آشنایی با جنگ نرم

جنگ سایبر (۳)

تألیف و گردآوری:
محمد ابراهیم‌نژاد
حمید اسکندری

انتشارات

سرشناسه : ابراهیم‌نژاد شلمانی، محمد، ۱۳۵۶
عنوان و نام پدیدآور : آشنایی با جنگ نرم: جنگ سایبر/ تدوین و گردآوری محمد ابراهیم‌نژاد، حمید اسکندری.
مشخصات نشر : تهران: بوستان حمید، ۱۳۹۰-
مشخصات ظاهری : ج.: مصور ، جدول ، نمودار.
شابک : دوره: ۴-۱-۹۲۲۹۳-۶۰۰-۹۷۸ ؛ ج.۱: ۷-۰-۹۲۲۹۳-۶۰۰-۹۷۸ ،
ج.۲: ۲-۰۹-۶۴۱۲-۶۰۰-۹۷۸ ، ج.۳: ۰-۱۶-۶۴۱۲-۶۰۰-۹۷۸
وضعیت فهرست نویسی: فیپا
یادداشت : ج.۲. (چاپ اول: زمستان ۱۳۹۰).
یادداشت : ج.۲. (چاپ دوم: ۱۳۹۲).(فیپا)
یادداشت : ج.۳. (چاپ اول: ۱۳۹۲) (فیپا)
یادداشت : کتابنامه
عنوان دیگر : جنگ سایبر
موضوع : جنگ نرم
موضوع : جنگ اطلاعاتی
موضوع : ترویسم رایانه‌ای
شناسه افزوده : اسکندری، حمید، ۱۳۳۸ - گرد آورنده
رده بندی کنگره : ۳۹۰ آ ۵ الف ۱ UB۲۱۰
رده بندی دیویی : ۳۳۴/۳۵۵
شماره کتابشناسی ملی : ۲۲۹۸۲۶۶

انتشارات بوستان حمید

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

تلفن ناشر و پخش کتاب: ۶۶۴۸۲۳۸۹ ۰۹۱۲۲۳۷۵۰۳۹ ۰۹۱۲۷۷۵۷۸۳۸
فروشگاه اینترنتی: boostanhamid-pub.ir «این کتاب با کاغذ حمایتی منتشرشده 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 بیندازند.

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 بخش هایی از مراکز حساس مانند نفت، صنعت، بانک و ... 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 و 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 این‌که هجوم کرم جاسوس استاکس نت به رایانه‌های ایرانی می‌تواند دارای دلایل اقتصادی یا سیاسی باشد، گفت: آلودگی ناشی از 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 می توان 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[1]، پس از حمله ناموفق سایبری به سامانه اینترنت، اینترانت و مخابراتی مخابراتی مجموعه وزارت نفت در روزهای نخست اردیبهشت ماه سال ۱۳۹۱، یک گروه از هکرهای عربستان سعودی به سایت یکی از شرکت‌های نفتی ایران حمله کرد. بر این اساس سایت اطلاع رسانی شرکت نفت ایرانول روز گذشته توسط یک گروه از هکرهای عربستان سعودی (HP GROUUP (HACKهک 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 طوریکه شبکه اینترنت برخی از شرکت‌های تابع ملی نفت برای مدت چند روز قطع شد .

اما در این مدت یکی از جدی ترین 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 تعددی داشت و علاوه بر جاسوسی، یک ویروس مخرب به شمار می رفت.

چند روز پس از انتشار اخبار مربوط به این بدافزار، مرکز ماهر مدعی شد که برای نخستین بار در دنیا، ابزار پاک‌سازی بدافزار Flame را تولید و 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 این حوزه، 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.

---

[1] – منبع: همشهری آنلاین(www.hamshahrionline.ir/news) چاپ شده در تاریخ پنجشنبه ۴ خرداد ۱۳۹۱ –

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 می شود این بدافزار آغاز به کار می کند.[۲]

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

شبیه حملات فوق در دستگاه ها یا شرکت های دولتی ممکن است اتفاق بیفتد. لذا آموزش و آگاه سازی مدیران و کارکنان در این خصوص اهمیت زیادی پیدا کرده است.

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

در بند ۱۱ سیاست‌های کلی نظام، ابلاغ شده در حضرت پدافند غیرعامل این چنین آمده است:[۳]

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

سیاست های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا)[۴] ابلاغ شده از سوی رهبر انقلاب:

۱- ایجاد نظام جامع و فراگیر در سطح ملی و ساز و کار مناسب برای ایمن سازی ساختار های حیاتی، حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقاء مداوم امنیت شبکه های الکترونیکی و سامانه های 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- پیش ، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هر گونه تهدید در حوزه فناوری اطلاعات و ارتباطات.

۶- تعامل مؤثر و سازنده منطقه ای و جهانی، همکاری و سرمایه گذاری مشارکت در حوزه های دانش، فناوری مربوط 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 نظردولت به منظور هدایت، نظارت و تدوین استاندارد های لازم برای حفظ و توسعه امنیت فضای تولید وتبادل 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 را هکار 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