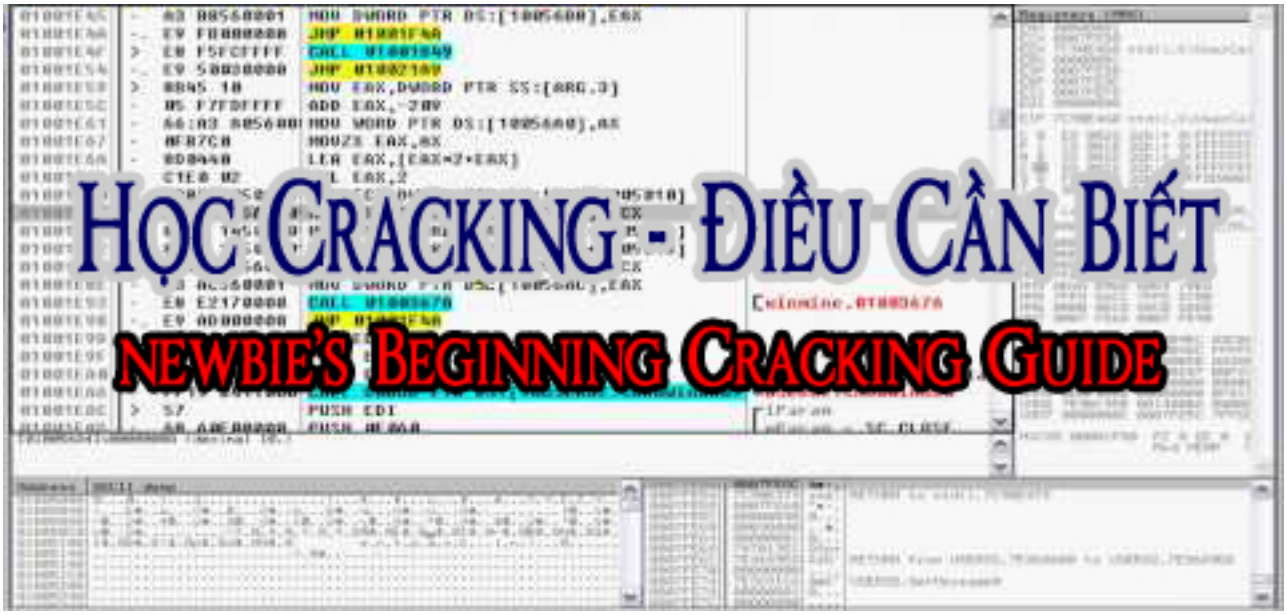
HỌC CRACKING - ĐIỀU CẦN BIẾT
NEWBIE'S BEGINNING CRACKING GUIDE

Học Cracking – Điều cần biết
(Newbie´s Beginning Cracking Guide)

-DTB.2011-

Bài chỉ dẫn này tôi xin viết dành cho bạn - cracker newbie mới gia nhập, để có thể nắm những kiến thức cơ bản nhập môn. Bài chỉ dẫn này không hướng dẫn cách thức crack. Nó cũng không cho bạn tất cả những thông tin cần biết. Đơn giản, nó chỉ là chỉ dẫn đầu tiên hướng dẫn bạn với thế giới cracking. Tôi có cung cấp những bài hướng dẫn thực sự trong bài chỉ dẫn này ở phần cuối. Chỉ dẫn chỉ hướng dẫn cho bạn, cung cấp cho bạn những cái bạn cần, cần để biết, cần để làm những việc chuyên sâu hơn trong thế giới cracking ... à chào mừng bạn đến với thế giới này

Cracker & Hacker

Một trong những điều ngốc ngếch thường thấy chính là ở việc nhiều người không phân biệt được 2 cái trên. Đã từng có bạn hỏi tôi như thế này: "**hack** phần mềm như thế nào vậy bạn?". Chính vì thế tôi sẽ cố gắng giải thích sự khác nhau giữa 2 danh từ trên để những câu hỏi đại loại như vậy sẽ ít đi ^^!

.. Hacker

Hacker (hay tin tặc) là những người mà hiểu đơn giản là những người có khả năng phá hoại những website. Họ khai thác, tìm kiếm những lỗ hổng trong phần mềm và website.

