آشکارسازی هک، بدافزارها و روت‌کیت‌ها

(رازهای امنیتی و روش‌های مقابله با بدافزارها و روت‌کیت‌ها)

نویسنده:
مایکل آ.دیویس
سین م. بودمر
آرون لمسترز

مترجم:
علی نایب‌پور

نگارستان اندیشه
تهران، ۱۳۹٤

سرشناسه: اسکمبری، جوئل Scambray, Joel
عنوان و نام پدیدآور: آشکارسازی هک، بدافزارها و روت‌کیت‌ها (رازهای امنیتی و روش‌های مقابله با بدافزارها و روت‌کیت‌ها) / نویسنده مایکل آ.دیویس، سین م. بودمر، آرون لمسترز؛ مترجم علی نایب‌پور.
مشخصات نشر: تهران: نگارستان اندیشه ،۱۳۹۴.
مشخصات ظاهری: ۵۳۲ ص. مصور
شابک: ۲۵۰۰۰۰ریال 978-600-93744-1-0
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: Hacking exposed: network security secrets & solutions, ©2001.
یادداشت: کتاب حاضر در توسط انتشارات طاهریان با عنوان «آموزش گام به گام هک و ضد هک» در سال ۱۳۸۹ ترجمه و منتشر شده است.
موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی. تأمین خسارت. حفاظت اطلاعات.
شناسه افزوده: مکلور، استوارت. McClure, Stuart. کورتس، جورج، نویسنده همکار. Kurtz, George
شناسه افزوده: نایب‌پور، علی، ۱۳۶۵ –
رده‌بندی کنگره: ۱۳۹۴ ۸آ۷م/ TK۵۱۰۵/۵۹ رده‌بندی دیویی: ۰۰۵/۸ شماره کتابشناسی ملی: ۳۹۹۴۵۰۲

آشکارسازی هک، بدافزارها و روت‌کیت‌ها

رازهای امنیتی و روش‌های مقابله با بدافزارها و روت‌کیت‌ها

نویسنده: مایکل آ.دیویس ـ سین م. بودمر ـ آرون لمسترز
مترجم: علی نایب‌پور
ناشر: نگارستان اندیشه
چاپ و صحافی: نسیم
طراح جلد: سعید صحابی
حروفچینی و صفحه‌آرایی: مرتضی انصاف‌منش
ویرایش و نمونه‌خوانی: وحید دریابیگی
نوبت چاپ: نخست، ۱۳۹۴
شمارگان: ۱۰۰۰ نسخه
قیمت: ۲۵۰۰۰ تومان

نشانی ناشر: م. انقلاب اسلامی، ابتدای خ آزادی، خ استاد بهزاد، پلاک ۲۹، واحد۷
تلفن: ۶۶۴۳۵۴۲۳ ـ نمابر: ۶۶۹۴۳۵۴۲

فهرست مطالب

تحلیل‌های مختلف در مورد کتاب *آشکارسازی هک، بدافزار و ردگم‌کن‌ها* «روت کیت»

«برایان کربس[1]» خبرنگار مرکز روزنامه واشنگتن پُست و نویسنده وب‌سایت امنیت پابرجا[2] معتقد است که: «این کتاب به صورت روان و قابل فهم، همراه با مثال‌های مشهودی است که این موضوع موجب ماندگاری این کتاب به عنوان پرفروش‌ترین ابزار کمکی در حوزه امنیتی شده است. مدیرهای سیستم و کاربرهای کامپیوتر نیاز دارند تا بتوانند به‌طور پنهانی و با مهارت بالا با بدافزارهای جدید مقابله کنند، که این کتاب تمام نکات را برای این منظور توضیح داده است».

«دان کامینسکی[3]» مدیر بخش آزمون نفوذ مهاجم‌ها در شرکت IOActive معتقد است که: «این کتاب راهنمای کاملی است که چگونگی پنهان‌شدن افراد بد(هکرها)، و نحوه شناسایی آن‌ها را نشان می‌دهد».

