

Stay ahead of the curve

**Strong Software Anti-Piracy  
Solution - Know the  
Components Needed**

**Jan Samzelius, CEO  
ByteShield, Inc.  
[www.byteshield.net](http://www.byteshield.net)**

# Agenda

- Detail the software cracking problem
- Recommend a software security/protection process for publishers
- Define a state of the art Software Copy-Protection and Anti-Piracy solution

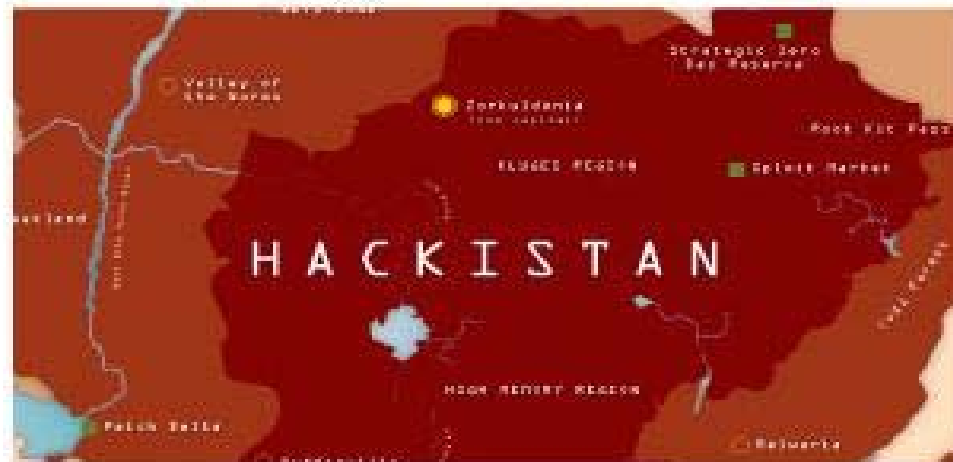
# The Software Cracking Problem



**Anybody here thinks software theft is  
not a problem????**

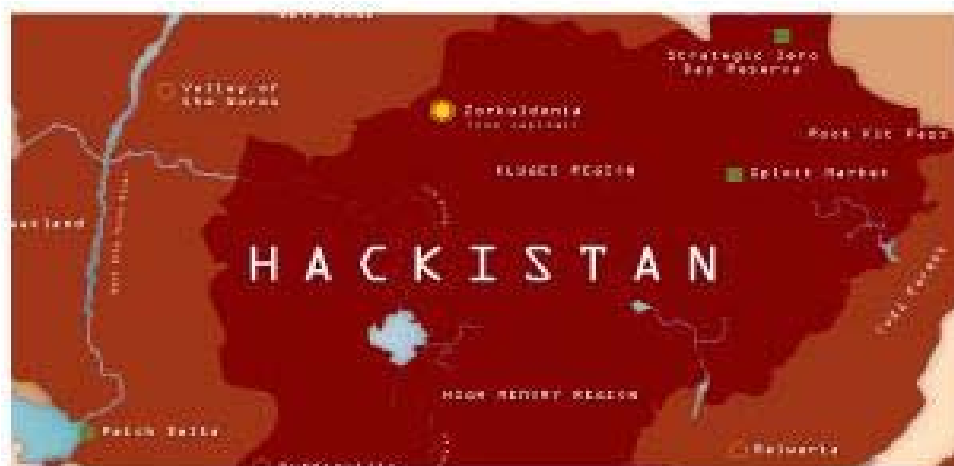
# Know The Components

- Industrial/professional piracy
- Casual copying/underlicensing
- Honest users



The Pilfering Department issued its quarterly update on our glorious nation's accomplishments today, stressing the recent productivity gains in the pharming industry, including the well-planned raid against European, US, and Australian financial institutions.

