رویکردی خودکار جهت تحلیل و دسته‌بندی خانوادهٔ باج‌افزارهای رمزگذار

سید عطاالله سید جعفری[1]، محمدهادی علائیان[2]* و سعید پارسا[3]

دانشگاه علم و صنعت ایران، تهران، ایران
ataa1370@gmail.com[1]
hadi.alaeiyan@yahoo.com[2]
parsa@iust.ac.ir[3]

چکیده

بدافزارها یکی از تهدیدات همیشگی برای دستگاه‌های رایانه‌ای به‌شمار می‌آیند. بدافزارها با ورود به دستگاه‌های رایانه‌ای بسته به اهدافشان، سعی دارند در روند عادی دستگاه‌های رایانه‌ای اخلال ایجاد کنند. دراین‌بین، بدافزارهایی به نام باج‌افزار وجود دارند که پس از ورود به دستگاه‌های رایانه‌ای و محدودکردن دسترسی قربانی به دستگاه رایانه‌ای خود با رمزگذاری فایل‌های قربانی یا قفل‌گذاری دستگاه درصدد اخاذی از قربانی برمی‌آید. این نوع بدافزارها، یک تفاوت بسیار آشکار با دیگر بدافزارها دارد، باج‌افزارها باصراحت قربانی را از وجود خود بر روی دستگاه رایانه‌ای باخبر می‌سازند. این بدافزارها، برخلاف آسیب‌های جدی‌ای که بر روی دستگاه‌های قربانی وارد می‌سازند، می‌توانند با ویژگی‌های منحصربه‌فردی 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 بدافزار حاصل خواهد شد. این گزارش‌ها ما را در کشف ویژگی‌های تمایزکنندهٔ 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: بدافزار، باج‌افزار، باج‌افزارهای رمزگذار، باج‌افزارهای قفل‌گذار، دسته‌بندی خانواده باج‌افزارها.

۱- مقدمه

امروزه نمی‌توان تأثیر نرم‌افزارها را در زندگی روزمرهٔمان انکار کرد. نرم‌افزارها با کارایی و دقت بالای خود از ملزومات زندگی امروزی ما به‌حساب می‌آیند و استفاده از آن‌ها در محیط‌های محاسباتی نه‌فقط یک امتیاز، بلکه به یک نیاز ضروری تبدیل شده است؛ اما در کنار این نرم‌افزارهای سودمند نرم‌افزارهایی هم همواره با عنوان بدافزار 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. بدافزارها انواع مختلفی دارند که باج‌افزارها یکی از آن‌ها به‌حساب می‌آید. این دسته از بدافزارها که هدف آن‌ها بیشتر جنبه مالی دارند، با حمله به فایل‌های شخصی بر روی دستگاه قربانی آن‌ها را غیرقابل‌دسترس می‌کند [3] که در قبال دریافت مبلغی، این فایل‌ها را دوباره به حالت قبل برمی‌گرداند. به‌عبارت‌دیگر باج‌افزار را می‌توان بدافزاری برای اخاذی از کاربر به‌صورت 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 به‌ترتیب ۳۰ و ۲۹ درصد از اهداف این نوع از بدافزارها را شامل می‌شدند. دلیل اصلی این افزایش مربوط به دو باج‌افزار WannsCry 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 به‌دلیل قدرت در گسترش به‌عنوان خطرناک‌ترین باج‌افزارهای این

*نویسندهٔ مسؤول

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

سال‌ها در نظر گرفته شده‌اند. همچنین، بیماری کووید۱۹ 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 مورداستفاده توسط باج‌افزارها، به‌اندازه کافی محافظت نمی‌شود؛ همچنین به‌دلیل تعاملات بالای بین کارمندان، دریافت فایل‌های مخرب حاوی باج‌افزارها افزایش یافته است. همه این موارد موجب شده تا پژوهش پیش رو انجام شود [7].

