

تهدید امنیتی ۲۰۱۴-۲۰۱۲

گزارش امنیت رایانه‌ای SOPHOS

به انضمام روندهای تهدید امنیتی ۲۰۱۵

نویسنده: گرهارد اسلر

مترجم: مهدی تهران

ناظر علمی: محسن زارع تاجیک

سرشناسه: اشلیک، گرهارد (Gerhard Eschelbeck) / مترجم: مهدی تهرانی / ناظر علمی: محسن زارع تاجیک

عنوان و نام پدیدآور: تهدید امنیتی ۲۰۱۲-۲۰۱۴: گزارش شرکت رایانه‌ای سوفوس (SOPHOS)

مشخصات نشر: تهران، انتشارات دیده‌بان

مشخصات ظاهری: ۱۶۲ ص. مصور، جدول

وضعیت فهرست‌نویسی: فیبا

موضوع: شبکه‌های کامپیوتری - تدابیر امنیتی - تروریسم رایانه‌ای - کامپیوترها - ایمنی اطلاعات - اینترنت -

ایالات متحده

رده‌بندی کنگره: ۱۳۹۴ ق ۵۵ الف / ۵۱۰۵ / ۵۹ / TK۵ - رده‌بندی دیویی: ۰۰۵/۸ - کتابشناسی ملی: ۳۹۱۶۷۸۴



انتشارات دیده‌بان

❖ عنوان کتاب: تهدید امنیتی - ۲۰۱۲-۲۰۱۴: گزارش شرکت رایانه‌ای سوفوس (SOPHOS)

❖ نویسنده: اشلیک، گرهارد

❖ ناشر: انتشارات دیده‌بان

❖ مترجم: مهدی تهرانی

❖ ناظر علمی: محسن زارع تاجیک

❖ ویراستار ادبی: میترا مشهدی رجب

❖ طرح روی جلد: رضا حسنی

❖ لیتوگرافی، چاپ و صحافی: انتشارات دیده‌بان

❖ شمارگان: ۵۰۰ جلد

❖ نوبت چاپ: اول، پاییز ۹۴

❖ قیمت: ۱۵۰۰۰۰ ریال

ISBN: 978-600-95520-2-3

شابک: ۹۷۸-۶۰۰-۹۵۵۲۰-۲-۳

حق چاپ برای ناشر محفوظ است

آدرس: تهران، چهارراه پاسداران، انتشارات دیده‌بان، تلفن: ۲۲۷۶۲۸۳۷

فهرست مطالب

الف..... سخن ناشر.....

۱..... فصل اول - گزارش سال ۲۰۱۲.....

۱..... مقدمه.....

۴..... مروری بر سال ۲۰۱۱: اطلاع‌رسانی در مورد هکتیویسم.....

۵..... علت حمله.....

۵..... هکتیویسم: کانون توجه.....

۷..... ویروس کانفیکر به رغم پیچ و پچنان شایع.....

۹..... راهبردهای حفاظت در برابر بدافزار.....

۹..... سقوط آنتی‌ویروس تقلبی (Fake).....

۱۱..... از پا درآمدن سریع هرزنامه: حذف باکنت.....

۱۲..... ریسک نسبی اجرای شبکه‌های کامپیوتری در براسر دنیا.....

۱۵..... تهدیدهای آنلاین.....

۱۵..... چشم‌انداز امروز برای تهدیدات وب.....

۱۶..... تشریح یک حمله: داندوده‌های غیرارادی و سیاه چاله.....

۱۹..... حفاظت در مقابل تهدیدات شبکه: دروازه‌های امن.....

۲۰..... سیستم‌ها و تهدیدات نرم‌افزاری.....

۲۰..... سیستم‌های عامل: ظهور بدافزار Mac.....

۲۳..... رسانه‌های جدانشدنی: از دست دادن داده، قابل پیشگیری.....

۲۵..... ریسک در مسیر کار ما.....

۲۵..... گسترش فناوری اطلاعات از طریق مشتری.....

۳۰..... پردازش ابری.....

۳۲..... شبکه‌های اجتماعی.....

۳۶..... امنیت کامل Sophos.....

۳۷..... ۱۰ روند جدید در سال ۲۰۱۲.....

۳۹..... کلام آخر.....

۴۱..... فصل دوم - گزارش سال ۲۰۱۳.....

۴۱..... پیشگفتار.....

۴۴	مقدمه
۴۶	گسترش حملات مرتبط با فیس‌بوک و سایر پایگاه‌های رسانه‌ای اجتماعی
۴۸	مخاطرات در حال ظهور برای خدمات ابری
۵۰	سیاه‌چاله: سردهسته بازار بدافزارهای امروزی
۵۲	چهار مرحله چرخه حیات سیاه‌چاله
۵۵	آنچه ما درخصوص سیاه‌چاله در حال انجام هستیم و آنچه شما می‌توانید انجام دهید
۵۶	حملات جاوا به حد حساس توده‌ای خود رسیده است
۶۱	اندروید: بزرگ‌ترین هدف امروزه
۶۱	غیرپیچید: اما مفید: نرم‌افزار جعلی، پیامک‌های غیرمجاز
۶۳	پیوستن به امنیت
۶۳	دریافت پیام‌ها و حساب بانکی شما
۶۶	کاهش میزان ریسک در فضای که هنوز قابل مدیریت هستند
۶۹	پایگاه‌ها و فناوری‌های متنوع فرصت برای حمله را افزایش می‌دهند
۷۱	باج‌افزار بار دیگر بازمی‌گردد
۷۳	سیستم عامل ایکس (X) و ایکس (۱۷۶۳)
۷۳	ضد ویروس و فلش‌بک تقلبی
۷۵	بدافزار مورکات/بحران: پیچیده‌تر و به مراتب بالقوه خطرناک‌تر
۷۷	بدافزارهای ویندوز که به مخفیانه در مک (OS X) پنهان هستند
۷۸	بهینه‌سازی امنیتی اخیر سیستم عامل ایکس (OS X) و محدودیت‌های آن
۷۹	اجرایی کردن راهکار جامع ضدبدافزار مک
۸۱	مسئولان ذی‌ربط اقدام به دستگیری و توقیف اموال تولیدکنندگان می‌کنند
۸۳	افزایش حملات هدفمند خطرناک
۸۵	حملات چند شکلی و هدفمند: انتهای طولانی
۸۶	چندشکلی بودن: نه چندان جدید؛ ولی پردردسرن
۸۷	مقابله با حملات چندشکلی سرور جاتی
۸۸	حملات هدفمند؛ باریک، متمرکز و خطرناک
۸۹	دفاع در عمق علیه حملات SSP
۸۹	امنیت کامل
۹۲	چه انتظاراتی در سال ۲۰۱۳ وجود دارد؟
۹۴	کلام آخر
۹۵	فصل سوم - گزارش سال ۲۰۱۴
۹۵	پیشگفتار

۹۸	مقدمه: بدافزارهایی که در سال ۲۰۱۳ پدیدار شدند
۹۹	باتنت‌ها در اندازه و مخفی بودن رشد کرده‌اند
۱۰۴	پول خرد (بیت‌کوین) کاوی باتنت: بدافزار دیگر مسیر کسب درآمد
۱۰۵	بدافزار اندروید: در حال تغییر و هوشمندتر شدن
۱۱۱	لینوکس؛ فناوری مهم که تبهکاران را جذب می‌کند
۱۱۲	سیستم عامل Mac OS X: سالی پر از حملات کوچک بسیار زیاد
۱۱۶	بدافزار تحت وب: پیچیده تر، متنوع تر و مخفی تر
۱۲۲	تهدیدات هدفمند نسبت به حساب‌های مالی شما
۱۲۴	ویندوز: خطر رونق افزایش سیستم‌های فاقد وصله امنیتی
۱۲۷	هرزنامه خرد را ابداع مجدد می‌کند
۱۲۹	آزمایشگاه‌های سوفین؛ پیشگام در پیچیده‌ترین حملات امروزی
۱۳۱	روندهایی که در سال ۲۰۱۴ دیده خواهند شد
۱۳۵	کلام آخر

۱۳۷	فصل چهارم - روندهای تهدید امنیتی سال ۲۰۱۵
۱۳۷	امنیت سایبری در سال ۲۰۱۵
۱۳۸	کاهش تبعات مربوط به کدهای مخرب از تعداد تیریه‌های مفید می‌کاهد
۱۳۹	حملات مربوط به اینترنت اشیا
۱۴۱	رمزنگاری معیاری عمومی می‌شود
۱۴۲	رخنه‌های اصلی که بیشتر در مورد نرم‌افزارهای پرکاربرد
۱۴۳	چشم‌انداز تنظیم مقررات
۱۴۴	مهاجمان تمرکزشان را روی سیستم‌های پرداخت موبایل بیشتر کرده‌اند
۱۴۶	شکاف در مهارت‌های جهانی با وجود واکنش به رویداد و آموزش
۱۴۶	خدمات مربوط به حمله و کیت‌های کدهای مخرب
۱۴۸	فقط شکاف میان ICS/SCADA و امنیت در دنیای واقعی بیشتر شده است
۱۴۹	توانمندی‌های جالب توجه روت کیت‌ها و بات‌ها
۱۵۱	منابع



سخن ناشر

همان‌طور که فضای مجازی دارای ویژگی‌های متعددی است و به‌صورت روزمره در زندگی اشخاص، حاکمیت و خدمات دولت‌ها، عملکرد نهادها و سازمان‌ها و بسیاری دیگر از موضوعات، مورد استفاده قرار می‌گیرد، فقدان امنیت آن باعث گردیده تا صدقات جبران ناپذیری به کاربران آن اعم از حقیقی و حقوقی، وارد گردد. همچنان که گزارش‌های متعددی از نقض امنیتی در فضای سایبر را در این گزارش خواهید دید.

امروزه تأمین امنیت فضای سایبر و ارتقاء آن، مسئله اصلی سازمان‌ها، نیروهای نظامی و امنیتی، سازمان‌های اطلاعاتی، شرکت‌ها، نهادها، اشخاص و... بوده و این مسأله بر شناسایی نقاط ضعف امنیتی در فضای سایبر و بررسی گزارشات اتفاقات امنیتی رخ داده، راه‌حل دیگری نمی‌تواند داشته باشد تا ضمن آشنایی با راه‌های نفوذ، هوشیاری در کاربران فناوری اطلاعات که بالاترین درجه آسیب‌رسانی را در فضای سایبر دارند، بالا رود.

کتاب حاضر، مشتمل بر گزارش‌هایی از نقض امنیت در حوزه فناوری اطلاعات و رویکردهای امنیتی در سراسر دنیا از سال‌های ۲۰۱۲ تا ۲۰۱۵ بوده که توسط شرکت سوفوس، به صورت سالانه و به همراه تحلیل‌های تخصصی خود و برآورد وقوع تهدیدات و نقاط آسیب‌پذیر جدید ارائه شده در سال‌های مذکور ارائه شده است. این شرکت، توصیه‌های امنیتی به منظور ارتقاء سطح امنیت فناوری اطلاعات را نیز مطرح کرده است. انتشارات دیده‌بان با تجميع ۴ ساله گزارش‌های یادشده، آن را در قالب این کتاب گردآوری نموده است.

این نکته نیز قابل ذکر است که گزارش‌های ارائه شده توسط این شرکت بصورت جامع و با رصد کل رخدادهای امنیتی در حوزه فناوری اطلاعات در سراسر جهان نمی‌باشد و بیشتر کشورهای حوزه آمریکا را مورد پایش و بررسی قرار داده است. به عنوان مثال می‌توان به اتفاق امنیتی ¹HeartBleed در اینترنت اشاره نمود که در اوائل سال ۲۰۱۴ رخ داد (تا دو سال قبل از ۲۰۱۴، این آسیب‌پذیری روی سرورهای آژانس امنیتی ملی آمریکا وجود داشته است) و این آسیب‌پذیری موجب شد تا کل ارتباطات رمز Open SSL مورد حمله و بشود هکرها قرار گیرد. آسیب‌پذیری یادشده به اندازه‌ای عمیق و گسترده بود که امنیت سایر وبسایت‌های بزرگی مانند یاهو، گوگل، جی‌میل، فیسبوک، توئیتر، ویرچوال‌باکس و دراب‌باکس به خطر انداخت و به "خونریزی قلبی اینترنت" معروف شد.

اما با در نظر گرفتن کم‌مطابق می‌توان گفت این گزارش‌ها، با توجه به این‌که فناوری اطلاعات تمامی کشورها و نقاط جهان را دربر گرفته است و بالتبع آن آسیب‌پذیری‌ها نیز به همین منوال منتقل شده است، لذا تقریباً به بیشتر نقص‌های امنیتی در حوزه فناوری اطلاعات اشاره داشته است.

از جمله نکاتی که در این گزارش می‌توان صورت اجمالی به آنها پرداخت شامل: شش قانونی اطلاعات توسط پلیس (یا به عبارت دیگر توسط آژانس امنیت ملی آمریکا)، حضور و پیشرفت روزافزون باج‌افزارها، سرقت اطلاعات خصوصی افراد، سرقت اطلاعات افراد و سازمانها در فضای پردازش ابری، سرقت حسابهای بانکی، زنده‌شدن دوباره شبکه‌های بانکی به منظور ارسال پیام‌های آلوده، حملات هکری سیاسی علیه دولت‌ها مانند فلیم^۲، حضور بدافزارها در سیستم‌های عامل OS X و MAC و Unix با الگوبرداری از بدافزارهای سیستم عامل ویندوز، حمله به سرورهای اینترنتی (علی‌رغم این‌که تعداد آنها نسبت به ویندوز کمتر است، اما دارای اطلاعات و ارتباطات با اینترنتی هستند)، حضور گسترده بدافزارهای اندروید، پیچیده‌تر شدن بدافزارها از لحاظ چندریختی عملیات و رمزنگاری و جلوگیری از مهندسی معکوس خود، تبلیغ محصولات شرکت سوفوس و ضعف همیشگی در استفاده از راه‌های امنیتی توسط شرکت‌های تولیدکننده نرم‌افزار و از همه مهم‌تر عدم توجه کاربران به نصب این وصله‌ها می‌باشد.

همچنین راه‌حل‌های کلی نیز برای رفع اشکالات و جلوگیری از صدمه و ضربه آسیب‌پذیری‌ها در حوزه فناوری اطلاعات توسط شرکت سوفوس مطرح گردیده است.

اما مهمترین نکته‌ای که در الزامات و اقدامات امنیتی به آن اشاره شده و بارها در گزارش مورد تأکید قرار گرفته، توجیه کاربران و افراد استفاده‌کننده از فناوری اطلاعات می‌باشد و شاید بتوان گفت بزرگترین ابزاری

که می‌تواند جلوی بیشتر حملات را بگیرد، کاربر می‌باشد. چرا که اگر کاربر رمز خود را ساده انتخاب کند، یا در محیط‌های ناامن حضور پیدا کند، یا وصله‌های امنیتی را نصب نکند، یا تنظیمات امنیتی لازم را انجام ندهد، یا ضدبدافزار را غیرفعال و بروزرسانی نکند و یا... باعث بروز صدماتی می‌گردد که به هیچ عنوان ابزارهای امنیتی نمی‌توانند جلوی این حملات را بگیرند.

در هر صورت امیدواریم کاربران، مدیران، روسا، مدیران فناوری اطلاعات، مدیران امنیتی فناوری اطلاعات با مطالعه این گزارش‌ها از وضعیت آسیب‌پذیری‌های امنیتی در حوزه فناوری اطلاعات مطلع شده و در جهت ارتقاء سطح امنیت فناوری اطلاعات در حوزه اطلاعات شخصی، سازمانی، مأموریتی و غیره استفاده نمایند.