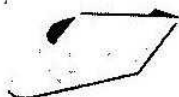


به نام خدا



مؤسسه فرهنگی هنری
دیباکراں تهران

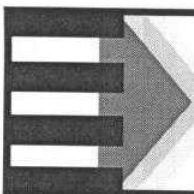
تجزیه و تحلیل بدافزارها

راهنمای جامع مهندسان معکوس، تجزیه و تحلیل بدافزارها،
جاسوس افزارها و روتک های کامپیوتری

مؤلفان

مهندس رضا مقدم

مهندس میلاد کهساری الهادی



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

تجزیه و تحلیل بدافزارها

راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها، جاسوس افزارها و روتکیت های کامپیوتری

مؤلفان: مهندس رضا مقدم - مهندس میلاد کهساری الهادی

ناشر: مؤسسه فرهنگی هنری دیپاگران تهران

حروفچینی و صفحه آرای: مجتمع فنی تهران

طرح روی جلد: مجتمع فنی تهران

چاپ: نگین

نوبت چاپ: اول

تاریخ نشر: اسفند ماه ۱۳۹۴

تیراژ: ۳۰۰ نسخه

قیمت: ۵۰۰۰۰۰ ریال

برش نایب: مقدم، رضا، ۱۳۶۹ -

عنوان و نام پدیدآور: تجزیه و تحلیل بدافزارها؛ راهنمای جامع مهندسی معکوس، تجزیه و تحلیل

بدافزارها، جاسوس افزارها و روتکیت های کامپیوتری / مؤلفان رضا مقدم، میلاد کهساری الهادی.

مشخصات نشر: تهران: مؤسسه فرهنگی هنری دیپاگران تهران، ۱۳۹۴.

مشخصات ظاهری: ۵۴۸ س. ش. - دور.

شابک: 978-600-124-430-8

وضعیت فهرست نویسی: فیا

عنوان دیگر: راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها، جاسوس افزارها و

روتکیت های کامپیوتری.

موضوع: نرم افزار بدافزار

موضوع: ویروس های کامپیوتری

موضوع: مهندسی معکوس -- نرم افزار

شناسه افزوده: کهساری الهادی، میلاد، ۱۳۷۲ -

رده بندی کنگره: ۱۳۹۴ ۹م۷/۹۶/۷۶ QAV۶

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۴۱۷۸۴۱۳

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۳۰-۸

ISBN: 978-600-124-430-8

نشانی دفتر مرکزی: تهران، سعادت آباد، میدان کاج، خ سرو شرقی، روبه روی خ علامه، پلاک ۴۹

وب سایت: dibakaran.mft.info

صندوق پستی: ۱۴۳۳۵/۹۴۳

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، قبل از چهارراه لبافی نژاد، پلاک ۱۲۵۱

کد پستی: ۱۳۱۴۹۸۳۱۸۵

تلفن: ۲۲۰۸۵۱۱۱-۱۲

فروش اینترنتی: www.mftshop.com

پست الکترونیکی: bookmarket@mftmail.com

فهرست مطالب

۹	مقدمه ناشر
۱۰	مقدمه مؤلفان
	بخش اول، درآمدی بر مفاهیم پایه و تحلیل ساده بدافزار
	فصل اول: مقدمه‌ای بر مفاهیم پایه تحلیل بدافزار
۱۶	تجزیه و تحلیل بدافزار چیست؟
۱۷	هدف از تجزیه و تحلیل بدافزار چیست؟
۱۸	تکنیک‌های تجزیه و تحلیل بدافزار
۲۰	انواع بدافزارها
۲۳	قوانین عمومی تجزیه و تحلیل بدافزار
۲۳	روش تجزیه و تحلیل ایستا
۲۴	پوشش با ضدویروس‌ها، رین گاه خودمند
۲۵	هش، یک نشانه شناسایی و صرف‌فرد برای شناسایی بدافزار
۲۶	شناسایی رشته‌ها
۲۹	بدافزارهای مهم‌سازی و بست‌نوی شده
۳۲	قالب فایل اجرایی قابل حمل
۳۲	توابع و کتابخانه‌های پیوندی
۳۶	قراردادهای نام‌گذاری توابع
۳۷	تجزیه و تحلیل عملی استاتیک
۴۱	بخش‌ها و سرایندهای فایل PE
۴۹	خلاصه سرایند PE
۵۰	نتیجه‌گیری
۵۰	آزمایشگاه اول
	فصل دوم: تجزیه و تحلیل بدافزار در ماشین مجازی
۵۴	ساختار ماشین مجازی
۵۵	ایجاد ماشین تجزیه و تحلیل بدافزار
۵۸	استفاده از ماشین مجازی تجزیه و تحلیل بدافزار
۶۲	خطرهای استفاده از برنامه VMware در تحلیل بدافزار
	فصل سوم: تجزیه و تحلیل پویای بدافزار
۶۳	جمعیه‌های شنی، رویکردی کثیف و سریع
۶۶	اجرای بدافزار
۶۹	نظارت با Process Monitor
۷۴	مشاهده فرایندها با Process Explorer
۷۹	مشاهده ساختار درختی فرایندها با Plist
۸۱	مقایسه رجیستری Snapshotها با Regshot
۸۲	یک شبکه جعلی

