Non-Classical Computer Forensics

R9

Line Line

R

E

E

Caps Lock

PF16

A

G

N

H

7

2

R11

M

R13

8

S

R5

S

Esc

0

0

Recrd

Q

Delete

K

0

13

PF22

C

Control

R6

M

8

DACO

E2

W

PF20

Q

PF17

R10

Stop

Y

R8

.

Put

Open

0

Dr. Neal Krawetz Hacker Factor Solutions www.hackerfactor.com

Contents

- Classical Investigative Science
 - Forensics and Profiling
 - Computer Science
- Non-Classical Approaches
 - Gender Guessing
 - Author Analysis
 - Keyboard Profiling
- Approaches that don't work
 - When theory fails...

Classical Investigative Science

Time Tested, Court of Law



Forensics vs Profiling

- Forensics
 - Raw analysis, unbiased
 - This item exists
 - This location contains
 - Provable and repeatable
 - Multiple approaches generate same results
 - Asks:
 - Did this happen?
 - What was happening?
 - How many involved?

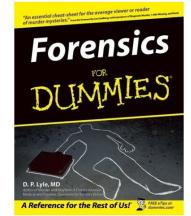
- Profiling
 - Interpreted analysis
 - Estimates
 - Conjectures
 - Probabilistic
 - He is likely...
 - Confidence < 100%
 - Asks:
 - Are there patterns?
 - Why was he doing that?
 - What are physical or personal attributes?

Examples

Copyright 2006 Hacker Factor

- Forensics
 - Fingerprints
 - 1000 BC: China
 - August 1892: First crime solved via prints, Argentina
 - Matches person to location

- Profiling
 - Blood splatter
 - Location, Direction
 - Movement
 - Quantity, Tackiness
 - Number of strikes
 - And more!



Sample Computer Tools

	System-Oriented	Network-Oriented
Collection	ChecksumsMirror, dd, cpio	Tcpdump, Ethereal/Wireshark, Snort
Forensics	 Common TCT, Sleuthkit, Autopsy Undelete John the Ripper Uncommon Spinrite, Un-format File-to-sector location 	 Common nmap, scanrand DNS, WHOIS Snort, Ethereal, ngrep Uncommon Honeypots
Profiling	 Common 'file', text content Log, email, web analysis Uncommon stegdetect, image analysis Common usage patterns (time, server type, etc.) Application identification 	Common • 'nmap -O -sV', p0f • IP-to-user Uncommon • snacktime • httprint

Tool Limitations

- System/Network Access
 - Hard drive may be inaccessible
 - Networks spread/modify data (P2P, NNTP, SMTP)
- Dynamic Data
 - Temporary Web and FTP sites
 - Ephemeral network traffic; No storage on network
 - Collection tools (sniffers) do not record all details
- Data Only?
 - No timestamps, no relationships, no owners...

Non-Classical Forensics

You are what you type...



Anonymity

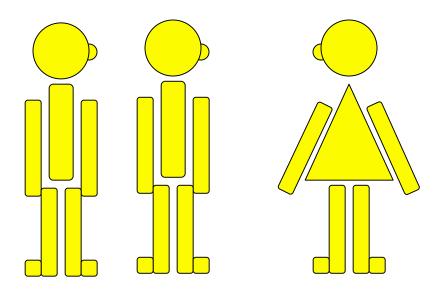
- Easy to be anonymous online
 - Proxies, botnets, TOR
 - Change name, age, gender
 - Enter name: Susan Olsen
 - Enter age: 45
 - Modify browsers, IRC clients, applications
 - Firefox, Opera: Allows changing client string
 - IRC: Recompile IRSSI with new identification

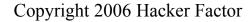
Anti-Anonymity

- Assume
 - No access to original system
 - No access to originating network traffic
- "Get everything you can!"
 - Physical attributes
 - Gender; Nationality
 - Left/right handed; Finger drumming
 - Type of keyboard

- Any information is better than no information

Gender Determination





Gender Determination

- "Gender, Genre, and Writing Style in Formal Written Texts" (2003)
 - Shlomo Argamon, Moshe Koppel, Jonathan Fine, and Anat Rachel Shimoni
 - Bayesian network
 - Weighted word frequencies and parts of speech
 - Two genres: fiction and non-fiction
 - Determine gender
- Gender Genie by BookBlog
 - Fewer words
 - Expanded to cover fiction, non-fiction, and blog text
- Gender Guesser by Hacker Factor Solutions
 - Elaborate on Gender Genie
 - Two categories: formal and informal

Words and Weights

Informal (Blog, IN	I, Chat-room)
actually -49	am -42
as 37	because -55
but -43	ever 21
everything -44	good 31
has -33	him -73
if 25	in 10
<mark>is</mark> 19	like -43
more -41	now 33
<mark>out</mark> -39	since -25
<mark>so</mark> -64	some 58
something 26	the 17
this 44	<mark>too</mark> -38
well 15	

Formal (Fiction, N	on-fiction, News)
<mark>a</mark> 6	above 4	and -4
are 28	around 42	2
as 23	at 6	<mark>be</mark> -17
below 8	her -9	hers -3
<mark>if</mark> -47	is 8	it 6
many 6	<mark>me</mark> -4	more 34
myself -4	<mark>not</mark> -27	said 5
she -6	should -7	the 7
these 8	to 2	was -1
we -8	what 35	when -17
where -18	8 <mark>who</mark> 19	with -52
your -17		

Gender Example

Black Hat 2006 CFP

"The Black Hat Briefings was created to fill the need for computer security professionals to better understand the security risks to information infrastructures and computer systems. Black Hat accomplishes this by assembling a group of vendor-neutral security professionals and having them speak candidly about the problems businesses face and the solutions to those problems. No gimmicks—just straight talk by people who make it their business to know the information security space."

Gender Example: It's a Boy!

score of 6, seen once

score of -4, seen 3 times

- Black Hat 2006 CFP
 - "Formal" writing
 - A = 6×1 And = -4×3
 - $It = 6 \times 1$
 - The = 7×6
 - To $= 2 \times 5$
 - Was = -1 x 1

Who = 19×1

Total = 6 + -12 + 6 + 42 + 10 + -1 + 19 = 70 (Male!)

Validation

Ping Look

 Black Hat Conference Admini
 Date: Sun, 11 Jun 2006 23:23:38 -0700
 To: Dr. Neal Krawetz
 From: Ping Look
 Subject: Re: Black Hat USA 2006 Schedule

Total words: 50 Too few words. Try 300 words or more.

Genre: Informal Female = 122 Male = 32 Difference = -90; 20.77% Verdict: FEMALE

Well it has been a long time and a lot of people have touched it. The original text was written by Jeff a few years ago. I modified it when I came on board and 2 other females have edited it since. So yes, it was written by a male.

Gender Limitations

- Simple algorithm = 60% 70% accurate
 - Better than random guessing (50%)
- Different genres use different writing styles
 - E.g., "Male" for formal, "Female" for informal
 - Lists, poems, prose, lyrics
 - Email can be formal AND informal
- Other factors
 - Block quotes, copy-editors
 - Familiarity, age, nationality, experience, and education
 - All impact writing styles!

