

تحلیل بدافزار با رویکرد کلان داده

تألیف: مهندس زهرا خربه



علوم رایانه

سرشناسه : نفریه، زهرا، ۱۳۶۴ -

عنوان و نام پدیدآور : تحلیل بدافزار با رویکرد کلان داده/ تالیف زهرا نفریه.

مشخصات نشر : بابل: علوم رایانه، ۱۳۹۹.

مشخصات ظاهری : ۶۶ ص.؛ مصور، جدول، نمودار.

شابک : ۹۷۸-۶۰۰-۲۰۵-۱۶۳-۹

وضعیت فهرست‌نویسی : فیبا

یادداشت : کتابنامه: ص. ۶۴ - ۶۶

موضوع : نرم‌افزار بدافزار

موضوع : Malware (Computer software)

موضوع : داده‌های کلان

موضوع : Big Data

رده‌بندی کنگره : QA ۷۶/۷۶

ردف بندی دیوب : ۰۰۵ / ۸

شماره کتابشناسی ملی : ۷۳۰۱۷۰۱

این اثر، مشمول قانون حمایت مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ است، هرکس تمام یا قسمتی از این اثر را بدون اجازه مؤلف (ناشر) نشر یا پخش یا عرضه کند مورد پیگرد قانونی قرار خواهد گرفت.

تلفن : ۳۲۳۶۰۷۷۲ - ۱۱

www.olomrayaneh.net

بابل، صندوق پستی ۴۷۱۳۵-۸۹۱



علوم رایانه

تحلیل بدافزار با رویکرد کلان داده

تألیف : مهندس زهرا نفریه

چاپ اول

تابستان ۱۳۹۹

شمارگان : ۲۰۰ نسخه

قیمت : ۲۵۰۰۰ تومان

چاپ و صحافی: چاپ دیجیتال میلاد بابل

شابک : ۹۷۸-۶۰۰-۲۰۵-۱۶۳-۹

نشانی ناشر: بابل، خیابان شریعتی، مجتمع میلاد، واحد ۱۷

حروفچینی و صفحه‌آرایی : علوم رایانه

تهران، خیابان انقلاب، خیابان منیری جاوید، نیش وحید نظری، شماره ۱۴۲، تلفکس : ۶۶۴۰۰۲۲۰ - ۶۶۴۰۰۱۴۴

فهرست مطالب

فصل ۱: شناسایی حملات اینترنتی

- ۱-۱. امنیت اطلاعات ۹
- ۲-۱. تحلیل ترافیک شبکه برای شناسایی حملات ۱۱

فصل ۲: شناسایی بدافزار

- ۱-۲. بدافزار ۱۲
- ۲-۲. باتنت ۱۳
- ۳-۲. دسته‌بندی بات‌ها براساس معماری C&C ۱۴
- ۴-۲. چرخه حیات باتنت‌ها ۱۹
- ۵-۲. شناسایی باتنت‌ها ۲۴
- ۶-۲. رویکردهای شناسایی باتنت براساس ترافیک شبکه ۲۸
- ۷-۲. ویژگی درخواست‌های ایجاد شده توسط باتنت در DNS ۳۱
- ۸-۲. تکنیک‌های تغییرات پی‌درپی سریع استفاده شده توسط شبکه‌های باتنت ۳۳

فصل ۳: تحلیل بدافزار و استفاده از Splunk

- ۱-۳. مقدمه ۴۱
- ۲-۳. بررسی شاخص‌های مختلف جهت تحلیل ترافیک مشکوک ۴۸

فصل ۴: تجزیه و تحلیل داده‌ها در مقیاس کلان داده

- ۴-۱. مقدمه ۵۱
- ۴-۲. نمونه رخداد DNS ۵۲
- ۴-۳. بررسی دو نمونه رخداد CTI ۵۳
- ۴-۴. شناسایی بات‌نت مبتنی بر امضا ۵۵
- ۴-۵. شناسایی بات‌نت مبتنی بر رفتار ۵۶

فصل ۵: نتیجه‌گیری

- واژه‌نامه انگلیسی به فارسی ۶۲
- منابع و مراجع ۶۴

بسم الله الرحمن الرحيم

بدون شک یکی از پایه‌های توسعه‌ی فرهنگ و رشد و شکوفایی استعدادها، مقوله‌ی کتاب و کتابخوانی است. یکی از معیارهای مورد بررسی در میزان پیشرفت یک جامعه، توجه به کتاب و مطالعه‌ی سرانه است. آنچه که موجب گرایش فرهیختگان به مطالعه‌ی کتاب می‌شود، وجود کتاب‌های باکیفیت و جذاب و نویسندگان ماهر و اندیشمند و توزیع مناسب است.

جهت تحقق این امر و گام برداشتن به سمت خودکفایی، انتشار کتاب‌های دانشگاهی و نتایج پژوهش ممتاز فرهیخته‌ی کشور، در دستور کار انتشارات علوم رایانه قرار گرفته است.

انتشارات علوم رایانه توانسته است با شبکه‌ای از اساتید برجسته‌ی کشور ارتباط برقرار کرده و آثار ارزشمند آن‌ها را منتشر کند. در همین راستا، انتشارات علوم رایانه در بیست و پنجمین و بیست و هفتمین نمایشگاه بین‌المللی کتاب تهران به عنوان ناشر برتر کشور انتخاب شده است.

عین الله جعفر نژاد قمی

انتشارات علوم رایانه