GAME HACKING 1 – ANTI CHEAT BYPASS

JOAS ANTONIO

HTTPS://WWW.LINKEDIN.COM/IN/JOAS-ANTONIO-DOS-SANTOS

PROGRAMMING LANGUAGE - NECESSARY

- Assembly
- C
- C++
- C#
- Python

PROGRAMMING LANGUAGE - ASSEMBLY

- https://stackoverflow.com/questions/775108/x86-jump-to-an-address
- https://www.felixcloutier.com/x86/jmp
- http://www.math.uaa.alaska.edu/~afkjm/cs221/handouts/irvine4-5.pdf
- https://c9x.me/x86/html/file_module_x86_id_147.html
- https://flint.cs.yale.edu/cs421/papers/x86-asm/asm.html
- https://www.tutorialspoint.com/assembly_programming/assembly_logical_instructions.htm
- https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf
- https://www.intel.com/content/dam/develop/external/us/en/documents/introduction-to-x64-assembly-181178.pdf
- https://www.felixcloutier.com/x86/
- https://www.youtube.com/watch?v=lUbPUWtmVUU
- https://superuser.com/questions/1188364/what-is-the-size-of-an-address-of-a-variable-in-memory-on-a-64-bit-processor-in
- https://stackoverflow.com/questions/49708291/find-address-in-x64-executable-from-memory-address

PROGRAMMING LANGUAGE – C++

- https://github.com/TyrarFox/encstr
- https://github.com/tomLadder/WinLib
- https://www.unknowncheats.me/forum/c-and-c-/298579-pattern-class-nibble-support.html
- https://www.unknowncheats.me/forum/c-and-c-/287571-dll-injection-creating-hijacking-threads.html
- https://www.geeksforgeeks.org/virtual-function-cpp/
- https://www.programiz.com/cpp-programming/virtual-functions
- https://www.javatpoint.com/cpp-virtual-function
- https://github.com/adrianyy/nasm_shellcode
- https://www.unknowncheats.me/forum/c-and-c-/262156-reading-writing-process-memory-baseaddress-offset.html
- https://www.guru99.com/cpp-dynamic-array.html
- https://cplusplus.com/doc/tutorial/dynamic/

PROGRAMMING LANGUAGE – C++

C++ Beginner Tutorials:
C++ Beginner's Guide
Tutorials hosted on MSDN containing excercises and answers.

An Introduction to C++ Programming:
EDM/2 - An Introduction to C++ Programming - Part 1/13
13 part C++ programming tutorial.

C++ Annotations Version 5.1.0b:
http://ari.cankaya.edu.tr/~guvenc/ceng112/cplusplus.html
This document is intended for knowledgeable users of C who would like to make the transition to the C++ programming language.

C++ Language Tutorial:
C++ Language Tutorial
12 printer-friendly chapters for those already proficient in C.

Introduction to Object-Oriented Programming Using C++:
http://www.gnacademy.org/text/cc/Tutorial/tutorial.html
This tutorial is a collection of lectures for an online course.

PROGRAMMING IN C++:
Cprogramming.com - Programming Tutorials: C++ Made Easy and C Made Easy
Online tutorial that can also be downloaded and some graphics tutorials for downloading.

C++ Tutorials:
C++ Tutorials
Includes introductions to namespaces and the standard template library (stl), a bunch of examples of "C++ as a Better C" and some miscellaneous topics.

The cplusplus.com tutorial:
C++ Language Tutorial
Complete C++ language tutorial.

An Introductory STL tutorial:
CodeProject: An Introductory STL tutorial. Free source code and programming help
This tutorial gives a basic introdution of the concepts of the STL.

An Introduction to C++:
An Introduction to C++
This is the first installment in a series called "Objective Viewpoint" that will teach you about C++ and Java

CSpot:
visual c programming book at cppspot.com
C++ tutorials and help for beginners that you can actually understand. Includes forums, downloads and much more.

PROGRAMMING LANGUAGE – C++

C++ Programming Tutorial:
http://cplus.about.com/library/blcplustut.htm
This tutorial features a series of lessons designed to teach you the basics of C++ programming. Includes 35 lessons that start with good old Hello World and progress through variables, constants, I/O, conditions, looping, arrays, vectors, functions, overloading, constructors, templates, inheritance, polymorphism and a bunch of other topics.

