

رویکردی خودکار جهت تحلیل و دسته‌بندی خانواده‌ی باج‌افزارهای رمز‌گذار

سید عطاالله سید جعفری^۱، محمدهادی علائیان^{۲*} و سعید پارسا^۳

دانشگاه علم و صنعت ایران، تهران، ایران

ataa1370@gmail.com¹

hadi.alaeiyan@yahoo.com²

parsa@iust.ac.ir³

چکیده

باج‌افزارها یکی از تهدیدات همیشگی برای دستگاه‌های رایانه‌ای به‌شمار می‌آیند. باج‌افزارها با ورود به دستگاه‌های رایانه‌ای بسته به اهدافشان، سعی دارند در روند عادی دستگاه‌های رایانه‌ای اختلال ایجاد کنند. در این بین، باج‌افزارهایی به نام باج‌افزار وجود دارند که پس از ورود به دستگاه‌های رایانه‌ای و محدود کردن دسترسی قربانی به دستگاه رایانه‌ای خود با رمزگذاری فایل‌های قربانی یا قفل‌گذاری دستگاه درصدد اخاذی از قربانی برمی‌آید. این نوع باج‌افزارها، یک تفاوت بسیار آشکار با دیگر باج‌افزارها دارد، باج‌افزارها باصراحت قربانی را از وجود خود بر روی دستگاه رایانه‌ای باخبر می‌سازند. این باج‌افزارها، برخلاف آسیب‌های جدی‌ای که بر روی دستگاه‌های قربانی وارد می‌سازند، می‌توانند با ویژگی‌های منحصر به فردی که بر روی سامانه برجای می‌گذارند، شناسایی شوند. در این مقاله، محیط مناسب را جهت اجرای باج‌افزارها و ویژگی‌های مؤثر را در شناسایی آن‌ها ارائه می‌کند. با اجرای باج‌افزارها در محیط ارائه‌شده، گزارش‌هایی از روند اجرای باج‌افزار حاصل خواهد شد. این گزارش‌ها ما را در کشف ویژگی‌های تمایزکننده رفتارهای مخرب باج‌افزارها یاری خواهند کرد؛ با کمک این ویژگی‌ها و الگوریتم‌های یادگیری ماشین می‌توان با دقت ۹۸/۹۸ درصد علاوه بر شناسایی باج‌افزارها، خانواده باج‌افزارها را نیز تعیین کرد.

واژگان کلیدی: باج‌افزار، باج‌افزار، باج‌افزارهای رمز‌گذار، باج‌افزارهای قفل‌گذار، دسته‌بندی خانواده باج‌افزارها.

۱- مقدمه

امروزه نمی‌توان تأثیر نرم‌افزارها را در زندگی روزمره‌مان انکار کرد. نرم‌افزارها با کارایی و دقت بالای خود از ملزومات زندگی امروزی ما به حساب می‌آیند و استفاده از آن‌ها در محیط‌های محاسباتی نه فقط یک امتیاز، بلکه به یک نیاز ضروری تبدیل شده است؛ اما در کنار این نرم‌افزارهای سودمند نرم‌افزارهایی هم همواره با عنوان باج‌افزار وجود دارند که امنیت دستگاه‌های رایانه‌ای را تهدید می‌کنند [2] [1]. این برنامه‌ها صدمات جدی و در برخی موارد خسارات جبران‌ناپذیری به دستگاه‌های رایانه‌ای وارد می‌کنند. باج‌افزارها انواع مختلفی دارند که باج‌افزارها یکی از آن‌ها به حساب می‌آید. این دسته از باج‌افزارها که هدف آن‌ها بیشتر جنبه مالی دارند، با حمله به فایل‌های شخصی بر روی دستگاه قربانی آن‌ها را غیرقابل دسترسی می‌کند [3] که در قبال دریافت مبلغی، این فایل‌ها را دوباره به حالت قبل

برمی‌گرداند. به عبارت دیگر باج‌افزار را می‌توان بدافزاری برای اخاذی از کاربر به صورت دیجیتالی دانست. نخستین باج‌افزار در سال ۱۹۸۹ با نام AIDS شناسایی شد [4]. به گزارش سیمنتک در شش ماه نخست سال ۲۰۱۷ سازمان‌ها ۴۲ درصد از اهداف باج‌افزارها را تشکیل می‌دهند. این در حالی است که در سال‌های ۲۰۱۶ و ۲۰۱۵ سازمان‌ها به ترتیب ۳۰ و ۲۹ درصد از اهداف این نوع از بدافزارها را شامل می‌شدند. دلیل اصلی این افزایش مربوط به دو باج‌افزار WannasCry و Petya است [5]. از سال ۲۰۰۵ تا سال ۲۰۱۴ تنها چهارده خانواده از باج‌افزارها تولید شده بودند. این در حالی است که تنها در فصل نخست سال ۲۰۱۵ شاهد ایجاد ۲۷ خانواده از باج‌افزارهای جدید بودیم [6].

حال که در اواخر سال ۲۰۲۰ هستیم، خطرناک‌ترین باج‌افزارها، REvil، Sodinokibi، Nemty، Nephilim و NetWalker را می‌توان نام برد [7]. این باج‌افزارها به دلیل قدرت در گسترش به‌عنوان خطرناک‌ترین باج‌افزارهای این

از کار انداختن ویژگی رونوشت سایه^۵ بر روی فایل‌ها و پارتیشن‌ها، از کار انداختن ویژگی‌های بازیابی و درنهایت غیرفعال‌سازی نرم‌افزارهای ضد بدافزاری و گزارش‌گیری بر روی دستگاه.

در حملات باج‌افزاری، به محض اینکه کد مخرب نصب و راه‌اندازی شد [10]، باج‌افزار درصدد ایجاد ارتباط با سرور کنترلی خواهد بود و منتظر دستور از جانب سرور می‌شود [8]. این دستورها بسته به نوع باج‌افزار و اهداف آن می‌تواند هر چیزی باشد. مانند شناسایی نوع فایل‌هایی که بر روی سامانه قرار دارند، مدت انتظار باج‌افزار تا شروع آلودگی سامانه و دستورهای متعدد دیگر که طراح باج‌افزار تمایل دارد قبل از شروع آلودگی از آن‌ها مطلع شود.

در برخی از باج‌افزارها اطلاعات بسیار مهمی از سامانه قربانی به سرور مرکزی بدافزار، جهت کنترل و دریافت دستور، ارسال می‌شود که از جمله این اطلاعات می‌توان به نشانی IP، سیستم‌عامل، مرورگرها و محصولات ضد بدافزاری نصب‌شده اشاره کرد. این مرحله کلیدی، برای قفل‌گذاری سامانه‌های رایانه‌ای یا رمزنگاری فایل‌ها توسط بدافزارها بر روی دستگاه قربانی لازم است [11]. فایل‌های موردنظر باج‌افزار نسبت به نوع خانواده باج‌افزارها متفاوت است؛ اما از جمله انواع فایل‌های بسیار محبوب بین باج‌افزارها می‌توان به مستندات آفیس مایکروسافت، GIF، JPG و هر نوع فایل دیگری اشاره کرد. بسیاری از گونه‌های باج‌افزارها نه تنها فایل‌ها، بلکه اسامی فایل‌ها را هم رمزنگاری می‌کنند تا قربانی را از پی‌بردن به این که کدام فایل‌ها رمزنگاری شده‌اند، ناتوان سازد. رمزگذاری فایل‌ها به سه صورت متقارن، نامتقارن و یا ترکیبی از این دو انجام می‌پذیرد؛ درنهایت در مرحله اخذی آگاه‌سازی کاربر از نوع حمله انجام‌شده بر روی دستگاه خود توسط باج‌افزار صورت می‌گیرد. بعد از آن که همه فایل‌های موردنظر باج‌افزار رمزگذاری شدند، به قربانی صفحه‌ای مبنی بر آسیب سامانه نمایش داده می‌شود [8].

جهت کشف رفتارهای باج‌افزار، روش‌های گذشته همچون [12] [13] [14] [15]، به دو دسته روش‌های مبتنی بر فریب [16] و روش‌های مبتنی بر رفتار تقسیم می‌شوند [12]. هرچند روش‌های مبتنی بر امضا هم هستند که قادر به شناسایی باج‌افزارها در لحظه صفر نیستند [4] [12].

⁵ Shadow Copy:

فناوری که در سیستم‌عامل ویندوز تعبیه‌شده که امکان کپی‌برداری از فایل‌های پشتیبان را حتی در مواقع کار کردن با فایل‌ها را برای کاربر فراهم می‌سازد.

سال‌ها در نظر گرفته شده‌اند. همچنین، بیماری کوید ۱۹ در این روزها موجب شده تا کارمندان در خانه کارهای خود را انجام دهند و این افزایش کار در منزل موجب افزایش میزان حملات باج‌افزارها شده است. چون دستگاه‌های رایانه‌ای مورد استفاده توسط باج‌افزارها، به اندازه کافی محافظت نمی‌شود؛ همچنین به دلیل تعاملات بالای بین کارمندان، دریافت فایل‌های مخرب حاوی باج‌افزارها افزایش یافته است. همه این موارد موجب شده تا پژوهش پیش رو انجام شود [7].

به طور کلی، باج‌افزارها به دودسته باج‌افزارهای قفل‌گذار و باج‌افزارهای رمزگذار، تقسیم می‌شوند. باج‌افزارهای قفل‌گذار سرویس‌های متعددی مانند دسکتاپ، دستگاه‌های ورودی بر روی سیستم‌عامل قربانی را قفل کرده و فعالیت‌های کاربر را به تعدادی فعالیت مرتبط با فرآیند واریز مبلغ معین‌شده توسط باج‌افزار محدود می‌سازد [3]؛ اما نوع دیگر باج‌افزار یعنی رمزگذار، با رمزگذاری داده‌ها و فایل‌های شخصی کاربر سعی در اعمال محدودیت برای کاربر می‌کند.

