تاریخ دریافت:۱۳۹۷/۱۰/۱۶
تاریخ پذیرش:۱۳۹۷/۱۲/۰۶

فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی- ترویجی
سال سیزدهم، شمارهٔ چهل و نهم، زمستان ۱۳۹۷

مروری بر روش‌های مقابله با بدافزارها و نرم‌افزارهای جاسوسی

(مورد مطالعه بدافزار استاکس‌نت)

علیرضا لرستانی[۱]

چکیده

زمینه و هدف: در دوران کنونی نرم‌افزارهای مخرب و تهدید علیه امنیت داده‌ها و اطلاعات، تبدیل به فرایندی پیچیده‌ای شده است. تنوع این حمله‌ها و تهدیدها سبب ایجاد انواع مختلف روش‌های دفاعی شده که صرف هزینه‌های فراوان را برای شرکت‌ها و سازمان‌های مختلف به‌وجود آورده است. با رشد فنّاوری‌های مربوط مهاجمان این صنعت نیز با به‌کارگیری روش‌های نوین اقدام به تولید بدافزارها و کدهای مخرب برای ناامن‌سازی این فضا و همچنین کسب اطلاعات مختلف برای تأمین نیاز واحدهای نظارتی نموده‌اند. در این بین تولید بدافزارها به‌عنوان یکی از راه‌کارهای مخرب و قوی همواره مورد توجه این مهاجمان و سازمان‌های پشتیبان آنهاست. جمهوری اسلامی ایران به عنوان محور مقابله با استکبار جهانی به دلیل دارا بودن اطلاعات باارزش همواره یکی از هدف‌های اصلی سازمان های اطلاعاتی متخاصم هستند. یکی از قوی‌ترین بدافزارهایی که تا کنون تولید شده است بدافزار استاکس‌نت است که علیه مواضع صنعت هسته‌ای کشور عزیزمان به‌کار گرفته شده است.

روش‌شناسی: در این تحقیق که به روش مروری انجام شده است برای گردآوری داده‌ها از اسناد کتابخانه‌ای و اینترنت بهره گرفته شده است.

یافته‌ها و نتیجه‌گیری: در این تحقیق با بررسی شیوه‌های تشخیص بدافزار و نرم‌افزار جاسوسی، روش‌هایی مناسب برای جلوگیری از نفوذ در سازمان‌های اطلاعاتی مطرح می‌گردد. همچنین یک کالبدشکافی دقیق از بدافزار استاکس‌نت و نحوهٔ راه‌یابی آن به تأسیسات هسته‌ای جمهوری اسلامی ایران ارائه خواهد شد.

کلیدواژه‌ها: استاکس‌نت، بدافزار، سیستم تشخیص نفوذ[۲]، نرم‌افزار جاسوسی.

---

۱. کارشناس ارشد نرم‌افزار دانشگاه پیام نور واحد شمیرانات (رایانامه: Lorestani.reza@gmail.com).

2 Intrusion detection system

مقدمه

در عصر حاضر، خلق فنّاوری‌های جدید و ایجاد فنّاوری نوین امروزی گسترهٔ فعالیت افرادی که در به چالش‌کشیدن امنیت سایبری فعالیت دارند را بیش از پیش پررنگ نموده است. در واقع در دنیای کنونی افرادی را که به‌عنوان نفوذگر شناخته می‌شوند با هدف‌های مختلفی که به‌واسطهٔ آنها اقدام به ایجاد بدافزارهای گوناگون می‌کنند هر روزه امنیت موجود در شبکه‌ها و سامانه های رایانه‌ای را به مخاطره می‌کشانند. با وجود این مطلب تمامی سازمان‌ها و شرکت‌های فعال در حوزهٔ رایانه و سامانه‌های اینترنتی، باید با در نظر گرفتن اهمیت تأمین امنیت، با فعالیت بدافزارها و آثار سوء ناشی از بروز تهدیدهای امنیتی به‌خوبی مقابله کنند (احمدی، ۱۳۹۶).

نرم‌افزارهای جاسوسی[1]، برنامه‌های مخربی هستند که ممکن است توسط مهاجمان، برای کارهای سودجویانه، نفوذ به سامانه‌ها و اثرگذاری بر روی عملکرد آنها، جمع‌آوری اطلاعات مهم و حتی دسترسی به مجوزها مورد استفاده قرار گیرند. همچنان که با روند رو به رشد در استفاده از فنّاوری اطلاعات روبه‌رو هستیم، مهاجمان نیز از آنها به‌عنوان توان قدرتمند برای رسیدن به هدف‌های خود استفاده می‌کنند تا از طریق این امر بتوانند به اطلاعات محرمانه و شخصی کاربران و حتی اطلاعات مربوط به حساب‌های بانکی آنها دسترسی داشته باشند. بایستی توجه داشت که در اکثر مواقع کاربران از برنامه‌های کاربردی، برای دسترسی به اطلاعات شخصی موجود در دستگاه‌ها استفاده می‌کنند. به طور معمول بدافزارها در برنامه‌های کاربردی مختلفی جاسازی می‌شوند؛ حال اگر این‌گونه برنامه‌ها توسط کاربر دریافت و استفاده شوند، مهاجمان خواهند توانست به اطلاعات شخصی کاربران دسترسی داشته باشند (لرستانی، ۱۳۹۶).

---

1 Spyware Software

فعالیت‌های مخرب وارد مرحلهٔ جدیدی شده است که در آن کدهای مخرب به‌جای آلوده‌کردن رایانه‌ها، به‌دنبال سرقت اطلاعات شخصی کاربران به‌منظور سرقت و کلاه‌برداری از آنها هستند. بر همین اساس تعداد و آثار زیان‌بار بدافزارها به طور روزافزون در حال افزایش است. در همین راستا ارائه ابزارهایی که با بررسی فایل‌ها بتوانند تحلیلی روی آنها انجام دهند منجر به شکل‌گیری زمینه‌ای در هوش مصنوعی و فنّاوری اطلاعات گردیده که به تشخیص بدافزار معروف است.

این حوزه تمام فعالیت‌هایی که به‌نوعی به دنبال نفوذ در سامانه هستند را شامل می‌گردد. آنالیز پرونجاها توسط راه‌کنش‌های یادگیری ماشین، یا روش‌های مرتبط دیگر همگی در زمرهٔ تشخیص بدافزار قرار می‌گیرند. یکی از روش‌هایی که ذکر گردید، استفاده از راه‌کنش‌های یادگیری ماشین و داده‌کاوی در این زمینه است (فرضعلی‌وند ۱۳۹۶).

بدافزار برنامه‌ای است که به طور عمده برای انجام فعالیت‌های مخرب مختلف از سرقت اطلاعات کاربر گرفته تا جاسوسی اینترنتی طراحی‌شده است. پویایی رفتاری بدافزار وابسته به عوامل مختلف مانند ماهیت حمله، فنّاوری پیشرفته و افزایش سریع آسیب‌پذیری قابل بهره‌برداری است. حمله های مخرب نیز همراه با رشد سریع در استفاده از دستگاه‌های دیجیتال و اینترنت افزایش‌یافته است. افزایش چشمگیر در نرخ ایجاد نرم‌افزارهای مخرب جدید در پنج سال گذشته روش‌های تشخیص بدافزار را به‌عنوان یک مسئلهٔ مهم تحقیقی مطرح کرده است (Kumar, Kuppusamy & Aghila, 2017).

رشد سریع بدافزار باعث ایجاد تهدیدهای بسیاری در حوزه امنیت اطلاعات شده است؛ بنابراین، مراکز دفاع سایبری اهمیت زیادی در بسیاری از کشورها دارد. همانند مرزهای یک کشور که می‌تواند مورد تهدید و هجوم قرار گیرد، فضای مجازی نیز می‌تواند مورد این تهدیدها قرار گیرد (Ravi, C & Manoharan 2012).

در طول زمان، نرم‌افزارهای مخرب از یک مزاحمت غیرجدی به یک تهدید امنیتی جدی تبدیل‌شده‌اند و به این ترتیب توجه محققان امنیتی از سراسر جهان را به خود

جلب می‌کنند. همهٔ انواع نرم‌افزارهای مخرب باید به‌منظور تعیین رفتار، حالت وخیم بودن و عملیات مورد تجزیه و تحلیل قرار گیرد (Jamalpur, Navya, Raja, Tagore & Rao 2018).

