

آشنایی با جنگ نرم

جنگ سایبر (۳)

تألیف و گردآوری:

محمد ابراهیم نژاد

حمید اسکندری



انتشارات

سرشناسه : ابراهیم نژاد شلمانی، محمد، ۱۳۵۶
 عنوان و نام پدیدآور : آشنایی با جنگ نرم: جنگ سایبر/ تدوین و گردآوری محمد ابراهیم نژاد، حمید اسکندری.
 مشخصات نشر : تهران: بوستان حمید، ۱۳۹۰-
 مشخصات ظاهری : ج.: مصور، جدول، نمودار.
 شابک : دوره: ۱-۴-۹۲۲۹۳-۶۰۰-۹۷۸ ؛ ج. ۱: ۷-۰-۹۲۲۹۳-۶۰۰-۹۷۸،
 ج. ۲: ۲-۰-۹۲۲۹۳-۶۰۰-۹۷۸، ج. ۳: ۰-۰-۹۲۲۹۳-۶۰۰-۹۷۸،
 وضعیت فهرست نویسی: فیا
 یادداشت : ج. ۲: (چاپ اول: زمستان ۱۳۹۰).
 یادداشت : ج. ۲: (چاپ دوم: ۱۳۹۲). (فیا)
 یادداشت : ج. ۳: (چاپ اول: ۱۳۹۲). (فیا)
 یادداشت : کتابنامه
 عنوان دیگر : جنگ سایبر
 موضوع : جنگ نرم
 موضوع : جنگ اطلاعاتی
 موضوع : ترسیم رایانه‌ای
 شناسه افزوده : «سنگین»، حمید، ۱۳۳۸ - گردآورنده
 رده بندی کنگره : ۲۹۰ آ ۵ الف UB۲۷
 رده بندی دیویی : ۳۲۳۴/۳۵۵
 شماره کتابشناسی ملی : ۲۲۹۸۲۶۶



انتشار

عنوان : آشنایی با جنگ نرم جنگ سایبر (۳)
 تألیف و گردآوری: محمد ابراهیم نژاد - حمید اسکندری
 ناشر: بوستان حمید
 چاپ: سوم (۱۳۹۸)
 شمارگان: ۲۵۰
 قیمت: ۲۶۰۰۰ تومان

• کلیه حقوق اعم از چاپ و تکثیر، نسخه برداری برای ناشر محفوظ است.

تلفن ناشر و پخش کتاب: ۶۶۴۸۲۳۸۹ ۰۹۱۲۲۳۷۵۰۳۹ ۰۹۱۲۷۷۵۷۸۳۸

فروشگاه اینترنتی: boostanhamid-pub.ir «این کتاب با کاغذ حمایتی منتشر شده است»

پیش گفتار

تهاجم سایبری اکنون چنان گسترش یافته که از سال ۲۰۱۲ به عنوان سال جهنمی در این زمینه نام برده و اینگونه اظهار می‌شود که در این فضا، گروهی با داشتن یک میلیارد دلار و کمتر از پنجاه نفر نیروی متخصص قادر خواهند بود یک کشور را از کار ببندازند.

این تهدید بر روی کشور ما نیز بی تأثیر نبوده و طی این مدت ایران نیز در فضای سایبری مورد حملات مختلف قرار گرفته و تلاش‌هایی شده است تا بخش‌هایی از مراکز حساس مانند نفت، صنعت، بانک ... از کار افتاده و یا دچار اختلال شوند.

استاکس نت و حمله به بخش صنعتی

اواسط سال ۱۳۸۰ بود که رسانه‌های مختلف در سطح دنیا بحث حمله بدافزار جاسوسی به نام استاکس نت خبر دادند. این نکته تأکید کردند که این بدافزار بخش صنعتی کشورها را مورد حمله قرار داده و برخی رایانه‌های ایران را هم تحت تأثیر قرار داده است. البته در همان زمان معاون وقت وزیر صنایع، با اشاره به این که هجوم کرم جاسوس استاکس نت به رایانه‌های ایرانی می‌تواند دارای دلایل اقتصادی یا سیاسی باشد، گفت: «آلودگی به این بدافزار از حدود هشت ماه پیش در ایران آغاز شده و مشخص نیست چرا رسانه‌های بیگانه هم‌اکنون این موضوع را مطرح می‌کنند؟»

وی عمده مراکز مورد تهاجم این کرم، صنایع مربوط به بخش نفت و نیرو دانسته و از شناسایی IPهای آلوده و طراحی آنتی ویروس خبر داده بود. البته این بدافزار کشورهای متعددی مانند هند، اندونزی و پاکستان را هم مورد حمله قرار داده بود.