Weak Matches

- 40% < |male| ÷ (|male|+|female|) < 60%
 - Close to 0% is likely female
 - Close to 100% is likely male
 - Mid-range? Weak score
 - Sample too small
 - Too many authors
 - Weights for "American English"
 - European English can appear "Weak"

MySpace Blogs

Says:	Male	Female
Tests as:	57% (1946)	43% (1456)
Male	22% (748)	20% (681)
Weak Male	11% (370)	14% (481)
Weak Female	6% (207)	12% (393)
Female	4% (123)	11% (383)



Total samples: 3402

Minimum word count: 300 Only samples with gender specified

Virtual Drag

- Why so many females test as male?
 Formal vs Informal
 - Many female entries are formal
 - Stories, essays, news, editorials
 - Not informal blogging
 - Males writers
 - Some explicitly include text from male authors
 - Some appear written by "friends"
 - And some are just not female

Example: Psycho Bitch I'd rather be hated for who I am than loved For someone I am not

< Back



Last Updated: Jun 20, 2006 Send Message Instant Message Email to a Friend Subscribe

Gender: Female Age: 26 Sign: Leo June 9, 2006 - Friday

MySpace

SEX WITH FECES-SCATOLOGY Current mood:
 dirty Category: Blogging

Oh yeah. I'm going to talk about it. Scatologists...d who have an extreme infatuation with human fee For the record...Ew. Wait...let me repeat that for th

Mother fucker that is soooo fucking gross. What or Please tell me WHY? I don't get it, and don't fuckin try it all in life." PEOPLE: THAT'S ONE THING I WILL NO jizz on me, spit on me, and fucking do weird thing: on me. Genre: Informal Female = 2646 Male = 1693

Total words: 1009

Difference = -953; 39.01% Verdict: FEMALE

Genre: Formal Female = 1423 Male = 917 Difference = -506; 39.18% Verdict: FEMALE

I'd like to tell you all a story.

Once upon a mother fucking time, there was a fucktard who contacted me on myspace asking me to have sex with him. You can imagine my reaction "Of

http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=29924823&blogID=130716483

Example: Ashley

Ashley's Blog

< Back

Ashley Mizassaro

Last Updated: Jun 10, 2006

<u>Send Message</u> <u>Instant Message</u> <u>Email to a Friend</u> <u>Subscribe</u>

Gender: Female Status: In a Relationship

Friday, June 09, 2006

Conneti- what! See you in a few!

Top o the mornin to ya. I am drinking the relation to juice though cuz it is NASTY getting ready to leave for CT. I just found told yall I'd be coming back soon. :o) Wh my friend Eliana who runs Tripp clothing hair. Tobeys coming to the signing. So we them. :o) See you punks later. xoxo ashley post song-Don't cry Out-Shiny Toy Gur "You look beat. Soft mattress?"

"Soft mattress? Yeah, it could have been One of those three probably contributed Yep I watched it again. Makes me laugh e from the hospital Ali. He's so rad. I hope he Laterrr xox dirty diva

Total words: 315

Genre: Informal Female = 474 Male = 723 Difference = 249; 60.4% Verdict: MALE

Genre: Formal Female = 160 Male = 261 Difference = 101; 61.99% Verdict: MALE

n a Relationship 0105 AM - 72 Comments - 96 Kudos - Add-Comment http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=61214741&blogID=130779711

Example: Samantha Jee

< Back

MySpace.com



Last Updated: Jun 13, 2006

Send Message Instant Message Email to a Friend Subscribe

Gender: Female Status: In a Relationship Age: 100 Sign: Pisces

Friday, June 09, 2006

What's Up with this HINCITY competition? Current mood: (9) high

So I'm getting a lot of emails of people who are confused

What is Who's on Top:

Who's on Top is a voting style competition that pits in competition. Each competition consists of 16 competimay vote once per day per match-up. Non-members m

Prizing is available for all competitors making it past the the competition. COMPETITOR PRIZING. Prizing is a better chance you have to win. VOTER PRIZING.

Competition winners will also receive exclusive I'm o linking back to the competition results.

How to Win:

Winning is very easy. Simply get more votes than your member competition with the 4 th round crowning the morning at 12:00 am and concluding the following Sund system.

Voter Prize Pool:

1 grand prize - xm Satellite radio

20 other awards will be randomly selected

Genre: Informal Female = 291 Male = 518 Difference = 227; 64.02% Verdict: MALE

Total words: 330

Genre: Formal Female = 144 Male = 508 Difference = 364; 77.91% Verdict: MALE

http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=1000679&blogID=131000794

Example: Alia

< Back	
alia	Friday, June 09, 2006 Michael Berg on al-Zargawi and Bush
	Current mood: Contemplative Category: <u>News and Politics</u> Total words: 2333
	I am so impressed by this man's abi Peace. Genre: Informal Female = 2002
Last Updated: May 28, 2006 <u>Send Message</u> <u>Instant Message</u> <u>Email to a Friend</u>	[Michael Berg is a long-time supporter of in 2004.] Beheaded man's father: Revenge breeds r Michael Berg talks about the death of his s
Subscribe	http://www.cnn.com/2006/WORLD/meast Thursday, June 8, 2006; Posted: 11:19 p.m Female = 1870
Gender: Female Status: In a Relationship Age: 27 Sign: Gemini	(CNN) – The U.Sled coalition's No. 1 wa al-Zarqawi – who conducted a campaign of and killings of Americans and Iraqi civilian airstrike.
City THESON	· A grupsome video was nosted on Islamic Web sites in May 2004 depicting a



http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=2150152&blogID=130805539 Copyright 2006 Hacker Factor 2

Gender Guesser ONLINE

http://www.hackerfactor.com/

Click on "Forensics"



Gender Guesser

Hacker Factor Safe Computing

Ho	me	
Co	nsult	ting

Research

Forensics

About

Contact Blog

In the News

INTRODUCTION

The words you use can disclose identifying features. This tool attempts to determine an author's gender based on the words used.

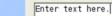
Submitted text is evaluated based on two types of writing: formal and informal. Formal writing includes fiction and non-fiction stories, articles, and news reports. Informal writing includes blog and chat-room text. (Email can be formal, informal, or some combination.) You should view the results based on the appropriate type of writing.

Analyze

Analyze Clear

Results

Type or paste a list of words to be gender analyzed. Then click on "Analyze" to see the results. For best performance, use at least 300 words -- more words is generally more accurate.





Copyright 2003-2006 Hacker Factor. All rights reserved.

Author Analysis

- Are two texts by the same person?
 - Don Foster: Author Unknown: On the Trail of Anonymous
 - Joe Klein wrote Primary Colors (1996)
 - Core words and vocabulary size
 - Punctuation frequency
 - Sentence lengths
 - Word usage, parts of speech, hyphenated words, made up words, spelling errors, grammar differences, …

Text Example: Mark Rasch

Home Bugtraq	Vulnerabilities Mailing Lists See	curity Jobs Tools Search:
News Infocus		(page 1 of 4) next
 Foundations Microsoft Unix IDS Incidents Virus Pen-Test Firewalls 	MARK RASCH and U.S. wiretap laws at legal protections ava	ying NSA eyes Amendment, the Stored Communications Act to the Pen-register statute, Mark Rasch looks ailable to the telecommunication companies ke of the NSA's massive spying program.
Mailing Lists Newsletters Bugtraq Focus on IDS Focus on Linux Focus on Microsoft Forensics Pen-test Security Basics Vuln Dev Vulnerabilities Jobs Resumes Job Opportunities Resumes Job Seekers Employers Tools	Imagine being the head of a major telecommunications company in the United States. You and your lawyers have developed a carefully worded privacy policy to conform with the law. In it you tell your customers that you do not share information about your customers' use of your services except for particular business purposes, and to ensure that the calls get through. You also tell your customers that you, of course, give information in response to lawful subpoenas or lawful mandates of law enforcement agencies. And that's about it.	Attackers are targeting you
RSS > News > Mulns	One day, you receive a visit from agents of the National Security	" Note here [in Title 18 U.S.C. 2702(a)(3)] that it is the telephone companies which

Example: Mark Rasch

Core Words

#Total words: 3734
#Total distinct words: 935 (25.04%)
#Single words:
 298 7.98% the

- 117 3.13% to
- 113 3.03% of
- 91 2.44% that
- 84 2.25% and
- 77 2.06% a
- 64 1.71% or
- 56 1.50% in
- 45 1.21% for
- 39 1.04% you
- 35 0.94% it
- 35 0.94% government
- 34 0.91% not
- 33 0.88% is

Core Words #Total words: 1974 #Total distinct words: 679 (34.40%) #Single words: 116 5.88% the 71 3.60% to 58 2.94% a 56 2.84% in 49 2.48% of 45 2.28% and 34 1.72% that 28 1.42% is 28 1.42% be 1.37% forensic 27 24 1.22% or 20 1.01% computer 19 0.96% not 17 0.86% by

. . .