به‌عنوان یک تهدیدِ بسیار شایع، بدافزار به طور گسترده‌ای توانسته است توجه محافل دانشگاهی و متولیان امنیت فنّاوری اطلاعات را به خود جذب نماید. به دلیل تشابه رفتاری بدافزارهای مختلف در هنگام اجرا، می‌توان با تخمین رفتاری پرونجاهایی که قرار است وارد سامانه شوند از ادامهٔ کار پرونجاهای مشکوک ممانعت به عمل آورد. در این تحقیق، ابتدا یک مرور بر تاریخچهٔ کارهایی که در خصوص این موضوع انجام‌گرفته است بیان می‌شود. در بخش دوم انواع مختلف بدافزار با معرفی طبقه‌بندی معروف شرکت کسپرسکی[1] ارائه شده است. در بخش بعدی روش‌های تشخیص بدافزار و مکانیسم اصلی آن توضیح داده می‌شود. سپس بدافزار استاکس‌نت به همراه مکانیسم ساخت و حمله آن به تأسیسات ایران مورد بررسی قرار می‌گیرد. در قسمت پایانی روش‌هایی به‌منظور ممانعت از نفوذ بدافزارهای مشابه در ساختار سازمان‌هایی دارای شبکهٔ اختصاصی بیان می‌شود. نویسنده در این تحقیق به دنبال پاسخ‌گویی به سؤال «بر چه اساسی بدافزارها تشخیص داده می‌شوند و مقابله با تهدیدهای بدافزار بر چه اصولی است؟» می‌باشد.

هدف اصلی: بررسی کلی روش‌های تشخیص و مقابله با بدافزارها و نرم‌افزارهای جاسوسی در سازمان‌های اطلاعاتی

سؤال‌های تحقیق

سؤال اصلی: بر چه اساسی بدافزارها تشخیص داده می‌شوند و مقابله با تهدیدهای بدافزار بر چه اصولی است؟

سؤال‌های فرعی:

۱) کدام روش برای تشخیص بدافزار در سازمان‌های اطلاعاتی مناسب است؟

---

1 Kaspersky

۲) استاکس‌نت به چه طریقی توانست در سامانه‌های هسته‌ای نفوذ کند؟

۳) روش‌های مقابله با نفوذ بدافزارها بر چه اساسی استوار است؟

٤) با چه سازوکاری می‌توان با نفوذ بدافزارهای مشابه استاکس‌نت در سامانه‌های متعلق به سازمان‌های دارای شبکهٔ خصوصی برخورد کرد؟

مبانی نظری: بدافزارها و انواع آنها: بیشتر نرم‌افزارهای مخرب بر پایه و علیه سیستم‌عامل ویندوز طراحی و نوشته می‌شوند و دلیل آن هم وجود آسیب‌پذیری‌ها و ضعف‌های متعدد در ساختار این سیستم‌عامل است که از دیرباز مورد توجه مهاجمان و نگارندگان بدافزارها قرارگرفته است و هم‌اکنون حمله ها از جوانب گوناگون متوجه این سیستم‌عامل است. نرم‌افزارهای مخرب یا بدافزارها رایانه‌ای از جمله موارد اسرارآمیز و مرموز در دنیای رایانه بوده که توجه بیشتر کاربران، برنامه‌نویسان و مشاوران امنیتی شبکه‌های رایانه‌ای و حتی افراد عادی را که از رایانه برای کارهای معمولی خود استفاده می‌کنند به خود جلب کرده است و در بازه‌های مختلف هزینه‌های هنگفتی صرف مبارزه و ممانعت از نشر این نوع نرم‌افزارهای مخرب می‌گردد.

بدافزار یک برنامهٔ متخاصم و سرزده است که بدون کسب اجازه از کاربر دستگاه به‌صورت مخفیانه اقدام به دسترسی به منابع آن می‌کند. این برنامه شامل توابعی مخرب برای صدمه واردکردن به دستگاه است. این برنامه‌ها می‌توانند بدون کسب اجازه وارد دستگاه شده و باعث مداخله در امور سامانه و دست‌کاری در پیکربندی خاص در سیستم‌عامل گردند. به طور معمول کاربرانِ معمولی تمامی این نرم‌افزارهای مخرب را «ویروس» می‌نامند و تفاوتی را از لحاظ عملکرد بین آنها قائل نمی‌شوند، در صورتی که انواع مختلفی از نرم‌افزارهای مخرب در دنیای رایانه وجود دارند و هر کدام دارای عملکردی متفاوت از دیگری هستند. نخستین بدافزار «ویروس» در حدود سال ۱۹۰۰ تشخیص داده شد که آن را کرم رایانه‌ای می‌نامیدند. پس از آن، انواع بدافزارهای دیگر توسط نویسندگان آنها تولید شد که به مرور زمان با استفاده از ابزارها و روش‌های

«مبهم‌سازی» پیچیده‌تر شدند به‌گونه‌ای که امروزه تشخیص آنها بسیار دشوار شده است (لرستانی، ۱۳۹٦: ٤).

با توجه به افزایش تهدیدها از سوی بدافزارها، آشنایی با انواع آنها می‌تواند در شناخت و مقابله با آنها بسیار مؤثر باشد.

بدافزار: در این قسمت ابتدا مفهوم بدافزار، نحوهٔ تشکیل و بازآرایی آن و سپس معرفی گونه‌های اصلی آن به همراه مکانیسم عملکرد در مجموعهٔ هدف تشریح می‌گردد.

الف) مفهوم بدافزار: بدافزارها که در اصطلاح کلی به نرم‌افزارهای مخربی گفته می‌شود که با هدف‌های مختلفی از جمله جمع‌آوری اطلاعات حساس، دسترسی به دستگاه‌های رایانه‌ای خصوصی و در برخی موارد تخریب سامانه‌ها در شکل‌های گوناگون مانند اسکریپت، کد، محتوای فعال و... طراحی‌شده و با کمک عوامل انسانی یا به‌صورت خودکار و به شیوه‌های خاص و رسانه‌های چندگانه در بین رایانه‌ها منتشر می‌شوند.

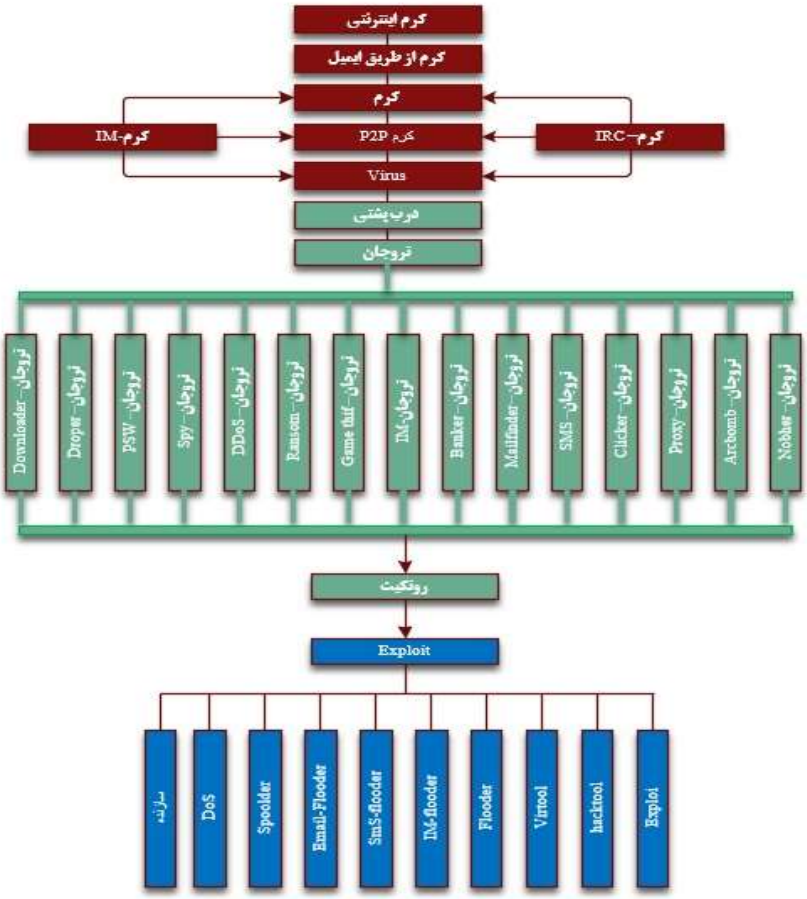
انواع بدافزار: برای دسته‌بندی بدافزارها تقسیم‌بندی‌های مختلفی وجود دارد. یکی از این دسته‌بندی‌ها توسط شرکت کسپرسکی انجام‌شده است.

