root kit

2000 年 9 月 7 日版

penetration technique research site

http://www.geocities.co.jp/SiliconValley/1667/index.htm

Hideaki Ihara

hideaki@port139.co.jp

---

1. はじめに

この文書は、悪意のあるプログラムがカーネルモードで実行されている場合、どのような危険性があるかを管理者が理解することを目的としています。実際のアプリケーションの例として *Tripwire 2.2.1** を利用していますが、ここに記述している内容はユーザーモードで実行されるアプリケーションのいずれについても同じセキュリティ上の問題を抱えていると言えます。

2. ファイルやレジストの改竄検知は万全か？

ファイルが以前と同じ状態にあるかをチェックするためによく使われる方法として、MD5 などを使いファイルのハッシュを保存し、そのハッシュを現在のファイルのハッシュと比較するという方法があります。より進んだ方法としては、ファイルのアクセス権やサイズ、タイムスタンプなどを同様の方法で保存しておくことで、システムに対する改竄を検知するというツールもあります。有名なものとしては *Tripwire* などがあります。また、ホストベースの侵入検知ソフトやログ監視ソフト（例えば *Intruder Alert**）でも同様の機能を持っているものがあります。
より身近なソフトウェアとしては、ウイルスチェックソフトもある意味ファイルの変化を検知することができると言えるかもしれません。（ウイルスによりファイルが変更された場合）
ウイルスチェックは別として、ファイルのハッシュを計算し検証するタイプのツールの基本的な動作は以下のような流れになります。

ファイルを読み取る
↓
ハッシュを計算する
↓
以前に保存してあるハッシュと比較する
↓
同じであれば OK

ハッシュの方式が十分安全なものであれば、ファイルをこれらのツールに検知されずに改竄することは基本的に不可能です。（*Tripwire* では複数のハッシュ方式を指定することで安全性を高められます）

しかし、これらのツールにも限界があります。*Tripwire* などハッシュを計算する場合、それらのプログラムはユーザーモードで実行されます。このため、カーネルモードで実行される ***root kit*** を使うことで、これらの検知ツールにチェックされることなくトロイの木馬を仕掛けたりすることが可能になります。

事前に誤解のないように言っておきますが、私個人は Tripwire の利用を推奨しています。
多くのセキュリティツールが、root kit のようにカーネルモードで悪意を持って動作するプログラムに対抗することができません。
もちろんここに書いてある内容を実際に実行し、それによりシステムに何らかの問題が発生しても一切責任は負えません、自己責任で実行してください。

3. root kit のインストール

root kit の機能を知るには実際に実行してみることが一番です。まず以下の URL から Windows 版の *root kit* を入手します。

Windows Rootkit, build 0.31 alpha
http://www.rootkit.com/new_build.shtml

alpha_031.zip を展開すると、以下のファイルが出来上がります。

root.sys　　deploy.exe
root_readme.txt　rk_src_031a.zip

インストールに必要になるものは、_root_.sys と deploy.exe の二つのファイルです。
Deploy.exe を実行することで、_root_.sys をシステムにサービスのイメージとして登録することができますが、実行には管理者の権限が必要になります。今回は日本語版 Windows 2000 に *root kit* をインストールしてみることにします。
まず、_root_.sys をインストールするシステムのフォルダにコピーします。ファイルを置く場所はパスが通っているところであれば大丈夫ですが、今回は c:\winnt に置くことにします。
予め *Tripwire* では、c:\から全てのファイルをチェック対象としてハッシュのデータベースを作成しておき、ファイルのコピー後にチェックを行います。以下の図は *Tripwire* のレポートを表示しているところです。＋マークはファイルが追加されたことを示しており、_root_.sys と deploy.exe が追加されていることがわかります。