C++ Programming Language Tutorials:
http://www.cs.wustl.edu/~schmidt/C++/
This material was developed as part of a series of courses on C++ and consists of a number of pdf documents.

C++ Ripped Apart:
Re-direction page to [warebiz] :: Programming - http://www.warebizprogramming.com
C++ tutorial designed to help anyone who wants to learn C++, especially students considering the tutorial was based on notes, examples, assignments, and projects from college classes and written by a student.

Crashproof C++:
Crashproof C++
Avoid some of the common pitfalls with strings, buffers, stacks and memory leaks.

Object Oriented Programming:
UU/IT/Education at the IT department
Extensive C++ OOP resources that can be read online or downloaded as well as some smalltalk information.

C++ tutorial for C users:
http://www.4p8.com/eric.brasseur/cppcen.html
This text enunciates and illustrates features and basic principles of C++. It is aimed at experienced C users who wish to learn C++.

C++ Tutorial - FunctionX:
C++ Tutorial - FunctionX
This tutorial is an introduction to C++ that addresses computer programming using the C++ language.

Function Pointer Tutorials:
Page has moved!
The site dedicated to C and C++ Function Pointers.

Notes on (re)learning C++:
Notes on (re)learning C++
Mostly OOP material for C++.

Windows API Tutorials:
Windows API Tutorial
Excellent tutorials for windows programming from the basic hello world window to a graphics tutorial on DirectDraw. Souce examples can be downloaded.

C++ Programming Tutorial II:
http://appsrv.cse.cuhk.edu.hk/~csc4510/cxx/tutorial.2/1.htm
Classes and Objects

PROGRAMMING LANGUAGE – C++

An Introduction to OOP:
An Introduction to OOP
Sample date program done in Borland C++ Builder with screenshots and sample code.

Online C++ tutorial:
http://www.intap.net/~drw/cpp/index.htm
This is a C++ tutorial site that is under construction and has gotten as far as pointers.

theForger's Win32 API Tutorial:
theForger's Win32 API Tutorial
This tutorial attempts to get you started developing with the Win32 API as quickly and clearly as possible.

FoosYerDoos programming:
http://www.foosyerdoos.fsnet.co.uk/
Website that is devoted to win32 C++ programming with a variety of different compilers including but not necessarily limited to Borland BCC5.5 command line, mingw(DevC++ IDE) and msvc++.

Bytamin-C:
http://www.bytamin-c.com/
This page was created by developers for developers working with C++Builder.

Yet Another Code Site:
http://home.att.net/~robertdunn/Yacs.html
This site is dedicated to advancing the understanding of Borland's C++ Builder, the Borland Visual Component Library (VCL), and related Microsoft Windows API issues.

C++ Builder Tutorial:
http://visualcomponentlibrary.com/bcb/
This site is dedicated to the VCL and its documentation as it relates to C++ Builder.

Steve's Borland C++ Builder 3 Page - Tutorials:
http://www.users.bigpond.com/SHaworth/tutorial.html
This section of my Builder web pages will present several tutorials on how to do things in Builder. The type of tutorials will range from beginner to advanced.

Dev-C++ Tutorial:
http://www.uniqueness-template.com/devcpp/
Tutorial for programming with and configuring Dev C++ and the Insight Debugger.

Using the Borland 5.5 Compiler and command-line tools:
Using the Borland 5.5 Compiler and command-line tools
This article takes a look at what's contained in the free download and shows how you can start building programs.

Creating And Using DLLs:
http://www.flipcode.com/tutorials/tut_dll01.shtml
This document will attempt to show you how to create a basic DLL and how to use it (with import library linking and without).

V Girish's Page:
http://www.geocities.com/contactgirish/homepage.html
Tutorials and code snippets.

Online C++ Tutorial:
http://www.intap.net/~drw/cpp/
This is under construction and looks promising. At the moment it seems to cover up to function basics and some object basics, but the advanced sections are yet to be completed.

Installing Cygwin:
http://cplus.about.com/library/weekly/aa031202a.htm
A Unix-like Environment For Your PC With C/C++ Development Tools.