به‌طورکلی، باج‌افزارها به دودستهٔ 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[1] ۴- تخریب ۵- اخاذی [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[2]، 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 به‌محض اینکه بدافزار وارد دستگاه شد، کد بدخواه خود را اجرا کرده و سپس دستگاه میزبان را مورد تحلیل قرار می‌دهد تا واقعی‌بودن و یا محیط تحلیل (جعبه‌شنی[3]) بودن سامانه را شناسایی کند؛ سپس، باج‌افزار با به‌کارگیری روش‌هایی مانند استفاده از نشانی MAC[4] سعی می‌کند خود را منحصربه‌فرد کنند تا طراح باج‌افزار اطلاع داشته باشد که کدام دستگاه آلوده‌شده است. بعد، باج‌افزار چندین اسکریپت برای اطمینان از غیرفعال‌بودن دستگاه‌های حفاظتی بر روی دستگاه قربانی اجرا می‌کند. ازجمله این فن‌ها را می‌توان به موارد زیر اشاره کرد:

ازکارانداختن ویژگی رونوشت سایه[5] بر روی فایل‌ها و پارتیشن‌ها، از کار انداختن ویژگی‌های بازیابی و درنهایت غیرفعال‌سازی نرم‌افزارهای ضد بدافزاری و گزارش‌گیری بر روی دستگاه.

در حملات باج‌افزاری، به‌محض 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 ازجمله 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 ازجمله انواع فایل‌های بسیار محبوب بین باج‌افزارها می‌توان به مستندات آفیس مایکروسافت، JPG، GIF و هر نوع فایل دیگری اشاره کرد. بسیاری از گونه‌های باج‌افزارها نه‌تنها فایل‌ها، بلکه اسامی فایل‌ها را هم رمزنگاری می‌کنند تا قربانی را از پی‌بردن به این که کدام فایل‌ها رمزگذاری شده‌اند، ناتوان سازد. رمزگذاری فایل‌ها به سه صورت متقارن، نامتقارن و یا ترکیبی از این دو انجام می‌پذیرد؛ درنهایت در مرحله اخاذی آگاه‌سازی کاربر از نوع حمله انجام‌شده بر روی دستگاه خود توسط باج‌افزار صورت می‌گیرد. بعدازآن‌که 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 دستهٔ 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].

[1] C2(Command & Control)
[2] E-mail
[3] Sandbox
[4] media access control address

[5] Shadow Copy:
فنّاوری که در سیستم‌عامل ویندوز تعبیه‌شده که امکان کپی‌برداری از فایل‌های پشتیبان را حتی در مواقع کار کردن با فایل‌ها را برای کاربر فراهم می‌سازد.

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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 سامانهٔ تحلیل باج‌افزار، جهت تحلیل و همچنین دسته‌بندی باج‌افزارها ارائه شده است. در رویکرد مطرح‌شده، با استخراج ویژگی‌هایی همچون آنتروپی شانون[1]، تعداد فایل‌های اضافه‌شده در مسیر فایل‌های عسل[2]، دسترسی به VSSAdmin، دسترسی به Recent files، تغییر حجم فایل‌ها و نحوه رمزگذاری فایل‌های عسل و سپس با ایجاد یک مجموعه‌داده از این ویژگی‌ها و درنهایت 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 باج افزارهای بر روی این نوع از فایل‌ها بررسی می‌شوند.

۲- مطالعات پیشین

در این قسمت، اطلاعات تکمیلی در مورد باج‌افزارها و نحوهٔ 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[3]، 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. بااین‌حال، این دیسک همچنین حاوی یک برنامه بدافزار بود که در ابتدا در رایانه‌ها خفته باقی‌مانده بود. پس از نود بار روشن‌شدن 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، TROJ.RANSOM.A، Archiveus، Krotten، 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؛ درحالی‌که، در ژوئن ۲۰۰۸، گونهٔ دیگری از این باج‌افزار با نام Gpcode.AK با استفاده از یک کلید RSA 1024 بیتی شناسایی شد. اعتقاد بر این بود که به‌اندازهٔ 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

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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 به‌وجود 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 به‌صورت پیام کوتاه برای شماره‌ای خاص ارسال شود. این پیام کوتاه باارزش حدود ۱۰ دلار آمریکا بود. این کلاه‌برداری از تعداد زیادی کاربر در سراسر روسیه و کشورهای همسایه اخاذی کردند. طبق گفته‌ها، این بدافزار بیش از شانزده میلیون دلار درآمد داشت.

