

حملات سایبری

حفاظت از زیرساخت ملی

تألیف:

ادوارد جی. آموروسو

مترجمین:

مهندس نوید فرخی

مهندس حامد فرخی



سرشناسه	آموروسو، ادوارد جی.
عنوان و نام پدیدآور	حملات سایبری: حفاظت از زیرساخت ملی / تألیف ادوارد جی. آموروسو؛ مترجمین نوید فرخی، حامد فرخی.
مشخصات نشر	بابل: علوم رایانه، ۱۳۹۳.
مشخصات ظاهری	۲۰۰ص: مصور، جدول، نمودار.
شابک	۹۷۸-۶۰۰-۲۰۵-۰۸۲-۳
وضعیت فهرست‌نویسی	فیبا
یادداشت	عنوان اصلی: Cyber attacks: protecting national infrastructure, c2011.
موضوع	تروریسم رایانه‌ای -- ایالات متحده -- پیشگیری
موضوع	کامپیوترها -- ایالات متحده -- ایمنی اطلاعات
موضوع	امنیت ملی -- ایالات متحده
موضوع	فضای مجازی -- تدابیر ایمنی
موضوع	جرایم کامپیوتری -- ایالات متحده -- پیشگیری
شناسه افزوده	فرخی، نوید، ۱۳۶۸-، مترجم
شناسه افزوده	فرخی، حامد، ۱۳۶۰-، مترجم
رده‌بندی کنگره	۱۳۹۳ ج ۸ / HV۶۷۷۳/۲/آ۸
رده‌بندی دیویی	۳۶۳/۳۲۵۹۰۰۴۶۷۸۰۹۷۳
شماره کتابشناسی ملی	۲۶۶۶۷۱۷

این اثر، مشمول قانون حمایت مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ است، هر کس تمام یا قسمتی از این اثر را بدون اجازه مؤلف (ناشر) نشر یا پخش یا عرضه کند مورد پیگرد قانونی قرار خواهد گرفت.



www.olomrayaneh.net

تلفن: ۳۲۳۶۰۷۷۲ - ۱۱

بابل، صندوق پستی ۸۹۱-۴۷۱۳۵ علوم رایانه

حملات سایبری: حفاظت از زیرساخت ملی

تألیف: ادوارد جی. آموروسو

مترجمین: مهندس نوید فرخی - مهندس حامد فرخی

چاپ اول

پاییز ۱۳۹۳

شمارگان: ۵۰۰ نسخه

قیمت: ۲۰۰۰ تومان

چاپ و صحافی: فرنگار رنگ

شابک: ۹۷۸-۶۰۰-۲۰۵-۰۸۲-۳

نشانی ناشر: بابل، خیابان شریعتی، مجتمع میلاد، واحد ۱۷

حروفچینی و صفحه‌آرایی: علوم رایانه

تهران، خیابان انقلاب، خیابان اردیبهشت، نبش وحید نظری، شماره ۱۴۲ - تلفکس: ۶۶۴۰۰۲۲۰ - ۶۶۴۰۰۱۴۴

فهرست مطالب

فصل اول : مقدمه

۱-۱. حملات، آسیب پذیری ها و تهدیدهای سایبری ملی	۱۲
۲-۱. تهدید باتنت	۱۴
۳-۱. مؤلفه های متدولوژی امنیت سایبری ملی	۱۷
۴-۱. فریب	۱۸
۵-۱. جدایی	۲۰
۶-۱. گوناگونی	۲۲
۷-۱. سازگاری	۲۳
۸-۱. عمق	۲۴
۹-۱. احتیاط	۲۶
۱۰-۱. گردآوری	۲۷
۱۱-۱. همبستگی	۲۸
۱۲-۱. آگاهی	۳۰
۱۳-۱. پاسخ دهی	۳۱
۱۴-۱. پیاده سازی ملی اصول امنیتی	۳۳

فصل دوم : فریبکاری

۱-۲. مرحله ی اسکن کردن	۳۹
۲-۲. پورت های عمداً باز	۴۱
۳-۲. مرحله ی کشف	۴۳
۴-۲. اسناد فریبکاری	۴۴
۵-۲. مرحله ی بهره برداری	۴۵
۶-۲. تله های تأمین منبع	۴۷
۷-۲. مرحله ی افشاگری	۴۸
۸-۲. واسط میان انسان و کامپیوتر	۴۹
۹-۲. برنامه ی فریبکاری سایبری در سطح ملی	۵۰

فصل سوم: جدایی

۵۴	۱-۳. جدایی چیست؟
۵۶	۲-۳. جدایی تابعی
۵۷	۳-۳. فایروال‌های زیرساخت ملی
۶۰	۴-۳. DDOS فیلترینگ
۶۱	۵-۳. معماری جدایی SCADA
۶۳	۶-۳. جدایی فیزیکی
۶۵	۷-۳. جداسازی در داخل
۶۸	۸-۳. جداسازی دارایی
۶۹	۹-۳. امنیت چندسطحی (MLS)

فصل چهارم: گوناگونی

۷۴	۱-۴. گوناگونی و شیوع کرم کامپیوتری
۷۵	۲-۴. گوناگونی در سیستم‌های دسکتاپ
۸۰	۳-۴. گوناگونی فناوری شبکه‌ای
۸۲	۴-۴. گوناگونی فیزیکی
۸۴	۵-۴. برنامه‌ی گوناگونی ملی

