Non-Classical Computer Forensics

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

Copyright 2006 Hacker Factor
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

• 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

<table>
<thead>
<tr>
<th></th>
<th>System-Oriented</th>
<th>Network-Oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection</strong></td>
<td>• Checksums</td>
<td>• Tcpdump, Ethereal/Wireshark, Snort</td>
</tr>
<tr>
<td></td>
<td>• Mirror, dd, cpio</td>
<td></td>
</tr>
<tr>
<td><strong>Forensics</strong></td>
<td><strong>Common</strong></td>
<td><strong>Common</strong></td>
</tr>
<tr>
<td></td>
<td>• TCT, Sleuthkit, Autopsy</td>
<td>• nmap, scanrand</td>
</tr>
<tr>
<td></td>
<td>• Undelete</td>
<td>• DNS, WHOIS</td>
</tr>
<tr>
<td></td>
<td>• John the Ripper</td>
<td>• Snort, Ethereal, ngrep</td>
</tr>
<tr>
<td></td>
<td><strong>Uncommon</strong></td>
<td><strong>Uncommon</strong></td>
</tr>
<tr>
<td></td>
<td>• Spinrite, Un-format</td>
<td>• Honeypots</td>
</tr>
<tr>
<td></td>
<td>• File-to-sector location</td>
<td></td>
</tr>
<tr>
<td><strong>Profiling</strong></td>
<td><strong>Common</strong></td>
<td><strong>Common</strong></td>
</tr>
<tr>
<td></td>
<td>• ‘file’, text content</td>
<td>• ‘nmap -O -sV’, p0f</td>
</tr>
<tr>
<td></td>
<td>• Log, email, web analysis</td>
<td>• IP-to-user</td>
</tr>
<tr>
<td></td>
<td><strong>Uncommon</strong></td>
<td><strong>Uncommon</strong></td>
</tr>
<tr>
<td></td>
<td>• stegdetect, image analysis</td>
<td>• snacktime</td>
</tr>
<tr>
<td></td>
<td>• Common usage patterns (time, server type, etc.)</td>
<td>• htprint</td>
</tr>
<tr>
<td></td>
<td>• Application identification</td>
<td></td>
</tr>
</tbody>
</table>
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 IRSSSI 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, IM, Chat-room)**
- actually: -49
- am: -42
- as: 37
- because: -55
- but: -43
- ever: 21
- everything: -44
- good: 31
- him: -73
- in: 10
- like: -43
- now: 33
- since: -25
- some: 58
- the: 17
- too: -38
- well: 15

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

- Black Hat 2006 CFP
  - “Formal” writing
    - A = 6 x 1 score of 6, seen once
    - And = -4 x 3 score of -4, seen 3 times
    - It = 6 x 1
    - The = 7 x 6
    - To = 2 x 5
    - Was = -1 x 1
    - Who = 19 x 1

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

- $40\% < |\text{male}| \div (|\text{male}|+|\text{female}|) < 60\%$
  - 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

<table>
<thead>
<tr>
<th>Tests as:</th>
<th>Says:</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td></td>
<td>57% (1946)</td>
<td>43% (1456)</td>
</tr>
<tr>
<td>Weak Male</td>
<td></td>
<td>22% (748)</td>
<td>20% (681)</td>
</tr>
<tr>
<td>Weak Female</td>
<td></td>
<td>11% (370)</td>
<td>14% (481)</td>
</tr>
<tr>
<td>Female</td>
<td></td>
<td>6% (207)</td>
<td>12% (393)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4% (123)</td>
<td>11% (383)</td>
</tr>
</tbody>
</table>

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

SEX WITH FECES-SCATOLOGY

Current mood: 😖 dirty
Category: Blogging

Oh yeah. I'm going to talk about it. Scatologists...people who have an extreme infatuation with human feces. For the record...Ew. Wait...let me repeat that for the record...Ew. Scatologists...people who have an extreme infatuation with human feces. I don't even know why I'm talking about this.

Mother fucker that is soooo fucking gross. What on earth? Please tell me WHY? I don't get it, and don't fucking try it all in life.” PEOPLE: THAT’S ONE THING I WILL NOT jizz on me, spit on me, and fucking do weird things on me.