همچنین در سال ۲۰۱۱، باج‌افزاری، اخطار فعال‌سازی محصول ویندوز را شبیه‌سازی کرد تا از قربانیان اخاذی کند. این باج‌افزار پیغامی به کاربران نمایش می‌داد که نصب ویندوز رایانه به‌دلیل 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 واردکردن 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 استفاده‌شده است. این اخطار 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. درحالی‌که، برخی نسخه‌ها فیلم‌هایی را از وب کم قربانی نشان می‌دهند تا باورپذیری کاربر را افزایش دهد.

نسل دیگر باج‌افزارهای غیر رمزگذاری باج‌افزارهای نَشت[1] است. هدف این باج‌افزار، یک حمله بدون رمزنگاری است. در این حمله، به‌جای قطع دسترسی قربانی به اطلاعات درون دستگاه خود، وی را تهدید به انتشار اطلاعات دزدیده‌شده می‌کند. در حمله نَشت، بدافزارها داده‌های حساس میزبان را به‌صورت متناوب برای یک مهاجم ارسال می‌کنند و مهاجم، قربانی را به انتشار اطلاعات تهدید می‌کند، مگر مبلغی به‌عنوان باج پرداخت شود.

در سال ۲۰۱۶، یک فشار جدید از باج‌افزار ظاهر شد که سرورهای JBoss را هدف قرارداد. 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 به‌طوری غیرقابل‌بازگشت، رمز و از کاربر رایانه قربانی درخواست باج از طریق بیت کوین برای بازگشایی رمز فایل‌ها می‌کند. این بدافزار به‌صورت غیرقابل‌باوری در سراسر جهان پخش‌شده که یکی از مهم‌ترین عامل گسترش WannaCry نفوذ به تعدادی از سامانه‌های مهم و مشهور، ازجمله بسیاری از مراکز ملی بهداشت کشور انگلیس است. کد برنامه این بدافزار مبهم‌سازی نشده و برای تجزیه‌وتحلیل تاحدودی 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 مسدودکردن پیام سرور از پیام مایکروسافت سوءاستفاده می‌کند. پس از سوءاستفاده از این آسیب‌پذیری، این باج‌افزار مسیر اصلی روشن‌شدن سیستم را به‌جای رمزگذاری بر روی فایل‌ها مسدود می‌کند. در نخستین اجرا، یک پیام برای انجام راه‌اندازی مجدد رایانه به کاربر می‌دهد، پس‌ازآن رایانه غیرقابل‌دسترس 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

[1] Doxware

[Downloaded from monadi.isc.org.ir on 2024-12-18]

[DOR: 20.1001.1.24763047.1398.8.2.6.4]

می‌کند. عمده تفاوت این دو باج‌افزار در نوع قفل‌کردن رایانه است. بدافزار Santa از Master Boot Record (MBR) برای قفل‌کردن رایانه استفاده می‌کند؛ درحالی‌که باج‌افزار Petya از Master File Table (MFT) برای قفل‌کردن رایانه استفاده می‌کند. MBR بخشی از لوح سخت است. این اطلاعات در مورد سیستم فایل‌هایی است که به‌وسیلهٔ پارتیشن‌های لوح سخت مختلف مورداستفاده 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 باقابلیت‌های 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. بااین‌وجود، 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 مظنون توزیع می‌شود. این بدافزارها سعی می‌کنند پیام مسدودکننده را قبل از اجرای هر برنامه دیگر نشان دهند.

