فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
فصلنامهٔ علمی ـ ترویجی
سال دوازدهم، شمارهٔ چهل‌وچهارم، پاییز ۱۳۹۶

تاریخ دریافت: ۱۳۹۶/۰۷/۲۳
تاریخ پذیرش: ۱۳۹۶/۰۸/۱۲

شیوه‌های تشخیص بدافزارها و نرم‌افزارهای جاسوسی در سازمان‌های اطلاعاتی

علیرضا لرستانی[۱]

چکیده:

زمینه و هدف: در عصر کنونی تکیه بر فنّاوری اطلاعات و قسمت‌هایی مانند رایانه‌ها، دوربین‌های نظارتی، دستگاه‌های هوشمند و شبکه‌های بسیار وسیع مانند اینترنت به یکی از نیازمندی‌های اساسی جوامع به‌خصوص جوامع اطلاعاتی تبدیل شده است. حضور نرم‌افزارهایی باهدف خرابکاری و تهاجم سایبری که دارای مصادیق خرابکارانه‌ای مانند سرقت اطلاعات محرمانه، بر هم زدن تعادل سامانه‌ها، اجرای دستورهایی که بدون خواست کاربر؛ سبب تعریف پدیده‌ای به نام بدافزار[۲] گردیده است که دارای رشد بسیار سریعی نیز هست. برای برخورد سریع و کارا با این پدیده در گام نخست می‌بایست یک شناخت دقیق از نوع این بدافزارها و نحوهٔ برخورد با آنها داشته باشیم. نظر به گستردگی و تنوع بدافزارها با ویژگی‌های مختلف نحوهٔ عملکرد این‌گونه بدافزارها نیز متفاوت بوده که به‌دلیل به‌کارگیری روش‌های گوناگون برای سالم جلوه دادن فایل‌های مخرب، روش‌های تشخیص فایل سالم از مخرب نیز متنوع است. در ضدبدافزارهای تجاری از روش تشخیص بر اساس امضا استفاده می‌شود که دارای کارایی بالا امّا بامحدودیت است در مقابل روش‌های تشخیص ایستا و پویا مطرح است که اولی بر اساس ساختار فایل و دومی بر اساس رفتار فایل در محیط به دسته‌بندی[۳] بدافزارها می‌پردازند. هدف در این تحقیق ضمن معرفی انواع بدافزارهای ثبت‌شده؛ روش‌های شناسایی آنها هم معرفی می‌شود؛ و روش‌هایی با کارایی بالا به‌منظور تشخیص دقیق بدافزارها موردبررسی قرارگرفته و معرفی می‌شوند.

روش‌شناسی: این پژوهش با روش کتابخانه‌ای و رجوع به اسناد و مدارک صورت گرفته است.

یافته‌ها و نتیجه‌گیری: نتایج این تحقیق نشان می‌دهد، با اقدام‌های پیشگیرانه خطر ابتلا به بدافزارها کاهش می‌یابد. روش‌های مختلف برای تشخیص این بدافزارها وجود دارد که هر یک دارای نقاط ضعف و قوتی است؛ امّا در این میان روشی ترکیبی مطرح است که می‌تواند با استفاده از نقاط قوت روش‌های دیگر و پوشش دادن نقاط ضعف آنها برای سازمان‌های اطلاعاتی یک گزینهٔ کامل و پوشش هرچه بهتر بخش فنّاوری اطلاعات و ارتباطات خود در مقابل مهاجمان باشد.

کلیدواژه: بدافزار، تشخیص ایستا، تشخیص پویا، دسته‌بندی، نرم‌افزار جاسوسی.

---

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

2. Malware
3. Classification

بیان مسئله

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 روبه‌رشد در استفاده از فنّاوری اطلاعات روبه‌رو هستیم، مهاجمان نیز از آنها به‌عنوان نیروی ذخیرهٔ قدرتمندی 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. باید توجه داشت که در اکثر مواقع کاربران از برنامه‌های کاربردی، برای دسترسی به اطلاعات شخصی موجود در دستگاه‌ها استفاده می‌کنند. به‌طورمعمول 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 (Kabakus, Dogru & Cetin, 2015:3).

دنیای بدافزارها و نرم‌افزارهای مخرب امروزی وسعت بسیار زیادی پیدا کرده است و همهٔ تجهیزات و منابع اطلاعاتی را تحت تأثیر قرار داده است. این نوع نرم‌افزارها همیشه در علم رایانه و شبکه مطرح بوده و هستند و یکی از دغدغه‌های اصلی مدیران سامانه‌ها و امنیت بوده است. اکنون بدافزارها بسیار فعال‌تر از گذشته شده و از هوشمندی بالایی برخوردارند، ازاین‌رو ممکن است ضدبدافزارها نتوانند به‌خوبی بدافزارها را شناسایی کنند. در این حوزه همواره کمبود یک ابزار برای تجزیه‌وتحلیل دقیق رفتار و ساختار این نوع بدافزار مطرح بوده است (داوری دولت‌آبادی، ۱۳۹۳: ۷).

به‌موازات تکامل نرم‌افزارهای خوش‌خیم، توسعه‌دهندگان آن، اقدامهای امنیتی را پیاده‌سازی می‌کنند تا مطمئن شوند محصول‌های‌شان از امنیت بالایی برخوردار است. با کامل شدن این نرم‌افزارها، نویسندگان مخرب‌ها نیز سعی دارند تا با استفاده از

1 Spyware Software

روش‌های چندریختی، مبهم‌سازی، دگردیسی و... بدافزارهای به‌روزتری را تولید کنند که در دام ضد بدافزارها قرار نگیرد (Sain, 2012: 3).

برای تشخیص بدافزارها روش‌های گوناگونی ارائه‌شده است: اساس و پایهٔ روش‌های قدیمی برای تشخیص مخرب‌ها، استفاده از روش مبتنی بر امضاست که در این روش‌ها، قسمتی از بدافزار به‌عنوان یک امضا برای آن در نظر گرفته می‌شود و بدافزار توسط همین امضا شناسایی و تشخیص داده می‌شوند. این امضاها در داخل یک پایگاه داده ذخیره می‌شوند (Ravi, 2012: 2).

اهمیت و ضرورت

به‌دلیل وجود آرمان‌های ارزشمند و والای نظام جمهوری اسلامی ایران؛ همواره دستگاه‌های مختلف ایران مورد حمله‌های گستردهٔ دستگاه‌های متخاصم و از جنبه‌های مختلف ازجمله سایبری قرار دارند. همچنین توجه به ظهور انواع بدافزارها با اشکال پیچیده و حمله‌های مکرر به تأسیسات و اطلاعات دستگاه‌های مختلف ضروری است تا یک شناخت از انواع بدافزار و نحوهٔ کارکرد آنها ارائه گردد؛ بنابراین، شناخت دقیق نحوهٔ عملکرد بدافزارها و نقاط هدف آنها می‌تواند ما را در پیشگیری از حمله‌ها و یا تقلیل اثرهای مخرب این بدافزارها هدایت کند. به‌دلیل شکست روش‌های قدیمی در تشخیص و شناسایی بدافزارهای جدید و ناشناخته، در سال‌های اخیر محققان تلاش کرده‌اند با استفاده از بعضی ویژگی‌های تغییرناپذیر بدافزارها، روش‌های مطمئن‌تری را برای تشخیص آنها ارائه دهند. نتایج به‌دست‌آمده نشان می‌دهد که روش‌های جدید دارای نرخ بالاتر تشخیص نسبت به روش‌های قدیمی‌تر هستند.

باتوجه به چالش مهمی که امروزه گریبان‌گیر دولت‌ها، سازمان‌ها، شرکت‌ها و افراد شده است. در این مقاله سعی شده است تا یک معرفی از انواع بدافزارهای شایع و نحوهٔ کارکرد آنها به‌عمل آید و در ادامه با نگاهی دقیق به مشکل بدافزارها و نحوهٔ انتشار آنها، دید جامع و فراگیری در این خصوص و راه‌های مؤثر مقابله با این تهدید ارائه گردد و اینکه بررسی شود که آیا اصول تشخیص بدافزارها در سازمان‌های دیگر با سازمان‌های اطلاعاتی تفاوت دارد یا خیر.

