جعبه شن و معرفی محصولات موجود

سوسن نادری
naderi@cert.um.ac.ir

شهاب نمازی‌خواه
namazikhah@cert.um.ac.ir

راضیه بزی
sogolbazi@gmail.com

آزمایشگاه تخصصی آپا در زمینه امنیت فن‌آوری اطلاعات و ارتباطات

http://cert.um.ac.ir

cert@um.ac.ir

ویرایش اول – بهمن‌ماه ۱۳۹۲

شماره سند: APA_FUM_W_MAL_0112

چکیده

امروزه میزان تهدیدهای امنیتی بسیار بالا است که آسیب‌های زیادی به سیستم‌های میزبان وارد می‌کنند. در واقع، شناسایی بدافزارهای معروف و شناخته شده کافی نیست، آن‌چه در شناخت بدافزارها مهم و حیاتی است، درک ساز و کارها، انگیزه‌ها، اهداف و چگونگی تاثیر آن بر سیستم می‌باشد. به همین دلیل باید بتوان رفتار این ابزارهای مخرب را به طور دقیق بررسی و تحلیل کرد که برای این منظور استفاده از جعبه شن یکی از بهترین روش‌ها است. هدف این مقاله معرفی جعبه شن، انواع و روش‌های استفاده از آن است.

واژه‌های کلیدی

تحلیل بدافزار، تهدید امنیتی، جعبه شن.

۱- مقدمه

بدافزارها نقش مهمی را در نفوذ به سیستم‌های کامپیوتری و حوادث امنیتی بر عهده دارند. هر نرم‌افزاری که باعث آسیب‌رسانی به کاربر، کامپیوتر و شبکه شود به عنوان بدافزار شناخته می‌شود که شامل ویروس‌ها، اسب‌های تروی، کرم‌ها، روت‌کیت‌ها و نرم‌افزارهای جاسوسی می‌باشد.

از آن‌جا که یک بدافزار خیلی سریع نصب و منتشر می‌شود، مبارزه با آن دشوار است. بیشتر محصولات امنیتی مثل *پویش‌گرهای ویروس*[1] برای تشخیص کد مخرب به دنبال امضا[2] و دنباله‌ای از بایت‌های خاص می‌گردند. کرم‌های چندریختی با تغییر دادن ظاهرشان مانع از تشخیص می‌شوند، در حالی که کرم‌های فلش که عمل شناسایی را به صورت مخفی و بدون آلوده کردن ماشین‌های آسیب‌پذیر انجام می‌دهند، سعی در گسترش برنامه‌های استراتژیک خود دارند که می‌توانند هزاران ماشین را در عرض چند ثانیه آلوده کنند.

با وجود این‌گونه تهدیدهای امنیتی که به صورت خودکار انجام می‌شوند، محققان امنیتی قادر به مبارزه با نرم‌افزارهای مخرب با استفاده از روش‌های دستی مانند دی‌اسمبل و مهندسی معکوس نیستند. بنابراین، ابزارهای تحلیل باید بدافزار را به صورت خودکار و صحیح تحلیل کنند. انجام این فرآیند به صورت خودکار به این معنی است که ابزار تحلیل باید گزارشی با جزئیات کامل از نمونه‌ی بدافزار به سرعت و بدون مداخله‌ی کاربر ایجاد کند. سپس، تحلیل‌گر می‌تواند از گزارشی که توسط ماشین قابل خواندن است، برای ایجاد پاسخ خودکار استفاده کند و امضای *سیستم‌های تشخیص نفوذ*[3] را به طور خودکار به‌روزرسانی کرده و از شبکه در مقابل بدافزارهای جدید محافظت کند. یک ابزار مؤثر تحلیل باید رفتار مرتبط با بدافزار را ثبت کند و هیچ یک از قابلیت‌های اجرایی آن نباید نادیده گرفته شود، زیرا تحلیل‌گران از این اطلاعات برای ارزیابی تهدید استفاده خواهند کرد. در نهایت، این ابزار باید به درستی بدافزار را تحلیل کرده و شروع به ثبت هر واقعه‌ای برای جلوگیری از نتایج اشتباه کند. از آن‌جا که نرم‌افزارهای مخرب کارهای متفاوتی انجام می‌دهند، ابزارهای متفاوتی به عنوان تحلیل‌گر بدافزار وجود دارد.

[1] Virus scanners
[2] Signature
[3] Intrusion Detection Systems (IDS)

تحلیل بدافزار به دو روش ایستا و پویا انجام می‌شود. در تحلیل ایستا بدافزار بدون این که اجرا شود، مورد بررسی قرار می‌گیرد؛ اما در تحلیل پویا بدافزار اجرا شده و سپس رفتار آن مورد تحلیل و بررسی قرار می‌گیرد. یکی از نرم‌افزارهایی که برای انجام تحلیل پویا وجود دارد جعبه شن است.

۲- تعریف جعبه شن

در بحث امنیت کامپیوتر، جعبه شن یک مکانیزم امنیتی برای جداسازی برنامه‌های در حال اجرا است. اغلب برای اجرای کدهایی که مورد آزمایش قرار نگرفته‌اند و همچنین برنامه‌های غیرقابل اطمینانی که از طرف اشخاص ثالث تأیید نشده‌اند و یا تأمین‌کنندگان، کاربران غیرقابل اطمینان و وب‌سایت‌های غیرقابل اطمینان از جعبه شن استفاده می‌شود.

معمولاً جعبه شن مجموعه‌ای از منابع به شدت کنترل شده مانند فضای مورد نیاز دیسک و حافظه برای برنامه‌هایی که قرار است در آن اجرا شوند را فراهم می‌کند. همچنین، دسترسی به شبکه، قابلیت جستجو و تجسس در سیستم میزبان یا خواندن از دستگاه‌های ورودی معمولاً غیرمجاز یا محدود شده است. از این جهت، جعبه شن را می‌توان نمونه‌ای از مجازی‌سازی دانست.

جعبه شن موجود در بحث تحلیل بدافزار را نباید با آن‌چه در مبحث توسعه‌ی نرم‌افزار تحت وب است، اشتباه گرفت. زیرا در بحث توسعه‌ی نرم‌افزار، جعبه شن یک محیط آزمون است که تغییرات ایجاد شده توسط کد بررسی نشده و فعالیت‌های بی‌درنگ آن را از محیط عملیات مجزا می‌کند.

از نظر کاربردی، جعبه شن یک سازوکار امنیتی است که برنامه‌های ناامن را بدون این که به سیستم اصلی آسیب برسد، در یک محیط امن اجرا می‌کند. همچنین، جعبه‌های شن دارای محیط‌های مجازی هستند که اغلب خدمات شبکه را شبیه‌سازی می‌کنند و رفتار نرم‌افزار مشکوک را کنترل کرده و در انتها گزارشی را تولید می‌کنند که برای کاربران از جمله مبتدیان قابل فهم است.

