
بسم الله الرحمن الرحيم

دانشگاه ازاد اسلامی واحد تهران مرکز

ساختمان فنی و مهندسی هاشمی رفسنجانی

گروه کامپیوتر

بدافزار ها

نام درس: روش پژوهش و ارائه

نام استاد: استاد مریم افشاری

گردآورنده: مهدی هادی

بهار ۱۴۰۰

فهرست مطالب

تاریخچه طور

اولین چیزی که بعد از شنیدن کلمه بدافزار به ذهن خیلی هامون خطور می‌کنه ویروس ها هستند. جالبه بدونید اولین ویروس Creeper بود که در اوایل دهه‌ی ۱۹۷۰،یعنی ده سال پیش از اینکه لئونارد آدلمن، دانشمند کامپیوتر آمریکایی، این بدافزارهای خبیث را «ویروس کامپیوتری» نام‌گذاری کند، خودش را نشان داد. ویروس Creeper در سیستم عامل Tenex ظاهر شد و با انتقال از سیستمی به سیستم دیگر، این پیام را نمایش می‌داد: «من کریپرم: اگر می‌توانی من را گیر بیانداز!» این ویروس وقتی دستگاه جدیدی برای آلوده کردن پیدا می‌کرد، از سیستم قبلی حذف می شد؛ چون قادر به آلوده کردن چندین دستگاه به‌طور هم‌زمان نبود. کریپر فقط به قصد آزار و اذیت طراحی شده بود و کارکرد دیگری نداشت؛ اما اولین نرم‌افزاری بود که رفتاری مشابه بدافزار داشت.

مقدمه

برنامه های کامپیوتری که معمولا کاربر را اذیت میکنند یا خسارتی بجای میآورند میگویند به طور کلی هر برنامه که هدف بداندیشانه ای داشته باشد و برای آلوده کردن و آسیب رساندن به سیستم میزبان نوشته شده است را بدافزار میگویند . واژه بدافزار(malware) مخفف کلمات نرم افزار بداندیش (software malicious) است.

بدافزار ها از نظر هدف به سه دسته تقسیم می‌شوند:

❖ **بدافزارهایی که تکثیر (Spread) می شوند:**

این نوع از بدافزارها به خودی می توانند از کدهای خود اســـتفاده کرده و مثل یک ویروس همه جا را مبتلا کنند. کدهای مخربی هستند 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 ســیســـتم دارند که هر کدام را می توان بصـورت جداگانه طبقه بندی کرد ، مهمترین روش های تکثیر ویروس ها به شکل زیر می باشد.

- Appending:

- در این روش ویروس خود را به انتهای فایل ها می چســـباند یا در اصـــطلاح فنی خود را در انتهای فایل مورد نظر Append می کند. فایل اجرایی ویروس همانطور که گفته شد در انتهای فایل طعمه قرار می گیرد . اما همین مقدار کفایت نمی کند ، ویروس با استفاده از تکنیک خاصی سه بایت ابتدای فایل آلوده را تغییر می دهد و در آن یک دستور پرش یا Jump به کد اصلی ویروس که در انتهای فایل قرار دارد ، قرار می دهد . حال با اجرا شـــدن فایل مورد نظر ابتدا ویروس اجرا می شود و سپس فایل آلوده اجرا می شود.

- Swiss cheese:

- حتما شـــما هم با کارتون های تام و جری زندگی کرده اید ، اگر دقت کرده باشـــید پنیرهایی که در این کارتون معروف اســـتفاده می شـــد دارای ســـوراخ 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 سوئیسی ، ویروس ها کد خود را در درون کدهای فایل اجرایی تزریق می کنند . کد اصـــلی نرم

افزار موجود در درون کد های ویروس قرار می گیرد و بعد از اجرای فا یل آلوده ابتدا ویروس اجرا شده و سپس فایل را اجرا خواهد کرد.

- Split:

- در این روش ویروس کدهای اجرایی خود را به چندین بخش تقسیم می کند و این قطعه کد ها را بصـورت تصـادفی در قسـمت های مختلف کد اجرایی نرم افزار کاربردی مخفی می کند.نقطه شـروع فایل اجرایی ویروس در ابتدای فایل قرار می گیرد و برای کنترل کردن سایر ق سمت های کد مخربی ا ستفاده می شـود که در فایل تقسـیم شـده اند ، با اجرا شـدن فایل ، ابتدا کد کنترلری ویروس اجرا شده و قطعات را به هم می چسباند و کد مخرب اجرا می شود.

- Computer Viruses:

- زمانی که نرم افزار آلوده شده با کد ویروس اجرا می شود ، ویروس خود را با چسباندن و گسترش دادن به سایر فایل های موجود بر روی همان کامپیوتر تکثیر می کند و سـپس کد مخرب خود را به سـرعت 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 ر سانی برای کاربر نمایش می دهند. البته این موضـوع کاملا به نوع ویروسـی که بر روی کامپیوتر اجرا می شـود 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 سیستم می شوند ، برخی هارد درایو شـما را فرمت می کنند و یا فایل های شـما را حذف می کنند ، برخی دیگر تنظیمات و تهمیدات امنیتی انجام شده بر روی سیستم عامل شـما را عوض می کنند. نکته بسـیار مهم در خصـوص ویروس ها این اسـت که آنها نمی توانند بصـورت 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 استفاده از انتقال فایل آلوده است که کامپیوتر دیگری نیز آلوده می شود.

