فصل اول

کلیات تحقیق

۱-۱- مقدمه

فایل‌های اجرایی مخرب یک تهدید بزرگ برای کامپیوترها و امنیت کامپیوترهاست. فایل اجرایی مخرب به برنامه‌ای که یک عمل مخرب را انجام می‌دهد اطلاق می‌شود، مانند به خطر انداختن سیستم‌های امنیتی، آسیب رساندن به یک سیستم یا بدست آوردن اطلاعات حساس بدون اجازه کاربران. انواع متعددی از کدهای مخرب از طریق تصادم اینترنت در هزاران کامپیوتر در سراسر جهان گسترش یافته‌اند. انواع دیگر از کدهای مخرب استاتیک هستند مانند ویروس‌ها که گاهی اوقات مرگبارتر از همتایان خود هستند. یکی از مسائل ابتدایی جامعه برای مواجه با ویروس‌ها ارائه تدبیری برای تشخیص برنامه‌های مخرب است که تا بحال آنالیز نشده‌اند و اغلب نمی‌توانند شناسایی شوند تا وقتی که برای آن‌ها امضائی تولید شود. در طی این مدت زمان، سیستم‌ها بوسیله‌ی الگوریتم‌های مبتنی برامضا محافظت می‌شود که در برابر حملات آسیب‌پذیر هستند. فایل‌های اجرایی مخرب به عنوان حملات برای انواع بسیاری از نفوذ مورد استفاده قرار می‌گیرند. در ارزیابی تشخیص نفوذ DARPA1998 بسیاری از حملات روی سیستم‌عامل ویندوز توسط برنامه‌های اجرایی مخرب صورت گرفته بود. در گذشته نه چندان دور یک قطعه کد مخرب، در شبکه داخلی مایکروسافت یک حفره ایجاد کرد، حمله ابتکاری با یک فایل اجرایی مخرب صورت گرفت که داخل شبکه داخلی مایکروسافت یک درپشتی باز کرد، و منجر به سرقت رفتن منبع کد مایکروسافت شد

(فن[1] و همکاران، ۲۰۱۶).

[1] Fan

تکنیک‌های مورد استفاده برای تشخیص مخرب‌ها را می‌توان به طور گسترده به دو دسته طبقه‌بندی کرد، تشخیص مبتنی بر ناهنجاری و تشخیص مبتنی بر امضا. تکنیک تشخیص مبتنی بر ناهنجاری از دانش خود از این که چه چیزی تشکیل‌دهنده رفتار عادی است برای تصمیم‌گیری مخرب بودن یا نبودن یک برنامه تحت بازرسی استفاده می‌کند. تکنیک تشخیص مبتنی بر امضا از آن خصوصیات شناخته شده برنامه مخرب برای تصمیم‌گیری استفاده می‌کند. شناسایی فایل‌های اجرایی مخرب کلیدی برای محافظت سیستم در برابر این نوع حملات است. اسکنرهای خودکار مبتنی بر امضا در بازار موجود است، اما آن‌ها در شناسایی فایل‌های اجرایی مخرب جدید از دقت بالایی برخوردار نیستند. بطور معمول آنتی‌ویروس‌ها از تطابق امضا برای شناسایی مخرب‌ها استفاده می‌کنند. آن‌ها یک تک الگوی منحصربفرد برای هر مخرب می‌سازند بطوری‌که فایل‌های اجرایی مخرب بعدی آن بتوانند بدرستی طبقه‌بندی شوند(دینگ[۲] و همکاران، ۲۰۱۸). اشکال سیستم‌های مبتنی بر امضا این است که آن‌ها نمی‌توانند مخرب‌های ناشناخته و جدید را تشخیص دهند. به بیان دیگر آن‌ها در برابر حملات روز صفر و روش‌های متعدد مبهم‌سازی کارآمد نیستند. بنابراین نیاز رو به رشدی برای تشخیص کارآمد و سریع وجود دارد که بتوانند حملات جدید را تشخیص دهند (کوبر[۳]، ۲۰۱٤).