یک حمله موفق از سوی باج‌افزار از پنج مرحله تشکیل می‌شود: ۱- استقرار ۲- نصب و راه‌اندازی ۳- دستور و کنترل ۴- تخریب ۵- اخذی [8]. در نخستین مرحله حمله، باج‌افزار نیازمند به بارگذاری فایل اصلی بر روی سامانه قربانی است که برای این کار می‌تواند از بردارهای حمله متعددی مانند رایانه^۱، بهره‌گیری از آسیب‌پذیری‌های متعدد، بارگذاری و راه‌اندازی خودکار استفاده کند. گام بعدی یعنی مرحله نصب و راه‌اندازی می‌تواند بسیار پیچیده باشد. در بسیاری از گونه‌های جدید باج‌افزارهای رمزنگار، ابتدا از ویروس‌های ماکرو و یا پی‌دی‌اف آلوده جهت ورود به سامانه استفاده می‌کنند [9]؛ سپس به محض اینکه بدافزار وارد دستگاه شد، کد بدخواه خود را اجرا کرده و سپس دستگاه میزبان را مورد تحلیل قرار می‌دهد تا واقعی بودن و یا محیط تحلیل (جعبه‌شنی^۲) بودن سامانه را شناسایی کند؛ سپس، باج‌افزار با به‌کارگیری روش‌هایی مانند استفاده از نشانی MAC^۳ سعی می‌کند خود را منحصر به فرد کنند تا طراح باج‌افزار اطلاع داشته باشد که کدام دستگاه آلوده شده است. بعد، باج‌افزار چندین اسکریپت برای اطمینان از غیرفعال بودن دستگاه‌های حفاظتی بر روی دستگاه قربانی اجرا می‌کند. از جمله این فن‌ها را می‌توان به موارد زیر اشاره کرد:

¹ C2 (Command & Control)

² E-mail

³ Sandbox

⁴ media access control address

۲- مطالعات پیشین

در این قسمت، اطلاعات تکمیلی در مورد باج‌افزارها و نحوه شناسایی روش‌های ارائه‌شده در مقالات گذشته به‌همراه نقاط قوت و ضعف آن‌ها شرح داده می‌شود:

۲-۱- باج‌افزارها و انواع آن

نخستین حمله باج‌افزارها در سال ۱۹۸۹ توسط دکتر جوزف پوپ^۳، پژوهش‌گر ایدز، آغاز شد و با توزیع ۲۰,۰۰۰ دیسک فلاپی به پژوهش‌گران که بیش از نود کشور جهان را شامل می‌شدند، حمله را انجام داد و ادعا کرد که این دیسک‌ها حاوی برنامه‌ای هستند که با یک پرسش‌نامه، بررسی می‌کند که آیا فرد دارای ایدز است یا خیر. با این حال، این دیسک همچنین حاوی یک برنامه بدافزار بود که در ابتدا در رایانه‌ها خفته باقی‌مانده بود. پس از نود بار روشن شدن رایانه، این بدافزار پیامی را برای پرداخت ۱۸۹ دلار و ۳۷۸ دلار دیگر برای اجاره نرم‌افزار نشان می‌داد. این حمله باج‌افزار به‌عنوان AIDS Trojan یا همان PC Cyborg معروف شد. این در حالی است که به‌هیچ‌وجه نیاز به پرداخت مبلغی نبود. این باج‌افزار تنها فایل‌ها را در دیسک پنهان و نام آن‌ها را رمزگذاری می‌کرد. همچنین، کد بازگشایی در داخل کد باج‌افزار وجود داشت. این باج‌افزار از رمزنگاری متقارن که کلید رمزگشایی آن در باج‌افزار بوده استفاده می‌کرد؛ لذا به این فکر افتادند که از رمزهای نامتقارن برای رمزگذاری استفاده کنند و کلید رمز را در سرور کنترل نگهداری کنند.

در سال‌های ۲۰۰۵ و ۲۰۰۶، باج‌افزارهایی مانند Gpcode، Krotten، Archiveus، TROJ.RANSOM.A، Cryzip و MayArchive با افزایش اندازه کلید رمزگذاری RSA برای قفل‌گذاری فایل‌های قربانیان استفاده کردند. باج‌افزار Gpcode.AG، که در ژوئن ۲۰۰۶ کشف شد، با یک کلید عمومی ۶۶۰ بیتی RSA رمزگذاری می‌شد؛ در حالی که، در ژوئن ۲۰۰۸، گونه دیگری از این باج‌افزار با نام Gpcode.AK با استفاده از یک کلید RSA 1024 بیتی شناسایی شد. اعتقاد بر این بود که به‌اندازه کافی غیرقابل شکست است.

باج‌افزار CryptoLocker با استفاده از بستر دیجیتال بیت‌کوین برای جمع‌آوری پول باج به‌عنوان یکی از برترین باج‌افزارها به‌شمار می‌آید که در سال ۲۰۱۳ انتشار یافت و حدود ۲۷ میلیون دلار از کاربران آلوده‌شده، باج دریافت کرده است. این باج‌افزار یک جفت‌کلید ۲۰۴۸ بیتی RSA

³ Joseph Popp

روش‌های مبتنی بر فریب با استفاده از فایل‌های طعمه باج‌افزار را شناسایی می‌کنند. روش‌های مبتنی بر فایل نیز بر اساس میزان استفاده بر روی فایل‌ها تصمیم‌گیری می‌کنند. ما در این مقاله روشی را ارائه می‌دهیم که از هر دو روش مبتنی بر رفتار و مبتنی بر فریب استفاده کند.

در این مقاله، یک سامانه تحلیل باج‌افزار، جهت تحلیل و همچنین دسته‌بندی باج‌افزارها ارائه شده است. در رویکرد مطرح‌شده، با استخراج ویژگی‌هایی همچون آنتروپی شانون^۱، تعداد فایل‌های اضافه‌شده در مسیر فایل‌های عسل^۲، دسترسی به VSSAdmin، دسترسی به Recent files، تغییر حجم فایل‌ها و نحوه رمزگذاری فایل‌های عسل و سپس با ایجاد یک مجموعه داده از این ویژگی‌ها و در نهایت استفاده از الگوریتم جنگل‌ها تصادفی جهت آموزش یک مدل دسته‌بند، می‌توان رفتارهای باج‌افزاری را شناسایی و باج‌افزارها را بر اساس ویژگی‌های مطرح‌شده دسته‌بندی کرد. به‌منظور مقایسه نتایج به‌دست‌آمده در این مقاله، از مجموعه نمونه باج‌افزارهای به‌کاربرده‌شده در [17] استفاده شده است. نوآوری‌های مطرح‌شده در این مقاله در زیر فهرست شده‌اند:

۱. استفاده از فایل‌های عسل جهت تحریک باج‌افزارها است که با روش‌های گذشته به‌دلیل اهمیت‌دادن در محل قراردادن فایل و کاهش تعداد فایل به‌دلیل انتخاب نوع فایل تفاوت دارد.

۲. استخراج ویژگی‌هایی جدید، جهت شناسایی باج‌افزارها، که ارزیابی اختلاف بین فایل‌های دامی که استفاده می‌کند، تفاوت زیادی را بین خانواده‌های مختلف جهت تمایز، نشان می‌دهد.

۳. دسته‌بندی باج‌افزارها بر اساس خانواده‌هایشان به‌کمک ویژگی‌های استخراج‌شده که قادر است بین بدافزارها، خانواده‌های سالم و باج‌افزارها دسته‌بندی انجام دهد.

در ادامه، در بخش دوم به کارهای مرتبط در حوزه شناسایی باج‌افزارها و نحوه کار روش‌های ارائه‌شده در مقالات گذشته و نقاط قوت و ضعف این روش‌ها پرداخته می‌شود. روش پیشنهادی جهت شناسایی خانواده باج‌افزارها در قسمت سوم ارائه شده و در بخش چهارم، نتایج به‌دست‌آمده از اعمال روش پیشنهادی بر روی مجموعه‌ای از باج‌افزارهای [17] شرح داده شده است. همچنین، در بخش پایانی، نتیجه‌گیری از روش مطرح‌شده توضیح داده می‌شود.

¹ Shannon Entropy

² Honey files:

این فایل‌های فایل‌هایی قلابی می‌باشند که تأثیرات باج‌افزارها بر روی این نوع از فایل‌ها بررسی می‌شوند.

درون دستگاه خود، وی را تهدید به انتشار اطلاعات دزدیده شده می‌کند. در حمله نشت، بدافزارها داده‌های حساس میزبان را به صورت متناوب برای یک مهاجم ارسال می‌کنند و مهاجم، قربانی را به انتشار اطلاعات تهدید می‌کند، مگر مبلغی به عنوان باج پرداخت شود.

در سال ۲۰۱۶، یک فشار جدید از باج‌افزار ظاهر شد که سرورهای JBoss را هدف قرار داد. این نسل با نام SamSam معرف شد تا روند فیشینگ یا بارگیری‌های غیرقانونی را به نفع استثمار آسیب‌پذیری بهره ببرد. این بدافزار از یک حمله بر روی Remote Desktop Protector استفاده می‌کند تا رمزهای ضعیف را حدس بزند. این باج‌افزار جهت حملات بر روی سرورهای دستگاه‌های دولتی و مراکز بهداشتی و درمانی طراحی شده است.

بدافزار WannaCry یکی از باج‌افزارهای معروف است که سوءاستفاده خود را از طریق یک آسیب‌پذیری بر روی سیستم‌عامل ویندوز انجام می‌دهد و فایل‌های موجود در رایانه قربانی را به طوری غیرقابل بازگشت، رمز و از کاربر رایانه قربانی درخواست باج از طریق بیت کوین برای بازگشایی رمز فایل‌ها می‌کند. این بدافزار به صورت غیرقابل باوری در سراسر جهان پخش شده که یکی از مهم‌ترین عامل گسترش WannaCry نفوذ به تعدادی از سامانه‌های مهم و مشهور، از جمله بسیاری از مراکز ملی بهداشت کشور انگلیس است. کد برنامه این بدافزار مبهم‌سازی نشده و برای تجزیه و تحلیل تا حدودی آسان است. پس از نخستین اجرای این بدافزار بر روی رایانه‌های قربانی، سعی می‌کند به سرور دسترسی پیدا کند. در صورت عدم امکان، به جستجو و رمزنگاری فایل‌ها با استفاده از فرمت‌های مهم، از فایل‌های Microsoft Office گرفته تا MP3 و MKV، می‌پردازد و آن‌ها را در دسترس کاربر قرار نمی‌دهد؛ سپس یک اعلامیه باج را نمایش می‌دهد و برای رمزگشایی فایل‌ها تا سیصد دلار در بیت کوین می‌خواهد؛ همچنین، باج‌افزار Petya از آسیب‌پذیری CVE-2017-0144 در اجرای پروتکل مسدود کردن پیام سرور از پیام میکروسافت سوءاستفاده می‌کند. پس از سوءاستفاده از این آسیب‌پذیری، این باج‌افزار مسیر اصلی روشن شدن سیستم را به جای رمزگذاری بر روی فایل‌ها مسدود می‌کند. در نخستین اجرا، یک پیام برای انجام راه‌اندازی مجدد رایانه به کاربر می‌دهد، پس از آن رایانه غیرقابل دسترس خواهد شد. این باعث می‌شود سیستم‌عامل نتواند به فایل‌های خود دست یابد و راهی برای رمزگشایی فایل‌ها وجود نخواهد داشت.