«کریستوفر جوردان[4]» محقق اصلی تیم تحقیقاتی بات‌نت‌ها و انواع تهدیدها در شرکت مک‌آفی معتقد است: «نویسنده‌های این کتاب موضوع مقابله با بدافزار، که مسئله مهم و حیاتی در امنیت کامپیوتر می‌باشد را با استفاده از اصطلاحات و عبارت‌های معمول و مثال‌های مناسب بیان کرده‌اند. بدافزار به عنوان ابزار مورد استفاده در هک سیستم‌ها است که نویسنده‌های نشانه‌ها و قابلیت‌های آن‌ها را با دید فنی بالایی توضیح داده‌اند. مطالب کتاب حتی برای خواننده‌های حرفه‌ای در این زمینه نیز بسیار مفید است و اطلاعات آن‌ها را کامل می‌کند».

«ران دوج[5]» عضو ارشد ارتش ایالات‌متحده آمریکا معتقد است که: «به یاد داشته

1. Brian Krebs
2. Security Fix
3. Dan Kaminsky
4. Christopher Jordan
5. Ron Dodge

باشید که پس از اتمام هر فصل، مطالب خوانده شده را به سرعت مرور کنید تا با تمام جزئیات به‌طور کامل آشنا شوید، با این کار تمام نکات کلیدی را به راحتی درک می‌کنید، البته در انتهای کتاب منابع مفیدی نیز معرفی شده‌اند که برای عمیق‌تر شدن مطالب هر قسمت می‌توانید به آن‌ها مراجعه نمایید. کتاب چاآشکارسازی هک، بدافزار و روت‌کیت‌ها(ردگم‌کن‌ها) یکی از آن منابع است! این کتاب مرجع مناسبی برای افراد تازه کار، حرفه‌ای و متخصص در زمینه امنیت است، که تمام عناوین و مطالب مورد نیاز با جزئیات کامل در آن ارائه شده است، اما توضیحات بیان شده چندان زیاد و طولانی نیست که افراد تازه کار را از یادگیری منصرف کند».

«مت کانوور[1]» مهندس ارشد نرم‌افزار در آزمایشگاه تحقیقاتی شرکت سیمانتک بر این باور است که: «این کتاب چگونگی شناسایی و حذف بدافزارها و روت‌کیت‌ها(ردگم‌کن‌ها) را با نگاهی بسیار منحصر به فرد از روش‌ها و تکنیک‌های پشت پرده به خوانندگان ارائه می‌دهد. اگر شما مسئول واحد امنیت هستید، حتماً این کتاب را مطالعه کنید».

1. Matt Conover

مقدمه نویسنده

پیش‌گفتار لنس اسپیتزنر[1]، رئیس پروژه هانی‌نت[2]

«بدافزار[3]»؛ در طی حدود ۱۵ سال مطالعات در زمینه امنیت اطلاعات، بدافزار قوی‌ترین ابزار در بین ابزارها و مهماتی برای حمله‌های سایبری بوده است. تقریباً در تمام حمله‌های موفق از جمله مشاهده عملیات مالی و سرقت اطلاعات در شبکه‌های نظیربه‌نظیر[4] و قابلیت به‌روزرسانی اتوماتیک، بدافزار مؤلفه اصلی و کلیدی بود. به یاد می‌آورم در سال ۱۹۹۸ زمانی که تحقیقات و مطالعاتم حول موضوع امنیت اطلاعات و به خصوص توسعه اولین تکنیک‌های «هانی‌پات[5]» را آغاز نمودم، این تکنیک‌ها به من امکان مشاهده و بررسی چگونگی عملکرد مهاجم‌ها و کنترل کامپیوترهای واقعی را می‌دادند. من به عملکرد، روش‌ها و تکنیک‌های اصلی آن‌ها آگاه شدم. در آن زمان، مهاجم‌ها با پویش[6] دستی تمام بلوک‌های شبکه، حمله را شروع می‌کردند. هدف آن‌ها

---

1. Lance Spitzner
2. Honeynet:
- [مترجم: یک سازمان تحقیقات امنیت بین‌المللی پیشرو، اختصاص داده شده به تحقیق در زمینه آخرین حمله‌های، توسعه ابزار امنیتی منبع باز برای بهبود امنیت اینترنت و یادگیری چگونگی رفتار مخرب هکرها است.]