۱-۲- بیان مسئله

بدافزار به نرم‌افزارهایی گفته می‌شود که باعث هرگونه خرابی در کامپیوتر شخصی، سرویس‌دهنده یا شبکه‌ی کامپیوتری شوند؛ از جمله گونه‌های مختلف بدافزارها می‌توان به ویروس‌ها، کرم‌ها، جاسوس-افزارها، اسب‌های تروا، روت‌کیت‌ها و بات‌ها اشاره کرد. روت‌کیت یک بدافزار است که توانایی مخفی‌سازی خود و فعالیت‌هایش را در سیستم هدف دارد. مالک روت‌کیت قادر به اجرای فایل و انجام تنظیمات بر روی سیستم قربانی است، بدون آن‌که مالک سیستم متوجه آن شود. روش‌های تحلیل کد در حالت کلی به دو صورت تحلیل ایستا و تحلیل پویا مطرح می‌باشند. در تحلیل ایستای بدافزار، تمامی مسیرهایی از کد که بدافزار ممکن است در هر اجرای خود طی کند، شناسایی و تحلیل می‌گردد. در این روش تحلیل، فایل اجرایی بدون در نظر گرفتن دستورات آن بررسی

[2] Ding
[3] Kuber

می‌شود. این روش بسیار سریع و ساده است؛ اما به شکل قابل ملاحظه‌ای در برابر بدافزارهای پیچیده، ناکارآمد می‌باشد و یک سری ویژگی‌های رفتاری مهم را در نظر نمی‌گیرد. در تحلیل پویای کد، با اجرای باینری بدافزار، رفتار و خصوصیات اجرایی آن شناسایی می‌شوند. این روش برای حذف آلودگی در سیستم و تولید امضاهای موثر، خود را درگیر اجرای بدافزار و مشاهده رفتار آن در سیستم می‌کند.

امروزه افزایش انواع مختلف بدافزارها چالش بزرگی در صنعت آنتی‌ویروس‌ها ایجاد کرده‌است. برای محققان این موضوع که چگونه روند رو به‌رشد نمونه‌های بدافزارها را بطور موثر پردازش کنند و تکنیکی سریع برای محافظت کاربران ارائه دهند، یک زمینه‌ی تحقیقاتی مهم محسوب می‌شود. در این پایان‌نامه روشی نوین مبتنی بر رفتار با استخراج فراخوانی‌های API برای تشخیص بدافزار روت‌کیت ارائه شده است.

۱-۳- اهمیت موضوع

تهدیدها علیه امنیت داده‌ها و اطلاعات و حمله‌های نرم‌افزاری مخرب، فرآیندی پیچیده است. تنوع و تعداد این حملات و تهدیدها نتیجه فراهم‌کردن انواع مختلف روش‌های دفاع در مقابل آن‌هاست؛ اما متأسفانه فناوری‌های تشخیص امروزی برای مقابله با رویکردهای جدید طراحان بدافزار که از آن‌ها برای گریز از ضد مخرب‌ها استفاده می‌کنند، موثر نیستند. محققین تلاش فراوان انجام داده‌اند تا سیستم‌های ضدبدافزار با روش‌های مؤثر تشخیص بدافزار ارائه دهند و از سیستم‌های کامپیوتری محافظت کنند. این تهدیدات سبب بوجود آمدن سیستم‌های تشخیص بدافزار شده است. در واقع یک سیستم تشخیص بدافزار سیستمی است که برای تعیین این مسأله بکار می‌رود، که آیا یک برنامه قصد خرابکاری دارد یا خیر. امروزه فعالیت‌های مخرب وارد مرحله جدیدی شده است که در آن کدهای مخرب نه تنها سیستم‌ها را آلوده می‌نمایند بلکه اطلاعات شخصی کاربران را به سرقت می‌برند. بر همین اساس تعداد و اثرات زیان‌بار بدافزارها به طور روزافزون در حال افزایش است (اگل[4] و همکاران، ۲۰۱۲).

[4] Egele