روش‌های قفل‌گزاری مختلفی در تلفن‌های همراه مبتنی بر سیستم‌عامل iOS مانند بهره‌برداری از حساب‌های iCloud و استفاده از سامانهٔ Find My iPhone استفاده‌شده است. به‌عنوان نمونه، در نسخه iOS 10.3، در مرورگر سافاری با استفاده از پنجره‌های پاپ آپ JavaScript راه نفوذ برای قفل گزاری 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 پرداخت باج استفاده می‌کرد. این برنامه وانمود می‌کرد که یک سازمان حقوقی است و از قربانی می‌خواهد جریمه‌ای بین صد دلار تا دویست دلار بپردازد یا در غیر این صورت، با یک اتهام ساختگی روبه‌رو شود. این پرداخت‌ها به‌صورت کارت‌های هدیه iTunes بوده و با نمایش یک زمان‌سنج بر روی صفحه‌نمایش بر اضطراب کاربران می‌افزود. این بدافزار، به‌عنوان یک پخش‌کننده ویدیو وارد تلفن‌های همراه شده و زبان مورداستفاده در دستگاه را بررسی می‌کند. درصورتی‌که از زبان‌های روسی یا برخی از زبان‌های اروپای شرقی استفاده نشود، تلفن همراه قفل خواهد شد.

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 - مورداستفاده 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.

۲-۲- روش‌های شناسایی باج‌افزارها

در راستای شناسایی این باج‌افزارها، در [18] به مطالعه رفتارهای ترس‌افزارها[1] و باج‌افزارها پرداخته شده است و سازوکارهای رمزگذاری، تعاملات فایل بسیاری از باج‌افزارها در طی یک سال رصد شده است. روش‌های متعددی در این مقاله جهت مقابله با این نوع از بدافزارها پیشنهاد شده اما به ارزیابی روش‌های ارائه‌داده‌شده، نپرداخته است.

راه‌کار ارائه‌شده در [19] بر پایه رصد فراخوانی‌های فایل باج‌افزارها در محیط جعبه‌شنی است. در این روش معرفی‌شده، زمانی که باج‌افزار با فایل‌های شخصی کاربر در

[1] 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.

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

تعامل باشد، آن‌ها را رصد می‌کند و به‌صورت موازی هم همهٔ تغییرات دسکتاپ کاربر را زیر نظر می‌گیرد و سعی دارد تا رفتارهای شبه باج‌افزاری فایل 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 جریانی 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 ElderRan، 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 جمع‌آوری‌شده‌اند: ۱- زمانی که سامانه وضعیت عادی دارد و هیچ‌گونه باج‌افزاری بر روی آن موجود نیست ۲- زمانی که سامانه موردحمله باج‌افزار قرارگرفته باشد. راه‌حل پیشنهادی این روش، از سه راه‌انداز[1] ساخته شده است. یک راه‌انداز مسئول ترمیم فایل‌ها است؛ برای هر عملیات نوشتن و باز نام‌گذاری[2] از فایل مربوطه یک نسخه پشتیبان تولید می‌شود. راه‌انداز دوم هم مسئول تشخیص پایه رمزگذاری[3] در فایل‌ها است. درنهایت، راه‌انداز سوم به‌کمک الگوریتم جنگل‌های تصادفی[4] 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 موردبررسی 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 رمزنگاری‌شده 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؛ به‌عنوان‌مثال 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 ا 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-gramها، 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 قابل گریز 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 موردبررسی 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 با

[1] Driver
[2] Rename
[3] Cryptographic primitive
[4] Random forest classifier

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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 ایجادی 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 مورداستفاده قرار می‌دهد. این روش حتی قادر به دسته‌بندی خانواده باج‌افزارها هم نیست و فقط باج‌افزارها را از فایل‌های سالم متمایز می‌کند.