3. Malware:
- [مترجم: بدافزارها عبارتند از هر نوع کد نرم‌افزاری که روی سیستم کامپیوتری خواسته یا ناخواسته نصب شود و عملیاتی ناخواسته را انجام دهد. بدافزارها دسته‌بندی‌های مختلفی دارند که عبارتند از: بدافزارهای قابل انتشار(کرم‌ها و ویروس‌ها)، روت‌کیت(ردگم‌کن‌ها)، درب‌های پشتی و تروجان‌ها، جاسوس‌افزارها (صفحه‌کلیدنگارها)، آگهی‌افزارها.]

4. Peer-to-peer(P2P)
5. Honeypot:
- [مترجم: یک تله برای کمک به مبارزه با دسترسی غیر مجاز به کامپیوتر است.]

6. Scan

ایجاد فهرستی از آدرس‌های پروتکل‌های اینترنتی[1] بود که به واسطه آن امکان دسترسی و بررسی درگاه‌های مشترک بر روی هر کامپیوتر، جستجوی آسیب‌پذیری‌های شناخته‌شده از جمله سرویس‌دهنده‌های FTP آسیب‌پذیر یا فایل‌های به اشتراک گذاشته‌شده باز را پیدا می‌کردند. زمانی که این آسیب‌پذیری‌ها شناسایی شد، مهاجم‌ها برای سوءاستفاده از سیستم‌ها باز می‌گشتند. این امکان وجود داشت که کل فرآیند بررسی و استفاده از اطلاعات هر مکان و نقطه‌ای، از چندین ساعت تا چندین هفته به طول بیانجامد و هم‌چنین ابزارهای متفاوتی برای انجام هر مرحله نیاز بود. برای هر بار سوءاستفاده، مهاجم باید ابزارهای اضافی را به‌روزرسانی کند که هر کدام اهداف جداگانه‌ای داشتند و معمولاً به صورت دستی اجرا می‌شدند. به عنوان مثال، ابزاری برای پاک‌سازی فایل‌های شرح‌وقایع[2]، ابزاری مخصوص امنیت سیستم و ابزار ویژه بازیابی اسم رمزها یا شناسایی سایر سیستم‌های آسیب‌پذیر بودند. حال قضاوت کنید که مهاجم چقدر باید در راه‌اندازی با اجرای دستورهای سیستم توانایی داشته باشد. مشاهده و یادگیری چگونگی عملکرد، شناسایی و انگیزه مهاجم‌ها جالب بود. هم‌چنین با هوشیاری می‌توانید ورود و دسترسی افراد را به سیستم‌های شخصی خود متوجه شوید.

امروزه حرکت به سمت پیشرفت سریع است و همه چیز به کلی فرق کرده است. در گذشته، در هر مرحله برای حمله و دسترسی به سیستم‌ها باید اعمالی به صورت دستی انجام می‌شد. اما تقریباً همه حمله‌ها تا حد زیادی به‌طور اتوماتیک و با استفاده از ابزارها و فناوری‌های پیشرفته انجام می‌شوند. در گذشته، می‌توانستید تهدیدها را پیگیری و مشاهده نمایید و از هر مرحله انجام آن مطلع شوید.

اما امروزه، کل روند حمله بسیار حساب‌شده و فقط در عرض چند ثانیه انجام می‌شود. هر مرحله از حمله، از بررسی اولیه تا دسترسی به اطلاعات توسط فناوری‌های پیشرفته‌ای انجام می‌شوند که بدافزار نامیده شده‌اند. این مجموعه ابزارها، مهاجم‌ها را قادر می‌سازند تا به سادگی به میلیون‌ها سیستم در کل جهان دسترسی پیدا کنند. زمانی که برای اولین بار ویروس‌ها منتشر شدند، ابزارهای ساده‌ای بودند که چندین فایل را

1. IP
2. Log File

بر روی سیستم تغییر می‌دادند و احتمالاً برخی اسناد را به سرقت می‌بردند یا تلاش می‌کردند تا رمزهای عبور سیستم را بشکنند. امروزه بدافزارها بسیار پیچیده شده‌اند و می‌توانند اطلاعات روی حافظه‌های آسیب‌دیده و بخش‌های آلوده بوت(راه‌انداز سیستم)، بایاس‌ها(BIOs) و روت‌کیت‌های مبتنی بر هسته را بازیابی کنند.

