معرفی بدافزارها و ارائه الگوریتم‌های تشخیص

مولفین

فریدون رضایی

سعید رضایی

محسن طاهریان

علی افراز

NAGHOOS
PUBLICATION

سرشناسه : رضایی، فریدون، ۱۳۵۲-
عنوان و نام پدیدآور : معرفی بدافزارها و ارائه الگوریتم‌های تشخیص
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۳.
مشخصات ظاهری : ۱۵۸ ص.: مصور، جدول.
شابک : ۷-۷۵۱-۳۷۷-۹۶۴- ۹۷۸ بها: ۱۱۰.۰۰۰ ریال به همراه DVD
وضعیت فهرست‌نویسی : فیپای مختصر
یادداشت : این مدرک در آدرس http://opac.nlai.ir قابل دسترسی است.
یادداشت : مولفین: فریدون رضایی، سعید رضایی، محسن طاهریان، علی افراز
شمارهٔ کتابشناسی ملی : ۳۷۶۶۱۱۱

برای خرید Online به آدرس زیر مراجعه کنید:
www.naqhoospress.ir

انتشارات ناقوس
NAGHOOS PUBLICATION

نام کتاب : معرفی بدافزارها و ارائه الگوریتم‌های تشخیص
ناشر : انتشارات ناقوس
مؤلفین : فریدون رضایی، سعید رضایی
محسن طاهریان و علی افراز
چاپ اول : ۱۳۹۳
تیراژ : ۲۰۰ جلد
چاپ و صحافی : نارنجستان
سرپرست صفحه‌آرا : صدف پورعبدی
قیمت به همراه DVD : ۱۱۰.۰۰۰ ریال
شابک : ۷-۷۵۱-۳۷۷-۹۶۴- ۹۷۸
ISBN : 978-964-377-751-7

چاپ اول

« در نوبت چاپ اول از دستگاه چاپ دیجیتال استفاده شده است »

S.M.S : ۳۰۰۰۲۵۲۳۱۳۰

مراکز پخش:
۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگرجنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲
تلفن و فاکس: ۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳
۲- کتابفروشی گلریزان، ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰
۳- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

مقدمه مؤلفان

روند تکامل ویروس‌ها یا همان بدافزارهای کامپیوتری نشاندهندهٔ رشد فزآینده و افزایش هوشمندی آنها می‌باشد. این روزها تشخیص ویروس‌ها یکی از مهمترین کارهای علم کامپیوتر شده است که شرکت-های بزرگی همچون مایکروسافت، کاسپرسکی و سیمانتیک، آویرا و ... تیم‌های توانمندی را برای نوشتن آنتی‌ویروس ایجاد کرده‌اند.

در این کتاب که مقدمه‌ای بر این علم وسیع می‌باشد، شما را با انواع بدافزارها و تعدادی از الگوریتم‌های تشخیص آنها، آشنا خواهیم کرد.در مقدمه کتاب یا پیش زمینه مفهوم تهدید سایبری و دلایل اهمیت کار بر روی برنامه های تشخیص بدافزار شرح داده شده است. در فصل اول تعاریف بدافزار و روش‌های کلی تشخیص بدافزار گفته شده است. در فصل دوم ساختار فایل‌های اجرایی در ویندوز با جزئیات شرح داده شده است و سه پروژه مختلف در این زمینه توضیح و شرح داده شده است. فصل سوم به بررسی ساختار Packer ها پرداخته است و چهار پروژه مختلف در آن ارائه شده است. در فصل چهارم مفهوم Binder بررسی و یک پروژه در رابطه با آن ارائه شده است. در فصل های پنجم و ششم مدل مخفی مارکف و الگوریتم‌های سنجش تشابه که از روابط آن ها در الگوریتم های تشخیص استفاده می‌شود به طور کامل توضیح داده شده‌اند. در فصل هفتم راهکارهای تشخیص بدافزار به همراه دو الگوریتم تشخیص شرح داده شده‌اند. در این کتاب در مجموع هشت پروژه مختلف در محیط visual C++ ارائه شده است . تمامی فایل‌های مورد نیاز فصل‌ها به همراه پروژه‌ها و همچنین برنامه Visual studio 2012 در DVD همراه کتاب قرار دارد.

قطعاً این کتاب خالی از اشکال نبوده و از تمامی خوانندگان، پژوهشگران و اساتید گرانقدر خواهشمندیم پیشنهادات، انتقادات و نقطه نظرات خود را با ایمیل‌های زیر با مؤلفین مطرح کنند.