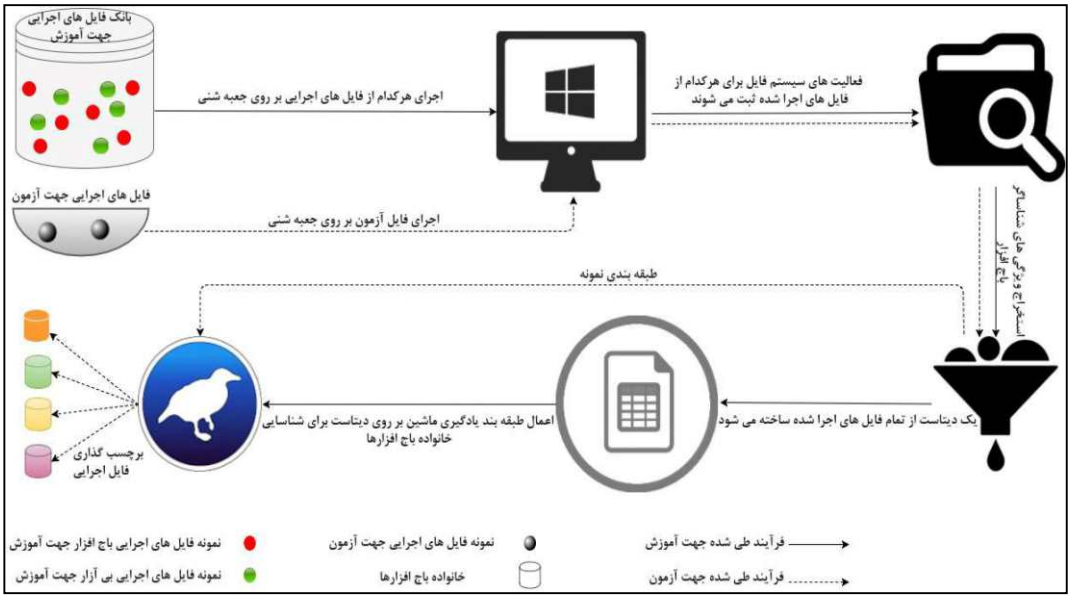
با وجود همه روش‌هایی که مطرح شده، روش ما قادر است همه رفتارهای باج‌افزارها را ازجمله فعالیت‌های شبکه، همه فراخوانی‌های سامانه‌ای و تعاملات مربوط به فایل‌ها را در جهت کشف رفتارهای مخرب باج‌افزارها به‌دست می‌آورد.

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.



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

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

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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[1] 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 مواجه‌شدن 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. ازجمله 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.
٤. 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 درنظرگرفته‌شده بر روی جعبه‌شنی را در این مقاله می‌توان به چهار دسته تقسیم کرد که در جدول (۱) بیان‌شده 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. ازآنجاکه باج‌افزارها از روش‌های مختلفی برای پیمایش تمام فایل‌های موجود بر روی دستگاه استفاده می‌کنند، بایستی این فایل‌ها چنان جانمایی شوند تا در مدت‌زمان محدودِ تحلیل یعنی بیست دقیقه اجرا برای هر باج‌افزار [19]، بتوان رفتار بدخواهانه باج‌افزارها را به‌دست آورد.

ازجمله 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

ازآنجاکه ما هیچ دسترسی به کد منبع[2] باج‌افزارها نداریم [23] پس اطلاعی از توانایی شناسایی فایل‌های عسل به‌وسیلهٔ 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:

[1] Honey Files

[2] Source code

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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. ازآنجاکه 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 درنتیجه 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، مسیرها[1] به‌صورت الفبایی پردازش و پیمایش می‌شوند [8]. به این خاطر، به‌طورمعمول C:\$Recycle.Bin در بیش‌تر موارد جز نخستین دایرکتوری‌هایی است که توسط باج‌افزار موردحمله قرار می‌گیرد. لذا، ما در این پروژه فایل‌های عسل را در دو فایل با نام‌های C:\$$0Decoyfiles\ 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 (Z تا A) 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. به‌عنوان‌مثال، فعالیت‌های فایل را می‌توان با قلاب‌اندازی[2] مجموعه‌ای از توابع API[3] مرتبط با فایل یا فراخوانی‌های سامانه‌ای با استفاده از جدول SSDT[4] رصد شوند؛ اما این راه‌کارها می‌توانند معایب زیر را به‌همراه داشته باشد [19]:

۱. باج‌افزارها می‌توانند از دستگاه‌های رمزنگاری[5] منحصربه‌فرد خود به‌جای APIهای استاندارد به‌منظور رمزگذاری فایل‌های کاربر استفاده کنند.