ویروس[1]: ویروس‌ها دسته‌ای از کدهای مخرب هستند که مشخصهٔ اصلی آنها خودهمتاسازی هنگام اجرا به همراه برنامهٔ میزبان هستند. پس از اجرای یک ویروس، زمینهٔ آلوده کردن دیگر برنامه‌ها یا مستندات نیز فراهم می‌گردد. به برنامه‌ای که کد ویروس به آن افزوده‌شده باشد برنامهٔ آلوده می‌گویند. در واقع نخستین نویسندگان ویروس‌ها متخصصان علوم رایانه در زمان خود بودند و انگیزه‌های متفاوتی برای این کار داشتند. در کل به غیر از بدافزارهایی که تنها باانگیزهٔ مردم‌آزاری نوشته می‌شوند، بدافزارهای فراوانی هم هستند که باانگیزه‌های سیاسی یا مالی به وجود می‌آیند. برای نمونه، بدافزارهایی هستند که در روز خاصی از هر سال حمله‌های خود را به یک نهاد دولتی یا نظامی معطوف می‌کنند و یا بدافزارهایی که با نمایش‌دادن پیام‌هایی به انتقاد از وضعیت سیاسی یا اقتصادی کشور خاصی می‌پردازند (لرستانی، ۱۳۹٦).

---

1 Virus

در ذیل نمودار این تقسیم‌بندی دیده می‌شود:



شکل ۱: دسته‌بندی بدافزارها توسط کسپرسکی

۲- کرم[1]: یکی دیگر از برنامه‌های مخرب کرم‌ها هستند که می‌توانند خود را به طور پنهانی در یک شبکه انتشار داده و منتقل شوند. اثرگذاری کرم‌ها متفاوت از بدافزارهاست چرا که ویروس‌ها برای جابه‌جایی خود نیاز به یک پرونجای کمکی دارند در حالی‌که کرم‌ها با استفاده از شبکه و یا ارسال از طریق رایانامهٔ ناخواسته آلوده، خود را پخش می‌کنند. نمونه‌ای از کرم‌ها، Conficker است.

1 Worm

۳- روت‌کیت‌ها[1]: شامل برنامه‌هایی است که نفوذگر برای گریز از کشف و ردیابی در هنگام دسترسی غیرمجاز به رایانهٔ هدف از آنها استفاده می‌کند. این نوع از نرم‌افزارهای مخرب عملیاتی کلی مانند جابه‌جایی فایل‌های اصلی و کتابخانه‌ای یا نصب ماژول هستهٔ سیستم‌عامل را انجام می‌دهند. نفوذگر ابزار روت‌کیت را پس از دسترسی به مجموعهٔ هدف در سطح یک کاربر مدیر، روی دستگاه نصب می‌کند. این دسترسی می‌تواند از طریق در هم شکستن گذرواژه و با بهره‌گیری از نقاط آسیب‌پذیر دستگاه صورت گیرد. در ادامه نفوذگر اقدام به جمع‌آوری ID کاربران مجموعهٔ هدف از طریق ابزار روت‌کیت می‌کند تا به حساب کاربری اصلی مانند حساب کاربری سطح مدیر[2] دست یابد (داوری دولت‌آبادی، ۱۳۹۳: ٤٦).

تروجان[3]: این دسته از بدافزارها قادر به دست‌یابی از راه دور به رایانهٔ کاربر برای مقاصد خود از جمله جاسوسی و کسب اطلاعات حساس هستند. تروجان‌ها سعی می‌کنند در ابتدا اطلاعات حساسی مانند گذرواژه‌ها را به سرقت برده و فعالیت کاربر را مشاهده کنند و در مراحل بعدی حتی پرونجاهای دستگاهی رایانه را تخریب نمایند.

اکسپلوت[4]: اگر نفوذگری با استفاده از بررسی کردن یک برنامه و یا حتی یک گام جلوتر با اجرای کدهای آن در برنامهٔ خود بتواند خطاهایی را که از دید برنامه‌نویس و گروه نظارت امنیت پنهان مانده است مانند سرریز بافر[5] را کشف کند و همان را تبدیل به حفره‌ای برای نفوذ به دستگاه کند این عمل را استثمارکردن دستگاه نامند که شامل انواع مختلفی است (شکل ۱).

تشخیص بدافزار: بدافزار به طورکلی به نرم‌افزارهایی گفته می‌شود که باعث هرگونه خرابی در رایانهٔ شخصی، خدمات‌دهنده یا شبکهٔ رایانه‌ای شوند. با متداول‌شدن حمله‌ها از این نوع، روش‌های مقابله با ویروس‌ها و جاسوس‌افزارها به سمت مقابله با بدافزارها

---

1 Rootkits
2 Administrator
3 Trojan

٤ معنای لغوی آن استثمارگر (Exploit)

5 Buffer Overflow

هدایت‌شده‌اند و در این زمینه نرم‌افزارهای گوناگونی نیز تهیه‌شده است. در حال حاضر، کاربرد اینترنت به بخش جدایی‌ناپذیری از زندگی مدرن تبدیل‌شده است. مرورگر اینترنت، انواع مختلفی از نرم‌افزارها را بارگیری[1] می‌کند که می‌تواند شامل بدافزار نیز باشد. یکی از اشکالات عمدهٔ استفادهٔ گسترده از اینترنت، آسیب‌پذیری در مقابله با نفوذ بدافزارهاست. نام‌های مختلفی برای بدافزارها مانند کدهای مخرب و برنامه‌های مخرب وجود دارد.

بدافزار یک نرم‌افزار مخرب است که با قصد نقض سیاست سامانهٔ رایانه‌ای با توجه به محرمانه‌بودن، یکپارچگی و در دسترس بودن داده‌ها استفاده می‌شود. این نرم‌افزار می‌تواند هر برنامه‌ای از دستگاه را تغییر دهد و یا حذف کند تا به‌عمد به توابع مورد نیاز دستگاه آسیب برساند. این تهدیدها باعث به وجود آمدن سامانه‌های تشخیص بدافزار شده است. در واقع، سامانهٔ تشخیص بدافزار سامانه‌ای است که برای تعیین این مسئله به کار می‌رود که آیا یک برنامه قصد خرابکاری دارد یا خیر. دستگاه تشخیص شامل دو وظیفه اصلی می‌شود، ۱- تجزیه و تحلیل و ۲- تشخیص (فرضعلی‌وند ۱۳۹۶).

٤- تجزیه و تحلیل بدافزار: روش‌های متنوعی برای تجزیه و تحلیل[2] نرم‌افزار مخرب و روش‌های تشخیص بدافزارها وجود دارند؛ که هدف از تدوین این روش‌ها به حداقل رساندن توزیع برنامه‌های مخرب و یک دسته‌بندی واحد است. روش‌های تشخیص در اصل بر اساس روش تجزیه و تحلیل به‌کار گرفته شده استوار است؛ اما تجزیه و تحلیل یک بدافزار بر اساس سه روش اصلی که شامل روش ایستا[3]، روش پویا[4] و ترکیبی قرار دارد.

روش ایستا: این روش بدون اجرای بدافزار و از طریق مشخصات ساختاری آن، جریان اطلاعات و ویژگی‌های آماری برنامه به‌دست می‌آید. یکی از اصول اصلی در این نوع از تجزیه و تحلیل مهندسی معکوس[5] است؛ اما به دلیل در دسترس‌نبودن کد منبع برنامه روند استفاده از این روش کاهش‌یافته است.

---

1 Download
2 Analysis
3 Static
4 Dynamic
5 Reverse Engineering

در صورت استفاده بدون کد منبع، مجبوریم از تجزیه و تحلیل کدهای دودویی استفاده نماییم که به‌شدت پیچیده است. این روش که به همراه مهندسی معکوس است، کدهای باینری به‌دست‌آمده مورد بررسی قرارگرفته و بدافزارها بر اساس کدهای باینری شناسایی می‌گردند؛ اما استخراج کدهای باینری از بدافزارها کاری دشوار است (نامداری و نورمندی‌پور، ۱۳۹۲).

روش پویا: در مقابل روش تجزیه و تحلیل پویا نیاز به اجرا در یک محیط مجازی دارد. این روش اطلاعاتی را در ارتباط با پایش و جریان داده به ما می‌دهد که موجب درک عمیق‌تری از برنامه می‌گردد؛ اما تجزیه و تحلیل ترکیبی شامل روش‌های ایستا و پویاست. این روش که هدف اصلی استفاده از آن احراز از اشکالات روش‌های ایستا و پویا به‌تنهایی است و تا حد زیادی هم این اشکالات را پوشش می‌دهد هدف اصلی از روش پویا تدوین یک استاندارد برای رفتار بدافزارهاست که امروزه تبدیل به یکی از اصلی‌ترین بخش‌های تحقیقاتی درزمینهٔ فنّاوری اطلاعات گردیده است (نامداری و نورمندی‌پور، ۱۳۹۲).