می‌توان مدعی شد که بیشتر سازمان‌های دولتی از ویندوز به‌عنوان سیستم‌عامل استفاده می‌کنند و بیشترین آمار تولید بدافزارها نیز مربوط به سیستم‌عامل ویندوز است؛ بنابراین، ضروری است تا بدافزارها و تهدیدهای مربوط به این سیستم‌عامل به همراه روش‌های تشخیص آن مورد بررسی قرار گیرد تا از اثرهای تخریبی این بدافزارها در سطح این سیستم‌عامل ممانعت به‌عمل آید (دغدغهٔ اصلی).

شناخت دقیق عملکرد سیستم‌عامل ویندوز و نحوهٔ استفاده از حفره‌های آن در این تحقیق ذکر نگردیده است. در قسمت اول تحقیق به هدف‌ها و سؤال‌های تحقیق اشاره‌شده است. در قسمت دوم مروری بر کارهای پیشین آمده و در قسمت سوم یک معرفی جامع از انواع بدافزارها و نرم‌افزارهای جاسوسی ذکر گردیده و در قسمت پایانی روش مورد پیشنهاد به همراه راه‌کارهایی برای ارگان‌های مختلف که در سازمان‌های اطلاعاتی نیز می‌تواند مفید باشد ذکر گردیده است.

هدف‌های تحقیق

هدف اصلی

بررسی روش‌های تشخیص انواع بدافزارهای رایج در سیستم‌عامل ویندوز

هدف‌های فرعی

۱. آشنایی با انواع بدافزارها و مکانیسم آنها
۲. بررسی روش‌های محتمل شیوع بدافزارها و نرم‌افزارهای جاسوسی
۳. تشریح روش‌های کشف بدافزارها
۴. شناسایی روش‌های بهینهٔ تشخیص بدافزارها در سازمان‌های اطلاعاتی

سؤال‌های تحقیق

سؤال اصلی

بهترین رویکرد در سازمان‌های اطلاعاتی برای تشخیص بدافزارها و نرم‌افزارهای جاسوسی کدام است؟

سؤال‌های فرعی

۱. انواع بدافزارهای رایج در حمله‌ها کدام‌اند و چه ویژگی و ساختاری دارند؟
۲. روش‌های محتمل شیوع بدافزارها و نرم‌افزارهای جاسوسی کدام‌اند؟
۳. روش‌های تشخیص بدافزار کدام‌اند؟
۴. روش‌های بهینهٔ تشخیص بدافزارها در سازمان‌های اطلاعاتی کدام‌اند؟

پیشینهٔ تحقیق

در دهه‌های اخیر، روش‌های جدیدی مبتنی بر امضا به وجود آمدند؛ امّا یکی از ضعف‌های عمدهٔ این روش‌ها، ناتوانی آنها در کشف و تشخیص بدافزارهایی بود که نویسندگان آنها از روش‌های مبهم‌سازی در نوشتن آن استفاده می‌کردند. به همین دلیل پژوهش‌های زیادی برای بهبود روش‌های مبتنی بر امضا ارائه‌شد که یکی از روش‌های مفید، پروژه‌ای بانام save بود که تمرکز آن بر روی اندازه‌گیریِ میزان شباهت و تفاوت‌ها بین رمزهای مخرب شناخته‌شده و رمزهای مشکوک بود. در این روش امضای بدافزارها توسط دنباله‌ای از (Api Call)ها تعیین می‌شود؛ امّا این روش همچنان در شناسایی و تشخیص بدافزارهای جدید و چندشکلی، ناتوان بود. این پروژه شامل دو عیب اساسی بود:

الف) ابزار مورد استفاده در این روش یعنی W32Dasmversion8.9 ضعیف بود.

ب) این روش هنگامی‌که نویسندهٔ مخرب از روش‌های مبهم‌سازی مانند درج رمز مرده یا... استفاده کند، دچار مشکل می‌شود؛ زیرا ترتیب (Apicall)ها عوض می‌شود (Patel,2008:6).

یکی دیگر از راه‌حل‌های ایستا که در اواخر سال ۲۰۱۲ توسط گیل‌تهان[1] و همکارانش ارائه شد، برای تشخیص بدافزارها از امضا استفاده می‌کرد. اساس این روش تجزیه‌وتحلیل بخش مشترک بین بدافزارها بود. روش آنها که Mal-ID نام دارد قادر به جداسازی فایل‌های مخرب از فایل‌های خوش‌خیم است. این الگوریتم که بر پایهٔ

1 . GilTahan

الگوریتم‌های یادگیری ماشین است، ابتدا فایل اجرایی را به فایل دودویی تبدیل کرده و سپس آن را به زیر بخش‌هایی از بایت‌ها تقسیم می‌کند و درنهایت هر یک از این زیر بخش‌ها به‌عنوان یک داده یا یک قطعه رمز، دسته‌بندی می‌شوند که از این قطعه رمزها به‌عنوان امضای بدافزار استفاده می‌شد و در تشخیص فایل‌های مخرب می‌توان از آنها بهره برد. عیب اساسی این روش، ضعف و ناتوانی آن در تشخیص بدافزارهای جدید بود که از روش‌های چندشکلی و مبهم‌سازی استفاده می‌کردند (Tahan,2012).

اخیراً تیان و همکاران، با استفاده از ویژگی‌های رشته‌های چاپ موجود در نمونه‌های بدافزار به تمایز بین بدافزار اجرایی و خوش‌خیم رسیدند مانند بسیاری از سامانه‌های طبقه‌بندی موجود، فرض می‌کنیم که نمونه‌های نرم‌افزارهای مخرب غیربسته‌ای همهٔ رویکردهای مبتنی بر محتوا نیاز به پیاده کردن دودویی دارند که این به علت وجود مخرب‌ها بسته‌بندی اغلب دشوار، آهسته و مبهم است (M. Gheorghescu, 2005: 6).

سزار و زیانگ روش طبقه‌بندی جدیدی را ارائه دادند که گراف‌های جریان، برای شناسایی بدافزارهای چندشکلی استفاده می‌شدند. آنان از الگوریتم اکتشافی یا هیوریستیک برای انطباق گراف جریان هنگام یافتن هم‌ریختی‌های گراف، استفاده کردند؛ بنابراین، آنان توانستند شباهت بین فایل‌های PE[1] را تخمین بزنند و درنهایت آنان الگوریتم دسته‌بندی را بر اساس روش خود ارائه کردند (D. Gao, M. Reiter & D. Song, Binhunt, 2008:5).

بدافزارها و انواع آنها

بیشتر نرم‌افزارهای مخرب بر پایه و علیه سیستم‌عامل ویندوز طراحی و نوشته می‌شوند و دلیل آن‌هم وجود آسیب‌پذیری‌ها و ضعف‌های متعدد در ساختار این سیستم‌عامل است که از دیرباز مورد توجه مهاجمان و نگارندگان بدافزارها قرارگرفته است و هم‌اکنون حمله‌ها از جوانب گوناگون متوجه این سیستم‌عامل است. نرم‌افزارهای مخرب یا بدافزارهای رایانه‌ای ازجمله موارد اسرارآمیز و مرموز در دنیای رایانه‌اند که توجه بیشتر

1. Portable execution

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 می‌شود. بدافزار، برنامه‌ای 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 و می‌توانند بدون کسب اجازه وارد دستگاه شده و باعث مداخله در امور دستگاه و دست‌کاری در پیکربندی خاص در سیستم‌عامل شوند. به‌طورمعمول کاربران معمولی تمامی این نرم‌افزارهای مخرب را ویروس می‌نامند و تفاوتی را از لحاظ عملکرد بین آنها قائل نمی‌شوند، درصورتی‌که انواع مختلفی از نرم‌افزارهای مخرب در دنیای رایانه وجود دارند و هرکدام دارای عملکردی متفاوت از دیگری هستند (داوری دولت‌آبادی، ۱۳۹۳: ۲۰).

نخستین بدافزار در حدود سال ۱۹۰۰ تشخیص داده شد که آن را کرم رایانه‌ای می‌نامیدند. پس‌ازآن، انواع بدافزارهای دیگر توسط نویسندگان آنها تولید شد که به‌مرورزمان با استفاده از ابزارها و روش‌های «مبهم‌سازی» پیچیده‌تر شدند به‌گونه‌ای که امروزه تشخیص آنها بسیار دشوار شده است. درواقع بدافزار شامل مجموعه‌ای از رمزهای طراحی‌شده برای اجرای فعالیت‌های غیرقانونی است که موجب آسیب رساندن به دستگاه می‌شود و بر یکپارچگی و عملکرد آن تأثیر منفی می‌گذارد (Egele,2012:4).