I'd like to tell you all a story.

Once upon a mother fuc*ing time, there was a fucktard who contacted me on myspace asking me to have sex with him. You can imagine my reaction "Oh...
Example: Ashley

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
Example: Samantha Jee

Total words: 330

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

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
Copyright 2006 Hacker Factor
Example: Alia

http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=2150152&blogID=130805539

Total words: 2333

Genre: Informal
Female = 2002
Male = 3624
Difference = 1622; 64.41%
Verdict: MALE

Genre: Formal
Female = 1870
Male = 3152
Difference = 1282; 62.76%
Verdict: MALE

Copyright 2006 Hacker Factor
Gender Guesser ONLINE

http://www.hackerfactor.com/

Click on “Forensics”

Gender Guesser

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

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.

Enter text here.

Results
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

Protection from prying NSA eyes
Mark Rasch, 2006-05-15

From the U.S. Fourth Amendment, the Stored Communications Act and U.S. wiretap laws to the Pen-register statute, Mark Rasch looks at legal protections available to the telecommunication companies and individual Americans in the wake of the NSA's massive spying program.

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.

One day, you receive a visit from agents of the National Security Agency, who make a formal request:

“Note here [in Title 18 U.S.C. 2702(a)(3)] that it is the telephone companies which

Attackers are targeting you

Note here [in Title 18 U.S.C. 2702(a)(3)] that it is the telephone companies which
### Example: Mark Rasch

#### Core Words

<table>
<thead>
<tr>
<th>Rank</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>298</td>
<td>7.98%</td>
<td>the</td>
</tr>
<tr>
<td>117</td>
<td>3.13%</td>
<td>to</td>
</tr>
<tr>
<td>113</td>
<td>3.03%</td>
<td>of</td>
</tr>
<tr>
<td>91</td>
<td>2.44%</td>
<td>that</td>
</tr>
<tr>
<td>84</td>
<td>2.25%</td>
<td>and</td>
</tr>
<tr>
<td>77</td>
<td>2.06%</td>
<td>a</td>
</tr>
<tr>
<td>64</td>
<td>1.71%</td>
<td>or</td>
</tr>
<tr>
<td>56</td>
<td>1.50%</td>
<td>in</td>
</tr>
<tr>
<td>45</td>
<td>1.21%</td>
<td>for</td>
</tr>
<tr>
<td>39</td>
<td>1.04%</td>
<td>you</td>
</tr>
<tr>
<td>35</td>
<td>0.94%</td>
<td>it</td>
</tr>
<tr>
<td>35</td>
<td>0.94%</td>
<td>government</td>
</tr>
<tr>
<td>34</td>
<td>0.91%</td>
<td>not</td>
</tr>
<tr>
<td>33</td>
<td>0.88%</td>
<td>is</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

#### Core Words

<table>
<thead>
<tr>
<th>Rank</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>116</td>
<td>5.88%</td>
<td>the</td>
</tr>
<tr>
<td>71</td>
<td>3.60%</td>
<td>to</td>
</tr>
<tr>
<td>58</td>
<td>2.94%</td>
<td>a</td>
</tr>
<tr>
<td>56</td>
<td>2.84%</td>
<td>in</td>
</tr>
<tr>
<td>49</td>
<td>2.48%</td>
<td>of</td>
</tr>
<tr>
<td>45</td>
<td>2.28%</td>
<td>and</td>
</tr>
<tr>
<td>34</td>
<td>1.72%</td>
<td>that</td>
</tr>
<tr>
<td>28</td>
<td>1.42%</td>
<td>is</td>
</tr>
<tr>
<td>28</td>
<td>1.42%</td>
<td>be</td>
</tr>
<tr>
<td>27</td>
<td>1.37%</td>
<td>forensic</td>
</tr>
<tr>
<td>24</td>
<td>1.22%</td>
<td>or</td>
</tr>
<tr>
<td>20</td>
<td>1.01%</td>
<td>computer</td>
</tr>
<tr>
<td>19</td>
<td>0.96%</td>
<td>not</td>
</tr>
<tr>
<td>17</td>
<td>0.86%</td>
<td>by</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
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
   17  0.77% this
   17  0.77% is
   15  0.68% on
   15  0.68% all
   14  0.64% was
Both Examples