۲-۱- انواع جعبه شن

جعبه‌های شن به دو دسته‌ی *مبتنی بر وب*[1] و *مبتنی بر میزبان*[2] تقسیم می‌شوند.

۲-۱-۱- جعبه‌های شن مبتنی بر وب

در جعبه‌های شن مبتنی بر وب، بدافزار از طریق وب‌سایت مربوطه بارگذاری شده و نتیجه از طریق ارسال پست الکترونیکی یا صفحه‌ی دیگری نشان داده می‌شود. در واقع، هیچ‌گونه ابزاری بر روی سیستم کاربر نصب نمی‌شود و همچنین، عملیات انجام شده برای تحلیل بدافزار قابل مشاهده نیست، چرا که جعبه شن و عملیات آن بر روی سرویس‌دهنده‌ی دیگری در حال اجرا است.

۲-۱-۲- جعبه‌های شن مبتنی بر میزبان

این مدل از جعبه‌های شن باید بر روی سیستم کاربر نصب شوند. بدافزار را از روش‌های مختلفی می‌توان در سیستم کاربر بارگذاری کرد و به این ترتیب، تمام عملیات انجام شده برای تحلیل بدافزار مورد نظر در ماشین مجازی قابل مشاهده است. در پایان، گزارش تهیه شده در مسیری از سیستم میزبان قرار می‌گیرد.

۲-۲- انواع محصولات موجود

۲-۲-۱- ThreatTrack

ThreatTrack ابزاری برای تحلیل بدافزار به صورت پویا است. این ابزار امکان تحلیل هر گونه برنامه‌ی تحت ویندوز یا فایلی که آلوده است را از قبیل فایل‌های Office، PDF و URL های مخرب فراهم می‌کند. شرکت امنیتی ThreatTrack در شناسایی و متوقف کردن *تهدیدات مداوم پیشرفته*[3]، حملات هدفمند و سایر نرم‌افزارهای مخرب پیچیده تخصص دارد که برای عبور از سیستم امنیتی طراحی شده توسط شرکت‌ها به کار می‌رود.

[1] Web base
[2] Client base
[3] Advanced Persistent Threats (APTs)

ThreatTrack ابزارهای امنیتی پیشرفته‌ای تولید کرده است که جدیدترین تهدیدات مخرب را مورد تشخیص و تحلیل قرار داده و از بین می‌برد. این ابزار شامل ThreatAnalyzer برای تحلیل رفتار بدافزار، ThreatIQ به عنوان سرویس آگاهی تهدیدات بی‌درنگ و همچنین نرم‌افزارهای VIPRE business antivirus و VIPRE home antivirus می‌باشد. ابتدا فایل مربوطه از طریق وب‌سایت مربوط به این شرکت به آدرس http://www.threattrack.com بارگذاری شده و سپس، گزارش تحلیل را به صورت PDF و XML که شامل تمام اطلاعات رفتاری که در طول تحلیل به دست آمده است از طریق پست الکترونیکی ارسال می‌کند.

GFI Sandbox -۲-۲-۲

این جعبه شن یک ابزار تجزیه و تحلیل پویای صنعتی است. با استفاده از این ابزار می‌توان هر فایل اجرایی تحت ویندوز یا فایل‌های مستندات مانند Office، PDF و همچنین URL های مخرب، آگهی‌های FLASH و برنامه‌های کاربردی رایج را به صورت مجازی تحلیل کرد.

حملات هدفمند، وب‌سایت‌های هک شده و پیوست‌های الکترونیکی آلوده، بخشی از تهدیدات اینترنتی امروزه محسوب می‌شوند که تنها GFI Sandbox یک دید کامل از تمام جنبه‌های این تهدیدات را ارائه می‌دهد. این ابزار با استفاده از تکنولوژی Digital Behavior Traits رفتار بدافزار را سریع و هوشمندانه تشخیص می‌دهد.

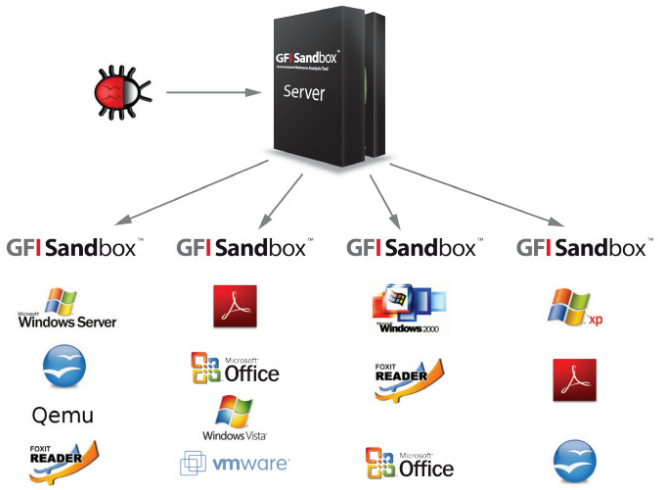
فن‌آوری DBT[1] امکان شناخت رفتار هر فایلی را در یک نگاه فراهم می‌کند. DBT با برجسته کردن ویژگی‌های کلیدی که می‌تواند رفتار مخرب را تشخیص دهد، راهنمای سریع و آسانی برای تحلیل‌گران فراهم می‌کند که آن‌ها را قادر می‌سازد تا فایل‌های واقعاً مشکوک را از همه‌ی فعالیت‌های بی‌ضرر جدا کنند.

ابزار Threat Intelligence تهدیدات ممکن را به صورت پویا تحلیل می‌کند. همچنین، این ابزار چگونگی اجرای یک برنامه در صفحه‌ی نمایش ویندوز، تغییرات سیستمی ایجاد شده و ترافیک کامپیوتری تولید شده را نشان می‌دهد. هنگامی که این ابزار با DBT همراه می‌شود، امکان تشخیص عملیات مخرب و رفتار یک تهدید به صورت خودکار به وجود می‌آید. GFI Sandbox رفتار را درون یک محیط نظارت شده تحلیل می‌کند و تمام عملیات مخرب را از قبیل

[1] Digital Behavior Traits

تغییرات سیستمی، ترافیک شبکه‌ای، عملیات انجام شده روی فایل، روبرداری[1] از حافظه و تصویر آن ثبت می‌کند. این جعبه شن نیازی به شبیه‌سازی و مجازی‌سازی ندارد.

GFI Sandbox توانایی مقایسه‌ی چندین تحلیل را برای دریافت شباهت‌ها و تفاوت‌های بین آن‌ها دارد. نمونه‌ها می‌توانند به چند جعبه شن فرستاده شوند و این در حالی است که مدیریت و اجرای فرآیندها به طور خودکار انجام می‌شود.