در حقیقت نرم‌افزارهای مخرب که معروف‌ترین آنها، ویروس نام دارند را می‌توان نخستین تخریب‌گران دنیای رایانه به شمار آورد. قدمت بدافزارها به زمان ابداع نخستین نرم‌افزار می‌رسد؛ درزمانی که مفهومی به نام شبکه وجود نداشت و کسی حتی در رؤیا هم نمی‌توانست ساختاری شبیه به اینترنت را تصور نماید. کاربران قدیمیِ رایانه به یاد دارند در زمانی که سیستم‌عامل اصلی سامانهٔ DOS بود هزاران بدافزار وجود داشت و تنها یک ابزار برای مقابله با بدافزارها و آن ابزار دکتر سالامون[1] بود که یک‌تنه تمامی

1. Toolkit

بدافزارها را نابود می‌کرد. درزمانی که فنّاوری اطلاعات به میزان پیشرفت امروز نبود نیازی به حضور یک گارد ویروس برای مبارزه با بدافزارها نبود و پویش دوره‌ای دستگاه توسط ضدبدافزارها یا نظارت دیسکت‌های ورودی می‌توانست برای مبارزه با آنها کافی باشد (داوری دولت‌آبادی، ۱۳۹۳: ۱).

بدافزار

در این قسمت ابتدا مفهوم بدافزار نحوهٔ تشکیل و بازآرایی آن و سپس معرفی گونه‌های اصلی آن به همراه مکانیسم عملکرد در دستگاه هدف تشریح می‌شود (پاسخ سؤال‌های اول و دوم).

مفهوم بدافزار

واژهٔ بدافزار معادل خلاصه‌شدهٔ نرم‌افزارهای بدخواه[1] بوده و به ویروس، تروجان و یا هر برنامهٔ دیگری گفته می‌شود که با نیت اعمال خرابکارانه ایجاد شود. این برنامه‌های مخرب دارای تنوعی به نسبت فراوان است که این تنوع سبب ایجاد برنامه‌های ضدویروس با مکانیسم‌های مختلف می‌شود (*همان*: ۶). نام دیگر نرم‌افزارهای ویران‌گر، بدافزار یا نرم‌افزارهای مخرب است. این بدافزارها برای آسیب رساندن به دستگاه و شبکه‌های رایانه‌ای در نظر گرفته‌شده‌اند.

چرخهٔ حیات

بدافزارها و بدافزارهای رایانه‌ای نیز مانند بدافزارهای زیست‌محیطی دارای یک ظهور و یک افول هستند و منظور از چرخهٔ حیات بدافزار حدفاصل بین ظهور و افول آن است. یک بدافزار زمانی به وجود می‌آید که یک نویسندهٔ بدافزار آن را ایجاد نماید؛ و زمانی از بین می‌رود که به‌طورکامل از روی رایانهٔ قربانی پاک‌سازی شود (*همان*: ۶).

باوجوداینکه این چرخهٔ حیات برای هر حمله بدافزاری جدید تکرار می‌شود، امّا برای تمامی بدافزارها و حمله‌ها یکسان نیست. بسیاری از حمله‌ها به‌سادگی نسخهٔ تغییریافته

1 Malicious Software

قسمتی از رمز یک بدافزار اصلی هستند؛ بنابراین، زیربنای رمز و شیوهٔ حملهٔ جدید، با بدافزار پیشین یکسان است، امّا تغییرهای کوچکی برای جلوگیری از شناسایی و حذف بدافزار توسط ضدبدافزارها، ایجاد می‌شود. به‌طورمعمول در حمله‌های بدافزاری موفق، نسخه‌های جدیدی از بدافزار در هفته‌ها و ماه‌های اولیه انتشار پیدا می‌کنند. این وضعیت به‌نوعی مسابقهٔ تسلیحاتی تبدیل می‌شود که از طرفی بدافزارنویسان تلاش می‌کنند تا برای رسیدن به هدف‌های‌شان که می‌تواند هدف‌های مالی، شهرت یا کنجکاوی باشد، از خطر تشخیص توسط ضدبدافزارها در امان بمانند. از سوی دیگر شیوه‌های دفاعی ضدبدافزارها نیز به‌روز رسانی و اصلاح می‌شود و یا به شیوه‌هایی تغییر می‌یابد تا خطرها و تهدیدهای جدید را کاهش دهد (دولت‌آبادی، ۱۳۹۳: ۱۷).

دسته‌بندی انواع بدافزار[1]

بدافزار

بدافزارهای رایانه‌ای برنامه‌هایی هستند که مشابه بدافزارهای زیست‌محیطی گسترش‌یافته و پس از وارد شدن به رایانه اقدام‌های غیرمنتظره‌ای را انجام می‌دهند. بدافزارهای رایانه‌ای به‌همین دلیل بدافزار نامیده شده‌اند، زیرا دارای برخی وجوه مشترک با بدافزارهای زیست‌محیطی هستند. بدافزارها دسته‌ای از رمزهای مخرب هستند که شاخص اصلی آنها خود همتاسازی هنگام اجرا به همراه برنامهٔ میزبان است. پس از اجرای یک بدافزار، زمینهٔ آلوده کردن دیگر برنامه‌ها یا مستندها نیز فراهم می‌شود. به برنامه‌ای که رمز بدافزار به آن افزوده شده باشد برنامهٔ آلوده می‌گویند. پس در حقیقت بدافزار هیچ فعالیتی ندارد و فقط هنگامی‌که در یک دستگاهِ نرم‌افزاری دیگر قرار می‌گیرد با استفاده از اجزای آن خود را تکثیر می‌کند و به تخریب می‌پردازد که این کار به‌طورمعمول بدون آگاهی کاربر صورت می‌گیرد. با وجودی‌که تمامی بدافزارها خطرناک نیستند، امّا بسیاری از آنها با هدف تخریب انواع مشخصی از فایل‌ها،

۱بدافزارها دارای تنوع بسیاری بوده که در این تحقیق به مهم‌ترین آن‌ها اشاره‌شده است.

برنامه‌های کاربردی و یا سیستم‌عامل‌ها نوشته‌شده‌اند. بدافزارها هم همانند تمامی برنامه‌های دیگر از منابع دستگاه مانند حافظه و فضای دیسک سخت، توان پردازندهٔ مرکزی و دیگر منابع بهره می‌گیرند و می‌توانند اعمال خطرناکی را انجام دهند.

همچنین یک بدافزار می‌تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد. تولد بدافزارها به‌روزهایی مربوط می‌شود که رایانه شخصی وجود نداشت و رایانه‌ها دستگاه‌هایی حجیم و پرهزینه بودند و تنها در اختیار نهادهایی قرار داشتند که به استفاده از آنها نیاز بود. در واقع نخستین نویسندگان بدافزارها متخصصان علوم رایانه در زمان خود بودند و انگیزه‌های متفاوتی برای این کار داشتند. درکل به‌غیراز بدافزارهایی که تنها با انگیزهٔ مردم‌آزاری نوشته می‌شوند، بدافزارهای فراوانی هم هستند که با انگیزه‌های 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 نمایش دادن پیام‌هایی به انتقاد از وضعیت سیاسی یا اقتصادی کشور خاصی می‌پردازند (داوری دولت‌آبادی، ۱۳۹۳: ۳۰).

کرم

یک کرم برنامهٔ مخربی است که به‌طور مستقل عمل کرده و می‌تواند به عنوان نسخه‌ای کامل بر روی دستگاه دیگری منتشر شود. کرم در محیط‌های شبکه‌ای مانند اینترنت به شدت رایج است. مهم‌ترین خصیصهٔ کرم، طبیعت خودتکرار شونده آن است که منجر به اشغال حافظه و استفاده بی‌جا از پهنای باند شبکه می‌شود (Herath, 2009: 2).

اسب تراوا[1]

در مفاهیم رایانه‌ای، اسب تراواست که می‌تواند خرابی‌های زیادی را به بار آورد و یا اعمالی غیر از آنچه مدنظر کاربر است را انجام دهد. این اصطلاح به‌تازگی به برنامه‌های ویران‌گری گفته می‌شود که بدون اجازه و آگاهی کاربر، وارد دستگاه شده و موجب از بین بردن یکپارچگی دستگاه می‌شود (Ravi, 2012: 3).

---

۱. این نوع از بدافزار دارای تنوع بسیار بالایی است؛ امّا همگی بر روی یک چارچوب پیاده‌سازی شده‌اند که همین امر کار تشخیص را دشوار می‌کند.