۲. قلاب اندازی SSDT بر روی دستگاه‌های ۶۴ بیتی به‌علت KPP[6] نمی‌تواند انجام شود.

۳. بسیاری از توابع SSDT غیر مستند هستند و در نسخه‌های مختلف ویندوز می‌توانند تغییر یابند.

لذا، روش‌های قلاب اندازی در این سامانه به‌منظور رصد فعالیت‌های ورودی/ خروجی فایل از راه‌انداز مینی‌فیلتر[7] استفاده شده است. این روش راه‌کاری استاندارد مبتنی بر هسته سیستم‌عامل برای رصد فعالیت‌های فایل در نسخه‌های مختلف ویندوز است [19]. در سیستم‌عامل ویندوز درخواست‌های ورودی/ خروجی به‌صورت بسته‌های درخواست ورودی/ خروجی (IRP) هستند.

۳-۳- استخراج ویژگی‌ها

در معماری پیشنهادی، در زمان ثبت فعالیت‌های فایل به‌وسیلهٔ 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

آنتروپی فایل‌ها، که میزان تصادفی‌بودن داده‌ها درون فایل‌های عسل را نشان می‌دهد، تعداد فایل‌های اضافه‌شده به مسیرهای فایل‌های عسل، دسترسی به VSSAdmin جهت

[1] Directory
[2] Hooking
[3] Application Programming Interface
[4] System Service Descriptor Table
[5] Cryptosystem
[6] Kernel path protection
[7] Minifilter driver

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

پاک‌سازی فایل‌های پشتیبان[1]، فایل‌های اجرایی اضافه‌شده به‌وسیلهٔ 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.

آنتروپی شانون: آنتروپی، اطلاعاتی در مورد عدم قطعیت داده ارائه می‌دهد. به این معنی که مقدار تصادفی‌بودن یک مجموعه‌داده 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[2] 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.

$$e = \sum_{i=0}^{n} P_{B_i} log_2 \frac{1}{P_{B_i}} \qquad (۱)$$

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 satana!.txt! در هر مسیر واردشده قرار می‌دهد که در این فایل متنی تمامی اطلاعات در رابطه با نحوه رمزگذاری فایل‌ها و چگونگی رمزگشایی فایل‌ها آمده است. (به‌الزام مطالب موجود در این فایل متنی هم نمی‌تواند درست باشد).

دسترسی به VSSAdmin: بسیاری از باج‌افزارهای جدید سعی می‌کنند تمامی فایل‌هایی را که در VSC[3] ذخیره است با استفاده از VSS[4] 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. به‌عنوان‌مثال، 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 تمام‌کارهای مخرب را آن فایل انجام می‌دهد در مسیرهایی مانند: \Downloads، \Temp یا مسیرهایی در %Appdata% قرار می‌دهد. به‌عنوان‌مثال، باج‌افزار CTB Locker به‌محض اجراشدن یک فایل اجرایی در مسیر c:\Users\alha\AppData\Local\Temp می‌سازد؛ سپس با اجرای فایل جدید اضافه‌شده تمام‌کارهای 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 رمزگذاری 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.

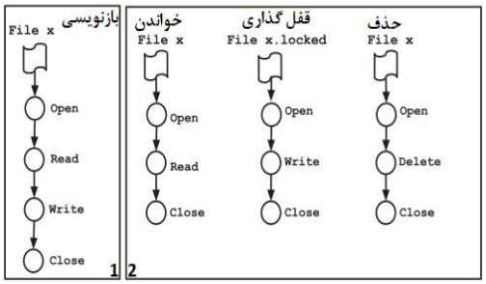
نحوه رمزگذاری فایل‌ها: باج‌افزارها به‌منظور رمزگذاری فایل‌های می‌توانند به دو صورت عمل کنند [19]:

[1] File backup
[2] Compressed
[3] Volume Shadow Copy
[4] Volume Shadow Copy Service

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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 نسخهٔ رمزگذاری‌شده از فایل اصلی بازنویسی می‌کند. ازجمله این نوع باج‌افزارها Satana و CTB هستند.



