

تشخیص و تحلیل رفتار بدافزارهای مدرن

مؤلف:

دانیال جواهری

(دانشجوی دکتری تخصصی دانشگاه آزاد اسلامی واحد علوم و تحقیقات)



علوم رایانه

سرشناسه	جواهری، دانیال، ۱۳۶۹ -
عنوان و نام پدیدآور	تشخیص و تحلیل رفتار بدافزارهای مدرن / مولف دانیال جواهری.
مشخصات نشر	بابل: علوم رایانه، ۱۳۹۶.
مشخصات ظاهری	۱۳۹ ص.: مصور، جدول.
شابک	۹۷۸-۶۰۰-۲۰۵-۱۲۲-۶
وضعیت فهرست‌نویسی	فیفا
یادداشت	کتابنامه.
موضوع	ویروس‌های کامپیوتر
موضوع	نرم‌افزار بدافزار
موضوع	Malware (Computer software) :
موضوع	Computer viruses :
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	Computer networks -- Security measures :
رده‌بندی کنگره	۱۳۹۶ ج ۸۶ و ۷۶/۷۶ QA
رده‌بندی دیویی	۰۰۵/۸ :
شماره کتابشناسی ملی	۴۸۶۱۲۳۰

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

تلفن: ۰۱۱-۳۲۳۶۰۷۷۲

www.olomrayaneh.net

بابل، صندوق پستی ۸۹۱-۷۱۳۵



علوم رایانه

تشخیص و تحلیل رفتار بدافزارهای مدرن
تألیف: دانیال جواهری (دانشجوی دکتری تخصصی دانشگاه آزاد اسلامی)، واحد علوم و تحقیقات، گروه مهندسی کامپیوتر، تهران، ایران)
چاپ اول
تابستان ۱۳۹۶
شمارگان: ۵۰۰ نسخه
قیمت: ۱۵۰۰۰ تومان
چاپ و صحافی: چاپ دیجیتال میلاد بابل
شابک: ۹۷۸-۶۰۰-۲۰۵-۱۲۲-۶
نشانی: بابل، خیابان شریعتی، مجتمع میلاد، واحد ۱۷
حروفچینی و صفحه‌آرایی: علوم رایانه

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

فهرست مطالب

فصل اول: تهدیدات نوین سایبری

۱-۱. مقدمه	۷
۲-۱. بدافزارهای نوین	۸
۳-۱. ضرورت پژوهش	۹
۴-۱. ضرورت دانش فنی	۹

فصل دوم: پیکره‌ی دد فنی سیستم‌عامل

۱-۲. مقدمه	۱۱
۲-۲. ساختار فایل‌های اجرایی فایل‌های حجیم	۱۱
۳-۲. قلاب‌اندازی	۱۳
۴-۲. دیگر مفاهیم	۱۳
۵-۲. مدخل‌های درایور	۱۷
۶-۲. ارتفاع درایور	۱۸
۷-۲. اولویت‌گره	۱۸
۸-۲. پکت درخواست ورودی/خروجی	۱۹
۹-۲. گذر از فضای کاربر به هسته	۲۰
۱۰-۲. فرآیندهای سبک‌وزن	۲۰
۱۱-۲. سرویس‌های سیستم‌عامل	۲۰
۱۲-۲. انواع درایورها	۲۱
۱۳-۲. انواع درایور از حیث مدیریت سخت‌افزار	۲۲
۱۴-۲. حالت تست سیستم‌عامل	۲۲
۱۵-۲. حالت اشکال‌زدایی سیستم‌عامل	۲۳
۱۶-۲. نتیجه	۲۳

فصل سوم: رصد و رهگیری رفتار برنامه‌ها

۱-۳. مقدمه	۲۴
۲-۳. قلاب‌اندازی با تزریق کتابخانه	۲۵
۳-۳. قلاب‌اندازی به جداول توصیف‌گر سرویس‌های سیستم	۲۵
۴-۳. فیلتر درایورها	۲۸
۵-۳. قلاب‌اندازی به جدول توصیف‌گر وقفه‌های سیستم	۲۸
۶-۳. دقت و سرعت تحلیل	۳۱
۷-۳. چالش‌های رهگیری	۳۱

۳۲	۳-۸. مقایسه‌ی روش‌های رهگیری
۳۳	۳-۹. رهگیری تعاملات با منابع سیستم عامل
۳۳	۳-۱۰. رهگیری رجیستری
۳۴	۳-۱۱. رهگیری فایل سیستم
۳۵	۳-۱۲. رهگیری شبکه
۴۰	۳-۱۳. ابزارهای رصدگر
۴۸	۳-۱۴. مهندسی مجدد

