تشخیص و تحلیل رفتار بدافزارهای مدرن

مؤلف:

دانیال جوانمردی

(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	: فیپا
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 ۸۶ ج ۹ و QA ۷۶/۷۶
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۴۸۶۱۲۳

علوم رایانه

www.olomrayaneh.net

بابل، صندوق پستی ۸۹۱-۷۱۳۵

تلفن : ۳۲۳۶۰۷۷۲ – ۰۱۱

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

بسمه تعالی

پیش‌گفتار

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 آمری غیرقابل اجتناب است.

برحسب آمارهای منتشر شده از شرکت‌های معتبر امنیتی در جهان هم اکنون، روزانه بیش از ۲۵ هزار حمله‌ی سایبری در حال رخداد است و همچنین در هر ثانیه بیش از ۴ بدافزار در حال تولید و انتشار است. علاوه‌بر این روند افزایشی، حملات سایبری روز به روز در حال پیچیده‌تر شدن هستند به گونه‌ای که امروزه 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 اِستاکس‌نِت (Stuxnet) در گذشته با هدف تخریب صنعتی و جاسوس‌افزارهای دینو (Dino) و گِرَبیت (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 سخت‌افزاری 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 آمن‌سازی سامانه‌های ارتباطی و اطلاعاتی، نویسنده با هدف برطرف نمودن خلاءهای آموزشی موجود و نَشر دانش 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