Example: Scott Granneman

Core Words

#Total words: 1812 #Total distinct words: 700 (38.63%) #Single words:

- 118 6.51% the
- 53 2.92% that
- 48 2.65% of
- 47 2.59% a
- 45 2.48% to
- 34 1.88% and
- 32 1.77% in
- 21 1.16% it
- 19 1.05% was
- 17 0.94% by
- 16 0.88% you
- 16 0.88% or
- 16 0.88% on
- 14 0.77% web

Core Words #Total words: 2196 #Total distinct words: 939 (42.76%) #Single words: 138 6.28% the 68 3.10% of 62 2.82% to 62 2.82% and 56 2.55% a 51 2.32% in 37 1.68% that 22 1.00% for 20 0.91% it 0.77% this 17 17 0.77% is 15 0.68% on 15 0.68% all 14 0.64% was

Both Examples

Mark Rasch

#Total words: 1974 #Total distinct words: 679 (34.40%) #Single words:

- 116 5.88% the
- 71 3.60% to
- 58 2.94% a
- 56 2.84% in
- 49 2.48% of
- 45 2.28% and
- 34 1.72% that
- 28 1.42% is
- 28 1.42% be
- 27 1.37% forensic
- 24 1.22% or
- 20 1.01% computer
- 19 0.96% not
- 17 0.86% by

Scott Granneman #Total words: 2196 #Total distinct words: 939 (42.76%) #Single words: 138 6.28% the 68 3.10% of 62 2.82% to 62 2.82% and 56 2.55% a 51 2.32% in 1.68% that 37 22 1.00% for 20 0.91% it 0.77% this 17 17 0.77% is 15 0.68% on 15 0.68% all 14 0.64% was

. . .

Punctuation Examples

	Mark	Rasch		S	Scott	Granneman
	Sample	#1		S	ample	#1
	. 140	(22.44%)			81	(26.56%)
	? 18	(2.88%)		?	16	(5.25%)
	! 1	(0.16%)		!	4	(1.31%)
	, 218	(34.94%)		,	95	(31.15%)
	: 4	(0.64%)		:	3	(0.98%)
	;	(0.00%)		;	2	(0.66%)
	(27	(4.33%)		(7	(2.30%)
) 27	(4.33%))	7	(2.30%)
	- 59	(9.46%)		-	16	(5.25%)
	" 93	(14.90%)		"	32	(10.49%)
	Sample	#2		S	ample	#2
	. 95	(27.14%)			99	(27.50%)
	? 6	(1.71%)		?	5	(1.39%)
	! 3	(0.86%)		!	4	(1.11%)
	, 122	(34.86%)		,	131	(36.39%)
	: 2	(0.57%)		:	11	(3.06%)
	;	(0.00%)		;	3	(0.83%)
	(10	(2.86%)		(7	(1.94%)
Ħ) 10	(2.86%))	7	(1.94%)
	- 42	(12.00%)		-	27	(7.50%)
	" 44	(12.57%)	6	"	20	(5.56%)
			6			

Sentence Length Examples

Mark	F	Rasch
#Sentenc	e	word-count/length:
49	3	(2.91%)
43	2	(1.94%)
31	2	(1.94%)
	_	
		(2.91%)
		(3.88%)
24	3	(2.91%)
22	3	(2.91%)
21	3	(2.91%)
20	8	(7.77%)
18	3	(2.91%)
17	3	(2.91%)
16	5	(4.85%)
15	4	(3.88%)
13	10) (9.71%)
12	3	(2.91%)
10	4	(3.88%)
9	4	(3.88%)
7	3	(2.91%)
6	5	(4.85%)
		-

Scott Granneman

#Sentence word-count/length:

39	2	(1.96%)
33	2	(1.96%)
31	3	(2.94%)
30	2	(1.96%)
27	3	(2.94%)
26	2	(1.96%)
25	5	(4.90%)
23	5	(4.90%)
22	6	(5.88%)
21	4	(3.92%)
20	3	(2.94%)
19	3	(2.94%)
18	4	(3.92%)
17	4	(3.92%)
16	3	(2.94%)
14	4	(3.92%)
13	2	(1.96%)
11	4	(3.92%)
7		

How to Use Author Analysis

- Rules out suspects!
 - Does not identify "same author"
 - Metrics not unique enough
 - Indicates different authors!

- Multiple samples
 - Similar topics
 - Similar word count
- Accuracy varies
 - Punctuation usage
 - More accurate
 - Sentence lengths
 - Less accurate

Author Analysis Results

- Nationality and Native Language
 - American: Small core, small vocabulary
 - European: Large core, large vocabulary, alternate spelling (colour, flavour)
 - Australian: Small core, European spelling
- Co-author identification
- Expand to analyze source code
 - Comment types, line lengths, variable naming, etc.

Phatbot Investigation



Phatbot Author Analysis

- Phatbot worm
 - Derivation of Agobot
 - aka Gaobot, Nortonbot, Polybot
 - First appeared in October 2002
 - Source code released
 - Multiple copies and versions available online
 - Source code contains comments and docs!
 - 7-May-2004: Author "Ago" arrested
 - 21-year-old "Alex G" in Waldshut, Germany
 - 5 other people also charged

Source Differences

- Agobot source (agobot3-0.2.1-pre4-priv)
 - Dated: October 2003
 - 103 primary source files (excludes OpenSSL, etc.)
- Phatbot source (phatbot_current)
 - Dated: March 2004
 - 145 primary source files
- Comparisons
 - 2 files identical
 - 77 files with different SHA1 checksums
 - 24 files unique to Agobot source
 - 66 files unique to Phatbot source

Source Code Styles

utility.cpp

{

```
// Only alphanumeric characters
```

```
void gen unique id(char *szString, int iLen)
        memset(szString, 0, iLen);
        for(int i=0; i<iLen; i++)</pre>
                int sel=brandom(1, 3);
                 switch(sel)
                 case 1: // Numeric characters
                         szString[i]=(char)brandom(48, 57);
                         break;
                 case 2: // Uppercase letters
```

harvest cdkeys.cpp

```
/* Leet cdkey code by thegeek:)
 * CDKey List, With GameNames and Registry Entries ?
 * Here Is Where You Would Add New Games If You Wanted Too
 * TODO: add support for getting from files.
 */
        CDKeyList[] =
items
        { "[Windows Product ID: ", HKEY LOCAL MACHINE, "Software\\Microsoft\\
Windows\\CurrentVersion", "ProductID" },
```

PhatBot Source Control (svn)

- wonk. Most active developer He is a Windows programmer (only touches Windows code)
- thegeek. Created "harvest_cdkeys.cpp"
 He uses ANSI-C comments in C++
 He also uses a 1024x768 screen with an editor opened all the way
- silencer. IRC programmer Heavy uses C++ comments to document his code
- Nils. C++ programmer who does rarely comments his code One source file claims that this is "nils@rBot.org" and includes the comment "I know, sorry, the code looks kinda fucked up. ;-)"
- **d4t4**. Created the "todo.txt" file and "ddos.cpp" module He uses C++ and no comments, similar to Nils
- glow. Created the sqlscanner He is an ANSI-C programmer using C++
- evilbyte. Created "harvest_aol.cpp" and "wonk.cpp" He uses both ANSI-C and C++ comments, very few comments

Nils .svn/entries <entry radminscanner.cpp committed-rev="469" /* name="radminscanner.h text-time="2004-03-21 Title: Radmin Massrooter committed-date="2004-Author: Nils <nils@rBot.org checksum="91c40f3194d Comments: I know, sorry, the code looks kinda fucked up. ;-) last-author="Nils" kind="file" */ prop-time="2004-03-21 . . . #include "main.h" <entry #include "radminscanner.h" committed-rev="469" #include "mainctrl.h" name="radminscanner.d #include "utility.h" text-time="2004-03-21 #include "shellcode.h" committed-date="2004checksum="a3d568133b0 #include <windows.h> last-author="Nils" #include <process.h> kind="file" #pragma comment(lib, "ws2 32.lib") prop-time="2004-03-21 #include <stdio.h> #include <string.h> #include <stdlib.h> #include <sys/types.h> #include <time.h>

Nils@rBot.org

http://nopaste.php-q.net/37901
From: "Johnathan Lake" <abuse@aol.com>
To: <nils@rbot.org>
Sent: Sunday, January 25, 2004 8:05 PM
Subject: Re: Abuse (Distributed Denial of Service / Breaking the Computer security Laws.)

