

به نام خداوند جان و خرد

بدافزارها و راه کارهای مقابله

(Virus, Worm, Trojan horse, Spyware,)

www.ketab.ir

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	: ۲۷۰۰۲۲۴
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	: ۱۳۹۳۷۶/۷۶۴۸ : ۹۵۳/و
سرشناسه	: داوری دولت‌آبادی، مجید، ۱۳۵۹ -
وضعیت فهرست نویسی	: قیفا

انتشارات پندار پارس



www.pendarepars.com

info@pendarepars.com

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶
تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴

نام کتاب	: بدافزارها و راهکارهای مقابله
ناشر	: انتشارات پندار پارس
ترجمه و تالیف	: مجید داوری دولت‌آبادی
چاپ نخست	: دی‌ماه ۹۳
شمارگان	: ۵۰۰ نسخه
طرح جلد	: رامین شکرآلهی
چاپ و صحافی	: روز

شابک : ۹۷۸-۶۰۰-۶۵۲۹-۶۸-۴

: ۱۸۰۰۰ تومان

قیمت

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد.

فهرست

۳	فصل نخست: معرفی انواع بدافزارها.....
۴	۱-۱ مفهوم بدافزار.....
۶	۱-۲ چرخه حیات بدافزار.....
۸	۱-۳ ویروس چیست؟.....
۱۲	۱-۴ انواع کونکون ویروس ها.....
۲۳	۱-۵ کرم های اینترنتی.....
۲۶	۱-۶ اسب های تروا (تروجان).....
۲۷	۱-۷ انواع اسب های تروا.....
۲۸	۱. اسب های تروای ایجاد کننده درپشتی.....
۲۹	۲. اسب های تروای عمومی.....
۲۹	۳. اسب های تروای ارسال کننده رمز.....
۳۰	۴. اسب های تروای ویرانگر.....
۳۰	۵. Trojan Clickers.....
۳۰	۶. Trojan Downloaders.....
۳۱	۷. Trojan Droppers.....
۳۱	۸. Denial of Service (DoS) Attack Trojans.....
۳۲	۹. اسب های تروای سرور پراکسی.....
۳۲	۱۰. اسب های تروای جاسوس.....
۳۳	۱۱. اسب تروای مخصوص پروتکل FTP.....
۳۳	۱۲. اسب های تروای اخطار دهنده.....
۳۳	۱۳. Security Software Disablers Trojans.....
۳۳	۱۴. اسب تروای ArcBombs.....
۳۴	۱۵. اسب های تروای ثبت کننده کلید.....
۳۴	۱۶. اسب های تروای حمله ائتلاف منابع.....
۳۴	۱۷. اسب تروای BO2K.....
۳۵	۱-۸ جاسوس افزارها.....
۳۶	۱-۹ انواع نرم افزارهای جاسوسی.....
۳۸	۱-۱۰ تبلیغ افزارها.....
۳۹	۱-۱۱ Honeypot.....
۴۰	۱-۱۲ Trapdoors.....
۴۰	۱-۱۳ درهای پشتی.....
۴۰	۱-۱۴ انواع درپشتی.....
۴۱	۱-۱۵ پاکتری ها.....
۴۲	۱-۱۶ زامبی.....
۴۲	۱-۱۷ Botnet ها.....
۴۵	۱-۱۸ باج افزارها یا زور گیرها.....
۴۵	۱-۱۹ ترس افزار.....
۴۶	۱-۲۰ Rootkit ها.....
۴۸	۱-۲۱ قابلیت های کلی Rootkit ها در انواع مختلف.....
۵۱	۱-۲۲ SPAM.....