شکل ۱- تحلیل چند بدافزار در GFI Sandbox

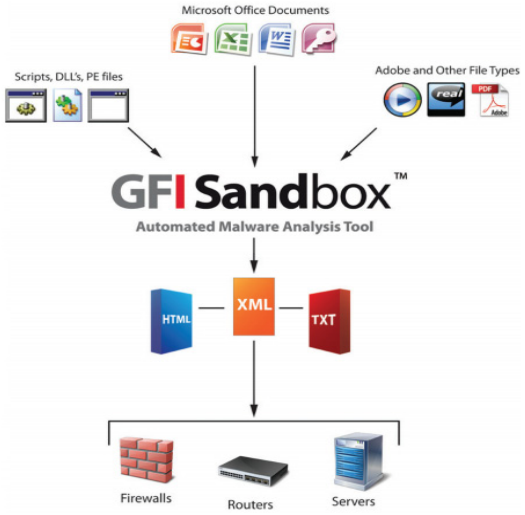
در GFI Sandbox بدافزار در سیستم‌های متفاوتی بررسی می‌شود تا تشخیص داده شود که بدافزار از کدام آسیب‌پذیری سوءاستفاده می‌کند.

داده‌هایی که GFI Sandbox پس از تحلیل در مورد فایل‌ها ارائه می‌دهد شامل تغییرات رجیستری و فایل‌های سیستمی، اطلاعات مربوط به DLLها، فرآیندها و سرویس‌ها، رشته‌های درهم *فایل*[2] (MD5، SHA-1) و فایل‌های ایجاد شده توسط بدافزار می‌باشد. همچنین، ترافیک شنود شده‌ی شبکه، اطلاعات جستجوی صورت گرفته برای DNS، اطلاعات خارجی از پویش‌گرها و URLهای مشاهده شده و مشخصات فایل‌های دانلود شده توسط بدافزار نیز از جمله داده‌هایی است که توسط GFI Sandbox در زمینه‌ی شبکه ارائه می‌گردد. در کنار این دو مورد، رویدادهای دیگری مانند بررسی اطلاعات Mutexها، روبرداری از فرآیندهای بدافزار، تصویر گرفتن از تمام پنجره‌هایی که در زمان تحلیل ایجاد شده‌اند نیز توسط این جعبه شن صورت می‌گیرد. در نهایت، گزارش تحلیل انجام شده به صورت فایل XML به

[1] Dump
[2] File hashes

همراه فایل PCAP از تمام فعالیت‌های شبکه که توسط فرآیندهای مخرب و آلوده در مدت انجام تحلیل ایجاد شده است به همراه تصاویر ممکن ارائه می‌شود.

در حالت معمولی یک پژوهش‌گر هر تهدید را با جزئیات با استفاده از تعدادی برنامه‌ی کاربردی به صورت دستی تحلیل می‌کند. توابع خودکار در GFI Sandbox مطابق با انتظار بدافزار از برخورد کاربر با برنامه‌های کاربردی، فایل‌ها یا وب‌سایت‌های آلوده تعامل می‌کند و تمام فعالیت‌ها را بدون هیچ مداخله‌ی کاربر تحلیل و ثبت می‌کند.



شکل ۲- چگونگی عملیات GFI Sandbox

CWSandbox -۳-۲-۲

CWSandbox یک ابزار برای تحلیل بدافزار است که سه معیار طراحی کنترل خودکار، اثربخشی و صحت را برای سیستم‌های عامل ویندوز ۳۲ بیتی پیاده‌سازی می‌کند.

کنترل خودکار از طریق انجام تحلیل بدافزار به صورت پویا به دست می‌آید؛ به این معنی که بدافزار توسط اجرا در یک محیط شبیه‌سازی شده تحلیل می‌شود. این روش برای انواع بدافزارها در اکثر شرایط کار می‌کند. ایراد تحلیل پویا این است که تنها اجرای بدافزار مورد نظر را بررسی می‌کند، در حالی که در تحلیل ایستا کد منبع بدافزار بررسی می‌شود و امکان مشاهده‌ی اجراهای متفاوتی از بدافزار را فراهم می‌کند.

با توجه به این موضوع که کد منبع بیشتر بدافزارها موجود نیست و مستنداتی از آن‌ها نیز وجود ندارد، نمی‌توان مطمئن بود که تغییری در فایل اجرایی آن صورت نگرفته باشد. تحلیل ایستا در سطح کد ماشین معمولاً دشوار است،

زیرا بدافزارها غالباً از سازوکارهای *مبهم‌سازی*[1] کد مانند فشرده‌سازی و رمزنگاری برای فرار از تحلیل و بررسی استفاده می‌کنند.

اثربخشی با استفاده از فرآیند جعل API به دست می‌آید. جعل API به معنی فراخوانی APIهای ویندوز ۳۲ بیتی است که در آن کد API اصلی فراخوانی شده به کد API جعل شده تغییر مسیر داده است. به واسطه‌ی این تغییر مسیر، توالی عملیات سیستمی انجام شده توسط بدافزار را می‌توان مشاهده کرد. جعل API می‌تواند توسط برنامه دور زده شود، به گونه‌ای که برای جلوگیری از استفاده از API ویندوز کد هسته را فراخوانی می‌کند. نتایج تجربی نشان داده است که بیشتر بدافزارهای پیشرفته و مستقل به گونه‌ای طراحی شده‌اند که هدف آن‌ها حمله به پایگاه‌های کاربری بزرگی است که از APIهای ویندوزی فراوانی استفاده می‌کنند.

روشی که برای به دست آوردن صحت استفاده می‌شود، تزریق DLL است. این DLL توابع API ویندوز را جعل می‌کند تا بتواند رفتار بدافزار را در طول تحلیل به دست آورد. این روش نتایج خوبی به همراه دارد، اما اگر بدافزار بتواند عملیات جعل را دور بزند و به طور مستقیم کد هسته را فراخوانی کند، باعث می‌شود که نظارتی بر بدافزار انجام نشود. در واقع، تزریق DLL اجازه می‌دهد که جعل API در یک روش ماژولار و قابل استفاده‌ی مجدد پیاده‌سازی شود که در نهایت اطمینان در پیاده‌سازی و صحت گزارش تحلیل را فراهم می‌آورد.

ترکیب این سه سازوکار در CWSandbox اجازه‌ی ردیابی و نظارت بر تمام فراخوانی‌های سیستمی مربوطه را داده و یک گزارش خودکار و خوانا توسط ماشین تولید می‌کند. این گزارش توصیف می‌کند که بدافزار چه فایل‌هایی را ایجاد کرده یا تغییر داده است. همچنین، تغییرات صورت گرفته در رجیستری ویندوز، DLLهای بارگذاری شده قبل از اجرا، دسترسی داده شده به حافظه‌ی مجازی، فرآیندهای ایجاد شده، ارتباطات شبکه‌ای و اطلاعات ارسال شده از طریق آن، از جمله مطالبی است که در گزارش CWSandbox می‌آید.