Một số trong họ tự gọi mình là MŨ TRẮNG (White hat) hay **Chính Phái** - họ sẽ thông báo với chủ nhân của website hay phần mềm về những lỗ hổng mà họ tìm được để chủ nhân đó có thể sửa chữa hay nhờ vả họ giúp đỡ sửa chữa. Một số khác (đang chiếm đa số hacker) lại sử dụng những lỗ hổng mà họ tìm được đó để gây nguy hiểm cho phần mềm và website, họ được gọi là MŨ ĐEN (Black hat) hay **Tà Phái**. Còn những người **Chính Tà bất phân** thì được gọi là MŨ XÁM (Grey hat) hay MŨ SỌC (đen và trắng).

Gamehacker vốn là một thành phần của hacker nhưng nhiều người lại xem họ là một phần của cracker, thực sự mà nói họ sử dụng kỹ thuật và kiến thức của cả hacker và cracker cho mục đích của mình.

.. Cracker

Cho đơn giản, từ đây khi nhắc đến Cracker thì ta nói đến Software Cracker (cracker phần mềm) - đây chính là nhân vật mà người có hứng thú đọc bài viết này muốn hướng đến, muốn trở thành.

Cracker (hay thợ khóa) là người có khả năng sửa đổi phần mềm để gỡ bỏ các biện pháp bảo vệ bản quyền (như: chống sao chép, phiên bản dùng thử giới hạn, kiểm tra số serial, kiểm tra CD hay các phiền toái trong phần mềm như cửa sổ thông báo (screennag) và phần mềm quảng cáo (adware). Họ làm ra các phiên bản cracks, patcher, keygen ... Và đôi lúc, cracker còn thêm những phần mở rộng cho phần mềm thông qua các phiên bản cracks của họ (các bản mod mở rộng chức năng/ thay đổi 1 phần chương trình gốc) …

.. So sánh nhanh

Về cơ bản, nếu bạn là môt Cracker thì công việc của bạn là gỡ bỏ biện pháp bảo vệ/ đăng ký của phần mềm, còn nếu bạn là một Hacker thì công việc của bạn là tìm lỗ hổng trong ứng dụng web, máy tính và cả phần mềm.

Hacker và Cracker ai có trước ai? Ai quan trọng hơn ai? Tạm thời chưa có câu trả lời thỏa đáng, xong nó chẳng liên quan đến bài viết này nên tôi cũng không dẫn chứng thêm làm gì. Nếu hacker xem trọng sự nổi tiếng và tiền tài, thì cracker lại là những người tìm niềm vui trong cracking, đơn thuần đều là những người lãng mạn và vui tính cả

nếu là 1 cracker bạn sẽ có những điều:

Nên làm & Không làm

Những điều sau đây có thể bạn sẽ không đồng tình ngay, nhưng nó thật sự quan trọng và chính xác ...

.. NÊN LÀM

- Kiểm tra lai các bản cracks của bạn

Không ai muốn tải về một bản crack hay một keygen mà không dùng được chúng. Bạn cũng không muốn những người tải về crack/keygen của bạn và nói chúng không hoạt động được. Ngoài ra, chẳng ai muốn tải về một crack hay keygen mà nó có thể gây hại cho máy tính của họ cả. Vì vậy, trước khi phát hành nó hãy chắc chắn 1000000% là nó an toàn và hoạt động tốt trước khi phát hành nó.

- Đừng vội vã

Cracking là một việc làm tốn nhiều thời gian. Vậy hãy cho phép mình dành nhiều thời gian để làm nó, một là sản phẩm crack/keygen của bạn sẽ có chất lượng tốt, hai là có thể qua đó học hỏi thêm để sửa chữa những sai lầm mà khi vội vã làm bạn thường mắc phải.

- Xem nó như niềm vui của chính bạn

Cracking (hay bất cứ thứ gì khác) đều là sở thích, đều sẽ trôi qua theo thời gian. Hãy giữ niềm vui thích và hứng thú của bạn khi bạn cracking. Vì đến ngày mà bạn không còn hứng thú với nó thì đó là ngày bạn nên dừng cracking.