نکته جالب دیگر این است که، بدافزارها به کمک بوت‌نت‌ها[1]، قابلیت ایجاد و کنترل شبکه‌های سیستم‌های در معرض خطر را دارا می‌باشند. این بوت‌نت به شکلی سازمان‌یافته تحت کنترل مجرمان اینترنتی می‌باشند. مجرمان سایبری از آن‌ها به منظور دستیابی به اطلاعات، ارسال هرزنامه، حمله به شبکه‌ها یا وب‌سایت‌های میزبان استفاده می‌کنند. بدافزارهای جدید امکان عملکرد این بوت‌نت‌ها را امکان‌پذیر می‌سازند. در شرایط بدتر، مهاجم‌های سایبری بدافزارها را از سراسر جهان به دست آورده و به‌طور مداوم آن‌ها را پیشرفته‌تر می‌سازند. تا زمان نوشتن این مقدمه، جهان تا به حال با حمله یکی از پیشرفته‌ترین بدافزارها به نام «کرم کامپیوتری کانفلیکر[2]» مقابله نموده است که بر اثر آن میلیون‌ها کامپیوتر در معرض خطر و تحت کنترل گروه سازمان‌یافته نیرومندی از مجرمان قرارگرفته بودند. حمله‌ها بسیار موفقیت‌آمیز بودند به‌طوری که کل سازمان‌های دولتی، از جمله وزارت دفاع ایالات‌متحده آمریکا مجبور به اعلام ممنوعیت استفاده از رسانه‌های تلفن همراه شدند تا به سادگی بتوانند سرعت گسترش آن بدافزار را کاهش دهد. کرم کامپیوتری کانفلیکر هم‌چنین نشان‌دهنده برخی از قابلیت‌های پیشرفته موجود در بدافزارها، از جمله استفاده در فن‌آوری‌های رمزنگاری تا نام دامنه، دامنه‌های تصادفی و ارتباطات مستقل افراد بود. متأسفانه، شرایط تهدید بدتر شده بود. شرکت‌های تولیدکننده ضد ویروس‌ها به معنای واقعی هر روز هزاران بدافزار جدید را شناسایی و این تعداد رو به افزایش بودند.

نه تنها فناوری بدافزارها، بلکه مهاجم‌ها پشتیبان این فنّاوری و انگیزه آن‌ها در ایجاد و توسعه بدافزارها از جمله بزرگ‌ترین تغییراتی است که شاهد آن هستیم. بسیاری از مهاجم‌ها را که در اصل تنها نظاره‌گر هستند می‌توان به عنوان هکرهای جوان در نظر گرفت، نوجوانان بی‌تجربه و غیرمتخصصی که به سادگی از نسخه‌برداری ابزارهای دیگران استفاده می‌کنند. هم‌چنین گروه کوچک دیگری هم وجود دارد که از ابزارهای

1. botnet
2. Conficker Worm

تولیدی خود استفاده می‌کنند و آن‌ها را توسعه می‌دهند، اما انگیزه آن‌ها اغلب حس کنجکاوی است و هدف آن‌ها آزمایش ابزارهایشان و به خطر انداختن سیستم‌ها است، یا می‌خواهند به این وسیله برای خود شهرت به دست آورند. تهدیدهایی که امروزه با آن مواجه هستیم کاملاً متفاوت است، این تهدیدها سازمان‌دهی‌شده، موثر، کارآمد، مهلک و خطرناک‌تر می‌باشند.