بمب منطقی

بمب منطقی خود را منتشر نمی‌کند، بلکه بر روی یک دستگاه نصب می‌شود و منتظر می‌ماند تا زمانی که اتفاقی خارجی مانند ورود داده، رسیدن به تاریخی خاص، ایجاد یا حذف و یا حتی ویرایش یک فایل خاص رخ دهد و آنگاه به دستگاه آسیب می‌رساند (Doherty, 2009: 2).

درب‌های پشتی

به‌طورمعمول برای دسترسی به یک سامانهٔ رایانه‌ای نیاز به وارد کردن نام کاربری و رمز عبور دارید. اگرچه این سطح از امنیت گاهی وقت‌ها دستگاه‌ها را ایمن می‌سازد و تنها افراد خاصی می‌توانند با استفاده از اطلاعات صحیح وارد سامانه شوند؛ امّا وجود درب‌های پشتی باعث بی‌اثر کردن تمامی تنظیم‌های امنیتی شده و اجازهٔ دسترسی رایانه شما را به دیگر کاربران، از راه دور می‌دهد (Herath, 2009: 2).

جاسوس‌افزارها[1]

جاسوس‌افزارها به نسبت بدافزارها و اسب تروا جدید هستند. این نرم‌افزارها هم‌زمان با توسعهٔ اینترنت بیشتر موردتوجه نفوذگران قرار گرفتند. نمونه‌های ابتدایی جاسوس‌افزارها توسط پایگاه‌های اینترنتی مورد استفاده قرار گرفت که به علایق شخصی کاربران خود توجه داشتند و در مواردی جنبهٔ تجاری و تاحدودی مثبت داشتند. نرم‌افزارهای جاسوسی در دو نوع خانگی[2](درونی) و تجاری[3] عرضه شده‌اند.

خانگی

این نرم‌افزار برخلاف خواستهٔ کاربر اقدام به بررسی فعالیت‌های وی در سامانه می‌کند. مجریان قانون از نرم‌افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی استفاده می‌کنند که این مجرمان خود از همین نرم‌افزارهای جاسوسی برای دست‌یابی به رایانه‌های شخصی به‌قصد دزدی دارایی‌ها استفاده می‌کنند.

---

1 Spyware
2 Domestic Spyware
3 Commercial Spyware

تجاری

امّا در نوع دوم با ارائه گستردهٔ این نرم‌افزارها در فضای مجازی به‌نوعی تلاشی را برای کسب سلایق افراد از جوامع هدف مختلف برای هدف‌های اقتصادی در دستور کار خود قرار می‌دهند (داوری دولت‌آبادی، ۱۳۹۳: ۳۷).

هانی‌پات[1]

یک منبع دستگاه اطلاعاتی است که بر روی خود اطلاعات کاذب و غیرواقعی دارد و با استفاده از ارزش اطلاعات دروغ خود تلاش می‌کند تا اطلاعات و فعالیت‌های غیرمجاز و غیرقانونی را بر روی شبکه کشف و جمع‌آوری کند. به زبان ساده هانی‌پات یک سامانه یا دستگاه رایانه‌ای متصل به شبکه و یا اینترنت است که دارای اطلاعات دروغ بر روی خود است. از عمد در شبکه قرار می‌گیرد تا به‌عنوان یک تله عمل کرده و مورد تهاجم یک نفوذگر واقع شود و با استفاده از این اطلاعات آنها را فریب داده و اطلاعاتی را از نحوهٔ ورود آنها به دستگاه جمع‌آوری کند. هانی‌پات‌ها به دو دلیل استفاده می‌شوند: اول اینکه نقاط ضعف دستگاه را شناسایی کنند و دوم جمع‌آوری اطلاعات لازم برای ردگیری و تعقیب نفوذگران به سامانه (داوری دولت‌آبادی، ۱۳۹۳: ۳۹).

بات‌نت[2]

شبکه‌هایی از رایانه‌های آلوده هستند. این رایانه‌ها بانظارت مجموعه‌ای از دستورها هستند که از طریق نرم‌افزاری که عمدی یا ناآگاهانه نصب شده است مدیریت‌شده و تغییر می‌کند. این نرم‌افزار توسط رایانه‌ای خرابکار نظارت می‌شود. ممکن است بات‌نت‌ها دارای کارکرد قانونی نیز باشند؛ امّا بیشتر موارد با فعالیت‌های مجرمانه برای انتشار هرزنامه، بدافزار یا حمله‌های سرقت هویت در ارتباط‌اند. بر اساس مطالعات انجام گرفته ده درصد از تمام رایانه‌های متصل به اینترنت توسط بات‌نت‌ها نظارت

1 Honeypoot
2 Botnet

می‌شوند. زمانی که یک رایانه با استفاده از بات‌نت‌ها آلوده شود دیگر توان مقاومت در برابر دستورهای مالک بات‌نت را ندارد و به‌طورکامل در اختیار دستگاه بات‌نت قرار می‌گیرد. اندازهٔ بات‌نت‌ها به میزان پیچیدگی معماری آنها ارتباط دارد و ممکن است از چندین رایانه تا ده‌هاهزار رایانه منفرد در این شبکه حضور داشته باشند؛ و به‌طورمعمول کاربران رایانه‌های قربانی از اینکه در نظارت دستگاه دیگری باشند اطلاع ندارند.

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 نمونهٔ هستهٔ سیستم‌عامل را انجام می‌دهند. نفوذگر ابزار روتکیت را پس از دسترسی به سامانهٔ هدف در سطح یک کاربر مدیر، روی دستگاه نصب می‌کند. این دسترسی می‌تواند از طریق درهم شکستن گذرواژه و با بهره‌گیری از نقاط آسیب‌پذیر دستگاه صورت گیرد. در ادامه نفوذگر اقدام به جمع‌آوری ID کاربران دستگاه هدف از طریق ابزار روتکیت می‌کند تا حساب کاربری اصلی مانند حساب کاربری سطح مدیر[2] دست یابد (داوری دولت‌آبادی، ۱۳۹۳: ۴۶).

بررسی موارد شیوع بدافزارها و نرم‌افزارهای جاسوسی

به‌تازگی جنگ جدیدی بین مؤسسات و انجمن‌های امنیتی و توسعه‌دهندگان نرم‌افزارهای مخرب صورت گرفته است. متخصصان امنیتی از همهٔ روش‌ها و راهبردهای ممکن برای حذف و متوقف کردن تهدیدها بهره می‌برند درحالی‌که توسعه‌دهندگان بدافزارها از روش‌های جدید برای دور زدن ویژگی‌های امنیتی استفاده می‌کنند. همه‌ساله تعداد بسیار زیادی از بدافزارها باقدرت انتشار و راهبردهای مختلف ساخته می‌شوند. برای اینکه بتوان در این جنگ به نتیجهٔ مطلوب رسید و سازمان خود

1 Rootkits
2 Administrator

را از این آسیب‌ها و تهدیدها در امان نگه داشت باید اطلاعات کامل‌تری در خصوص بدافزارها، انواع آنها و از همه مهم‌تر نحوهٔ انتشار آنها کسب کرد.

بدافزارها که در اصطلاح کلی به نرم‌افزارهای مخربی گفته می‌شود که با هدف‌های مختلفی ازجمله جمع‌آوری اطلاعات حساس، دسترسی به سامانه‌های رایانه‌ای خصوصی و در برخی موارد تخریب دستگاه‌ها در شکل‌های گوناگون مانند اسکریپت، رمز، محتوای فعال و ... طراحی‌شده و با کمک عوامل انسانی یا به‌صورت خودکار و به شیوه‌های خاص و رسانه‌های چندگانه در بین رایانه‌ها منتشر شوند. یکی از راه‌های انتشار رایج و انتقال بدافزارها، فرآیند دریافت اطلاعات آن از اینترنت است. در برخی موارد بدافزارها فقط اقدام به تخریب نمی‌کنند بلکه می‌توانند عملکرد دستگاه را تحت تأثیر خود قرار دهند و بار اضافی به دستگاه تحمیل کنند. در موارد جاسوسی بدافزارها خود را پنهان می‌کنند به‌طوری‌که حتی آنتی‌بدافزارها نیز قادر به تشخیص آنها نیستند و این بدافزارها اطلاعات ارزشمند و حیاتی از قربانی خود را به مبدأ ارسال می‌کنند.