- Hãy hỏi nhiều

Nếu bạn không hiểu điều gì thì nên mạnh dạn hỏi và tìm hiểu. Hầu hết các kiến thức bạn có được đều từ người khác, nên nếu bạn không hiểu, không biết thì chỉ có cách nhanh nhất là hỏi người khác. Dấu dốt, tự cao chỉ làm bạn tụt hậu.

.. KHÔNG LÀM

- Không phát hành một bản crack không phải của bạn

Nói trắng ra là đừng nên làm một cracks mà dựa trên bản crack của người khác - chẳng hạn như so sánh file đã crack và file gốc, rồi tạo patcher và phát hành nó như chính bạn làm ra nó; hay là dùng kỹ thuật dịch ngược để dịch ngược code một keygen, rồi sau đó viết lại code và phát hành nó như chính bạn đã tìm ra giải thuật tạo key/serial.

-Không dùng thứ gì mà không có sự cho phép hay ghi nhận công lao

Nếu bạn đang dùng tài nguyên của vài người để tạo ra các bản crack/keygen, chẳng hạn như chiptunes hay GFXs, thì hãy luôn ghi nhận công lao của những người đã tạo ra chúng, trừ phi họ cho phép bất kỳ ai đều có thể sử dụng chúng mà không cần họ cho phép.

- Không bán

Tôi nghĩ bạn đã hiểu khi đọc tiêu đề trên. Đừng làm việc vô bổ đó, nếu bạn có thể giàu vì nó thì thật sự thiên hạ đã giàu hết rồi

- Không dùng cracks của bạn

Nghe có vẻ bất hợp lý, nhưng crack để nhận những niềm vui, là sở thích và cũng để giúp cho công việc chính của bạn tốt hơn; không phải đơn giản là để sử dụng phần mềm free. Mua phần mềm nếu nó có ích cho công việc của bạn, ai cũng phải sống mà

Các phương pháp

Bạn mới bắt đầu và không biết mình nên học phương pháp crack nào, phần này sẽ chia ra cơ bản các phương pháp hiện có để bạn có thể chọn học: Patching, Keygenning, Serial Fishing, ...v.vv và vài dòng mô tả về chúng.

- Patching

Patching (vá) là phương pháp tìm nơi mà chương trình kiểm tra xem nó đã được đăng ký hay chưa (hay bất kỳ nơi nào quyết định cho phép hay không cho phép bạn dùng chương trình) sau đó, ta sẽ sửa đổi tập tin chạy của chương trình để làm cho nó luôn chạy như đã được đăng ký, hoặc là chấp nhận mọi số serial mà ta nhập vào như là số serial chính xác.

- Keygenning

Keygenning (tạo key) là phương pháp tìm nơi chương trình kiểm tra số serial đúng hay sai, và quy trình tạo số serial, rồi từ đó viết một chương trình nhỏ để tạo ra số serial chính xác. Tất nhiên, số serial này là chính xác nên chương trình luôn chấp nhận nó.

- Serial Fishing

Serial Fishing (câu serial) là phương pháp tìm nơi mà chương trình so sánh số serial được nhập với số serial chính xác, rồi từ đó cố gắng thiết lập sao cho số serial chính xác được tạo ra, tìm nó với các thông tin liên quan, cuối cùng phát hành nó theo dạng chương trình nhỏ có hộp kiểm Name/Serial.

- Self-Keygenning

Self-Keygenning (tạo key trong) là phương pháp pha trộn giữa Serial Fishing và Patching. Về cơ bản, Self-Keygenning là phương pháp sửa đổi chương trình để qua đó thay vì chương trình hiện thông báo lỗi khi nhập số serial sai thì nó sẽ hiện cho người dùng biết số serial chính xác.

- Unpacking

Unpacking (giải nén) là phương pháp tạo ra một tập tin chạy không bị nén. Về cơ bản, một tập tin chạy khi bị nén (tức packed) sẽ rất khó hay không thể sử dụng các phương pháp cracking thông thường (Patching, Serial Fishing, Self-Keygenning, Keygenning ...) để crack được. Vì vậy cần phải có bước unpacking trước, rồi mới tiến hành các phương pháp cracking thông thường trên được. Để hiểu thêm về thế nào là "một tập tin chạy bị nén" tôi sẽ giải thích ở gần cuối bài viết này.