باج‌افزار Sanata نیز مشابه باج‌افزار Petya عمل

ایجاد می‌کرد و در سرور کنترلی قرار می‌داد و به کاربران سه روز فرصت می‌داد تا پرداخت باج را انجام دهند.

در کنار باج‌افزارهای رمزگذار، باج‌افزارهای غیر رمزگذار در سال ۲۰۱۰ به وجود آمدند. یکی از این موارد WinLock می‌باشد. WinLock دسترسی به سیستم‌عامل را محدود کرده است و از کاربران خواسته تا کدی که می‌تواند برای بازکردن قفل دستگاه‌هایشان استفاده شود به صورت پیام کوتاه برای شماره‌ای خاص ارسال شود. این پیام کوتاه با ارزش حدود ۱۰ دلار آمریکا بود. این کلاهبرداری از تعداد زیادی کاربر در سراسر روسیه و کشورهای همسایه اخذی کردند. طبق گفته‌ها، این بدافزار بیش از شانزده میلیون دلار درآمد داشت.

همچنین در سال ۲۰۱۱، باج‌افزاری، اختراع فعال‌سازی محصول ویندوز را شبیه‌سازی کرد تا از قربانیان اخذی کند. این باج‌افزار پیغامی به کاربران نمایش می‌داد که نصب ویندوز رایانه به دلیل مجوز تقلبی دچار نقض شده است و نیاز به فعال‌سازی مجدد دارد. گزینه فعال‌سازی برخط (مانند فرآیند واقعی) ارائه شد، اما در دسترس نبود و کاربر را ملزم به تماس با یکی از شش شماره بین‌المللی برای وارد کردن کد شش رقمی می‌کرد. برخلاف این که این بدافزار ادعا می‌کرد این تماس رایگان خواهد بود، از طریق یک اپراتور در کشوری با نرخ تلفنی بین‌المللی بالا، تماس را در انتظار قرار می‌داد و کاربر هزینه تماس بین‌المللی زیادی را متقبل می‌شد.

در سال ۲۰۱۲، یک تروجان باج‌گیر به نام Reveton که خود برگرفته از ایده باج‌افزار Citadel است، شروع به گسترش کرد. این باج‌افزار هشدارهایی از طرف دادگاه نشان می‌داد و ادعا می‌کرد از این رایانه برای فعالیت‌های غیرقانونی، مانند بارگیری نرم‌افزار بدون مجوز استفاده شده است. این اختراع به کاربر اطلاع می‌دهد که برای بازکردن قفل دستگاه خود، باید با استفاده از بیت‌کوین جریمه پرداخت شود. برای افزایش باورپذیری جهت ردیابی رایانه توسط نیروی انتظامی، نشانی IP رایانه در صفحه‌نمایش نشان داده می‌شد. در حالی که، برخی نسخه‌ها فیلم‌هایی را از وب کم قربانی نشان می‌دهند تا باورپذیری کاربر را افزایش دهد.

نسل دیگر باج‌افزارهای غیر رمزگذاری باج‌افزارهای نشت^۱ است. هدف این باج‌افزار، یک حمله بدون رمزنگاری است. در این حمله، به جای قطع دسترسی قربانی به اطلاعات

^۱ Doxware

می‌کند. عمده تفاوت این دو باج‌افزار در نوع قفل کردن رایانه است. بدافزار Santa از Master Boot Record (MBR) برای قفل کردن رایانه استفاده می‌کند؛ درحالی‌که باج‌افزار Petya از Master File Table (MFT) برای قفل کردن رایانه استفاده می‌کند. MBR بخشی از لوح سخت است. این اطلاعات در مورد سیستم فایل‌هایی است که به‌وسیله پارتیشن‌های لوح سخت مختلف مورد استفاده قرار می‌گیرد و همچنین اینکه کدام سیستم‌عامل در کدام پارتیشن قرار دارد. اگر MBR خراب یا رمزگذاری شود، رایانه دسترسی به یک قطعه از اطلاعات مهم را از دست می‌دهد. اگر رایانه نتواند سیستم‌عامل را پیدا کند، نمی‌تواند آن را روشن کند؛ لذا باج‌افزارهایی مانند Satana از این تنظیم استفاده و رمزنگاری خود را با قابلیت‌های bootlocker تقویت کردند. باج‌افزار نویسان مقدار MBR را عوض، آن را با کد یادداشت باج جایگزین می‌کنند و MBR را درجایی دیگر رمزگذاری و انتقال می‌دهند. به‌نظر می‌رسد که Satana به‌تازگی کار باج‌افزار خود را آغاز کرده و هنوز به‌خوبی گسترده نشده است و پژوهش‌گران نقص‌هایی در کد آن مشاهده کرده‌اند. باین‌وجود، شانس خوبی وجود دارد که با گذشت زمان بهبود یابد و به یک تهدید بسیار جدی تبدیل شود.

نسل دیگر باج‌افزارها، باج‌افزارهای تلفن همراه هستند که تاکنون تمایلی به رمزگذاری داده‌ها نداشته‌اند و در گروه باج‌افزارهای غیر رمزگذاری قرار می‌گیرند. به‌طورمعمول، باج‌افزارهای تلفن‌های همراه مسدودکننده هستند. بیشتر باج‌افزار تلفن همراه سکوی Android را هدف قرار می‌دهد، زیرا امکان نصب برنامه‌ها را از منابع شخص ثالث فراهم می‌کند. باج‌افزارها به‌طورمعمول به‌صورت فایل APK نصب‌شده توسط یک کاربر مظلوم توزیع می‌شود. این بدافزارها سعی می‌کنند پیام مسدودکننده را قبل از اجرای هر برنامه دیگر نشان دهند.

روش‌های قفل‌گذاری مختلفی در تلفن‌های همراه مبتنی بر سیستم‌عامل iOS مانند بهره‌برداری از حساب‌های iCloud و استفاده از سامانه Find My iPhone استفاده شده است. به‌عنوان نمونه، در نسخه iOS 10.3، در مرورگر سافاری با استفاده از پنجره‌های پاپ‌آپ JavaScript راه نفوذ برای قفل‌گذاری را باز می‌کرد.

۲-۲- روش‌های شناسایی باج‌افزارها

روش‌های قفل‌گذاری دیگر باج‌افزارها، باج‌افزارهای تلفن همراه هستند که تاکنون تمایلی به رمزگذاری داده‌ها نداشته‌اند و در گروه باج‌افزارهای غیر رمزگذاری قرار می‌گیرند. به‌طورمعمول، باج‌افزارهای تلفن‌های همراه مسدودکننده هستند. بیشتر باج‌افزار تلفن همراه سکوی Android را هدف قرار می‌دهد، زیرا امکان نصب برنامه‌ها را از منابع شخص ثالث فراهم می‌کند. باج‌افزارها به‌طورمعمول به‌صورت فایل APK نصب‌شده توسط یک کاربر مظلوم توزیع می‌شود. این بدافزارها سعی می‌کنند پیام مسدودکننده را قبل از اجرای هر برنامه دیگر نشان دهند.

روش‌های قفل‌گذاری مختلفی در تلفن‌های همراه مبتنی بر سیستم‌عامل iOS مانند بهره‌برداری از حساب‌های iCloud و استفاده از سامانه Find My iPhone استفاده شده است. به‌عنوان نمونه، در نسخه iOS 10.3، در مرورگر سافاری با استفاده از پنجره‌های پاپ‌آپ JavaScript راه نفوذ برای قفل‌گذاری را باز می‌کرد.

۱ Scareware:

این نوع از بدافزارها با نمایش گزارش‌های قلابی، به کاربر هشدار می‌دهد تا به‌منظور جلوگیری از آسیب به دستگاه خود ابزار ضد بدافزاری معرفی‌شده را بارگیری و نصب کند تا بدافزارهای موجود بر روی سیستم خود را به‌کمک این ابزار از بین ببرد اما در اصل از این طریق بدافزار را وارد سیستم قربانی می‌کند.

در سال ۲۰۱۹، پژوهش‌گران ثابت کردند که ممکن است دوربین‌های DSLR نیز به باج‌افزارها آلوده شوند. دوربین‌های دیجیتالی، اغلب از پروتکل انتقال تصویر استفاده می‌کنند (پروتکل استاندارد PTP - مورد استفاده برای انتقال فایل‌ها). محققان دریافتند که می‌توان از آسیب‌پذیری‌های موجود در پروتکل سوءاستفاده کرد و دوربین هدف را با استفاده از باج‌افزار آلوده کرد.

در بین این بدافزارها CryptoLocker یکی از سودآورترین باج‌افزار زمان خود بود. این باج‌افزار فقط به‌دنبال فایل‌ها می‌گشت و آن‌ها را رمز می‌کرد. بین سپتامبر و دسامبر ۲۰۱۳، CryptoLocker بیش از ۲۵۰,۰۰۰ دستگاه را آلوده کرد. که بیش از سه میلیون دلار درآمد برای سازندگانش فراهم کرده بود.

روش‌های قفل‌گذاری مختلفی در تلفن‌های همراه مبتنی بر سیستم‌عامل iOS مانند بهره‌برداری از حساب‌های iCloud و استفاده از سامانه Find My iPhone استفاده شده است. به‌عنوان نمونه، در نسخه iOS 10.3، در مرورگر سافاری با استفاده از پنجره‌های پاپ‌آپ JavaScript راه نفوذ برای قفل‌گذاری را باز می‌کرد.

Fusob یکی از بزرگ‌ترین خانواده‌های باج‌افزار تلفن همراه است. بین آوریل ۲۰۱۵ و مارس ۲۰۱۶، حدود ۵۶ درصد از باج‌افزار تلفن‌های همراه Fusob بودند. مانند یک باج‌افزار معمولی تلفن همراه، از ترفندهای اخاذی برای

در فایل‌ها است. در نهایت، راه‌انداز سوم به کمک الگوریتم جنگل‌های تصادفی^۴ اقدام به شناسایی باج‌افزار می‌کند. این روش در مقابل باج‌افزارهایی که از توابع رمزگذاری ناشناخته استفاده می‌کنند، کارساز نیست.