۱. نحوهٔ انتشار بدافزارها

در این مقاله سعی شده است تا از زوایای مختلف به نحوهٔ انتقال بدافزارها نگاه شود و علاوه بر روش‌های دیجیتالی، ارتباطاتی و شبکه‌های رایانه‌ای به مفاهیم و روش‌های پیچیده و نوین در جهان نیز اشاره شود. انتشار بدافزار به روش‌هایی الکترونیکی گفته می‌شود که به‌وسیلهٔ آن بدافزار به یک سامانه یا ابزار اطلاعاتی منتقل می‌شود و به دنبال تأثیرگذاری بر روی آن است.

از طریق سیستم‌عامل

بدافزارها سیستم‌عامل‌های مختلفی مانند اندروید، مک، ویندوز یا لینوکس را هدف خود قرار داده‌اند امّا میزان تأثیرگذاری، سطح و قدرت آن به‌دلیل مکانیسم‌های امنیتی متمایز در هر یک از سیستم‌عامل‌ها متفاوت است. بدافزارها برای حمله به معماری سیستم‌عامل‌ها، سطوح امنیتی آنها و شکستن این امنیت از روش‌های پویا و انتشار

تطابقی استفاده می‌کنند. یکی از راه‌های انتشار، آلوده‌سازی فایل‌های اجرایی و ایجاد وظایف مجازی است که باعث کاهش عملکرد سیستم‌عامل می‌شود. انتشار و آلوده‌سازی بدافزارها وابستگی کامل به سیستم‌عامل دارد به‌عنوان‌مثال بدافزاری که روی دستگاه فایل مکینتاش کار می‌کند ممکن است روی ویندوز کار نکند ازاین‌رو توسعه‌دهندگان رمزهای مخرب با روش‌های جدیدی برنامه‌هایی را تولید کرده‌اند که بتواند روی چندین سیستم‌عامل کار کند، امّا ممکن است روی تمام این سیستم‌عامل‌ها نتواند کارآیی مشابهی داشته باشد.

از طریق شبکه‌های بیسیم

شبکه‌های بیسیم امروزه سطح وسیعی از ابزارها و بسترهای ارتباطی را تحت پوشش خود قرار داده به‌طوری‌که در گوشی‌های تلفن‌همراه نیز از آن برای انتقال اطلاعات و دسترسی به اینترنت به‌شدت استفاده شده است. فنّاوری بیسیم بسیار متنوع بوده و در اینجا به بلوتوث و wifi اشاره می‌شود. بلوتوث به‌دلیل نقاط ضعفی که دارد موردعلاقهٔ رخنه‌گرها برای انتقال رمزهای مخرب خود هستند. در زیر روش‌های حمله و انتشار بدافزارها بیان می‌شود.

- BlueSnarf: این روش برای اجرای خدمات و حمله و گرفتن دسترسی بدون هیچ‌گونه احراز هویتی است و در حمله‌های توسعه‌یافتهٔ جدید از این نوع، مهاجم دسترسی کامل را برای خواندن و نوشتن روی ابزار قربانی دارد.
- Bluejacking: در این روش مهاجم یک پیام متنی کوتاه شیّادانه از طریق گفتگوی احراز هویت‌شده می‌فرستد و قربانی با دسترسی به رمزهای این پیام فریب، به مهاجم اجازهٔ دسترسی و نظارت کامل دستگاه خود را می‌دهد.
- BlueBug: در این روش مهاجم قادر است از قسمت خدمات گوشی تلفن‌همراه مانند تماس ورودی و خروجی، ارسال و دریافت پیامک‌های کوتاه و تمامی خدمات گوشی بهره‌مند گردد.

- BlueBump: در این روش مهاجم با بهره‌گیری از ضعف بلوتوث و دست‌کاری کلیدهای لینک می‌تواند به داده‌ها دسترسی یافته و از خدمات تلفن‌همراه مانند اینترنت، WAP و GPRS و خدمات دیگر سوءاستفاده کند.
- Blue Smack: در این روش به‌سادگی می‌توان خدمات را از کار انداخت.
- HeloMoto: این روش ترکیبی از BlueBug و BlueSnarf است.
- Blue Dump: مهاجم خودش را در روند جفت‌سازی از طریق بلوتوث بعد از رونوشت‌برداری از کلید لینک ذخیره‌شده، خود را درگیر می‌کند و فرصتی را برای شنود کلید مبادله در اختیار مهاجم قرار می‌دهد.
- Car Whisperer: تنظیمات پیش‌فرض بعضی از ابزارها، پین‌کدهای ثابتی را برای جفت‌سازی و مبادله فراهم می‌کنند که کار را برای مهاجمان بسیار ساده می‌کند و منجر به سوءاستفاده می‌شود که پس از نخستین دست‌یابی، پین‌کد تغییرناپذیر است.
- Blue Chop: مهاجم فرصت مناسبی برای قطع اتصال و پایان اتصال جاری دارد حتی اگر اتصال اصلی از اتصال چندگانه نیز پشتیبانی کند.

روش‌های بالا تحت پروژه‌ای به نام Blue Bag قرار دارند. ازآنجایی‌که اکثر ابزارهای تلفن‌همراه، رایانه‌های همراه، چاپگرها و ... دارای فنّاوری بلوتوث هستند؛ بنابراین، امکان انتشار بدافزار از طریق آن بسیار محتمل است. زمان قابل‌رؤیت بودن نیز در آلوده شدن مؤثر است. ۷٫۵ درصد از صاحبان ابزارهای تلفن‌همراه بدون رعایت هیچ‌گونه ملاحظه‌ای فایل دریافت می‌کنند و پیام‌های ناشناس را قبول می‌کنند.

تحقیقات نشان می‌دهد که رشد فنّاوری سریع‌تر از روش‌های امن‌سازی مرتبط با این فنّاوری‌های جدید است و فاصلهٔ قابل‌ملاحظه‌ای بین فنّاوری و روند ارتقای امنیت وجود دارد که بر روی قابلیت اطمینان و پایداری این فنّاوری‌ها تأثیرگذار است.

الگوسازی‌های اخیر نشان می‌دهد که روند انتشار کرم رایانه‌ای از طریق بلوتوث در مناطقی با جمعیت بالا و دارای مکان‌های عمومی بیشتر از سرعت بالاتری برخوردار است.

انتقال رمزهای مخرب از طریق شبکه‌های wifi که بر روی رایانه‌های همراه، رایانه‌های شرکت‌ها و سازمان‌ها و تلفن‌های همراه قرار دارد، می‌تواند به روش‌های زیر صورت گیرد:

- رایانه‌ها و تلفن‌های همراه و ابزارهای دیگر از طریق کارت شبکهٔ بیسیم و با شناسایی نقاط دست‌یابی[1] موردنظر و به‌صورت مجاز به یک شبکهٔ داخلی متصل شوند. در این شبکه انتشار بدافزارها می‌تواند مانند شبکهٔ عادی باسیم و یا اینترنت صورت گیرد.
- ابزارها دارای کارت شبکهٔ بیسیم بوده و با جستجو و کشف نقاط دست‌یابی مختلف و در محیط اطراف خود، شبکه‌های مختلف را شناسایی می‌کند. وظیفهٔ بدافزار ابتدا اتصال به این شبکه‌هاست. اگر این شبکه‌ها دارای مکانیزم احراز هویت و رمزنگاری مانند WEP، WPA یا WPA2 باشد، بدافزار با استفاده از نقاط ضعف موجود در شبکه‌های وای‌فای ابتدا اقدام به شکستن این مکانیزم کرده و سپس خود را به‌عنوان عضوی از آن شبکه قرار می‌دهد. سپس اقدام به آلوده‌سازی دستگاه‌های دیگر می‌کند؛ امّا درصورتی‌که مکانیزم امنیتی فعال نباشد، به‌راحتی خود را عضو یک شبکهٔ دیگر کرده و عملیات خود را انجام می‌دهد (Damshenas, M, Dehghantanha, A, & Mahmoud, R. 2013: 4).

