آموزش امنیت اطلاعات قسمت ۴ : بدافزار چیست و معرفی انواع بدافزار (نسخه PDF)

در این سـری از مقالات شـما با مفهوم بدافزار یا Malware و همچنین انواع بـدافزارها و حملات مهندسـی اجتماعی یا Social Engineering آشـنا خواهید شد. در ادامه تفاوت بین ویروس و کرم (Virus and Worm) را متوجه خواهیـد شد ، کمی در خصوص بدافراهایی که تغییر شکل می دهند و خود را از شکلی به شکل دیگر تبدیل می کنند آشنا خواهید شد.

با انواع بدافزارهایی که برای رسیدن به اهداف مالی خود تلاش می کنند آشنا خواهید شد، با انواع ویروس ها و کرم های اینترنتی معروف آشـنا خواهیـد شد و در نهایت شـما می توانید انواع حملات مهندسـی اجتماعی یا حملاتی که بدون نیاز به دانش فنی انجام می شوند را شناسایی و روش های مقابله با آنها را یاد بگیرید.

حمله با استفاده از بدافزار

در ابتدا بایستی بررسـی کنیم که واژه بدافزار به چه معناست ؟ شـما با واژه نرم افزار یا Software ، سخت افزار یا Hardware آشنایی دارید اما بد افزار چیست ؟ بدافزارها یا Malware ها در واقع نرم افزارهایی هستند که برعکس یک نرم افزار عادی که نیاز ما را برطرف می کند و به مـا در جهت رسـیدن به اهـدافمان کمک می کنـد ، جهت تخریب یا سوء اسـتفاده از کاربران نوشـته شـده است ، قطعا یک بـدافزار در زیرمجموعه های یک نرم افزار قرار می گیرد ، با توجه به اینکه بد افزارها با اسـتفاده از روش های معمول برنامه نویسی و با استفاده از کد نویسی ایجاد می شوند بنابراین آنها کدهای مخرب یا سوء استفاده کنند هستند.

یک بدافزار چه می کند ؟ نرم افزارهای مخرب به نرم افزاری گفته می شود که در وهله اول بدون اینکه کاربر بداند بر روی سیستم قربانی یا هدف نصب و شـروع به فعالیت می کنند و ممکن است در بسـیاری مواقع کاربر از نصب شدن چنین نرم افزاری بر روی سیستم عامل خود اطلاع نداشـته باشد. اینگونه نرم افزارها انواع و اقسام تخریب ها و سوء اسـتفاده هایی را که فکر کنید را می توانند بر روی سیستم شما یا فرد قربانی انجام دهند .

هدف اصـلی بدافزارها را می توان به صورت کلی به سه دسـته تقسـیم کرد : آلوده سازی سیستم ها ، مخفی ماندن و رسیدن به مقاصد یا اهداف از پیش تعیین شده و در نهایت بدست آوردن سود و منفعتی که قصد رسیدن به آن را دارند. بصورت کلی تمامی انواع بدافزارهایی که شناسایی شده اند در سه دسته بندی کلی قرار می گیرند که به ترتیب زیر می باشند :

- بدافزارهایی که تکثیر (Spread) می شوند
- بدافزارهایی که مخفی (Conceal) می شوند
- بدافزارهایی که برای سازنده خود منفعت (Profits) دارند

بدافزارهایی که تکثیر می شوند !

منظور از منتشـر شـدن یعنی تکثیر شدن ، این نوع از بدافزارها به خودی می توانند از کدهای خود اسـتفاده کرده و مثل یک ویروس همه جـا را مبتلاـ کننـد. معروفترین نوع از این نوع بـدافزارها به نـام ویروس یـا بهتر بگوییم Computer Virus شنـاخته می شود. ویروس های کامپیوتری کـدهای مخربی هسـتند که خودشان را بر روی همان کامپیوتری که بر روی آن قرار گرفته اند تکثیر می کنند. این نوع از کدهای مخرب روش های متنوعی برای آلوده کردن فایل ها و سیسـتم دارنـد که هر کـدام را می توان بصورت جداگانه طبقه بندی کرد ، مهمترین روش های تکثیر ویروس ها به شکل زیر می باشد :

- **روش اضـافه کردن یا Appender :** در این روش ویروس خود را به انتهـای فایـل ها می چسـباند یا در اصـطلاح فنی خود را در انتهای فایل مورد نظر Append می کنـد.فایل اجرایی ویروس همـانطور که گفته شـد در انتهای فایل طعمه قرار می گیرد . اما همین مقدار کفایت نمی کند ، ویروس با اسـتفاده از تکنیک خاصی سه بایت ابتدای فایل آلوده را تغییر می دهد و در آن یک دستور پرش یا Jump به کـد اصـلی ویروس که در انتهای فایل قرار دارد ، قرار می دهـد . حال با اجرا شدن فایل مورد نظر ابتدا ویروس اجرا می شود و سپس فایل آلوده اجرا می شود.