Fereidoon.rezaei@aosmd.ir

Saeid.rezaei@aosmd.ir

info@aosmd.ir

در انتها جا دارد که از اساتید ارجمند بخصوص جناب آقای دکتر قرائی، دکتر پاینده و همچنین دوستان عزیز جناب آقای اصغر غلامی، اسماعیل شعبانلو، دکتر محمد جواد شامانی، مهندس داود سیاوشی، مهندس شایان هنربخش، مهندس امین محمدی، امین زمانی، نعیم فرخزاد، جلال‌الدین آقازاده، سرکار خانم پریسا بی‌خویش و فرشته رضائی کمال تشکر و قدردانی را داریم. همچنین از مدیریت و کارکنان انتشارات ناقوس به خصوص آقایان تجملی و پورحسین و خانم پورعبدی بابت زحمات بسیار در چاپ کتاب تشکر و قدردانی می‌کنیم.

به امید موفقیت

فهرست مطالب

مقدمه

تهدیدات سایبری

مفهوم تهدیدهای سایبری

در همایشی که در ۲ مارس ۲۰۱۰ از سوی مؤسسه بین‌المللی (CACI) و مؤسسه مطالعاتی نیروی دریایی ایالات‌متحده با عنوان «تهدیدهای سایبری امنیت‌ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزارشد، تهدیدهای سایبری به صورت«وقایعی که به صورت طبیعی و یا توسط انسان (به صورت عمدی یا غیرعمدی) بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد» تعریف شد.

انواع تهدیدات سایبری

در ادامه انواع تهدیدات سایبری با ذکر مثالی برای هر کدام بیان می‌شود.

جاسوسی سایبری

جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع‌آوری کند. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی. اسناد منتشر شده از سوی ادوارد اسنودن نشان می‌دهد زمانی که شرکت‌های رایانه‌ای برای ارائه خدمات بهتر به کاربران در زمینه تبلیغات اقدام می‌کنند، زمینه لازم برای آژانس امنیت ملی آمریکا فراهم می‌شود تا بتواند با استفاده از فایل‌های کوکی در اینترنت اهداف سایبری خود را هدف حملات هکری و جاسوسی قرار دهد. براساس این گزارش اسناد فاش شده توسط اسنودن در زمینه اقدام آژانس امنیت ملی آمریکا در جاسوسی تجاری و بازرگانی از کاربران سایبری می تواند مباحث جدیدی را در زمینه جاسوسی تجاری و اقتصادی به وجود آورد. بر اساس این اسناد، سازمان امنیت ملی آمریکا به همراه سازمان جاسوسی انگلیس با استفاده از فایل‌های کوکی که در زمینه تبلیغات کاربری دارند، اقدام به شناسایی و جاسوسی از افراد فعال در فضای اینترنت کرده‌اند. نهادهای جاسوسی انگلیس و آمریکا با استفاده از مکانیسم خاصی در گوگل موسوم به "کوکی‌پرف" اقدام به جاسوسی سایبری از کاربران کرده‌اند.

فایل‌های کوکی معمولا حاوی اطلاعات شخصی نیستند ولی این فایل‌ها حاوی کدهای ویژه ای هستند که وب‌سایت‌ها را قادر می‌سازد تا به هویت کاربران اینترنتی و اطلاعات آنها دسترسی داشته‌باشند. علاوه بر شناسایی و رهگیری کاربران یک وبسایت فایل‌های کوکی این اجازه را به سازمان امنیت ملی آمریکا داده‌است تا با ارسال نرم‌افزارهای خاصی اقدام به هک کردن سیستم‌های رایانه‌ای اهداف خود در سراسر جهان کنند. این اسناد همچنین نشان می‌دهد که سازمان امنیت ملی آمریکا با استفاده از اطلاعات تجاری جمع‌آوری‌شده برای جاسوسی و رهگیری مکالمات تلفن همراه در سراسر جهان استفاده کرده‌است. بسیاری از گوشی‌های آیفون و آندروید و همچنین سیستم عامل‌های گوگل و اپل بدون آنکه هشداری را به کاربران خود بدهند، زمینه لازم برای جاسوسی و رهگیری سازمان امنیت ملی آمریکا را فراهم کرده‌اند.

