

rootkitの技術

Windows Kernel Hacking

愛甲健二

自己紹介



- 愛甲健二
- セキュリティエンジニア
- Kernel歴4年くらい
- <http://d.hatena.ne.jp/kenjaiko/>

rootkitとは？

ルートキット (rootkitあるいはroot kit) はコンピュータシステムへのアクセスを確保したあとで第三者 (通常は侵入者) によって使用されるソフトウェアツールのセットである。こうしたツールには作動中のプロセスやファイルやシステムデータを隠蔽する狙いがあり、ユーザに察知させることなく侵入者がシステムへのアクセスを維持することを支援する。Linux、Solaris、複数のバージョンのMicrosoft WindowsといったOSにルートキットが存在することが知られている。

(Wikipediaより)

rootkitとは？

ルートキット (rootkitあるいはroot kit) はコンピュータシステムへのアクセスを確保したあとで第三者 (通常は侵入者) によって使用されるソフトウェアツールのセットである。こうしたツールには作動中のプロセスやファイルやシステムデータを隠蔽する狙いがあり、ユーザに察知させることなく侵入者がシステムへのアクセスを維持することを支援する。Linux、Solaris、複数のバージョンのMicrosoft WindowsといったOSにルートキットが存在することが知られている。

(Wikipediaより)

要するに**高度なバックドア**みたいなもの？

rootkitとは？

ルートキット (rootkitあるいはroot kit) はコンピュータシステムへのアクセスを破損したあとで第三者 (通常は侵入者) によって使用されるソフトウェアツールのセットである。こうしたツールには**作動中のプロセスやファイルやシステムデータを隠蔽する**狙いがあり、ユーザに察知させることなく侵入者がシステムへのアクセスを維持することを支援する。Linux、Solaris、複数のバージョンのMicrosoft WindowsといったOSにルートキットが存在することが知られている。

(Wikipediaより)

要するに**高度なバックドア**みたいなもの？

作動中のプロセスやファイルや
システムデータって隠蔽できるの？

基本は関数フック

- Windowsは、OSの機能をDLLにまとめて、アプリケーションに提供している
 - ファイルアクセスのためにCreateFile関数
 - プロセス列挙のためにCreateToolhelp32Snapshot関数
- これらの関数群はすべてDLLとして提供されているため、書き換え(関数フック)が可能。また、関数フックの方法も様々…
 - Detours方式
 - <http://research.microsoft.com/en-us/projects/detours/>
 - IAT書き換え
 - http://ruffnex.oc.to/kenji/text/api_hook/
 - DLL差し替え
 - <http://ruffnex.oc.to/kenji/text/listexport/>

プロセスの隠蔽

- プロセス隠蔽の方法は数多くあるが、今回は一番シンプルなNtQuerySystemInformation関数フック法を紹介

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00007510	75	65	72	79	53	79	73	74	65	6D	45	6E	76	69	72	6F	uerySystemEnviro
00007520	6E	6D	65	6E	74	56	61	6C	75	65	45	78	00	4E	74	51	nmentValueEx.NtQ
00007530	75	65	72	79	53	79	73	74	65	6D	49	6E	66	6F	72	6D	uerySystemInform
00007540	61	74	69	6F	6E	00	4E	74	51	75	65	72	79	53	79	73	ation.NtQuerySys
00007550	74	65	6D	54	69	6D	65	00	4E	74	51	75	65	72	79	54	temTime.NtQueryT
00007560	69	6D	65	72	00	4E	74	51	75	65	72	79	54	69	6D	65	imer.NtQueryTime

DEMO

<http://ruffnex.oc.to/kenji/win/HideProcess.zip>

ファイルの隠蔽

- 実は、ドライバ(.sysファイル)は、OSへのインストールが終わると、削除可能
- .sysファイル以外のファイルを隠す場合は、FsRtlIsNameInExpression関数をフック
- マルウェアの場合は、他の実行ファイルの中に自身を隠す場合もある

キーボードログの取得

- フィルタドライバを作成し、キーボードドライバにフックをかけ、キーボードの入カログを取得

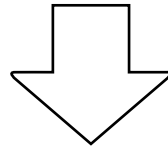


DEMO

<http://ruffnex.oc.to/kenji/src/drvkey.zip>

メモリ空間隠蔽

- 特定のメモリ空間を、OSから隠したい場合



- メモリアクセス違反(例外)時のジャンプ先アドレスを書き換える
- 隠したいメモリ空間に対して読み書き保護をつける
- 例外発生時に、どのメモリに対して例外が出たかを調べ、もし隠蔽したい部分だったら、別のデータを参照元へ返す

まとめ

- カーネルランドで動作するため、基本的に何でもアリ
- 64ビットWindowsだと、インストールするドライバには署名(?)が必要であり、完全なrootkit対策が施されているらしい
- 逆に32ビットWindowsだと、OSカーネルに直接手を加えられるとどうしようもなく、完全な対策法は無い(ハイパーバイザなど一部例外はある)
- 興味があれば、これを機会にぜひKernel Hackingを！

参考資料

Windows Server 2003 DDK

<http://www.microsoft.com/japan/whdc/DevTools/ddk/default.msp>

WDK and WDF (無料アカウント登録が必要)

<https://connect.microsoft.com/site/sitehome.aspx?SiteID=148#>

UsefullCode.net

<http://www.usefullcode.net/2006/12/ddk.html>

ローレイヤー勉強会

<http://groups.google.co.jp/group/lowlayer>

やや温め納豆

<http://d.hatena.ne.jp/eggarden/>

ROOTKIT

<http://rootkit.com/>

ご清聴、有難うございました
m(_ _)m

Any Questions?