قسمت ۱ – تجزیه و تحلیل کاربردی بدافزارها

راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها،
باج‌افزارها، جاسوس‌افزارها، روت‌کیت‌ها و بوتکیت‌های رایانه‌ای

آزمایشگاه امنیت کی‌پاد

مقدمه

امروزه با پیشرفت و توسعه علوم رایانه‌ای درکلیه زمینه‌ها، این رشته به عنوان بخش جدا نشدنی از دیگر علوم در آمده است و کاربرد آن هر روز در جامعه بشری بیشتر احساس می‌گردد. همچنین استفاده و به‌کارگیری رایانه در تمامی علوم و رشته‌ها گویای نقش واقعی این پدیده برای زندگی ما است.

اما همینطور که رایانه راه پیشرفت خود را با قدرت ادامه می‌دهد، خطراتی هم حوزه استفاده کاربران آن را تهدید می‌کند. خطراتی از قبیل هکرها، درهای‌پشتی، روت‌کیت‌ها، بوت‌کیت‌ها، اکسپلویت‌کیت‌ها، جاسوس‌افزارها، باج‌افزارها، آگهی‌افزارها، حملات سایبری مبتنی بر زیرودی، سایت‌های فیشینگ که شناخته‌شده‌ترین حملات در این حوزه هستند.

اما از آنجایی‌که منبع آموزشی به روز و جامعی به زبان پارسی در این حوزه برای علاقمندان و متخصصین علوم رایانه وجود نداشت، بر آن شدیم تا حد توان خود تلاش کرده و یک منبع مفید برای علاقمندان به مباحث تحلیل بدافزارها ایجاد کنم.

شایان ذکر است در تالیف این اثر فقط منابع انگلیسی به پارسی ترجمه نشده‌اند، در برخی موقعیت‌ها توضیحات بیشتر لحاظ کرده و یا از جملات و کلمات دیگری برای ارائه مفاهیم تخصصی به شخص خواننده استفاده کرده‌ایم، تا بتوانیم حداکثر مطالب این سلسله مقالات را به شخص خواننده منتقل کنیم.

با این حال، علاوه بر تمام تلاش و کوشش‌هایی که در راه تالیف و ترجمه این سلسله مقالات به عمل آمده است، مجموعه حاضر خالی از مشکالات فنی نیست. لذا از تمامی اساتید ارجمند، صاحب‌نظران و دانشجویان محترم استدعا داریم با نظرات و پیشنهادات خودشان بنده را راهنما باشند. امیدوارم، این سلسله مقالات مورد توجه جامعه مهندسین امنیت و اطلاعات کشور عزیزمان قرار بگیرد.

فصل اول : مقدمه‌ای بر مفاهیم تحلیل بدافزار

بدافزار یا Malware مخفف جمله لاتین Malicious Software است که نقش کلیدی و بسزایی در اکثر حوادث‌های نفوذگری و امنیت رایانه‌ای و صنعتی دارد. تمامی نرم‌افزارهایی که بتوانند به یک کاربر[1]، کامپیوتر یا شبکه آسیب برسانند در خانواده بدافزارها قرار می‌گیرند.

این خانواده خرابکار، شامل یک گروه خاص از برنامه‌های رایانه‌ای می‌شوند، از قبیل ویروس‌ها[2]، تروجان‌ها[3]، کرم‌ها[4]، باج‌افزارها[5]، بوتکیت‌ها[6]، اکسپلویت‌کیت‌ها[7]، روت‌کیت‌ها[8] و جاسوس‌افزارها[9] که سرکردگان این خانواده وحشی رایانه‌ای هستند.

علاوه بر این، به عنوان تحلیلگران بدافزار، یک مجموعه از ابزارهای گوناگون و تکنیک‌های معمولی در اختیارمان قرار دارد که با استفاده از آن‌ها می‌توانیم بدافزارها را تحلیل کنیم، در حالی‌که، هر کدام از بدافزارها قابلیت‌های خاص خود را دارند و عملیات‌های گوناگونی را انجام می‌دهند (در طول این مجموعه مقالات این موضوع را مشاهده خواهید کرد).