۵۱	۱-۲۳ بمب‌های منطقی.....
۵۲	Joke ۱-۲۴.....
۵۲	Wild ۱-۲۵.....
۵۲	Zoo ۱-۲۶.....
۵۳	Dialer ۱-۲۷ شماره‌گیرها یا.....
۵۳	Downloader ۱-۲۸ بارگیرها یا.....
۵۳	Adclicker ۱-۲۹ کلیک‌کننده‌ها یا.....
۵۳	Password-Stealer ۱-۳۰ گذرواژه‌دزد یا.....
۵۳	Keylogger ۱-۳۱ کلیدنگارها یا.....
۵۴	Black Code ۱-۳۲.....
۵۴	Exploit ۱-۳۳.....
۵۵	Exploit ها ۱-۳۴ انواع.....
۵۵	Shell Code ۱-۳۵.....
۵۶	۱-۳۶ بدافزارهای ترکیبی.....
۵۶	۱-۳۷ ابزارهای نفوذ.....
۵۷	۱-۳۸ مواردی که بدافزار نیستند.....
۶۰	۱-۳۹ آینده بدافزارها.....
۶۱	فصل دوم؛ ساختار و کارکرد بدافزارها
۶۲	۲-۱ علائم و نشانه‌های وجود بدافزار.....
۶۳	۲-۲ منظور از امضای ویروس.....
۶۳	۲-۳ عدم شناسایی امضای ویروس در مقابل ضدویروس.....
۶۴	۲-۴ خطاهای مبتنی بر ویروس‌ها.....
۶۴	۲-۵ تأثیرات بدافزارهای متصل به نامه‌های الکترونیکی.....
۶۵	۲-۶ راه‌حل برخورد با بدافزارهای متصل به نامه‌های الکترونیکی.....
۶۶	۲-۷ کارکرد ویروس‌ها.....
۶۸	۲-۸ کارکرد کرم‌های اینترنتی.....
۶۹	۲-۸-۱ مراحل حیات یک کرم اینترنتی.....
۶۹	۲-۸-۲ طرح هدف‌یابی.....
۷۰	۲-۸-۲-۱ پوشش کورکورانه.....
۷۰	۲-۸-۲-۲ پوشش غیرفعال.....
۷۰	۲-۸-۲-۳ پوشش فهرست هدف.....
۷۱	۲-۸-۲-۴ پوشش مسیر یاب.....
۷۲	۲-۸-۲-۵ پوشش توپولوژیک.....
۷۲	۲-۸-۲-۶ پوشش تقسیم و غلبه.....
۷۳	۲-۸-۲-۷ ارزیابی و بحث.....
۷۴	۲-۸-۲-۸ مخفی‌کاری و سرعت.....
۷۴	۲-۸-۳ طرح انتقال.....
۷۵	۲-۸-۴ طرح پروتکل انتشار.....
۷۶	۲-۸-۵ روش‌های ضدتشخیص.....
۷۶	۲-۸-۵-۱ فرمت کدهای بدنه کرم.....
۷۷	۲-۸-۵-۲ کد سوءاستفاده چندریختی.....
۷۸	۲-۹ محل استقرار بدافزارها.....
۷۸	۲-۱۰ محل فعالیت بدافزارها.....
۷۹	۲-۱۱ تقسیم‌بندی ویروس‌ها براساس جایگاه تأثیرگذاری.....

۸۰	۲-۱۲ تقسیم‌بندی پایه‌ای ویروس‌ها براساس نوع عملکرد
۸۳	۲-۱۳ روش‌های نوین برای انتشار بدافزارها
۸۴	۲-۱۴ عملگرهای استاندارد اسپ‌های تروا
۸۴	۲-۱۵ کارکرد اسپ‌های تروا
۸۸	۲-۱۶ پیاده‌سازی Rootkit‌های سطح هسته
۸۸	۲-۱۷ انواع و اهداف نرم‌افزارهای جاسوسی مختلف
۹۰	۲-۱۸ تجزیه و تحلیل بدافزارها
۹۲	۲-۱۸-۱ ابزارهای متمرکز بر سیستم
۹۳	۲-۱۸-۲ تجزیه و تحلیل نرم‌افزاری
۹۴	۲-۱۹ مهندسی معکوس یک بدافزار
۹۵	۲-۱۹-۱ تجزیه و تحلیل رفتاری
۹۷	۲-۱۹-۲ تجزیه و تحلیل کد
۹۸	۲-۲۰ کارکرد Botnet در شبکه
۹۹	۲-۲۱ ویژگی‌های کلی بدافزارها
۱۰۶	۲-۲۲ مبهم‌سازی بدافزارها
۱۰۷	۲-۲۲-۱ دسته‌بندی بدافزارها
۱۰۷	۲-۲۲-۱-۱ بدافزارهای رمز شده
۱۰۷	۲-۲۲-۱-۲ بدافزارهای چندریخت
۱۰۸	۲-۲۲-۱-۳ بدافزارهای دگر دس
۱۰۹	۲-۲۲-۲ مبهم‌سازی بدافزارها
۱۰۹	۲-۲۲-۳ انواع روش‌های مبهم‌سازی بدافزارها
۱۰۹	۲-۲۲-۳-۱ افزودن کد مرده
۱۱۱	۲-۲۲-۳-۲ تغییر نام ثبات‌ها
۱۱۲	۲-۲۲-۳-۳ جابه‌جایی زیرروال‌ها
۱۱۲	۲-۲۲-۳-۴ جایگزینی دستورات معادل
۱۱۲	۲-۲۲-۳-۵ به هم ریختن کد
۱۱۴	۲-۲۲-۳-۶ یکپارچه‌سازی کد
۱۱۴	۲-۲۲-۳-۷ بسته‌بندی کد
۱۱۴	۲-۲۳ نرمال‌سازی بدافزارها
۱۱۵	۲-۲۳-۱ نرمال‌سازی بدافزارها
۱۱۶	۲-۲۳-۱-۱ نرمال‌سازی به هم ریختن کد
۱۱۹	۲-۲۳-۱-۲ نرمال‌سازی درج کدهای مرده
۱۱۹	۲-۲۳-۱-۳ نرمال‌سازی برنامه‌های خود تولید
۱۲۵	فصل سوم؛ نحوه نوشتن انواع بدافزارها
۱۲۵	۳-۱ زبان‌های برنامه‌نویسی بدافزارها
۱۲۶	۳-۲ نحوه بدافزارنویسی و بررسی ساختار آن
۱۲۸	۳-۳ بررسی کد منبع یک ویروس از نوع ماکرو
۱۳۰	۳-۴ ویروس‌سازی با برنامه‌های آماده
۱۳۰	۳-۵ مفاهیم کلی بدافزارنویسی
۱۳۳	۳-۶ بررسی ابزار AutoIT
۱۳۶	۳-۷ بدافزارنویسی با استفاده از دستورات خطرمان
۱۴۲	۳-۸ کدنویسی Keylogger
۱۵۴	۳-۹ آشنایی با ویروس‌های vbs و طریقه مقابله با آنها
۱۵۹	۳-۱۰ استفاده از رجیستری در بدافزارنویسی