یکی دیگر از روش‌های پیشنهادی در این حوزه روش CryptoDrop است که در [9] شرح داده شده است. این روش شامل، سامانه‌ای پیش‌هشداردهنده برای شناسایی باج‌افزار است. این روش، تمامی فعالیت‌های فایل را مورد بررسی قرار داده و در مورد شناسایی عمل‌های مشکوک به کاربر هشدار می‌دهد. شناسایی در این سامانه با استفاده از سه ویژگی تغییر در نوع فایل، مقدار شباهت فایل و آنتروپی صورت می‌گیرد. البته این روش، هیچ تضمینی در رابطه با داده‌هایی که قبل از شناسایی از دست می‌رود، نداده و همچنین امکان ترمیم فایل‌های رمزنگاری شده هم در این سامانه وجود ندارد. یکی از ویژگی‌هایی که در این سامانه در نظر گرفته شده است، ویژگی تغییر در نوع فایل‌ها بعد از رمزگذاری فایل‌ها است؛ اما این ویژگی نمی‌تواند برای تمامی باج‌افزارها صادق باشد؛ به‌عنوان مثال باج‌افزار satana هیچ تغییری در نوع فایل ایجاد نکرده و تنها نام آن را تغییر می‌دهد.

سیونگ و همکارانش، [12]، توانستند با استفاده از تحلیل مبتنی بر رفتار باج‌افزارها از فایل‌های سالم تشخیص دهد. روش ایشان، بدافزارها را در محیط جعبه‌شنی اجرا می‌کند و بر اساس دنباله فراخوانی‌های سامانه‌ای که توسط باج‌افزار فراخوانی می‌شود، n-gram هایی را ایجاد می‌کند. با تحلیل آماری بر روی این n-gram ها، ویژگی‌هایی را استخراج می‌کند که قادر است با استفاده از یادگیری ماشین، باج‌افزارها را از فایل‌های سالم تمییز کند. هرچند این روش، با استفاده از مبهم‌سازی رفتاری باج‌افزار، یعنی اضافه و تغییردادن در ترتیب فراخوانی‌های سامانه‌ای قابل‌گریز است. تانگ و همکاران، [15]، RansomSpector را جهت دسته‌بندی خانواده بدافزارها ارائه دادند. این تحلیل‌گر باج‌افزار همچون روش ما [21]، بدافزار را سطح درایورهای سیستم‌عامل مورد بررسی قرار می‌دهد تا در مقابل باج‌افزارهایی که به سیستم‌عامل بدون دریافت مجوز عبور می‌کنند، از سامانه محافظت کند؛ ولی RansomSpector فقط ارتباط‌های فایلی و فعالیت تحت شبکه را در نظر می‌گیرد. در حالی محیط تحلیل ما قادر است همه فراخوانی‌های سامانه‌ای را نظارت کند. RansomSpector

⁴ Random forest classifier

تعامل باشد، آن‌ها را رصد می‌کند و به‌صورت موازی هم همه تغییرات دسکتاپ کاربر را زیر نظر می‌گیرد و سعی دارد تا رفتارهای شبه باج‌افزاری فایل‌های اجرایی را شناسایی کند. این روش حتی قادر به شناسایی باج‌افزارهای قفل‌گذار نیز است و به‌صورت بلادرنگ باج‌افزارها را شناسایی کند.

اما در [20]، شناسایی باج‌افزار بر روی سیستم‌عامل اندروید مطالعه شده است. این روش، به دو صورت ایستا و پویا اقدام به شناسایی رفتار باج‌افزارها در سطح کاربر می‌کند. این روش از تحلیل لکه‌گذاری ایستا و شبیه‌سازی جریان از فراخوانی‌های توابع را که منجر به رمزنگاری فایل‌ها یا قفل صفحه‌نمایش می‌شوند، بهره می‌برد. این روش رفتارهای تهدیدآمیز بر پایه یادگیری و فن پردازش زبان طبیعی (NLP) برای شناسایی استفاده می‌کند.

روش ارائه‌شده در [6] با نام EldeRan، یک روش تحلیل پویا با رویکرد یادگیری ماشین است. این روش باج‌افزارها را بر اساس مجموعه فعالیت‌هایی که برنامه‌ها در مرحله نصب انجام می‌دهند، شناسایی می‌کند. فرضیه اصلی این سیستم این است که باج‌افزارها شامل ویژگی‌های یکتایی هستند که در زمان تحلیل پویای آن‌ها شباهت زیادی به هم دارند؛ پس می‌توان از این ویژگی‌ها برای شناسایی باج‌افزارها استفاده کرد. این سامانه ابتدا ویژگی‌های مرتبط به رفتار باج‌افزارها را انتخاب کرده و سپس برنامه تازه‌نصب‌شده بر روی رایانه را به‌وسیله الگوریتم یادگیری ماشین بدون استفاده از فن‌های بر پایه اکتشافی یا امضا دسته‌بندی می‌کند. این روش نشان می‌دهد که یک باج‌افزار می‌تواند با دقت بالایی بر اساس ویژگی‌های محدودی قبل از آلودگی شناسایی شود.

روش مطرح‌شده در [17] از روش یادگیری ماشین برای فعالیت‌های لوح سخت استفاده می‌کند. ویژگی‌های انتخاب‌شده برای یادگیری ماشین از میلیون‌ها درخواست ورودی/خروجی استخراج شده‌اند. این ویژگی‌ها در دو حالت جمع‌آوری شده‌اند: ۱- زمانی که سامانه وضعیت عادی دارد و هیچ‌گونه باج‌افزاری بر روی آن موجود نیست ۲- زمانی که سامانه مورد حمله باج‌افزار قرار گرفته باشد. راه‌حل پیشنهادی این روش، از سه راه‌انداز^۱ ساخته شده است. یک راه‌انداز مسئول ترمیم فایل‌ها است؛ برای هر عملیات نوشتن و باز نام‌گذاری^۲ از فایل مربوطه یک نسخه پشتیبان تولید می‌شود. راه‌انداز دوم هم مسئول تشخیص پایه رمزگذاری^۳

¹ Driver

² Rename

³ Cryptographic primitive

این امر ما را قادر می‌سازد، برخلاف روش‌های گذشته که فقط قادر بود باج‌افزارها را تشخیص دهند، با استفاده از ابزارمان، خانواده باج‌افزارها، بدافزارها و فایل‌های سالم را از هم تمییز کنیم. چون هم مبتنی رفتار و هم مبتنی بر دام در حال نظارت بر روی باج‌افزارها هستیم.

۳- روش پیشنهادی جهت شناسایی خانواده باج‌افزارها

در این بخش، تمامی مراحل روش پیشنهادی برای شناسایی خانواده باج‌افزارها به‌طور کامل توضیح داده می‌شود. معماری کلی روش پیشنهادی در شکل (۱) نشان داده شده است. باج‌افزارها به برنامه‌های مخربی گفته می‌شود که رفتارهای باج‌گیرانه را از خود نشان می‌دهند. و بدافزارها به برنامه‌های رایانه‌ای گفته می‌شود که از پروتکل‌های امنیتی تجاوز می‌کنند. از طرفی برنامه‌های سالم به برنامه‌های رایانه‌ای گفته می‌شود که بعد از تحلیل هیچ نقض امنیتی در آن مشاهده نشده باشد.

استفاده از الگوهایی خواندن و نوشتن بر روی فایل‌ها و ارتباط‌های شبکه، به‌صورت تجربی استخراج شده است، قادر است خانواده باج‌افزارها را شناسایی کند.

رامش و همکارش، [14]، با استفاده از تئوری ماشین‌های متناهی، قادر است، تغییرات ایجاد در وضعیت دستگاه‌های رایانه‌ای را بر اساس نوع استفاده، میزان پایداری و عملیات‌های دیگر بر روی منابع، نظارت کند و به وضعیت دستگاه نمره‌ای تخصیص دهد و اعلام کند که آیا دستگاه دارای باج‌افزار است یا خیر. این روش بعد از اجرای هر نمونه از خانواده باج‌افزارها، از روی رفتار باج‌افزار، مدل ماشین متناهی استخراج می‌کند. مدل‌های ماشین متناهی را با استفاده الگوریتم‌های تصمیم‌گیری یادگیری ماشین، جهت تشخیص باج‌افزار مورد استفاده قرار می‌دهد. این روش حتی قادر به دسته‌بندی خانواده باج‌افزارها هم نیست و فقط باج‌افزارها را از فایل‌های سالم متمایز می‌کند.

با وجود همه روش‌هایی که مطرح شده، روش ما قادر است همه رفتارهای باج‌افزارها را از جمله فعالیت‌های شبکه، همه فراخوانی‌های سامانه‌ای و تعاملات مربوط به فایل‌ها را در جهت کشف رفتارهای مخرب باج‌افزارها به‌دست می‌آورد.



(شکل-۱): فرآیند طرح پیشنهادی (در معماری پیشنهادی ابتدا فایل اجرایی بر روی جعبه‌شنی اجرا می‌شود و سپس بر اساس ویژگی‌های مطرح شده که از تعاملات باج‌افزار با سیستم فایل استخراج می‌شوند و اعمال آن بر مدل ساخته شده می‌توان خانواده باج‌افزار را شناسایی کرد.)

سامانه فایل‌ها توسط مینی‌فیلتر نظارت می‌شود و ویژگی‌های متمایزکننده باج‌افزارها استخراج می‌شود. در گام بعد، یک ماتریس از تمامی ویژگی‌های استخراج شده از کل برنامه‌ها تهیه و با ایجاد یک مدل به‌وسیله الگوریتم جنگل‌های

همان‌طور که در شکل (۱) مشاهده می‌شود، ابتدا هرکدام از باج‌افزارها و برنامه‌های سالم بر روی جعبه‌شنی که ساختار آن در بخش‌های بعد توضیح داده خواهد شد، اجرا می‌شوند؛ سپس، در زمان اجراء تمامی تعاملات برنامه با

تصادفی، دسته‌بندی نمونه‌ها انجام می‌شود.

۱-۳- محیط جعبه‌شنی

یکی از مهم‌ترین مراحل، آماده‌سازی محیطی مناسب جهت اجرای فایل‌های اجرایی بر روی جعبه‌شنی است. همان‌طور که در مقدمه بیان شد، بسیاری از باج‌افزارها فایل‌های شخصی موجود بر روی سامانه قربانی را مورد هدف قرار داده و با رمزگذاری بر روی فایل‌های کاربر سعی می‌کنند تا درازای واریز مبلغی از سوی قربانی کلید فایل‌های رمزگذاری شده بر روی دستگاه را به کاربر ارائه دهند. پس به‌منظور تحلیل باج‌افزار باید محیطی آماده شود که بتوان در یک مدت محدود رفتارهای باج‌افزار را مشاهده کرد.