۸۵	شنود بسته‌های شبکه با Wireshark
۸۷	استفاده از InetSim
۸۹	ابزارهای تجزیه و تحلیل پویا در عمل
۹۳	نتیجه‌گیری
۹۳	آزمایشگاه دو

بخش دوم: تمرین و تحلیل ایستای پیشرفته

فصل چهارم دیس اسمبلی در معماری x86

۹۷	سطوح انتزاعی یا تجریدی
۱۰۰	مهندسی معکوس
۱۰۱	معماری x86
۱۰۲	حافظه اصلی
۱۲۶	نتیجه‌گیری

فصل پنجم: دیس اسمبلی IDA Pro

۱۲۸	بارگذاری یک فایل اجرایی
۱۳۰	رابط کاربری دیس اسمبلی IDA Pro
۱۳۹	استفاده از ویژگی فراراجاعات
۱۴۱	تجزیه و تحلیل توابع
۱۴۲	استفاده از گزینه‌های تولید گراف
۱۴۵	بهبود دیس اسمبلی
۱۴۹	توسعه IDA Pro با پلاگین‌ها
۱۵۲	استفاده از پلاگین‌های تجاری
۱۵۲	نتیجه‌گیری
۱۵۳	آزمایشگاه سوم

فصل ششم: شناخت ساختمان‌های کد C در اسمبلی

۱۵۶	متغیرهای عمومی در مقابل محلی
۱۵۸	دیس اسمبل عملیات‌های محاسباتی
۱۶۰	شناخت عبارات شرطی
۱۶۱	تجزیه و تحلیل گرافیکی توابع با IDA Pro
۱۶۲	شناخت عبارات if تو در تو
۱۶۴	شناخت حلقه‌ها
۱۶۷	درک قراردادهای فراخوانی توابع
۱۶۹	دستورالعمل Push در مقابل Mov
۱۷۱	تحلیل عبارات Switch
۱۷۳	جدول پرش
۱۷۶	دیس اسمبلی آرایه‌ها
۱۷۸	شناسایی ساختمان‌ها
۱۸۰	تجزیه و تحلیل لیست‌های پیوندی پیمایشی