- **روش آلوده سازی پنیر سوئیسی یا Swiss Cheese :** حتما شما هم با کارتون های تام و جری زندگی کرده اید ، اگر دقت کرده باشید پنیرهایی که در این کارتون معروف استفاده می شد دارای سوراخ هایی زیادی بود که برخی اوقات به قدری زیاد می شدند که جری به راحتی می توانست در داخل این سوراخ ها مخفی شود. به این نوع پنیر در اصطلاح پنیر سوئیسی گفته می شود. در روش آلوده سازی پنیر سوئیسـی ، ویروس ها کد خود را در درون کدهای فایل اجرایی تزریق می کنند . کد اصلی نرم افزار موجود در درون کدهای ویروس قرار می گیرد و بعد از اجرای فایل آلوده ابتدا ویروس اجرا شده و سپس فایل را اجرا خواهد کرد.

- **روش آلوده سازی شکافته شدن یا Split :** در این روش ویروس کدهای اجرایی خود را به چندین بخش تقسـیم می کند و این قطعه کـد هـا را بصورت تصـادفی در قسـمت های مختلف کـد اجرایی نرم افزار کاربردی مخفی می کنـد.نقطه شـروع فایل اجرایی ویروس در ابتدای فایل قرار می گیرد و برای کنترل کردن سایر قسمت های کد مخربی استفاده می شود که در فایل تقسیم شده اند ، با اجرا شدن فایل ، ابتدا کد کنترلری ویروس اجرا شده و قطعات را به هم می چسباند و کد مخرب اجرا می شود.

زمانی که نرم افزار آلوده شده با کد ویروس اجرا می شود ، ویروس خود را با چسـباندن و گسترش دادن به سایر فایل های موجود بر روی همان کامپیوتر تکثیر می کند و سـپس کد مخرب خود را به سرعت فعال می کند . معمولا ویروس ها بعد از اجرا شدن بر روی سیستم ها اثراتی از خود نشان می دهند برای مثال یک پیام تهدید آمیز یا اطلاع رسانی برای کاربر نمایش می دهند. البته این موضوع کاملا به نوع ویروسی که بر روی کامپیوتر اجرا می شود وابستگی دارد و هر کدام از آنها تخریبی از نوع خود را انجام می دهند.

برخی از ویروس ها باعث Crash کردن یا هنگ گردن سیسـتم می شوند ، برخی هارد درایو شـما را فرمت می کنند و یا فایل های شما را حذف می کنند ، برخی دیگر تنظیمات و تهمیدات امنیتی انجام شده بر روی سیستم عامل شما را عوض می کنند و بسیاری از موارد مشابه دیگر. نکته بسـیار مهم در خصوص ویروس ها این است که آنها نمی تواننـد بصورت خودکار از کامپیوتری به کامپیوتری دیگر تکثیر شوند ، انتشار ویروس کاملا به فعالیت هایی دارد که کاربر با آن انجام می دهد ، ویروس ها به فایل ها متصل می شوندو تنها با اسـتفاده از انتقال فایل آلوده است که کامپیوتر دیگری نیز آلوده می شود.