فصل چهارم: تشخیص بدافزارها با تحلیل رفتار ایستا

۷۱	۴-۱. مقدمه
۷۱	۴-۲. بدافزار
۷۵	۴-۳. معرفی روش‌های تشخیص بدافزار
۷۸	۴-۴. معرفی محاسبات‌های تحلیل‌گر
۸۰	۴-۵. انواع خانواده‌ی بدافزارها
۹۵	۴-۶. تحلیل رفتار ایستا برای کشف بدافزارها و بیشینه‌ی آن
۹۷	۴-۷. خواص روش پیشنهادی
۱۰۴	۴-۸. میزان بدخیمی
۱۰۴	۴-۹. ابزارهای تحلیل رفتار ایستا
۱۰۶	۴-۱۰. نتیجه‌گیری

فصل پنجم: دفاع از خود و مقابله با بدافزار

۱۰۸	۵-۱. ایمن‌سازی
۱۰۸	۵-۲. دفاع از منابع حساس
۱۱۱	۵-۳. مقابله با بدافزارها
۱۲۰	۵-۴. جرم‌یابی دیجیتال
۱۲۱	۵-۵. تله‌عسل

فصل ششم: داده‌کاوی و سنجش روش‌های تشخیص بدافزار

۱۲۳	۶-۱. مقدمه
۱۲۳	۶-۲. داده‌کاوی
۱۲۷	۶-۳. نرم‌افزار وکا
۱۲۹	۶-۴. ارزیابی دقت روش تحلیل رفتار ایستا و کیفیت خوشه‌بندی آن
۱۳۰	۶-۵. نتیجه‌گیری
۱۳۱	پیوست ۱: نرم‌افزارهای مورد نیاز
۱۳۲	پیوست ۲: طرح‌های در دست اقدام
۱۳۶	منابع و مآخذ

پیش گفتار

رشد سریع فناوری اطلاعات و فراگیری آن در ابعاد مختلف زندگی شخصی و تعاملات روزمره‌ی اداری در کنار فواید و مزایای بسیار، مخاطرات و تهدیدات متعددی را نیز به همراه دارد. این روند رو به رشد سبب شده دارایی‌ها و اطلاعات اشخاص و سازمان‌ها به صورت داده‌های دیجیتالی ذخیره و انباشته شوند. لذا حفاظت از این دارایی‌های ارزشمند امری غیرقابل اجتناب است.

برحسب آمارهای منتشر شده از شرکت‌های معتبر امنیتی در جهان هم اکنون، روزانه بیش از ۲۵ هزار حمله سایبری در حال رخداد است و همچنین در هر ثانیه بیش از ۴ بدافزار در حال تولید و انتشار است. علاوه بر این، حملات سایبری روز به روز در حال پیچیده‌تر شدن هستند به گونه‌ای که امروز حملات مانای پیشرفته (APT) با هدف عملکرد مخفی و ماندگاری بالا مطرح شده‌اند. عملکرد بدافزارها نیز به سمت هوشمند شدن و رفتارهای مبهم و فریبنده سازمان‌دهی شده است. بدافزار استاکس‌نت (Stuxnet) در گذشته با هدف تخریب صنعتی و جاسوس‌افزارهای دینو (Dino) و گریت (Grabit) با هدف سرقت اطلاعات نمونه‌های واقعی از تهدیدات نوین در حوزه‌ی فناوری اطلاعات بوده‌اند.

پر واضح است که منشأ بسیاری از این تهدیدات، وجود آسیب‌پذیری‌هایی است که در اثر عدم آموزش کافی، پیکربندی نامناسب تجهیزات، اختلالات و نرم‌افزاری، عدم به‌روزرسانی و به‌کارگیری تجهیزات امنیتی به وجود آمده‌اند. با علم به موارد ذکر شده و همچنین تأکید مکرر و مداوم اسناد بالادستی سازمان‌ها و نهادها مطبوع مبنی بر آشنایی، همکاری ارتباطی و اطلاعاتی، نویسنده با هدف برطرف نمودن خلأهای آموزشی موجود و نشر دانش تخصصی حاصل از چند سال تحقیق و پژوهش دانشگاهی در خصوص تحلیل رفتار بدافزارهای نوین و مقابله با آنها این اثر بومی را تألیف نموده است.

با تشکر و آرزوی توفیق روزافزون

تابستان ۹۶- دانیال جواهری