از طریق اشتراک فایل

اشتراک اطلاعاتی و فایل‌ها به‌صورت یک برنامهٔ معمولی در شبکه‌های P_2P یا شبکه‌های سازمانی بزرگ تبدیل‌شده است و به کاربران اجازه می‌دهد تا به‌راحتی تعداد زیادی از اطلاعات ذخیره‌شدهٔ دیجیتالی را با دیگران به اشتراک بگذارند. یکی از شبکه‌های به اشتراک‌گذاری فایل که در سال ۲۰۰۱ توسعه یافت، کازا[2] بود. در این شبکه که به‌منظور به اشتراک‌گذاری موسیقی راه‌اندازی شده بود و رایانه‌های کلاینت بی‌شماری به آن متصل بودند و کلاینت‌ها به یک Super node (SN) این شبکه از یک خزنده و کاوشگر به نام

1. Access point
2 . Kazaa

Krawler (A KaZaA Crawler) استفاده می‌کند. اگر کلاینتی درخواست فایلی را می‌داد، درخواست به SNاش منتقل می‌شد اگر SN می‌توانست فایل را پیدا کند که به کاربر اعلام می‌کرد در غیراین صورت درخواست را به سایر SNهای متصل به خودش می‌فرستاد تا فایل را پیدا کنند. این شبکه برای انتقال فایل بین کلاینت‌ها از رمزنگاری استفاده می‌کرد.

برای انتشار بدافزارها در این شبکه، بدافزارها ترفندهای بسیاری را استفاده کردند ازجمله رونوشت به تعداد زیاد از فایل بدافزاری بانام‌های مختلف به‌منظور افزایش احتمال دریافت اطلاعات توسط دیگران و آلوده شدن آنها. باتوجه به تدابیر امنیتی این شبکه ازجمله استفاده از امضا و hash فایل‌های اصلی و تمایز آنها از فایل‌های جعلی و بدافزاری؛ بااین‌حال این شبکه و شبکه‌های مشابه آن برای به اشتراک‌گذاری فایل‌ها بسیار خطرناک شناخته شدند.

تحلیل شبکه‌های P_2P نشان می‌دهد که ۱۵درصد از فایل‌های اجرایی قابل دریافت اطلاعات به رمزهای بدافزاری آلوده بودند و طی بررسی در سال ۲۰۰۶ در شبکهٔ کازا مشخص شد ۷۱ درصد از موارد آلوده‌شده در کلاینت‌ها و میزبان‌ها از نوع کرم SdDrop و انواع آن و بدافزار Tanked بودند (Damshenas, et.al 2013).

از طریق شبکه‌های اجتماعی

در سال‌های اخیر شبکه‌های اجتماعی از محبوبیت بالایی در بین کاربران اینترنتی برخوردار شده‌اند به‌گونه‌ای که به طرز خارق‌العاده‌ای گوی سبقت را در برقراری ارتباط بین افراد از دنیای واقعی ربوده است. این محبوبیت بالا به‌خاطر ویژگی روش‌های تعامل مجازی است؛ بر این اساس شبکه‌های اجتماعی برخط[1] (OSN)، خدمات زیادی ازجمله به اشتراک‌گذاری عکس، کلیپ، فایل و برنامه‌های کاربردی مانند گفتگوی اینترنتی و تماس را به‌وجود می‌آورند. در دو سال اخیر ثابت‌شده است که OSNها فقط یک تارنما برای ارتباط‌ها و تفریح نیستند بلکه می‌توانند در فرایند تغییر فرهنگ و سبک زندگی شرکت داشته باشند. از دیدگاه امنیتی OSNها محیطی به‌طورکامل خطرناک و پر از تهدیدهای امنیتی هستند که بدافزارها در آن منتشر می‌شوند.

1 Online social networks

در این محیط چهار تهدید عمده وجود دارد:

- حمله‌های نقض حریم خصوصی
- بازاریابی بدافزاری
- حمله‌های ساختاری شبکه
- حمله‌های بدافزاری (Damshenas, et.al 2013).

از طریق سامانه‌های مجازی

روش مجازی‌سازی به‌سرعت در حال تبدیل‌شدن به استانداردی برای کسب‌وکارهاست. در این فنّاوری به یک رایانه یا سرور اجازه می‌دهد تا چندین سیستم‌عامل یا چندین نشست از یک سیستم‌عامل را به‌طور هم‌زمان اجرا کند درنتیجه به کاربران اجازه می‌دهد تا برنامه‌های کاربردی بیشتری را روی تنها یک رایانه یا سرور داشته باشند. بزرگ‌ترین چالشی که سازمان‌ها هم‌اکنون با آن روبه‌رو هستند چگونگی امن‌سازی سامانه‌های مجازی است که در مقابل تهدیدهای مشابه سامانه‌های واقعی آسیب‌پذیر هستند. سامانه‌های مجازی همیشه نمی‌توانند با روش سامانه‌های واقعی امن شوند چراکه هر سامانهٔ مجازی روی یک دستگاه ممکن است با تهدید متفاوتی روبه‌رو شود درنتیجه نیاز به سطح امنیتی متفاوتی دارد و همچنین نیاز است از روش‌های امنیتی اضافی برای امن کردن کانال‌های ارتباطی بین سامانه‌های مجازی روی یک دستگاه استفاده کرد. یکی از این روش‌ها، ناحیه‌بندی امنیتی (Security zone) برای هر یک از سامانه‌های مجازی روی یک دستگاه و تعریف سیاست‌ها و نقش‌ها و سطح امنیتی خاص متناسب با نیاز برای هر ناحیه روی یک دستگاه است (Damshenas, et.al 2013).

از طریق پایگاه‌های اینترنتی و رایانامه

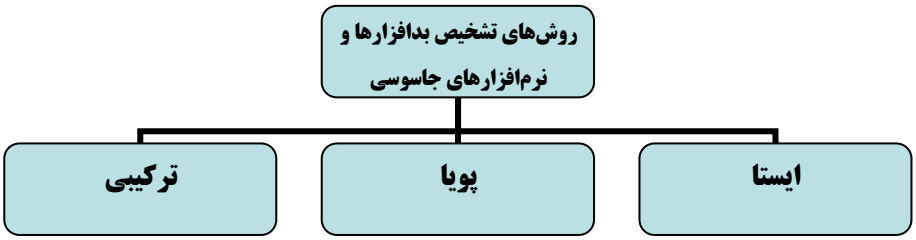
راه‌های مختلفی برای حمله از طریق رایانامه‌ها و انتشار رمزهای مخرب وجود دارد. استفاده از فایل‌های الحاقی به رایانامه، قرار دادن لینک به پایگاه‌های اینترنتی آلوده، رایانامهٔ جعلی (Fake mail) و اسپم‌ها روش‌های انتشار بدافزارها از طریق رایانامه هستند. رخنه‌گرها نیز برای انتشار بدافزارها روش‌های مختلفی را روی تارنماها

پیاده‌سازی می‌کنند تا کاربران به‌طور اتفاقی یا با استفاده از روش‌های فریب، کاربر را به‌سوی این پایگاه‌های اینترنتی هدایت کنند. پایگاه‌های اینترنتی دارای نرم‌افزارهای مخرب بوده که پس از دریافت اطلاعات روی رایانه، موجب آلوده‌سازی آن می‌شوند.

هدف‌ها و روش‌های تجزیه‌وتحلیل و تشخیص بدافزار

هدف از تجزیه‌وتحلیل بدافزار به‌دست آوردن اطلاعاتی است که بتوانیم با استفاده از آنها جلوی نفوذ غیرمجاز به شبکه را بگیریم. هدف ما به‌طورمعمول تعیین واقعی چیزی است که اتفاق افتاده است و مطمئن شدن از شناسایی و تعیین محل همهٔ دستگاه‌ها و فایل‌های آلوده است. در روش‌های سنتی و تجاری مخصوص ضدبدافزارهای موجود زمانی که فایلی یا برنامه‌ای نیازمند تجزیه‌وتحلیل باشد در آن زمان امضاهای بدافزارهای قبلی یافت‌شده را در شبکه قرار داده و با فایل مشکوک به بدافزار مقایسه می‌شود و اگر رشته مطابق بود به‌عنوان بدافزار و در غیر این صورت فایل سالم تشخیص داده می‌شود. این کار خود نیازمند به‌روزرسانی مکرر بانک امضاء[1] دارد (رضایی و دیگران، ۱۳۹۳: ۱۷).