ویروس ها از نظر نوع کاری که بر روی سیسـتم عامل انجام می دهنـد به انواع و اقسام مختلفی طبقه بنـدی می شونـد که از آن جمله می توان به ویروس های نرم افزاری که به فایل اجرایی نرم افزارها متصل می شونـد ، ویروس های ماکرو که یک اسـکریپت را اجرا می کننـد ، ویروس های رزیدنت که با باز کردن فایل ها و یا سیستم عامل شروع به فعالیت می کنند ، ویروسهای بوت که قسمت Master Boot Record یا MBR سیسـتم را دچـار اختلاـل می کننـد ، ویروس های رترو که دیتابیس آنتی ویروس ها را مورد هجوم قرار می دهنـد اشاره کرد ، در صورت نیاز به اطلاعات بیشتر می توانید به مقاله زیر مراجعه کنید :

- معرفی انواع ویروس های کامپیوتری

اما نوع دیگری از کدهای مخرب تکثیر شونده وجود دارد که به نام کرم یا Worm شناخته می شود. تفاوت این نوع برنامه مخرب با ویروس ها در این است که این نوع کد مخرب می تواند از نقاط ضـعف موجود بر روی نرم افزارهای کاربردی و سیستم عامل ها برای سوء استفاده و رسـیدن به اهـداف خود اسـتفاده کند. این نوع کد مخرب می تواند بدون نیاز به فایل میزبان خود را توسط شـبکه تکثیر کرده و در یک

شبکه بزرگ تکثیر شود.

Worm ها می توانند منابع سیستم را تا حد زیادی استفاده کنند و از ترافیک زیادی را در شبکه شما ایجاد کنند ، Worm ها نیز می توانند همانند ویروس ها هر گونه تخریبی که نویسنده آن مد نظر داشته باشد را بر روی سیستم شما انجام دهند ، از جمله اینکه می توانند فایل های شما را حذف کرده و یا اینکه دسترسی از راه دور را برای مهاجم به کامپیوتر شما فراهم کنند.

بدافزارهایی که مخفی می شوند !

ویروس ها هم ممکن است سعی کنند خود را از دید کاربر پنهان کنند اما برخی از بدافزارها وجود دارند که بصورت ویژه ای طراحی شده اند تا کارهای خود را بصورت مخفی انجام دهند. تروجان ها یا اسب های ترو ا ، Rootkit ها ، Backdoor ها و Logic Bomb ها از انواع این نوع کدهای مخرب هستند. تروجان یا اسب تروا نرم افزار مخربی است که خود را به جای یک نرم افزار سالم و کاربردی جا می زند و کاربر فریب خورده و آن را اجرا و نصب می کند.

اینگونه کدهای مخرب به نرم افزارهای کاربردی مفید متصل می شوند و کدهای خود را مخفی می کنند ، به محض اجرا نرم افزار مربوطه این کد مخرب نیز خود را اجرا کرده و به سیستم عامل حمله می کند. برخی اوقات تروجان ها می توانند خود را به عنوان فایل داده یا فایل اطلاعات نیز معرفی کنند. تروجان ها معمولا خود را به عنوان نرم افزارهای کاربردی رایگان در اینترنت معرفی می کنند ، نمونه بارزی از تبلیغات در اینترنت را می توانید به این روش مشاهده کنید ، برای مثال تبلیغی مثل نرم افزار دانلود رایگان می تواند مستعد وجود یک تروجان در این نرم افزار باشد. معمولا کاربرد تروجان ها معمولا اسکن کردن سیستم برای بدست آوردن اطلاعات شخصی و شماره کارت های اعتباری و رمزهای عبور و انتقال این اطلاعات به مهاجم می باشد.

RootKit چیست ؟

Rootkit ها از انوع دیگر کدهای مخرب مخفی شونده هستند ، این نوع از کدهای مخرب تا حدود زیادی ساختار کاریشان مشابه ساختار کاری تروجان ها و Backdoor ها می باشد با این تفاوت که کدهای خود را با کدهای سیستم عامل ترکیب می کنند و در برخی اوقات فایل های خود را جایگزین فایل های سیستم عامل می کنند ، این نرم افزارها می توانند فعالیت هایی که هکر انجام می دهد را براحتی مخفی کرده و عملیات های تخریبی خود را انجام دهند زیرا سیستم عامل به آنها شکی نمی برد.

این نوع بدافزار تمامی لاگ های سیستم و یا رکوردهای مورد نظر مهاجم را می تواند حذف کند و بصورت ویژه برای مخفی نگاه داشتن فعالیت های یک هکر مورد استفاده قرار می گیرد. با توجه به اینکه این نوع بدافزارها می توانند خود را جایگزین فایل های سیستمی کنند بنابراین شناسایی آنها بسیار بسیار دشوار است و همیشه برای راه درمان پیشنهاد می شود که از راهکارهای SIV استفاده شود. Rootkit ها در درجه اول مخفی کاری در میان بدافزارها قرار می گیرند. سریعتری راهکار برای از بین بردن Rootkit ها نصب مجدد سیستم عامل یا فرمت کردن کامل هارد دیسک کامپیوتر می باشد.

