anti-debugging

yoggy@チームチドリ
www.t-dori.net

チームチドリ

anti-debuggingとは?

- デバッガを使用した解析を妨害する手法
  - プログラムの動作を解析されるのを阻止するため、プログラム自身に実装
- malwareなどに実装されている？
  - malwareが長生きするための工夫
    - Honeypotなどによる解析の対抗策
    - デバッグ環境で実行すると動かない、自滅するとか…

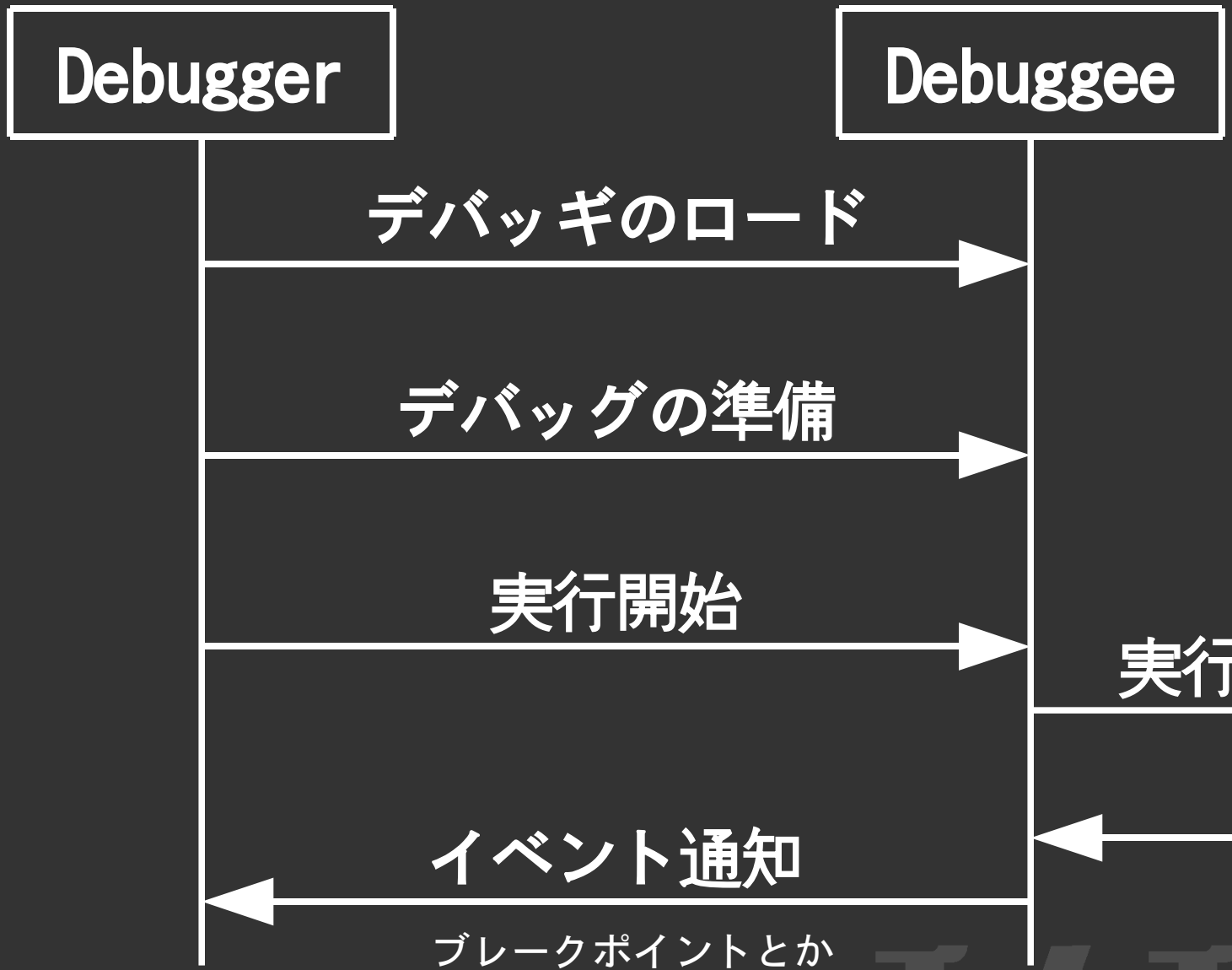
anti-debuggingの手法

- デバッガ対策
  - IsDebuggerPresent()
  - INT3の検出
  - ハードウェアブレークポイントの監視
  - SEH(Structured Exception Handle)の監視
  - SoftICE対策
- VM(Virtual Machine)環境対策
- その他いろいろ…

デバッガの基本動作

- デバッギのロード
  - プログラムをメモリにロードするだけで、実行はしない。
- デバッギと通信するための仕掛けを準備
  - デバッギのメモリを書き換えたり。
  - ブレークポイントなど
- デバッギを実行
- デバッギがデバッグ用イベントを通知
  - ブレークポイントで停止した際のイベントなど。

デバッガの基本動作



デバッガ対策

- ポイント
  - デバッガによって書き換えられる部分を検知する
  - デバッグを行う場合、かならずプログラム内の環境が変化する

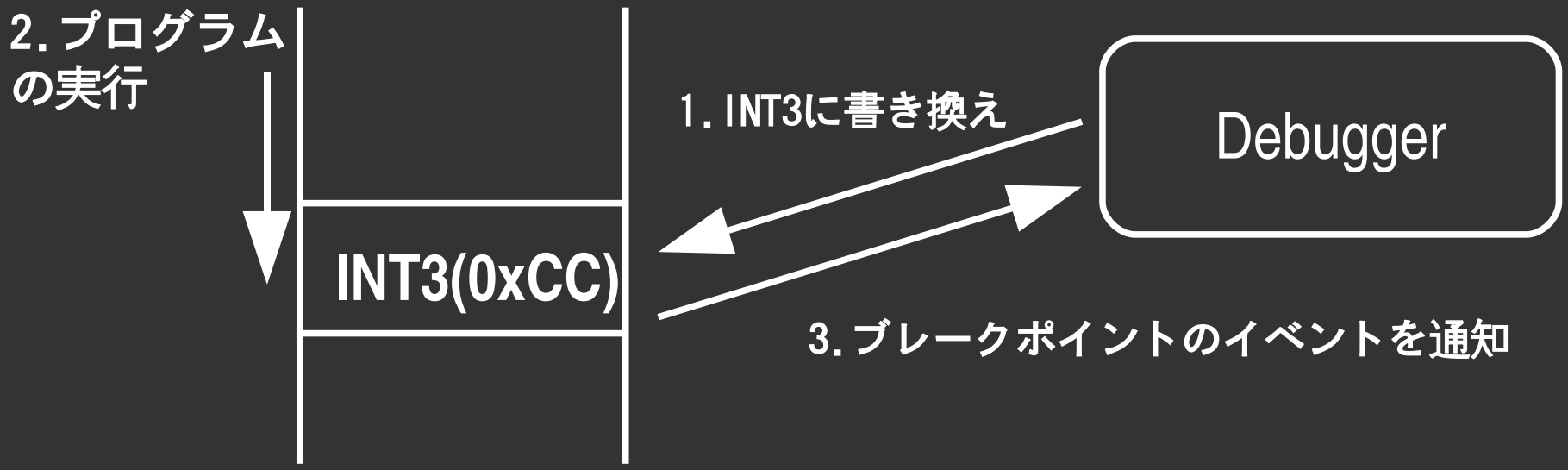
IsDebuggerPresent()

- Win32 API
- デバッガにアタッチされていた場合、TRUEを返す関数

```
int _tmain(int argc, _TCHAR* argv[])
{
    if (IsDebuggerPresent() == TRUE) {
        exit(0);
    }
    printf(”ほげふが”);
    return 0;
}
```