REVERSE ENGINEERING

- Recommended Programming Books
- Hooking
- MakeFiles
- Detecting/Removing API Hooks
- Usefull Websites To Read
- Handbook of Applied Cryptography
- Import Functions Through Code Injection
- Programming Links
- How WPM Works
- Important Miscellaneous Programming Threads
- Two Usefull Very Simple Perl Scripts
- Basic Introduction To Perl
- Programming in Python #1
- C++ Trainer Example
- Hacking in D
- Easy Python Hooking
- IDA Python CVar Renamer
- Vector X,Y,Z Class
- Perfect Aim Prediction
- Calling A Process' Methods

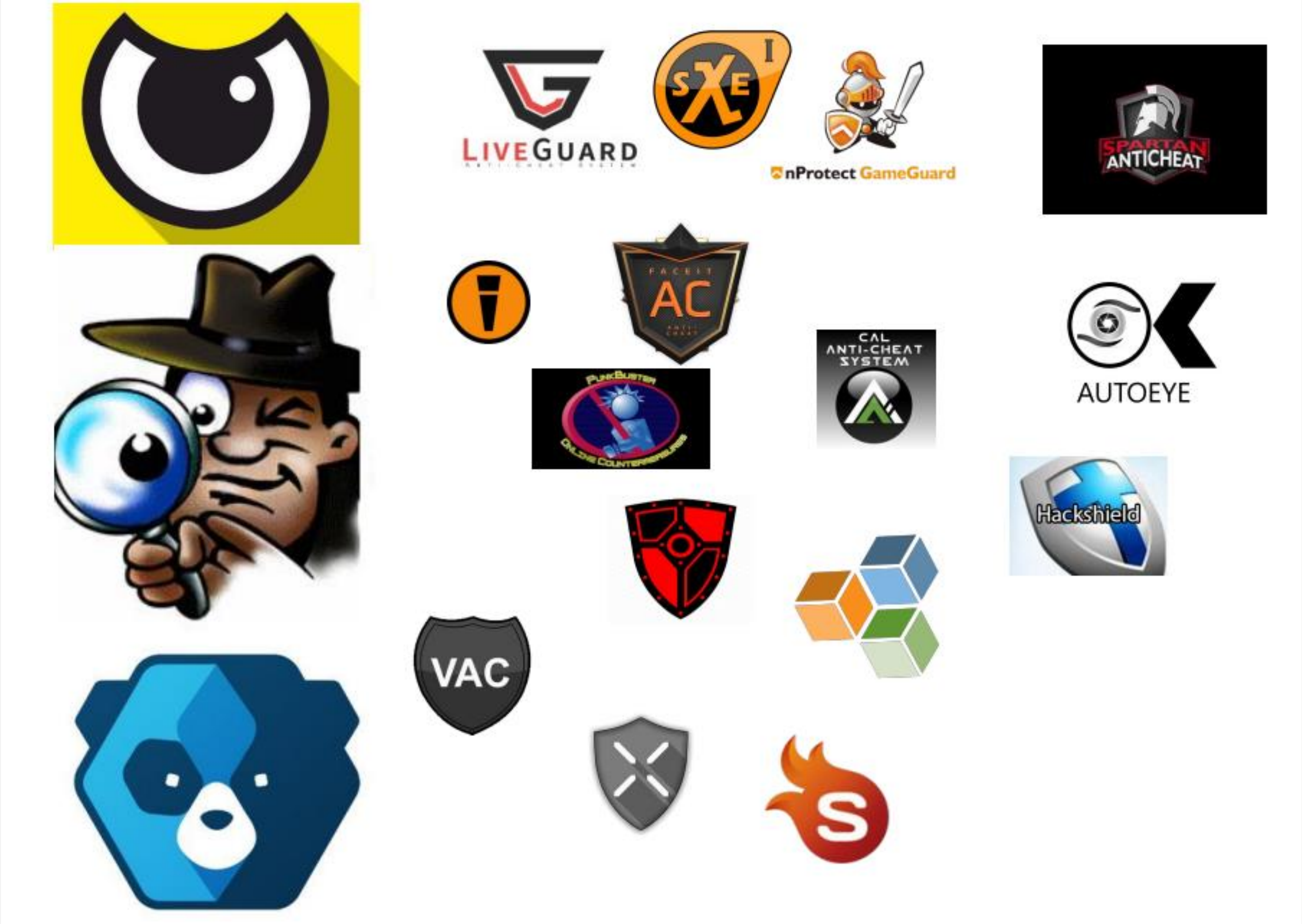
REVERSE ENGINEERING 2

- Reverse Engineering Tutorial Links
- ReBit - Application For Reversing Bits
- How to Force a DLL Auto Load in a App With Dependancies
- CodeCave with OllyDbg
- How To Unpack SmartAssembly
- How to Unpack .Net Reactor 4.x.x
- Unpack Any Version of UPX
- Minesweeper Auto-Solver
- Lua UPX 3.x OEP Finder
- Identifying And Reversing Structures
- Patching CIL instructions [IDA + HxD]
- https://www.unknowncheats.me/forum/general-programming-and-reversing/161393-programming-reversing-complete-sources-releases-list.html