جنگ سایبری

جنگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی توانیم آن را به طور کامل درک کنیم در عین حال، روشن است که در دنیای امروز، میدان جنگ حوزه خود را به فضای مجازی گسترش داده و باید آن را به عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین،هوا، دریا و فضا در نظر گرفت. از نمونه‌های معروف جنگ سایبری می‌توان به جنگ سایبری بین آمریکا و چین اشاره کرد. نزدیک به ۱۰۰ حمله سایبری بین آمریکا و چین درگرفته است که مشهورترین آنها در مارس و آوریل سال ۲۰۰۱ بوده است و دامنه‌های آن تا حدودی به اروپا نیز کشیده شد. این جنگ بر سر موضوع تصادم هواپیمای جاسوسی آمریکا با جت چینی بوده است با حمله‌های کنترل از راه دور به سایت دولت چین آغاز گردید و در نهایت این حملات منجر به تخریب اطلاعات، دزدیدن و صدمه به منافع و سرورهای دو کشور شد. درصد تخریب حاصل از این جنگ در چین، ۱۰ برابر آمریکا بود.

تروریسم سایبری

آژانس مدیریت فوق‌العاده فدرال، تروریسم سایبری را اینگونه تعریف می‌کند: تهدید وحمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن، زمانی که برای ترساندن یا مجبورکردن حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد. ایران در دهه‌های اخیر همواره یکی از قربانیان تروریسم بوده است که در زمینه تروریسم سایبری هم شاهد یکی از بزرگترین حملات در قالب بدافزار استاکس‌نت بوده است. در ۲۶ سپتامبر سال ۲۰۰۹ میلادی مسئولان نیروگاه اتمی بوشهر از ویروسی شدن سیستم‌های نیروگاه سخن گفتند، اما تاکید کردند، این موضوع موجب از کار افتادن کامل سیستم‌های رایانه‌ای نیروگاه نشده‌است. پس از آن یک پایگاه اطلاع‌رسانی روسی به نقل از (یوگنی کسپرسکی)، کارشناس روس و یکی از معروف ترین دانشمندان علوم رایانه ای جهان اعلام کرد که دنیا وارد عرصه جدیدی از جنگ‌ها شده که تسلیحات به کار رفته در آن ویروس‌ها هستند و به این ترتیب اعلام کرد که قرن بیست و یک بیش از هر چیز با اصطلاحات و واژه‌های همچون "تروریسم الکترونیکی" و "سلاح الکترونیکی" و "جنگ‌های الکترونیکی" مواجه خواهد بود.

مشخصات ویروسی که واحدهای صنعتی را آلوده کرده است	
نام ویروس	استاکسنت
تعداد کامپیوترهای آلوده شده	۱۵ تا ۲۰ هزار دستگاه
نقاط هدف	واحدهای صنعتی بزرگ
سیستم های مورد هدف	نرم افزار مدیریت سیستم کنترل زیمنس
کشورهای مورد هدف	ایران، هند و اندونزی
اولین مورد کشف شده	ایران
احتمالات دلایل انتشار	جاسوسی صنعتی، تروریسم صنعتی، ناراضایتی کارکنان
عملکرد	ربایش و انتشار اطلاعات محرمانه صنعتی
شکل گسترش	از طریق پورت USB و اینترنت
میزان خطرپذیری	بسیار بالا (برای واحدهای صنعتی)