<table>
<thead>
<tr>
<th>Mark Rasch</th>
<th>Scott Granneman</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Total words: 1974</td>
<td>#Total words: 2196</td>
</tr>
<tr>
<td>#Total distinct words: 679 (34.40%)</td>
<td>#Total distinct words: 939 (42.76%)</td>
</tr>
<tr>
<td>#Single words:</td>
<td></td>
</tr>
<tr>
<td>116 5.88% the</td>
<td>138 6.28% the</td>
</tr>
<tr>
<td>71 3.60% to</td>
<td>68 3.10% of</td>
</tr>
<tr>
<td>58 2.94% a</td>
<td>62 2.82% to</td>
</tr>
<tr>
<td>56 2.84% in</td>
<td>62 2.82% and</td>
</tr>
<tr>
<td>49 2.48% of</td>
<td>56 2.55% a</td>
</tr>
<tr>
<td>45 2.28% and</td>
<td>51 2.32% in</td>
</tr>
<tr>
<td>34 1.72% that</td>
<td>37 1.68% that</td>
</tr>
<tr>
<td>28 1.42% is</td>
<td>22 1.00% for</td>
</tr>
<tr>
<td>28 1.42% be</td>
<td>20 0.91% it</td>
</tr>
<tr>
<td>27 1.37% forensic</td>
<td>17 0.77% this</td>
</tr>
<tr>
<td>24 1.22% or</td>
<td>17 0.77% is</td>
</tr>
<tr>
<td>20 1.01% computer</td>
<td>15 0.68% on</td>
</tr>
<tr>
<td>19 0.96% not</td>
<td>15 0.68% all</td>
</tr>
<tr>
<td>17 0.86% by</td>
<td>14 0.64% was</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Punctuation Examples

Mark Rasch
Sample #1
. 140 (22.44%)
? 18 (2.88%)
! 1 (0.16%)
, 218 (34.94%)
: 4 (0.64%)
; (0.00%)
( 27 (4.33%)
) 27 (4.33%)
- 59 (9.46%)
" 93 (14.90%)

Sample #2
. 95 (27.14%)
? 6 (1.71%)
! 3 (0.86%)
, 122 (34.86%)
: 2 (0.57%)
; (0.00%)
( 10 (2.86%)
) 10 (2.86%)
- 42 (12.00%)
" 44 (12.57%)

Scott Granneman
Sample #1
. 81 (26.56%)
? 16 (5.25%)
! 4 (1.31%)
, 95 (31.15%)
: 3 (0.98%)
; 2 (0.66%)
( 7 (2.30%)
) 7 (2.30%)
- 16 (5.25%)
" 32 (10.49%)

Sample #2
. 99 (27.50%)
? 5 (1.39%)
! 4 (1.11%)
, 131 (36.39%)
: 11 (3.06%)
; 3 (0.83%)
( 7 (1.94%)
) 7 (1.94%)
- 27 (7.50%)
" 20 (5.56%)
# Sentence Length Examples

## Mark Rasch

<table>
<thead>
<tr>
<th>Sentence Length</th>
<th>Word Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>43</td>
<td>2</td>
<td>1.94%</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>1.94%</td>
</tr>
<tr>
<td>28</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>27</td>
<td>4</td>
<td>3.88%</td>
</tr>
<tr>
<td>24</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>21</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>20</td>
<td>8</td>
<td>7.77%</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>17</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>16</td>
<td>5</td>
<td>4.85%</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>3.88%</td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>9.71%</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>3.88%</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>3.88%</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>2.91%</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>4.85%</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>5.88%</td>
</tr>
</tbody>
</table>

## Scott Granneman

<table>
<thead>
<tr>
<th>Sentence Length</th>
<th>Word Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>2</td>
<td>1.96%</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
<td>1.96%</td>
</tr>
<tr>
<td>31</td>
<td>3</td>
<td>2.94%</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>1.96%</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>2.94%</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>1.96%</td>
</tr>
<tr>
<td>25</td>
<td>5</td>
<td>4.90%</td>
</tr>
<tr>
<td>23</td>
<td>5</td>
<td>4.90%</td>
</tr>
<tr>
<td>22</td>
<td>6</td>
<td>5.88%</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
<td>3.92%</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>2.94%</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>2.94%</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>3.92%</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>3.92%</td>
</tr>
<tr>
<td>16</td>
<td>3</td>
<td>2.94%</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>3.92%</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>1.96%</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>3.92%</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>5.88%</td>
</tr>
</tbody>
</table>
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