ضدبدافزارهای موجود دائم مورد چالش قرار می‌گیرند. چندین روش تجزیه‌وتحلیل نرم‌افزار مخرب و روش‌های تشخیص بدافزارها برای به‌حداقل رساندن توزیع برنامه‌های مخرب، پیشنهاد شده است. بااین‌وجود نویسندگان بدافزار، روش‌های جدیدی مانند مبهم‌سازی، تغییر رفتار برنامه و ... را به‌منظور ایجاد بدافزارهای جدید، بدافزارهای غیرقابل تشخیص و... گسترش داده‌اند (Tahan, 2012: 7). در نوعی دسته‌بندی، روش‌های مختلف تشخیص بدافزار بر اساس ماهیت عملکرد آن در سه دسته ایستا، پویا و ترکیبی تقسیم می‌شوند در شکل زیر نمایشی از این دسته‌بندی آمده است (P. Szor, 2005):



شکل ۱: روش‌های تشخیص بدافزارهای مختلف

۱. در ضدبدافزارهای موجود در بازار نیاز داریم در طول زمان آنها را به‌روزرسانی کنیم که این خود همان به‌روزرسانی پایگاه اینترنتی امضاست.

در سه نوع تشخیص روش‌های ایستا[1]، پویا[2] و ترکیبی[3] مورداستفاده قرار می‌گیرند در زیر توصیف این سه نوع تشخیص آمده است:

تشخیص ایستا

تجزیه‌وتحلیل استاتیک، اطلاعاتی در مورد نظارت برنامه، جریان اطلاعات و ویژگی‌های آماری بدون نیاز به اجرای برنامه به‌دست می‌آورد. روش اصلی مورداستفاده در تجزیه‌وتحلیل ایستا، مهندسی معکوس است. یکی از مشکلات پیش روی تجزیه‌وتحلیل ایستا این است که رمز منبع برنامه به‌طورمعمول در دسترس نیست که این امر استفاده از روش‌های تجزیه‌وتحلیل ایستا را کاهش می‌دهد و درنتیجه منجر به تجزیه‌وتحلیل رمزهای باینری آنها می‌شود که این تجزیه‌وتحلیل هم به‌شدت پیچیده است (Tahan, 2012: 9).

درروش ایستا که همراه با مهندسی معکوس است، رمزهای باینری چک می‌شوند و بدافزارها بر اساس رمزهای باینری شناسایی می‌شوند که در واقع جزء کلیدی درروش ایستاست. استخراج رمزهای باینری کار تاحدودی دشوار است.

تشخیص پویا

روش تجزیه‌وتحلیل پویا نیاز به اجرای برنامه دارد تا بتواند آن را در یک محیط مجازی تحلیل کند. این روش، اطلاعاتی را در ارتباط با نظارت و جریان داده به ما می‌دهد که موجب کسب نگاهی عمیق‌تر از برنامه می‌شود (Gurrutxaga,2008: 6). در این روش با استفاده از محیطی شبیه‌سازی‌شده ابتدا برنامه اجراشده و سپس با استفاده از برنامه‌های نظارت و ثبت این رفتار بدافزار بودن یا نبودن برنامه مشخص می‌شود.

روش ترکیبی

تجزیه‌وتحلیل ترکیبی شامل ترکیبی از روش‌ها یعنی ایستا و پویاست. در این روش ابتدا ویژگی‌های امضا، تحلیل می‌شود سپس آن را با کمیت‌های رفتاری ترکیب کرده تا

1 Static
2 Dynamic
3 Hybrid

تجزیه‌وتحلیل را تقویت نماید. باتوجه به این روش، تحلیل ترکیبی می‌تواند باعث بهبود درک از رفتار بدافزارها شود و درنتیجه نرخ مثبت کاذب ۲ را کاهش دهد؛ همچنین روش ترکیبی بر محدودیت‌های تجزیه‌وتحلیل پویا غلبه می‌کند، زیرا یکی از اشکالات مهم در تجزیه‌وتحلیل پویا، کند بودن 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 (Damodhare,2012:4).

روش‌های مختلفی برای تشخیص بدافزار وجود دارد؛ امّا باتوجه به پیچیده‌تر شدن بدافزارها توسط روش‌های مبهم‌سازی، نیاز به روش‌های پیشرفته‌تری برای تشخیص آنهاست. تمامی روش‌های تشخیص بدافزار که بر اساس پیچیدگی بدافزارها و پیچیدگی آنها قرار دارند در یکی از دسته‌های زیر قرار می‌گیرند:

الف) مبتنی بر امضاء

ب) مبتنی بر رفتار

تشخیص بر اساس امضاء

روش مبتنی بر امضا بر اساس بررسی رمزهای مشکوک و جمع‌آوری اطلاعات به‌منظور توصیف هدف‌های مغرضانهٔ نرم‌افزارهای مخرب است. هدف اصلی این روش، استخراج توالی بایت‌های ویژه از رمزها به‌عنوان امضاست؛ همچنین جستجو برای یک امضا در داخل فایل‌های مشکوک یکی از هدف‌های این روش است. بیشتر ضدبدافزارهای تجاریِ امروزی از مجموعه‌ای از امضاها به‌منظور تشخیص برنامه‌های مخرب استفاده می‌کنند که این رمزهای مشکوک با یک توالی منحصربه‌فرد از ساختارهای برنامه یا بایت‌ها، مقایسه می‌شود.

اگر این امضا در داخل پایگاه داده وجود نداشته باشد، به این معناست که این فایل خوش‌خیم است نه مخرب؛ بنابراین، یکی از محدودیت‌ها در روش تشخیص مبتنی بر امضا، نیاز به دخالت انسان در به‌روزرسانی پایگاه داده امضا، با امضاهای جدید است. علاوه بر این، گروهی از محققان نشان دادند که برخی از نویسندگان بدافزارهای

چندریختی می‌توانند به‌آسانی روش مبتنی بر امضا را به‌وسیلهٔ روش‌های مبهم‌سازی، شکست دهند. این امر باعث شد ما به این نتیجه برسیم که این روش تشخیص، مستعد ابتلا به منفی کاذب است. همچنین هنگامی‌که انواعی از مخرب‌ها شناخته می‌شوند، پایگاه دادهٔ امضاها رشد می‌کند.

تشخیص بر اساس رفتار:

برخلاف روش ایستا که بر روی رمز بدافزارها تکیه می‌کند، رفتار زمان اجرا را موردتوجه قرار می‌دهد. در واقع تجزیه‌وتحلیل یک برنامه در زمان اجرای آن را تجزیه‌وتحلیل پویا می‌نامند که به تجزیه‌وتحلیل رفتارها نیز معروف است و شامل اجرای نرم‌افزار و مشاهدهٔ رفتار آن، تعامل دستگاه و اثرهای آن روی دستگاه میزبان است. روش تجزیه‌وتحلیل پویا نیاز به اجرای فایل‌های آلوده در یک محیط مجازی؛ مانند یک دستگاه مجازی، یک شبیه‌ساز جعبه‌شن[1] و ... دارد تا بتواند آن را آنالیز کند.

روش‌های مناسب برای تشخیص بدافزارها در سازمان‌های اطلاعاتی

بدون شک بدافزارها یکی از تهدیدهای مهم امنیتی برای فنّاوری اطلاعات بوده و هستند. در طی سالیان گذشته، از زمان بدافزارهای ساده تا تهدیدهای پیشرفته‌تری همچون بدافزارهای پیشرفتهٔ امروزی، همواره یکی از دلایل مهم رخدادهای امنیتی این بدافزارها بوده‌اند. نرخ صعودی میزان بدافزارها و نرم‌افزارهای جاسوسی نشان می‌دهد که یکی از اصول جاسوسی و خرابکاری نوین استفاده از ترفندهایی برای نفوذ در فنّاوری اطلاعات شرکت‌ها و سازمان‌های هدف به‌ویژه سازمان‌های اطلاعاتی است.