- Inline Patching

Inline Patching (vá khi nén) là phương pháp cracking dành riêng cho các tập tin chạy bị nén. Như ở trên, thông thường khi gặp một tập tin chạy bị nén, thì cần phải unpack (giải nén bằng công cụ (unpack tools/ unpack scripts) hay bằng thủ công (manual unpack)) rồi mới tiến hành phương pháp cracking khác được. Nhưng với inline patching thì khác, nó là sự pha trộn giữa Patching và Unpacking cùng với kinh nghiệm từng trải, tốt nhất nếu bạn chưa có kinh nghiệm thì đừng động tới nó vì bạn sẽ hiểu bạn sẽ có ít hơn là được.

Không nhiều phương pháp, nhưng bạn nên bắt đầu với cái dễ nhất là Patching/Serial Fishing, sau đó hãy thử sức với Self-Keygenning/Unpacking, cuối cùng nếu muốn bạn hãy học Keygenning/Inline Patching. Dục tốc bất đạt 

Công cụ

Vậy... để crack thì cần những công cụ nào?

Dưới đây là một số chương trình thông dụng nhất được sử dụng trong cracking. Nếu bạn biết nhiều công cụ thì bạn nên chọn những cái mà mình thích dùng nhất - ai cũng có những ý thích của riêng mình. Ngoài ra, trên mạng có nhiều bộ "Cracker's Kits" được tổng hợp, nhưng theo tôi thì quá nhiều công cụ trong đó không cần thiết (quá cũ, trùng chức năng, chức năng quá nhiều) hoặc chứa malware (rõ ràng là không nên). Tôi đã thiết kế 1 bộ KIT nhỏ dành riêng cho các bạn, bạn có thể tải về nó ở link phần này. Chúc vui!

- OllyDbg

OllyDbg là một chương trình gỡ lỗi (debugger). Nó cho phép bạn xem code bên trong chương trình khi chương trình chạy. Nó là một vũ khí liệt vào hàng quan trọng nhất trong kho vũ khí của bạn đấy. Hiện tại, có rất nhiều các bản được mod lại của nó trên mạng. Hiện tôi đang dùng bản OllyFck, khuyến cáo bạn dùng bản DeFixed OllyDbg của nhóm FOFF, hay tải về dùng bản mà bạn thấy hợp nhãn và có ích cho mình nếu như bạn không thích.

Tải về OllyDbg gốc tại: http://ollydbg.de/

- .NET Reflector

.NET Reflector là một chương trình cho phép bạn xem, điều hướng, phân tích, dịch ngược mã và gỡ lỗi cho một ứng dụng .NET, một chương trình cracking đặc biệt cho .NET. Với nó bạn không cần đến mã nguồn của một ứng dụng .NET, bạn hoàn toàn có thể dịch ngược và phân tích mã .NET trong C# hay Visual Basic. Ví dụ, để tạo một keygen cho một ứng dụng .NET, bạn chỉ đơn giản là dùng chương trình .NET Reflector để trích đoạn code tạo key rồi dùng nó để tạo ra keygen bằng ngôn ngữ .NET, đơn giản và nhanh chóng.

Tải về .NET Reflector tại: http://www.red-gate.com/products/reflector/

- PeiD

PEiD là một chương trình tiện lợi để xác định chương trình được viết bằng ngôn ngữ gì và bị pack bởi packer nào, nó giúp đỡ rất lớn trong quá trình cracking. Ví như nếu chương trình bị pack (nén) thì bạn không thể thực hiện crack nó được hay bạn sẽ không hiểu tại sao mình không crack được chương trình đó. Với PEiD, bạn sẽ có thông tin về packer (trình nén) và phiên bản của nó, sử dụng chúng bạn có thể unpack (giải nén) được tập tin chạy của chương trình và crack được nó bình thường. PEiD còn cung cấp thông tin về compiler (trình biên dịch) nào đã tạo ra tập tin chạy khi nó không bị pack, vì vậy bạn có thể tránh việc tải nhầm chương trình .NET vào Ollydbg để rồi ngồi ngó những dòng code miên man bất tận,...bất lực lắm đó

Tải về PEiD gốc tại: http://peid.has.it/

- Hex Editor

Hex Editor (trình chỉnh sửa hệ 16) là một chương trình rất tiện lợi khác, nếu gặp vấn đề khi không thể lưu lại những sửa đổi trong code của chương trình với OllyDbg, thì một hex editor có thể giải quyết nó dễ dàng. Không có một chương trình Hex Editor nào là tốt nhất, chỉ có những chương trình được sử dụng nhiều và được đánh giá cao. Chúng là:

+ WinHex (http://x-ways.net/winhex/)
+ Hex Workshop (http://www.hexworkshop.com/)

Nếu thích Free và tính năng vừa tầm sử dụng thì bạn có thể dùng:

+ HxD Hex Editor (http://mh-nexus.de/en/hxd/)
+ MiTec HexEdit (http://www.mitec.cz/hex.html)

- dUP

dUP (hay diablo2oo2's Universal Patcher) là một công cụ tuyệt vời để tạo các bản patcher, đặc biệt là khi bạn không có khả năng lập trình. Nó cho phép bạn so sánh giữa tập tin chạy đã crackk (cracked) với tập tin chạy gốc, rồi tạo ta một bản patcher hoàn chỉnh với GUI và nhiều thứ khác, tất cả đều có thể tùy chỉnh bởi chính dUP hay Resource Hacker. Tập tin trợ giúp (helpfile) rất đáng để bạn đọc, nó sẽ chỉ dẫn cho bạn sử dụng tất cả các tính năng của chương trình nhanh nhất và dễ hiểu.

Tải về tại: http://diablo2oo2.di.funpic.de/dup.html

- Resource Hacker

Resource Hacker không phải là một công cụ cracking, nó là công cụ mod chương trình. Nó cho phép bạn có thể thêm/xóa/sửa các form, các ảnh, các nội dung hộp thoại và nhiều thứ khác bên trong bất kỳ một tập tin chạy hay tập tin dll nào. Nó tỏ ra rất tiện lợi trong việc xóa bỏ các dòng chữ có từ "unregistered" trong chương trình, hay đơn giản là chỉnh sửa giao diện chương trình ... cho vui . Tải về tại: http://www.angusj.com/resourcehacker/

- IDE/Compiler

IDE (Integrated Development Environment) và Compiler (trình biên dịch) là những thứ quan trọng nhất nếu như bạn muốn viết code cho chính các patcher và keygen của mình, hay muốn trở thành lập trình viên của team. Chúng sẽ giúp bạn viết code và dịch code bạn viết thành một tập tin chạy chứa những tính năng bạn viết, chúng làm cho việc tạo GUI cho patcher hay keygen của bạn dễ dàng hơn nhiều.

Quý hồ tinh, bất quý hồ đa

Một số trang web download công cụ Cracking:
http://www.woodmann.com/collaborative/tools/index.php/Category:RCE_Tools
http://exelab.ru/download.php
http://www.unpack.cn
http://tuts4you.com/download.php

Bộ KIT: **TinRE Begin Alpha**

1 bộ KIT được tạo ra chỉ nhằm một mục đích, dành tặng cho bạn khi mới bước chân vào thế giới Cracking.

Download: http://www.mediafire.com/?44bk3hiswcsoe

Bộ **CRACKLAB DVD 2011**

1 DVD về các chương trình dành riêng cho Cracker, được tạo ra hàng năm bởi trang web số 1 của Nga: Cracklab.ru

Download:

Phần 1	http://www.fileserve.com/file/JTSCQr8/	Phần 2	http://www.fileserve.com/file/XWPvGEQ/
Phần 3	http://www.fileserve.com/file/w2BRkg2/	Phần 4	http://www.fileserve.com/file/6HuxseD/
Phần 5	http://www.fileserve.com/file/Et5zXyy/	Phần 6	http://www.fileserve.com/file/MKEF6Am/
Phần 7	http://www.fileserve.com/file/XctE329/	Phần 8	http://www.fileserve.com/file/GR2Zfcf/
Phần 9	http://www.fileserve.com/file/HuqhAW4/	Phần 10	http://www.fileserve.com/file/cxxUhEP/
Phần 11	http://www.fileserve.com/file/xtEsuRs/		

Download: http://www.mediafire.com/?u9x9itnsjxpfe

Các yêu cầu khác

Công cụ không phải là tất cả những gì bạn cần để cracking, bạn cần nhiều hơn thế ... đó chính là **kiến thức**!

- Assembly (hợp ngữ) - một ngôn ngữ lập trình

Hợp ngữ là ngôn ngữ máy cấp thấp nhất, là ngôn ngữ máy mà con người có thể đọc hiểu. Khi bạn load bất kỳ một phần mềm nào vào trong Ollydbg thì những dòng code bạn thấy chính là code hợp ngữ. Trong quá trình cracking bạn sẽ tiếp xúc và làm việc với hợp ngữ rất nhiều, tuy nhiên thực tế không có mấy phần mềm viết bằng ngôn ngữ lập trình hợp ngữ, những phần mềm viết bằng hợp ngữ chủ yếu là các keygen, và người viết chúng không ai khác là crackers. Vậy bạn đã thấy tầm quan trọng của nó? Chắc chắn rằng nếu bạn không biết về hợp ngữ thì bạn không thể cracking, hoặc nếu bạn bắt chước giỏi thì cũng chắc chắn bạn không hiểu và không biết mình thực sự đang làm những gì, nói chi đến việc tìm niềm vui trong đó)

- Hệ số

Có rất nhiều hệ số: hệ nhị phân (hệ 2), hệ thập lục phân (hệ 16), hệ lục thập tứ phân (hệ 64) ... v.v và tất cả những hệ số đó đều được sử dụng trong quá trình cracking, không lúc này thì lúc khác. Tuy nhiên, ban đầu bạn cần học và hiểu về hệ nhị phân (hệ 2 - bin) và hệ thập lục phân (hệ 16 - hex), đây là 2 hệ được sử dụng nhiều nhất. (Tôi sẽ có bài viết riêng về phần này sau)

- Lập trình

Kỹ năng lập trình thực ra cũng chưa cần thiết vào lúc này, nhưng nếu bạn muốn tự tay mình code những keygen và patcher của chính mình thì lại rất cần kỹ năng lập trình. Nhưng nếu bạn không thể thì vẫn không sao cả vì những công cụ hỗ trợ tạo patcher và keygen giúp bạn là rất **NHIỀ**U. Tuy là nói vậy nhưng nếu có khả năng lập trình là bạn đã có một lợi thế rất **LỚN** và tiến gần đến trở thành một Cracker hơn bất kỳ newbie nào khác.

- **Một máy tính đủ mạnh**

Nghe chẳng có vẻ gì liên quan nhỉ ^^! Nhưng thực tế nếu như bạn đang dùng máy tính cũ hơn 3 năm thì nên vứt nó đi, sắm con Core 2 Duo + 2GB RAM chạy cho nó mượt, về hệ điều hành thì nên dùng Windows XP là tốt nhất, phần lớn các công cụ dùng trong cracking chạy trên nó. Windows 7 và Mac OS tốt nhất nếu có sử dụng thì cài song song với Windows XP và không dùng khi cracking, chỉ dùng để test sản phẩm xem nó có tương thích với nhiều hệ điều hành hay không thôi.

- Quyết tâm, kiên nhẫn, có thời gian, và chịu khó học hỏi

Trên đây chỉ là những chỉ dẫn cơ bản, để học những điều cơ bản đó bạn cần có thời gian và sự quyết tâm không gục ngã, tinh thần ham hố những kỹ thuật và thông tin mới của cracking, không biết thì hỏi, không trả lời … ta hỏi người khác ... cứ như thế bạn sẽ thực hiện được ƯỚC MƠ trở thành một Cracker. Ừm, mọi bắt đầu đều có những thất bại, tôi chắc chắn với bạn rằng không một cracker nào lại có thể thành công ngay khi Step Into vào một lệnh CALL, chắc chắn cũng phải gặp vài lệnh CALL sai trước khi "xử" xong. Không việc gì phải "xoắn" khi ta làm sai, đơn giản là bắt đầu lại

Tạo cracks đầu tiên của bạn

Chúc mừng bạn đã crack được chương trình đầu tiên ^^ Bạn đã làm gì thế? Bạn đã patch nó ư? Bạn tìm được vòng lặp tạo serial à? Rất tốt, nếu bạn làm được điều ấy thì bạn đã có những thông tin cần thiết để tạo cho mình bản cracks đầu tiên rồi đó Tuyệt!!