۱۸۲.....	نتیجه گیری.....
۱۸۳.....	آزمایشگاه چهارم.....
	فصل هفتم: تجزیه و تحلیل برنامه‌های مخرب ویندوز
۱۸۵.....	رابط‌های برنامه‌نویسی ویندوز.....
۱۸۷.....	هندل‌ها.....
۱۹۲.....	ایجاد یک درپشتی.....
۱۹۳.....	دور زدن جعبه‌شنی Avast با استفاده از جایگزینی جریان داده.....
۱۹۴.....	رجیستری ویندوز.....
۱۹۵.....	کلیدهای ریشه رجیستری.....
۱۹۸.....	تجزیه و تحلیل کدهای رجیستری به صورت عملی.....
۲۰۰.....	اسکرپت‌نویسی رجیستری با فایل‌های .reg.....
۲۰۰.....	رابط‌های برنامه‌نویسی شبکه.....
۲۰۳.....	رابط‌های برنامه‌نویسی WinINet.....
۲۰۴.....	دنبال کردن پهنای‌های در باز اجرا.....
۲۰۶.....	فرایندها.....
۲۰۹.....	تردها.....
۲۱۴.....	سرویس‌ها.....
۲۲۰.....	سرور COM بدافزار.....
۲۲۱.....	استثنا: هنگامی که اشتباهی پیش می‌آید.....
۲۲۲.....	حالت کاربر در برابر حالت کرنل.....
۲۲۳.....	رابط‌های برنامه‌نویسی (API) محلی.....
۲۲۶.....	نتیجه‌گیری.....
۲۲۶.....	آزمایشگاه پنجم.....
	بخش سوم: تجزیه و تمایز دیباگرها
	فصل هشتم: دیباگر
۲۳۱.....	دیباگرهای سطح کد در مقابل دیباگرهای سطح اسمبلی.....
۲۳۲.....	دیباگر در حالت کاربر در برابر حالت کرنل.....
۲۳۳.....	استفاده از یک دیباگر.....
۲۳۵.....	توقف موقت اجرای برنامه با نقاط توقف.....
۲۴۰.....	استثناها.....
۲۴۲.....	تغییر مسیر اجرا با دیباگر.....
۲۴۳.....	تغییر مسیر اجرا به صورت عملی.....
۲۴۴.....	نتیجه‌گیری.....
	فصل نهم: دیباگر OllyDBG
۲۴۶.....	بارگذاری بدافزار.....
۲۴۷.....	رابط کاربری دیباگر OllyDBG.....
۲۵۰.....	نقشه حافظه.....

۲۵۳	مشاهده تردها و پشته‌ها
۲۵۴	اجرای کد
۲۵۶	نقاط توقف
۲۶۱	بارگذاری کتابخانه‌های پیوندی پویا
۲۶۲	ردیابی
۲۶۶	مهار یا اصلاح کردن
۲۶۷	تجزیه و تحلیل شکلد
۲۶۸	ویژگی‌های کمکی
۲۶۹	پلاگین‌های OllyDBG
۲۷۱	نشانه‌گذاری
۲۷۲	توسعه دیباگر با قابلیت اسکریپت‌نویسی
۲۷۴	نتیجه‌گیری
۲۷۵	آزمایشگاه ششم

فصل دهم: دیباگ در سطح کرنل WinDBG

۲۷۷	کد کرنل و درایورها
۲۷۹	آماده‌سازی محیط برای دیباگ کرنل
۲۸۳	استفاده از WinDBG
۲۸۸	سمبول‌های مایکروسافت
۲۹۳	دیباگ کرنل در عمل
۲۹۸	شناسایی اشیای درایور
۲۹۹	روت‌کیت‌ها
۳۰۵	بارگذاری درایورها
۳۰۶	دیباگ کرنل ویندوز ویستا، هفت و نسخه‌های ۶۴ بیتی
۳۰۷	نتیجه‌گیری
۳۰۷	آزمایشگاه هفتم

بخش چهارم: عملکرد بدافزار

۳۱۱	فصل یازدهم: رفتار بدافزار
۳۱۲	بارگذارها و راه اندازه‌ها
۳۱۵	دره‌های پستی
۳۲۴	سارقین اعتبارنامه‌ها
۳۳۰	مکانیسم‌های ماندگاری
۳۳۲	بالا بردن سطح دسترسی
۳۳۵	روت‌کیت‌های سطح کاربر
۳۳۵	نتیجه‌گیری
۳۳۵	آزمایشگاه هفتم
۳۳۷	فصل دوازدهم: راه‌اندازی مخفیانه بدافزار
	راه اندازه‌ها

۳۳۸.....	تزریق فرایند
۳۴۱.....	تزریق مستقیم
۳۴۲.....	جایگزینی فرایند
۳۴۴.....	تزریق هوک
۳۴۸.....	تزریق API
۳۴۹.....	نتیجه گیری
۳۴۹.....	آزمایشگاه هشتم

