

به نام خدا

مهندسی معکوس نرم افزار

تألیف: سید داود ملک حسینی

(گروه امنیتی هامن)

انتشارات پندار پارس

سرشناسه	: ملک حسینی، سید داود، ۱۳۶۷-
عنوان و نام پدیدآور	: مهندسی معکوس نرم افزار / تالیف داود ملک حسینی.
مشخصات نشر	: تهران : پندار پارس ، ۱۳۹۸.
مشخصات ظاهری	: ۲۵۶ ص: مصور، جدول.
شابک	: 978-600-8201-66-3
وضعیت فهرست نویسی	: فیا
یادداشت	: کتابنامه.
موضوع	: مهندسی معکوس-- نرم افزار
موضوع	: Reverse engineering-- Software
رده بندی کنگره	: ۱۳۹۷ ۹م۶۶/۵/۱۰۸۲۸
رده بندی دیویی	: ۰۰۴۲۰۲۸۵/۶۱
شماره کتابشناسی ملی	: ۵۴۴۰۱۱

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتخوار، واحد ۱۶ www.pendarepars.com
 تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۱ ۴۵۲۳۴۸ info@pendarepars.com



نام کتاب	: مهندسی معکوس نرم افزار
ناشر	: انتشارات پندار پارس
تالیف	: سید داود ملک حسینی
چاپ نخست	: بهمن ۹۸
شمارگان	: ۵۰۰ نسخه
طرح جلد	: سارا یعسوی
چاپ، صحافی	: روز
قیمت	: ۲۵۰,۰۰۰ تومان

شابک : ۹۷۸-۶۰۰-۸۲۰۱-۶۶-۳

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

۳	بخش نخست: کیژن (Keygen).....
۵	فصل نخست: دو روش در ساخت کیژن مربوط به الگوریتم MD5.....
۵	مقدمه.....
۶	کیژن MD5.....
۶	۱-۱ پیشگفتار.....
۶	۱-۲ پیش از شروع.....
۸	۱-۳ آمادگی لازم برای آغاز کار.....
۱۰	۱-۴ تجزیه و تحلیل الگوریتم.....
۲۱	۱-۵ پیدا کردن یک کلید معتبر.....
۲۶	۱-۶ معکوس کردن الگوریتم.....
۲۷	۱-۷ حرف آخر.....
۲۸	روش دوم کان نمودن MD5.....
۲۸	۱-۸ چیده.....
۲۸	۱-۹ هدف.....
۲۸	۱-۱۰ تجزیه تحلیل هدف.....
۲۹	۱-۱۱ پیدا کردن روال الگوی تأیید (verification).....
۳۰	۱-۱۲ پیدا کردن شروع الگوی MD5.....
۳۱	۱-۱۳ پیدا کردن رشته های که هش شده اند.....
۳۲	۱-۱۴ استفاده از MD5 hash.....
۳۲	۱-۱۵ خلاصه مطلب.....
۳۳	۱-۱۶ نتیجه گیری.....
۳۵	فصل دوم: Keygenning GameShield.....
۳۵	مقدمه.....
۳۶	موارد مورد نیاز.....
۳۶	۲-۱ نرم افزار آزمایشی.....
۳۶	۲-۲ ابزارهای مورد نیاز.....
۳۶	۲-۳ تحقیقی در مورد ساختار گواهی.....
۳۷	۲-۴ Authorization Definitions (AD).....
۳۷	۲-۵ AUTHORIZATIONS REQUEST CODES (ARC).....
۳۷	۲-۶ ACTIVATION CODES (AC).....
۳۸	۲-۷ SERIAL NUMBERS.....
۳۹	۲-۷-۱ بازیابی Password Global و License Password.....
۳۹	۲-۸ Dump کردن DLL.....
۳۹	۲-۸-۱ از مشکل Stack Overflow می گذریم.....
۴۰	۲-۹ موقعیت یابی پروسه آنپک.....
۴۱	۲-۱۰ بدست آوردن DLL.....