あとは、deploy.exe を実行すれば *root kit* がシステムに登録されます。

4．レジストリを隠す

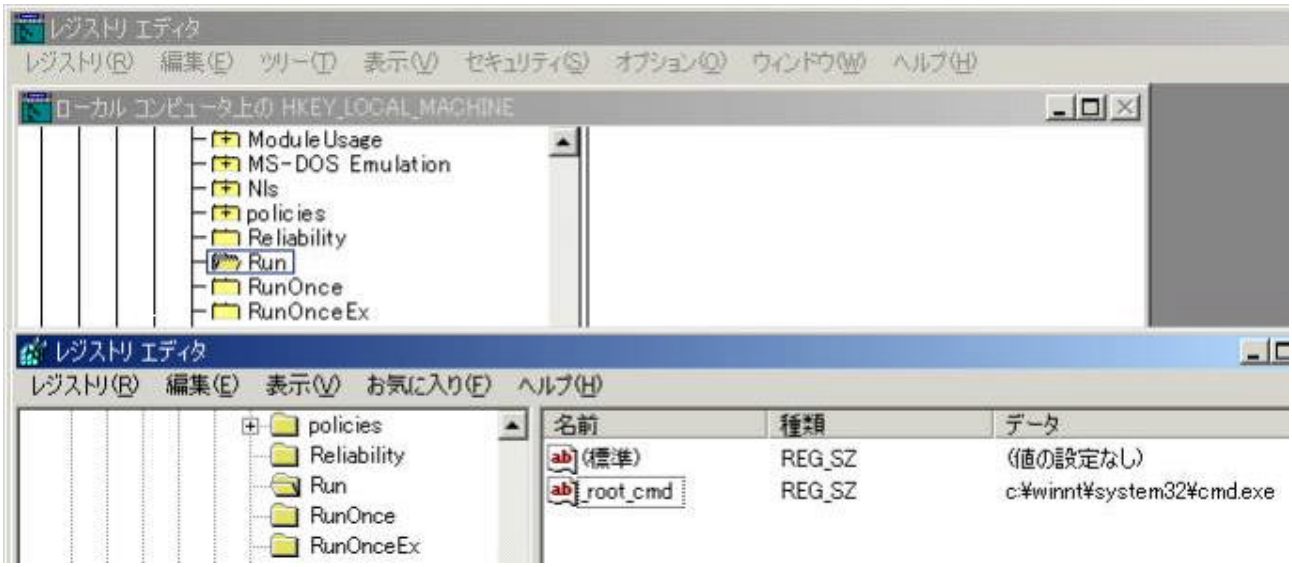
では *root kit* のインストールによってレジストリがどう変化したかを、先ほどと同様に *Tripwire* でチェックしてみます。

多数のレジストリに変化が見られますが、HKLM\SYSTEM\CurrentControlSet\Services の項目に注目してください。AppMgmt\Enum に追加が見られますが、*root kit* のサービスがインストールされたことは、この情報からだけではよくわかりません。（とはいえ、システムに対してなんらかの新たなサービスが登録されたことは、レポートから読み取れます）

実は、すでに deploy.exe の実行後から、*root kit* の機能が有効になっていて、カーネルモードで動作している_root_.sys が、プログラムに正確なレジストリの姿を見せていないのです。
カーネルモードで実行されている *root kit* は、ユーザーモードのプログラムがレジストリを読もうとすると、一定のパターンの文字列を持つレジストリキーやレジストリ値をフィルタします。そのため、ユーザーモードで実行されるアプリケーションは、レジストリの内容をチェックしようとしても、*root kit* により悪意のあるキーや値がフィルタされてしまい、レジストリの正しい内容を読み取ることができません。
コマンドプロンプトから net stop _root_コマンドを実行して *root kit* のサービスを停止し、もう一度 *Tripwire* でチェックしてみます。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_|DisplayName
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_|ErrorControl
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_|ImagePath
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_|Start
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_|Type
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Enum
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Enum|0
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Enum|NextInstance
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Enum|Count
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Security
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥_root_¥Security|Security
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥AppMgmt¥Enum
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥AppMgmt¥Enum|0
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥AppMgmt¥Enum|NextInstance
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥AppMgmt¥Enum|Count

今度は、HKLM\SYSTEM\CurrentControlSet\Services の下に、先ほどは存在していなかった_root_が検知されました。このように *root kit* では、レジストリのキーや値の先頭に“ _root_ ”が付いている場合、それを隠すという機能を持っています。
また、わざわざ *root kit* のサービスを停止しなくても、レジストリエディタの先頭に_root_を付けたコピーを作成することで root kit の動作中でも正しいレジストリの値を見ることができます。
まず、regedit.exe をコピーして_root_regedit.exe という名前に変更します。
実際に、regedt32.exe と_root_regedit.exe で同じレジストリキーを見てみたのが下図になります。いずれも、ローカルコンピュータの HKLM\SOFTWARE\Microsoft\CurrentVersion\Run キーを表示していますが、regedt32 では_root_cmd が表示されていません。ここでは値として cmd.exe が指定されていますが、ここにトロイの木馬を設定しておけば、ツールや管理者に発見されることなくバックドアを作成することが可能になります。



5. EXE リダイレクション

root kit のもう一つの機能は EXE リダイレクションです。(現在のバージョンでは、ハードコーディングされているようですので、以下の手順でテストできます)
まず、c:\winnt\system32 にある cmd.exe を c:\にコピーし、ファイル名を_root_cmd.exe に変更します。
次に、calc.exe を c:\にコピーします。
root kit のサービスが稼動していることを確認し、_root_cmd.ex を実行してみましょう。すると、calc.exe が実行されます。(_root_cmd.exe が実行されると、calc.exe が起動するようになっている)
root kit のサービスが停止している場合には、_root_cmd.exe を実行すると CMD.EXE が起動してきます。