گاوس و سیستم بانکی: ویروس گاوس را می‌توان به عنوان یکی دیگر از حملات سایبری دانست که هدف اصلی آن کشورهای خاورمیانه بود. این ویروس که به عقیده بسیاری از کارشناسان جهان توسط همان طراحان استاکس نت طراحی شده بود، قابلیت حمله به زیرساخت‌های اصلی کشورها را داشت. این بدافزار در ۱۰ آگوست سال ۲۰۱۲ تحت خانواده تروجان‌ها شناسایی و در اواسط سال ۲۰۱۱ به عنوان تروجان بانکی توسط مهاجمین مورد استفاده قرار گرفته و سیستم‌های هدف این بدافزار، سیستم‌های خانواده ویندوز ارزیابی شده بود.

در واقع این تروجان به منظور دستیابی به اطلاعات سیستم‌های قربانی و سرقت اطلاعات اعتباری، پست الکترونیکی و شبکه‌های اجتماعی ایجاد شده بود و کارکرد آن به این شکل نبود که همه نوع اطلاعات قابل جمع‌آوری در آن ذخیره شود بلکه مشخصات سیستم استفاده شده و اطلاعات بانکی و اینترنتی مرورگر مورد علاقه این بدافزار بود.

شعله آتش در تجهیزات نفتی

به گزارش همشهری آنلاین^۱، پس از حمله ناموفق سایبری به سامانه اینترنت، اینترنت و مخابراتی مخابراتی مجموعه وزارت نفت در روزهای نخست اردیبهشت ماه سال ۱۳۹۱، یک گروه از هک‌های عربستان سعودی به سایت یکی از شرکت‌های نفتی ایران حمله کرد. بر این اساس سایت اطلاع‌رسانی شرکت نفت ایرانول روز گذشته توسط یک گروه از هک‌های عربستان سعودی (HP GROUUP) (HACK) و از دسترس خارج شده است. یکشنبه سوم اردیبهشت ماه هم گروه ناشناسی به سامانه اصلی اینترنت و مخابرات شرکت ملی نفت ایران حمله کردند و اختلالاتی در سطح این شرکت ایجاد کردند. به تازگی شبکه اینترنت برخی از شرکت‌های تابع ملی نفت برای مدت چند روز قطع شد. اما در این مدت یکی از جدی‌ترین حملات سایبری حمله‌ای بود که نسبت به تجهیزات نفتی کشورهای خاورمیانه صورت گرفت. این بدافزار که با نام فلیم (شعله آتش) به کشورهای مختلفی ارسال شده بود، پیچیدگی‌های متعددی داشت و علاوه بر جاسوسی، یک ویروس مخرب به شمار می‌رفت.

چند روز پس از انتشار اخبار مربوط به این بدافزار، مرکز ماهر مدعی شد که برای نخستین بار در دنیا، ابزار پاک‌سازی بدافزار Flame^۱ تولیدی به زودی از طریق سایت مرکز ماهر در اختیار کاربران قرار خواهد داد.

شعله آتش از جمله بدافزارهای پیچیده‌ای محسوب می‌شد که از طریق ۴۳ آنتی ویروس مختلف، امکان شناسایی این بدافزار وجود نداشت. علاوه بر ایران در لبنان، فلسطین، مجارستان، لبنان، استرالیا، سوریه، روسیه، هنگ کنگ و امارات از جمله کشورهایی بودند که مورد هدف این بدافزار قرار گرفتند.

اواخر تیرماه امسال بود یک ویروس که بیش از هشت ماه از شروع فعالیت آن می‌گذشت، شناسایی شد و اینگونه اعلام شد که حدود ۸۰۰ رایانه توسط این بدافزار آلوده شده است.

^۱ - منبع: همشهری آنلاین (www.hamshahrionline.ir/news) چاپ شده در تاریخ پنجشنبه ۴ خرداد

مینی فلیم

اوایل مهر ماه امسال و در شرایطی که تنها چند ماه از انتشار بدافزارهایی مانند فلیم و گاوس می گذشت این بار بدافزاری با نام مینی فلیم جاسوسی خود را آغاز کرد.

در ارتباط با این بدافزار اینگونه اعلام شده بود که مینی فلیم در واقع شکلی جدید از بدافزار فلیم است که توسط حکومت‌ها پشتیبانی می‌شود و به‌طور خاص برای جاسوسی طراحی شده و جایی که کار فلیم تمام می‌شود این بدافزار آغاز به کار می‌کند.^۲

در توضیحات «کسپرسکای» درباره مینی فلیم آمده بود: «پس از اینکه داده‌ها جمع‌آوری و بازبینی شدند، با قبایلی جالب توجه انتخاب شده و شناسایی می‌شود. سپس مینی فلیم بر روی سیستم قربانی انتخاب نصب می‌شود تا به نظارت عمیق‌تر و جاسوسی دقیق‌تر ادامه دهد».