شکل ۱مشخصات عمومی بدافزار اکستاکس‌نت

بدافزار اکستاکس‌نت پیشرفته‌ترین سلاح سایبری است که تاکنون ساخته شده‌است. معاینات این کرم نشان می‌دهد که آن موشکی سایبری است که برای نفوذ در سیستم‌های امنیتی پیشرفته طراحی شده است. این موشک سایبری مجهز به کلاهکی است که نشانه روی شده و کنترل سیستم‌های سانتریفیوژدر مرکز فرآوری اورانیوم نطنز را در دست می گیرد و کلاهک دومی دارد که توربین عظیم راکتور بوشهر را هدف می گیرد. پس از آزمایش‌های گستردهٔ استاکس‌نت توسط چند شرکت امنیتی، این مساله محرز شده است که هدف استاکس‌نت آسیب رساندن به سامانه‌های خاصی است که بر اساس نرم‌افزارهای شرکت زیمنس کار کرده و از دو نوع قطعهٔ سخت‌افزاری خاص استفاده می‌نماید که فقط در ایران و فنلاند استفاده می‌شود. دولت فنلاند تا کنون عکس‌العملی نسبت به این مساله نشان نداده و گزارش‌ها نیز این کشور را به عنوان محل آلودگی گسترده معرفی نمی‌کنند در حالی که ایران در تمام بازهٔ ۲۰۰۹ – ۲۰۱۰ که اکستاکس‌نت در حال انتشار بود همواره در کنار هند و اندونزی یکی از سه کشور بالای فهرست آلودگی بوده است تا سرانجام در اواخر ۲۰۱۰ فاصله ایران با بقیه بیشتر شده و بالاترین میزان آلودگی به این ویروس را به ثبت رساند. تحقیقات نشان می دهند که هدف اصلی اکستاکس‌نت از آلوده کردن رایانه‌های صنعتی دسترسی به قطعات سخت افزاری موسوم به پی‌ال‌سی (PLC)است که مستقیما با تجهیزات صنعتی در ارتباط است و ضمن دریافت فرمان از رایانه و انتقال آن به دستگاه، وضعیت دستگاه را به رایانه گزارش می‌دهد. هدف استاکس‌نت، فقط نوع خاصی از پی‌ال‌سی است که توسط شرکت زیمنس و شرکای آن به برخی از شرکت‌های واسط ایرانی فروخته شده است و به همین دلیل، آلودگی رایانه‌ها در سایر نقاط دنیا به این کد مخرب چندان مسئله ی مهمی نیست چون در نهایت به تخریبی منجر نخواهد شد. هدف استاکس‌نت مشخصا شبکه‌های صنعتی ایران بوده‌است. استاکس‌نت پس از آلوده‌کردن رایانه صنعتی متصل به پی‌ال‌سی، به کمک آسیب‌پذیری‌های موجود در نرم‌افزارهای زیمنس که روی این رایانه‌ها نصب شده‌بودند، نرم‌افزار سطح پائین کنترلگر داخل پی‌ال‌سی را دستکاری می‌کند. هدف این دستکاری، گزارش غلط بسامد و دامنهٔ چرخش یکی از قطعات داخلی یک سخت‌افزار خاص می‌باشد تا هم این سخت‌افزار پیش از حد بچرخد و هم اپراتورهای سیستم از این

واقعیت مطلع نشوند. بررسی‌های بعدی نشان داد که ترکیب رایانه‌های صنعتی مورد نظر، پی‌ال‌سی خاص مذکور و سایر تنظیماتی که توسط اکستاکس‌نت به آن‌ها دست‌اندازی می‌شود فقط در چرخه غنی سازی اورانیوم کشور کاربرد دارند. به بیان دیگر، هدف اصلی اکستاکس‌نت، ضربه زدن به سانتریفیوژها به منظور تخریب چرخهٔ غنی‌سازی هسته‌ای است. سانتریفیوژ تنها عنصر چرخهٔ هسته‌ای است که قطعات سخت‌افزاری داخل آن با بسامد بالا می‌چرخد و از پی‌ال‌سی و کانورتورهای[1] خاص مورد نظر اکستاکس‌نت استفاده می‌کند. در صورت بالا رفتن بی‌رویهٔ بسامد و عدم نظارت صحیح (که هر دو از اهداف اکستاکس‌نت می‌باشند) سانتریفیوژ به احتمال زیاد از کار خواهد افتاد گرچه یک رخداد الکترومکانیکی برنامه‌ریزی نشده (که در نیروگاه‌ها و به طور کل سیستم‌های کنترلی امر نادری نیست) حتی ممکن است به انفجار و تخریب کامل منجر شود. در نتیجه هدف اکستاکس‌نت کندکردن چرخهٔ هسته‌ای از طریق از کار انداختن سانتریفیوژها و امیدواری به انفجار کل مرکز غنی‌سازی بوده‌است.

اهمیت کار بر روی ساخت آنتی‌ویروس

پس از بیان مفاهیم فوق، اکنون شاید به اهمیت زیاد ساخت آنتی ویروس در داخل کشور رسیده باشیم. موارد زیر را می توان دلایل اهمیت کار بر روی ساخت آنتی‌ویروس بیان کرد:

۱. ساخت بدافزارهای قوی توسط دشمنان کشور برای وارد کردن آسیب‌های جدی:

ساخت بدافزار اکستاکس‌نت که در بخش قبلی توضیح داده‌شد خود به تنهایی میزان اهمیت برای کار در این زمینه را بیان می‌کند. تا قبل از این موارد بدافزارها توسط گروه‌های تبهکار کوچک طراحی می‌شدند و میزان آسیب‌رسانی آن‌ها در حد پائینی قرار داشت ولی طی چند سال اخیر مسیر جدیدی در این عرصه آغاز شده است. البته به جز اکستاکس‌نت، بدافزارهای زیاد دیگری با هدف خرابکاری‌های گسترده و یا جاسوسی در ابعاد وسیع طراحی شده‌اند که می‌توان در این زمینه به بدافزار فلیم هم اشاره کرد.