فایل‌های عسل^۱ جهت شناسایی فعالیت‌های مخرب بر روی سامانه قرار می‌گیرند. این نوع فایل‌ها در صورت دسترسی و تغییر از سوی افراد متخلف [22] [16] یا بدافزارها می‌توانند دریافتن برنامه‌های مخرب ما را یاری کنند. این فایل‌ها در اصل هیچ ارزشی برای کاربر نداشته و هدف از آن‌ها شناسایی اقدامات مخرب است. با قراردادن این فایل‌ها در نواحی که پتانسیل بالایی در مواجهه‌شدن با اقدامات مخرب دارند، می‌توانند کمک بسیار زیادی در شناسایی باج‌افزارها داشته باشند. می‌توان با قراردادن این نوع از فایل‌ها در نقاط مختلف سامانه و رصد مداوم این فایل‌ها افراد متخلف و همچنین بدافزارهای مختلفی را که بر روی فایل‌ها تأثیر مخربی دارند، شناسایی کرد. از جمله ویژگی‌هایی که این نوع از فایل‌ها باید داشته باشند، می‌توان به موارد زیر اشاره کرد [22]:

۱. واقعی به نظر رسیدن: به این معنی که باج‌افزارها این نوع از فایل‌ها را به‌عنوان فایل واقعی ببینند و همانند دیگر فایل‌های اصلی با آن‌ها رفتار کنند.
۲. تحریک‌کننده باشند: بایستی این نوع از فایل‌ها برای باج‌افزارها و در حالت کلی برای بدافزارها طوری تعیین شوند تا بدافزارها رفتار واقعی خود را نشان دهند.
۳. قابلیت دسترسی: فایل‌های عسل باید در مسیرهایی قرار گیرند که باج‌افزارها به‌راحتی به آن‌ها دسترسی داشته باشند.
۴. قابلیت شناسایی: این نوع از فایل‌ها باید به‌گونه‌ای باشند که با رصد این نوع فایل‌ها، فایل اجرایی مخرب شناسایی شود.
۵. تنوع: باج‌افزارهای مختلف فایل‌های مختلفی را

مورد هدف قرار می‌دهند؛ پس برای این که محیط اجرا را برای بیش‌تر باج‌افزارها تحریک‌پذیر کنیم، باید فایل‌های عسل متنوع باشند.

فایل‌های عسل در نظر گرفته‌شده بر روی جعبه‌شنی را در این مقاله می‌توان به چهار دسته تقسیم کرد که در جدول (۱) بیان شده است. این نوع فایل‌ها بیشترین آسیب‌دیدگی را در مقابل حملات باج‌افزارها متحمل می‌شوند [19]. پس برای اینکه بتوان از فایل‌های عسل به‌منظور شناسایی باج‌افزارها استفاده کرد، بایستی این نوع از فایل‌ها در مسیرهای مشخصی قرار گیرند تا با تحریک باج‌افزارها، بتوان رفتار تخریبی آن‌ها را رصد کرد. از آنجاکه باج‌افزارها از روش‌های مختلفی برای پیمایش تمام فایل‌های موجود بر روی دستگاه استفاده می‌کنند، بایستی این فایل‌ها چنان جانمایی شوند تا در مدت‌زمان محدود تحلیل یعنی بیست دقیقه اجرا برای هر باج‌افزار [19]، بتوان رفتار بدخواهانه باج‌افزارها را به‌دست آورد.

از جمله چالش‌هایی که در شناسایی باج‌افزار با استفاده از فایل‌های عسل روبه‌رو هستیم، می‌توان به موارد زیر اشاره کرد:

۱. باج‌افزارها تشخیص دهند که این فایل‌ها، فایل‌های عسل هستند. در این صورت، باج‌افزارها به رمزگذاری این فایل‌ها نخواهند کرد.
۲. فایل‌های عسل، در زمان محدودی که برای تحلیل باج‌افزار اختصاص داده شده است، رمزگذاری نشوند. در این صورت تأثیر باج‌افزارها بر روی فایل‌های عسل غیرقابل رصد خواهد بود.

(جدول-۱): فایل‌های هدف باج‌افزارها

| | |
|--------------|----------------------------------|
| دسته فایل‌ها | پسوندهای موردنظر |
| مستندات | txt, doc(x), ppt(x), xls(x), pdf |
| لایسنس | key, pem, crt, cer |
| آرشیو | zip, rar |
| مدیا | jp(e)g, mp3, avi |

از آنجاکه ما هیچ دسترسی به کد منبع^۲ باج‌افزارها نداریم [23] پس اطلاعی از توانایی شناسایی فایل‌های عسل به‌وسیله باج‌افزارها در اختیار نداریم و حتی در صورت آگاهی از این امکان در باج‌افزار، چگونگی انجام این عمل توسط باج‌افزار هم برای ما مبهم است؛ اما می‌توان جهت گریز از چالش‌های مطرح به‌صورت زیر عمل کرد:

² Source code

¹ Honey Files

۱. همان‌طور که در جدول (۱) مشاهده می‌شود، فایل‌ها متنوع هستند. برخی از باج‌افزارها فایل‌هایی با یک حجم کمتر از یک مقدار پیش‌فرض را رمزگذاری نمی‌کنند، پس لازم است تا فایل‌های عسل حجم‌های متنوعی داشته باشند.

۲. یکی دیگر از کارهایی که می‌توان انجام داد، استفاده از نام‌های یکتا و بامعنا برای فایل‌های عسل است. به این منظور فایل‌های عسل نباید اسامی تکراری یا اسامی خاصی داشته باشند. در بسیاری از موارد باج‌افزارها می‌توانند با شناسایی فایل‌ها با اسامی خاص و یا تکراری در محیط‌های تحلیل، رفتار خود را پنهان کنند.

۳. اما چالش دیگری که همواره در استفاده از فایل‌های عسل برای شناسایی باج‌افزارها وجود دارد، رمزگذاری و دست‌کاری فایل‌های عسل است. از آنجاکه ما هیچ اطلاعی در مورد چگونگی پیمایش فایل‌ها توسط باج‌افزارها نداریم، امکان دارد در زمان محدود اجرای باج‌افزار بر روی جعبه‌شنی نتوان رفتار بدخواهانه آن‌ها را شاهد بود و در نتیجه باعث بروز منفی اشتباه شود.

همچنین، قبل از اجرای نسخه‌های مختلف از باج‌افزار، قادر به تشخیص نوع انتخاب و دریافت فایل‌ها توسط باج‌افزار نیستیم تا آنها مورد رمزنگاری قرار بگیرند. ولی عموماً، مسیره‌ها^۱ به‌صورت الفبایی پردازش و پیمایش می‌شوند [8].

به این خاطر، به‌طور معمول C:\\$Recycle.Bin در بیش‌تر موارد جز نخستین دایرکتوری‌هایی است که توسط باج‌افزار مورد حمله قرار می‌گیرد. لذا، ما در این پروژه فایل‌های عسل را در دو فایل با نام‌های C:\\$Decoyfiles\ و C:\ZDecoyfiles\ جای‌گذاری کرده‌ایم؛ همان‌طور که مشاهده می‌کنید، فایل‌های عسل را در دو پوشه قرار داده‌ایم چون برخی از باج‌افزارها همانند باج‌افزار shadow فایل‌ها را به‌صورت الفبایی ولی از پایین به بالا (A تا Z) پیمایش می‌کنند.

۳-۳- استخراج ویژگی‌ها

در معماری پیشنهادی، در زمان ثبت فعالیت‌های فایل به‌وسیله مینی‌فیلتر، استخراج ویژگی‌های متمایزکننده باج‌افزارها صورت می‌گیرد. ویژگی‌های در نظر گرفته‌شده را می‌توان همان‌طور که در جدول (۲) نشان داده‌شده، به هفت گروه دسته‌بندی کرد.

(جدول-۲): فهرست ویژگی‌های در نظر گرفته‌شده

برای سامانه پیشنهادی

| ردیف | ویژگی |
|------|--------------------------------------|
| ۱ | آن‌تروپی فایل‌ها |
| ۲ | تعداد فایل‌های اضافه‌شده |
| ۳ | دسترسی به VSSAdmin |
| ۴ | فایل‌های اجرایی اضافه‌شده |
| ۵ | دسترسی به RecentFiles |
| ۶ | تغییر حجم فایل‌ها |
| ۷ | نحوه رمزگذاری فایل‌ها توسط باج‌افزار |

در زمان اجرای باج‌افزار بر روی جعبه‌شنی، تمامی فعالیت‌های فایل برنامه‌های اجرایی ثبت می‌شوند. روش‌های مختلفی برای رصد فعالیت‌های فایل برنامه‌های اجرایی وجود دارد. به‌عنوان مثال، فعالیت‌های فایل را می‌توان با

^۴ System Service Descriptor Table

^۵ Cryptosystem

^۶ Kernel path protection

^۷ Minifilter driver

۱. همان‌طور که در جدول (۱) مشاهده می‌شود، فایل‌ها متنوع هستند. برخی از باج‌افزارها فایل‌هایی با یک حجم کمتر از یک مقدار پیش‌فرض را رمزگذاری نمی‌کنند، پس لازم است تا فایل‌های عسل حجم‌های متنوعی داشته باشند.

۲. یکی دیگر از کارهایی که می‌توان انجام داد، استفاده از نام‌های یکتا و بامعنا برای فایل‌های عسل است. به این منظور فایل‌های عسل نباید اسامی تکراری یا اسامی خاصی داشته باشند. در بسیاری از موارد باج‌افزارها می‌توانند با شناسایی فایل‌ها با اسامی خاص و یا تکراری در محیط‌های تحلیل، رفتار خود را پنهان کنند.

اما چالش دیگری که همواره در استفاده از فایل‌های عسل برای شناسایی باج‌افزارها وجود دارد، رمزگذاری و دست‌کاری فایل‌های عسل است. از آنجاکه ما هیچ اطلاعی در مورد چگونگی پیمایش فایل‌ها توسط باج‌افزارها نداریم، امکان دارد در زمان محدود اجرای باج‌افزار بر روی جعبه‌شنی نتوان رفتار بدخواهانه آن‌ها را شاهد بود و در نتیجه باعث بروز منفی اشتباه شود.