۵- روش ترکیبی[1]: تجزیه و تحلیل ترکیبی شامل ترکیبی از روش‌ها یعنی ایستا و پویاست. در این روش ابتدا ویژگی‌های امضا، تحلیل می‌شود سپس آن را با پارامترهای رفتاری ترکیب کرده تا تجزیه و تحلیل را تقویت نماید. با توجه به این روش، تحلیل ترکیبی می‌تواند باعث بهبود درک از رفتار بدافزارها شود و در نتیجه نرخ مثبت کاذب را کاهش دهد؛ همچنین روش ترکیبی بر محدودیت‌های تجزیه و تحلیل پویا غلبه می‌کند، زیرا یکی از اشکالات مهم در تجزیه و تحلیل پویا، کندبودن این روش است. امروزه تشخیص بدافزارها مسئله مهمی برای کاربران رایانه است و همواره یکی از مسائل مهم در خصوص امنیت اطلاعات نیز به شمار می‌آید (لرستانی، ۱۳۹۶).

---

1 Hybrid

٦- تشخیص بدافزار: برای ایجاد امنیت کامل در یک دستگاه رایانه علاوه بر دیوارهٔ آتش و دیگر تجهیزات جلوگیری از نفوذ، دستگاه‌های دیگری به نام «سیستم‌های تشخیص نفوذ» مورد نیاز هستند تا بتوانند در صورتی‌که نفوذگر از دیوارهٔ آتش، ضدبدافزار و دیگر تجهیزات امنیتی عبور کرد و وارد دستگاه شد آن را تشخیص داده و چاره‌ای برای آن بیندیشند.

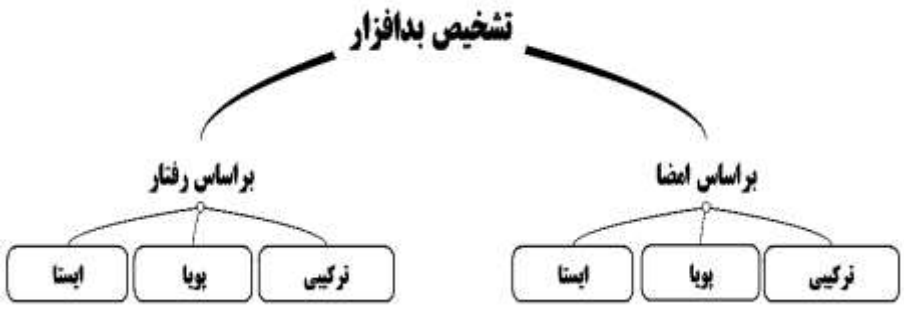
«سیستم‌های تشخیص نفوذ» برای کمک به مدیران امنیتی مجموعه برای کشف نفوذ و حمله به کار گرفته شده‌اند. هدف یک «سیستم تشخیص نفوذ» تنها جلوگیری از حمله نیست بلکه باید به کشف و شاید شناسایی حمله‌ها و تشخیص اشکالات امنیتی در سامانه یا شبکهٔ رایانه‌ای و اعلام آن به مدیر شبکه نیز بپردازد. «سیستم‌های تشخیص نفوذ» در کنار دیواره‌های آتش و به‌صورت مکمل امنیتی برای آنها مورد استفاده قرار می‌گیرند. امروزه دو روش اصلی برای تشخیص نفوذ به شبکه‌ها مورد استفاده قرار می‌گیرد.

الف) مبتنی بر امضا

ب) مبتنی بر رفتار

۷- تشخیص بر اساس امضا: روش تشخیص بر اساس امضا که یک روش با ماهیت ایستاست به این منظور و مقابله با بدافزارهایی با رشد روزانه توسط ضدبدافزارهایی به‌کار گرفته می‌گردد. یک امضا مجموعه‌ای از یک‌رشته باینری منحصربه‌فرد است که از ساختار بدافزار حاصل می شود. این امضا ممکن است از روش‌های ایستا، پویا و ترکیبی حاصل گردد؛ اما به دلیل اینکه هر روز بدافزار جدید ساخته و کشف می‌شوند، لازم است تا امضای مربوط به آنها هم بعد از تولید در پایگاه دادهٔ امضا ذخیره گردد. این به روز رسانی مکرر یکی از نقاط اصلیِ ضعف روش مبتنی بر امضاست؛ که در هر مرحله از به‌روزرسانی تعداد مقایسه‌های بین اعضای پایگاه داده امضا و برنامه مورد بررسی افزایش می‌یابد (Shijo and Salim, 2015).

۸- تشخیص بر اساس رفتار: بر خلاف روش ایستا که بر روی کد بدافزارها تکیه می‌کند، رفتار زمان اجرا را مورد توجه قرار می‌دهد. در واقع تجزیه و تحلیل یک برنامه در زمان اجرای آن را تجزیه و تحلیل پویا می‌نامند که به تجزیه و تحلیل رفتارها نیز معروف است و شامل اجرای نرم‌افزار و مشاهده رفتار آن، تعامل مجموعه و آثار آن روی دستگاه میزبان است. روش تجزیه و تحلیل پویا نیاز به اجرای پرونجاهای آلوده در یک محیط مجازی؛ مانند یک ماشین مجازی، یک شبیه‌ساز جعبه‌شن[1] و... دارد تا بتواند آن را آنالیز کند (نامداری و نورمندی‌پور، ۱۳۹۲).



شکل شمارهٔ ۲: تجزیه تحلیل و تشخیص بدافزار

۹- مقابله با بدافزارها و نرم‌افزارهای جاسوسی: باوجود شبکهٔ اینترنت و رسانه‌های ذخیره‌ساز قابل حمل سرعت انتشار بدافزارها بسیار زیاد شده است حتی با وجود ضدبدافزارهای به‌روز در برخی موارد قادر به پاک‌سازی بدافزارها به‌صورت خودکار نیستیم به دلیل اینکه نویسندگان این‌گونه نرم‌افزارها به طور دائم در حال تلاش برای استفاده از روش‌های دفاعی در برابر ضدبدافزارها و نیز پاک‌کردن دستی آنها هستند. بدافزارهای نگاشته شده در دوره‌های اخیر با استفاده از قوی‌ترین الگوریتم‌های رمزنگاری به دستگاه قربانی نفوذ می‌نمایند. پس از آلوده‌شدن دستگاه بازیابی با مشکلات و هزینهٔ فراوانی انجام خواهد شد؛ بنابراین، بهترین راه مقابله، جلوگیری از آلوده‌شدن به آنهاست.

---

1 Sand box

برای مقابله با نفوذ بدافزارهای جاسوسی موارد ذیل مطرح است:

الف) پیشگیری: مهم‌ترین مسئله در رویارویی با بدافزارها، آگاهی افراد از این تهدید و پیشگیری از آن است.

ب) اطلاع‌رسانی و آموزش کاربران برای پرهیز از رفتار خطرناک: می‌بایست آموزش‌های کافی به کاربران از طریق ویدیوها و بروشورهای آموزشی برای پرهیز از رفتارهای خطرناک نظیر بازکردن پرونجاهای پیوست رایانامه، مراجعه به پایگاه‌های اینترنتی ناشناس یا کلیک روی لینک‌های مشکوک و غیره ارائه شود.

ج) پشتیبان‌گیری منظم: مهم‌ترین و مؤثرترین رکن در مقابله با بدافزارهای باج‌گیر، داشتن پشتیبان‌های منظم دوره‌ای و غیرمتصل است. مقصود از پشتیبان غیرمتصل، این است که رسانه‌هایی که اطلاعات روی آن پشتیبان گرفته می‌شود، باید پس از انجام عملیات پشتیبان‌گیری از سامانه جدا شود تا در صورت آلوده‌شدن به بدافزارها، خود اطلاعات پشتیبان رمزگذاری نشوند. مهم‌ترین داده‌ها عبارت‌اند از:

- سیستم‌عامل‌ها و سامانه‌های فعال
- داده‌های عملیاتی و حساس

بسیاری از بدافزارها به‌خصوص بدافزارهای باج‌گیر علاوه بر رمزکردن پرونجاها و اطلاعات معمول، اطلاعات پشتیبان و حتی پوشه‌های اشتراکی شبکه و مانند آن را نیز رمز می‌کنند تا همهٔ اطلاعات در دسترس رمز شده و قربانی مجبور به پرداخت باج گردد. بدیهی است تنها پشتیبان‌گیری منظم کافی نیست و حتماً باید با انجام بازیابی‌های دوره‌ای از امکان انجام بازیابی صحیح و بدون مشکل در صورت وقوع حوادث اطمینان حاصل نمود. پشتیبان‌گیری تنها روش تضمینی جلوگیری از تهدید بدافزارهای باج‌گیر به شمار می‌رود.