۲۴	۲-۱۱ بررسی خروجی‌ها
۲۵	۲-۱۲ بدست آوردن گواهی‌های توابع
۴۶	۲-۱۳ نوشتن رباینده پسورد
۴۷	۲-۱۴ تعریف الزامات
۴۷	۲-۱۴-۱ آغاز کردن پروسه
۲۸	۲-۱۵ تنظیم Virtual Protect و PAGE-NOACCESS
۴۸	۲-۱۶ جست‌وجو کردن توابع مربوط به آنیک
۵۰	۲-۱۷ انتظار برای عملکرد نقاط ترمز (Break points)
۵۰	۲-۱۸ پاک کردن و بستن
۵۱	۲-۱۹ خروجی Gameshield 4.6
۵۱	۲-۲۰ بدست آوردن پسورد مجاز و معتبر
۵۱	۲-۲۰-۱ رمز گشایی گواهی
۵۲	۲-۲۰-۲ ساختار فایل گواهی
۵۵	۲-۲۱ استفاده از Delphi Parser
۵۶	۲-۲۲ انتخاب یک Authorization Definition
۵۸	۲-۲۳ ساختن کلید
۵۸	۲-۲۴ رمزگشایی به کمک XOR
۶۱	۲-۲۵ ساختن یک کد فایل ساز
۶۳	۲-۲۶ نتیجه گیری
۶۵	بخش دوم: آنیک کردن (Unpack)
۶۷	فصل سوم: آنیک کردن HASP SL
۶۷	چکیده
۶۷	۳-۱ یک نرم‌افزار آزمایشی
۶۷	۳-۲ چگونگی انجام پروسه آنیک
۷۴	نتیجه گیری
۷۵	فصل چهارم: آنیک کردن PECompact v2.79 beta
۷۵	مقدمه
۷۵	۴-۱ آنیک کردن
۸۳	۴-۲ گزینه‌ها و موارد بیشتر
۸۹	فصل پنجم: آنیک molbox
۹۷	۵-۲ نگاهی کلی به Virtual DLL#2
	۵-۳ بحثی در مورد OEP مربوط به Molebox، تصحیح صدا زدن‌ها، مخفی کردن فایل
۱۰۰	ها
۱۰۳	۵-۴ فایل‌های پنهان شده
۱۰۹	فصل ششم: آنیک کردن Private exe protector (PEP)
۱۱۰	۶-۱ مقدمه
۱۱۲	۶-۲ تعیین مکان و موقعیت OEP
۱۱۳	۶-۳ OEP

۱۱۷	۶-۴ محافظت وارد شده
۱۱۹	۶-۵ محافظت anti - dump
۱۲۰	۶-۶ PE Header
۱۲۱	۶-۷ Code Section Section Header
۱۲۲	۶-۸ ابهام سازی
۱۲۶	۶-۹ بازکردن محافظ
۱۲۷	۶-۱۰ پارامترها
۱۲۷	۶-۱۰-۱ hModule
۱۳۶	۶-۱۰-۲ MORPH macro
۱۴۳	۶-۱۱ Main handler
۱۵۰	۶-۱۱ 0x00 (VM_EXIT) handler
۱۵۱	۶-۱۳ 0x0D handler
۱۵۲	۶-۱۴ 0x0E handler
۱۵۴	۶-۱۵ 0x12 handler
۱۵۵	۶-۱۶ 0x13 handler
۱۵۸	۶-۱۷ تست پایانی
۱۵۸	چه موارد باقی مانده ؟
۱۵۸	از Trial استفاده کنیم یا Demo ؟
۱۶۱	فصل هفتم: ExeCryptor
۱۶۲	۷-۱ ابزارهای مورد نیاز
۱۶۲	۷-۲ آنپک کردن و به هم ریختن (dumping)
۱۷۱	۷-۳ بازسازی ورودی‌ها (imports)
۱۷۶	۷-۴ حذف محدودیت‌ها
۱۸۱	۷-۵ loader در بهترین حالت
۱۹۱	۷-۶ نتیجه‌گیری
۱۹۳	بخش سوم: مبحث دانگل کرکینگ
۱۹۵	فصل هشتم: برداشتن قفل سخت‌افزاری Sentinel SuperPro از سر و قرارها
۱۹۵	۸-۱ روش‌ها و رویکردهای ممکن: تقلید کننده در مقابل شبیه ساز
۱۹۵	۸-۲ دانگل چگونه کار می‌کند
۱۹۸	۸-۲-۱ تقلید کننده یک دانگل
۱۹۸	۸-۲-۲ تقلید کننده چگونه کار می‌کند؟
۲۰۰	۸-۲-۳ شبیه ساز چگونه کار می‌کند؟
۲۰۱	۸-۳ دیس اسمبل کردن یک برنامه محافظت شده توسط Sentinel
۲۰۲	۸-۳-۱ دیس اسمبل کردن توسط IDA
۲۰۷	۸-۳-۲ دیس اسمبل کردن توسط OllyDbg
۲۰۹	۸-۴ برخی جزئیات در مورد برنامه نویسی رابط کاربری Sentinel Applications
۲۰۹	۸-۴-۱ Sentinel SuperPro چیست؟
۲۱۰	۸-۴-۲ ساختار حافظه کلید