همچنین، قبل از اجرای نسخه‌های مختلف از باج‌افزار، قادر به تشخیص نوع انتخاب و دریافت فایل‌ها توسط باج‌افزار نیستیم تا آنها مورد رمزنگاری قرار بگیرند. ولی عموماً، مسیره‌ها^۱ به‌صورت الفبایی پردازش و پیمایش می‌شوند [8]. به این خاطر، به‌طور معمول C:\\$Recycle.Bin در بیش‌تر موارد جز نخستین دایرکتوری‌هایی است که توسط باج‌افزار مورد حمله قرار می‌گیرد. لذا، ما در این پروژه فایل‌های عسل را در دو فایل با نام‌های C:\\$Decoyfiles\ و C:\ZDecoyfiles\ جای‌گذاری کرده‌ایم؛ همان‌طور که مشاهده می‌کنید، فایل‌های عسل را در دو پوشه قرار داده‌ایم چون برخی از باج‌افزارها همانند باج‌افزار shadow فایل‌ها را به‌صورت الفبایی ولی از پایین به بالا (A تا Z) پیمایش می‌کنند.

۳-۲- ثبت فعالیت‌های فایل

در زمان اجرای باج‌افزار بر روی جعبه‌شنی، تمامی فعالیت‌های فایل برنامه‌های اجرایی ثبت می‌شوند. روش‌های مختلفی برای رصد فعالیت‌های فایل برنامه‌های اجرایی وجود دارد. به‌عنوان مثال، فعالیت‌های فایل را می‌توان با

^۱ Directory

^۲ Hooking

^۳ Application Programming Interface

پاک‌سازی فایل‌های پشتیبان^۱، فایل‌های اجرایی اضافه‌شده به‌وسیله برنامه اجرایی، رمزگذاری آخرین فایل‌های دست‌کاری‌شده توسط قربانی، تغییرات حجم فایل‌ها پس از رمزگذاری و درنهایت نحوه رمزگذاری فایل‌ها به‌صورت بازنویسی و یا ایجاد یک فایل جدید اشاره کرد. در این قسمت تمام ویژگی‌های یادشده در بالا موردبررسی قرار می‌گیرند.

پاک‌سازی فایل‌های پشتیبان^۱، فایل‌های اجرایی اضافه‌شده به‌وسیله برنامه اجرایی، رمزگذاری آخرین فایل‌های دست‌کاری‌شده توسط قربانی، تغییرات حجم فایل‌ها پس از رمزگذاری و درنهایت نحوه رمزگذاری فایل‌ها به‌صورت بازنویسی و یا ایجاد یک فایل جدید اشاره کرد. در این قسمت تمام ویژگی‌های یادشده در بالا موردبررسی قرار می‌گیرند.

دسترسی به VSSAdmin: بسیاری از باج‌افزارهای جدید سعی می‌کنند تمامی فایل‌هایی را که در VSC^۳ ذخیره است با استفاده از VSS^۴ حذف کنند [8]. این ویژگی یکی از ویژگی‌هایی است که می‌توان گفت مختص باج‌افزارها است. به این معنی که هیچ برنامه یا سرویس دیگری در تلاش برای حذف این حجم از اطلاعات از VSC نمی‌کند. به‌عنوان مثال، باج‌افزار Cerber از دستورهای زیر برای حذف همه فایل‌ها استفاده می‌کند:

```
C:\Windows\system32\vssadmin.exe"delete shadows /all /quiet
```

دستور بالا تمامی فایل‌های ذخیره‌شده در VSC را حذف می‌کند. در اثر اجرای این دستور فایل اجرایی vssadmin.exe اجرا خواهد شد.

فایل‌های اجرایی اضافه‌شده: بسیاری از باج‌افزارها به‌محض اجراشدن، یک فایل اجرایی دیگر که می‌توان گفت تمام کارهای مخرب را آن فایل انجام می‌دهد در مسیرهایی مانند: Temp\، Downloads\، یا Appdata% قرار می‌دهد. به‌عنوان مثال، باج‌افزار CTB Locker به‌محض اجراشدن یک فایل اجرایی در مسیر c:\Users\alpha\AppData\Local\Temp می‌سازد؛ سپس با اجرای فایل جدید اضافه‌شده تمام کارهای رمزنگاری توسط آن انجام می‌شود.

دسترسی به Recent Files: همان‌طور که درقبل هم اشاره شد، استراتژی حملات در باج‌افزارها می‌تواند متفاوت باشد. بدین معنا که برخی از باج‌افزارها سعی دارند تا فایل‌ها را طبق شرایط مختلفی موردحمله قرار دهند. حال دراین‌بین باج‌افزارهایی هستند که فایل‌های کاربر را بر طبق آخرین دسترسی، رمزنگاری می‌کنند. مانند باج‌افزار Cerber که فایل‌های کاربر را بر طبق آخرین دسترسی‌ها رمزنگاری می‌کنند.

تغییر حجم فایل‌ها: رمزگذاری بر روی فایل‌ها موجب می‌شود تا حجم آن‌ها تغییر کند. این ویژگی هم می‌تواند یک ویژگی دیگر در شناسایی باج‌افزارها باشد.

نحوه رمزگذاری فایل‌ها: باج‌افزارها به‌منظور رمزگذاری فایل‌های می‌توانند به دو صورت عمل کنند [19]:

آنتروپی شانون: آنتروپی، اطلاعاتی در مورد عدم قطعیت داده ارائه می‌دهد. به این معنی که مقدار تصادفی بودن یک مجموعه داده مشخص را نمایش می‌دهد. هرچقدر داده تصادفی‌تر باشد، درصورت محاسبه آنتروپی، عدد بزرگ‌تری را نشان خواهد داد [9]. برخی از انواع داده‌ها مانند داده‌های رمزگذاری‌شده و فشرده‌شده^۲ آنتروپی بالایی دارند؛ پس بنابراین، حمله باج‌افزار به فایل‌ها همواره باعث افزایش آنتروپی می‌شود؛ زیرا که در حملات باج‌افزار، این بدافزار، فایل قربانی را خوانده و محتوای رمزگذاری‌شده را می‌نویسد. همین امر باعث افزایش آنتروپی می‌شود. آنتروپی شانون را برای آرایه‌ای از بایت‌ها، در فرمول (۱) می‌توان مشاهده کرد.

$$e = \sum_{i=0}^n P_{B_i} \log_2 \frac{1}{P_{B_i}} \quad (1)$$

در این فرمول $P_{B_i} = \frac{F_i}{\text{totalbytes}}$ است که F_i تعداد نمونه‌های بایت را با مقدار i در آرایه نشان می‌دهد. این فرمول مقداری بین صفر تا هشت را به‌عنوان خروجی می‌دهد که مقدار هشت نشان می‌دهد که مقادیر بایت در آرایه دارای توزیع یکنواخت است. مقادیر آنتروپی فایل‌های رمزگذاری‌شده بیشتر میل به مقدار هشت را دارند [9]. به همین علت، وقوع هر بایت در فایل رمزگذاری‌شده بایستی یک احتمال یکنواخت داشته باشد.

تعداد فایل‌های اضافه‌شده: شاید یکی از مهم‌ترین ویژگی‌هایی که باج‌افزارها را از دیگر بدافزارها متمایز می‌کند، این است که باج‌افزار بعد از انجام مراحل رمزگذاری فایل‌های کاربر، به‌صورت به‌طورکامل واضح قربانی را در جریان حمله قرار می‌دهد. یکی از روش‌های انجام این کار اضافه‌کردن فایل‌های مختلف جهت آگاه‌سازی کاربر در مسیرهای مختلفی است که باج‌افزار برای انجام رمزگذاری به آن‌ها وارد می‌شود. برای مثال، باج‌افزار satana بعد از ورود به یک مسیر و انجام کارهای رمزگذاری خود فایل متنی را با نام

³ Volume Shadow Copy

⁴ Volume Shadow Copy Service

¹ File backup

² Compressed

وجود دارد: هرچقدر تعداد درختان زیاد باشد، نتیجه دقیق‌تر خواهد بود. مزایای دسته‌بندی جنگل‌های تصادفی:

- یکی از مشکلات اساسی در فرآیند آموزش مسأله بیش‌برازش^۵ است. اما در جنگل‌ها تصادفی در صورت کافی بودن تعداد درختان در جنگل، مشکل بیش‌برازش به‌وجود نمی‌آید.

- مقادیری را که در مجموعه داده موجود نیست، می‌تواند مدیریت کند.

- بر روی پایگاه داده‌های بسیار بزرگ به‌صورت مؤثر عمل می‌کند.

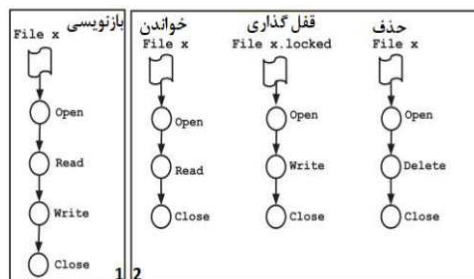
۳-۶- فرآیند آزمون

همان‌طور که در شکل (۱) مشاهده می‌شود، فرآیند آزمون و فرآیند آموزش به‌طور تقریبی عملیات مشابهی را طی می‌کنند. در هر دو فرآیندهای آموزش و آزمون، ابتدا می‌بایست نمونه فایل‌های اجرایی (شامل بدافزار، سالم و باج‌افزار) متعلق به مجموعه آموزش و آزمون، باید بر روی جعبه‌شنی اجرا شوند. در هنگام اجرای این نمونه‌ها فعالیت‌های مرتبط با فایل هر نمونه به‌کمک مینی‌فیلتر ثبت خواهد شد تا گزارشی از فایل‌های ارتباطی ثبت گردد. در گام بعد، ویژگی‌های متمایزکننده باج‌افزارها، از روی گزارش‌ها، استخراج می‌شود. در ادامه، ویژگی‌های استخراج‌شده به دسته‌بندی جنگل تصادفی آموزش‌دیده در مرحله آموزش داده خواهد شد تا که خروجی این عمل برچسب خانواده آن نمونه را اعلام کند.

۴- نتایج و ارزیابی

برای ارزیابی این سامانه از نمونه باج‌افزارهای موجود در [17] استفاده شده است. مشخصات نمونه‌ها در جدول (۳) نمایش داده شده است. به‌منظور مقایسه رفتار باج‌افزارها با برنامه‌های سالم یا بی‌آزار، شصت‌وشش برنامه بی‌آزار هم به‌منظور رصد فعالیت‌های فایل به اجرا درآمدند. همچنین، به تعداد صد بدافزار از خانواده‌های Zeus و Melissa, Bagle نظر گرفته شده که از هر خانواده به‌ترتیب ۳۶، ۲۷ و ۳۷ نمونه هستند. جهت مقایسه باکارهای گذشته، کارهای [15] و [12] را اجرا و نمونه‌های نشان داده‌شده در جدول (۳) را اجرا کردیم.

۱- بازنویسی روی فایل اصلی ۲- ایجاد یک فایل جدید. همان‌طور که در شکل (۲) و در حالت ۱ مشاهده می‌شود باج‌افزار فایل‌های کاربر را با نسخه رمزگذاری‌شده از فایل اصلی بازنویسی می‌کند. از جمله این نوع باج‌افزارها Satana و CTB هستند.