نکته مهم: همچنین باید نسبت به صحت و سلامت کامل نسخه‌های پشتیبان اطمینان حاصل کرد.

الف) امن‌سازی سامانه‌ها

۱. نصب و به‌روز کردن ضدبدافزار
۲. نصب و استفاده از ابزار خاص ضدبدافزار
۳. پیکربندی امن سیستم‌عامل و نرم‌افزارها

به‌روز کردن سیستم‌عامل و نرم‌افزارهای مورد استفاده به‌خصوص مرورگرها و نرم‌افزارهای ارتباطی یا رایج مانند کلاینت رایانامه و مجموعه آفیس[1] و غیره تأثیر بالایی در کاهش ریسک آلودگی به تهدیدهای بدافزاری دارد. امروزه بسیاری از تهدیدهای بدافزاری از طریق روش‌ها و آسیب‌پذیری‌های شناخته‌شده انجام می‌شوند و در نتیجه امن‌سازی و به‌روزبودن می‌تواند حداقل این اطمینان را بدهد که آلوده‌کردن سامانه، کار ساده‌ای نبوده است. به‌خصوص در مورد بدافزارهای باج‌گیر به علت رواج استفاده از کیت‌های حمله[2] در آلوده‌سازی، این مسئله بسیار مهم است. از جمله این امن‌سازی‌ها در بحث شامل موارد ذیل است:

۱) در صورت امکان خدمات دسترسی از را دور[3] غیرفعال شود و یا از سایر روش‌های دسترسی در این خصوص استفاده شود.
۲) به کاربران سازمان حداقل مجوزهای لازم و پایش دسترسی را بدهید به اندازه‌ای که نیاز سازمانی آنها را مرتفع کنند.
۳) از رمزهای قوی استفاده کنید، به طوری‌که با روش‌های کشف رمز عبور مانند حملات دیکشنری به‌راحتی قابل‌شناسایی نباشد.
٤) از فهرست سفید برنامه‌های کاربردی که تنها به برنامه‌های شناس و مورد تأیید، بر اساس سیاست‌های امنیتی اجازهٔ اجرا می‌دهند، استفاده کنید.
۵) برای انجام کارهای روزانه و غیرضروری به‌عنوان کاربر نرمال و یا کاربری غیر از اَدمین[4] در سامانه وارد شوید. خدمات و ورودی‌های غیرضروری را غیرفعال کنید. پنجره‌های پوپوپ‌ها[1] را بر روی مرورگر بلوک کنید.

---

1 Office
2 Exploit kits
3 RDP(Remote Desktop Protocol)
4 Admin

۹- دستگاه تشخیص نفوذ: گسترش روزافزون ارتباط‌های رایانه‌ای و شدآمد ایجاد شده، تأمین امنیت در برابر حمله‌هایی نظیر دست‌کاری اطلاعات، افزودن اطلاعات، استراق‌سمع، قطع ارتباطات کاربر و محرومیت از خدمات امری اجتناب‌ناپذیر است. با توجه به عبور نفوذگرها از دیوار آتش و انواع ضدبدافزارهای تجاری، سامانه‌های تشخیص نفوذ یک ابزار مناسب برای اعلام نفوذ به شبکه برای اتخاذ تدابیر مناسب است. در حوزهٔ شبکه، امنیت، پایش دسترسی و تشخیص به‌موقع با دقت بالا از شدآمد شبکه از مباحث مهم است. در عمل می‌توان مدعی شد هیچ سامانه‌ای امنیت کامل ندارد. دستگاه‌های تشخیص نفوذ برای تشخیص نفوذ به‌موقع در ساختار شبکه بسیار جای خود را بازکرده و نیاز اساسی در هر شبکه‌ای است در این میان محققان به دنبال روش‌های مختلف برای برآورده کردن این نیاز به کشف و طراحی انواع دستگاه‌های خبره به‌منظور پوشش تمامی موارد حمله هستند.

۱۰- روش‌های مناسب برای تشخیص بدافزارها در سازمان‌های اطلاعاتی: در نظر گرفتن ملاحظه‌های اشاره شده مانند یک پدافند غیرعامل سبب می‌گردد تا با صرف هزینهٔ کمتر از وقوع حمله‌ها پیشگیری شود. با توجه به ساختار سازمان‌های اطلاعاتی به‌کارگیری روشی که تمامی جوانب طراحی و تولید یک بدافزار را مورد بررسی قرار دهد مدنظر خواهد بود. (سؤال دوم)؛ بنابراین، استفاده از روش ترکیبی برای سازمان‌های اطلاعاتی با مدنظر قراردادنِ طبقه‌بندی‌های مختلف مطلوب خواهد بود (لرستانی، ۱۳۹۶).

بدافزار استاکس‌نت[2]: ویژگی‌ها و مکانیسم عملکرد: استاکس‌نت به‌عنوان یکی از بدافزارهای معروف نگاشته شدهٔ سایبری است که با هدف ضربه‌زدن به تأسیسات غنی‌سازی اورانیوم کشور عزیزمان ایران و برای متوقف‌ساختن برنامهٔ هسته‌ای توسط دولت‌های آمریکا و رژیم غاصب صهیونیست تولید شد. این بدافزار در نگاه اول یک

1 popup
2 Stuxnet

کرم رایانه و در نگاه دقیق‌تر به‌عنوان یک تروجان است. با توجه به این خاصیت که از کرم به ارث برده قادر خواهد بود تا در دستگاه قربانی نفوذ و به‌تمامی دستگاه‌های مرتبط با آن بسط یابد و با ویژگی تروجان قادر به عبور از انواع سامانه‌های امنیتی و ایجاد درب پشتی[1] زمینهٔ دست‌کاری در دستگاه را فراهم می‌کند. این بدافزار در زمان انتشار با استفاده از نقص امنیتی موجود در رایانه‌های صنعتی اقدام به آلوده‌کردن سامانه‌های رایانه‌ای و سپس اطلاعات مشخص را گرداوری و آنها را به یک سرور ویژه ارسال می‌کند. این بدافزار در سال ۲۰۱۲ توسط ضدبدافزار «وی‌بی‌ای ۳۲»[2] شناسایی و کشف شد. این بدافزار به دستور مستقیم باراک اوباما رئیس‌جمهور وقت آمریکا و با هدف ایجاد نقص امنیتی در سامانه‌ها و جمع‌آوری اطلاعات مشخص و سپس ارسال به یک سرور و در سیستم غنی‌سازی نطنز ایجاد گردید (احمدی، ۱۳۹٦: ۱٤۷).

برای طراحی این بدافزار طبق ادعای روزنامه تایمز ابتدا در مرکز اتمی دی‌مونا و بر روی سانتریفیوژهای مشابه پایگاه نطنز نصب و با شبیه‌سازی اقدام‌های آن به نسخه نهایی آن دست یافتند.

در یک نگاهِ همه جانبه مطالعات صورت گرفته‌شده از جانب شرکت سیمانتک[3] دربارهٔ میزان گسترش بدافزار استاکس‌نت در سطح جهان نشان داد که کشورهای اصلی آسیب‌دیده از این بدافزار ایران، اندونزی و هند بوده است. برابر همین گزارش این بدافزار تمامی دستگاه‌هایی که در بر دارندهٔ مبدلی بسامدی بودند و برای پایش سرعت موتور از آنها استفاده می‌شد را مورد حمله قرار داد و در ادامه به دنبال دستگاه‌های مشابه و با شناسایی دستگاه‌هایی با بسامد ۸۰۰ تا ۱۲۰۰ آنها را نشانه‌گذاری و در یک بازهٔ بسامد را تا ۱٤۰۰ بالابرده و در بازهٔ بعد پایین می‌آورد و با بالا و پایین‌آوردن این

---

1 Back door
2 Vba32
3 Symantec

سرعت سبب وقوع اتفاق های ناگواری در تأسیسات هسته‌ای مانند انفجار سانتریفیوژها می گردید (عبدالهی صفی‌آبادی، ۱۳۹٤).

مکانیسم عملکرد: این بدافزار در سه مرحله، نفوذ و خرابکاری را انجام می‌داد (عبدالهی صفی‌آبادی، ۱۳۹٤: ۷).

۱. آلوده‌سازی: استاکس‌نت از طریق یواس‌پی خود را وارد دستگاه می‌کند و اقدام به آلوده‌کردن سایر دستگاه‌های مبتنی بر سامانهٔ مورد هدف می‌کند و از طریق جعل شناسهٔ دیجیتال[1] خود را متعلق به شرکتی قابل اطمینان نشان می‌دهد و از طریق کد کردن ساختار از دید دستگاه‌های تشخیص نفوذ[2] پنهان می‌ماند.