۲. تعداد زیاد کاربران سیستم عامل ویندوز در ایران:

طبق برآوردهای موجود بیش از نود درصد کاربران ایرانی از سیستم‌عامل‌های ویندوز شرکت مایکروسافت استفاده می‌کنند. تعداد بدافزارهایی که برای سیستم عامل ویندوز نوشته می‌شود خیلی بیشتر از بدافزارهایی است که برای سیستم عامل لینوکس نوشته می‌شود که حتی خود مایکروسافت در این زمینه اعلام هشدار کرد. رشد میزان بدافزارهای تولید شده برای ویندوز به خصوص از سال ۲۰۱۲ به بعد دارای شیب بسیار زیادی است که اهمیت وجود آنتی‌ویروس در ویندوز را نشان می دهد.

۳. نقش مهم آنتی‌ویروس و خطر وابستگی به محصولات خارجی:

همان‌طور که در بحث اکستاکس نت بیان شد یکی از دلایل اصلی موفقیت اکستاکس‌نت استفاده از آسیب‌پذیری‌های ویندوز بود. متاسفانه استفاده از نرم‌افزارهای تولید خارج ما را در معرض سواستفاده‌های این چنینی قرار می‌دهد. حال با توجه به نقش مهم برنامه آنتی‌ویروس در زمینه دفاع در

---

[1]. Convertor

مقابل حملات، استفاده از آنتی‌ویروس‌های خارجی می‌تواند در طول زمان دارای ریسک بسیار بالا باشد. مانند هر نرم‌افزاری قطعا آنتی‌ویروس‌های خارجی دارای آسیب‌پذیری‌هایی هستند که کاربران مصرف‌کننده، شاید هرگز متوجه آن نشوند.

وضعیت کنونی

با وجود تلاش‌هایی که توسط محققین و پژوهشگران صورت گرفته است تا کنون پروژه خوبی در راستای طراحی، تولید و توسعه آنتی‌ویروس در کشور صورت نگرفته است. مشکلات زیادی در این عرصه وجود دارد که بعضی از آن‌ها عبارتند از:

۱. **مشکلات جمع‌آوری منابع:** یکی از مهم‌ترین مشکلات در تحقیق برای ساخت برنامه آنتی‌ویروس نبود منابع لازم برای تحقیق است. هیچ‌کدام از شرکت‌های ساخت آنتی‌ویروس، کوچکترین اطلاعاتی درباره الگوریتم‌ها و نحوه ساخت و کارکرد برنامه‌هایشان نمی‌دهند. اطلاعات اولیه ساده در این زمینه به طور پراکنده در سایت‌های مختلف است. محققین برای تحقیق نیاز به فایل‌های اجرایی بدافزارها دارند که جستجوی آن زمان زیادی را هدر می‌دهد. برای مثال سایت اینترنتی http://vxheaven.org اقدام به جمع‌آوری بدافزارهای زیادی کرده بود و مورد استفاده محققین قرار می‌گرفت ولی به طور ناگهانی وب سرورهای آن توسط پلیس جنایی اوکراین توقیف شد و محققین تا مدت‌ها هیچ نمونه بدافزاری را روی اینترنت نمی‌توانستند پیدا کنند.

۲. **هدر رفتن زمان زیاد بر روی بحث‌های ابتدایی:** حتی در صورتی که محققین منابع لازم را دسترسی پیدا می‌کردند، به دلیل اطلاع نداشتن از نتیجه تحقیقات و پژوهش‌های افراد قبلی، مجبور به کار برروی بحث‌های ابتدایی و یا زمان گذاشتن بر روی کارهایی که نتیجه آن در تحقیقات قبلی به دست آمده است می‌شدند.

۳. **تعداد کم کاربران استفاده‌کننده از محصولات:** به دلیل این که بسیاری از نتایج پژوهش‌ها در برنامه‌های کاربران پیاده‌سازی نمی‌شود و همچنین عدم اطلاع‌رسانی محصول و ویژگی‌های آن به کاربران، بسیاری از کاربران داخلی همچنان از محصولات خارجی استفاده می‌کنند.