شبیه حملات فوج در دستگاه‌ها یا شرکت‌های دولتی ممکن است اتفاق بیفتد. لذا آموزش و آگاه‌سازی مدیران و کارکنان در این خصوص اهمیت زیادی پیدا کرده است.

هدف از تدوین این سری کتاب‌ها شناسایی ابعاد مختلف جنگ سایبر و تهدیدات در فضای مجازی بوده. در ادامه، به مستندات قانونی سیاست ملی کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات اشاره می‌گردد:

در بند ۱۱ سیاست‌های کلی نظام، ابلاغ شده در حد رخصت پدافند غیرعامل این چنین آمده است:^۲

«اصول و ضوابط مقابله با تهدیدات نرم‌افزار و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و باندها»

سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)^۳ ابلاغ

شده از سوی رهبر انقلاب:

۱- ایجاد نظام جامع و فراگیر در سطح ملی و ساز و کار مناسب برای این‌سازی ساختارهای حیاتی، حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به منظور:

^۲ - منبع: همشهری آنلاین (www.hamshahrionline.ir/news) چاپ شده در تاریخ ۴ خرداد ۱۳۹۱

^۳ - این سیاست‌ها که در ۱۳ بند در جلسات مجمع تشخیص مصلحت نظام به تصویب رسیده و از سوی مقام معظم رهبری ابلاغ شده است.

^۴ - ویژه نامه نخستین همایش ملی دفاع سایبری - پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی - سال ۱۳۹۰

- استمرار خدمات عمومی پایداری زیر ساخت های ملی ، صیانت از اسرار کشور ، حفظ فرهنگ و هویت اسلامی- ایرانی و ارزش ها، حراست از حریم خصوصی و آزادی های مشروع و سرمایه های مادی و معنوی .

۲- توسعه فن آوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی.

۳- ارتقاء سطح دانش و ظرفیت های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی.

۴- تکیه بر فناوری بومی و توانمند های تخصصی داخلی در توسعه زیرساخت های علمی و فنی امنیت شبکه های الکترونیکی و سامانه های اطلاعاتی و ارتباطی.

۵- پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هر گونه تهدید در حوزه فناوری اطلاعات و ارتباطات.

۶- تعامل و برقراری روابط با مراکز منطقه ای و جهانی، همکاری و سرمایه گذاری مشارکت در حوزه های دانش، فناوری و فنون مرتبط به امنیت شبکه های الکترونیکی و سامانه های اطلاعاتی و ارتباطی با حفظ منافع و امنیت ملی.

۷- تعیین نهاد متولی و هماهنگ کننده زیر نظر دولت به منظور هدایت، نظارت و تدوین استاندارد های لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیه پیش نویس قوانین مورد نیاز.

۸- فرهنگ سازی، آموزش و افزایش آگاهی و مهارت های عمومی در حوزه افتا.

۹- رعایت موازین شرعی و مقررات قانونی مربوط به حفظ حقوق فردی و اجتماعی در اجرای این سیاست ها.

بخش های ترجمه شده در این کتاب برگرفته از دیدگاه های نویسنده اصلی متن بوده و بیانگر تحلیل صاحب نظران در باره تروریسم و جنگ سایبری جامعه جهانی می باشد. لذا با بهره برداری حکیمانه و تحلیلی فنی از مطالب علمی آن می توان از تهدیدات سایبری دیدگاه های اجتماعی و فنی آگاه شد و راهکار های ایمن سازی فضای سایبر را آموخت.

این مجموعه در چهار جلد تنظیم گردیده که بخش یک در جلد اول ، بخش های دو و سه آن در جلد دوم چاپ شده و بخش های بعدی در جلد سوم و چهارم چاپ گردیده و چاپ های اول مورد استقبال محققین در این حوزه قرار گرفته و سه جلد آن بیش از دو بار چاپ شده است.

فهرست مطالب

..... جلد اول

مقدمه	۱۵
بخش اول - اصطلاحات، مفاهیم و تعاریف	۲۳
فصل ۱ حملات تروریسم سایر	۲۷
فصل ۲ تدبیر دانش، تروریسم و تروریسم سایر	۳۷
فصل ۳ ده روند در جنگ اطلاعات	۴۹
فصل ۴ بیت و بایتهای در مقابل گلوله‌ها و بمب‌ها: شکلی نوین از جنگ	۶۳
فصل ۵ زیرساخت‌های جنگ سایر	۷۵
فصل ۶ تروریسم و اینترنت	۸۷
فصل ۷ پنهان نگاری	۹۳
فصل ۸ رمزنگاری	۱۰۵
فصل ۹ یک نقشه راه برای ارائه فرایندهای مطمئن فناوری اطلاعات	۱۲۱