۲. جستجو: به دلیل شناسایی دستگاه‌های مستقر در تأسیسات نطنز بدافزار بررسی می‌کرد آیا این سامانه از نوع زیمنس[3] است یا نه؛ که نمونه‌های زیادی از این سیستم در تأسیسات هسته‌ای ایران مستقر است.

۳. به‌روزرسانی: اگر سیستم مورد حملهٔ سیستم موردنظر نباشد، بدافزار بلاک شده و اقدام خاصی را انجام نمی‌دهد. در غیر این صورت اقدام به برقراری ارتباط با اینترنت برای به‌روزرسانی آخرین نسخهٔ خود می‌کند.

شکل ۳: مکانیسم عملکرد استاکس‌نت در مرحلهٔ استقرار

پس از استقرار و اطمینان مهاجمان از استقرار درست در سامانه‌های هدف مرحلهٔ تخریب که شامل سه مرحله است انجام می‌گیرد. این سه مرحله شامل موارد ذیل است:

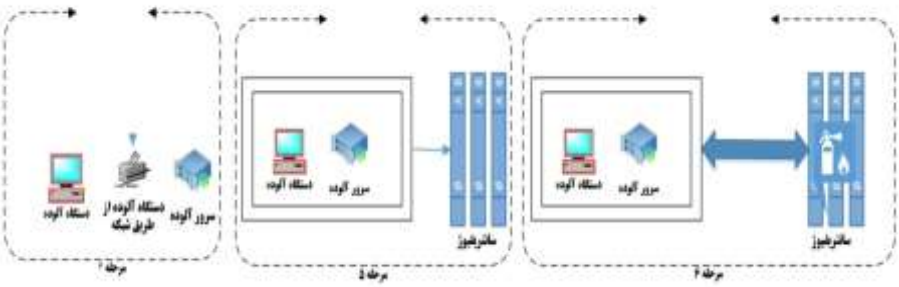
---

1 ID
2 IDS
3 Zimense Setup7

٤. به‌کارگیری: در این مرحله استاکس‌نت با شناسایی منابع موجـود در مقصـد اقـدام به بهره‌برداری از حفره‌های امنیتی دستگاه موسوم به‌روز صفر می‌نماید که این حفـره‌هـا ممکن است از دید کارشناسان امنیتی نادیده گرفته شده و یا شناسایی نشده باشد.

٥. پایش‌کردن: استاکس‌نت اقدام به شناسایی و جاسوسی از اقدام‌های دستگاه هـدف می‌پردازد. سپس از آنها برای پایش و از کار انداختن سانتریفیوژها استفاده می‌کند.

٦. فریب و تخریب: اقدام به ایجاد پس‌خوردهای نادرست در خروجی پایش‌کننده‌هـا می‌کند با این عمل شناسایی مشکل، زمان‌بر شده تا آنکـه هـر اقـدامی بـرای مهـارکردن فعالیـت‌هـای ایـن بـدافزار غیـرممکن باشـد. در ایـن مرحلـه بـا افـزایش دور گـردش سانتریفیوژها منجر به آتش‌سوزی و از رده خارج‌شدن آنها می‌شود.



شکل ٤: استاکس‌نت در مرحلهٔ استقرار و تخریب

استاکس‌نت با استفاده از روش‌های مختلفی توانست در سامانه‌هـای هسـته‌ای نفـوذ کنـد (عبدالهی صفی‌آبادی، ١٣٩٤). این روش‌ها به شرح ذیل هستند (سؤال سوم):

١. انتشار از طریق درایو فلش یواس‌پی و بـا اسـتفاده از آسـیب‌پـذیری موسـوم بـه «LNK»: استاکس‌نت از یک آسیب‌پذیری به نام زِرودِی[1] برای رونوشت‌برداری از خود در دستگاه یواس‌پی استفاده می‌کند. که ایـن عمـل از طریـق پرونجـای ایجـاد شـده بـا پسوند.LNK بر روی درایو فلش یـواس‌پـی و بـا اجـرا از طریـق اسـتفاده از مرورگـر پرونجا[2] صورت می‌گیرد. اگرچه پرونجاهایی با پسوند مزبور، شامل مسیری به پرونجای

1 Zero day
2 File manager

CLP[1] مربوط می‌شود، اما یک کاربر مخرب می‌تواند مسیر یک الگوی دلخواه را در آن قرار دهد که در این صورت به هنگام مشاهدهٔ آن توسط مرورگر پرونجا، الگوی مربوط به اجرا در خواهد آمد. در صورتی‌که یک درایو فلش غیرآلوده، به رایانه متصل گردد؛ استاکس‌نت پس از برخی بررسی‌های اولیه از قبیل فرایندهای در حال اجرا، سیستم‌عامل میزبان اقدام به آلودگی آن درایو می‌کند. سیستم‌عامل‌های ٦٤ بیتی میزبان خوبی برای استاکس‌نت نیست و در صورت نصب استاکس‌نت آن را متوقف خواهد کرد. ازجمله ویژگی‌های استاکس‌نت در صورت آلوده‌سازی یک درایو فلش یواس پی می‌توان به موارد ذیل اشاره کرد:

- فضای منطقی مربوط به درایو
- جانبی‌بودن درایو
- آلوده‌بودن و یا نبودن درایو توسط نسخهٔ حال حاضر استاکس‌نت بر روی میزبان؛ در صورت آلوده‌بودن درایو، کمتربودن مدت آلودگی آن از ۲۱ روز.
- فضای کافی داشتن درایو به اندازهٔ پنج‌مگابایت.
- وجود حداقل سه پرونجا بر روی درایو
- تنظیم‌بودن پیکربندی بدافزار مبنی بر آلوده‌کردن درایو.
- تاریخ فعلی فراخوانی شده قبل از ٢٤ ژوئن ۲۰۱۲ باشد (توابع آن در این بازه بارگیری شده باشند).

۲. انتشار به‌وسیلهٔ ویژگی اجزای خودکار: نوع اولیهٔ استاکس‌نت از ویژگی اجرای خودکار ویندوز بدون بهره‌برداری از آسیب موسوم به «lnk» استفاده کند. این نوع از استاکس‌نت از یک پرونجای اجرایی در قالب یک پرونجای موسوم به اتوران[2] با محتوای معتبر برای آن، در انتهای خود به این شیوه عمل می‌کند که جستجوگر ویندوز، دستورهای نامعتبر برای فایل اتوران که متعلق به پرونجای اجرایی ضمیمه‌شده است را صرف‌نظر کرده تا به دستورها برسد. از طرفی دستورهای منطبق بر اتوران که به‌عنوان یک پرونجای اجرایی است. در نتیجه پرونجای اجرایی ضمیمه شده اجرا می‌شود.

---

1 Control panel file
2 autorun.inf

۳. توزیع نظیر به نظیر: به هنگام اجرای استاکس‌نت، اقدام به ایجاد یک سرور تماس از راه دور می‌کند. تا ارتباط های داخلی را همانند یک کلاینت تماس از راه دور شنود کند. از این طریق رایانه‌های آلوده‌شده می‌توانند با هم ارتباط برقرار کرده و از به‌روزبودن خود اطمینان حاصل کنند و در صورت نیاز به‌روز شوند؛ بنابراین، باعث می‌شود تا نسخه‌های جدید گسترش یابد.

٤. توزیع موسوم به وین‌سی‌سی[1]

استاکس‌نت شامل تابعی برای ارتباط با سرورهای پایگاه داده وین سی سی است. زمانی که مانند یک سرور عمل می‌کند، از یک گذرواژه و رمز ورود پیش‌فرض برای ارتباط با سرور پایگاه داده استفاده می‌کند و با تزریق کد «اِس کیو اِل[2]» سرور پایگاه داده رمز استاکس‌نت را خواهد پذیرفت؛ بنابراین، اجرای رمزهای استاکس‌نت بر روی سرور پایگاه داده وین‌سی‌سی میسر می‌شود.

۵. توزیع به‌واسطهٔ اشتراک‌های شبکه: با استفاده از اعمال زمان‌بندی‌شده[3] در ویندوز و یا ابزارهای مدیریتی ویندوز[4] تمام حساب‌های میزبان آلوده‌شده را برای اینکه می‌تواند از خود بر یک اشتراک راه دور رمزها را اجرا کند یا امکان‌پذیر نیست. یک عمل شبکه‌ای ایجاد و برنامه‌ریزی می‌شود تا باعث اجرای پرونجا بعد از دو دقیقه شود.