۲۱۲	سلول‌های انتخاب شده و قابل برنامه نویسی	۸-۴-۳
۲۱۲	کدهای دسترسی (Access Code)	۸-۵
۲۱۴	انواع سلول	۸-۵-۱
۲۱۴	مرجع تابع API	۸-۵-۲
۲۱۸	نوشتن مجدد روی API‌های Sentinel	۸-۵-۳
۲۱۸	SproFormatPacket	۸-۵-۴
۲۲۰	SproFindFirstUnit	۸-۵-۵
۲۲۱	SproOverWrite	۸-۵-۶
۲۲۱	SproFindNextUnit	۸-۵-۷
۲۲۲	SproRead	۸-۵-۸
۲۲۹	رویکرد SproRead	۸-۵-۹
۲۳۱	SPROQuery	۸-۵-۱۰
۲۳۶	موارد بیشتر	۸-۵-۱۱
۲۳۷	فصل نهم: یک بررسی عمیقتر - HASP SL	
۲۳۷	مقدمه	۹-۱
۲۳۷	۹-۱ بدست آوردن ابزار آزمایشی	۹-۲
۲۳۷	۹-۲ ترفندهایی برای دور زدن آنتی-دیباگ به صورت دستی	۹-۳
۲۴۶	۹-۳ چه نسخه‌ای را بکار ببریم؟	۹-۴
۲۴۷	۹-۴ ترفندهای جدید HASP در Minitab I	

پیشگفتار مؤلف

کتابی که در دستان شماست شامل کلیدی‌ترین و تخصصی‌ترین مباحث مهندسی معکوس نرم‌افزار در شاخه کرک می‌باشد که پس از تست کامل و دقیق همه مثال‌ها و دستورات مندرج در کتاب، اقدام به چاپ آن نمودیم. جلد دوم آن نیز در دست آماده‌سازی است که امیدوارم به زودی به عرصه چاپ و نشر برسد.

اینجانب سید داود ملک حسینی دارای بورس تخصصی هک و امنیت و مهندسی معکوس نرم‌افزار می‌باشد و تسلط به زبان‌های برنامه‌نویسی سطح بالا و سطح پایین و متخصص در شبکه‌های مخابراتی و ارتباطی هستم. این کتاب، حاصل دانش چندین ساله و سال‌ها تجربه‌ام در این زمینه است و آنرا به نام اعضای جامعه مهندسی کامپیوتر تقدیم می‌کنم و امیدوارم روزی کشور عزیزمان به سمت پیشرفت واقع در مسیر علوم کامپیوتر برود.

جا دارد از همه عزیزان که طی این سال‌ها حامی و پشتیبانم بوده‌اند، به‌ویژه پدر و مادر گرانقدرم تقدیر و تشکر نمایم. همچنین، رون این نام زحمات سرکار خانم مهندس مریم قارونی، فارغ التحصیل کارشناسی ارشد امنیت اطلاعات از دانشگاه ایزد، کتاب به مرحله تألیف و چاپ نمی‌رسید و لازم می‌دانم از ایشان قدردانی کنم و امیدوارم در تمام مراحل زندگی موفق و پیروز باشند.

با امید رسیدن به فردایی بهتر و ایرانی پیشرفته و قدرتمند

در پناه حق

سید داود ملک حسینی

گروه امنیتی هامان