自己暗号化 rootkit

佐々木　慎[†1]　大山恵弘[†1]

1. はじめに

近年のマルウェアは，アンチウィルスソフトによる検出やコードの解析を困難にすることに焦点を当てている．ユーザーレベルで動作するマルウェアには，ポリモーフィック型マルウェアやメタモーフィック型マルウェアと呼ばれるものが存在する．ポリモーフィック型マルウェアは，自らのコードを暗号化することが可能なマルウェアであり，メタモーフィック型マルウェアは，感染のたびに自身のコードを書き換えることが可能なマルウェアである[1)]．

これらのウィルスは，アンチウィルスソフトによるパターンマッチングを用いた検出や，逆アセンブルによる動作解析が困難である．

今後，カーネルレベルで動作するマルウェアにも，自己暗号化機能を有するものが出現することが予想される．本研究では，自己暗号化機能を有するカーネルレベル rootkit を実装し，その危険性を示す．

2. rootkit の概要

rootkit とは，攻撃者が攻撃対象のコンピュータへのアクセスを確保した後に使用するツールセットである．プロセス，ファイル，ディレクトリなどを隠蔽し，侵入の形跡を隠す．侵入したシステムを攻撃するユーティリティーを隠すために用いられることが多い．

rootkit には，ユーザーレベル rootkit とカーネルレベル rootkit の 2 種類が存在する．それぞれ、次のような手法[2)–4)] を用いて実装される．

- ユーザーレベル rootkit
  - インポートアドレステーブルの改竄
  - DLL インジェクション
  - インライン・フック
- カーネルレベル rootkit
  - SSDT の改竄
  - 割り込みディスクリプタテーブルの改竄
  - IRP テーブルの改竄

†1 電気通信大学 電気通信学部 情報工学科

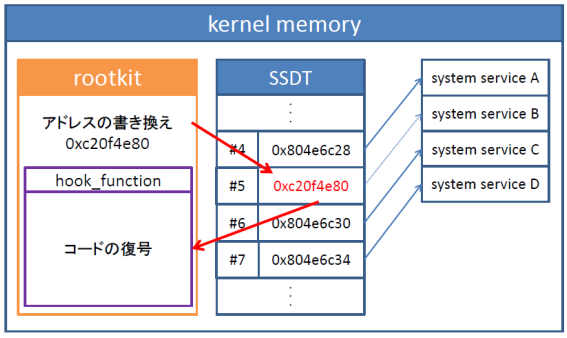

図 1　システムの概要図 1

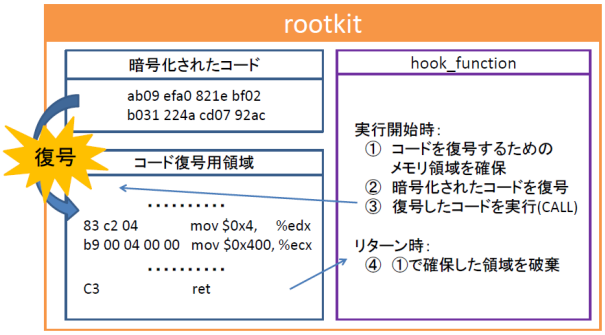

図 2　システムの概要図 2

3. SSDT の改竄

SSDT(System Service Dispatch Table) は，Windows OS により作成されるカーネルメモリ内のデータ構造であり，System Service のアドレスが System Service 番号順に並べられている．System Service とは，ユーザープログラムが Windows OS が提供する機能を利用するための関数であり，UNIX 系 OS における System Call に対応する，System Service はカーネルモードで実行される．Nt または Zw から始まる名前の関数がこれにあたる．

SSDT を改竄する rootkit は，System Service のアドレスを書き換え，フックすることで悪意ある関数を実行させる．

4. 設 計 方 針

カーネルレベル rootkit を，SSDT を改竄する手法を用いて実装する．システムの概要図を，図 1，2 に示す．ユーザープログラムでは，カーネルメモリ内に存在する SSDT を書き換えることはできないため，rootkit はデバイスドライバとして実装する．デバイスドライバのインストール時に呼ばれる DriverEntry 関数で SSDT のフックする System Service に対応するアドレスを暗号化されたコードを復号する関数のアドレスに書き換える．これにより，フックされた System Service が呼ばれるとコードを復号する関数が実行される．この関数は実行開始時にメモリ領域を確保し，確保した領域に暗号化されたコードを復号する．メモリの確保には，ExAllocatePoolWithTag 関数を用いる．確保したメモリの保護属性を変更して実行可能とし，アセンブリ言語の CALL 命令により，復号されたコードを実行する．復号されたコードの実行が終了したら，確保したメモリ領域を解放する．このようにすることで，復号されたコードがメモリ上に存在するのは，そのコードの実行中のみとなる．

5. 現状と今後

Visual Studio 2010 と Windows のデバイスドライバ開発ツールである Windows Driver Kit (WDK) を用いて，システムの実装を行っている．OS は，Windows 7 32bit である．SSDT の書き換えを行い，基本となる rootkit を実装した．また，ユーザーレベルのプログラムで，暗号化されたコードをメモリ上に復号し，実行する予備実験を行い動作を確認した．今後は，暗号化・復号化の処理において，カーネルコードならではの問題について考察し，実装を進めていく．最終的にはデバイスドライバファイル (.sys) を入力とし，暗号化して出力するパッカーを作成する予定である．

参 考 文 献

1) Xufang Li and Peter K.K.Loh. Mechanisms of polymorphic and metamorphic viruses. *2011 European Intelligence and Security Informatics Conference (EISIC)*, pp. 149–154, 2011.
2) Greg Hoglund and James Butler. *Rootkits: Subverting the Windows Kernel*. Addison-Wesley Software Security Series. Pearson Education Inc., 2006.
3) Bill Hoglund. *The Rootkit Arsenal:Escape and Evasion in the Dark Corners of the System*. Wordware Publishing, 2009.
4) Desmond Lobo, Paul Watters, Xin-Wen Wu, and Li Sun. Windows rootkits:attacks and countermeasures. *2010 Second Cybercrime and Trustworthy Computing Workshop*, pp. 69–78, 2010.