به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

تجزیه و تحلیل بدافزارها

راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها،
جاسوس‌افزارها و رونکت‌های کامپیوتری

مؤلفان
مهندس رضا مقدم
مهندس میلاد کهساری الهادی

تجزیه و تحلیل بدافزارها

راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها، جاسوس‌افزارها و روتکیت‌های کامپیوتری

مؤلفان: مهندس رضا مقدم - مهندس میلاد کهساری الهادی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی: 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

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۳۰-۸

ISBN: 978-600-124-430-8

مقدم، رضا، ۱۳۶۹-
عنوان و نام پدیدآور: تجزیه و تحلیل بدافزارها: راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها، جاسوس‌افزارها و روتکیت‌های کامپیوتری/ مؤلفان رضا مقدم، میلاد کهساری الهادی.
مشخصات نشر: تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۴.
مشخصات ظاهری: ۵۴۸ ص.: مصور.
شابک: 978-600-124-430-8
وضعیت فهرست‌نویسی: فیپا
عنوان دیگر: راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها، جاسوس‌افزارها و روتکیت‌های کامپیوتری.
موضوع: نرم‌افزار بدافزار
موضوع: ویروس‌های کامپیوتری
موضوع: مهندسی معکوس -- نرم‌افزار
شناسه افزوده: کهساری الهادی، میلاد، ۱۳۷۳-
رده‌بندی کنگره: ۱۳۹۴ ۷م۹و/QA۷۶/۷۶
رده‌بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۴۱۷۸۳۱۳

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

صندوق پستی: ۱۴۳۳۵/۹۴۳ وب سایت: **dibagaran.mft.info**

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

تلفن: ۱۲-۲۲۰۸۵۱۱۱ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: **bookmarket@mftmail.com** فروش اینترنتی: **www.mftshop.com**

فهرست مطالب

بخش دوم: تجزیه و تحلیل ایستای پیشرفته

فصل بیستم: تجزیه و تحلیل C++

فصل بیست و یکم: بدافزارهای بر پایه معماری x64

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرضه کتاب هایی است که بتواند خواسته های به روز 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. گسترندگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی 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، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود 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 مهندس رامتین مقدم و مهندس میلاد کهساری الهادی**" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته 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 برنگردانده‌ایم، در برخی بخش‌ها توضیحات بیشتر لحاظ کرده یا از جملات و کلمات دیگری برای ارائه مفهوم مورد نظر به شخص خواننده استفاده کرده‌ایم تا بتوانیم حداکثر مطالب کتاب را به شخص خواننده منتقل کنیم. با این حال، علاوه بر تمام تلاش و کوشش‌هایی که در راه ترجمه و تألیف این کتاب به عمل آمده است، مجموعه حاضر خالی از اشکال نمی‌باشد لذا از تمامی اساتید ارجمند، صاحبنظران و دانشجویان محترم استدعا داریم با نظرات و پیشنهادات خود ما را راهنما باشند. امیدواریم به لطف پروردگار، این کتاب مورد توجه جامعه مهندسین امنیت و اطلاعات کشور عزیزمان قرار بگیرد. قابل ذکر است، خوانندگان گرامی می‌توانند به منظور دریافت فایل‌های مرتبط با این پژوهشگاه‌ها، به روزرسانی‌ها و اخبار این کتاب به وب سایت http://myfreetime.ir رجوع کنند.

رضا مقدم

R.moghadam@hotmail.com

میلاد کهساری الهادی

Rce.milad@hotmail.com