Courtesy Fortify Software



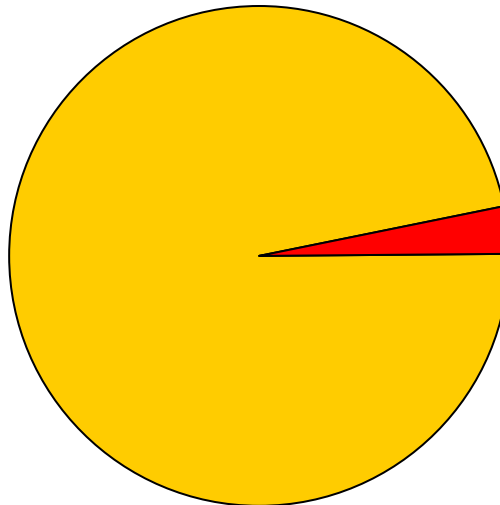
Rather than blindly investing based on published results, Phr33k acquired corporate news releases before they were issued and based his trades on this information. “Making money on the stock market really can be a slam-dunk,” a beaming Phr33k told NNTP News.

Courtesy Fortify Software

# Professional Crackers Are Many And Very Clever

## Hackers

- Very intelligent
- Often highly educated
- Few opportunities



**8M**

## Crackers

- Release teams
- Organized crime
- Government sanctioned
- Competitors

# Crackers' Motivations Include

- **Glory**
- **Challenge**
- **Greed**

# Crackers Think Differently

- Erosion of respect for the law
- All software should be free



# What Is Cracked – Everything!

- Complete detailed instructions on removing protection from US Software on Foreign Government sponsored websites
- Counterfeit key generators, blogs describing how to crack widely available on the net
- Example of Warez website with over 12K titles:  
[http://www.fullreleases.com/tour\\_programs.php](http://www.fullreleases.com/tour_programs.php)

Pirate Access - Apps - Full Downloads - Mozilla Firefox    EN English (United States)

File Edit View History Bookmarks Tools Help

http://www.pirateaccess.com/apps.html    crack keygens

# Pirate Access

[Bookmark Us](#)    [Signup Now!](#)

[Home](#)   [Applications](#)   [Games](#)   [Movies](#)   [TV Shows](#)   [Music](#)   [eBooks](#)   [Erotica](#)

## Apps

Download the latest applications, operating systems and more for your PC.

We have all the latest antispysware tools, antivirus and more!

Please avoid searching for terms such as: warez, crack, serial, full - as this may give false results or no results

Top Apps	Speed	Downloads
Macro Expert ver.2.8.1 Pro	4996KB/s	708 Times
Fluid Mask 3	4052KB/s	52 Times
Google Earth Pro Edition '07	2842KB/s	832 Times
PowerDVD Ultra Deluxe 7.3	3632KB/s	59 Times
Autodesk Land Desktop 2007	2569KB/s	246 Times
Apple QuickTime Pro 7.2	2598KB/s	370 Times

Done

start    E.    I.    B.    Z.    D    M    B.    P.    64    5:18 PM

Stay ahead of the curve

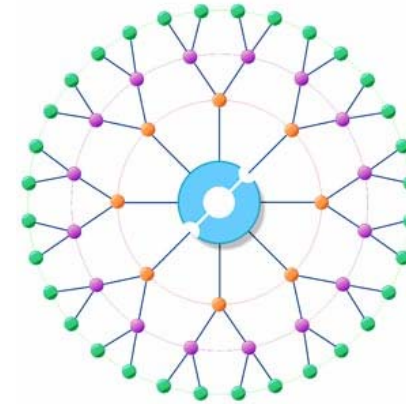
# What Is Most Attractive To Crack?