امروزه، با مجرم‌هایی مواجه هستیم که بر روی موضوع بهبود بازگشت سرمایه[1] تمرکز و تاکید دارند. آن‌ها تیم‌های تحقیقات و توسعه‌ای دارند که در زمینه ایجاد حمله‌های سودآورتر فعالیت‌هایی را انجام داده‌اند. دقیقاً مشابه هر کسب‌وکاری که به دنبال کسب سود هستند، این مجرم‌ها بر کارایی و فعالیت‌های اقتصادی تمرکز نموده، و تلاش می‌کنند تا حدی که می‌توانند پول بیشتری در مقیاس جهانی به دست آورند. به علاوه، این مجرمان بازار سیاه خود را در تولید و تکثیر بدافزارها ایجاد و توسعه می‌دهند. همان‌طور که به کمک هر اقتصاد دیگری، می‌توان کل بازار سیاهی را شناسایی کرد که در آن سازمان‌های جنایی آخرین ابزارهای بدافزار را خرید و فروش می‌کنند. بدافزار حتی می‌تواند به عنوان یک سرویس ارائه شود. مجرم‌ها بدافزارهای سفارشی را برای مشتریان تولید می‌کنند یا آن‌ها را به عنوان یک سرویس ارائه می‌دهند، خدمات یا سرویس‌هایی که شامل پشتیبانی، به‌روزرسانی، و حتی قراردادهای عملکردی می‌باشد. برای مثال، مجرم‌ها می‌توانند تضمین کنند که بدافزارهای سفارشی بیش‌ترین برنامه‌های ضد ویروسی را از میان برداشته یا برای بهره‌برداری از آسیب‌پذیری‌های ناشناخته طراحی‌شده‌اند.

واحدهای دولتی نیز آخرین ابزارهای جنگ سایبری را تولید می‌کنند. بودجه این واحدها تقریباً نامحدود است و به پیشرفته‌ترین افکار و مهارت‌ها در جهان دسترسی دارند. بدافزارهای آن‌ها به منظور نفوذ بالا و تحت کنترل قرار دادن کشورها و آگاهی از اطلاعات استفاده می‌شوند که مصداق این موضوع در حمله‌های اخیر به شبکه‌های دولتی ایالات‌متحده آمریکا قابل مشاهده است. هم‌چنین واحدهای مهاجم دولتی که از بدافزارها استفاده می‌کنند، می‌توانند در فعالیت‌های سایبری کشورهای دیگر اخلال ایجاد نمایند. به عنوان مثال، حمله‌های سایبری «عدم پذیرش سرویس[2]» گرجستان و

1. ROI - Return of Investment
2. Ddos

استونی را در نظر بگیرید، که به کمک بدافزارها سازمان‌دهی و راه‌اندازی شده است. بدافزار، عامل مشترک تمام حمله‌های غیرقابل مشاهده امروزی می‌باشد. به منظور دفاع و محافظت از شبکه‌های خود، بدون در نظر گرفتن آن‌که چه کسانی مهاجم هستند، باید دفاع در برابر بدافزارها را دریابید.

من از آشنایی با مایکل دیویس که راهنما و همکارم در تألیف و نگارش این کتاب در مورد بدافزار ویندوز است، بسیار خوشحالم و فکر نمی‌کنم از نظر شخصیت کسی بالاتر از او باشد. از زمانی که برای اولین بار مایک به عنوان یکی از بهترین محقق‌ها در زمینه ویندوزها به پروژه «هانی‌پات» ملحق شد تا به حال، حدود ۱۰ سال می‌گذرد. «مایک دیویس» یکی از قوی‌ترین ابزارهای دسترسی به اطلاعات به نام «سِبک[1]» را تولید نمود. سِبک، هسته پیشرفته ابزار ویندوز است. به علاوه، «دیویس» تجربه بسیاری در زمینه بدافزار و ضد ویروس‌ها از جمله نرم‌افزار امنیتی شرکت مک‌آفی دارد. او هم‌چنین در زمینه فعالیت‌های کمک به امنیت مشتریان در سراسر جهان بسیار باتجربه است. هم‌چنین او جزو افرادی است که چگونگی روند تبدیل بدافزارها به بزرگ‌ترین تهدید برای سازمان‌های امروزی را مشاهده کرده است. این کتاب منبع جالبی در زمینه هک و امنیت اطلاعات است و بر آنچه برای درک بهتر و دفاع در رویارویی با بزرگ‌ترین تهدیدهای سایبری نیاز است، تاکید نموده است. من این کتاب را به عنوان منبعی لازم و البته ناکافی در این زمینه توصیه می‌کنم.