REVERSE ENGINEERING 3

- Trainer Tools
- OldSchool SigScanner
- Potentially Useful Tool
- IDA
- ReClass Aka StructBuild 2
- CrackMe #1 By Scrapdizle
- CrackMe #2 by Scrapdizle
- CrackMe #3 by Scrapdizle
- Packet Viewer [IMV]
- Ida Plugin [SigMaker Update]
- DiSav0ws Tracer
- NSearch FindPattern Logger
- .NET CrackMe by Mi4uric3
- CrackMe #1 By LowHertz
- Memory Viewer [IMV] V0.8
- ReClass 2011 Beta
- Hooking Windows API - Technics of hooking API functions on Windows
- ZedJect
- API Bypass Tool w/ Source
- ReClass 2011 Incomplete AMD64 Port
- ReClass Parser
- GUI Based Universal Injector
- Snatch - Source Included
- General Chams 1.1 [Create your own Chams without Coding Skillz]
- ReClass x64
- Configurable Injector V3
- Extreme Injector 3.3 by master131
- Xenos Injector v2.3.2 by DarthTon
- Simple DLL Injector
- CrySearch Memory Scanner

ANTI-CHEAT SOLUTIONS



ANTI-CHEAT COMPONENTS

- Features Anticheat Uses
- File Integrity Checks
- String Detection for cheat tools
- Classic AntiDebug
- Obfuscation
- Signature Based Detection
- Hook Detection
- Memory Integrity Checks
- Virtualization
- Kernel Drivers which block process access token creation & more
- Virtualization Detection
- https://www.youtube.com/watch?list=PLt9cUwGw6CYG-d7LGILKHmLWFBJqA2XSV&v=yJHyHU5UjTg&feature=emb_imp_woyt

ANTI-CHEAT WORK

- To bypass anticheat you must understand how it works. Anticheat work very similarly to Antivirus. These are the basic things it does to stop you from cheating, kinda going from simple to more advanced
- File Integrity Checks
- Detecting Debuggers
- Stops debugger from attaching
- Detect Cheat Engine & memory editors
- Signature Based Detection
- Detect DLL injection
- Detect Hooks
- Block Read/WriteProcessMemory
- Memory integrity checks
- Statistical Anomaly Detection
- Heuristics