همچنین شایان ذکر است، تحلیل بدافزار همانند هنر کالبدشکافی[10] است و متخصصین تحلیلگر بدافزار مانند یک پزشک‌جراح هستند که به منظور کالبدشکافی یک جسم نیاز به ابزارهای گوناگون دارند، با این تفاوت‌که متخصصین تحلیلگر بدافزار با یک جسم فیزیکی مواجه نیستند و باید کالبد یک نرم‌افزار مخرب رایانه‌ای را بشکافند و از اسرار مخفی درون آن سر در بیاورند. به عنوان مثال، بدافزار چگونه کار می‌کند؟ چگونه به شبکه نفوذ کرده است؟ چگونه توانسته با موفقیت سامانه‌های پیشگیری و شناسایی نفوذ را دور بزند؟ چگونه باید آن را شناسایی کرد؟ و چگونه باید با آن مقابله یا حذفش کرد.

---

[1] User
[2] Virus
[3] Trojans
[4] Worms
[5] Ransomwares
[6] Bootkits
[7] Exploitkits
[8] Rootkits
[9] Spywars
[10] Art of Dissecting

با استناد به میلیون‌ها بدافزاری که در جهان وجود دارد و هر روز هم بر تعداد آن‌ها افزوده می‌شود، در آینده نزدیک، تحلیل بدافزار یک حرفه مهم برای تمامی کسانی خواهد شد که در زمینه پاسخگویی به امنیت رایانه‌ها فعالیت می‌کنند. همچنین با وجود افراد متخصص بسیار کم در این زمینه مشاهده خواهید کرد که مهارت تحلیل بدافزار در زمان بسیار کوتاهی به یک مسئله جدی برای تمامی ارگان‌های امنیتی تبدیل خواهد شد.

در اینجا باید این نکته را هم بگویم، در تالیف این سلسله مقالات روی مسئله "چگونه بدافزارها را شناسایی کنیم؟" تمرکز نخواهیم کرد اگر چه یک سری اشارات کلی به آن خواهیم داشت ولی بیشتر تمرکز این سلسله مقالات روی تحلیل بدافزارهایی معطوف خواهد شد که قبلا کشف و شناسایی شده‌اند.

همچنین در این سلسله مقالات تمرکز اصلی ما روی بدافزارهای ویندوزی و لینوکسی و همچنین اندرویدی خواهد بود و مابقی سامانه‌های‌عامل را به صورت موردی مورد بررسی قرار خواهیم داد. زیرا سامانه‌عامل ویندوز و لینوکس، بیشترین سهمیه را میان سامانه‌عامل‌های مورد استفاده در رایانه‌های شخصی و اندروید بیشترین سهمیه را در سامانه‌های‌عامل تجهیزات نهفته بر عهده دارند و به همین دلیل بیشتر بدافزارهای تولیدی برای این سامانه‌های‌عامل هستند.

همچنین در این سلسله مقالات ما روی فایل‌های اجرایی[1] سامانه‌عامل ویندوز (PE-exe)، سامانه‌عامل لینوکس (ELF) و البته سامانه‌عامل اندروید (APK) متمرکز خواهیم شد، زیرا آن‌ها عمومی‌ترین و دشوارترین فایل‌هایی هستند که برای تحلیل با آن‌ها مواجه خواهید شد.

در پایان باید بگوییم، در طول این سلسله مقالات ما از تحلیل اسکریپت‌ها پرهیز خواهیم کرد و بجای آن‌ها به صورت عمیق روی تکنیک‌های کالبدشکافی تهدیدهای امنیتی پیشرفته از قبیل؛ درهای‌پشتی، روتکیت‌ها، بوتکیت‌ها، باج‌افزارها و بدافزارهای پنهان متمرکز خواهیم شد.