..... جلد دوم

مقدمه	۱۵۵
بخش دوم: جنبه‌های پویای جنگ سایر	۱۵۷
فصل ۱۰ موضوعات کلیدی در حوزه مسائل اقتصادی امنیت سایر	۱۵۹
فصل ۱۱ نقش اشتراک اطلاعات مالی و مراکز تجزیه و تحلیل	۱۶۵
فصل ۱۲ فریب در حملات سایر	۱۷۷
فصل ۱۳ فریب در دفاع از سیستم‌های رایانه‌ای در مقابل حملات	۱۸۷
فصل ۱۴ اصول اخلاقی حملات جنگ سایر	۱۹۷
فصل ۱۵ برون سپاری بین‌المللی، اطلاعات شخصی و حملات سایر	۲۰۵
فصل ۱۶ گردآوری اطلاعات شبکه بصورت غیر فعال	۲۱۵

فصل ۱۷ مدیریت پول الکترونیک در تجارت مدرن مبتنی بر شبکه.....	۲۲۹
فصل ۱۸ تحلیل روش های پول شویی.....	۲۳۹
فصل ۱۹ اسپم، اسپیم و تبلیغات غیر مجاز.....	۲۴۹
فصل ۲۰ نرم افزار پشت پرده: اسب تروجان.....	۲۵۹
فصل ۲۱ آلوده سازی کد SQL: شایع ترین روش برای حمله به پایگاه داده.....	۲۶۷

بخش سوم - جنبه‌های انسانی جنگ سایبر و تروریسم سایبر.....	۲۷۹
فصل ۲۲ نظارت الکترونیکی و حقوق شهروندی.....	۲۸۱
فصل ۲۳ مهندسی اجتماعی.....	۲۹۵
فصل ۲۴ مهندسی اجتماعی.....	۳۰۹
فصل ۲۵ امنیت اطلاعات در بازار.....	۳۲۱
فصل ۲۶ گامی بسوی یک درخت منطق تر از شناسایی ناهنجاری افراد.....	۳۲۹
فصل ۲۷ کمین های سایبری: چالشی برای امنیت وب.....	۳۴۱

جلد سوم

بخش چهارم - جنبه‌های فنی کنترل حملات سایبر.....	۳۶۵
فصل ۲۸ مدل‌های امنیت سایبر.....	۳۶۷
فصل ۲۹ دفاع سایبر: تلفیق امنیت در فرایند ایجاد سیستم.....	۳۸۳
فصل ۳۰ رویکرد های ضد اسپم در برابر جنگ اطلاعات.....	۳۹۷
فصل ۳۱ حملات انکار خدمت (DOS): جلوگیری، کشف نفوذ و کاهش آن.....	۴۰۷
فصل ۳۲ پایش زیرساخت های حیاتی دیجیتال در مقیاس وسیع.....	۴۲۱
فصل ۳۳ زیرساخت های کلیدی عمومی به عنوان ابزاری برای افزایش امنیت شبکه.....	۴۲۹
فصل ۳۴ استفاده از سیستم اطلاعات جغرافیایی در جنگ سایبر.....	۴۳۹
فصل ۳۵ استفاده از تصویربرداری سنجش از راه دور در جنگ سایبر.....	۴۴۷

بخش پنجم - تشخیص هویت، تصدیق اعتبار و کنترل دسترسی	۴۵۵
فصل ۳۶ هک و استراق سمع	۴۵۷
فصل ۳۷ مدل‌های کنترل دسترسی	۴۶۹
فصل ۳۸ مروری بر سیستم کشف نفوذ با استفاده از کشف حالت غیر عادی	۴۷۹
فصل ۳۹ مسلسل بیهوشی: حالت جدیدی از دسترسی تأیید هویت با استفاده از VEP	۴۹۱
فصل ۴۰ تعیین سیاست‌های مبتنی بر محتوی، برای مدل کنترل دسترسی و اعطای مجوز	۴۹۷
فصل ۴۱ داده کاوی	۵۱۱
فصل ۴۲ سنسایی و محل یابی آدرس های دیجیتال در اینترنت	۵۱۹
فصل ۴۳ تشخیص هویت با استفاده از داده کاوی	۵۲۷
بخش ششم استعمار کسب و کار	۵۳۳
فصل ۴۴ مدلی برای سامانه‌های واکاوی اضطرار	۵۳۵
فصل ۴۵ تکنیک‌های انحراف دهنده تشخیص (پیشی)	۵۴۵
فصل ۴۶ بازرسی علمی جرم سایبری	۵۵۱
فصل ۴۷ توان مقابله (پایداری) اجزاء نرم افزار در حمله اطلاعات	۵۵۹
فصل ۴۸ طبقه‌بندی وقایع مرتبط با امنیت رایانه	۵۶۹
کتابنامه	۵۷۶