> Dear AOL Support Team,

>

>

>

. . .

> Right now we're experiencing some problems caused by one of your
> customers. He is using the Distributed Denial of Service attack (DDoS)
> against our Servers (www/irc.rbot.org (Port(s) 80/6667). I attached 3
> Files. (Rob-MSN-log.txt (IP Address added) - that shows that he is
> using a stolen credit card, that means he's breaking the
> computer/security laws. / Rob-IRC-log.txt - that shows that he's going
> to DDoS our maintained Servers / Rob-IPTables.txt - All AOL based IP
> Tables (cached from 2 forums, and 2 Serverlogs) beg you to do something
> against that. I do not want to send another mail
> before AOL finally takes action. Thank you.

> Yours Sincerely,

> Nils Wiegner

Dear Mr. Nils Wiegner,

rBot.org Security	Portal	
Create an account		
Modules	IRC Community Started !	Survey
• <u>Home</u> • Forums	Hello !	What bot are you using?
Downloads FAQ	We started the IRC Community now ! We opened the server yesterday and our peak of users is 50. (that is not bad within 24 hours :-)).	🔿 rBot
 Feedback Journal Private Messages Search Statistics Stories Archive Submit News Surveys Top 10 Topics WebMail Your Account Languages 	This Network is going to allow Warez ! We're setting the iroffer Bots up at this moment. SERVER: irc.rBot.org:6667 CHANNEL: #rBot for IRC Newbies: Download mIRC (download) click on THIS LINK to get connected to the server. Now if you're connected type: /nickserv register yourpassword youremailaddress Now you type /join #rBot then you're connected to the community. :) We look forward to meet you on our IRC Community. - Nils	 Spybot GT Bot Agobot private version 2, Or more bots My Own Bot SDbot Something else I dont have a botnet
Select Interface Language:		Results Polls
English 💽		Votes: 89 Comments: 0
		Login

Dave Aitel

radminscanner.cpp

```
memset(overwrite, 0x41, 2000);
memset(overwrite+2000, 0x90, 44);
memcpy(exp buf, overwrite, 2044);
memcpy(exp buf+2044, &jmpesp, 4);
memset(exp buf+2048, 0x90, 16);
memcpy(exp buf+2064, sc, sizeof(sc));
if(spOne) {
        memset(unicode, 0x00, sizeof(unicode));
        for (x = 0, i = 0; i \le sizeof(unicode); x++, i+=2)
          // roll my own; stupid multibytetosuck broke my string.
                unicode[i] = exp buf[x];
          // my thanks goes to dave aitel for mentioning this to me.
} else {
        len = MultiByteToWideChar(CP ACP, NULL, exp buf, sizeof(exp buf),
(unsigned short *)unicodesp0,sizeof(unicodesp0));
MultiByteToWideChar(CP ACP, NULL, ip, 30, (unsigned short*)ipl, 60);
```

Dave Aitel and Wirepair

From: "wirepair" <wirepair@roguemail.net>
To: vuln-dev@securityfocus.com
Subject: ms03-049 sp1a and sp0 now working.
Date: Fri - Nov 14, 2003 12:25 PM

Thanks to Dave Aitel for suggesting there is a difference between how sp1 and sp0 processes unicode strings. Unfortunately this means you need to specify which SP level the remote host is. Does anyone know a way of requesting an XP machine return a unicode string? Maybe this way I can read in the string and determine which sp level its at and make my code automatically detect and use the correct formatting. Thanks,

-wire

http://sh0dan.org/files/0349.cpp http://sh0dan.org/files/0349.exe

Visit Things From Another World for the best comics, movies, toys, collectibles and more. http://www.tfaw.com/?qt=wmf

Wirepair's 0349.cpp

```
0349.cpp
                                                                 radminscanner.cpp
memset(overwrite, 0x41, 2000);
memset(overwrite+2000, 0x90, 44);
memcpy(exp buf, overwrite, 2044);
memcpy(exp buf+2044, &jmpesp, 4);
memset(exp buf+2048, 0x90, 16);
memcpy(exp buf+2064, sc, sizeof(sc));
if(abOne)argv[2]) == 1) {
        memset(unicode, 0x00, sizeof(unicode));
        for (x = 0, i = 0; i \le sizeof(unicode); x++, i+=2)  {
          // roll my own; stupid multibytetosuck broke my string.
                unicode[i] = exp buf[x];
          // my thanks goes to dave aitel for mentioning this to me.
} else {
        len = MultiByteToWideChar(CP ACP, NULL, exp buf, sizeof(exp buf),
(unsigned short *)unicodesp0,sizeof(unicodesp0));
MultiByteToWideChar(CP ACP, NULL, ip, 30, (unsigned short*)ipl, 60);
```

Other Code

• Wirepair: dcomuni.c

- Phatbot: dcom2scanner.cpp
 - Again, code checked in by Nils (according to changes.txt)
 - dcom2scanner.cpp is found in (older) Agobot source code
 - Timestamps show Wirepair had it in August 2003, and Agobot had it in October 2003.
 - dcom2scanner.cpp has comments! The code is documented.
- Wirepair: rs_cbbrute.c
 - Phatbot: wdscanner.cpp
 - Wirepair source: rs_cbbrute.c = April 2003
 - Agobot source: wdsscanner.cpp = October 2003

The Suspects

- Wirepair
 - www.sh0dan.org
 - C and C++
 - Windows exploits
 - Likely lives in New England (USA)
 - Works for a computer security company
 - English only

- Nils (Nils Wiegner)
 - Ran www.rbot.org
 - nils@rbot.org
 - Also nils@ryan1918.com
 - Same skills as Wirepair
 - Possibly
 - Fluent in German
 - Born 30-Sept-1975
 - MAY NOT BE SAME "Nils Wiegner"

Who Dunnit?

The Question:

- Is Wirepair the same as Nils Wiegner?
- Or did Nils "borrow" Wirepair's code?

The Answer?

- Author Analysis!
 - Wirepair has MANY writing samples
 - Nils has some writing samples (none large)

Compare

		epair	1 -	lils	-
	msrant		A		mail
	. 33	(32.35%)	•	8	(24.24%)
	? 5	(4.90%)	?		(0.00%)
	! 3	(2.94%)	!		(0.00%)
	, 30	(29.41 %)	,	2	(6.06%)
	: 1	(0.98%)	:		(0.00%)
	;	(0.00%)	;		(0.00%)
	(1	(0.98%)	(7	(21.21%)
) 1	(0.98%)		5	(15.15%)
	- 1	(0.98%)	-	8	(24.24%)
	" 2	(1.96%)	"		(0.00%)
	thesce	ne.html	w	ww.r	bot.org
	. 75	(35.55%)		6	(22.22%)
	?8	(3.79%)	?		(0.00%)
	!	(0.00%)	!	3	(11.11%)
	, 52	(24.64%)	,		(0.00%)
	: 5	(2.37%)	:	7	(25.93%)
	;	(0.00%)	;		(0.00%)
	(3	(1.42%)	(2	(7. 41 %)
) 3	(1.42%)		4	(14.81%)
	- 6	(2.84%)	-	2	(7.41%)
-	" 10	(4.74%)	"		(0.00%)

Results

- Word range
 - Wirepair: Dual core (6 primary, 7 secondary)
 - Nils: No core (short samples, inconclusive)
- Sentence lengths
 - Wirepair: Likes 7-27 words, up to 40
 - Nils: Short sentences (3-20 words)
 - Few samples; inconclusive
 - Punctuation
 - Different frequencies: Likely different people

Summary

- Nils is unlikely Wirepair
 - Different writing styles
- Wirepair wrote stand-alone exploits
- Nils watched Wirepair

"Dorrowod" ood

Epilogue

http://www.d3adlin3.8k.com/index2.html Unofficial report dated 23-June-2004

Rbot.org went down due to Nils and Ago being taken into custody. No official word on whether Nils was charged or convicted.

Keyboard Profiling

Reading Jibberish jfkdowam hfe heriojmfm



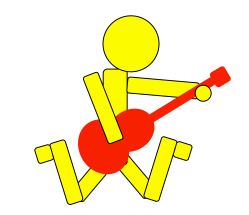
Keyboard Banging Appears...

- Web and Entry Forms
 - Must enter "any" text to continue
 - Account names, user names, addresses
- IRC, IM, Chat rooms
 - Frustration
 - Demonstration
 - Getting attention

szsoie opsurfdeslfjl ersjf!

Caught Red Handed

- Dominant hand performs simpler task
 - Guitar, Violin, Banjo
 - Which is simpler...
 - Mouse or Keyboard?
- Repetition = speed



- Dominant hand is slower at typing
- Random banging
 - More keys from the experienced hand

Left/Right Handed

Where's the mouse?



Ergonomic QWERTY Keyboard Layout

`	1	:	2	3	4	5	6	7	8	9	0	-	=	١	Del
Tab	Q	1	W	e	r	t	У	u	i	0	p]]		
Cap	s	a	S	Ċ	l f	ģ	g l	٦.	j k		;	1		E	nter
Sh	ift		z	X	С	V	b	n	m	,		1		Shi	ift
Ctrl	W	in	A	lt			Spa	ce			Alt	Win	0	pt	Ctrl

ujklhkljkldskl

Left keys: 14% Right keys: 86%

Verdict: Left handed

Left/Right Accuracy

- Roughly 70% accurate
- Requires additional information
 - Keyboard usage frequency
 - Game player, graphic designer, programmer
 - Typist, email, chat room, rarely use mouse
- External factors
 - Left/Right keyboard vs Left/Right handed
 - Carpel tunnel; other injuries

Finger Drumming?

• Inside/Outside drumming split?

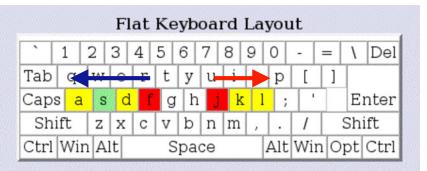
- Ouside-to-In: ASDF LKJH
- Inside-to-Out: FDSA HJKL
- Symmetrical, Asymmetrical, and No Drumming
- Group Experiment!
 - One direction is dominant
 - One direction: Faster, easier
 - Other direction: Slower, clumsier, harder

Finger Drumming!

- 1970 research on child development
- Statistically speaking...
 - Right/Left handed split: 70/30
 - Outside/Inside drumming split: 70/30
 - Outside-to-In = more common (70%)
 - Symmetrical, Asymmetrical, and No Drumming
 - Most people are symmetrical
 - Asymmetrical
 - Left-to-Right = Piano (esp. if they use multiple rows)
 - Right-to-Left = Piano or string instrument
 - No drumming? ADD



Drumming Direction



Ergonomic Keyboard Layout

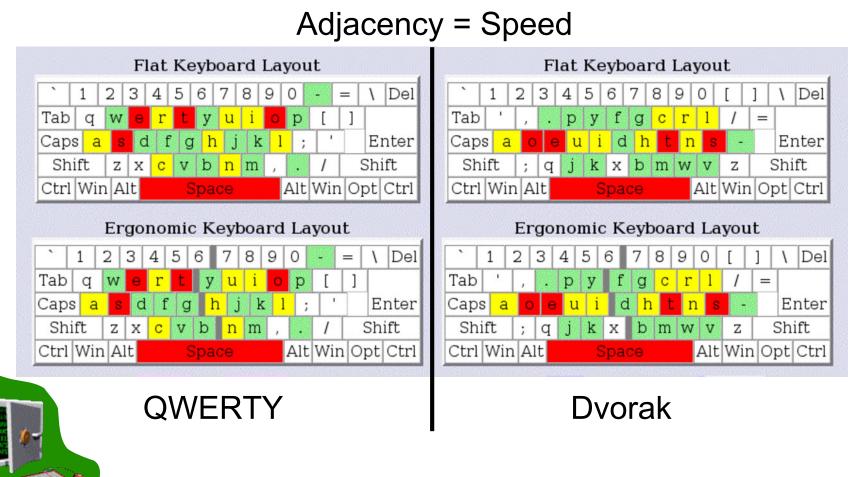
`	1	1	2	3	4	5	6	7	8	9	0	- :	=	١	Del
Tab	C		••	0	1	t	У	' u	i		p	[]		
Cap	s	а	s	d	f	g		h	k	:]	;	1		E	nter
Sh	ift		Z	X	С	V	b	n	m	,		1		Sh	ift
Ctrl	W	in	A	lt			Spa	ace			Alt	Win	0	pt	Ctrl

lfdjskafdjklafj

Right-hand Drumming: Inside-to-out

Left-hand Drumming: Inside-to-out

Sample: BlackHat CFP 2006



Keyboard Detection

lfdjskafdjklafj

Flat Keyboard Layout Del 3 2 4 5 6 7 8 9 0 = Tab W t q е r у р u 0 Caps Enter а S h a Shift Shift z Х С V b |n|m Ctrl Win Alt Alt Win Opt Ctrl Space

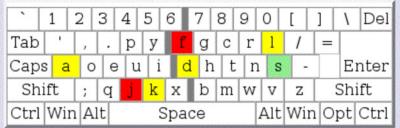
Ergonomic Keyboard Layout

`	1		2	3	4	5	6	7	8	9	0	-	=	: \	Del
Tab	q	[W	e	r	t	3	/ u	i	0	p]]	
Cap	s	a	s	C	l f	g	Į 🛛	h	j ł	2	1;			E	nter
Sh	ift		z	X	С	V	b	n	m	,		1		Sh	ift
Ctrl	W	ïn	A	lt			Spa	ace			Alt	Wi	n	Opt	Ctrl

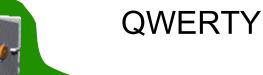
Flat Keyboard Layout

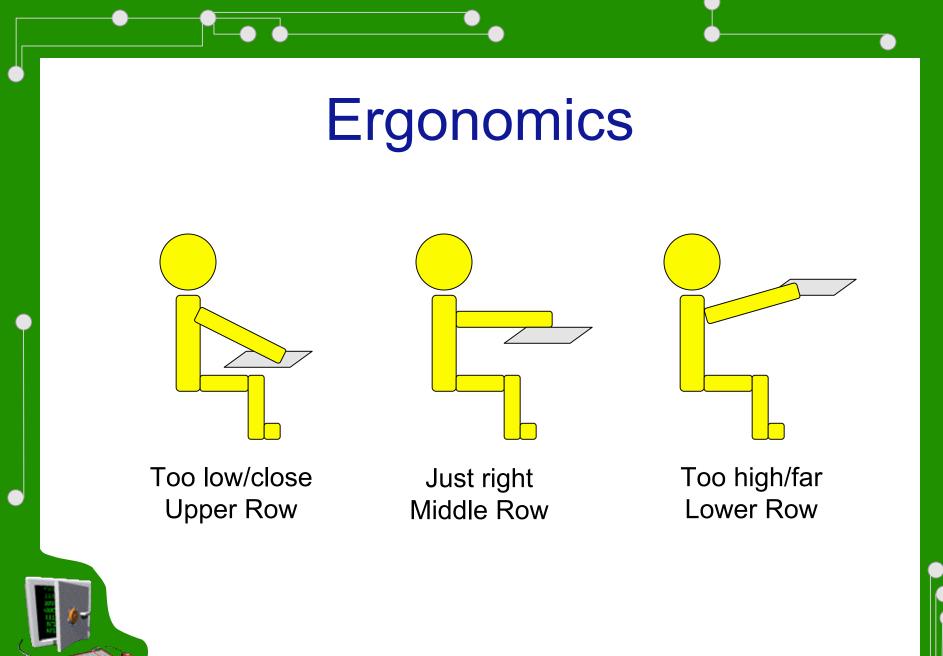
`	1		2	3	4	5	6	7	8	9	0	[]	1	Del
Tab		1	,		p	у	f	g	С	r	1	1	=	=	
Cap	s	а	С) (εl	ı i	d	h	ı t	1	n s	- 18		E	nter
Sh	if	t	;	q	j	k	х	b	m	W	v	Z		Sh	ift
Ctrl	V	Vin	A	lt		5	Spa	ce			Alt	Wi	n	Opt	Ctrl