هدف از تحلیل بدافزار چیست؟

قبل از این‌که به جزییات عمیق تحلیل بدافزارها بپردازیم، باید بعضی از واژگان‌تخصصی[2]، انواع بدافزارهای رایج و رویکردهای اساسی تحلیل بدافزارها را معرفی و تشریح کنیم.

---

[1] Executable
[2] Terminology

همان‌طورکه پیش از این توصیف شد هر برنامه‌ای که به یک کاربر، رایانه یا شبکه آسیب برساند، از قبیل ویروس‌ها، تروجان‌ها، کرم‌ها، اکسپلویت‌کیت‌ها، روت‌کیت‌ها و جاسوس‌افزارها در قالب یک بدافزار در نظر گرفته می‌شود.

با این‌که بدافزارها همواره در فرم‌های متفاوتی ظاهر می‌شوند، اما تکنیک‌های عمومی به منظور تحلیل آن‌ها مورد استفاده قرار می‌گیرد. شایان ذکر است، روش یا رویکردی که شما به منظور تحلیل بدافزارها انتخاب می‌کنید، کاملا به هدف شما بستگی دارد.

با این توضیحات، می‌توان گفت هدف از تحلیل بدافزار معمولا ارائه اطلاعاتی است که برای پاسخگویی به حمله بدافزارها به شبکه نیاز است. هدف متخصصین معمولا این است که مشخص کنند دقیقا چه اتفاقی افتاده است و اطمینان حاصل کنند تمامی فایل‌ها و ماشین‌های آلوده را شناسایی کرده‌اند.

هنگامی‌که یک فایل باینری مشکوک را تحلیل می‌کنند، باید مشخص سازند آن فایل باینری چه کاری دقیقا انجام می‌دهد، چگونه آن را در شبکه و سامانه‌عامل باید شناسایی کرد و چگونه باید میزان آسیب‌رسانی آن به سامانه‌ها را تخمین زد.

هنگامی‌که یک فایل مشکوک را شناسایی می‌کنید که به تحلیل کامل نیاز دارد تا هویت (سالم یا خراب بودن) آن تصدیق شود، می‌توانید برای جلوگیری موقت از فعالیت‌های آن نرم‌افزار یک سیگنیچر[1] تشخیص نفوذ در نرم‌افزارهایی مانند Yara برای آن تعریف کنید. این عمل باعث می‌شود موقتا از آلودگی سامانه‌ها به آن نرم‌افزار مشکوک جلوگیری به عمل آید.

در طول مطالعه این سلسله مقالات یاد خواهید گرفت، تحلیل بدافزار می‌تواند به منظور توسعه یک سیگنیچر مبتنی بر شبکه و یا یک سیگنیچر مبتنی بر میزبان[2] مورد استفاده قرار گیرد تا در نتیجه با استفاده از آن سیگنیچرها در ابزارهایی مانند Yara از آلودگی سامانه‌ها به آن بدافزار جلوگیری کرد.

---

[1] Signture
[2] Host-based and Network Signatures

سیگنیچرهای مبتنی بر میزبان

سیگنیچرهای مبتنی بر میزبان یا ایندیکِیتورها[1]، برای شناسایی برنامه‌های مخربی به کار گرفته می‌شود که در ماشین قربانی وجود دارند. این سیگنیچرها اغلب اوقات توسط تغییراتی که بدافزار در رجیستری یا ساختار سامانه‌عامل ایجاد می‌کنند، یا اطلاعات فایل باینری مانند هش MD5، هش SHA-1، استرینگ‌های درون فایل باینری و ... تعریف شده و مورد استفاده قرار می‌گیرند.

به عبارتی می‌توان اینطور تشریح کرد، ایندیکِیتورهای مبتنی بر میزبان، روی نحوه عملکرد بدافزار در سامانه‌عامل، و همچنین نوع ساختار باینری بدافزار تمرکز دارند، اگرچه که بدافزارها می‌توانند ساختار و همچنین استراتژی خود را تغییر دهند.