(شکل-۲): نحوه رمزگذاری فایل‌های به‌وسیلهٔ 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 درنهایت فایل اصلی کاربر را حذف می‌کند. مانند باج‌افزار Locky که به همین صورت عمل می‌کند.

۳-۴- ایجاد مجموعه‌داده

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.

۳-۵- یادگیری دسته‌بند

در این مرحله با استفاده از مجموعه‌دادهٔ ایجادشده در مرحله پیشین، دسته‌بندی صورت می‌پذیرد. دسته‌بند در نظر گرفته‌شده در این سامانه برای یادگیری، دسته‌بند جنگل‌های تصادفی[1] است. جنگل‌های تصادفی یک دسته‌بند ترکیبی[2] نظارت‌شده[3] است که شامل درختان تصمیم متعدد است. خروجی این دسته‌بند با محاسبه مد[4] خروجی‌های به‌دست‌آمده از کل درختان تصمیم تولید می‌شود. یک ارتباط مستقیمی بین تعداد درختان جنگل و نتیجه آن وجود دارد: هرچقدر تعداد درختان زیاد باشد، نتیجه دقیق‌تر خواهد بود. مزایای دسته‌بندِ جنگل‌های تصادفی:

۱. یکی از مشکلات اساسی در فرآیند آموزش مسأله بیش‌برازش[5] است. اما در جنگل‌ها تصادفی در صورت کافی‌بودن تعداد درختان در جنگل، مشکل بیش‌برازش به‌وجود نمی‌آید.
۲. مقادیری را که در مجموعه‌داده موجود نیست، می‌تواند مدیریت کند.
۳. 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 به‌طورتقریبی 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 متمایزکنندهٔ باج‌افزارها، از روی گزارش‌ها، استخراج می‌شود. در ادامه، ویژگی‌های استخراج‌شده به دسته‌بند 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 Bagle، Melissa و Zeus در 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.

[1] Random forests classifier
[2] Ensemble
[3] Supervised
[4] Mode
[5] Overfitting

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]

(جدول-۳): مشخصات باج‌افزارها

آزمون	آموزش	تعداد	خانواده	
۶۳	۹۴	۱۵۷	CryptoWall	Ransomware
۵۰	۷۵	۱۲۵	Crowti	
۳۱	۴۶	۷۷	CrytptoDefense	
۶	۸	۱۴	Critroni	
۴	۶	۱۰	TeslaCrypt	
۳۹	۴۶	۶۶	**Benign**	
۱۵	۲۱	۳۶	Bagle	Malware
۱۱	۱۶	۲۷	Melissa	
۱۵	۲۲	۳۷	Zeus	
		۵۴۹	مجموع	

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 درقبل 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 ویژگی 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؛ درنهایت 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 مجموعه‌داده از تمامی باج‌افزارها اقدام به ایجاد یک ماتریس جهت آموزش دسته‌بند جنگل‌های تصادفی شده است. برای آموزش دسته‌بند از ابزار وِکا[1] استفاده شده است.

خروجی وکا برای مجموعه‌دادهٔ 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 وایکاتو توسعه داده‌شده و برای تحلیل داده‌های عظیم کاربرد دارد.