واضح است که این گزارش کامل نیست، زیرا تنها از روی رفتار مشاهده شده از بدافزار به دست می‌آید و گویای این موضوع نیست که بدافزار با استفاده از چه الگوریتم‌هایی کار می‌کند. استفاده از CWSandbox می‌تواند همراه با خطرات ناشی از اجرای بدافزار در ماشینی که به شبکه متصل است، باشد. با این حال، اطلاعات به دست آمده از اجرای

[1] Obfuscation

تروجان برای دوره‌های حتی بسیار کوتاه از زمان در CWSandbox به صورت شگفت‌آوری باارزش بوده و در اکثر موارد برای ارزیابی خطر نشأت گرفته از نرم‌افزارهای مخرب کافی است.

در واقع، CWSandbox روشی برای تحلیل پویای بدافزار مبتنی بر تحلیل رفتاری است. نمونه‌ی بدافزار برای مدت محدودی در یک محیط شبیه‌سازی شده اجرا می‌شود و در این حین، تمام فراخوانی‌های سیستمی بررسی می‌شوند. در نهایت، CWSandbox گزارش کاملی از تحلیل رفتار بدافزار فراهم می‌کند. همچنین، از طریق وب‌سایت مربوطه به آدرس http://www.mwanalysis.org می‌توان فایل مورد نظر را بارگذاری کرد و گزارش تحلیل را بررسی کرد.

۲-۲-٤- ThreatExpert

ThreatExpert یک سیستم تحلیل تهدید است که رفتار ویروس‌ها، کرم‌ها، تروجان‌ها، نرم‌افزارهای جاسوسی و دیگر ریسک‌های امنیتی را به طور خودکار و پیشرفته تحلیل کرده و گزارش آن را به کاربر می‌دهد. این جعبه شن می‌تواند تنها در عرض چند دقیقه فرآیند تحلیل را پردازش کند و یک گزارش بسیار دقیق با جزییات فنی و مطابق با استانداردهای صنعتی آنتی‌ویروس‌ها تهیه کند. این ابزار، وضعیت[1] ماشین مجازی را قبل و بعد از اجرای بدافزار ذخیره کرده و در انتها با یکدیگر مقایسه می‌کند. گزارشی که ThreatExpert در پایان کار می‌دهد به طور خلاصه شامل رویدادهایی در مورد فایل‌ها، فرآیندها و کلیدهای رجیستری تولید شده از طریق اجرای بدافزار است. همچنین، فعالیت‌های انجام شده در شبکه از قبیل آدرس‌های IP که با بدافزار اجرا شده در ارتباط است و سایر اطلاعات کاربردی نیز در گزارش نهایی وجود دارد. از طریق وب‌سایت مربوطه به آدرس http://www.threatexpert.com می‌توان فایل مورد نظر را برای تحلیل بارگذاری کرد.

۲-۲-۵- Xandora

Xandora ابزاری برای تحلیل رفتار *فایل‌های اجرایی*[2] مبتنی بر ویندوز است که روی تحلیل بدافزار تمرکز خاصی به خرج داده است. اجرای این ابزار نوع جدیدی از گزارش را فراهم می‌کند که شامل اطلاعات کافی درباره‌ی هدف و

[1] Snapshot
[2] PE-executables

عملیات فایل تحلیل شده است. همچنین، این گزارش شامل اطلاعات دقیقی درباره‌ی تغییرات انجام شده روی کلیدهای رجیستری یا فایل‌های سیستمی و سایر پردازه‌ها می‌باشد. این ابزار تمام ترافیک تولید شده در شبکه را نیز ثبت می‌کند. تحلیل صورت گرفته توسط این ابزار بر پایه‌ی اجرای فایل مورد نظر در یک محیط شبیه‌سازی شده و مشاهده‌ی عملکرد آن است. از طریق بارگذاری فایل مورد نظر در وب‌سایت http://www.xandora.net/xangui می‌توان گزارش تحلیل را دریافت کرده و مورد بررسی قرار داد.

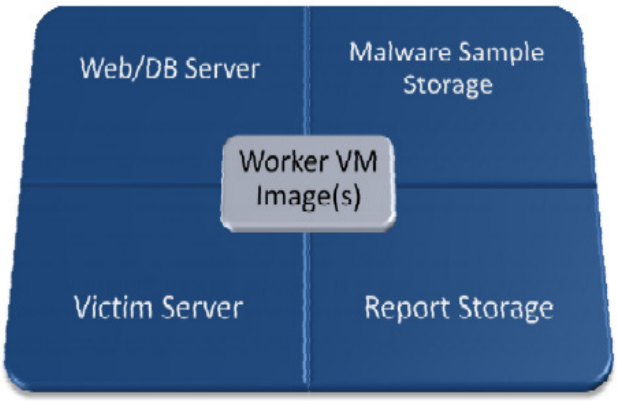
Anubis -٦-٢-٢

Anubis مجموعه‌ای از چندین ابزار برای تحلیل رفتار فایل‌های اجرایی مبتنی بر ویندوز به خصوص بدافزارها به صورت پویا است. گزارش حاصل از این تحلیل شامل اطلاعات کافی برای کاربر است که به او هدف و عملیات انجام شده توسط فایل باینری تحلیل شده را می‌دهد. این ابزار علاوه بر ثبت ترافیک شبکه، اطلاعاتی در مورد تغییرات ایجاد شده روی کلیدهای رجیستری، فایل‌های سیستمی و همچنین تعاملات انجام شده با سرویس‌های تحت ویندوز و پردازه‌ها را در گزارش خود ثبت می‌کند. این تحلیل بر پایه‌ی اجرای فایل باینری مورد نظر در یک محیط شبیه‌سازی شده است. این تحلیل روی جنبه‌های امنیتی عملیات برنامه‌ی مورد نظر تأکید می‌کند که باعث آسان شدن عملیات تحلیل می‌شود. آدرس وب‌سایت این ابزار http://anubis.iseclab.org می‌باشد. Anubis دارای پنج بخش اصلی است:

