بسمه تعالی

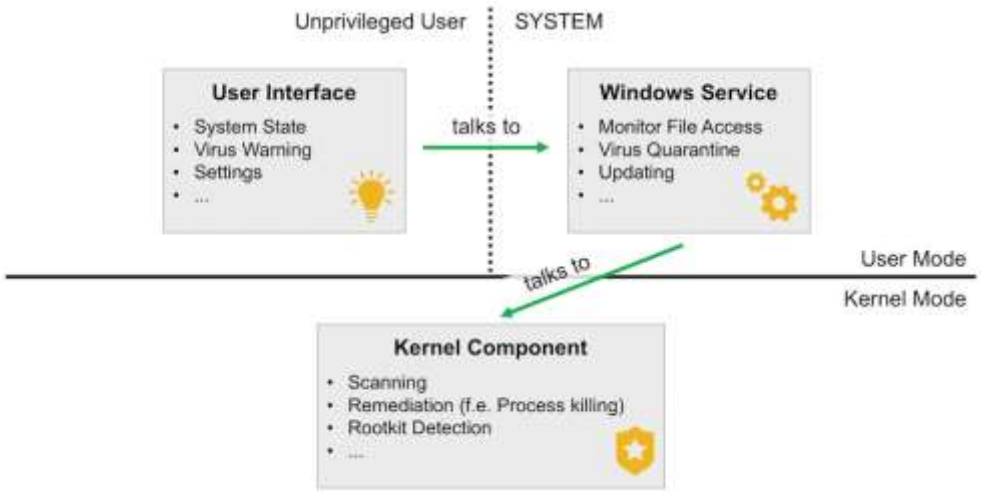
اجرای بدافزار با سطح دسترسی بالاتر با استفاده از فایلهای قرنطینه شده توسط آنتی ویروسها

به تازگی روشی توسط محققان امنیت سایبری کشف شده است که می توان سطح دسترسی در سیستم عامل ویندوز را توسط سوء استفاده از فایلهای قرنطینه شده در آنتی ویروسها، بالاتر برد که این روش بر روی اکثر برنامه های آنتی ویروس جوابگو می باشد. این آسیب پذیری که در نهایت دسترسی Full Access را به نفوذگر می دهد، توسط بازگردانی فایلهای قرنطینه شده توسط آنتی ویروسها می باشد که این دسترسی بر روی سیستم های End Point صورت می گیرد.

آقای Florian Bogner که این آسیب پذیری و روش استفاده از آن را کشف کرده است، نام #AVGater را انتخاب کرده است. حالا چرا؟؟؟ خدا داند...

در ابتدا نگاه کوچکی به انواع حالات دسترسی نرم افزار Antivirus ها در سیستم عامل می اندازیم. همانطور که در دیاگرام زیر مشاهده می فرمائید، نرم افزار آنتی ویروس در سه حالت زیر دارای دسترسی های مختلف می باشند:

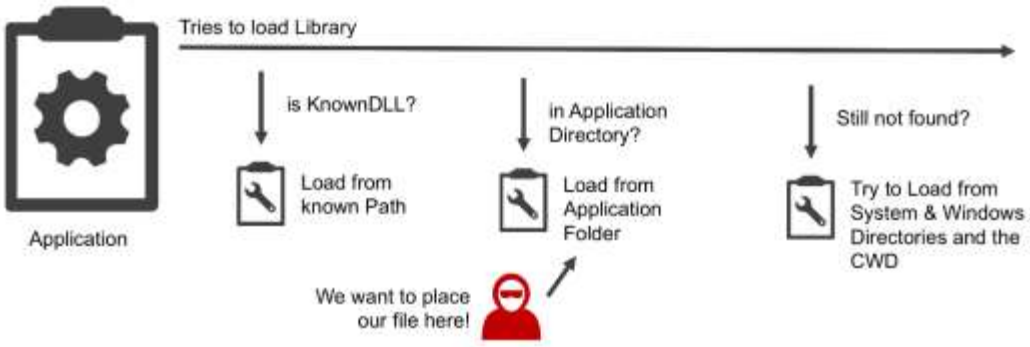
- The kernel mode
- The privileged user mode (SYSTEM)
- The unprivileged user mode



در دیاگرام بالا تفاوت این سه حالت دسترسی را مشاهده می فرمائید. همانطور که می بینید در حالت دسترسی unprivileged user mode می بینیم که به Interface برنامه AV دسترسی داریم. در این حالت هیچ گونه قدرتی در دست نفوذگر قرار ندارد، چراکه محدودیت های بسیاری برای user mode در سیستم عامل تعیین شده است. اما می توان با استفاده ارتباط با سرویس هایی که آنتی ویروس بر روی سیستم عامل نصب و اجرا می کند(AV Windows service)، عملکردهایی با سطح دسترسی بالاتری را هم انجام داد که در حالت user mode امکان انجام آنها وجود ندارد؛ به عنوان نمونه می توان فایلهای قرنطینه شده توسط Antivirus را بازیابی کرد. البته می دانیم که این کار توسط kernel component ها صورت می گیرد که این کمپوننت ها برای چک کردن و تشخیص بدافزارها هم مورد استفاده قرار می گیرد.