Ergonomic Keyboard Layout



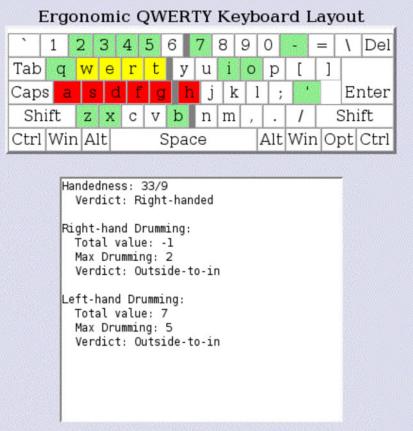
Dvorak





Example: Mark Litscher

(10:21:13) mlitsch: waorheg (10:21:16) mlitsch: -42 tq3 gawr (10:21:43) mlitsch: sdfb e thdfxz (10:22:14) Dr.Neal: Awesome.



Example: Mark Litscher

(10:21:13) mlitsch: waorheg
(10:21:16) mlitsch: -42 tq3 gawr
(10:21:43) mlitsch: sdfb e thdfxzh 57i sdf ghas fg'
(10:22:14) Dr.Neal: Awesome. Hold on.
(10:23:00) Dr.Neal: You are right handed. You drum your fingers from outside-to-in.
(10:23:43) Dr.Neal: Is this correct?
(10:26:05) Dr.Neal: Oh, and you are not using an ergonomic/split keyboard.
(10:28:06) mlitsch: mostly- right handed, non-ergo, drum outside-in correct



Keyboard Profiling Results

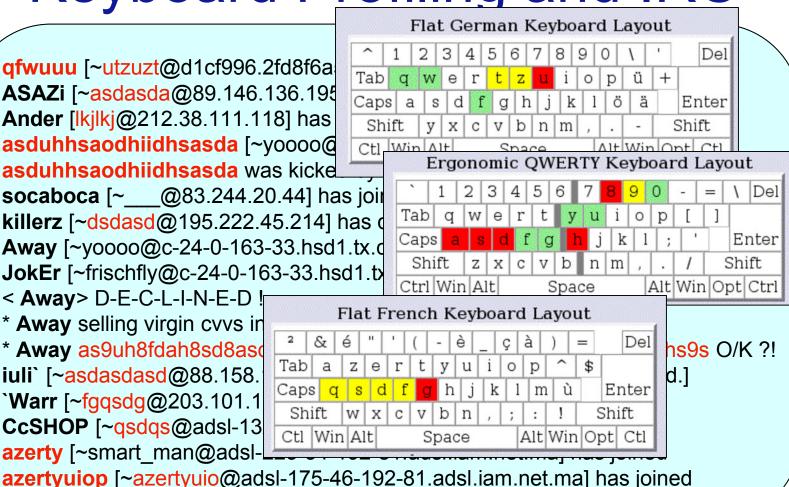
- Left/Right Handed
- Finger Drumming Direction
- Keyboard Type
- Keyboard Location (near/low, far/high)
- Musician, and more!

Keyboard Profiling and IRC

gfwuuu [~utzuzt@d1cf996.2fd8f6a ASAZi [~asdasda@89.146.136.195 Ander [lkjlkj@212.38.111.118] has asduhhsaodhiidhsasda [~yoooo@ asduhhsaodhiidhsasda was kicke socaboca [~ @83.244.20.44] has join killerz [~dsdasd@195.222.45.214] has o Away [~yoooo@c-24-0-163-33.hsd1.tx.d JokEr [~frischfly@c-24-0-163-33.hsd1.tx

< Away> D-E-C-L-I-N-E-D * Away selling virgin cvvs in

* Away as9uh8fdah8sd8asd iuli` [~asdasdasd@88.158. `Warr [~fgqsdg@203.101.1 CcSHOP [~qsdqs@adsl-13] azerty [~smart man@adsl-



Case Study: Dutch Maffia

Chaotic Phishing Group



It's Citibank!

We recently noticed one or more attempts to log in to your Citibank account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have initiated by you. However if you are the rightful holder of the account, click on the link below and submit, as we try to verify your account.

https://web.da-us.citibank.com/cgi-bin/citifi/scripts/login2/login.jsp

The log in attempt was made from: IP address: 66.224.29.186 ISP host: 66-224-29-186atgi.net

If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

We ask that you allow at least 48hrs for the case to be investigated and we strongly recommend not making any changes to your account in that time.

*Please do not respond to this email as your reply will not be received. For assistance, log in to your Citibank account and choose the "HELP" link.

Thanks for your patience as we work together to protect your account.

Regards,

. . .

The Citibank Team

Active URLs in Email

Real Citibank:

http://citibank.com/domain/images/36wav.gif http://citibank.com/domain/images/citi44a.gif Wells Fargo?

http://www.wellsfargo.com/help/jaws_setting.jhtml http://www.wellsfargo.com/auxiliary_access/aa_talkatmloc.jhtml

The link said:

https://web.da-us.citibank.com/cgi-bin/citifi/scripts/login2/login.jsp But links to:

http://web.da-us.inoutrequestinformation.com/citi/login.php

inoutrequestinformation.com

	Looking for: inoutrequestinformation.com
	inoutrequestinformation.com has address 68.142.234.46
	inoutrequestinformation.com has address 68.142.234.47
	inoutrequestinformation.com has address 68.142.234.45
	Domain Name inoutrequestinformation.com
	Creation Date 2005-05-29
	Registration Date 2005-05-29
	Expiry Date 2007-05-29
	Organisation Name Patrick Laxson
	Organisation Address. 1205 S. madison
	Organisation Address. Marion
	Organisation Address. 62959
	Organisation Address. IL
	Organisation Address. UNITED STATES
	Admin Name Patrick Laxson
	Admin Address 1205 S. madison
	Admin Address Marion
	Admin Address 62959
	Admin Address IL
	Admin Address UNITED STATES
	Admin Email patrickhowardtheuntouchable@yahoo.com
	Admin Phone +1.6189932216
т	

web.da-us.inoutrequestinformation.com has address 161.58.97.126

Server: 161.58.97.126

126.97.58.161.in-addr.arpa domain name pointer www.hustingtheuntouchable.com

Looking for: hustingtheuntouchable.com hustingtheuntouchable.com has address 161.58.97.126 Domain Name..... hustingtheuntouchable.com Creation Date..... 2005-06-16 Registration Date.... 2005-06-16 Expiry Date..... 2007-06-16 Organisation Name.... Hiram Shaish Organisation Address. 26218 Redlands Blvd. suite#150 Organisation Address. Redlands Organisation Address. 92373 Organisation Address. CA Organisation Address. UNITED STATES Admin Name..... Hiram Shaish Admin Address..... 26218 Redlands Blvd. suite#150 Admin Address..... Redlands Admin Address..... 92373 Admin Address..... CA Admin Address..... UNITED STATES Admin Email..... hustingtheuntouchable@yahoo.com Admin Phone..... 5126370



Web Server

- Web server on port 80/tcp
 - Server: Rapidsite/Apa/1.3.31 (Unix) FrontPage/5.0.2.2510 mod_ssl/2.8.17 OpenSSL/0.9.7c
 - Open directories: http://.../citi/login_files/
- Files
 - Mirrored using Mozilla "Save As"
 - File names, no line wraps, no CRLF