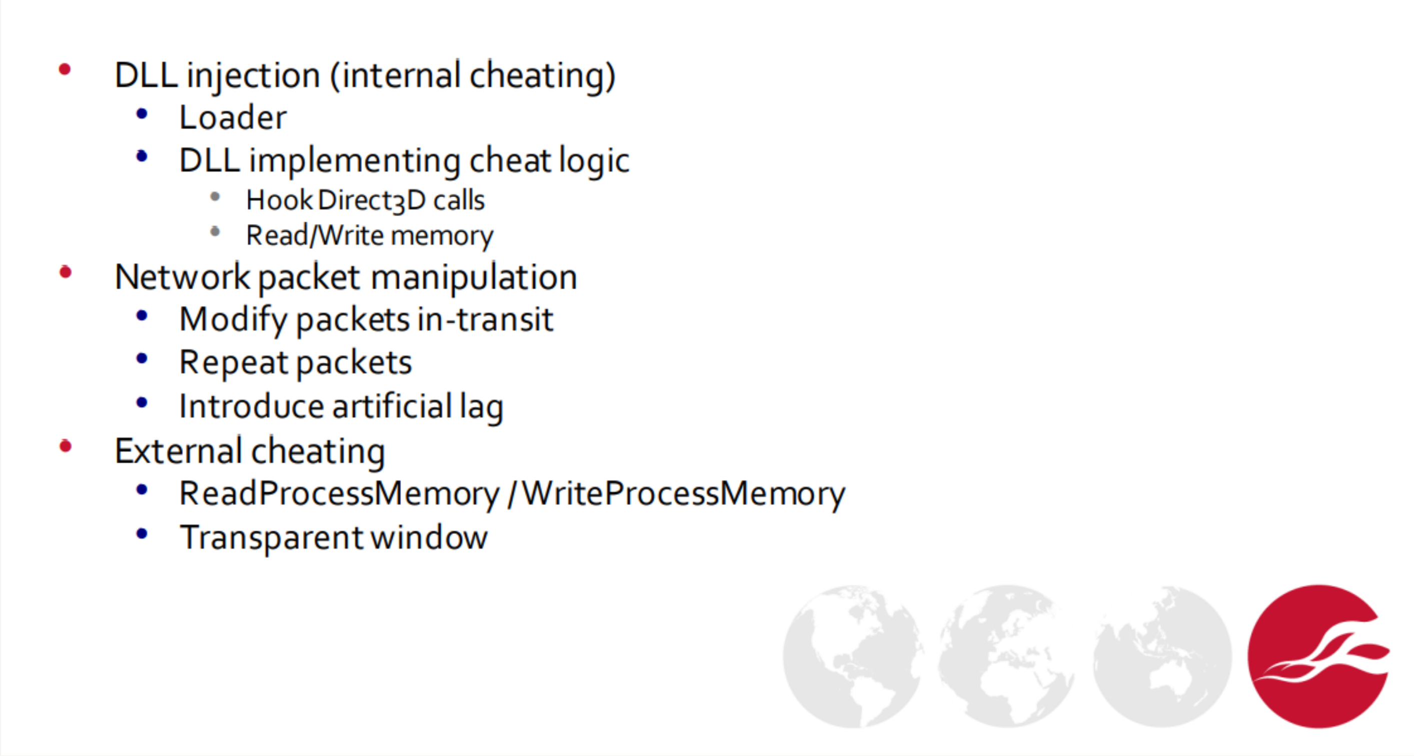
https://guidedhacking.com/threads/how-to-write-an-anti-cheat-part-1-detecting-external-cheats.14624/

https://guidedhacking.com/threads/how-to-bypass-anticheat-start-here-beginners-guide.9882/

ANTI-CHEAT GUIDE BYPASS

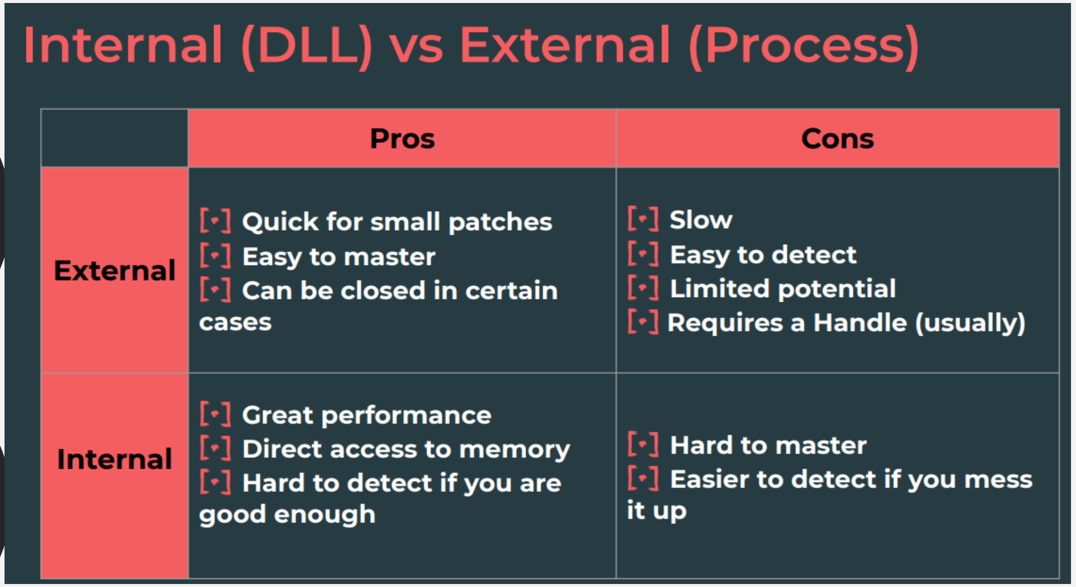
- Guide - How to Bypass EAC - Easy Anti Cheat
- Guide - Anticheat Battleye Bypass Overview
- Guide - How to Find Encrypted or Obfuscated Variables in Cheat Engine Guide
- Tutorial - Junk Code Generator and Polymorphic Code Engine Guide
- Guide - Kernel Mode Drivers Info for Anticheat Bypass
- Guide - How To Bypass VAC Valve Anti Cheat Info
- Guide - Battleye Anticheat Bypass Overview
- Guide - How to bypass XignCode Anticheat Guide
- Guide - Hackshield Anticheat Bypass Information
- Guide - How to Bypass FairFight Anticheat
- Download - GamersClub Anti-Cheat Information (Driver + user mode module)
- Tutorial - MTA: SA's kernel mode anticheat is a joke (information)
- Guide - CSGO Overwatch Bypass - How to Avoid Overwatch Bans