۱۶۵	۳-۱۱ نمونه‌ای از کدهای بدافزار
۱۷۶	۳-۱۲ استفاده از ابزارهای گوناگون برای آزمایش کدهای مخرب بر علیه سیستم‌ها
۱۸۳	فصل چهارم؛ محافظت و امن‌سازی سیستم‌ها در برابر بدافزارها
۱۸۳	۴-۱ نرم‌افزارهای ضدویروس و ضدبدافزار
۱۸۵	۴-۲ ابزارهای همانند ضدویروس‌ها
۱۸۵	۴-۳ نسل آغازین ضدویروس‌ها
۱۸۶	۴-۴ ویژگی‌های یک نرم‌افزار ضدویروس مناسب
۱۸۶	۴-۵ نرم‌افزارهای ضدویروس، چه کاری می‌کنند؟
۱۸۷	۴-۶ آگاهی از آخرین اخبار و اطلاعات مربوط به ویروس‌ها
۱۸۸	۴-۷ قابلیت‌های نرم‌افزارهای ضدویروس یا ضدبدافزار
۱۸۹	۴-۸ کارکرد و طرز کار برنامه‌های ضدویروس
۱۹۰	۴-۹ روش‌های شناسایی بدافزارها توسط ضدویروس‌ها
۱۹۵	۴-۱۰ زمان شناسایی بدافزارها توسط ضدویروس‌ها
۱۹۵	۴-۱۱ منظور از پوششگرها، Checksummerها و نرم‌افزارهای کاشف
۱۹۶	۴-۱۲ توانایی‌های متداول ضدویروس‌ها
۱۹۷	۴-۱۳ معیارهای انتخاب یک ضدویروس
۱۹۹	۴-۱۴ لایه‌های برقراری امنیت
۲۰۰	۴-۱۵ مراحل محافظت توسط ضدویروس تحت کلاینت
۲۰۰	۴-۱۶ لایه‌های دفاع در شبکه (Network Defense layer)
۲۰۰	۴-۱۷ طراحی و پیاده‌سازی سیستم ضدویروس
۲۰۱	۴-۱۷-۱ قابلیت‌های موجود در یک ضدویروس برای پیاده‌سازی
۲۰۱	۴-۱۷-۲ توانایی‌های زبان‌های برنامه‌نویسی برای ساخت ضدویروس
۲۰۱	۴-۱۷-۲-۱ زبان‌های C، C++ و VC++
۲۰۲	۴-۱۷-۲-۲ زبان‌های .NET Framework
۲۰۲	۴-۱۷-۲-۳ زبان VB کلاسیک (VB 6)
۲۰۲	۴-۱۷-۲-۴ دیگر زبان‌ها (جاوا، پاسکال، Python و غیره)
۲۰۲	۴-۱۷-۳ نحوه تشخیص ویروس
۲۰۳	۴-۱۷-۳-۱ کشف امضای ویروس
۲۰۳	۴-۱۷-۳-۲ الگوریتم استخراج امضای ویروس
۲۰۳	۴-۱۷-۳-۳ الگوریتم CRC32 در VB
۲۰۵	۴-۱۷-۴ پایگاه‌داده ضدویروس
۲۰۵	۴-۱۷-۵ ساختار فایل پایگاه‌داده
۲۰۶	۴-۱۷-۶ طرز کار ویرایشگر پایگاه‌داده
۲۰۶	۴-۱۷-۷ خواندن رکوردها از پایگاه‌داده
۲۰۷	۴-۱۷-۸ افزودن یک امضای جدید
۲۰۸	۴-۱۷-۹ حذف یک امضا از پایگاه‌داده
۲۰۸	۴-۱۷-۱۰ نوشتن پایگاه‌داده در فایل
۲۰۹	۴-۱۷-۱۱ منابع و کد منبع مورد استفاده در ویرایشگر پایگاه‌داده امضای ویروس
۲۰۹	۴-۱۷-۱۲ پوششگر ساده برای کشف ویروس
۲۰۹	۴-۱۷-۱۳ الگوریتم پوشش ویروس
۲۱۰	۴-۱۸ پیاده‌سازی نمونه نرم‌افزار بازسازی تخریب‌های بدافزارها
۲۱۷	۴-۱۹ خنثی‌سازی کارکرد Keyloggerها
۲۱۹	۴-۲۰ تشخیص Rootkit
۲۲۰	۴-۲۱ پیشگیری از آلودگی Rootkit‌های سطح هسته