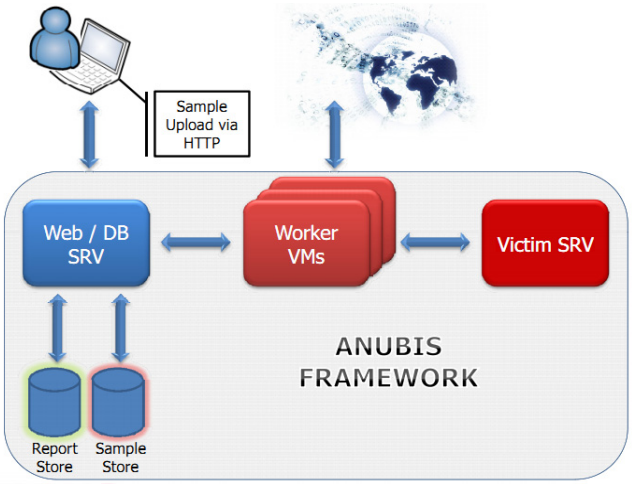
- **سرویس‌دهنده‌ی وب و پایگاه داده‌های بازدیدکنندگان HTTP و HTTPS برای بارگذاری و مدیریت:** این پایگاه داده‌ها، گزارش‌ها و نمونه‌های XML را ذخیره کرده و مقدار زیادی آمار و اطلاعات تولید می‌کند.
- **ذخیره‌سازی نمونه‌ی بدافزار:** در این قسمت، فایل‌های بارگذاری شده و نمونه‌های تحلیل شده‌ی قبلی ذخیره می‌گردد.
- **ذخیره‌سازی گزارش:** در این قسمت، فایل‌های گزارش از قبیل روبرداری از ترافیک و فایل‌های دانلود شده ذخیره می‌گردد.
- **سرویس‌دهنده‌ی قربانی:** این سرویس‌دهنده به عنوان *ظرف عسل محلی*[1] برای برخی از سرویس‌ها عمل کرده و ترافیک‌های مخرب محلی را نگهداری می‌کند.

[1] Local honeypot

- **چند ماشین مجازی:** *فن‌آوری بازگردانی وضعیت پیشین سیستم*[1] که ماشین مجازی سیستم عامل مورد آزمایش را به حالت شناخته شده‌ی قبلی در چند ثانیه برمی‌گرداند.



شکل ۳- پنج بخش اصلی Anubis



شکل ٤- معماری Anubis

۲-۲-٦-۱- ویژگی‌های پیشرفته‌ی Anubis

ابزار Anubis ترافیک شبکه‌ای مربوط به نمونه‌ها را ثبت و تحلیل می‌کند که در آن HTTP، FTP، SMTP، IRC و غیره به عنوان فایل PCAP وجود دارد.

گزارش‌های حاصل از تحلیل شامل تماس با سرویس‌دهنده، فایل‌های ایجاد شده، فایل‌های تغییر داده شده، فایل‌های پاک شده، کلیدهای رجیستری دستکاری شده و خلاصه‌ی کوتاهی از نوع تهدید می‌باشد.

[1] Snapshot technology

این جعبه شن دارای چندین قالب گزارش از قبیل XML، HTML، MHT، PDF و TXT است. همچنین، ابزار Anubis دارای تحلیل ایستای پویش‌گرهای AV و PE می‌باشد.

Malbox -۷-۲-۲

Malbox نیز سرویسی برای تحلیل بدافزار است که فایل‌های اجرایی تحت ویندوز یا فایل‌های فشرده را از طریق وب‌سایت http://malbox.xjtu.edu.cn دریافت کرده و گزارشی مبنی بر عملیات انجام شده تهیه می‌کند. همچنین، می‌توان URL مشکوک مورد نظر را به این وب‌سایت ارسال و گزارشی مبنی بر عملیات انجام شده در مورد این URL را هنگام مشاهده‌ی آن فراهم کرد.

Cuckoo Sandbox -۸-۲-۲

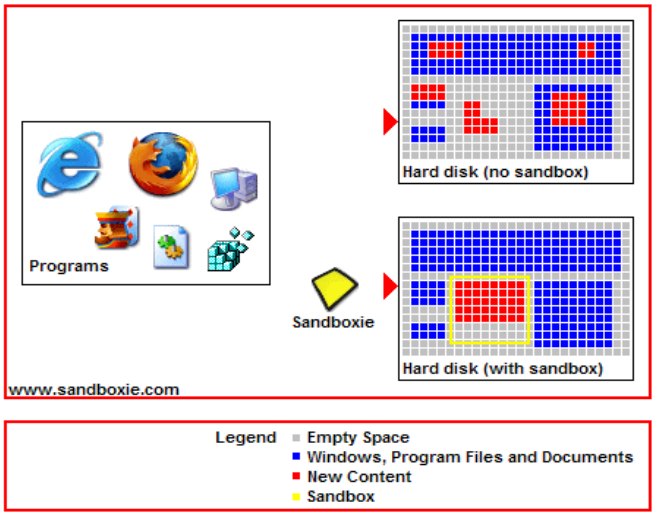
Cuckoo Sandbox یک سیستم *منبع‌باز*[1] برای تحلیل خودکار بدافزار است. Cuckoo Sandbox به عنوان پروژه‌ی کد تابستانی Google در سال ۲۰۱۰ میلادی همراه با پروژه‌ی Honeynet شروع شد و به یکی از بهترین جعبه‌های شن منبع‌باز محبوب تبدیل گردید. Cuckoo Sandbox یک سیستم کاملاً خودکار مهیا می‌کند که فایل را واکشی کرده و آن را در یک محیط ایزوله شده‌ی ویندوزی تحلیل می‌کند و نتیجه را برمی‌گرداند. هدف آن ایجاد روشی برای تحلیل خودکار فایل‌ها است و گزارشی در مورد فعالیت‌های فایل مورد نظر به هنگام اجرا در یک محیط ایزوله ارائه می‌دهد. فایل تحلیل شده می‌تواند از انواع متفاوتی از قبیل فایل اجرایی ویندوز، DLL، PDF، Office، اسکریپت‌های PHP، Python، URL و تقریباً هر فایل قابل تصور دیگر باشد. Cuckoo Sandbox داده‌های خام متفاوتی را به کاربر ارائه می‌دهد که شامل اطلاعاتی از قبیل ردیابی توابع اصلی و فراخوانی API های ویندوزی، رونوشت از فایل‌های ایجاد شده و پاک شده‌ی سیستمی، روبرداری از حافظه‌ی فرآیندهای انتخاب شده، روبرداری از کل حافظه‌ی ماشین مجازی، تصویر از صفحه‌ی نمایش ویندوز در حین اجرای بدافزار و شنود ترافیک شبکه‌ی ایجاد شده توسط بدافزار می‌باشد. از آن‌جایی که نتایج به دست آمده برای کاربران معمولی باید قابل فهم باشد، Cuckoo Sandbox اطلاعات به دست آمده را پردازش کرده و گزارشی با انواع متفاوت قالب‌ها از قبیل JSON، HTML، MAEC، رابط[2]

[1] Open Source
[2] Interface

MongoDB و رابط HPFeeds ایجاد می‌کند. در واقع، طراحی وسیع و ماژولار به کاربران این توانایی را می‌دهد که پردازش و گزارش‌گیری را در کنار یکدیگر داشته باشند.