به همین دلیل اگر ما این ایندیکِیتورها را مبتنی بر ساختار و استراتژی عملکرد بدافزارها تعریف کنیم، نمی‌توانند برای ما به شکل قابل توجه‌ای ثمر بخش باشند. زیرا به راحتی توسعه‌دهندگان بدافزارها می‌توانند با ایجاد تغییر در ساختار بدافزار خود، سیگنیچرها و همچنین وقفه‌های دفاعی را دور بزنند.

سیگنیچرهای مبتنی بر شبکه

سیگنیچرهای مبتنی بر شبکه برای شناسایی بدافزارها با استفاده از مانیتورینگ ترافیک شبکه مورد استفاده قرار می‌گیرند. همچنین شایان ذکر است، سیگنیچرهای مبتنی بر شبکه می‌توانند بدون تحلیل باینری بدافزار ایجاد گردند. اما اگر سیگنیچرهای مبتنی بر شبکه با کمک تحلیل ساختار ارتباطی و همچنین خود باینری بدافزار ایجاد گردند، نرخ شناسایی[2] بالاتری را ارائه می‌دهند.

پس از تعریف سیگنیچرهای مبتنی بر شبکه، هدف نهایی این است که به شکل دقیق بررسی شود که بدافزار چگونه کار می‌کند. برای ایجاد این نوع سیگنیچرها باید فایل تعاملات بدافزار تحلیل شود، مثلا اینکه با چه سرورهایی ارتباط برقرار می‌کند؟ این سرورها دارای چه آدرس IP و چه شماره پورتی هستند؟ مبتنی بر چه پروتکلی بدافزار با سرورهای کنترل و فرماندهی خود ارتباط برقرار می‌کند؟ تمامی این اطلاعات می‌توانند در توسعه سیگنیچر مبتنی بر شبکه موثر باشند.

---

[1] Indicators
[2] Rate detection

تکنیک‌های تحلیل بدافزار

در اغلب اوقات، هنگامی‌که تحلیل بدافزاری را انجام می‌دهید، فقط فایل‌اجرایی آن را خواهید داشت که کد درون فایل باینری آن برای انسان‌ها قابل خواندن و درک نیست چون تشکیل شده از مجموعه متوالی از ۱ و ۰ است. اما این آخر ماجرا برای یک متخصص تحلیلگر بدافزار نخواهد بود. زیرا می‌توان برای درک بهتر کد بدافزار از ابزارها و برنامه‌های گوناگونی استفاده کرد که هر کدام از آن‌ها مقدار کمی از اطلاعات بدافزار را در اختیار قرار دهند.

اما عموما دو روش برای تحلیل بدافزارها وجود دارد که تمام متخصصین آن‌ها را با تکنیک‌های تحلیل استاتیک[۱] و دینامیک[۲] می‌شناسند (در مهندسی‌معکوس آن‌ها را تحلیل مرده[۳] و زنده[۴] می‌نامند).

در روش تحلیل استاتیک متخصصین بدون آن‌که بدافزار را اجرا کنند، فایل‌اجرایی بدافزار را مورد تحلیل قرار می‌دهند، اما در روش تحلیل دینامیک، متخصصین بدافزار را اجرا کرده و سپس آن را تحلیل می‌کنند. هر دو این تکنیک‌ها دارای دو سطح ساده و پیشرفته هستند، که در این قسمت آن‌ها را کاملا توصیف خواهیم کرد.

تحلیل استاتیک ساده[۵]

روش تحلیل استاتیک ساده، شامل آزمایش ساختار فایل باینری بدافزار بدون دیدن اینستراکشن‌های واقعی[۶] آن در محیط زمان اجرا یا Runtime می‌شود. این روش در برخی شرایط می‌تواند تایید کند یک نرم‌افزار مخرب است یا خیر و همچنین در مورد توانایی‌های آن اطلاعات کاملی به متخصصین ارائه بدهد. در اغلب مواقع با اطلاعات دریافتی از این روش، متخصصین می‌توانند به راحتی برای جلوگیری از پیش‌روی بدافزارها یک سیگنیچر ساده تولید کنند. مزیت این روش این است که به راحتی و با سرعت بالایی می‌تواند انجام گیرد. اما در مواقعی که بدافزار پیچیده باشد، این روش ناکار آمد خواهد بود و باعث می‌شود خصوصیات مهم بدافزار از دیدمان پنهان بماند.