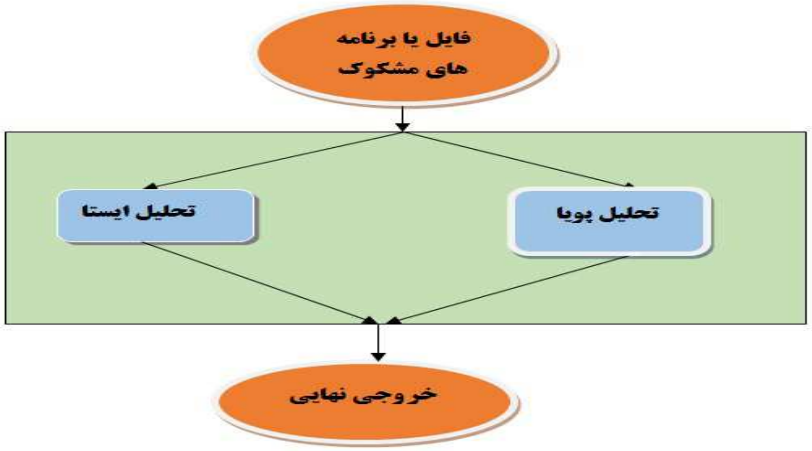
با توجه به ساختار سازمان‌های اطلاعاتی و سروکار داشتن این سازمان‌ها با حجم وسیعی از اطلاعات ارزشمند به‌طورقطع یکی از هدف‌های تمام دستگاه‌های مهاجم از سوی سازمان‌های جاسوسی بیگانه خواهند بود. همچنین به‌دلیل وجود ضوابط داخلی و امکان رصد توسط سازمان‌های جاسوسی دشمن، در این‌گونه سازمان‌ها در صورت

1 Sand box

بروز مشکلاتی از قبیل خرابکاری، حمله‌ها توسط بدافزارها و مواردی ازاین‌دست، بازگو کردن آن دارای یک بازخورد منفی در ابعاد گسترده بود و همچنین خسارت‌هایی را متوجه ساختار فنّاوری اطلاعات سازمان‌ها خواهد کرد. نحوهٔ استقرار ساختار فنّاوری اطلاعات در سازمان‌های اطلاعاتی چیزی برخلاف دیگر سازمان‌ها نیست؛ بنابراین، راه‌کارهای مورداستفاده در شرکت‌های مختلف در مورد سازمان‌های اطلاعاتی می‌تواند مورد بهره‌برداری قرار گیرد.

در قسمت‌های قبلی در مورد روش‌های تشخیص بدافزارها بحث گردید؛ بنابراین، پیشنهاد می‌شود تمامی موارد مشکوک در این سازمان‌ها توسط آزمایشگاهی انجام بگیرد که مجهز به تجزیه‌وتحلیل ترکیبی هر برنامه یا فایل مشکوکی باشند و تربیت افرادی که توانایی ارتقای این آزمایشگاه را باتوجه به به‌کارگیری انواع روش‌های نوین توسط نگارندگان بدافزار داشته باشند. همچنین ضروری است تا تمام برنامه‌های ورودی از شرکت‌های خارج از این سازمان‌ها همچنین فایل‌های مشکوک و تمامی اقلام ورودی از قبیل هدایای داخلی و خارجی که به‌نحوی کارکردی از فنّاوری اطلاعات را دارا باشند، قبل از به‌کارگیری موردبررسی و تجزیه‌وتحلیل دقیق قرارگرفته تا بی‌خطر بودن آنها اثبات گردد.

شمایی از روش پیشنهادی



به‌کارگیری روش‌های آزمایشگاهی جدید مانند روش‌های متنوع هوش مصنوعی مانند انواع روش‌های خوشه‌بندی[1] و دسته‌بندی قادرند برای تشخیص و دسته‌بندی دقیق این برنامه‌ها مورداستفاده قرار گیرند. باتوجه به ساختار اکثر زبان‌های مورداستفاده در سطح سازمان‌ها برای تولید برنامه‌های موردنیاز که از نوع شیءگرا[2] هستند و ریسک استفاده از این امّا تجهیز آزمایشگاه‌های مخصوص این عملیات و همچنین تربیت افراد متخصص دارای هزینه‌ای گاهی بالاست که در صورت محاسبه ریسک رخداد حمله‌های احتمالی می‌توان موافقت مدیران را برای صرف چنین هزینه‌ای به دست آورد.

جمع‌بندی و پیشنهادها

به‌علت پیشرفت روزافزون علم و سرعت سرسام‌آور این رشد در بخش فنّاوری اطلاعات و ارتباطات به‌موازات آن مهاجمان و نگارندگان نرم‌افزارهای جاسوسی نیز خود را مجهز به این علوم می‌کنند؛ بنابراین، باتوجه به تجارب گذشته در جمهوری اسلامی و اقدام‌های انجام‌شده در بخش‌های مختلف ازجمله صنعت نفت، هسته‌ای و بخش‌های دیگر ضروری است با اقدام‌های پیشگیرانه خطر ابتلا به این بدافزارها را کاهش دهیم. روش‌های مختلف برای تشخیص این نرم‌افزارها وجود دارد که هر یک دارای نقاط ضعف و قوتی است؛ امّا در این میان روش ترکیبی که با استفاده از نقاط قوت روش‌های دیگر و پوشش دادن نقاط ضعف آنها می‌تواند برای سازمان‌های اطلاعاتی یک گزینهٔ کامل و پوشش هرچه بهتر بخش فنّاوری اطلاعات و ارتباطات خود در مقابل مهاجمان باشد. در پایان موارد زیر به‌عنوان پیشنهاد ارائه می‌شود:

- باور این موضوع که جاسوسی سازمان‌های بیگانه بیشتر بر مبنای سامانه‌های رایانه‌ای بوده و وجود تبحر بالا در حصول اطلاعات به‌دلیل بومی بودن این سامانه‌ها در کشورهای مبدأ

1 Clustering
2 Object oriented

- توجیه دقیق افراد حاضر در هر رده برای وضع احتیاط کافی در مواجهه با موارد مشکوک چه در فضای اینترنت و چه هنگام نصب قطعه‌های جدید در دستگاه‌های هر رده
- به‌کارگیری افراد متخصص برای تحقیقات به‌روز در مورد بدافزارها
- تجهیز آزمایشگاه‌هایی برای بررسی دقیق هدایا، وسایل تازه خریداری‌شده باقابلیت پیاده‌سازی جدیدترین روش‌های تشخیص بدافزار و نرم‌افزارهای جاسوسی

منابع و مآخذ

منابع لاتین

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

D. Gao, M. Reiter, D. Song, Binhunt: automatically finding semantic differences in binary programs, Information and Communications Security (2008) 238-255.

Damodaran, Anusha, Fabio, Di Troia, Aaron Visaggio, Corrado, H Austin, Thomas, Stamp, Mark (2015). A comparison of static, dynamic, and hybrid analysis for malware detection. J Comput Virol Hack Springer-Verlag France.

Damshenas, M, Dehghantanha, A, & Mahmoud, R. (2013). A SURVEY ON MALWARE PROPAGATION, ANALYSIS, AND DETECTION. International Journal of Cyber-Security and Digital Forensics(IJCSDF), 10-29.

Doherty, N. F. Anastasakis, L. & Fulford, H. (2009). The Information Security Policy Unpacked: A Critical Study of the Content of University Policies. International Journal of Information Management, Vol.29, No.6, P.P 449–457.

Egele, M. S,A Survey on Automated Dynamic Malware-Analysis. ACM Comput er, 42, (2012).

G. Tahan,L.R.Y. Automatic Malware Detection Using Common Segment Analysis and Meta-Features. Journal of Machine Learning Research 13(2012) 949-979, (2012).

Herath, H. M. P. S. & Wijayanayake, W. M. J. I. (2009). Computer Misuse in the Workplace. Journal

I. Gurrutxaga,O.A.J.P,J.M,J.M,I.P, Evaluation of Malware clustering based on its dynamic behaviour. Seventh Australasian Data Mining, (2008) Conference.

I. Gurrutxaga,O.A.J.P,J.M,J.M,I.P, Evaluation of Malware clustering based on its dynamic behaviour. Seventh Australasian Data Mining, (2008). Conference.

K. Mathur, S.H,A Survey on Techniques in Detection and Analyzing Malware Executables, Advanced Research in Computer Science and Software Engineering, (2013).

Kabakus A. Dogru I. & Cetin A. (2015) ."APK Auditor Permission-based Android Malware Detection", Digital Investigation, Vol. 13, pp. 1-14, June 2015.

M. Gheorghescu, "An automated virus classification system," in Virus Bulletin Conference, 2005, pp. 294–300.

M. Sain, A.P,H.L. Survey on malware evasion techniques: state of the art and challenges, (2012).

P. Szor." The Art of Computer Virus Research and Defense". Addison Wesley for Symantec Press, New Jersey, 2005.

Patel, S. C, Graham, J. H. & Ralston, P. A. (2008). Qualitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Eenhancements. International Journal of Information Management, Vol.28, No.6. P.P 483–49.

S. Damodhare, P.G, INTELLIGENT MALWARE DETECTION SYSTEM, International Journal of Engineering Research and Applications (IJERA), (2012).

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

منابع فارسی

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

رضایی، فریدون؛ سعید رضایی؛ محسن طاهریان و علی افراز (۱۳۹۳)، *معرفی بدافزارها و ارائه الگوریتم‌های تشخیص AOSMD*. تهران:ناقوس.