Sandboxie -۹-۲-۲

Sandboxie توسط Ronen Tzur برای سیستم‌های عامل ویندوز ۳۲ بیتی و ۶۴ بیتی مبتنی بر NT توسعه یافته است. Sandboxie یک محیط ایزوله شده‌ی شبیه جعبه شن است که در آن برنامه‌ها بدون هیچ‌گونه تغییر دائمی در درایوهای محلی یا نگاشته شده اجرا یا نصب می‌شوند. این محیط مجازی ایزوله شده، برنامه‌های غیرمطمئن و گشت و گذار در وب را به صورت کنترل شده بررسی می‌کند.



شکل ۵- چگونگی عملیات در Sandboxie

فلش قرمز در شکل ۵ جریان تغییرات برنامه‌ی در حال اجرا را در کامپیوتر نشان می‌دهد. مستطیلی که برچسب *دیسک سخت (بدون Sandbox)*[1] دارد، تغییرات برنامه‌ای را نشان می‌دهد که به صورت عادی اجرا می‌شود. مستطیلی که برچسب *دیسک سخت (با Sandbox)*[2] دارد، تغییرات برنامه‌ای را نشان می‌دهد که تحت جعبه شن اجرا می‌شود. این شکل نشان می‌دهد که Sandboxie قادر به رهگیری تغییرات و ایزوله کردن آن‌ها در جعبه شن می‌باشد که در این شکل به صورت یک مستطیل زرد رنگ نشان داده شده است. همچنین، این شکل نشان می‌دهد که گروه‌بندی این تغییرات با هم، پاک کردن آن‌ها را در یک زمان آسان می‌کند.

[1] Hard disk (no Sandbox)
[2] Hard disk (with Sandbox)

از مزیت‌های جعبه شن ایزوله شده می‌توان به مرور در وب‌سایت‌ها به صورت امن، حریم شخصی پیشرفته و پست الکترونیکی امن نام برد.

برای مرور در وب‌سایت‌ها به صورت امن، مرورگر تحت حفاظت Sandboxie اجرا می‌شود؛ به این معنی که تمام نرم‌افزارهای مخربی که توسط مرورگر دانلود می‌شوند در این جعبه شن به دام افتاده و دور ریخته می‌شوند. Sandboxie برای ایجاد حریم شخصی پیشرفته، تاریخچه‌ی مرورگر، کوکی‌ها[1] و فایل‌هایی که به صورت موقتی نگهداری شده‌اند و در حین مرور در وب در جعبه شن باقی می‌مانند و راهی به ویندوز نمی‌یابند را جمع‌آوری می‌کند. همچنین، Sandboxie امن بودن پست الکترونیکی را نیز تضمین می‌کند. زیرا ویروس‌ها و دیگر نرم‌افزارهای مخرب که در پست الکترونیکی پنهان می‌شوند، نمی‌توانند از جعبه شن بیرون آمده و سیستم اصلی را آلوده کنند.

Buster Sandbox Analyzer -۱-۹-۲-۲

Buster Sandbox Analyzer ابزاری برای تحلیل رفتار فرآیندها و تغییرات ایجاد شده در سیستم است که بدافزار مشکوک را ارزیابی می‌کند.

تغییرات انجام شده در سیستم به شکل‌های متفاوتی از قبیل تغییرات فایل‌های سیستمی، تغییرات رجیستری و استفاده از درگاه‌ها صورت می‌گیرد. این تغییرات در فایل‌های سیستمی هنگامی اتفاق می‌افتد که یک فایل ایجاد، پاک یا دستکاری می‌شود و می‌توان بسته به نوع فایلی که ایجاد می‌شود مانند فایل اجرایی، کتابخانه‌ای، جاوااسکریپت، batch و غیره و اطلاع از مسیر آن، تحلیل دقیق‌تری را به دست آورد. این موضوع در مورد رجیستری نیز صادق است و تغییرات در رجیستری ویندوز مانند دستکاری مقادیر کلیدهای رجیستری و ایجاد یا حذف شدن کلیدها به تحلیل‌گران کمک شایانی می‌کند. منظور از تغییرات ایجاد شده در درگاه زمانی است که درخواستی برای استفاده از درگاه مانند اتصال به شبکه و یا کامپیوتر دیگر صورت می‌گیرد و در این زمان جعبه شن این درگاه را شنود می‌کند. با استفاده از تمام این تغییرات می‌توان اطلاعات لازم را برای ارزیابی خطر موجود در عملیاتی که بدافزارها در جعبه شن اجرا می‌کنند به دست آورد.

[1] Coockies

Buster Sandbox Analyzer مانند سایر ابزارهای تحلیل بدافزار جوانب مثبت و منفی دارد. این ابزار در هر کامپیوتری که Sandboxie نصب و در حال انجام کار باشد، اجرا می‌شود. در ضمن نیازی به اتصال به اینترنت ندارد، اما طبیعتا اگر اتصال به شبکه وجود داشته باشد، بهتر است.

این ابزار قادر است هرگونه فایل از قبیل EXE، BAT، VBS، PDF، XLS، DOC و غیره را تحلیل کند. اگر فایل قابل اجرا باشد، Buster قادر به تحلیل آن می‌باشد. معمولاً تحلیل‌گران بدافزار تنها فایل‌های PE[1] را پردازش می‌کنند. اگر نیاز به کتابخانه‌ای مانند DLL، OCX و غیره باشد، با استفاده از این ابزار می‌توان تنها با کپی یا نصب هر آن‌چه که برای انجام درست برنامه‌ی کاربردی لازم است، این احتیاجات را برآورده کرد. این در حالی است که سایر ابزارها فقط یک برنامه را در هر زمان اجرا می‌کنند و اگر نیاز به کتابخانه یا چیز دیگری باشد، عملیات تحلیل با شکست مواجه می‌شود.

این ابزار رایگان می‌باشد و تنها کافی است برای مجوز Sandboxie هزینه پرداخت شود که بسیار ارزان بوده و نیازی به پرداخت مجدد نیست. اگرچه سایر ابزارهای تحلیل مبتنی بر وب رایگان هستند، اما سرویس‌های آن‌ها در هر زمانی ممکن است قطع شوند.

Buster Sandbox Analyzer قابل تنظیم است. می‌توان تعریف کرد که چه نوع فایلی را بررسی کند یا چه کلید رجیستری به عنوان مکان شروع در نظر گرفته شود. حتی می‌توان این ابزار را طوری تنظیم کرد که ترافیک شبکه را ذخیره کند. این در حالی است که سایر ابزارها قابل تنظیم نمی‌باشند.