---

[1] Static
[2] Dynamic
[3] Dead
[4] Live
[5] Basic Static Analysis
[6] Actual Instructions

روش تحلیل دینامیک ساده

در روش تحلیل دینامیک ساده، بدافزار را اجرا کرده و رفتار ارتباطی آن را به دقت روی سامانه‌عامل مورد بررسی قرار می‌دهیم تا بتوانیم آلودگی‌های ایجاد شده توسط آن بدافزار را رفع کنیم و یا برای جلوگیری از پیش‌روی بدافزار، برای آن یک سیگنیچر تعریف کنیم و یا هر دو این کارها را انجام بدهیم.

در هر صورت قبل از این‌که بدافزار را اجرا کنید، باید یک محیط آزمایشگاهی مجازی راه‌اندازی کرده تا به شما اجازه بدهد در یک محیط ایمن بدون این‌که خطر آسیب رسیدن به شبکه و یا سامانه‌عامل وجود داشته باشد، روی بدافزار در حال اجرا مطالعه کنید.

همانند روش تحلیل استاتیک ساده، روش تحلیل دینامیک ساده می‌تواند توسط اغلب افراد و متخصصین انجام بگیرد، بدون آنکه دانش عمیق برنامه‌نویسی داشته باشند. با این حال این روش هم نمی‌تواند برای تمامی بدافزارهای تولیدی مورد استفاده قرار گیرد و ممکن است خیلی از کاربردهای بدافزارهای پیچیده از دیدمان پنهان بماند.

روش تحلیل استاتیک پیشرفته

تحلیل استاتیک پیشرفته، شامل مهندسی‌معکوس اجزای درونی یک بدافزار می‌شود. متخصصین باید فایل باینری بدافزار را درون یک دیزاسمبلر[1] بارگذاری کنند و با دقت اینستراکشن‌های اسمبلی بدافزار را دنبال کنند تا متوجه شوند بدافزار چه کاری انجام می‌دهد. بنابراین تحلیل استاتیک بدافزار به متخصصین می‌گوید، دقیقا برنامه چه کاری انجام می‌دهد.

یادگیری روش تحلیل استاتیک پیشرفته نسبت به روش ساده آن کمی دشوارتر و سخت تر است. زیرا که شخص متخصص باید دارای دانش و مهارت‌های گوناگونی مانند، کار با دیزاسمبلرها، آشنایی با استراکچر کدهای برنامه‌نویسی و آشنایی با مفاهیم اینترنالز سامانه‌عامل و برنامه‌نویسی اسمبلی و سیستمی داشته باشد که در این سلسله مقالات یاد خواهید گرفت.

[1] Disassembler

روش تحلیل دینامیک پیشرفته

در روش تحلیل دینامیک پیشرفته، از یک دیباگر استفاده می‌کنیم تا بتوانیم وضعیت درونی قسمت‌های گوناگون فایل‌اجرایی یک بدافزار را در محیط Runtime مورد بررسی قرار بدهیم. روش تحلیل دینامیک پیشرفته یک راه دیگر برای استخراج جزییات دقیق بدافزار به متخصصین ارائه می‌دهد.

این تکنیک‌ها به منظور جمع‌آوری اطلاعات از فایل‌هایی که به سختی می‌توان از آن‌ها با استفاده از تکنیک‌های دیگر اطلاعات به‌دست آورد، بسیار سودمند هستند. به همین دلیل در این سلسله مقالات از روش تحلیل دینامیک و استاتیک پیشرفته بدافزار استفاده خواهیم کرد تا یک تحلیل کامل بر روی یک بدافزار انجام دهیم.