(شکل-۲): نحوه رمزگذاری فایل‌های به‌وسیله باج‌افزارها (۱) بازنویسی فایل (۲) ایجاد یک فایل جدید [19]

اما در حالت دو باج‌افزار ابتدا یک فایل جدید می‌سازد، داده‌های فایل قربانی را خوانده و نسخه رمزگذاری‌شده فایل قربانی را تولید کرده و نسخه رمزگذاری‌شده را در فایل اصلی نوشته و در نهایت فایل اصلی کاربر را حذف می‌کند. مانند باج‌افزار Locky که به همین صورت عمل می‌کند.

۴-۳- ایجاد مجموعه داده

بدیهی است که در فرآیند آموزش بایستی مجموعه داده‌ای برای آموزش حاضر شود. در این قسمت از تمامی ویژگی‌های استخراج‌شده از اجرای تمامی فایل‌های اجرایی، ماتریسی ایجاد می‌شود.

۵-۳- یادگیری دسته‌بند

در این مرحله با استفاده از مجموعه داده ایجاد شده در مرحله پیشین، دسته‌بندی صورت می‌پذیرد. دسته‌بند در نظر گرفته شده در این سامانه برای یادگیری، دسته‌بند جنگل‌های تصادفی^۱ است. جنگل‌های تصادفی یک دسته‌بند ترکیبی^۲ نظارت‌شده^۳ است که شامل درختان تصمیم متعدد است. خروجی این دسته‌بند با محاسبه مد^۴ خروجی‌های به‌دست‌آمده از کل درختان تصمیم تولید می‌شود. یک ارتباط مستقیمی بین تعداد درختان جنگل و نتیجه آن

¹ Random forests classifier

² Ensemble

³ Supervised

⁴ Mode

⁵ Overfitting

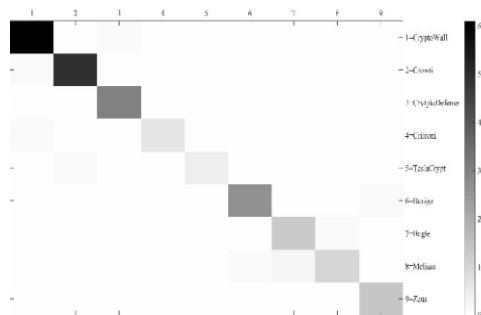
(جدول-۴): تعداد فایل‌های عسل

| تعداد | دسته فایل‌ها |
|--|--------------|
| ۲۱ | مستندات |
| ۹ | لایسنس |
| ۴ | آرشیو |
| ۱۵ | مدیا |
| مجموع تعداد فایل‌های عسل ۴۹ عدد می‌باشد. | |

(جدول-۵): میزان مقایسه دقت روش پیشنهادی با دقت روش‌های [12] و [15]. نتایج به صورت درصد بیان شده است.

| | روش پیشنهادی | [12] | [15] |
|-----------|--------------|-------|-------|
| Accuracy | ۹۸/۹۷ | ۹۷/۳۲ | ۹۵/۸۴ |
| F1 | ۹۳/۰۵ | ۸۰/۳۱ | ۷۲/۶۲ |
| Precision | ۷۰/۴۳ | ۷۹/۵۶ | ۹۱/۰۲ |
| Recall | ۹۵/۶۸ | ۸۳/۶۶ | ۷۷/۲۱ |

پس می‌توان نتیجه گرفت که این سامانه می‌تواند نمونه‌های مختلفی را در خانواده‌های خود دسته‌بندی کند. ماتریس درهم‌ریختگی^۲ برای هر سه روش در شکل‌های (۳ و ۴ و ۵) نشان داده شده است. همان‌طور که در شکل (۳) نشان داده شده است، روش پیشنهادی ما دارای ماتریس با حالت خطی بیشتری نسبت به ماتریس‌های درهم‌ریختگی روش‌های دیگر است که، اهمیت ویژگی‌های کشف‌شده با استفاده از فایل‌های دامی مؤثر مطرح‌شده در جدول (۴) را نشان می‌دهد؛ همچنین در جدول (۵) میزان دقت‌های به‌دست‌آمده برای بدافزارهای مطرح‌شده در جدول (۳)، تأکیدی بر این موضوع است که روش مطرح‌شده توسط ما قادر است (طبق جدول ۶) خانواده‌های بدافزارها را همراه با خانواده بدافزارها و فایل‌های سالم از هم متمایز کند. این به‌نوبه خود کاری نو و بارز است که در این مقاله مطرح شده است.



(شکل-۳): ماتریس درهم‌ریختگی روش پیشنهادی

² Confusion matrix

(جدول-۳): مشخصات باج‌افزارها

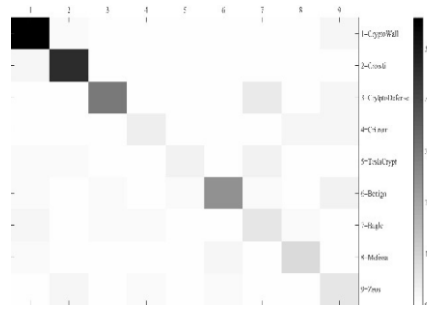
| آزمون | آموزش | تعداد | خانواده | | |
|------------|-------|-------|---------------|---------|----|
| Ransomware | ۶۳ | ۹۴ | CryptoWall | | |
| | ۵۰ | ۷۵ | Crowti | | |
| | ۳۱ | ۴۶ | CryptoDefense | | |
| | ۶ | ۸ | Critroni | | |
| | ۴ | ۶ | TeslaCrypt | | |
| Benign | | | ۳۹ | ۴۶ | ۶۶ |
| Malware | ۱۵ | ۲۱ | ۳۶ | Bagle | |
| | ۱۱ | ۱۶ | ۲۷ | Melissa | |
| | ۱۵ | ۲۲ | ۳۷ | Zeus | |
| | مجموع | | | ۵۴۹ | |

برای انجام این آزمایش از سیستم‌عامل ویندوز ۱۰ به‌عنوان سیستم‌عامل جعبه‌شنی استفاده شده است. از بین نمونه‌ها هفتاد درصد را برای آموزش و سی درصد باقی را برای آزمون در نظر گرفتیم. تعداد انواع مختلف فایل‌های عسل استفاده‌شده برای این سامانه هم در جدول (۴) آمده است. این تعداد فایل همان‌طور که در قبل هم اشاره شد در دو مسیر قرار می‌گیرند. هرکدام از باج‌افزارها به‌مدت بیست دقیقه بر روی جعبه‌شنی اجرا می‌شود. در این مدت تمامی ویژگی‌های اشاره‌شده استخراج می‌شوند. برای ویژگی‌های آنتروپی از اختلاف آنتروپی فایل‌های عسل استفاده شده است. به این معنی که ابتدا آنتروپی فایل‌ها قبل از اجرای باج‌افزار محاسبه، سپس اقدام به اجرای باج‌افزار و بعد از مدت بیست دقیقه دوباره آنتروپی فایل‌های عسل محاسبه می‌شود؛ در نهایت اختلاف این دو آنتروپی به‌عنوان ویژگی در نظر گرفته می‌شود. برای ویژگی تعداد فایل‌های اضافه‌شده هم از اختلاف تعداد فایل‌های قبل و بعد از اجرای باج‌افزار استفاده شده است. دیگر ویژگی‌های مطرح‌شده هم با یک مقدار دودویی مقداردهی می‌شوند (صفر یا یک). پس از جمع‌آوری یک مجموعه داده از تمامی باج‌افزارها اقدام به ایجاد یک ماتریس جهت آموزش دسته‌بند جنگل‌های تصادفی شده است. برای آموزش دسته‌بند از ابزار وکا^۱ استفاده شده است.

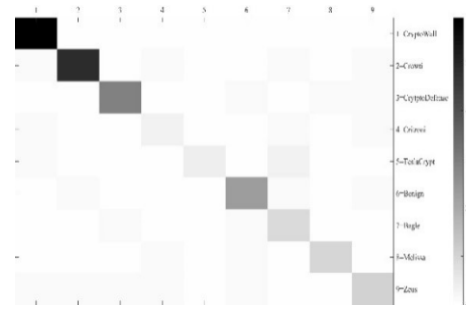
خروجی وکا برای مجموعه داده جمع‌آوری‌شده برای این سامانه در جدول (۵) ارائه شده است. این در حالی است که دقت تشخیص در [17] برابر با ۹۷/۷ درصد بوده است.

¹ Weka:

نرم‌افزاری که شامل مجموعه‌ای از الگوریتم‌های یادگیری ماشینی و داده‌کاوی است. این نرم‌افزار توسط دانشگاه ویکاتو توسعه داده‌شده و برای تحلیل داده‌های عظیم کاربرد دارد.



(شکل-۵): ماتریس درهم‌ریختگی روش [12]



(شکل-۴): ماتریس درهم‌ریختگی روش [15]

(جدول-۶): میزان مقایسه دقت روش پیشنهادی با دقت روش‌های [12] و [15] بر اساس خانواده‌های موجود در جدول (۳) نتیجه به صورت درصد بیان شده است.