- Glory:



- Greed: Popular applications and games
- Glory and Greed: Protection schemes

# Cracker Resources



Stay ahead of the curve

# Hide Debugger

**Hidedbg For themida1.9.5** October 28, 2007

Posted by reversengineering in [OLLY'S PLUGINS](#), [TOOLS](#).  
[trackback](#)

Hide OllyDBG Plugin V1.02  
 Functions:  
 1.Hide IsDebuggerPresent  
 2.Hide NtGlobalFlag  
 3.Hide ProcessHeapFlag  
 4.Patch ZwQueryInformationProcess (==patch UnhandledExceptionFilter)  
 5.Patch ZwSetInformationThread  
 6.Patch CheckRemoteDebuggerPresent  
 7.Patch OutputDebugStringA  
 8.Anti heap-checking (For themida1.9.5.0)

V1.02:  
 ! Fixed the bug of patching ZwSetInformationThread (For themida 1.9.5.0)  
 + ADD heap-checking.

Debug themida1.9.5  
 1.Modify window caption in the file ollydbg.exe (CPU,OLLYDBG...)  
 2.Click "Hide ALL" (choose HideDBG plugin)

dl this !!

[hidedbgrar.txt](#)

**Categories**

- ALL NEWS
- E-BOOK
- MUPS
- RCE
- TOOLS
  - .NET
  - DEBUGGER
  - Decompilers
  - DETECTOR
  - HEX EDITOR
  - MONITORING
  - OLLY'S PLUGINS
  - OTHER
  - PACKER
  - PROTECTOR
  - UNPACKERS
- www.fun.here!
- Zcripts

**Blog Roll**

- impostor
- mr.REM (old blog)
- sina\_dir
- scc

Scripts Partially Allowed, 4/5 (google-analytics.com, wordpress.com, snap.com, quantserve.com) | <SCRIPT>: 12 | <OBJECT>: 0

Done

start Eud... 2 M... 2 M... Sky... Hid... Micr... 10:42 AM

Stay ahead of the curve

# Reverse Code Engineering Videos



Stay ahead of the curve

# RCE Links

The screenshot shows a Mozilla browser window with the following details:

- Address Bar:** `http://arteam.accessroot.com/rce_links.html`
- Page Title:** ARTeam: Reverse Engineering Tutorials - RCE Links - Mozilla
- Page Content:**
  - Logo:** A green silhouette of a head with a recycling symbol and binary code inside.
  - Text:** "ARTeam" in large blue letters, with the tagline "I hear and I forget, I see and I remember, I do and I understand" below it.
  - Navigation:** Home, Forums, Tutorials, RCE Related, Team Info, eZine.
  - Breadcrumbs:** Home > RCE Related > RCE Links
  - Section Header:** RCE Links
  - Text:** "Here are other great sites related to reverse engineering :)"
  - List of Links:**
    - [Olly Debugger](#) - Olly Debugger Official Homepage.
    - [Woodman](#) - Great famous RCE site, It hosts the official support forums for olly debugger.
    - [Tuts4you](#) - Another great tutorials site be sure to check it out!
    - [Exetools](#) - One of the most old yet popular and great site about RCE.
    - [Unpack.cn](#) - Great community about unpacking in reverse engineering. In chinese most of it, but it has english sections. If you want to get serious about unpacking don't miss this one!
    - [Reversing Labs](#) - Tools, tutorials and a little bit of everything for reversers. Most of the site is in serbian, but it has english sections. Great tools by ap0x you don't want to miss.
- Status Bar:** Scripts Currently Forbidden | <SCRIPT>: 8 | <OBJECT>: 0
- Taskbar:** Windows XP taskbar with Start button, several open applications (Eudora, 2 M..., Sky..., AR..., Micr...), system tray showing 68° and 11:55 AM.