انواع بدافزارها

هنگامی‌که تحلیل یک بدافزار را انجام می‌دهید، درخواهید یافت که می‌توان سرعت تحلیل را با داشتن یک سری اطلاعات کلی و جزیی سرعت بخشید. به عنوان مثال، با حدس نوع عملیات بدافزارها به راحتی قادر خواهید بود بسیاری از اهداف آن بدافزار را شناسایی کنید و کار تحلیل خود را سرعت بخشید.

این را بخاطر بسپارید، هر نوع بدافزار یک عملیات خاص را انجام می‌دهد. البته هنگامی می‌توانید از این مزیت بهره‌مند شوید که با تمامی این گروه‌ها آشنا بوده باشید. به همین دلیل در ذیل یک نگاه کلی به گروه‌بندی این بدافزارها خواهیم کرد.

- **بک‌دور[1]:** بدافزارهایی که بر روی یک سامانه‌عامل نصب شده و به مهاجمان امکان دسترسی از راه دور به سامانه قربانی را ارائه می‌دهند، بک‌دور یا درپشتی گویند. بکدورها شرایطی را فراهم می‌آورند که مهاجمان می‌توانند به سامانه‌های قربانیان خود بدون هیچ اهرازهویتی[2] متصل شوند و مقاصد خود را روی سامانه‌عامل آنان اجرا کنند.

[1] Backdoor
[2] Authentication

- **باتنت[1]:** باتنت‌ها همانند بک‌دورها هستند، زیرا مانند بک‌دورها به مهاجمین اجازه می‌دهند که به سامانه قربانی دسترسی پیدا کنند، با این تفاوت‌که تمامی رایانه‌های آلوده به یک باتنت مشابه، یک فرمان را از مهاجم دریافت کرده و روی تمامی سامانه‌های آلوده اجرا می‌کنند.
- **دراپرها[2]:** کدهای‌مخربی که وظیفه آن‌ها دریافت یک فایل مخرب دیگر است، دراپر گویند. بدافزارهای دراپر، عموما هنگامی‌که مهاجمین دسترسی اولیه از سامانه هدف می‌گیرند، توسط مهاجمین بر روی سامانه‌های قربانیان نصب می‌شوند و بعدها می‌توانند از طریق آن‌ها روی سامانه قربانیان خود فایل نصب و اجرا کنند.
- **سرقت‌کننده اطلاعات[3]:** بدافزارهایی که از سامانه هدف اطلاعات جمع‌آوری کرده و آن اطلاعات را معمولا برای مهاجمین یا هکرها ارسال می‌کنند را سرقت‌کننده اطلاعات می‌نامند. به عنوان مثال، لیستنرها[4]، گرابر[5] رمزهای عبور هش شده و کیلاگر از این نوع خانواده هستند. این بدافزارها عموما برای دسترسی گرفتن به حساب‌های بانکی، حساب سایت‌های اجتماعی (فیسبوک، توئیتر، کلوب و...) و ایمیل‌ها به خدمت گرفته می‌شوند.
- **لانچرها[6]:** بدافزارهای نوع لانچر یا راه‌انداز برای اجرای بدافزارهای دیگر مورد استفاده قرار می‌گیرند. لانچرها اغلب از تکنیک‌های غیرسنتی برای اجرای بدافزارهای دیگر استفاده می‌کنند که با اجرای آن بدافزار موجب می‌شوند، دسترسی مهاجم بالاتر برود.
- **روت‌کیت[7]:** کدمخربی را که برای پنهان‌کردن یک کدمخرب دیگر طراحی شده باشد، روت‌کیت می‌گویند. روت‌کیت‌ها معمولا با دیگر نرم‌افزارهای مخرب به صورت زوج فعالیت می‌کنند. از قبیل بکدورها، که به مهاجمین اجازه دسترسی از راه‌دور به ماشین‌های قربانیان را ارائه می‌دهند. مهاجمین با استفاده از روت‌کیت‌ها می‌توانند شناسایی بکدورهای خود را سخت‌تر و گاهی اوقات غیر ممکن کنند.