Logic Bomb و Backdoor ها چه هستند ؟

Logic Bomb یا بمب های منطقی بدافزارهایی هستند که ممکن است چندین ماه یا حتی سال بدون انجام هیچگونه عملیات خاصی بر روی سیستم عامل هدف وجود داشته باشند و ساکت باقی بمانند. اینگونه بدافزارها به انجام شدن عملیات یا حرکت خاصی بر روی سیستم عامل توسط کاربر یا خود سیستم حساس هستند و به محض وقوع آن اتفاق شروع به فعالیت و اجرا خواهند کرد.

شناسایی اینگونه بدافزارها قبل از اجرا بسیار سخت است زیرا عملی انجام نداده اند که بتوان از طریق آن ، آنها را شناسایی کرد. نوع دیگری از بدافزارها وجود دارد که بنام درب پشتی یا Backdoor شناخته می شوند ، این نوع از بدافزارها معمولا از نقاط ضعفی استفاده می کنند که برنامه نویس ها برای وارد کردن یا بروز کردن نرم افزارهای خود از آنها استفاده می کنند. برای مثلا یک برنامه نویس تا عرضه کردن نسخه نهایی نرم افزار خود چندین نسخه آزمایش ارائه می کند که در هر کدام از آنها برای اینکه بتواند در مراحل بعدی کد جدید را

براحتی وارد کنـد و نرم افزار را بروز کنـد یک راه مخفی تعبیه می کنـد ، همین راه مخفی دقیقا چیزی است که مهاجم به ان نیاز دارد و به آن Backdoor گفته می شود. Backdoor ها تمهیدات امنیتی اصـلی نرم افزارها را دور می زنند. توجه کنید که برنامه نویس قصد دارد تا در نسخه نهایی این Backdoor را حذف کند اما ...

بدافزارهایی که برای سازنده خود سود دارند !

برخی از بدافزارها وجود دارد که بصورت ویژه برای سود رسانی به مهاجمین ایجاد شده اند. از انواع این بدافزارها می توان به Botnet ها ، Spywareها ، Adware ها و KeyLogger ها اشاره کرد.شاید در این میان ساختار Botnet ها از همه چیز جالبتر باشـد ، در ساختار Botnet ها یک یا چند کامپیوتر توسط یک نرم افزار مخرب یا همان بدافزار آلوده می شود به گونه ای که این سیسـتم در آینده تابع دستوراتی خواهد بود که از طرف کـامپیوتر مهاجمین صادر می شود. معمولا کاربرد Botnet ها در انتشار ویروس ها ، Worm ها و Trojan ها بسیار محسوس است ، به کامپیوتر آلوده شـده در این شـبکه در اصـطلاح فنی مرده متحرک یا Zombie گفته می شـود. در واقع مجموعه ای از Zombie ها هستند که تشکیل یک Botnet را می دهند.

در گذشته مهاجمینی که از Botnet ها استفاده می کردند از شبکه های چت آنلاینت یا همان IM ها استفاده زیادی می کردند و براحتی می توانستند Zombie ها را کنترل کننـد.اما امروزه از پروتکل های دیگری ماننـد HTTP هم اسـتفاده می شود. اما ممکن است از خود سـئوال کنیم که کاربرد یا مزیت وجود Botnet ها برای هکرها یا مهاجمین چیست ؟ در ابتدا توجه کنید که این شبکه در پس زمینه یا Background وجود دارد و Zombie ها از وجود چنین شـبکه هایی بی خبر هسـتند و این بزرگترین مزیت برای مهاجمین می باشـد تا به اهداف بعدی خود برسند .

این شـبکه ها می تواننـد تا چنـدین سال بر روی سیسـتم کلاینت فعالیت کننـد بدون اینکه ردی از خودشان به جای بگذارند ، مهاجم می توانـد از این شـبکه برای بالا بردن آمار بازدید وب سایت ها ، ارسال اسـپم و ایمیل های تبلیغاتی ، انجام حملات DDOS بر روی سرورهای قربانی و بسیاری دیگر از اینگونه اهداف استفاده کند.