- Worms:
  - تفاوت این نوع برنامه مخرب با ویروس ها در این است که این نوع کد مخرب می تواند از نقاط ضعف موجود بر روی نرم افزارهای کاربردی و سیستم عامل ها برای سوء استفاده و رسیدن به اهداف خود استفاده کند. این نوع کد مخرب می تواند بدون نیاز به فایل میزبان خود را توسط شبکه تکثیر کرده و در یک شبکه بزرگ تکثیر شود.

❖ **بدافزارهایی که مخفی (Conceal) می شوند:**

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. 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.

- Rootkit:
  - 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.

- Backdoor:

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

- 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 خا صی بر روی سیستم عامل تو سط کاربر یا خود سیستم حساس هستند و به محض وقوع آن اتفاق شروع به فعالیت و اجرا خواهند کرد. شنا سایی اینگونه بدافزارها قبل از اجرا بسیار سخت ا ست زیرا عملی انجام نداده اند که بتوان از طریق آن ، آنها را شناسایی کرد.

- Trojan Horses:

  - 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.

❖ **بدافزارهایی که برای سازنده خود منفعت (Profits) دارند:**

برخی از بدافزارها وجود دارد که بصورت ویژه برای سود رسانی به مهاجمین ایجاد شده اند.

- Botnet:

  - در ساختار Botnet ها یک یا چند کامپیوتر توسط یک نرم افزار مخرب یا همان بدافزار آلوده می شود به گونه ای که این سیستم در آینده تابع دستوراتی خواهد بود که از طرف کامپیوتر مهاجمین صادر می شود. معمولا کاربرد Botnet ها در انتشار ویروس ها ، Worm ها و Trojan ها بسیار

محسوس است ، به کامپیوتر آلوده شده در این شبکه در اصطلاح فنی مرده متحرک یا Zombie گفته می شـــود. در واقع مجموعه ای از Zombie ها هستند که تشکیل یک Botnet را می دهند.

- Adware:
  - Adware مخفف کلمات Advertisement یا تبلیغات و Software یا نرم افزار می باشـــد . اینگونه بدافزارها بر روی ســـیســـتم های هدف تبلیغات ناخواسته ایجاد می کنند. معمولا تبلیغات این بدافزار به شکل نمایش بنر ها و یا صـــفحات Pop-Up می باشـــد و در برخی اوقات صـــفحات اینترنتی را مرتب و پشـــت ســـر هم باز می کنند. یکی از کارهایی که Adware ها می توانند انجام دهند دنبال کردن فعالیت هایی است که کاربر بر روی سیستم انجام می دهد ، به ویژه فعالیت های آنلاینی که توســـط شـــخص انجام می شـــود. اینگونه بدافزارها واقعا می تواند کاربران را عصـــبی و ناراحت کند و همچنین می توانند ســـیســـتم کاربر را به اندازه زیادی کند کنند و از فعالیت عادی کاربر جلوگیری کنند.

- Spyware
  - Spyware مخفف کلمه Spy و Software می باشـــد و همانطور که از معنی کلمات پیدا است به معنای نرم افزار جاسوسی می باشد. اینگونه نرم افزارها بدون اطلاع کاربر اطلاعاتی در خصـــوص کاربر یا هر چیزی که می توانند را بدست آورده و برای مهاجم ارسال می کنند. کاربرد Spyware ها معمولا در زمینه های تبلیغات ، جمع آوری اطلاعات شـــخصـــی و اعمال تغییرات بر روی کامپیوترها می باشـــد. Spyware ها علاوه بر موارد ذکر شده یک سری تاثیرات منفی نیز بر روی سیستم قربانی دارند که از آن جمله می توان به پایین آمدن کارایی سیستم ، کم شدن ثبات نرم افزار ها ، اضافه

شدن و نصب شدن Toolbar های عجیب و غریب بر روی مرورگرها ، ایجاد شدن Shortcut های عجیب بر روی سیستم ، عوض شدن صفحه Home Page مرورگرها و باز شدن صفحات Pop-up اشاره کرد.

- Keylogger:

- Keylogger از دو کلمه Keyboard و Logger تشکیل 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 استفاده از این نوع بدافزارها معمولا مهاجم به دنبال اطلاعات قابل استفاده و مفیدی از جمله رمزهای عبور ، اطلاعات و شماره های کارت های اعتباری ، اطلاعات شخصی و ... می باشد. توجه کنید که Keylogger ها می توانند در قالب سخت 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.

منابع

- **security.tosinso.com**
- **cert.ir/news/entry/7493**
- **Ben roont,2011,malware is posing increasing danger, the wallstreet journal**
- **F-Secure Quarterly Security Wrap-up for the first quarter of 2008Asdfas**
- **Mary landesman.2008.malwarerevolation:achange integrated microsoft security research and response**
- **Eagle, M. S,A Survey on Automated Dynamic Malware-Analysis. ACM Computer, 42(۲۰۱۲) ,**
- **En.wikipedia.org/malware**
- **K. Mathur, S.H. ,A Survey on Techniques in Detection and Analyzing Malware Executables, Advanced Research in Computer Science and Software Engineering.(۲۰۱۳) ,**
- **M. Sain, A.P,H.L. Survey on malware evasion techniques: state of the art and challenges.(۲۰۱۲) ,**
- **G. Tahan, L.R.Y. Automatic Malware Detection Using Common Segment Analysis**