Buster Sandbox Analyzer این قابلیت را دارد که نرم‌افزارهایی مانند Process Monitor یا Process Explorer و سایر موارد دیگر را برای تحلیل دقیق‌تر در خود مورد استفاده قرار دهد، در حالی که این امکان در سایر ابزارهای تحلیل وجود ندارد. این ابزار مستقل از نسخه‌ی ویندوز است و در نسخه‌های ویندوز 2000، XP، Vista، 7 و 8 قابل استفاده است، اما سایر ابزارها بدافزار را تنها در نسخه‌های جدید ویندوز XP، Vista و 7 تحلیل می‌کنند[2].

Buster Sandbox Analyzer توانایی تحلیل چند بدافزار را در یک زمان دارد، اما سایر ابزارها تنها یک بدافزار را در هر زمان تحلیل می‌کنند.

[1] Win32 executables

[2] در زمان نگارش این مقاله

Sandboxie بستر مورد استفاده توسط Buster Sandbox Analyzer برای تحلیل بدافزار است و تقریباً از هیچ منبع سیستمی استفاده نمی‌کند. به همین دلیل این ابزار سرعت بالایی دارد، در حالی که در سایر ابزارهای تحلیل بدافزار از ماشین‌های مجازی مانند VirtualBox، VMWare و بسترهای دیگر که منابع سیستمی بسیاری مصرف می‌کنند، استفاده می‌شود که این امر باعث کاهش سرعت می‌گردد.

این ابزار قادر به مشاهده‌ی تمام تغییرات سیستمی که توسط برنامه‌هایی که درایور نصب می‌کنند نیست. این امر به خاطر محدودیت‌های Sandboxie است که نصب درایور به دلایل امنیتی انجام نمی‌شود. در ضمن، این ابزار قادر به مشاهده‌ی تزریق DLL در پردازه‌های سیستمی خاص نیست، به این دلیل که آن‌ها خارج از جعبه شن اجرا می‌شوند و Sandboxie این اجازه را نمی‌دهد. در نهایت، این ابزار در حالت تجزیه و تحلیل خودکار قادر به تحلیل نمونه‌هایی که نیاز به دخالت کاربر برای نصب دارد، نیست.

BitBlaze -۱۰-۲-۲

هدف پروژه‌ی BitBlaze طراحی و توسعه‌ی بستری برای تحلیل فایل‌های باینری است. علاوه بر آن، BitBlaze قادر به تشخیص و تحلیل بدافزار و همچنین، دفاع در برابر کد مخرب نیز می‌باشد. این پروژه یک فضای کاربردی جدید برای تحلیل فایل ارائه می‌دهد که نتایجی مؤثرتر و فراتر از نرم‌افزارهای امنیتی مانند پروتکل مهندسی معکوس و تولید اثر انگشت ایجاد می‌کند. وب‌سایت مربوط به این برنامه، آدرس http://bitblaze.cs.berkeley.edu می‌باشد.

Zero Wine -۱۱-۲-۲

Zero Wine یک پروژه‌ی تحقیقاتی منبع‌باز برای تحلیل رفتار بدافزار به صورت پویا است. Zero Wine بدافزار را با استفاده از Wine در یک جعبه شن مجازی امن که در واقع یک محیط ایزوله است، اجرا می‌کند و اطلاعاتی درباره‌ی APIهایی که توسط برنامه فراخوانی شده است، جمع‌آوری می‌کند. Wine با استفاده از یک متغیر محیطی برای اشکال‌زدایی به نام winedebug توالی APIهای فراخوانی شده و مقادیر استفاده شده توسط بدافزار را به عنوان خروجی ارائه می‌دهد. با استفاده از این اطلاعات، تحلیل رفتار بدافزار بسیار ساده می‌شود.

Wine که در اصل مخفف جمله‌ی "Wine Is Not an Emulator" است، قادر به اجرای برنامه‌های کاربردی ویندوز در چندین سیستم عامل سازگار با POSIX مانند لینوکس، مکینتاش و BSD است. Wine به جای شبیه‌سازی منطق ویندوزهای داخلی مانند یک ماشین مجازی و یا شبیه‌ساز، فراخوانی API تحت ویندوز را به فراخوانی POSIX ترجمه می‌کند، عملکرد و *خطاهای حافظه‌ی*[1] مربوط به روش‌های دیگر را از بین می‌برد و اجازه می‌دهد که برنامه‌های کاربردی ویندوز روی کامپیوتر انجام شوند.

Zero Wine به صورت ماشین مجازی QEMU همراه با سیستم‌عامل Debian توزیع می‌شود که شامل نرم‌افزاری برای بارگذاری و تحلیل بدافزار برای تولید گزارشی مبتنی بر اطلاعات جمع‌آوری شده است. این نرم‌افزار در مسیر /home/malware/zerowine ذخیره می‌شود. ماشین مجازی توزیع شده با دستورات صحیح خط فرمان اجرا می‌شود که از اسکریپت‌های پوسته‌ای برای اجرای ماشین مجازی استفاده می‌کند. یک رابط گرافیکی مبتنی بر وب که به زبان Python نوشته شده است، برای بارگذاری بدافزار مورد نظر وجود دارد. هنگامی که بدافزار جدید بارگذاری شد، یک نسخه از آن در مسیر /tmp/vir/MD5_OF_THE_FILE قرار می‌گیرد. بنا بر تشخیص کاربر، محیط Wine ایجاد شده‌ی قبلی به نام WINEPREFIX حذف شده و سیستم پشتیبان استخراج می‌گردد. بعد از این عملیات، بدافزار با استفاده از اسکریپت پوسته‌ای malware_launcher.sh که در /home/malware/bin نگهداری می‌شود، اجرا می‌گردد.

سیستم فعلی تنها به اجرای یک بدافزار در یک زمان می‌پردازد. در آینده هرگاه یک فایل بارگذاری شد، برای تحلیل به صف اضافه شده و یک WINEPREFIX جدید مختص اجرای این بدافزار ایجاد می‌گردد. وب‌سایت مربوط به Zero Wine آدرس http://sourceforge.net/projects/zerowine/ می‌باشد.