Server Files

16/Jun/2005:09:52:34 File: citi/loginerror_files/rtopic_h.gif 16/Jun/2005:09:52:35 File: citi/loginerror_files/citi44a.gif 16/Jun/2005:09:52:35 File: citi/loginerror_files/member_citigroup.gif 16/Jun/2005:09:52:36 File: citi/loginerror_files/footlogo.gif 16/Jun/2005:09:52:37 File: citi/loginerror_files/m4_2.gif 16/Jun/2005:09:52:39 File: citi/loginerror_files/error.gif 16/Jun/2005:09:52:40 File: citi/loginerror_files/36wav.gif 16/Jun/2005:09:52:43 File: citi/loginerror_files/pcdom 16/Jun/2005:09:52:45 File: citi/loginerror_files/sniffer.js 16/Jun/2005:09:52:51 File: citi/loginerror_files/loginutils.js 16/Jun/2005:09:52:56 File: citi/loginerror_files/branding.js 16/Jun/2005:09:52:57 File: citi/loginerror_files/1blue.gif

Ordering:Not alphabetical (inode)= TAR or SCPDelay:1-2 seconds between files= FTP or SSH

16/Jun/2005:09:53:08 File: citi/signoff_thanks.jsp_files/member_citigroup.gif 16/Jun/2005:09:53:09 File: citi/signoff_thanks.jsp_files/byg_arrow.gif 16/Jun/2005:09:53:11 File: citi/signoff_thanks.jsp_files/footlogo.gif 16/Jun/2005:09:53:13 File: citi/signoff_thanks.jsp_files/m4_2.gif 16/Jun/2005:09:53:14 File: citi/signoff_thanks.jsp_files/caret.gif 16/Jun/2005:09:53:16 File: citi/signoff_thanks.jsp_files/36wav.gif 16/Jun/2005:09:53:16 File: citi/signoff_thanks.jsp_files/citi44a.gif 16/Jun/2005:09:53:17 File: citi/signoff_thanks.jsp_files/pcdom 16/Jun/2005:09:53:18 File: citi/signoff_thanks.jsp_files/sniffer.js

Sightings of Similar Servers

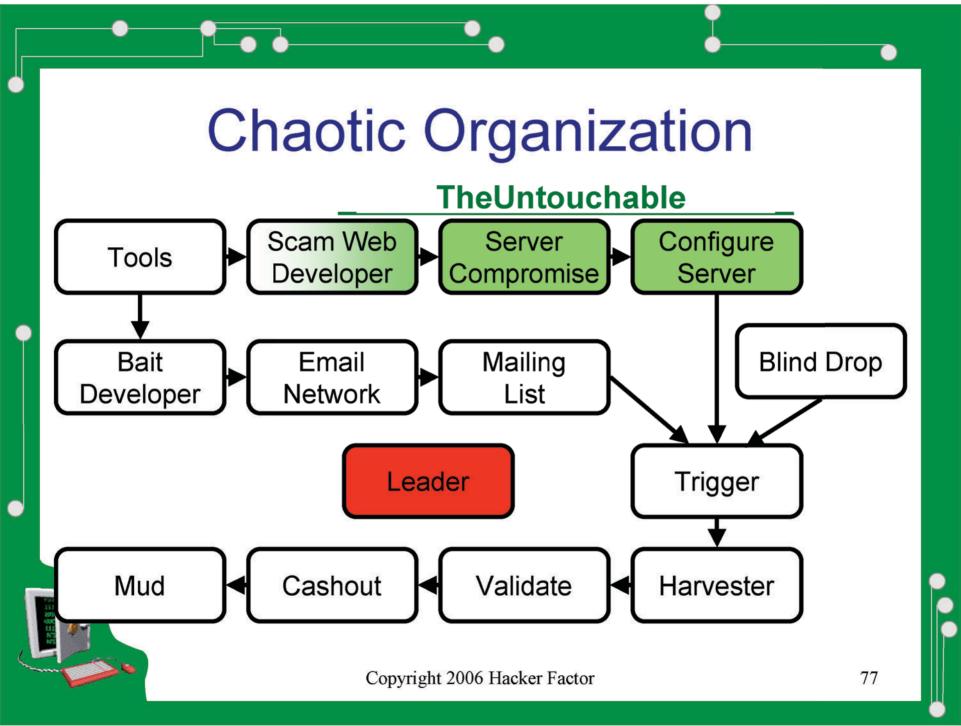
- 2005-01-14.ebay/ 2005-02-01.citizens/ 2005-02-02.huntington/ 2005-02-09.wamu/ 2005-02-12.southtrust/ 2005-02-15.domain/ 2005-03-07.ebay/ 2005-03-08.ebay/ 2005-03-16.ebay/ 2005-03-16.ebay-b/ 2005-03-17.ebay/ 2005-03-21.keybank/ 2005-03-25.union/
- 2005-03-30.keybank/ 2005-04-03.mibank/ 2005-04-04.egold/ 2005-04-15.ebay/ 2005-04-24.regions/ 2005-05-22.lasallebank/ 2005-05-27.southtrust/ 2005-06-03.paypal/ 2005-06-05.southtrust/ 2005-06-07.ebay/ 2005-06-11.ebay/ 2005-06-12.citi/ 2005-06-13.usbank/
- 2005-06-14.citi/ 2005-06-17.citi/ 2005-06-17.irc/ 2005-06-24.lasalle/ 2005-06-30.bofa/ 2005-07-04.ebay/ 2005-08-25.ebay/ 2005-09-10.ebay/ 2005-09-30.paypal/ 2005-10-06.chase/

- eBay & Citibank are favorites
- No target consistency, large variety
- No date consistency -- skips random days and weeks
- Volume drops after June 2005, stops in October 2005

Common Attributes

- Many common attributes
 - "TheUntouchable" in domain name
 - Open directories on server
 - Server file configured in inode order
 - tar or SSH's scp
- Server seems solid and consistent
 - Scams vary from amateurish to professional
 - No consistency in targets or volume
 - Even mass mailings vary in size!

		Received: from e-gold.com				
		(unknown[211.236.138.21] (misconfigured sender))				
		by sccrmxc16.comcast.net (sccrmxc16) w	ith SMTP			
		id <20050404095052s1600eda73e>; Mon, 4	Apr 2005			
		09:51:04 +0000				
		X-Originating-IP: [211.236.138.21]				
		From: <andybfbml@e-gold.com></andybfbml@e-gold.com>				
		To: <maandi@comcast.net></maandi@comcast.net>				
B	Received: from 80.97.187	Subject: Password failure, your e-gold.com accou	int, rechedk			
_	by rwcrmxc20.c	Data: Non 4 Jan 2005 05:52:20 0500				
x-	id <2005061716	Nime Mension, 1.0				
	Coriginating-IP: [80.97	Contont Three, tout /html, changet-up again				
		201 by ; Sat, 18 Jun 2005 22:04:57 +0500				
	Message-ID: <deflate@msn< td=""><td>-</td><td>id</td></deflate@msn<>	-	id			
	-	erservices@citibank.com>				
		stomerservices@citibank.com>				
			<u> </u>			
	Subject: Citibert					
D	Date: Sat, 18 Jun id 1-0504468221					
Re X	X-Mailer: Microso for <ne2@comcast.net>; Wed, 16 Mar 2005 16:23:41 -0500</ne2@comcast.net>					
n M	IIME-Version: 1.0 (EST)	101 (hez@comcast.het/, wed, 10 Mai 2005 10.25.41	-0300			
C	Contont_Trings mul	ed: (from pewotu@localhost)				
x-	boundary=	by pewoturh.com (8.12.11/8.12.9/Submit) id j2GLN	fig057130 ·			
Re X	-Priority: 1	Wed, 16 Mar 2005 16:23:41 -0500 (EST)	1)903/130/			
aı X	-MSMail-Priority	(envelope-from pewotu)				
Date	e: Tue, 01 Feb 20 Date:	Wed, 16 Mar 2005 16:23:41 -0500 (EST)				
Mes		-Id: <200503162123.j2GLNfjg057130@pewoturh.com>				
Fro		oop@comcast.net				
To:		t: Recover Your Account!				
	ject: Important (From:	eBay Notice <aw-confirm@ebay.com></aw-confirm@ebay.com>				
MIM	' /	To: aw-confirm@ebay.com				
Con		ersion: 1.0				
	-boundary=" Conten	t-Type: text/html				
		t-Transfer-Encoding: 8bit				
		-Detect:1				