حال نکته اینجاست که اگر بتوان مرزهای محدودیت دسترسی را توسط دستکاری های خاصی تغییر داد، همچون عملیات هایی مانند Privilege Escalation ، آنگاه می توانیم با سطح دسترسی بالاتری، عملیات تخریبی خود را انجام دهیم. می توان این بالاتر بردن سطح دسترسی را با استفاده از دستکاری پروسه بازآوری فایل های قرنطینه شده در Antivirus ها انجام داد.

توسط روش #AVGater می توان فایل های قرنطینه شده توسط AV را به هر بخش از آدرس File system که بخواهیم بازگردانی کنیم. این کار به این دلیل امکان پذیر می باشد که در بیشتر مواقع پروسه بازگردانی فایل، با سطح دسترسی AV Windows service انجام می گیرد. اما در برخی مواقع این دسترسی توسط ACL ها گیر انداخته می شود و به مشکل بر می خورد. این نوع از آسیب پذیری که بیشتر با نام آسیب پذیری Privileged File Write نامیده می شود این امکان را می دهد که فایل DLL آلوده را در هر جایی از سیستم که بخواهیم قرار دهیم. اگر این امکان به صورت صحیح اتفاق بیافتد، امکان اجرای کدهای آلوده دلخواه بر روی سیستم قربانی امکان پذیر می شود. در تصویر زیر می بینید که در چه حالتی این موضوع اتفاق می افتد:



حال سوالی که پیش می آید این است که چگونه می توان این اجرای کد را به پروسه بازگردانی فایل متصل کرد؟ راه حل این موضوع، استفاده از NTFS directory junctions می باشد. توسط این قابلیت می توان یک لینک به صورت سمبولیک به Directory مورد نظر خود ایجاد کنیم که این کار توسط هر سطح دسترسی در سیستم عامل امکان پذیر بوده و توسط ابزار mklink در سیستم عامل ویندوز قابل انجام می باشد.

Mklink

Updated: April 17, 2012

Applies To: Windows Vista, Windows Server 2008, Windows Server 2012, Windows 8

Creates a symbolic link.

For examples of how to use this command, see Examples.

Syntax

```
mklink [[/d] | [/h] | [/j]] <Link> <Target>
```

Parameters

Parameter	Description
/d	Creates a directory symbolic link. By default, **mklink** creates a file symbolic link.
/h	Creates a hard link instead of a symbolic link.
/j	Creates a Directory Junction.
<Link>	Specifies the name of the symbolic link that is being created.
<Target>	Specifies the path (relative or absolute) that the new symbolic link refers to.
/?	Displays help at the command prompt.

در حالت کلی می توان گفت توسط سوء استفاده از قابلیت NTFS directory junctions در سیستم فایل NTFS، می توان پروسه بازگردانی فایلهای قرنطینه شده توسط AV را دستکاری کرده و فایل مخرب اجرایی مورد نظر را در هر آدرسی که بخواهیم قرار دهیم.

حال می توانیم با استفاده از اطلاعات فوق، سناریو حمله را آماده کنیم. در ابتدا library آلوده توسط AV شناسایی و به بخش قرنطینه انتقال داده می شود. سپس با سوء استفاده از قابلیت directory junctions آدرس directory که بدافزار ما شناسایی شده را به آدرس دیگری تغییر می دهیم که می توان به شاخه هایی همچون C:\Program Files و یا C:\Windows تغییر داد. با بازگردانی فایل از قرنطینه، فایل آلوده به شاخه ای بازگردانده می شود که در حالت عادی کاربر با سطح دسترسی پایین، امکان write کردن فایل را در آن ندارد. این کار توسط دسترسی سطح SYSTEM انجام می گیرد که AV service توسط آن می تواند کار write کردن فایل در شاخه ی دلخواه را فراهم کند. در نهایت هم می توان توسط قابلیتی که DLL Search Order دارا می باشد، library خود را در یک پروسه با سطح دسترسی بالا اجرا کرد. حال بخش DLLMain از library آلوده ما اجرا می شود و نفوذگری که دارای سطح دسترسی admin نمی باشد، توانایی اجرای بدافزار خود را در سطح بالا خواهد داشت. دیاگرام کلی این حمله را در ادامه مشاهده می فرمایید: