



Livegrid™



システムレジスタの不足

と2つのシンプルなアンチフォレンジック攻撃

Tsukasa Ooi <li@livegrid.org>
Lead Analyst, Livegrid Incorporated



関連する事項

- ライブメモリフォレンジック
- アンチフォレンジック
- Rootkit



アンチフォレンジックとは？

- フォレンジック手法を欺く手法
- 気をつけるは“攻撃者”だけではない!
 - 監視から逃れたい者が自らのマシンを感染させることが考えられる。
- ただし今は忘れてください
 - 今日はその話はしません



Livegrid™



発表:

- PacSec 2009

ステルスルートキット：悪いヤツはどうライブメモリフォレンジックをすり抜ける？



ライブメモリフォレンジック

- 動作しているマシンのメモリを基にしたフォレンジック手法
- 取得は、専用ツールで行う
 - EnCase
 - dd
 - ...



メモリ取得ツールがすること

- 物理メモリの内容を出力する
- システムレジスタの内容を (必要であれば) 取得する

本当に“必要であれば”でいいの？

...というのが今回の話。



rootkit は何ができる？

- システムレジスタの内容なしに物理メモリダンプするツールおよびフォレンジックソフトウェアを欺く



本当にできるの？

- 多くのソフトウェアがそうしている!
 - EnCase
 - (RAW) dd
 - Memoryze
 - WinEN
 - FastDump
 - ...



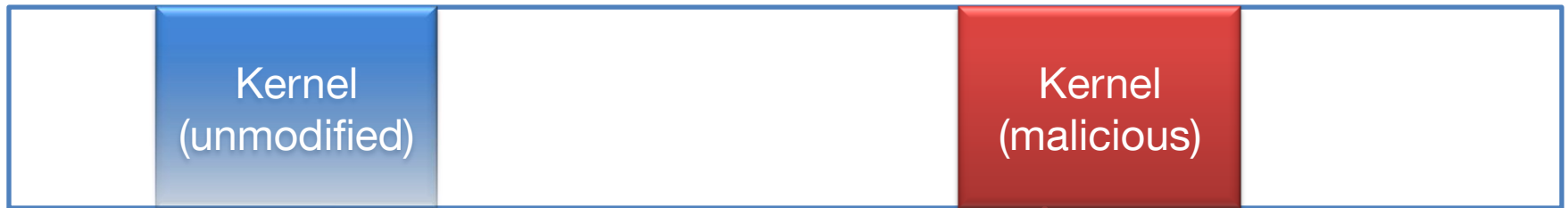
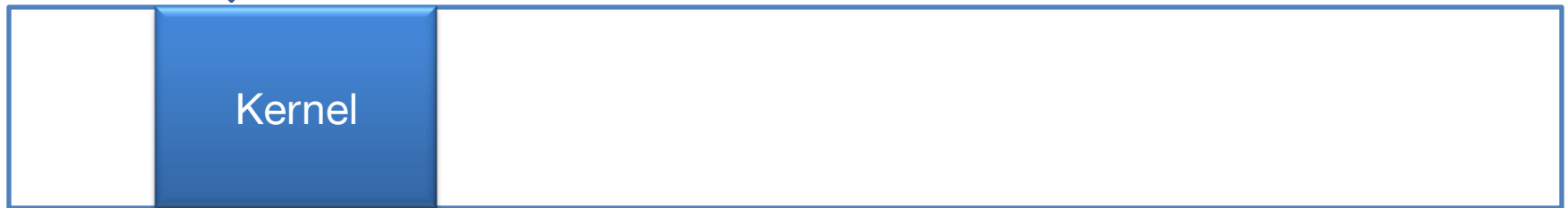
攻撃法その1 (1)

- CR3 レジスタ (ページング構造体へのポインタ) を変更する



攻撃法その1 (2)

フォレンジックソフトウェアに認識される CR3



本物の CR3



攻撃法その1 (3)

