به‌نام خداوند جان و خرد

بدافزارها و راه‌کارهای مقابله

(Virus, Worm, Trojan horse, Spyware, ….)

انتشارات پندار پارس

تألیف: مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

شابک : 978-600-6529-68-4: ۱۸۰۰۰۰ ریال
شماره کتابشناسی ملی : ۳۷۰۰۲۲۴
عنوان و نام پدیدآور : بدافزارها و راه‌کارهای مقابله (Worm, Trojan, Spyware, Virus, ...)/ تالیف مجید داوری دولت‌آبادی.
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۳.
مشخصات ظاهری : ۲۵۲ ص.: مصور.
موضوع : ویروس‌های کامپیوتر
موضوع : جرایم کامپیوتری
رده بندی دیویی : ۰۰۵/۸۴
رده بندی کنگره : ۱۳۹۳۷۶/۷۶QA ۲د۹و/
سرشناسه : داوری دولت‌آبادی، مجید، ۱۳۵۹ -
وضعیت فهرست نویسی : فیپا

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱٤، واحد ۱٦ www.pendarepars.com

تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨ همراه: ۰۹۲۱٤۳۷۱۹٦٤ info@pendarepars.com

نام کتاب	:	بدافزارها و راه‌کارهای مقابله
ناشر	:	انتشارات پندار پارس
ترجمه و تالیف	:	مجید داوری دولت آبادی
چاپ نخست	:	دی‌ماه ۹۳
شمارگان	:	۵۰۰ نسخه
طرح جلد	:	رامین شکرالهی
چاپ و صحافی	:	روز
قیمت	:	۱۸۰۰۰ تومان شابک : ٤-٦٨-٦٥٢٩-٦٠٠-٩٧٨

فهرست

سخنی با خوانندگان

امروزه در دنیای فناوری‌اطلاعات و کامپیوتر، حفظ و نگهداری اطلاعات به‌صورت سالم و مقوله امنیت اطلاعات از جایگاه ویژه‌ای برخوردار است که باید همواره در پایداری و استحکام آن کوشید. هم‌اینک وجود کدهای مُخرب و در اصطلاح بدافزارها تهدیدی جدی برای اطلاعات سازمان‌ها و کاربران به‌شمار می‌آیند که هر دم ممکن است صدمات جبران‌ناپذیری به منابع مالی و اطلاعاتی سازمان و یا کاربران وارد کنند. از بین رفتن اطلاعات و فایل‌های معتبر یک سازمان در واقع با درهم شکسته شدن آن سازمان در دنیای رقابت و کار برابری می‌کند که این امر در بیشتر مواقع توسط کدهای مُخرب و بدافزارهای تولید و منتشر شده در سطح اینترنت و شبکه‌های کامپیوتری صورت می‌گیرد. این روزها، محیط شبکه‌های کامپیوتری و اینترنت بستر مناسب و خوبی برای فعالیت و جولان بدافزارهای گوناگون به‌شمار می‌رود که باید هر متخصص و کارشناس فناوری اطلاعات با انواع آنها و روال‌ها و ساختارهای آنها و همچنین روش مقابله با آنها آشنایی کامل داشته باشد.

هدف از تألیف این کتاب آشنایی بیشتر کارشناسان و متخصصان با نحوه عملکرد و نوشتن نرم‌افزارها و کدهای مُخرب می‌باشد. با کمک این کتاب می‌توان آشنایی بیشتری در مورد ساختار انواع کدهای مُخرب به‌دست آورد. این آشنایی می‌تواند تا نوشتن یک کدمُخرب ادامه داشته باشد. الگوهای کدهای مُخرب در این کتاب به‌طور کامل بررسی خواهد شد. یک کارشناس و متخصص امنیت بایستی با ساختار و الگوهای مخصوص کدهای مُخرب آشنایی بیشتری داشته باشد تا در زمان انتشار یک کد مُخرب در سطح شبکه، اولا بتواند نوع و ساختار را شناسایی و تشریح کند و در ادامه بتواند برای برخورد با آن راه‌کارهایی ارائه نماید. محافظت از انواع کدهای مُخرب نیز باید در تمامی شبکه‌ها و سیستم‌ها مدنظر قرار گیرد. نحوه انجام این‌کار در این کتاب ارائه شده است. این کتاب تلاش می‌کند مخاطب را ابتدا با الگوهای انواع کدهای مُخرب آشنا کند و سپس به ارائه راه‌کارهایی برای محافظت از سیستم‌ها و شبکه‌ها درمقابل این‌گونه کدها بپردازد. کتاب تلاش دارد تا حد امکان تکنولوژی‌های نوین را در مورد انواع کدهای مُخرب معرفی نماید.

اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به‌منظور افزایش آگاهی متخصصان، دانشجویان و مدیران شبکه در زمینه ساختار و عملکرد بدافزارها و نرم‌افزارهای ضدویروس بودم تا آنها را با اصول فنی کدهای مُخرب آشنا و آگاه سازم تا بتوان از آن در طراحی و پیاده‌سازی بدافزارها و نرم‌افزارهای ضدویروس استفاده نمود (گرچه مدیران و متخصصان امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه برخود لازم دانستم که این آگاه‌سازی را انجام دهم.)

شیرازه اصلی کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه امنیت داده، بدافزارها، کدنویسی بدافزارها و نرم‌افزارهای ضدویروس و بررسی انواع کدهای مُخرب می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملا آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آنها را به دیده منت پذیرا هستم.

(m_Davari@TOP-co.ir)
(m_Davary@Parshack.zzn.com)

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، سپاسگزاری می‌کنم. برخود لازم می دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونهٔ مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانهٔ ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانه انتشارات پندار پارس جناب آقای مهندس یعسوبی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یا رب چو به وحدتت یقین می‌دارم

ایمان به تو عالم آفرین می‌دارم

دارم لب خشک و دیده‌ی‌تر بپذیر

کز خشک و تر جهان همین می‌دارم

(مجید داوری دولت آبادی – پاییز ۱۳۹۳)