لنس اسپیتزنر ـ رئیس پروژه هانی‌نت

1. Sebek

مقدمه مترجم

در طی چند دهه گذشته، انسان‌ها خود را سرگرم شناسایی روش‌هایی جدید برای برقراری ارتباط با دیگران کرده‌اند. تلفن‌های همراه، کامپیوترهای شخصی، پیامک، پست الکترونیکی و اینترنت سبب شده تا جمعیت بشر در ارتباطی سریع با یکدیگر باشند. می‌توان گفت که فضای سایبر یا فضای مجازی به‌عنوان کلید محیط الکترونیکی است که ارتباط افراد را با تکیه بر ابزارهای خاص به‌صورت سریع و سهل برقرار می‌سازد. این محیط با کاربردهای ویژه، بستر مناسبی را برای پیگیری و تبیین آنچه امروز به «جنگ نرم» مشهور است ایجاد می‌نماید.

توانایی فضای سایبر در کنترل و هدایت جنگ نرم منجرشده است، کشورهای سلطه‌گر حساب ویژه‌ای را برای نقش‌آفرینی در محیط مجازی در نظر بگیرند. به‌گونه‌ای که امروز عمده‌ترین ابزار هدایت جنگ نرم، همان فضای مجازی است. در این جنگ دیپلماسی، تبلیغات، جنگ روانی، انهدام و ترور شخصیتی، سیاسی و تهاجم فرهنگی مطرح است. در واقع جنگ نرم معرف یک عصر تازه در طیف اختلافات و تضادهایی است که اشکال اقتصادی، سیاسی، اجتماعی و نظامی را در بر می‌گیرد و هدف عمده آن، نابودی و یا اختلال در اطلاعات و ارتباطات است. از سویی تروریسم کامپیوتری نیز پدیده دیگری است که همزمان با ایجاد و در دسترس قرار گرفتن اینترنت و فضای سایبری به وجود آمده است. این نوع عملیات تروریستی به هرگونه اقدامات خرابکارانه‌ای اطلاق می‌شود که نفوذگران و اخلالگران کامپیوتری علیه شبکه‌های کامپیوتری و اینترنتی یک کشور انجام می‌دهند. دولت‌ها و شرکت‌ها سعی می‌کنند تا هرچه بیشتر شبکه‌های کامپیوتری را زیر نفوذ و کنترل خود درآورند، شبکه اینترنتی هم به محیطی مناسب برای تروریست‌های کامپیوتری، فعالان سیاسی و هکرها یا نفوذگران اینترنتی و حتی خود دولت‌ها تبدیل شده است.

امروزه دورنمای تهدید، بسیار چالش‌برانگیزتر از پیش است. پیشرفت‌های اخیر در تکنیک‌های جنگ سایبری نشان می‌دهد که بخش عمده‌ای از منازعات بین نظام جمهوری اسلامی ایران و جهان سلطه در عرصه مجازی در حال وقوع است. دشمنان از هر ابزاری برای آسیب و تهدید زیرساخت‌های حساس ایران استفاده می‌کنند. به عنوان مثال از مهم‌ترین حمله‌های بدافزاری به ایران می‌توان به حمله «استاکس‌نت[1]» که بدافزاری برای آلوده‌سازی کامپیوترهای کاربرهای صنعتی، و بدافزار «شعله[2]» به عنوان پیچیده‌ترین و مخرب‌ترین سلاح سایبری، اشاره کرد. سهم فضای مجازی از بودجه‌های میلیاردی که کنگره آمریکا و رژیم اشغالگر قدس برای مقابله با جمهوری اسلامی ایران تصویب می‌کنند، بیانگر اهمیت جایگاه این عرصه در تقابل امنیتی - سیاسی است. به این ترتیب، جنگ در فضای سایبری به میدان رقابت جدیدی برای ایران و غرب، به خصوص آمریکا تبدیل شده است.