- システムレジスタを取得していない場合、メモリシグニチャから構造体を検索する
- しかし、これらのメカニズムこそが付け入る隙である



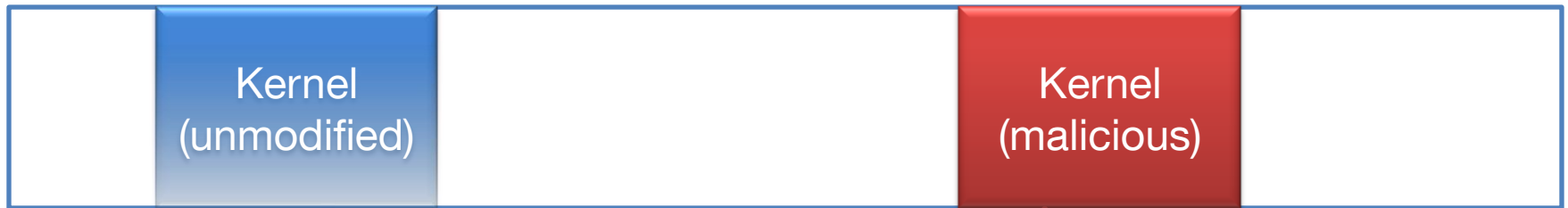
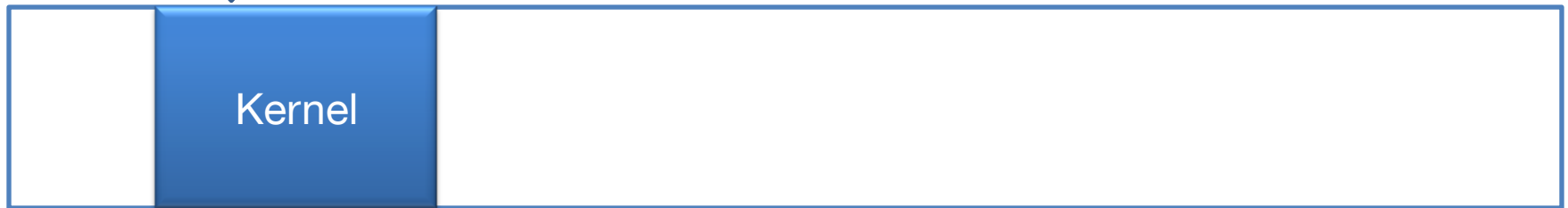
攻撃法その1 (4)

- システムのメモリ領域を未改変のまま残す
- バックアップ領域を作成する
- カーネルの一部をコピーし、パッチする
- CR3 を rootkit のものに変更する



攻撃法その1 (5)