---

[1] Botnet
[2] Droppers
[3] Information-stealing
[4] Listeners
[5] Grabber
[6] Launcher
[7] Rootkit

- **بوت‌کیت[1]:** بوت‌کیت، کد مخربی است که به درون Master Boot Record یک دیسک‌سخت تزریق می‌شود و اجازه می‌دهد بدافزار قبل از بارگذاری سامانه‌عامل اجرا شود و برخی از عملیات‌ها مانند غیرفعال‌سازی ویژگی امنیتی PatchGuard را انجام دهد. تشخیص این نوع بدافزارها به کار بسیار دشواری است.
- **اکسپلویت‌کیت[2]:** اکسپلویت‌کیت، یک کیت نرم‌افزاری است که به منظور اجرا بر روی یک وب سرور طراحی شده است که هدف از طراحی آن شناسایی آسیب‌پذیری‌های نرم‌افزاری در کلاینت‌هایی است که به آن متصل می‌شوند. بعد از اینکه این کیت نرم‌افزاری موفق به شناسایی آسیب‌پذیری بر روی سامانه کلاینت شد، اقدام به اکسپلویت آسیب‌پذیری می‌کند. بعد از اینکه آسیب‌پذیری به درستی اکسپلویت شد، بر روی سامانه مورد نفوذ قرار گرفته یک بدافزار بارگزاری خواهد کرد که هدف از بارگزاری آن بدافزار انجام کارهای مخربانه است.
- **ارسال‌کننده هرزنامه[3]:** بدافزارهایی که ماشین یک کاربر را آلوده کرده و سپس از آن برای ارسال هرزنامه استفاده می‌کنند، بدافزارهای ارسال کننده هرزنامه نامیده می‌شوند. این نوع بدافزارها به مهاجمین اجازه می‌دهند از طریق ارسال هرزنامه تبلیغات کنند یا بدافزارهای خودشان را بازنشر کنند.
- **کرم یا ویروس[4]:** به بدافزارهایی که می‌توانند خودشان را تاکثیر کنند و رایانه‌های دیگر را آلوده سازند را کرم یا ویروس می‌نامند.
- **باج‌افزارها[5]:** باج‌افزارها گونه‌ای از بدافزارهای رایانه‌ای هستند که دسترسی به سامانه را برای کاربران محدود می‌کنند و مهاجمین برای برداشتن محدودیت‌های اعمال شده بر روی سامانه قربانی درخواست باج (وجه نقد) می‌کنند.

با این حال بدافزارها همچنین می‌توانند بر مبنای انگیزه مهاجمین[6] در دو گروه تقسیم کرد. گروه اول این بدافزارها را در اصطلاح انگلیسی Mass می‌نامند. این نوع بدافزارها به گونه‌ای طراحی شده‌اند که روی

---

[1] Bootkit
[2] Exploitkits
[3] Spam-sending
[4] Worm or virus
[5] Ransomware
[6] Attacker's Objective

حداکثر ماشین‌ها بتواند تاثیر بگذارند و آن‌ها را مورد بهره‌برداری قرار بدهند. مانند بات‌نت‌ها و یا جاسوس‌افزارهای نظامی که جزوء این دسته هستند.

دسته دوم را بدافزارهای هدفمند[1] می‌نامند، مانند یک درپشتی که برای حمله به یک سازمان خاص طراحی شده است. بدافزارهای هدفمند تهدید بزرگتری نسبت به بدافزارهای جمعی به شمار می‌روند. زیرا که آن‌ها به صورت گسترده مورد استفاده قرار نمی‌گیرند و فقط هدفشان حمله به یک هدف خاص است. به همین دلیل احتمال زیادی وجود دارد که سامانه‌های دفاعی نتوانند آن‌ها را شناسایی کنند، زیرا تا به حال با آن بدافزار مواجه نشده‌اند و ساختار و نوع عملیات آن‌ها برایشان بی‌معنا و ایمن به نظر می‌رسد.