6. ‘root kit’ vs Integrity Protection Driver (IPD)

root kit の現在のバージョン(0.31)では、_root_サービスのイメージとして_root_.sys が設定され、サービスの起動時にロードされています。*root kit* のインストールを防ぐために Pedestal Software から *Integrity Protection Driver* (IPD)がオープンソースで公開されています。

Integrity Protection Driver (IPD)
http://pedestalsoftware.com.cnchost.com/intact/freesoftware.htm

IPD をインストールすると、*IPD* のドライバがロードされてから 20 分経過した時点で、以下のフォルダとレジストリへの書き込みが完全にブロックされるようになり、*root kit* のインストールを防ぐことが可能になります。

- System32\drivers (etc フォルダは除く)
- HKLM\System\CurrentControlSet\Services

しかし、*IPD* は完全な解決策になりません。*root kit* はかならずしもサービスとして登録される必要がなく、動的にカーネルモードのモジュールとしてロードすることが可能です。
すでに、root kit をサービスとして登録せずにロードするためのソースが公開されています。

No Driver Required ? SystemLoadAndCallImage http://www.rootkit.com/load_and_call.shtml

ここで公開されているロード用のプログラムを利用すると、_root_.sys を動的にロードすることが可能になります。(_root_.sys をロードするには管理者の権限が必要です)
動的に_root_.sys がロードされた場合、レジストリなどには何ら変化が起きませんので、発見することは非常に難しくなります。これを検知することができるセキュリティツールを筆者は今のところ知りません。もしご存知の方はぜひ教えてください。

7. 対策は？

いずれの方法を用いる場合でも、*root kit* をシステムにインストールするには管理者の権限が必要になります。日頃から管理者の権限でシステムを利用していると、受動的攻撃*などを受けた際に危険にさらされます。また、セキュリティ ホール(システムの権限で任意のコードが実行されるケース)などが潰れていない場合には、セキュリティ ホールを利用してインストールされるケースも想定されます。必ず OS やアプリケーションの最新バージョンを利用しましょう。

8．root kit の有効利用は？

root kit は、その使い方によっては不正アクセス者にとっての脅威となる場合もあります。例えば、不正アクセスを監視するサービスを *root kit* で隠しておくという方法があります。これにより、仮に不正アクセス者が、システムのサービスリストやレジストリから侵入検知システムを探ろうとしても、発見されずに済むかもしれません。

9．最後に

今回、*root kit* のチェックを行うにあたり *Tripwire* を利用しましたが、基本的には他のツールを使ったとしても、*root kit* により隠されたレジストリなどを発見することは困難です。
あなたがお使いのセキュリティ製品は例外だ、とは考えない方がいいでしょう。
ウイルスチェックにしても、本来読み出すべきファイルがカーネルモードで動く悪意のあるプログラムにより、ダミーのファイルに入れ替えられた場合には、検出することはできないでしょう。
カーネルモードで動作するこの手のツールは、単にレジストリの値を隠すだけでなく、特定のプロセスを表示しない、ファイルを表示しない、ユーザーを表示しないなど、作成者のアイデアしだいで様々なケースが考えられます。例えばシステムのセキュリティ設定をスキャンし脆弱性を報告するツールも多くありますが、それらもカーネルモードで偽った値を返されたら騙されてしまう部分があるでしょう。このため、どのセキュリティ製品についてもカーネルモードで動作する悪意のあるプログラムは大きな脅威となります。
また、この問題は Windows NT/2000 に限った問題ではありません。UNIX などの OS についても同じことが言えます。
しかし、基本的なセキュリティ対策を行っておくことで十分 root kit のインストールを防ぐことは可能です。また、*Tripwire* や *IPD* などのツールは *root kit* の発見が難しいからといって利用をやめるべきものではありません。むしろ、このような危険なものを発見する可能性が一番高いのも *Tripwire* などのツールなのです。*root kit* が動作していない状態で *Tripwire* などで監視されているファイルの改竄チェックを回避する方法は基本的にありません。
例えば扉に頑丈な鍵がかかっていても、扉を蹴破れば誰でも家に侵入することができます。しかしだからといって鍵をかけないという人はほとんどいないでしょう。

<u>間違ってもセキュリティツールが不要なのだと勘違いしないようにしてください。</u>

過信は禁物です。弱点をよく理解した上でセキュリティツールを使うことでより安全なシステムを構築することができます。
最後になりましたが、今回この文書を作成するにあたり、久保田氏ならびに三浦氏には貴重なコメントやお手伝いをいただきました。この場をお借りしてお礼申し上げます。

参考資料

* Tripwire（www.tripwire.com）
  http://www.jwntug.or.jp/softwarereview/
* Intruder Alert(www.elnis.com)
* 受動的攻撃について http://www.geocities.co.jp/SiliconValley/1667/index2.html