フォレンジックソフトウェアに認識される CR3



本物の CR3

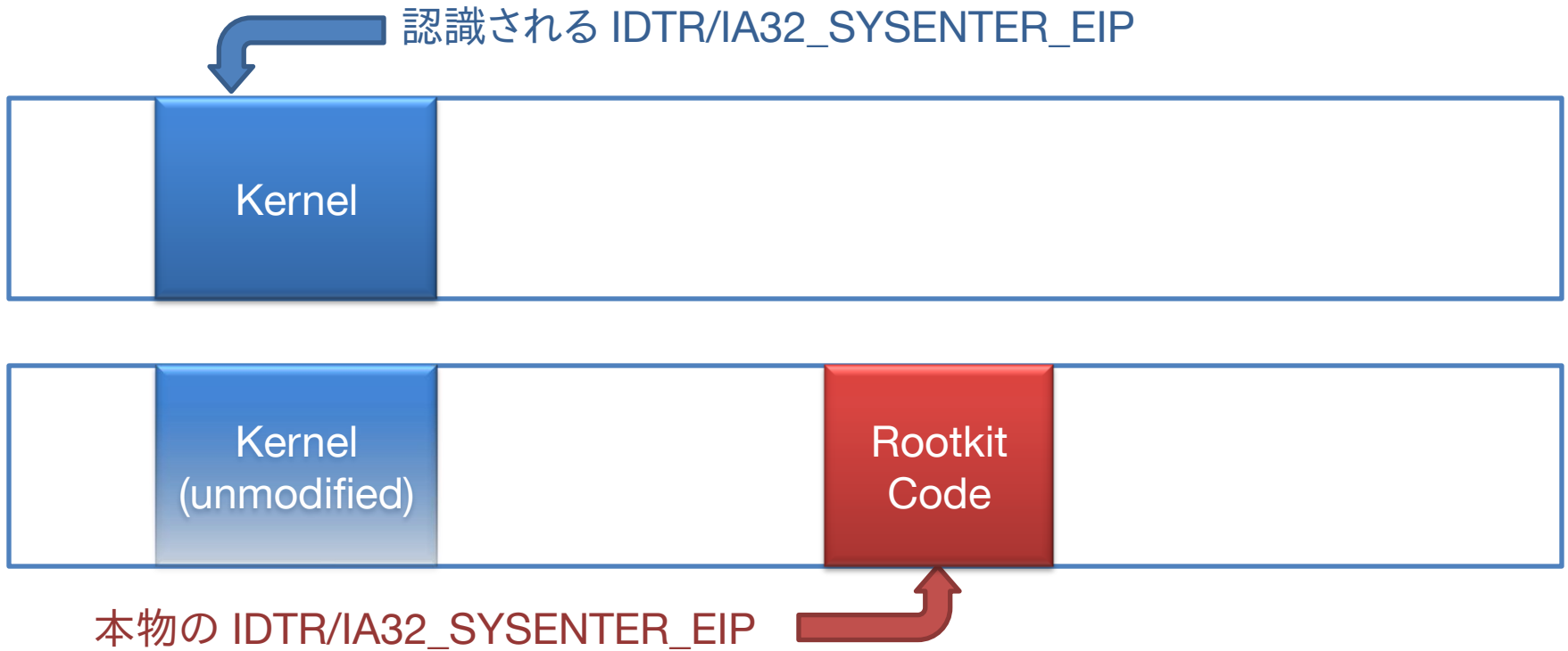


攻撃法その1 (6)

- ただこの手法では rootkit がページテーブルを管理しなければならないため、少し難しい
- もっと簡単な手法がある! (その2)



攻撃法その2 (1)





攻撃法その2 (2)

- IDTR は例外や割り込みを管理するレジスタ
 - ページフォルトもその中に含まれる
 - これはどちらかといえば“その1”や“その2後半”の補助用
- IA32_SYSENTER_EIP MSR / LSTAR_MSR はシステムコールの入り口へのポインタ
 - システムコールをフックし、改変することができる



攻撃法その2 (3)

- 実装法:
<始め> これらのレジスタを書き換える <終わり>
ね、簡単でしょ?
- これらの手法は現在の rootkit にも使われているが、
アンチフォレンジックにも役に立つ!
 - メモリの「どこか」に隠してしまえば、
それを見つける一般的な手段は存在しない!



攻撃への対抗法 (1)

- これらのシステムレジスタを取得すること
 - CR3
 - IDTR
 - IA32_SYSENTER_EIP MSR
 - LSTAR_MSR
- (rootkit が CR3/IDTR の改変を使用する場合)
物理的/論理的メモリアウトのチェック



攻撃への対抗法 (2)

- IDT や Page Table のシグニチャは検出が容易
- なので...
 - これらのテーブルをシグニチャで検出する
 - これらのテーブルが“悪意ある”ものかをチェックする



まとめ

- 可能な限りシステムレジスタを取得するツールやファイルを用いること!
 - Microsoft クラッシュダンプ
 - Windows 休止状態ファイル (hiberfil.sys)
 - windd (win32dd/win64dd)
- フォレンジックの新しいアプローチが必要だろう



Livegrid™



質問等ありますか？

THANK YOU

Tsukasa Ooi <li@livegrid.org>
Livegrid Incorporated, Lead Analyst



Livegrid™



技術文書とソースコード

- 2009年12月公開予定
- <http://a4lg.com/> にて