با توجه به این‌که پیش‌گیری از آسیب‌های موجود در فضای سایبری، امری بسیار حیاتی می‌باشد و آموزش به عنوان مهم‌ترین راهکار پیشنهادی برای پیش‌گیری از این آسیب‌ها است. لذا هدف از ترجمه کتاب «آشکارسازی هک، بدافزارها و روت‌کیت‌ها» ارائه راهنمای کاملی است که چگونگی نفوذ هکرها، و نحوه شناسایی آن‌ها را آموزش می‌دهد. این کتاب چگونگی از بین‌بردن بدافزارها و روت‌کیت‌ها(ردگم‌کن‌ها) را با نگاهی بسیار منحصربه‌فرد از روش‌ها و تکنیک‌های پشت پرده بدافزار و روت‌کیت‌ها به خوانندگان ارائه می‌دهد. لذا یکی از بهترین آثار برای آشنایی هرچه بیشتر مدیرهای امنیتی، برنامه‌نویس‌ها و کاربرهایی است که می‌خواهند به حفاظت از سیستم‌های کامپیوتری و حساس خود در مقابله آسیب بدافزارها و روت‌کیت‌ها بپردازند. در ترجمه این کتاب تلاش شده است تا علاوه بر حفظ امانت نویسنده‌ها، متن ساده، روان و قابل‌درک برای تمام کاربرهای مبتدی و حرفه‌ای فارسی‌زبان باشد. هم‌چنین تلاش شده است تا با ارائه توضیحات لازم برای عبارات و اصطلاحات تخصصی به صورت زیرنویس خواننده را با اطلاعات مفید بیشتری آشناسازیم.

بی‌گمان آنچه که بیش از هر اقدامی می‌تواند دشمنان و بدخواهان را از دستیابی به

1. StuxNet
2. Flame

اهداف بازدارد و آنان را ناکام گذارد، روشنگری، تبیین سیاست‌ها و اهداف آن‌ها است. همچنان که مقام معظم رهبری فرمودند: «این‌که بتوانیم طرح کلی دشمن را در مورد خود بدانیم، بخشی از توان دفاعی ما است. به این مسئله توجه داشته باشید که ندانستن این‌که دشمن چه در فکر دارد و چه می‌خواهد انجام دهد، غفلتی است که ما را از امکان مقابله و دفاع محروم می‌کند».

علی نایب‌پور ـ ۱۳۹٤

راهنما

در این کتاب هر تکنیک حمله به دو صورت زیر نشان داده شده است:

آیکون تهدید: شناسایی و تشخیص انواع بدافزارها و روش‌های خاص آن‌ها را ساده‌تر می‌سازد. هر حمله‌ای با نمونه‌های کاربردی مرتبط، تست‌شده و پاسخ داده شده است، که هر کدام آیکون مخصوص به خود را دارند.

آیکون اقدام متقابل: مشکل را حل و مهاجم‌ها را دور کنید.

- به ورودی رمز برجسته شده که به صورت متنی و پررنگ در لیست کدها نوشته‌شده، دقت کافی داشته باشید.
- هر حمله به همراه میزان خطر به‌روزرسانی، ارائه‌شده که این مقدار بر اساس سه معیار و با توجه به تجارب هر سه نویسنده حاصل شده است:

محبوبیت	فراوانی استفاده از آن در طبیعت در مقابل هدف‌های زنده: ۱ استفاده خیلی به ندرت ، ۱۰ استفاده به صورت گسترده
سادگی	میزان مهارت مورد نیاز برای اجرا: ۱ برنامه‌های نسبتاً امنیتی، ۱۰ میزان خیلی کم یا فاقد نیاز به مهارت
اثرگذاری	آسیب‌های جدی حاصل از اجرای موفقیت‌آمیز حمله: ۱ افشای اطلاعات هدف فاقد ارزش، ۱۰ اطلاعات مرتبط با حساب افراد یا مواردی معادل با آن
میزان خطر	سه مقدار فوق میانگین‌گیری می‌شود و رتبه خطر کلی برای هر حمله به دست می‌آید.

اطلاعاتی درباره وب‌سایت

از آنجا که بدافزارها و روت‌کیت‌ها همواره در حال انتشار هستند، از این رو می‌توانید آخرین ابزارها و روش‌های مقابله و هک نمودن آن‌ها را در وب‌سایت «http://www.malwarehackingexposed.com» بیابید. این وب‌سایت شامل کدها و ابزارهای ذکرشده در کتاب می‌باشد که حتی برخی از آن‌ها هرگز منتشرنشده و آن‌ها در پیوست آورده شده‌اند. ما هم‌چنین نسخه‌ای از تمام ابزارهای بیان‌شده در کتاب را در سایت قراردادیم تا بتوانید آن‌ها را حتی پس از توقف نوشتن توسط صاحب‌های آن‌ها دانلود کنید.