> register ≫ f.a.q. ≫ member list	
» <u>DutchMaffia Forums</u> » <u>View Profile</u> » TheUntouchable	User Name User Name Remember Me? Password Log in
View Profile: TheUntouchable	
TheUntouchable Administrator	Last Activity: 07-09-2005 01:51 Offline
Forum Info	Contact Info
Join Date: 23-04-2005 Posts Total Posts: 29 (0.11 posts per day)	Email: <u>Send a message via email to TheUntouchable</u> Private Message: <u>Send a private message to TheUntouchable</u>
Find all posts by TheUntouchable	

DutchMaffia

Name: DutchMaffia

Web servers: www.dutchmaffia.org (web forum)

IRC Servers:

irc.dutchmaffia.org

Channel Topics:

Welcome to #mafia, for chat, rooters and scanners join #mafia-chat Now serving: XXX.State.Of.The.Union.2005.DVDRip.XviD-iMBT, Area.51-Reloaded, House.Of.Ass.XXX.DVDRiP.XviD-DivXfacTory, Be.Cool.DVDSCR.XviD-DoNE, Assturbators.2.XXX.DVDRip.XviD-Pr0nStarS

.rm Welcome to #mafia, for chat, rooters and scanners join #mafiachat Now serving: Area.51-Reloaded, House.Of.Ass.XXX.DVDRiP.XviD-DivXfacTory, Be.Cool.DVDSCR.XviD-DoNE, Assturbators.2.XXX.DVDRip.XviD-Pr0nStarS

Join for all ur warez, talk about bots, or just aboyt something else :) If you want to link, contact TheUntouchable(at)dutchmaffia dot org

- TheUntouchable	-	(Dutch,English)
- AdolfO	_	(Dutch, English, German)

And the best part...

31-05-2005, 09:07	# <u>3</u>					
TheUntouchable Administrator	Join Date: Apr 2005 Posts: 29					
Heb ff je thread hierbij in gedrukt 🥶 Ik ben er zeker, met de trein maarja kan ik wel drinken 🥲	» ФИОТЕ					
11-06-2005, 02:46	# <u>4</u>					
TheUntouchable	Join Date: Apr 2005 Posts: 29					
OK het staat vast, om Zondag 12 juni, 13:00, Spido toren, Willemsplein 85, Rotterdam!						
BE THERE!	нь рирте					
	"OKAY is certain, for Sunday 12 June, 13:00, Spido toren, Willemsplein 85, Rotterdam! BE THERE!"					
http://www.dutchmaffia.org/showthread.php?t=4						
Copyright 2006 Hacker Factor	80					

👔 📄 http://www.dutchmaffia.org	/showthread.php?t=8 🕑 Go	
s - New		
DutchMaffia.org Forums * register * f.a.q. * member list		
TheUntouchable	Join Date: Apr 2005	
Administrator	FUSIS. 29	
New Feature: Flood pro	Handedness Right handed (70% of populat	tion
Hi peepz, I just build in flood protection.	Right handDrums outside-to-inLeft handDrums inside-to-out	liui
Anti-Flood fe	Asymmetrical drumming < 5% of the population He is less than 3.5% of the total population	
Example:		/11
<pre>*** Evil2 (~jcvibhcih@Clk-3472 *** Evil3 (<u>~toijhlihs@Clk-38D3</u> *** Evil4 (<u>~eihjifihi@Clk-5387E</u> snip XX lines *** Evil21 (<u>~jiovoihew@Clk-48</u> -server1.test.net: #test *** Ch *** server1.test.net sets mod fsdjfdshfdkjfdkjfdsgdskjgsdjgs fsdjfdshfdkjfdkjfdsgdskjgsdjgs fsdjfdshfdkjfdkjfdsgdskjgsdjgs fsdjfdshfdkjfdkjfdsgdskjgsdjgs</pre>	34D84B.blah.net) has joined #test 2A942.xx.someispcom) has joined #test 74A3.aol.com) has joined #test 342F.dfdfd.blablalba.be) has joined #test 2B26C3.e.something.org) has joined #test annel joinflood detected (limit is 20 per 15 seconds), putting +i e: +i sdsdfsfdujsflkhsfdl sdsdfsfdujsflkhsfdl sdsdfsfdujsflkhsfdl	
fsdjfdshfdkjfdkjfdsgdskjgsdjg snip Last edited by The Untouchable	sdsdfsfdujsfikhsfdl	81

10.00

Phishing Summary

DutchMaffia

- Focus:
 - System compromise & configuration
 - File swapping (warez, porn, music, video)
 - Dabbled in phishing; part of a chaotic phishing group
- Domain "dutchmaffia.org" no longer active
- TheUntouchable
 - No longer phishing: Stopped in October 2005
 - Not active web forum: Stopped in September 2005
 - Not observed active on IRC
 - As of May 2006, IRC server down
 - Right handed, asymmetrical drumming (from right to left)

Things that don't work...

Not every good theory works well in real life



Unique Typing

- Studies have shown
 - Typing speed/pressure are unique!
 - Great for biometric authentication systems
 - But there's a problem:
 - IRC, IM, and other online forums do not convey speed/pressure
 - Good in theory...
 - Poor for forensics/profiling

Age From Vocabulary

- Some words are generation-specific
 Neat, Neato, Cool, Bad, Rad, Wicked, the Bomb
- Online forums
 - People influence each other
 - Words by one person are used by another
 - Cut-n-paste
 - Translation systems

Conclusion



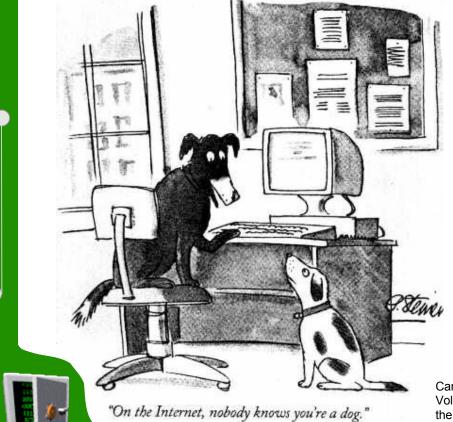
Computers and Science

- Investigative Science
 - Computers are a new field
 - Few Forensic and Profiling tools
 - Focus on collection, systems, and networks
 - Plenty of opportunity for new techniques
- Anonymity
 - Can protect identify to a degree
 - Be careful what you expose...

Topics Covered

- Gender Analysis
 - Surmise gender from writing style
 - Theorize nationality
- Author Analysis
 - Distinguish samples by different authors
- Keyboard Profiling
 - Random characters denote physical attributes

Non-Classical Forensics



"But they can tell if you are a left-handed, female, piano player with an ergonomic keyboard."

Cartoon by Peter Steiner, reproduced from The New Yorker, pg 61, July 5, 1993, Vol. 69 (LXIX) no. 20 for academic discussion and research. This complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

Questions?

Dr. Neal Krawetz Hacker Factor Solutions www.hackerfactor.com

Shameless self-promotion.

The topics covered in this presentation only have a passing mention in the book, but the book does cover topics of anonymity and network forensics.

INTRODUCTION to NETWORK SECURITY

 Provides an in-depth reference to current network security standards and procedures

 Uses examples based on the most common network protocols

 Defines applicable threat models, mitigation methods, and concepts

 Explores the International Standards Organization's Open Systems Interconnection (ISO OSI) net work stack

 Includes a CD-ROM with source code, RFC documents, and figures from the book



Networking Series

NEAL KRAWETZ