| خانواده | روش پیشنهادی | | | | [15] | | | | [12] | | | |
|---------------|--------------|---------|-----------|---------|----------|--------|-----------|-------|----------|--------|-----------|-------|
| | Accuracy | Recall | Precision | F1 | Accuracy | Recall | Precision | F1 | Accuracy | Recall | Precision | F1 |
| CryptoWall | ۹۸/۶۴ | ۹۶/۸۲۵۴ | ۹۸/۳۸ | ۹۷۶ | ۹۵/۴۹ | ۸۸/۸۸ | ۹۴/۹۱ | ۹۱/۸۰ | ۹۸/۱۹ | ۹۳/۶۵ | ۱۰۰ | ۹۶/۷۲ |
| Crowti | ۹۹/۰۹ | ۹۸/۰۰ | ۹۸/۰۰ | ۹۸ | ۹۷/۲۹ | ۹۲/۰۰ | ۹۵/۸۳ | ۹۳/۸۷ | ۹۷/۲۹ | ۹۶/۰۰ | ۹۲/۳۰ | ۹۴/۱۱ |
| CryptoDefense | ۹۹/۵۴ | ۹۶/۷۷ | ۱۰۰ | ۹۸۳۶۰۷ | ۹۵/۹۴ | ۹۳/۵۴ | ۸۰/۵۵ | ۸۶/۵۶ | ۹۷/۷۴ | ۹۳/۵۴ | ۹۰/۶۲ | ۹۲/۰۶ |
| Critroni | ۹۹/۵۴ | ۱۰۰ | ۸۵/۷۱ | ۹۲۳۰۷۷ | ۹۷/۲۹ | ۶۶/۶۶ | ۵۰/۰۰ | ۵۷/۱۴ | ۹۷/۲۹ | ۵۰/۰۰ | ۵۰/۰۰ | ۵۰/۰۰ |
| TeslaCrypt | ۹۹/۰۳ | ۱۰۰ | ۸۰/۰۰ | ۸۸۸۸۸۹ | ۹۴/۲۳ | ۷۵/۰۰ | ۳۷/۵۰ | ۵۰/۰۰ | ۹۶/۱۵ | ۱۰۰ | ۵۰/۰۰ | ۶۶/۶۶ |
| Benign | ۹۹/۰۹ | ۹۶/۲۹ | ۹۶۲۹۶۳ | ۹۶۲۹۶۳ | ۹۵/۴۹ | ۸۸/۸۸ | ۷۷/۴۱ | ۸۲/۷۵ | ۹۶/۸۴ | ۸۵/۱۸ | ۸۸/۴۶ | ۸۶/۷۹ |
| Bagle | ۹۸/۶۴ | ۸۶/۶۶ | ۹۲/۸۵ | ۸۹۶۵۵۲ | ۹۳/۶۹ | ۴۰/۰۰ | ۵۴/۵۴ | ۴۶/۱۵ | ۹۶/۳۹ | ۶۰/۰۰ | ۸۱/۸۱ | ۶۹/۲۳ |
| Melissa | ۹۸/۱۹ | ۹۰/۹۰ | ۷۶/۹۲ | ۸۳۳۳۳۳ | ۹۷/۲۹ | ۷۲/۷۲ | ۷۲/۷۲ | ۷۲/۷۲ | ۹۸/۶۴ | ۹۰/۹۰ | ۸۳/۳۳ | ۸۶/۹۵ |
| Zeus | ۹۹/۵۴ | ۹۳/۳۳ | ۱۰۰ | ۹۶/۵۵۱۷ | ۹۴/۱۴ | ۴۰/۰۰ | ۶۰/۰۰ | ۴۸/۰۰ | ۹۵/۹۴ | ۷۳/۲۳ | ۶۸/۷۵ | ۷۰/۹۶ |
| macro avg | ۹۸/۹۷ | ۹۵/۶۸ | ۹۱/۰۲ | ۹۳/۰۵ | ۹۵/۸۴ | ۷۷/۲۱ | ۷۰/۴۳ | ۷۲/۶۲ | ۹۷/۳۲ | ۸۳/۶۶ | ۷۹/۵۶ | ۸۰/۳۱ |
| weighted avg | | ۹۵/۹۴ | ۹۴/۵۸ | ۹۶/۰۲ | | ۸۱/۹۸ | ۷۸/۴۱ | ۸۱/۷۶ | | ۸۸/۲۸ | ۸۵/۱۵ | ۸۸/۳۹ |
| micro avg | | | | ۹۵/۹۴ | | | | ۸۱/۹۸ | | | | ۸۸/۲۸ |

باج‌افزار و در نهایت نحوه رمزگذاری فایل‌ها استفاده شده است. سامانه پیشنهادی همان‌طور که نشان داده شد توانست با دقت بالای ۹۸/۹٪ خانواده باج‌افزارهای اجرا شده را به‌درستی از بدافزارهای دیگر و از فایل‌های سالم شناسایی کند که در مقایسه با روش پیشین از دقت بیشتری برخوردار است.

۶- مراجع

- [1] M. F. Ab Razak, N. B. Anuar, R. Salleh and A. Firdaus, "The rise of "malware": bibliometric analysis of malware study," *Journal of Network and Computer Applications*, vol. 75, pp. 58-76, 2016.
- [2] M. Sikorski and A. Honig, *Practical malware analysis: the hands-on guide to dissecting malicious software*, 2012.
- [3] S. Song, B. Kim and S. Lee, "The effective ransomware prevention technique using process monitoring on android platform," *Mobile Information Systems*, vol. 2016, 2016.
- [4] B. A. S. Al-rimy, M. A. Maarof and S. Z. M.

۵- نتیجه‌گیری

امروزه، سخت‌افزارها و نرم‌افزارهای رایانه‌ای به‌شدت در حال رشد هستند؛ همچنین، نرم‌افزارهای بدخواه یک تهدید مهم در این حوزه به‌حساب می‌آیند. کاربران بدخواه برای رسیدن به هدف بدخواهانه خود، تعداد بدافزارهای هم‌ریخت را افزایش می‌دهند تا از شناسایی توسط نرم‌افزارهای امنیتی رهایی یابند. در همین راستا، روزانه هزاران بدافزار با روش‌های تحلیل متفاوت، شناسایی می‌شوند که از این تعداد حدود ۹۰٪ آن‌ها بدافزارهای هم‌ریخت هستند. به گفته پژوهش‌گران بیش‌تر بدافزارها، جزء تعداد محدودی از خانواده‌های بدافزار هستند و یکی از مسائل روز تشخیص خانواده بدافزار است. در سامانه پیشنهادی جهت شناسایی خانواده باج‌افزارها از ویژگی‌های استخراج‌شده از فعالیت‌های سیستم فایل همچون آنتروپی فایل‌ها، فایل‌های اضافه‌شده در مسیر فایل‌های عسل، دسترسی به VSSAdmin جهت پاک‌سازی فایل‌های پشتیبان، فایل‌ها اجرایی اضافه‌شده، رمزگذاری آخرین فایل‌های دست‌کاری‌شده توسط کاربر، تغییرات حجمی ایجادشده در فایل‌های عسل در اثر اجرای

- [19] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson and E. Kirida, "{UNVEIL}: A large-scale, automated approach to detecting ransomware," in *25th USENIX Security Symposium*, 2016.
- [20] N. Andronio, S. Zanero and F. Maggi, "Heldroid: Dissecting and detecting mobile ransomware," in *International Symposium on Recent Advances in Intrusion Detection*, 2015.
- [21] M. Alaeiyan, S. Parsa and M. Conti, "Analysis and classification of context-based malware behavior," *Computer Communications*, vol. 136, pp. 76-90, 2019.
- [22] B. M. Bowen, S. Hershkop, A. D. Keromytis and S. J. Stolfo, "Baiting inside attackers using decoy documents," in *International Conference on Security and Privacy in Communication Systems*, 2009.
- [23] P. M. Comparetti, G. Salvaneschi, E. Kirida, C. Kolbitsch, C. Kruegel and S. Zanero, "Identifying dormant functionality in malware programs," in *IEEE Symposium on Security and Privacy*, 2010.



سید عطاالله سید جعفری دارای کارشناسی ارشد مهندسی کامپیوتر گرایش نرم‌افزار از دانشگاه علم و صنعت ایران واحد نور است.



محمدهادی علایان دارای دکترای مهندسی کامپیوتر گرایش نرم‌افزار از دانشگاه علم و صنعت ایران است. وی مدارک کارشناسی و کارشناسی ارشد خود را نیز از دانشگاه علم و صنعت ایران دریافت کردند. همچنین، یک دوره فرصت مطالعاتی

نیز در دانشگاه پادوا ایتالیا حضور داشتند. وی دارنده دهها مقاله علمی از مجلات معتبر است و عضو برگزارکننده کنفرانس‌هایی همچون i4c و iscisc2020. امنیت نرم افزار و حفاظت از کد و آزمون و تحلیل قابلیت اتکاپذیری سیستم از حوزه‌های مورد علاقه ایشان است.



سعید پارسا، استاد دانشکده مهندسی کامپیوتر دانشگاه علم و صنعت ایران است. ایشان دکترای کارشناسی ارشد خود را از دانشگاه سالفورد در کشور انگلستان دریافت کردند. همچنین مقطع کارشناسی

خود را در دانشگاه صنعتی شریف گذراندند. علایق پژوهشی ایشان شامل مهندسی معکوس، معماری نرم‌افزار، آزمون نرم‌افزار، کامپایلرها و سوپر کامپایلرها است.

- Shaid, "A 0-day aware crypto-ransomware early behavioral detection framework," *International Conference of Reliable Information and Communication Technology*, pp. 758-766, 2017.
- [5] I. Security and T. Report, "Ransomware 2017," 2017.
- [6] D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen and E. C. Lupu, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," *arXiv preprint arXiv:1609.03020*, 2016.
- [7] keepnetlabs, "Top 11 Ransomware Attacks in 2020-2021," keepnetlabs, 2020. [Online]. Available: <https://www.keepnetlabs.com/top-11-ransomware-attacks-in-2020-2021/>. [Accessed 20 10 2020].
- [8] A. Liska and T. Gallo, Ransomware: Defending against digital extortion, O'Reilly Media, Inc., 2016.
- [9] N. Scaife, H. Carter, P. Traynor and K. R. Butler, "Cryptolock (and drop it): stopping ransomware attacks on user data," in *36th International Conference on Distributed Computing Systems (ICDCS)*, 2016.
- [10] M. Lindorfer, C. Kolbitsch and P. M. Comparetti, "Detecting environment-sensitive malware," in *International Workshop on Recent Advances in Intrusion Detection*, 338-357.
- [11] N. Idika and A. P. Mathur, "A survey of malware detection techniques," *Purdue University*, vol. 48, pp. 2-10, 2007.
- [12] S. I. Bae, G. B. Lee and E. G. Im, "Ransomware detection using machine learning algorithms," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 18, p. e5422, 2020.
- [13] O. Delgado-Mohatar, J. M. Sierra-Camara and E. Anguiano, "Blockchain-based semi-autonomous ransomware," *Future Generation Computer Systems*, 2020.
- [14] G. Ramesh and A. Menen, "Automated dynamic approach for detecting ransomware using finite-state machine," *Decision Support Systems*, vol. 138, p. 113400, 2020.
- [15] F. Tang, B. Ma, J. Li, F. Zhang, J. Su and J. Ma, "RansomSpector: An introspection-based approach to detect crypto ransomware," *Computers & Security*, vol. 97, p. 101997, 2020.
- [16] J. Yuill, M. Zappe, D. Denning and F. Feer, "Honeyfiles: deceptive files for intrusion detection," in *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop*, 2004.
- [17] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero and F. Maggi, "ShieldFS: a self-healing, ransomware-aware filesystem," in *32nd Annual Conference on Computer Security Applications*, 2016.
- [18] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirida, "Cutting the gordian knot: A look under the hood of ransomware attacks," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2015.