Stay ahead of the curve

# Russian Crack Site

CRACKL@B :: Russian crackers site - Mozilla Firefox

EN English (United States)

File Edit View History Bookmarks Tools Help

http://cracklab.ru/english.php

Vonage LINKS « Reverse Engineering b10g | R... CRACKL@B :: Russian crackers site

**CRACKL@B** **ALL YOU NEED - ON ONE DVD**  
ORIGINAL CRACKER'S DVDROM: CRACKL@B DVD GO >>>

Home | Articles | RAR-articles | Forum | Programming | Download | CD & DVD  
For Newbie | FAQ | Links | Interview | Archive | News | Contacts

## Welcome to CRACKL@B!

CRACKL@B is a Russian Speaking Portal for Crackers and Reversers, by far the largest site on the Russian Internet on the subject of RE/Cracking. CRACKL@B is not a Crack-Team, it is a site dedicated to education, developed and maintained by Russian Cracker "Bad\_guy" <bad\_guy@cracklab.ru> Unfortunately, The majority of the content housed here is for those who are Russian speaking, Below you will find my english section, which may be of interest to you:

- CRACKL@B Forum (with 100% english-translated engine)**  
 This is the most popular part of the Cracklab site. We have hundreds of visitors daily at our forum. Here you can ask a cracking question, make a request about cracking your favorite program, or share you experience with amazing Russian cracking community. <http://cracklab.ru/f/>
- Crack Tools**  
 Over 100 crack-tools can be downloaded here, downloads in section "Download"("Skachat") are free: <http://cracklab.ru/download.php>
- CRACKL@B DVD**  
 This is a huge collection of the best tools available to crackers, programmers and reversers. CRACKL@B DVD - is a unique and usefull tool and can be shipped to any country or address for a fee of \$20.00. Here you can find details - <http://cracklab.ru/dvde.php?lang=eng>
- Crackme collection**  
 To help you understand the tools and process needed to master the art of RE we host a number of crackmes from varios sources here: <http://cracklab.ru/crackme/>  
 Or you can test your skills with crackmes created by me (Bad\_guy) <http://cracklab.ru/crackme/cracklab/>
- Links**  
 Our links lead you to some of the best and most comprehensive knowledge sources on the topic of Reverse Engineering you can find them here: <http://cracklab.ru/links/>

You may have noticed google has no .RU 2 .EN support. If you want to see the Russian only pages you can click the following link, Enter the address (for example: <http://cracklab.ru>) and Use the automatic Russian-English web-pages translator to better navigate our other pages. Obviously this will not translate everything, but is one of the few resources for Russian-2English translation. Follow the link: <http://www.translate.ru/srvurl.asp?lang=en>

You can write me in English... may be i'll understand ;)  
Bad\_guy <bad\_guy@cracklab.ru>

Done

start Eu... 2 M. 2 M. Sk... Mic... CR... 68° 12:07 PM

Stay ahead of the curve

# Cracker Challenges

- **Easy**

- > Find and delete license parameters
- > Find and change license parameters – e.g. 30 day trials
- > Find and remove or change license calls

- **Medium**

- > Find keys for encryption
- > Determine key algorithm

- **Tough, lots of work**

- > Find in memory – HD DVD
- > iPhone
- > Reverse engineering – online game



# Cracker Facilitators

- Ability to clone the entire application
- Access to code – the ability to see it
- Ability to understand the code
- Ability to manipulate the code



Stay ahead of the curve

# Professional/Industrial Piracy - Examples

- Counterfeit license activation keys
- Clone the license manager with HostID spoofing
- Binary hacking

# Professional/Industrial Piracy

**To combat it, you simply must have the strongest copy protection available**



# Casual Copying/Underlicensing

- **Download pirated software**
  - > Warez sites
  - > P2P sites
  - > Torrent sites
- **Download key generator**
  - > Keygen sites
- **Very simple hacking**
  - > No CD patches
  - > Date Manipulation



# Casual Copying/Underlicensing

**Identify every instance of exceeding the license and turn it into a selling opportunity**



# Honest Users

- Many protection solutions
  - > Are cumbersome for the end-user
  - > Do not allow for multiple installations or backup
  - > Do not allow moving software to another PC
- Result
  - > Irritated customers
  - > Very expensive support for publisher