فصل سیزدهم: رمز گذاری داده ها

۳۵۲.....	هدف تحلیل الگوریتم های رمز گذاری
۳۵۲.....	سایفرهای ساده
۳۶۴.....	الگوریتم های رمزنگاری راین
۳۶۶.....	جستجوی بیت های رمزنگاری
۳۷۰.....	رمز گذاری در روشی
۳۷۳.....	رمز گشایی
۳۷۳.....	خود رمز گشایی
۳۷۴.....	برنامه نویسی دستی توابع رمز گشایی
۳۷۹.....	نتیجه گیری
۳۷۹.....	آزمایشگاه نهم

فصل چهاردهم: نشانه ارتباطات شبکه متمرکز: بدافزار

۳۸۱.....	اقدامات متقابل مبتنی بر شبکه
۳۸۲.....	مشاهده بدافزار در جایگاه طبیعی خود
۳۸۲.....	نشانه هایی از فعالیت های مخرب
۳۸۳.....	امنیت عملیاتی (OPSEC)
۳۸۴.....	بررسی آنلاین یک مهاجم به صورت ایمن
۳۸۶.....	اقدامات متقابل شبکه مبتنی بر محتوا
۳۹۲.....	ترکیب روش های تجزیه و تحلیل ایستا و پویا
۴۰۷.....	درک چشم انداز مهاجم
۴۰۸.....	نتیجه گیری
۴۰۸.....	آزمایشگاه دهم

بخش پنجم: ضد مهندسی معکوس

فصل پانزدهم: ضد دیس اسمبل

۴۱۴.....	درک روش ضد دیس اسمبلی
۴۱۵.....	غلبه بر الگوریتم های دیس اسمبلی
۴۲۱.....	روش های ضد دیس اسمبلی
۴۲۸.....	مهم سازی کنترل جریان
۴۳۶.....	خنثی سازی تحلیل ساختار پشته
۴۳۸.....	نتیجه گیری

۴۳۹.....	آزمایشگاه یازدهم.....
	فصل شانزدهم: روش های ضد دیباگ
۴۴۱.....	تشخیص دیباگرهای ویندوز.....
۴۴۷.....	تشخیص رفتار دیباگر.....
۴۵۰.....	مداخله در عملکرد دیباگر.....
۴۵۵.....	آسیب پذیرهای دیباگر.....
۴۵۷.....	نتیجه گیری.....
۴۵۸.....	آزمایشگاه دوازدهم.....
	فصل هفدهم: روش های ضد ماشین مجازی
۴۶۱.....	مصنوعات VMware.....
۴۶۵.....	دستورالعمل های آسیب پذیری.....
۴۷۲.....	تنظیمات افزایش سرعت.....
۴۷۳.....	گریز از ماشین مجازی.....
۴۷۴.....	نتیجه گیری.....
۴۷۴.....	آزمایشگاه سیزدهم.....
	فصل هجدهم: پکرها و آنپکرها
۴۷۷.....	آناتومی یک بسته بند.....
۴۸۱.....	تشخیص برنامه های بسته بندی شده.....
۴۸۳.....	آنپک خودکار مولفه اجرایی.....
۴۹۲.....	نکاتی در مورد بسته بند های رایج.....
۴۹۶.....	تحلیل بدون آنپک برنامه.....
۴۹۶.....	کتابخانه های پیوندی پویا بسته بندی شده.....
۴۹۷.....	نتیجه گیری.....
۴۹۷.....	آزمایشگاه چهاردهم.....
	بخش ششم: مباحث ویژه
	فصل نوزدهم: تجزیه و تحلیل شلکد
۵۰۱.....	بارگذاری شلکد به منظور تجزیه و تحلیل.....
۵۰۲.....	کد موقعیت مستقل.....
۵۰۳.....	شناسایی موقعیت اجرا.....
۵۰۶.....	استفاده از Fnstenv.....
۵۰۸.....	تفکیک دستی سمبول.....
۵۱۴.....	یک نمونه کامل Hello world.....
۵۱۷.....	رمزگذاری های شلکد.....
۵۱۸.....	NOP های حامل.....
۵۱۹.....	پیدا کردن شلکد.....
۵۲۰.....	نتیجه گیری.....
۵۲۱.....	آزمایشگاه پانزدهم.....