٦. توزیع به‌وسیلهٔ آسیب‌پذیری موسوم به پرینتر اسپلوئر[5]: ویندوز دارای یک آسیب‌پذیری در زمان به اشتراک‌گذاری چاپگر است. که اجازه به اشتراک‌گذاری پرونجا را از طریق مسیر سامانه[6] و سپس پوشه (فولدر)[7] می‌دهد. استاکس‌نت با استفاده از

---

1 Wincc
2 SQL
3 Scheduled jobs
4 Windows Management Instrumentation (WMI)
5 Printer Splooer
6 System
7 folder

ذکرشده اقدام به ارسال کد و رونوشت‌برداری از خود در مقصد می‌نماید. از این روش در تاریخ قبل از ۱ ژوئن ۲۰۱۱ استفاده شده است.

۷. توزیع به‌واسطهٔ آسیب‌پذیری ویندوز سرور: این آسیب‌پذیری به استاکس‌نت اجازه می‌دهد تا یک رونوشت از خودش بر روی رایانه راه دور قرار دهد که با استفاده از برآورده شدن شرایط ذیل امکان‌پذیر است:

- پرونجاهای Kernel32.dll و Netapi32.dll باید قبل از انتشار یک اصلاحیهٔ خاص ساخته باشند.
- پرونجاهای ضدبدافزار باید قبل از یکم ژانویهٔ ۲۰۰۹ ساخته شده باشند.
- تاریخ فعلی سامانه باید پیش از یکم ژانویه ۲۰۳۰ باشد.

اگر این شرایط برقرار باشد استاکس‌نت سعی به برقراری ارتباط با یک میزبان از راه دور می‌کند و از طریق قرارداد «اس‌ام‌بی»[1] یک‌رشته مسیر را که منجر به اجرای از راه دور استاکس‌نت می‌شود، تولید می‌کند.

پیشینهٔ تحقیق: به‌عنوان‌مثال، سانتوس و همکاران (۲۰۱۳) یک روش بر اساس تکرار ظاهرشدن توالی آپ‌کد[2] و آموزش چندین الگوریتم داده‌کاوی درخت تصمیم کا[3]، نزدیک‌ترین همسایگان، ماشین‌های بردار پشتیبانی، شبکه‌های بیزین را برای شناسایی بدافزارهای ناشناخته پیشنهاد می‌دهد (Santos, Igor, 2013).

خسروی و همکاران (۱۳۹۲) به‌منظور بررسی کارایی روش‌های شناسایی بدافزارهای دگردیسی، موتور «CLAEn» مطرح نمودند. این موتور به‌صورت پویا و با استفاده از اتوماتای سلولی یادگیر نسل‌های جدیدی از بدافزار پایه تولید می‌کند. بدافزارهای تولیدشده از نظر امضای دودویی و آماری با رمز بدافزار پایه متفاوت بوده و

---

1 Server Message Block (SMB)
2 Opcode
3 K

از لحاظ تشابه به برنامه‌های بی‌خطر با درصد بالایی متشابه به طور متوسط ۷۵ درصد است. ماهیت یادگیرنده و پویای اتوماتای سلولی یادگیر به‌کار گرفته‌شده در این امکان را فراهم می‌کند که برای تولید بدافزارهای نسل جدید از یک بدافزار پایه در هر بار اجرای موتور، مسیر ساخت و الگوریتم یادگیری از ابتدا و به‌صورت تصادفیِ کامل بر روی رمز بدافزار پایه عمل کند. نتایج حاصل از انجام آزمایش‌های تشابه در حالت‌های مختلف بیانگر توانایی موتور پیشنهادی در تولید بدافزارهایی با درصد تشابه بالا به برنامه‌های بی‌خطر، با کمترین تشابه به یکدیگر به طور متوسط درصد و مقاوم در برابر محصولات ضدبدافزاری است (خسروی و پارسا، ۱۳۹۲).

شیجو و سلیم (۲۰۱۵) با به‌کارگیری یک روش ترکیبی برای کشف بدافزارها و استفاده از هردو روش ایستا و پویا اقدام به کشف بدافزار نمودند. در این تحقیق مشخص شد که استفاده از روش ترکیبی سبب افزایش نرخ کشف در مقابل هر یک از روش‌ها به‌تنهایی می‌گردد. همچنین برای دسته‌بندی هم استفاده از ماشین بردار پشتیبان[1] بهترین روش بوده و استفاده از «راندم فورِست[2]» هم برای بهبود مقدار «اِف پی[3]» مناسب است و در پایان مشخص شد که روش ترکیبی در مقابل روش‌های دیگر دارای نرخ تشخیص به میزان ۱.۵ درصد بالاتر است (Shijo and Salim 2015).

فرضعلی‌وند (۱۳۹۶) با استفاده از یادگیری تقویتی و روش‌های داده‌کاوی[4] که یک حوزهٔ تحقیقاتی بسیار فعال در یادگیری ماشین است اقدام به طراحی یک مجموعهٔ هوشمند تشخیص بدافزار نمود. نتایج تحقیق ثابت کرد که عامل‌های یادگیری تقویتی در این نوع محیط با دقت و سرعت بالایی قادر به تشخیص بدافزار هستند و عامل

---

1 Support victor machine(SVM)
2 Random forest
3 FP
4 Data mining

یادگیری تقویتی که در این مطالعه پیشنهاد و پیاده‌سازی شده است کارایی بهتری را از خود نسبت به روش‌های قبلی تشخیص بدافزار نشان می‌دهد و می‌توان گفت که ترکیب عامل یادگیری تقویتی و روش‌های داده‌کاوی همیشه تشخیصی هوشمند نسبت به هر حوزه را بر می‌گرداند. تجربه های حاصل از این مطالعه، پایهٔ خوبی برای مطالعات آینده در به‌کارگیری روش‌های یادگیری تقویتی و داده‌کاوی برای مسائل مختلف و به‌خصوص مسائل مرتبط با تشخیص هوشمند فراهم می‌کند (فرضعلی‌وند، ۱۳۹۶).

احمدی و همکاران (۲۰۱۶) در تحقیقی با عنوان روشی نو در استخراج، انتخاب و پیوند خصیصه‌ها برای دسته‌بندی مؤثر بدافزارها، یک روش را برای ایجاد دسته‌بندی در گروه‌های مختلف بدافزار پیشنهاد داده است. در این تحقیق نوع استخراج و انتخاب خصیصه از الگوریتم دسته‌بندی مهم‌تر است. این خصیصه‌ها از ساختار و ارتباطات نمونه‌ها استخراج می‌گردد؛ بنابراین، روش بر اساس نمونه‌های رمز شده و مبهم کار می‌کند. آنها پیشنهاد کردند نمونه‌ها گروه‌بندی می‌شوند و بر اساس خصایص مختلف از رفتار و پیوند بدافزارها مطابق با الگوریتم‌های وزنی است. روش ذکرشده بر روی بدافزارهای ویندوز با نرخ ۹۹ درصد آزمایش گردید (Ahmadi, Ulyanov, Semenov, Trofimov, Giacinto, 2016).

دباغی زرندی و همکاران (۱۳۹۶) روشی جدید استخراج کرده که برای تشخیص انواع بدافزارها با استفاده از تجزیه و تحلیل ایستا ارائه می‌شود. این روش از امضای معنایی به‌جای امضای دستوری استفاده می‌کند؛ بنابراین، این امکان را به وجود می‌آورد که به‌وسیلهٔ تشخیص نمایه‌های مختلف رفتار مخرب، با روش‌های مبهم‌سازی حمله‌کننده مقابله کند. علاوه بر این، روش پیشنهادی به دلیل استخراج دقیق الگوهای رفتاری در تشخیص بدافزارها کارایی بالایی دارد و در مقایسه با سایر روش‌ها، مثبتِ کاذب کمتری تولید خواهد کرد (دباغی‌زرندی، حسینی و دباغی زرندی، ۱۳۹۶).

بحث و نتیجه‌گیری

جمع‌بندی نظر کارشناسان در خصوص مقابله با استاکس‌نت: آلودگی از طریق حافظه‌های جانبی همواره یکی از راه‌های آلوده‌سازی اماکن مختلف است و آلودگی مراکز هسته‌ای نیز با وجود اهمیت فراوان آن از همین طریق رخ داد؛ بنابراین، با وجود گزارش‌ها و هشدارهای فراوان برای مقابله با حافظهٔ جانبی به‌خصوص یواس‌پی باز هم شاهد آلودگی از همین طریق هستیم؛ بنابراین، باید سازمان‌ها با ایزوله‌کردن دستگاه‌های خود از این مهم ممانعت کنند (سؤال آخر).

در پایان این تحقیق پیشنهادهایی برای سازمان‌های مشابه به‌منظور پیشگیری از این گونه موارد به شرح ذیل ارائه می‌شود:

۱. ایزوله‌کردن سامانه‌های صنعتی و حساس از انتقال اطلاعات با استفاده از حافظهٔ جانبی و مدیریت تمامی درگاه‌های سامانه‌ها؛
۲. به‌روزرسانی دائم سیستم‌عامل به‌منظور پوشش‌دادن آسیب‌پذیری‌های نسخهٔ قدیمی؛
۳. استفاده از سیستم‌عامل مناسب؛
٤. در نظر گرفتن سیاست برای محدودیت تمامی درگاه‌های ورودی دستگاه‌های مورد استفاده؛
۵. ایجاد محدودیت بر حساب‌های کاربری و ممانعت از اعطای دسترسی کامل افراد؛
٦. به‌روزرسانی مداوم ضدبدافزارها (عبدالهی و همکاران، ۱۳۹٤).

پیشنهادها

موارد قابل‌توجه در سازمان‌های دارای شبکهٔ خصوصی: در افق دههٔ آیندهٔ جهان، رشد اقتصادی و فنّاوری، به نحو چشمگیری از کشوری به کشور دیگر تغییر خواهد کرد و توسعهٔ ارتباطات و فنّاوری اطلاعات چالش حاکمیتی در کشورهای جهان خواهد بود. همچنین جوامع با چالش‌های امنیتی بیشتری روبه‌رو خواهند شد چرا که

زیرساخت‌های فضای سایبری تمایل بیشتری برای هضم جوامع مقاوم مثل جمهوری اسلامی ایران خواهند داشت؛ بنابراین، رویکرد حاکمان جوامع مقاومی مانند ایران، مقابله با چالش‌های پدید آمده از فضای سایبری خواهد بود؛ بنابراین، تدوین پدافندهای عامل و غیرعامل به‌منظور مقابله با این عوامل همواره در دستورکار و برنامه‌های این سازمان‌ها قرار دارد. با توجه به امکان انباشت اطلاعات با طبقه‌بندی بالا در این سازمان‌ها لازم است تا بالاترین موارد امنیتی برای مقابله با تهدیدهای فنّاوری اطلاعات مورد توجه قرار گیرد. نحوهٔ تشخیص بدافزار دارای شکل واحدی برای تمامی سازمان‌ها و اشکال مختلف است؛ بنابراین، تنها نحوهٔ آلوده‌شدن سازمان‌ها به معماری شبکه[1] ایزوله‌نبودن دستگاه‌هاست در این بین همان‌گونه که ذکر شد به‌عنوان دیدگاهی در نفوذ استاکس‌نت مورد استفاده قرار گرفت؛ بنابراین، در درجهٔ اول سازمان‌ها باید نسبت به مواردی از قبیل اتصال شبکهٔ داخلی به شبکهٔ خارجی (اینترنت) به هر نحوی ممانعت به‌عمل‌آورند؛ در راستای جلوگیری از تکرار نفوذ سلاح‌های سایبری در واحدهای نظارتی موارد زیر مورد توجه است:

۱) استفاده از به‌روزترین سیستم‌عامل‌ها (ترجیحاً سیستم‌عامل‌های متن‌باز)؛

۲) ممانعت از برون‌سپاری امور فنّاوری اطلاعات از قبیل تعمیرهای سخت‌افزاری، نصب و راه‌اندازی و مواردی از این دست؛

۳) ایجاد ساز و کاری برای محرمانه‌ماندن ساختار فنّاوری اطلاعات و ارتباطات (در مورد استاکس‌نت در صورت تشخیص ندادن ساختار بر مبنای نرم‌افزارهای شرکت زیمنس درصد موفقیت حمله کاهش می‌یافت).

٤) واپایش دقیق شرکت‌های طرف قرارداد به‌صورت دوره‌ای؛

۵) ایجاد آزمایشگاه‌های پیشرفته برای آزمایش دقیق تمامی اقلام ورودی به مجموعه؛

٦) مدیریت دقیق کلیه درگاه‌های دستگاه؛

---

۱ منظور از معماری شبکه در اینجا متصل به اینترنت و یا استفاده ازشبکهٔ داخلی است.

۷) پشتیبان‌گیری دوره‌ای از اطلاعات سازمانی (بررسی صحت پرونجای پشتیبانی)؛

۸) آموزش نکات اولیهٔ محافظت از سامانه‌ها به تمامی کارکنان و برگزاری دوره‌ای توجیه به‌منظور افزایش دانش افراد؛

۹) استفاده از دانش افراد باتجربه و دعوت از آنها برای انتقال دانش و تجربه؛

منابع

احمدی، مهدی (۱۳۹٦)، *الگوسازی تهدیدها راه‌کاری برای مبارزه با بدافزارها و تأمین امنیت سایبری*، چاپ اول، تهران: انتشارات پندار پارس.

خسروی مهران و سعید پارسا (۱۳۹۲)، «طراحی و پیاده‌سازی موتور دگردیسی بدافزارها با رویکرد ارزیابی کارایی روش‌های شناسایی»، *مجلهٔ علمی پژوهشی علوم و فنّاوری پدافند غیرعامل*، سال چهارم، شمارهٔ ۳ پاییز، ص ۱٤٥-۱٥٦.

داوری دولت‌آبادی، مجید (۱۳۹۳)، *بدافزارها و راه‌کارهای مقابله*، چاپ اول، تهران: پندار پارس.

دباغی زرندی، ف و حسینی (۱۳۹٦)، «سیستم تشخیص رفتار بدافزار با استفاده از تکنیک‌های استخراج گراف». *کنفرانس ملی تحقیقات کاربردی در مهندسی برق کامپیوتر*، ۲، شیراز. ص. ۳٦٤-۳٥۰.

عبدالهی صفی‌آبادی، محمد و مهدی عبدالهی صفی‌آبادی (۱۳۹٤)، بررسی عوامل راه‌یابی بدافزار استاکس نت به تأسیسات هسته‌ای- امنیتی ایران، اجلاس ملی چشم‌انداز ۱٤۰٤ و دستاوردهای فنّاورانه علوم مهندسی، ص ۱۳۳-۱٤٤، شیراز تیرماه ۱۳۹٤.

فرضعلی‌وند حسین (۱۳۹٦)، «طراحی و پیاده‌سازی سیستم هوشمند تشخیص بدافزار با استفاده از تکنیک‌های داده‌کاوی و یادگیری تقویتی»، *دومین کنفرانس بین‌المللی پژوهش‌های نوین در مهندسی برق کامپیوتر و فنّاوری اطلاعات*، شهریورماه، ۱-۱۲، تهران.

لرستانی، علیرضا (۱۳۹٦)، «شیوه‌های تشخیص بدافزارها و نرم‌افزارهای جاسوسی در سازمان‌های اطلاعاتی»، *فصلنامهٔعلمی- ترویجی مطالعات حفاظت و امنیت انتظامی*، ص ۱۲۱-۱٤٦، سال دوازدهم، پاییز، شمارهٔ ٤٤.

نامداری غلامرضا، رضا نورمندی‌پور (۱۳۹۲)، «تشخیص بدافزار روتکیت با استفاده از روش شخیص ترکیبی و الگوریتم‌های یادگیری ماشین»، *فصلنامهٔ پژوهش‌های حفاظتی- امنیتی دانشگاه جامع امام حسین*(ع)، سال سوم، شمارهٔ ۱۳، بهار، ص ۱۲-۳۰.

Ahmadi, M, Ulyanov, D, Semenov, S, Trofimov, M, Giacinto, G, 2016. «Novel feature extraction, selection and fusion for effective malware family classification». In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. ACM, pp. 183–194.

C. Ravi, R. M, (2012). «Malware Detection using Windows Api Sequence and Machine Learning». International Journal of Computer Applications, (2012).

Jamalpur, S. Navya, Y.S. Raja, P. Tagore, G. & Rao, G.R. (2018), «Dynamic Malware Analysis Using Cuckoo Sandbox, Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1056-1060, Coimbatore, India

Kumar A. Kuppusamy K. Aghila G. (2017) «A learning model to detect maliciousness of portable executable using integrated feature set, Journal of King Saud University Computer and Information Sciences, vol. 29, no 33. 4, pp. 1-14 January 2017

Santos, Igor. (2013). «Opcode sequences as representation of executables for data-miningbased unknown malware detection«. Information Sciences 231 (2013): pp.64-82.

Shijo, P. V. and Salim, A. (2015) Integrated Static and Dynamic Analysis for Malware Detection. Procedia Computer Science 46, pp.804-811