# Honest Users

**The protection solution must be transparent to the end-user and allow back up and moving without calling support**

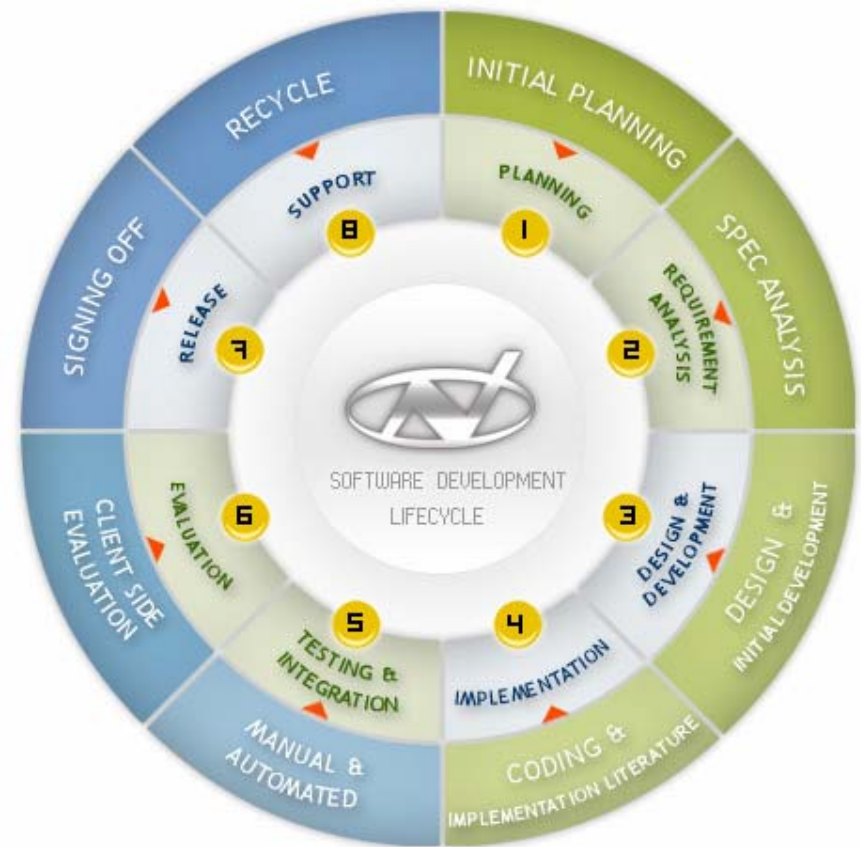


# The Requirements

- Industrial piracy: The strongest protection available
- Casual copying/Underlicensing: Identify every instance of exceeding the license and turn it into a selling opportunity
- Honest User: Transparent and allow back up and moving without calling support

# Software Security/Protection Process

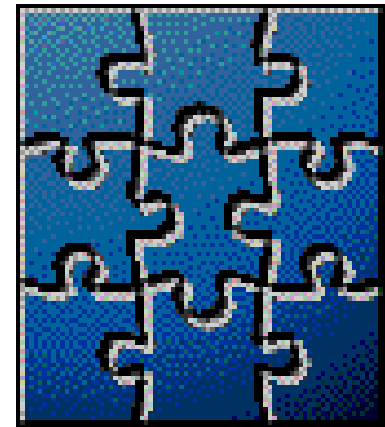
Successfully protecting software requires examining the complete process from development through interaction with customers and partners



# Software Security/Protection Process

- Securing software applications involves many different processes and technologies
  - > Code in the application
  - > Communication with server
  - > Customer support scripts