(جدول-۴): تعداد فایل‌های عسل

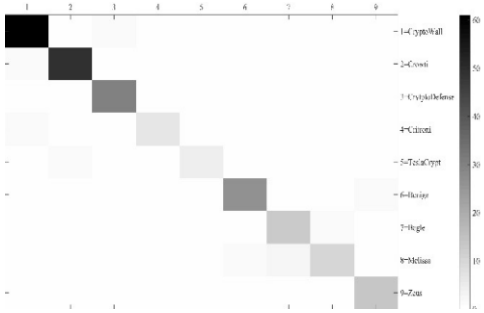
دسته فایل‌ها	تعداد
مستندات	۲۱
لایسنس	۹
آرشیو	۴
مدیا	۱۵
مجموع تعداد فایل‌های عسل ۴۹ عدد می‌باشد.	

(جدول-۵): میزان مقایسه دقت روش پیشنهادی با دقت روش‌های [12] و [15]. نتایج به‌صورت درصد بیان‌شده است.

	روش پیشنهادی	[12]	[15]
Accuracy	۹۸/۹۷	۹۷/۳۲	۹۵/۸۴
F1	۹۳/۰۵	۸۰/۳۱	۷۲/۶۲
Precission	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.

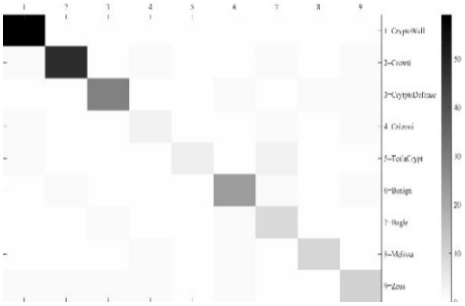
ماتریس درهم‌ریختگی[2] برای هر سه روش در شکل‌های (۳ و ۴ و ۵) نشان داده شده است. همان‌طور که در شکل (۳) نشان داده شده است، روش پیشنهادی ما دارای ماتریس با حالت خطی بیشتری نسبت به ماتریس‌های درهم‌ریختگی روش‌های دیگر است که، اهمیت ویژگی‌های کشف‌شده با استفاده از فایل‌های دامی مؤثر مطرح‌شده در جدول (۴) را 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 باج‌افزارها و فایل‌های سالم از هم متمایز کند. این به‌نوبهٔ خود کاری نو و باارزش است که در این مقاله مطرح شده است.



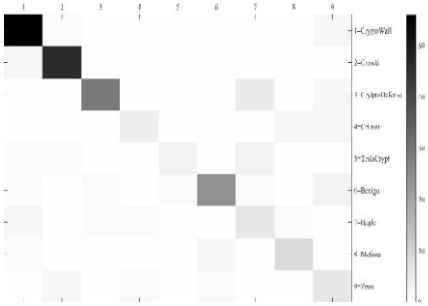
(شکل-۳): ماتریس درهم‌ریختگی روش پیشنهادی

[2] Confusion matrix

[Downloaded from monadi.isc.org.ir on 2024-12-18]
[DOR: 20.1001.1.24763047.1398.8.2.6.4]



(شکل-۴): ماتریس درهم‌ریختگی روش [15]



(شکل-۵): ماتریس درهم‌ریختگی روش [12]

(جدول-۶): میزان مقایسه دقت روش پیشنهادی با دقت روش‌های [12] و [15] بر اساس خانواده‌های موجود در جدول (۳) نتیجه به‌صورت 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
CrytptoDefense	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	۷۳/۳۳	۶۸۷۵	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

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 باج‌افزار و درنهایت نحوه رمزگذاری فایل‌ها استفاده شده است. سامانهٔ پیشنهادی همان‌طور که نشان داده شد توانست با دقت بالای ۹۸/۹٪ خانواده باج‌افزارهای اجراشده 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.

[Downloaded from monadi.isc.org.ir on 2024-12-18]

[DOR: 20.1001.1.24763047.1398.8.2.6.4]

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. Kirda, "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.

[19] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson and E. Kirda, "{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. Kirda, 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 کامپوتر گرایش نرم‌افزار از دانشگاه علم و صنعت ایران واحد نور است.

محمدهادی علائیان 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 دکترا و 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.

[Downloaded from monadi.isc.org.ir on 2024-12-18]

[DOR: 20.1001.1.24763047.1398.8.2.6.4]