INT3の検出

- デバッギをブレークポイントで停止させるために使用する割り込み
- デバッギの実行前に、デバッガが停止させたい箇所のコードを書き換える



ハードウェアブレークポイントの監視

- CPUが用意しているデバッグ用の仕掛け
  - デバッグ用レジスタに停止したいアドレスなどを設定する
  - x86の場合、レジスタDR0～DR7を使用
- レジスタにデバッグ用のハンドラが仕掛けられているかどうかを監視

SEH(Structured Exception Handle)の監視

- Windows特有の仕組み
- プログラム中で例外が発生した場合のハンドラテーブル
- SEHにデバッグ用のハンドラが仕掛けられているかを監視

SoftICE対策

- SoftICEとは？
  - Compuware社のDriverStudioに含まれる製品
  - カーネルレベルでのデバッグが可能
    - ドライバのデバッグとか
- 検出方法
  - 仮想デバイスドライバの有無を検出
    - \\.\SICE
    - \\.\NTICE
    - \\.\SIWDEBUG, \\.\SIWVID　...など

VM(Virtual Machine)環境対策

- ポイント
  - 実際のPCとは微妙にデバイス環境が異なる
    - HDD,NIC,VGA,メモリ,I/Oポート
    - バックドアポート
      - ホストOS-ゲストOS間の通信用など

VM(Virtual Machine)環境対策

- VMWareの場合
  - バックドアポートを叩いてみる

```
BOOL isVMWare() {
  unsigned int magic_num = 0;
    __try { __asm {
            mov eax, 564D5868h
            mov ebx, 0
            mov ecx, 0000000Ah
            mov edx, 5658h
            in  eax, dx
            mov magic_num, ebx
    } }__except(NULL, 1) {}

    if (magic_num != 0) return TRUE;
    return FALSE;
}
```

VM(Virtual Machine)環境対策

- Xenの場合
  - カーネルの違い
    - /proc/ksymallsにxen_～というシンボルが含まれている
  - Hypercallの有無？
    - HypercallはXenドメイン間の通信チャネル
    - Xen3.0から導入
  - Domain0以外はRing1で動作している
    - CPUがVanderpool Technologyをサポートしているとring0に見えるかも？
  - デバイス環境の違い
    - /proc/ioports,/proc/slabinfoとか

VM(Virtual Machine)環境対策

- VirtualPCとかBochsとか
  - Virtual Machine detection...
    - http://bos.asmhackers.net/forum/viewtopic.php?id=59&action=new
- その他VM環境いろいろ…
  - QEMU,coLinux,Plex86,UML(User Mode Linux)
  - OpenVZ,Virtuozzo,Parallels Workstation
  - etc,etc...

anti-debuggingを回避する方法？

- チェックコードの無効化
  - チェックコードが実行される前に消す。
  - 実行ファイルをバイナリエディタで書き換え
  - デバッグ中にメモリを書き換え
  - UPXなどのパッカーが使われていたり、難読化されているとちょっと難しい？
- 根性？（笑
  - デバッギ側とデバッグ側の知恵比べ
    - 結局はいたちごっこ
  - デバッグ側の方が必ず有利…なはず。

参考資料

- デバッガの理論と実装
  - http://www.ascii.co.jp/100satsu/program/program_029.htm
- Anti-Debugging & Software Protection Advice
  - http://www.woodmann.com/crackz/Tutorials/Protect.htm
- Know your Enemy: Tracking Botnets - Source Code
  - http://www.honeynet.org/papers/bots/botnet-code.html
  - デバッガ・VM環境検知するためのサンプルコード
- VMware fingerprinting counter measures.
  - http://honeynet.rstack.org/tools/vmpatch.c
  - VMWareのバックドアポートを偽装するパッチ

参考資料

- OllyDbg Q&A
  - http://hp.vector.co.jp/authors/VA028184/OllyDbgQA.htm
- SoftICE
  - http://en.wikipedia.org/wiki/SoftICE
  - http://www.compuware.co.jp/products/driverstudio/
- 仮想な背中
  - http://chitchat.at.infoseek.co.jp/vmware/indexj.html

ご静聴ありがとうございました。m(_ _)m