ANTI-CHEAT BYPASS TECHNIQUES



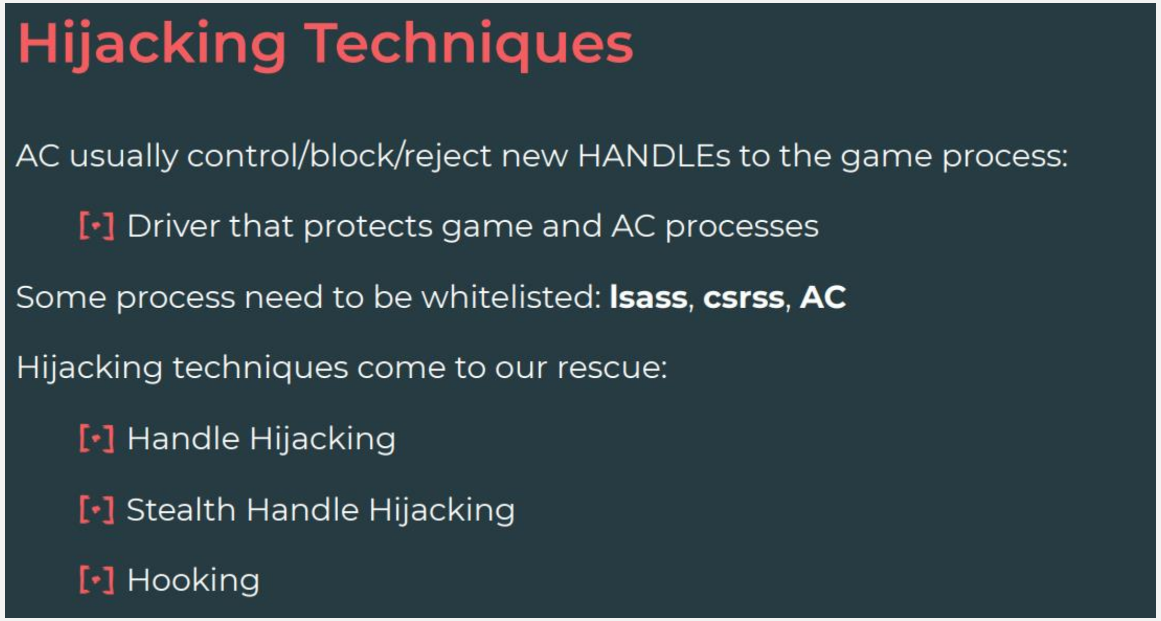
- DLL injection (internal cheating)
  - Loader
  - DLL implementing cheat logic
    - Hook Direct3D calls
    - Read/Write memory
- Network packet manipulation
  - Modify packets in-transit
  - Repeat packets
  - Introduce artificial lag
- External cheating
  - ReadProcessMemory / WriteProcessMemory
  - Transparent window

DLL INJECTION/HIJACKING



Internal (DLL) vs External (Process)

	Pros	Cons
External	[•] Quick for small patches [•] Easy to master [•] Can be closed in certain cases	[•] Slow [•] Easy to detect [•] Limited potential [•] Requires a Handle (usually)
Internal	[•] Great performance [•] Direct access to memory [•] Hard to detect if you are good enough	[•] Hard to master [•] Easier to detect if you mess it up



Hijacking Techniques

AC usually control/block/reject new HANDLEs to the game process:

- [•] Driver that protects game and AC processes

Some process need to be whitelisted: **lsass**, **csrss**, **AC**

Hijacking techniques come to our rescue:

- [•] Handle Hijacking
- [•] Stealth Handle Hijacking
- [•] Hooking

ANTI-CHEAT TECHNIQUES

- **[RELEASE]** drvmap with a safer capcom wrapper
  by @uint8 on October 30, 2018

  [INFORMATION] Detecting DMA Hardware-Cheats
  by @rodhad on October 25, 2018

  [SOURCE] HDD HWID spoofing using the Kernel-Bridge filtering subsystem
  by @HoShiMin on October 21, 2018

  [INFORMATION] What's faceit AntiCheat doing in 2018
  by @zwknby48520 on October 18, 2018

  [TUTORIAL] How to use CE on Battleye protected games.
  by @ca1nes on October 7, 2018

  [NEWS] Bypass BattlEye KernelMode Driver [Pseudo code]
  by @a60276468 on October 4, 2018

  [RELEASE] Turn off PatchGuard in real time [TEST] [UCDownload]
  by @ivanpos2010 on October 2, 2018

[SOURCE] PCIe DMA Cheat
by @Skyfail on September 27, 2018

[SOURCE] SymParser - convenient PDB parser
by @HoShiMin on September 24, 2018

[RELEASE] Binary File Difference Checker - check if your version of pasted cheat is good to go! [UCDownload]
by @samtulach on September 22, 2018

[TUTORIAL] [FAQ] Tips and tricks for kernel newbies and beginners
by @HoShiMin on September 21, 2018

[RELEASE] anti-vmware mitigation (anti-antivm)
by @hzqst007 on September 20, 2018

[SOURCE] Inline hooking in the kernel [UCDownload]
by @lordchanka on September 20, 2018

ANTI-CHEAT TECHNIQUES

- **[INFORMATION]** [PB] Screen Shot
  by @CyberDwak on April 25, 2010

  [RELEASE] dxtgaming Crossfire dll needs unpacking [UCDownload]
  by @dxtgamingsucks on April 13, 2010

  [RELEASE] Undetected method antibanned AntiCheat myA
  by @KerchNET on March 17, 2010

  [INFORMATION] Hex Editing
  by @dedead3232 on January 26, 2010

  [INFORMATION] punkbuster on cod4
  by @sjansen8 on January 8, 2010

  [RELEASE] Is VAC2 Loaded? [UCDownload]
  by @Nov on December 16, 2009

  [SOURCE] Combat Arms Hackshield Bypass
  by @Blubsi on September 29, 2009

  [SOURCE] Hackshield Bypass
  by @Blubsi on September 8, 2009

  [RELEASE] Gen's Hack Me .1 [UCDownload]
  by @SEGnosis on August 30, 2009

  [INFORMATION] DMW V4.01 (Pre-Pro Edition) goodies (alot)
  by @learn_more on August 15, 2009

  [RELEASE] DMW V4.01 (Pre-Pro Edition) pimpkey aka GUID
  by @okidoki on August 15, 2009

  [TUTORIAL] VAC2 bypassing
  by @Nov on July 21, 2009

  [SOURCE] Screenshot Blocker [UCDownload]
  by @ReUnioN on July 19, 2009

  [INFORMATION] Bypassing battle signatures
  by @sold67 on July 8, 2009

  [INFORMATION] Punkbuster PBCL'S Decompiled Everygame
  by @Jesus. on January 18, 2008

  [INFORMATION] Some games PB client offsets
  by @okidoki on June 28, 2007

  [INFORMATION] Welcome to Anti - Cheat Bypass Section
  by @Dawgster on January 23, 2007 on September 20, 2018

STUDY MATERIALS

- https://www.blackhat.com/docs/asia-15/materials/asia-15-StJohn-Next-Level-Cheating-And-Leveling-Up-Mitigations.pdf
- https://www.immunityinc.com/downloads/eu-19-Noguera-Unveiling-The-Underground-World-Of-Anti-Cheats.pdf
- https://www.unknowncheats.me/forum/anti-cheat-bypass/161321-anti-cheat-bypass-complete-sources-releases-list.html
- https://www.youtube.com/watch?v=_auePp1nTHs
- https://www.youtube.com/watch?v=7ARwpxZPpE8
- https://www.youtube.com/watch?v=m8EgSr19WaU
- https://www.youtube.com/watch?v=X0lMBRaZgL4
- https://www.youtube.com/watch?v=_auePp1nTHs
- https://www.youtube.com/watch?v=cglXyEjRric
- https://www.youtube.com/c/PlokTheMasterGamer
- https://www.youtube.com/c/StephenChapman