فصل بیستم: تجزیه و تحلیل C++

۵۲۳	برنامه‌نویسی شی‌گرا
۵۲۹	توابع مجازی در برابر توابع غیر مجازی
۵۳۴	ایجاد و نابود کردن اشیاء
۵۳۵	نتیجه‌گیری
۵۳۵	آزمایشگاه پانزدهم

فصل بیست و یکم: بدافزارهای بر پایه معماری x64

۵۳۸	چرا بدافزار ۶۴ بیتی؟
۵۳۸	کد کرنل
۵۳۸	پلاگین‌ها و کدهای تزریق شونده
۵۳۹	شلکد
۵۳۹	تفاوت‌ها در معماری x64
۵۴۵	ویندوز ۳۲ بیتی روی ویندوز ۶۴ بیتی
۵۴۶	امتیازات ۶۴ بیتی در عملکرد هزار
۵۴۶	نتیجه‌گیری
۵۴۷	آزمایشگاه شانزدهم

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرضه کتاب الکترونیکی است که تواند

نواره های بروز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگ این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هر چند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم. گنج‌بردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات بسیار چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، منتخبان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر، برای رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقه‌مندان قرار دهند.

کتابی که در دست دارید با همت "آقایان مهندسین و مهندسان میلاد کهساری الهادی" و تلاش جمعی از همکاران انتشارات میسر گشته که سبب شده است از یکایک این گرامیان تشکر و قدردانی کنیم.

ویراستار: فاطمه پورعبدل - راضیه گودرزی

ویرایش و صفحه‌آرایی کامپیوتری: معصومه گنجی‌پور

کارشناسی و نظارت بر محتوا: زهره قزلباش - راضیه گودرزی

طرح جلد: مریم فرجیان

ناظر چاپ: منصور عزیزی

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

publishing@mftmail.com

مقدمه مؤلفان

امروزه با پیشرفت و توسعه علوم کامپیوتری در کلیه زمینه‌ها، این رشته به عنوان جزء جدا نشدنی از دیگر علوم در آمده است و کاربرد آن هر روز در جامعه بشری بیشتر احساس می‌گردد. همچنین استفاده و به‌کارگیری کامپیوتر در تمامی علوم و رشته‌ها گویای نقش واقعی این پدیده برای زندگی ما است. اما همین‌طور که کامپیوتر راه پیشرفت خود را با قدرت ادامه می‌دهد، خطراتی هم حوزه استفاده کاربران آن را تهدید می‌کند. خطراتی از قبیل هکرها (نفوذگرها)، ویروس‌ها، روتکیت‌ها، جاسوس‌افزارها و سایت‌های بدون هویت و غیره. بنابر همین موضوع بر آن شدیم که قسمت‌هایی از کتاب Practical Malware Analysis که نویسندگان آن Michael Sikorski و Andrew Honig بوده‌اند را به زبان فارسی برگردانده و یک منبع مفید برای علاقه‌مندان به مباحث تجزیه و تحلیل بدافزارها ایجاد کنیم. شایان ذکر است در ترجمه این کتاب فقط متن انگلیسی را به فارسی برگردانده‌ایم، در برخی بخش‌ها توضیحات بیشتر لحاظ کرده یا از جملات و کلمات دیگری برای ارائه مفهوم مورد نظر به شخص خواننده استفاده کرده‌ایم. بتوانیم حداکثر مطالب کتاب را به شخص خواننده منتقل کنیم. با این حال، علاوه بر تمام تلاش‌ها و کوشش‌هایی که در راه ترجمه و تألیف این کتاب به عمل آمده است، مجموعه حاضر خالی از اشکال نمی‌باشد. لذا این تمامی اساتید ارجمند، صاحب‌نظران و دانشجویان محترم استدعا داریم با نظرات و پیشنهادات ارزشمندشان ما را راهنما باشند. امیدواریم به لطف پروردگار، این کتاب مورد توجه جامعه مهندسين امنیت و اطلاعات کشور عزیزمان قرار بگیرد. قابل ذکر است، خوانندگان گرامی می‌توانند به منظور دریافت فایل‌های مرتبط با این کتاب به وبسایت‌ها، به روزرسانی‌ها و اخبار این کتاب به وبسایت <http://myfreetime.ir> رجوع کنند.

رضا مقدم

R.moghadam@hotmail.com

میلاد کهساری الهادی

Rce.milad@hotmail.com