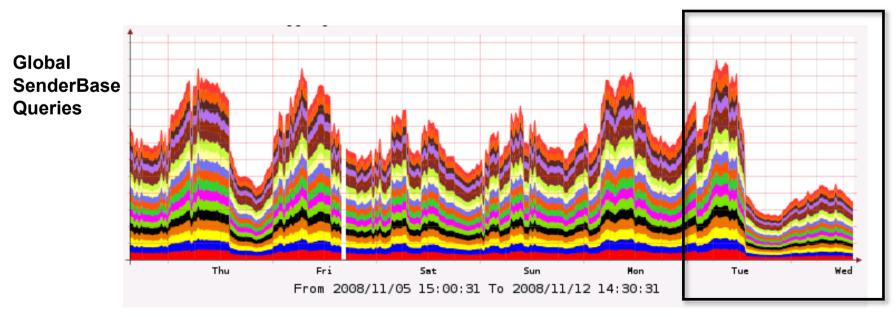


Spam Volume Growth Reprieve SenderBase Perspective

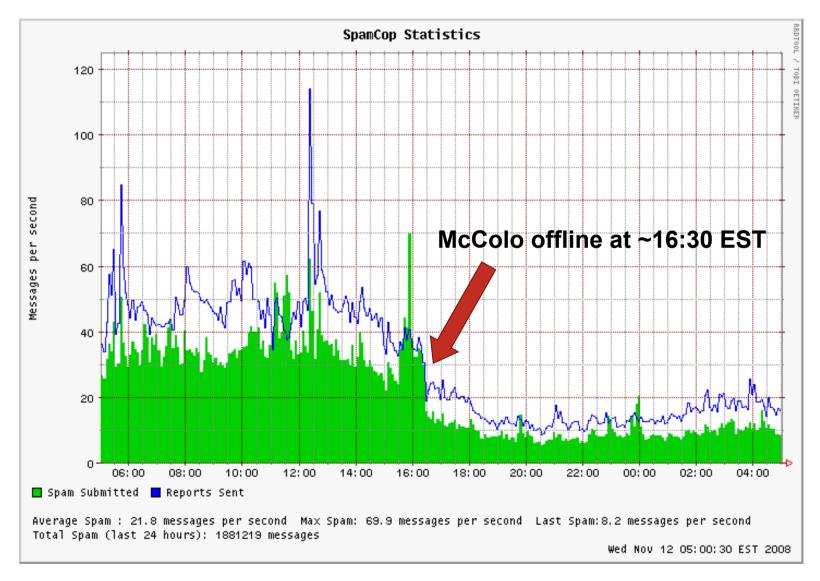


SenderBase provides unparalleled visibility

- •30B+ queries daily
- •150+ email and Web parameters
- •30% of the World's Traffic
- Cisco Network Devices



Spam Volume Growth Reprieve SpamCop Perspective



#