فصل پنجم: ویژگی مشترک

۸۹	۱-۵. بهترین اقدامات معنادار برای حفاظت از زیرساخت
۹۲	۲-۵. سیاست امنیتی مناسب به طور محلی
۹۳	۳-۵. رویه‌ی حفاظت امنیتی
۹۵	۴-۵. ساده‌سازی زیرساخت
۹۷	۵-۵. گواهی و آموزش
۱۰۰	۶-۵. مسیر شغلی و ساختار پاداش
۱۰۱	۷-۵. تجربه‌ی مسئولیت‌پیشین
۱۰۲	۸-۵. برنامه‌ی عمومی ملی

فصل ششم: عمق

۱۰۶	۱-۶. تأثیرگذاری عمق
۱۰۸	۲-۶. اعتبارسنجی لایه‌ای
۱۱۱	۳-۶. حفاظت لایه‌ای در برابر اسپم و ویروس‌های ایمیلی
۱۱۳	۴-۶. کنترل‌های دسترسی لایه‌ای
۱۱۵	۵-۶. رمزگذاری لایه‌ای
۱۱۶	۶-۶. کشف تهاجم لایه‌ای
۱۱۸	۷-۶. برنامه‌ی ملی عمقی

فصل هفتم: احتیاط

۱-۷	پایگاه پردازشی قابل اعتماد	۱۲۱
۲-۷	امنیت از طریق ابهام	۱۲۳
۳-۷	اشتراک‌گذاری اطلاعات	۱۲۶
۴-۷	اکتشاف اطلاعات	۱۲۷
۵-۷	لایه‌های ابهام	۱۲۹
۶-۷	تفکیک سازمانی	۱۳۱
۷-۷	برنامه‌ی احتیاط ملی	۱۳۲

فصل هشتم: گردآوری

۱-۸	گردآوری داده‌ی شبکه	۱۳۶
۲-۸	گردآوری داده‌ی سیستم	۱۳۹
۳-۸	مدیریت رویداد و اطلاعات امنیتی	۱۴۲
۴-۸	روند داده‌ها در مقیاس بالا	۱۴۴
۵-۸	ردیابی یک کرم	۱۴۶
۶-۸	برنامه‌ی گردآوری در سطح ملی	۱۴۸

فصل نهم: همبستگی

۱-۹	متدهای همبستگی امنیتی مرسوم	۱۵۴
۲-۹	مسائل مرتبط با کیفیت و قابلیت اعتماد در همبستگی داده	۱۵۶
۳-۹	همبستگی داده برای تشخیص کرم‌های اینترنتی	۱۵۷
۴-۹	همبستگی داده برای تشخیص بات‌نت	۱۵۹
۵-۹	فرآیند همبستگی با ابعاد بالا	۱۶۱
۶-۹	برنامه‌ی همبستگی ملی	۱۶۳

فصل دهم: آگاهی

۱-۱۰	تشخیص حملات زیرساختی	۱۶۸
۲-۱۰	مدیریت اطلاعات آسیب‌پذیری‌ها	۱۷۰
۳-۱۰	گزارشات اطلاعاتی امنیت سایبری	۱۷۲
۴-۱۰	فرآیند مدیریت خطر	۱۷۳
۵-۱۰	مراکز عملیات امنیتی	۱۷۵
۶-۱۰	برنامه‌ی آگاهی ملی	۱۷۶

فصل یازدهم: پاسخ‌دهی

۱-۱۱	پاسخ‌دهی پیش از حمله، و پس از حمله	۱۸۰
۲-۱۱	هشدارها و علائم	۱۸۱
۳-۱۱	تیم‌های پاسخ‌دهی به رویداد	۱۸۳

۱۸۵.....	۴-۱۱. ارزیابی استدلالی
۱۸۷.....	۵-۱۱. مسائل مرتبط با اجرای قانون
۱۸۸.....	۶-۱۱. بازیابی از فاجعه
۱۸۹.....	۷-۱۱. برنامه‌ی پاسخ‌دهی ملی

فصل دوازدهم: ملزومات نمونه‌ی حفاظت از زیرساخت ملی

۱۹۲.....	۱-۱۲. ملزومات نمونه در اصل فریبکاری (فصل دوم)
۱۹۳.....	۲-۱۲. ملزومات نمونه در اصل جدایی (فصل سوم)
۱۹۵.....	۳-۱۲. ملزومات نمونه در اصل گوناگونی (فصل چهارم)
۱۹۶.....	۴-۱۲. ملزومات نمونه در اصل ویژگی مشترک (فصل پنجم)
۱۹۶.....	۵-۱۲. ملزومات نمونه در اصل عمق (فصل ششم)
۱۹۷.....	۶-۱۲. ملزومات نمونه در اصل احتیاط (فصل هفتم)
۱۹۸.....	۷-۱۲. ملزومات نمونه در اصل گردآوری (فصل هشتم)
۱۹۸.....	۸-۱۲. ملزومات نمونه در اصل همبستگی (فصل نهم)
۱۹۹.....	۹-۱۲. ملزومات نمونه در اصل آگاهی (فصل دهم)
۲۰۰.....	۱۰-۱۲. ملزومات نمونه در اصل پاسخ‌دهی (فصل یازدهم)