Bây giờ, bạn có thể tạo:

- **1 Patcher:**

  Ừm, bạn đã crack một chương trình bằng cách patching. Chương trình chạy như được đăng ký rồi, và không có gì bất ổn sau khi test. Không cần thiết phải bê cái tập tin cracked nặng vài MB đi release trong khi bạn chỉ patch có vài byte. Chúng ta cần làm một patcher để cho nó chuyên nghiệp và cũng giảm kích thước khi bê đi release. Bạn có thể sử dụng một công cụ tạo patcher (như: dUP chẳng hạn) hay bạn có thể tự code cho chính patcher của mình. Để làm nó bạn cần một bài hướng dẫn, nó đây:

  - dùng dUP: (cập nhật sau....)
  - code patcher: http://lmgtfy.com/?q=Code+patcher

- 1 Keygen:

Bạn tìm ra được vòng lặp tạo serial và đã có những thông tin cần thiết về số serial đó (như: dài hơn 8 ký tự, tổng của ký tự thứ 2 và 8 là 15, ký tự thứ 5 bắt buộc phải là "j"). Tạo một keygen cần thu thập những thông tin như vậy, rồi sử dụng kỹ năng lập trình sẵn có để code nên keygen. Ở đây, tôi có những bài hướng dẫn về code keygen và kỹ năng lập trình:

- kỹ năng lập trình: http://lmgtfy.com/?q=Programming+Tutorials
- code keygen: http://lmgtfy.com/?q=Code+keygen

Nói gì thì nói kỹ năng lập trình là không thể thiếu để bạn tiến xa trong thế giới cracking. Học ngôn ngữ lập trình gì? Dùng công cụ soạn thảo và biên dịch (IDE/Compier) gì?

Ừm, về ngôn ngữ lập trình bạn nên học:

- **bắt buộc:** Assembly (hợp ngữ)
- **tùy chọn:** C++, Delphi (Pascal), Visual Basic .NET, ... v.v

Ở trên là theo cá nhân tôi, còn bạn thì có thể học bất cứ ngôn ngữ gì bạn thích, miễn là bạn có thể lập trình được với nó là OKEY! Bản thân tôi chọn ngôn ngữ Visual Basic .NET để học vì nó thời thượng ;P

Một vài IDE/Compiler được đánh giá tốt:

- MASM32 (http://www.masm32.com/masmdl.htm)
- Dev C++ (http://www.bloodshed.net/download.html)
- Borland Delphi (http://www.embarcadero.com/products/delphi/downloads)
- Microsoft Visual Studio (http://www.microsoft.com/visualstudio/en-us/try)

Tập tin chạy bị nén (PACKED)

Ở dưới đây, tôi dùng từ "nén" với nghĩa là "pack" (thay vì là "compress), "giải nén" với nghĩa là "unpack" (thay vì là "extract" hay "decompress"), tương tự sẽ có những từ "quá trình nén" với nghĩa là "packing" và từ "quá trình giải nén" với nghĩa là "unpacking". Từ ngữ trên chỉ dùng trong bài viết này và cả trong cracking, có thể gọi nó là từ "chuyên môn" để phân biệt với mấy cái "thường môn" khác T.T

Packing là phương pháp được sử dụng để nén tập tin chạy của chương trình, trước hết là để giảm kích thước, nhưng thực chất là để gây cản trở cho các quá trình dịch ngược. Một trình nén Packer tiêu chuẩn sẽ nén tập tin chạy, sẽ thay đổi một số mã nhị phân trong tập tin mà hệ điều hành không thể thấy được. Khi được gọi để chạy, thì tập tin chạy bị nén sẽ được giải nén vào trong RAM. Về cơ bản, một tập tin bị nén kiểu RAR/ZIP sẽ được giải nén trên ổ cứng, còn tập tin chạy bị nén thì nó sẽ được giải nén vào trong RAM.

Về cơ bản, ta không thể cracking được một tập tin chạy đã bị nén lại. Chính vì thế, những trình nén packer thương mại thường cung cấp các phương thức chống cracking, chống gỡ lỗi, chống nạp vào chương trình gỡ lỗi …v..v… Khi ta bất chấp mà tải tập tin chạy vào trong Ollydbg, nhẹ thì có 1 thông báo lỗi, nặng thì máy bị shut down ngay lập tức.