Spyware یا جاسوس افزار چیست ؟

Spyware مخفف کلمه Spy و Software می باشد و همانطور که از معنی کلمات پیدا است به معنای نرم افزار جاسوسـی می باشد. اینگونه نرم افزارها بـدون اطلاع کاربر اطلاعاتی در خصوص کاربر یا هر چیزی که می تواننـد را بـدست آورده و برای مهاجم ارسال می کنند. کاربرد Spyware ها معمولا در زمینه های تبلیغات ، جمع آوری اطلاعات شخصی و اعمال تغییرات بر روی کامپیوترها می باشد .

Spyware ها علاوه بر موارد ذکر شـده یک سـری تاثیرات منفی نیز بر روی سیسـتم قربانی دارنـد که از آن جمله می توان به پایین آمـدن کارایی سیسـتم ، کم شـدن ثبات نرم افزار ها ، اضافه شـدن و نصب شـدن Toolbar هـای عجیب و غریب بر روی مرورگرها ، ایجاد شـدن Shortcut های عجیب بر روی سیستم ، عوض شدن صفحه Home Page مرورگرها و باز شدن صفحات Pop-up اشاره کرد.

Adware یا تبلیغات افزار چیست ؟

Adware مخفف کلمات Advertisement یا تبلیغات و Software یا نرم افزار می باشد . اینگونه بدافزارها بر روی سیسـتم های هدف تبلیغات ناخواسـته ایجاد می کنند. معمولا تبلیغات این بدافزار به شـکل نمایش بنر ها و یا صفحات Pop-Up می باشد و در برخی اوقات صـفحات اینترنتی را مرتب و پشت سر هم باز می کنند .

یکی از کارهایی که Adware ها می تواننـد انجام دهنـد دنبال کردن فعالیت هایی است که کاربر بر روی سیسـتم انجام می دهد ، به ویژه

فعـالیت های آنلاینی که توسط شـخص انجام می شود. اینگونه بـدافزارها واقعا می توانـد کاربران را عصبی و ناراحت کنـد و همچنین می توانند سیستم کاربر را به اندازه زیادی کند کنند و از فعالیت عادی کاربر جلوگیری کنند.

Keylogger چیست ؟

Keyloggey از دو کلمه Keyboard و Logger تشـکیل شدن است و بدافزاری است که کلیه کلید هایی که کاربر بر روی کیبورد خود فشار می دهد را در قالب یک فایل ذخیره می کند. این اطلاعات بعد ها می تواند برای مهاجم ارسال شود و توسط وی مورد استفاده قرار بگیرد ، در اسـتفاده از این نوع بدافزارها معمولا مهاجم به دنبال اطلاعات قابل اسـتفاده و مفیدی از جمله رمزهای عبور ، اطلاعات و شماره های کارت های اعتباری ، اطلاعات شخصـی و ... می باشد. توجه کنید که Keylogger ها می توانند در قالب سـخت افزار نیز وجود داشته باشند که در انتهای کیبورد شما متصل شده و اطلاعات را ثبت و ضبط می کنند ، این اطلاعات بعد ها می تواند توسط هکر مورد استفاده قرار بگیرد.

نتیجه گیری

در این مقاله شـما با واژه بـدافزار و انواع آن از لحاظ روش های تکثیر و عملکرد آشـنا شدید ، با مهمترین تکنیک هایی که بدافزارها برای سوء اسـتفاده از کاربران اسـتفاده می کنند آشنا شدید و در این لحظه دیگر قادر هستید بین بدافزارهای مختلف تفکیک قائل شوید ، شاید قبل از خواندن این مقاله همه انواع بدافزار را به عنوان ویروس می شـناختید اما از این به بعد تفاوت هرکدام را به درستی درک می کنید ، در ادامه این سـری مقالاـت شـما در مقـاله بعـدی با مبحث حملات مهندسـی اجتماعی یا Social Engineering آشـنا خواهید شد. **ITPro باشید.**

نویسنده : محمد نصیری

منبع: جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

#معرفي_انواع_بدافزار #انواع_backdoor# #Malware_چیست #keylogger_چیست #انواع_ویروس #rootkit_چیست
#spyware_یا_جاسوس_افزار_چیست #logic_bomb_چیست #بدافزار_یا_MalWare_چیست_؟ #انواع_کدهای_مخرب

مطلب اصلی