// Format: xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
// Only alphanumeric characters

void gen_unique_id(char *szString, int iLen)
{
    memset(szString, 0, iLen);
    for(int i=0; i<iLen; i++)
    {
        int sel=brandom(1, 3);
        switch(sel)
        {
        case 1: // Numeric characters
            szString[i]=(char)brandom(48, 57);
            break;
        case 2: // Uppercase letters
            szString[i]=((char)brandom(65, 90));
            break;
        case 3: // Lowercase letters
            szString[i]=((char)brandom(97, 122));
            break;
        case 4: // Special characters
            szString[i]=((char)brandom(33, 126));
            break;
        }
    }
}

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.
 */
items CDKeyList[] =
{
    "[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

```
#include "main.h"
#include "radminscanner.h"
#include "mainctrl.h"
#include "utility.h"
#include "shellcode.h"

#include <windows.h>
#include <process.h>
#pragma comment(lib, "ws2_32.lib")

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <sys/types.h>
#include <time.h>
```

Title: Radmin Massrooter
Author: Nils <nils@rBot.org
Comments: I know, sorry, the code looks kinda fucked up. ;-)
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,
Create an account

Modules
- Home
- Forums
- Downloads
- FAQ
- Feedback
- Journal
- Private Messages
- Search
- Statistics
- Stories Archive
- Submit News
- Surveys
- Top 10
- Topics
- WebMail
- Your Account

Languages
Select Interface Language:

[English]

---

IRC Community Started!

Hello!

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 :-)).

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

---

Survey
What bot are you using?
- rBot
- Spybot
- GT Bot
- Ajobot private version
- 2, Or more bots
- My Own Bot
- SDbot
- Something else..
- I dont have a botnet

Vote

Results

Polls

Votes: 89
Comments: 0

Login

Nickname
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 <= 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);
...
From: "wirepair" <wirepair@rogueemail.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
null

0349.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(atoi(argv[2]) == 1) {
    memset(unicode, 0x00, sizeof(unicode));
    for (x = 0, i = 0; i <= 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);

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 <= 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: wdssscanner.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

<table>
<thead>
<tr>
<th>Wirepair</th>
<th>Nils</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>msrant.html</strong></td>
<td><strong>AOL email</strong></td>
</tr>
<tr>
<td>. 33 (32.35%)</td>
<td>. 8  (24.24%)</td>
</tr>
<tr>
<td>? 5 (4.90%)</td>
<td>?  (0.00%)</td>
</tr>
<tr>
<td>! 3 (2.94%)</td>
<td>!  (0.00%)</td>
</tr>
<tr>
<td>, 30 (29.41%)</td>
<td>, 2  (6.06%)</td>
</tr>
<tr>
<td>: 1 (0.98%)</td>
<td>:  (0.00%)</td>
</tr>
<tr>
<td>;               (0.00%)</td>
<td>;  (0.00%)</td>
</tr>
<tr>
<td>( 1 (0.98%)</td>
<td>( 7 (21.21%)</td>
</tr>
<tr>
<td>) 1 (0.98%)</td>
<td>) 5  (15.15%)</td>
</tr>
<tr>
<td>- 1 (0.98%)</td>
<td>- 8  (24.24%)</td>
</tr>
<tr>
<td>&quot; 2 (1.96%)</td>
<td>&quot;  (0.00%)</td>
</tr>
<tr>
<td><strong>thescene.html</strong></td>
<td>**<a href="http://www.rbot.org**">www.rbot.org**</a></td>
</tr>
<tr>
<td>. 75 (35.55%)</td>
<td>. 6  (22.22%)</td>
</tr>
<tr>
<td>? 8 (3.79%)</td>
<td>?  (0.00%)</td>
</tr>
<tr>
<td>!               (0.00%)</td>
<td>! 3  (11.11%)</td>
</tr>
<tr>
<td>, 52 (24.64%)</td>
<td>,  (0.00%)</td>
</tr>
<tr>
<td>: 5 (2.37%)</td>
<td>: 7  (25.93%)</td>
</tr>
<tr>
<td>;               (0.00%)</td>
<td>;  (0.00%)</td>
</tr>
<tr>
<td>( 3 (1.42%)</td>
<td>( 2 (7.41%)</td>
</tr>
<tr>
<td>) 3 (1.42%)</td>
<td>) 4  (14.81%)</td>
</tr>
<tr>
<td>- 6 (2.84%)</td>
<td>- 2  (7.41%)</td>
</tr>
<tr>
<td>&quot; 10 (4.74%)</td>
<td>&quot;  (0.00%)</td>
</tr>
</tbody>
</table>
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
  “Borrowed” code

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?

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?
  - Outside-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

**Right-hand Drumming:**
Inside-to-out

**Left-hand Drumming:**
Inside-to-out
Sample: BlackHat CFP 2006

Adjacency = Speed

QWERTY

Dvorak
Keyboard Detection

QWERTY  Dvorak
Ergonomics

Too low/close
Upper Row

Just right
Middle Row

Too high/far
Lower Row
Example: Mark Litscher

(10:21:13) mlitsch: waorheg
(10:21:16) mlitsch: -42 tq3 gawn
(10:21:43) mlitsch: sdfb e thdfxzh 57i sdf ghas fg'
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'
(10:23:00) 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

qfwuuu [~utzuzt@d1cf996.2fd8f6a5.dip.t-dialin.net] has joined
ASAZi [~asdasda@89.146.136.195] has quit [Ping timeout]
Ander [lkjlj@212.38.111.118] has joined
asduhhsaodhiddhsasdasdasda [~yoooo@c-24-0-163-33.hsd1.tx.comcast.net] has joined
asduhhsaodhiddhsasda was kicked by ChanServ [User has been banned]
socaboca [~___@83.244.20.44] has joined
killerz [~dsdasd@195.222.45.214] has quit
Away [~yoooo@c-24-0-163-33.hsd1.tx.comcast.net] has joined
JokEr [~frischfly@c-24-0-163-33.hsd1.tx.comcast.net] has joined
< Away> D-E-C-L-I-N-E-D !!
* Away selling virgin cvvs in cheap prices msg me!
* Away as9uh8fdah8sd8asd80ghasdghas08dyhas08hdas9dhas9dha8hs9s O/K ?!
iuli` [~asdasdasd@88.158.182.17] has quit [autokilled: You are banned.]
`Warr [~fgqsdg@203.101.176.65] has joined
CcSHOP [~qsdqs@adsl-132-230-192-81.adsl2.iam.net.ma] has joined
azerty [~smart_man@adsl-223-34-192-81.adsl.iam.net.ma] has joined
azertyuiop [~azertyuiop@adsl-175-46-192-81.adsl.iam.net.ma] has joined
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:
 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
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/2005:09:52:57 File: citi/loginerror_files/1blue.gif

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

### Sightings of Similar Servers

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>Date</th>
<th>Domain</th>
<th>Date</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-03-08</td>
<td>ebay/</td>
<td>2005-06-03</td>
<td>paypal/</td>
<td>2005-09-10</td>
<td>ebay/</td>
</tr>
<tr>
<td>2005-03-17</td>
<td>ebay/</td>
<td>2005-06-11</td>
<td>ebay/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-03-21</td>
<td>keybank/</td>
<td>2005-06-12</td>
<td>citi/</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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!
Email Headers