Một công cụ đã được đề cập ở trên là PeiD – một chương trình phát hiện packer/ compiler. Nếu một tập tin chạy bị nén, nó cung cấp rất nhiều thông tin về chương trình nào đã nén tập tin chạy, phiên bản của nó. Còn nếu tập tin không bị nén, thì nó sẽ cung cấp thông tin về trình biên dịch nào đã tạo ra tập tin, được viết bởi ngôn ngữ gì … Chương trình có sẵn nhiều plug-in để mở rộng các tính năng của nó. Tải về các plug-in tại: http://peid.has.it/

Ở phần trên, bạn đã biết thế nào là một tập tin chạy bị nén, thì ở phần dưới này bạn cần biết cách để giải nén nó. Đối với hầu hết các trình nén packer hiện có, sử dụng một trình giải nén unpacker để giải nén là nhanh nhất, nhưng kết quả thì không biết được có thành công hay không, chà cái này là hên xui :D Cách tốt nhất là học cách giải nén qua Ollydbg và các công cụ khác.

Khi giải nén xong một tập tin chạy, hãy kiểm tra nó ngay, xem nó có chạy tốt không, nếu tốt thì bạn có thể bắt tay vào cracking nó như bất cứ tập tin chạy không bị nén nào đó. Sau đó, bạn sẽ làm gì khi đã crack được nó? Nếu là một keygen thì bạn có thể phát hành nó mà không lo nghĩ gì nữa, nếu như bạn chỉ vá vài chỗ thì tốt nhất bạn nên phát hành tập tin chạy đã giải nén, đã crack đầy đủ, kèm một hướng dẫn chép đè tập tin hơn là tạo một patcher cho nó.

Tạm kết

Tôi hy vọng bạn sẽ thích bài chỉ dẫn cracking này, sẽ học được nhiều thông tin hữu ích từ nó. Hy vọng sẽ sớm gặp bạn trong cộng đồng vào một ngày gần nhất

Bạn nào có góp ý, có bổ sung, sửa chữa nào cho bài viết này, rất vui và luôn chào đón, email cho tôi tieutrong@live.com và tôi sẽ liên lạc với bạn ngay!

THỰC HÀNH LÀ TỐT NHẤT

Cách tốt nhất để học Cracking là thực hành. Thực hành liên tục, thực hành nhiều để tạo thói quen, kinh nghiệm và cảm giác. Dưới đây là một vài link target cho bạn thực hành: crackmes, keygenmes, reversemes

http://www.reversing.be/index.php?topic=crackmes
http://tuts4you.com/download.php?list.49

KẾ TIẾP PHẢI LÀM GÌ?

Bài chỉ dẫn này đã cung cấp cho bạn những gì cơ bản nhất về cracking. Nếu đã thành thạo những phương pháp ở trên thì vẫn còn nhiều lĩnh vực để bạn khám khá: Game Cracking/ Keygenning, Dongle Cracking …. luôn là vô tận

CÁC LIÊN KẾT KHÁC

http://www.tuts4you.com/
http://cracklab.ru/links/
http://reaonline.net
http://cin1team.biz

LỜI CẢM TẠ

Xin gửi lời cảm tạ đến các anh chị: hacnho, kienmanowar, Merc, why not bar, hoadongnoi, NhatPhuongLe … đã tạo nên một cộng đồng Reversing Engineering tại Việt Nam.

Xin gửi lời cảm ơn đến các bạn trong diễn đàn REAonline.net và CiN1Team.biz vì những điều mình đã học hỏi được từ các bạn, mong rằng tinh thần chia sẻ và học hỏi sẽ cháy mãi, không tàn lụi :D

Và cảm ơn bạn đã đến với Cracking, mong rằng bài viết này sẽ mở đầu cho hành trình chinh phục và phát triển cộng đồng của bạn sau này.

Vạn điều tốt lành đến với mọi người!

Nha Trang, ngày 3 tháng 10 năm 2011
Chỉ có 1 điều luôn thay đổi, đó là giới hạn những gì bạn có thể làm!