با قدرت می‌توان گفت، بدون تحلیل این نوع بدافزارها تقریبا غیرممکن است که بتوان از شبکه یا سامانه در برابر حمله آن‌ها محافظتی به عمل آورد. بدافزارهای هدفمند عموما خیلی پیچیده هستند و تحلیل آن‌ها نیاز به مهارت بالایی دارد.

نکته : یکی از این نوع بدافزارها که تا چند وقت پیش متخصصین ایرانی با آن درگیر بودند، جاسوس‌افزار استاکس‌نت بود. این جاسوس‌افزار توسط متخصصین اسرائیلی و آمریکایی با هدف منهدم ساختن سانتریفیوژهای نیروگاه اتمی ایران طراحی و عملیاتی شده بود.

این بدافزار با استفاده از یک اکسپلویت روزصفرم یا به عبارت دیگر 0Day خودش را در سطح سامانه‌های رایانه‌ای گسترش می‌داد و بعد از این‌که در هر سامانه نفوذ می‌کرد، بعد از بررسی سامانه مورد نفوذ، روی آن عملیات انجام می‌داد.

این بدافزار بطور مخصوصی برای آسیب رساندن به سامانه‌های زیر ساخت حیاطی و نیروگاه هسته‌ای ایران طراحی شده بود که خوشبختانه به موقع شناسایی و مهار شد و نتوانست اهداف خود را کاملا به سرانجام برساند.

---

[1] Targeted Malware

قوانین عمومی تحلیل بدافزار[1]

حال اجازه دهید با ذکر چند نکته که باید آن‌ها را در هنگام تحلیل مد نظر داشته باشیم این قسمت را به پایان برسانیم.

- **قانون اول:** اولین قانون تحلیل بدافزار شامل این نکته می‌شود "زیاد درگیر جزییات نشوید". اکثریت بدافزارهای تولیدی نسل فعلی بزرگ و بسیار پیچیده هستند و بعید است که یک شخص بتواند تمامی جزییات آن بدافزار را دریابد. با این حال فقط باید روی قابلیت‌های کلیدی آن بدافزار تمرکز کرد و هنگامی‌که تحلیل به بخش‌های پیچیده و دشوار رسید یک دید کلی گرفته و قبل از این‌که در مرداب سر درگمی قرار بگیرید خود را نجات دهید.
- **قانون دوم:** بخاطر بسپارید ابزارها و تکنیک‌های متفاوتی برای انجام کارهای گوناگون وجود دارند که دارای شباهت‌ها و قابلیت‌های مشابه‌ای با همدیگر هستند که باید تمامی آن‌ها را فرا بگیرید. در تحلیل بدافزار یک روش فقط وجود ندارد. هر موقعیت متفاوت است و باید از ابزارها و تکنیک‌های گوناگونی به منظور حل مسئله آن استفاده شود، تا ویژگی‌های آن بدافزار را شناسایی کنید. اگر با استفاده از یک ابزار به مقاصد خود نرسیده‌اید، از یک ابزار دیگر استفاده کنید. اگر در یک مسئله گیر افتادید زمان زیادی در آن صرف نکنید و تحلیل بدافزار را از یک زاویه دیگر آغاز یا یک روش دیگر اتخاذ کنید.
- **قانون سوم:** در نهایت، به یاد داشته باشید که تحلیل نرم‌افزارهای مخرب مانند یک بازی موش و گربه است. هنگامی‌که روش جدیدی در تحلیل بدافزار معرفی می‌شود، نویسندگان بدافزار روشی برای مقابله با آن ابداع می‌کنند. به عنوان یک فرد موفق در تحلیل بدافزارها، باید بتوانید آن‌ها را بشناسید، درک کنید و با آن تکنیک‌ها مقابله کنید.

[1] General Rules for Malware Analysis