X-Message-Info: vlt/R+275/AD/pd+6/6910983558178
Received: from hen830.lydia.support@citizensbank.com (bombay665.support@citizensbank.com [212.198.184.144]) by smtp-jackboot.deluge.support@citizensbank.com (Postfix) with SMTP id 9WJ20VO50QSZ for <mace3@comcast.net>; Wed, 02 Feb 2005 00:16:11 +0100
Received: from smtp-cutover.kenyon.support@citizensbank.com ([212.198.184.144]) by n662-fmo3.support@citizensbank.com with Microsoft SMPSVC(5.0.4239.5239); Wed, 02 Feb 2005 05:13:11 +0600
Received: from smtp-spa.lysergic.support@citizensbank.com ([212.198.184.144]) by ya17-ndh71.support@citizensbank.com with Microsoft SMPSVC(5.0.7003.3978); Wed, 02 Feb 2005 01:22:11 +0200
X-Message-Info: QHHL+%ND_LC_CHAR[1-3]944+m+YC+2/874399961700413
Received: from nasal.support@citizensbank.com ([63.255.198.31]) by around.support@citizensbank.com with MailEnable ESMTP; Tue, 01 Feb 2005 17:15:11 -0600
Date: Tue, 01 Feb 2005 22:15:11 -0100
Message-Id: <70484471930.69167@support@citizensbank.com>
From: CitizensBank <support@citizensbank.com>
To: Mace3 <mace3@comcast.net>
Subject: Important Online Banking Alert

MIME-Version: 1.0 (produced by maximilianmeddle 1.7)
Content-Type: multipart/alternative;
 boundary="--13383712623623368434"

Received: from 80.97.187.189 ([80.97.187.189])
 by rwcrmxc20.com [212.198.184.144] with SMTP id <20050617160944r200079cdae>; Fri, 17 Jun 2005 16:10:21 +0000
X-Originating-IP: [80.97.187.189]
Received: from 145.64.0.201 by ; Sat, 18 Jun 2005 22:04:57 +0500
Message-ID: <deflate@msn.com>
From: "Citibank" <customerservices@citibank.com>
Reply-To: "Citibank" <customerservices@citibank.com>
Subject: Citibank Fraud Verification Process!

Date: Wed, 16 Mar 2005 16:23:41 -0500
Message-Id: <200503162123.j2GLNfjg057130@pewoturh.com>
To: njoop@comcast.net
Subject: Recover Your Account!

From: eBay Notice <aw-confirm@ebay.com>
Reply-To: aw-confirm@ebay.com
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit

X-Loop-Detect: 1
Chaotic Organization

The Untouchable

Tools

Bait Developer

Scam Web Developer

Email Network

Server Compromise

Mailing List

Configure Server

Blind Drop

Leader

Mud

Cashout

Validate

Trigger

Harvester

Copyright 2006 Hacker Factor
View Profile: TheUnTouchable

TheUnTouchable
Administrator

Last Activity: 07-09-2005 01:51
Offline

Forum Info

Join Date: **23-04-2005**

Posts
Total Posts: 29 (0.11 posts per day)
Find all posts by TheUnTouchable
Find all threads started by TheUnTouchable

Referrals: 4

Contact Info

Email:
Send a message via email to TheUnTouchable

Private Message:
Send a private message to TheUnTouchable

Additional Information

N/A

Group Memberships

TheUnTouchable is not a member of any public groups

All times are GMT +2. The time now is 04:13.
DutchMaffia

**Name:** DutchMaffia  
**Web servers:** www.dutchmaffia.org (web forum)

**IRC Servers:**
- irc.dutchmaffia.org
- Warezundergound.of.dutchmaffia.org
- The.Extreme.Recruit.Center.of.dutchmaffia.org
- Get.the.latest.releases.at.irc.dutchmaffia.org
- Xdcc.Ownz.dutchmaffia.org

**Largest 5 channels / users**
- #movie-zone (869)
- #acapella-heaven (598)
- #mafia (550)
- #eternal-warez (531)
- #porn-r-us (293)

**Staff:**
- JonKol - (Dutch,English,German)
- TheUntouchable - (Dutch,English)
- AdolfO - (Dutch,English,German)

**Channel Topics:**
Welcome to #mafia, for chat, **rooters** and **scanners** join #mafia-chat  

rm Welcome to #mafia, for chat, rooters and scanners join #mafia-chat  

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

"OKAY is certain, for **Sunday 12 June, 13:00, Spido toren, Willemsplein 85, Rotterdam! BE THERE!""

http://www.dutchmaffia.org/showthread.php?t=4
Handedness  Right handed (70% of population)
Right hand  Drums outside-to-in
Left hand  Drums inside-to-out
Asymmetrical drumming  < 5% of the population
He is less than 3.5% of the total population
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.