**All working in concert**



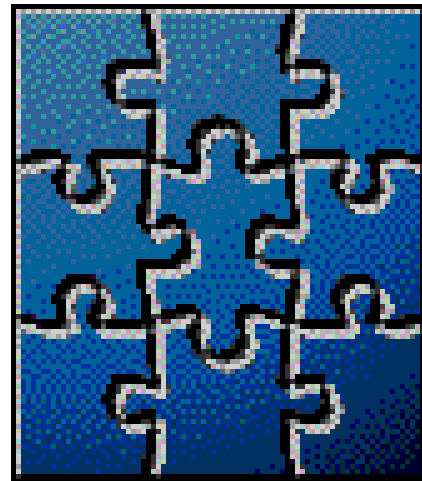
# Software Security/Protection Process

Access  
control

Restrict WAN-  
based usage

Protect  
multiple exes

Safe customer  
debug



Fingerprinting

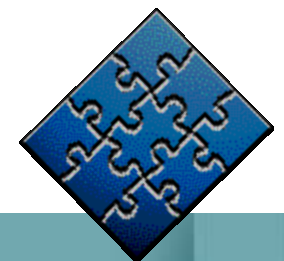
Atomic call

Cracking reporting

Plug  
holes

# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- Verify the identity of the customer
- Different permissions



# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- Every single installation identified
- Inform all users of fingerprinting
- Monitor P2P and crack sites
- Requires individual assembly



# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- Without a call to the server and validation of the installation, the application will not run



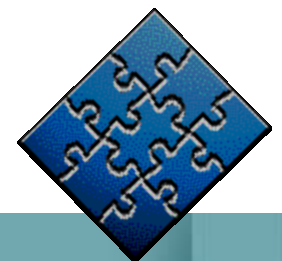
# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- **Cracking reporting**
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- Detect and report cracking attempts, so you can decide how to handle the customer



# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- All holes discovered and all other threats found through monitoring or crack forums can be plugged in all installations



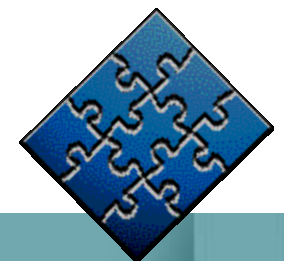
# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- **Safe customer debug**
- Protect multiple exes
- Restrict WAN-based usage
- Fingerprinted, short-lived version without anti-debug



# Software Security/Protection Process

- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- **Protect multiple exes**
- Restrict WAN-based usage
- Multiple exe files, all with separate protection, will drastically increase time to crack



# Software Security/Protection Process

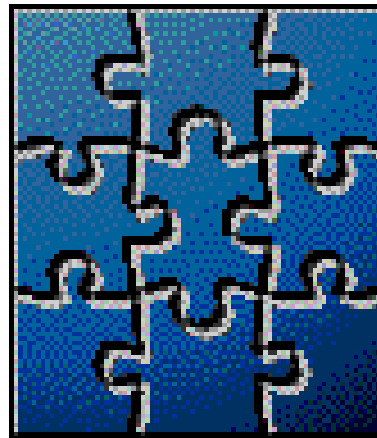
- Access control
- Fingerprinting
- Atomic call
- Cracking reporting
- Plug holes
- Safe customer debug
- Protect multiple exes
- Restrict WAN-based usage
- If heartbeat data can be provided you can receive usage data
- Activity-based license control is superior



# State of the art Software Copy-Protection and Anti-Piracy solution

You must change the game and improve the protection significantly, to include

- Binary Separation™
- Mutation
- Fingerprinting



- Remote server component, for application, LM and encryption keys
- All standard tools

# This Fulfills The Requirements Of:

- Strongest anti-piracy
  - > Application is locally in several pieces which are difficult to combine
  - > Dozens of barriers with 1000s of instances, without effect on performance
- Every license exception turned into a sales opportunity
- Friendly for honest users
  - > No limit on installations
  - > Easy to move application
  - > Completely transparent

# Thank You

BYTE | SHIELD

**Huge effort to crack**  
**+**  
**User transparency**  
**=**  
**Superior copy protection**  
**=**  
**Substantially higher revenues**  
**=**  
**ByteShield™**

[jan.samzelius@byteshield.net](mailto:jan.samzelius@byteshield.net)

+1-415-420-6636

Stay ahead of the curve