Joe Sandbox -۱۲-۲-۲

Joe Sandbox که همان JoeBox سابق است، یک سیستم تحلیل کاملاً خودکار برای تروجان‌ها، ویروس‌ها و بدافزارها است. این ابزار فایل‌های اجرایی مخرب مانند فایل‌های PE، PDF یا DOC را به عنوان ورودی می‌گیرد و گزارش دقیقی از رفتار اجرایی فایل مذکور برمی‌گرداند. این گزارش ساخت‌یافته نشان می‌دهد که چگونه بدافزار خودش

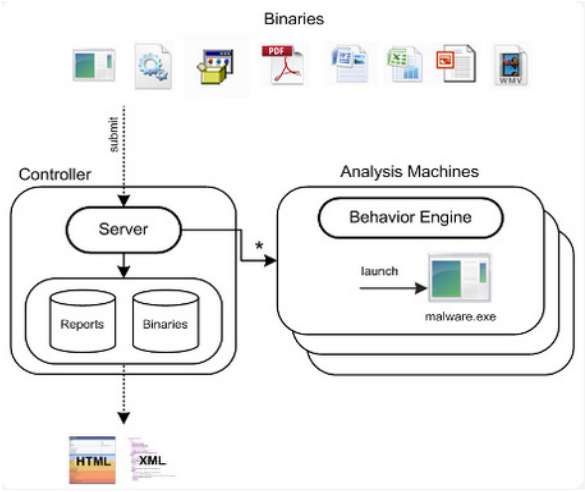
[1] Memory penalties

را نصب می‌کند، چگونه با اینترنت ارتباط برقرار کرده و چطور خودش را مخفی نگه می‌دارد. Joe Sandbox با استفاده از امضاهای رفتاری پیشرفته، عملیات را توضیح داده و فهم آن را آسان می‌کند. با استفاده از این ابزار می‌توان بدافزار مورد نظر را روی ویندوز XP، Vista و یا 7 اجرا کرد. در واقع این ابزار برای تحلیل بدافزار در مقیاس بالا بسیار مناسب است. وب‌سایت مربوط به این ابزار آدرس http://www.joesecurity.org/index.php است.

معماری Joe Sandbox به صورت ماژولار است و شامل یک ماشین هدایت‌کننده که با سیستم عامل لینوکس کار می‌کند و چند ماشین تحلیل که توسط محصولات مجازی مانند VMware یا VirtualBox راه‌اندازی می‌شوند، می‌باشد. کاربران، فایل و URL مورد نظر را برای آزمون از طریق رابط وب Joe Sandbox به سرویس‌دهنده‌ی کنترل‌کننده می‌فرستند و سرویس‌دهنده، فایل مشکوک را در یک پایگاه داده‌ها ذخیره کرده و آن را برای ماشین‌های تحلیل‌گر کنترل شده ارسال می‌کند.

موتور تجزیه و تحلیل تهدید[1] پیکربندی شده و Joe Sandbox تمام فعالیت‌ها را در حین اجرای فایل باینری مورد نظر بررسی کرده و داده‌های رفتاری را به کنترل‌کننده گزارش می‌دهد. موتور تجزیه و تحلیل تهدید این جعبه شن به طور کامل در هسته‌ی سیستم عامل قرار گرفته است که این امر باعث می‌شود تشخیص و دور زدن آن سخت شود.

هنگامی که عملیات تحلیل پایان می‌یابد، سرویس‌دهنده‌ی Joe Sandbox از الگوریتم‌های پیچیده و امضای عمومی برای انجام تحلیل و ارزیابی بیشتر عملیات رفتاری نظارت شده استفاده می‌کند. نتایج و عملیات ارزیابی شده با جزئیات در یک گزارش ساخت‌یافته تألیف می‌شود.



شکل ٦- چگونگی عملیات در Joe Sandbox

[1] Threat Analysis Engine (TAE)

Malwr -۱۳-۲-۲

Malwr یک سرویس تحلیل بدافزار رایگان است. با استفاده از این سرویس می‌توان فایل‌های مشکوک را تحلیل کرد و اطلاعاتی در مورد فرآیندها و رفتار شبکه در حین اجرای بدافزار به دست آورد. Malwr از روی یک سرویس تحلیل بدافزار منبع‌باز به نام Cuckoo Sandbox به وجود آمده است. ویژگی‌هایی از قبیل رایگان بودن، مستقل بودن از هرگونه فروش امنیتی، تجاری نبودن و توانایی اجرای چند ماشین توزیع شده برای انجام تحلیل بدافزار وجود دارد که این سرویس را منحصر به‌فرد کرده است. طریقه‌ی استفاده‌ی آن به این گونه است که فایل مورد نظر را انتخاب کرده و گزارش را ارائه می‌دهد.

می‌توان نوع بسته‌ی تحلیل را بین انواع موجود انتخاب کرد. البته اگر گزینه‌ای انتخاب نشود، به طور خودکار بسته‌ی مناسب انتخاب شده و اگر قالب فایل تأیید نشود، عملیات تحلیل انجام نمی‌شود. در نهایت، نتیجه‌ی تحلیل به آدرس پست الکترونیکی کاربر فرستاده می‌شود. Malwr توسط Claudio nex Guarnieri و Alessandro jekil Tanasi و گراف تحلیل رفتاری آن توسط Andy Nordbo ایجاد شده است. وب‌سایت مربوط به این ابزار آدرس https://malwr.com/submission می‌باشد.

۳- مراجع

[1] J. Berdajs and Z. Bosnic, *Extending applications using an advanced approach to DLL injection and API hooking.* Software - Practice & Experience, vol. 40, no. 7, pp. 567-584, 2010.

[2] Wikipedia. *http://en.wikipedia.org.* [Online] http://en.wikipedia.org/wiki/Sandbox_(computer_security).

[3] Wikipedia. *http://en.wikipedia.org.* [Online] http://en.wikipedia.org/wiki/Sandbox_(software_development).

[4] *Practical Malware Analysis.* Honig, Michael Sikorski and Andrew. San Francisco : William Pollock, 2012.

[5] Google. *www.google.com.* [Online] www.google.com/List of Sandboxes for Malware Analysis! — PenTestIT.htm.

[6] GFI Sandbox Powerful Automated Threat Analysis. 2011.

[7] Malware Analysis System CWSandbox :: Behavior-based Malware Analysis. http://www.mwanalysis.org. [Online] http://www.mwanalysis.org/?site=1&page=about.

[8] SecTechno Information Security Blog. *www.google.com.* [Online] www.google.com/Online Malware Sandboxes _ SecTechno.htm.

[9] Thomas Mandl, Ulrich Bayer, Florian Nentwich. ANUBIS ANalyzing Unknown BInarieS The automatic Way. 2009.

[10] Cuckoo: A Malware Analysis Sandbox! *www.google.com.* [Online] www.google.com/Cuckoo A Malware Analysis Sandbox! — PenTestIT.htm.

[11] *Buster Sandbox Analyzer.* 2009-2013.

[12] Zero Wine: Malware Behavior Analysis. *www.sourceforge.net.* [Online] http://zerowine.sourceforge.net/.

[13] Zero Wine Tryouts. *www.google.com.* [Online] www.google.com/Zero Wine Tryouts _ Official Website.htm.

[14] Joe Security LLC. *www.google.com.* [Online] 2012. www.google.com/standalone.htm.

[15] Malwr. *https://malwr.com.* [Online] https://malwr.com/about/.

[16] Wepawet. *www.wepawet.org.* [Online] http://wepawet.iseclab.org/about.php.

[17] Sandboxie. [Online] http://www.Sandboxie.com/.

[18] Wine. *http://www.winehq.org.* [Online] http://www.winehq.org/about/.