۲۲۲	۴-۲۲ استفاده از لیست سفید برای مقابله با بدافزارها
۲۲۳	۴-۲۳ تحلیل گره‌های بدافزارها
۲۲۴	۴-۲۳-۱ مفهوم Sandbox یا جعبه شن
۲۲۴	۴-۲۳-۲ انواع Sandbox یا جعبه شن
۲۲۴	۴-۲۳-۲-۱ جعبه‌های شن مبتنی بر وب
۲۲۵	۴-۲۳-۲-۲ جعبه‌های شن مبتنی بر میزبان
۲۲۵	۴-۲۳-۳ انواع محصولات موجود
۲۲۵	۴-۲۳-۳-۱ ThreatTrack ابزار
۲۲۵	۴-۲۳-۳-۲ GFI Sandbox ابزار
۲۲۶	۴-۲۳-۳-۳ CWSandbox ابزار
۲۲۸	۴-۲۳-۳-۴ ThreatExpert ابزار
۲۲۸	۴-۲۳-۳-۵ Xandora ابزار
۲۲۹	۴-۲۳-۳-۶ Anubis ابزار
۲۳۰	۴-۲۳-۳-۷ Malbox ابزار
۲۳۰	۴-۲۳-۳-۸ Cuckoo Sandbox ابزار
۲۳۱	۴-۲۳-۳-۹ Sandboxie ابزار
۲۳۱	۴-۲۳-۳-۱۰ Buster Sandbox Analyzer ابزار
۲۳۳	۴-۲۳-۳-۱۱ BitBlaze ابزار
۲۳۳	۴-۲۳-۳-۱۲ Zero Wine ابزار
۲۳۴	۴-۲۳-۳-۱۳ Joe Sandbox ابزار
۲۳۵	۴-۲۳-۳-۱۴ Malwr ابزار
۲۳۶	۴-۲۴ بهره‌گیری از Honeypot ها در شناسایی و کشف کدهای مخرب
۲۳۷	۴-۲۵ محافظت از فایل‌ها و پوشه‌های شخصی
۲۳۷	۴-۲۶ پیشگیری از بدافزارها
۲۳۸	۴-۲۷ روش‌های ایجاد امنیت در کار با کامپیوتر
۲۳۹	۴-۲۸ مقابله با Botnet ها

www.ir

سخنی با خوانندگان

امروزه در دنیای فناوری اطلاعات و کامپیوتر، حفظ و نگهداری اطلاعات به صورت 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 خدمات 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 کد مُخرب 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، اولاً 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 این کار 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 در مقابل این گونه 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 در صدد 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 حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخورد 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 کاملاً 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 می کنم. برخورد لازم می دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرهانه انتشارات پندار پارس جناب آقای مهندس یعسوبی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده اند، صمیمانه قدردانی می نمایم.

یا رب چو به وحدت یقین می دارم

ایمان به تو عالم آفرین می دارم

دارم لب خشک و دیده ی تر بپذیر

کز خشک و تر جهان همین می دارم

(مجید داوری دولت آبادی - پاییز ۱۳۹۳)