進化しつづけるマルウェア:
仮想マシン技術からの対策

慶應義塾大学 理工学部
河野 健二

ルートキットの脅威

sslab system software

Silent, Easily Made Android Rootkit Released At DefCon

Posted by **Soulskill** on Saturday July 31 2010, @11:26AM
from the it-slices-it-dices dept.

An anonymous reader writes with news that security experts from Spider Labs released a kernel level rootkit for Android devices at DefCon on Friday. "As a proof of concept, it is able to send an attacker a reverse TCP over 3G/WIFI shell upon receiving an incoming call from a 'trigger number.' This ultimately results in full root access on the Android device." The rootkit was developed over a period of two weeks, and

50 of **133** comn

Tech News

Rootkit Malware Found On Android Apps

Thursday, 3 Mar 2011, 9:17am (8 months ago)

Many have the impression that an antivirus software is redundant on a smartphone. However, a recent report published by Guardian News revealed that a malicious rootkit malware, dubbed as DroidDream, have already infected more than 50 apps on the widely popular Android Market.

アンチウィルスソフトを入れればいい？

- 一定の効果はある
- でも，一定の効果しか
- なぜ？
- アンチウィルスソ 作原理

新しいマルウェアには無力！

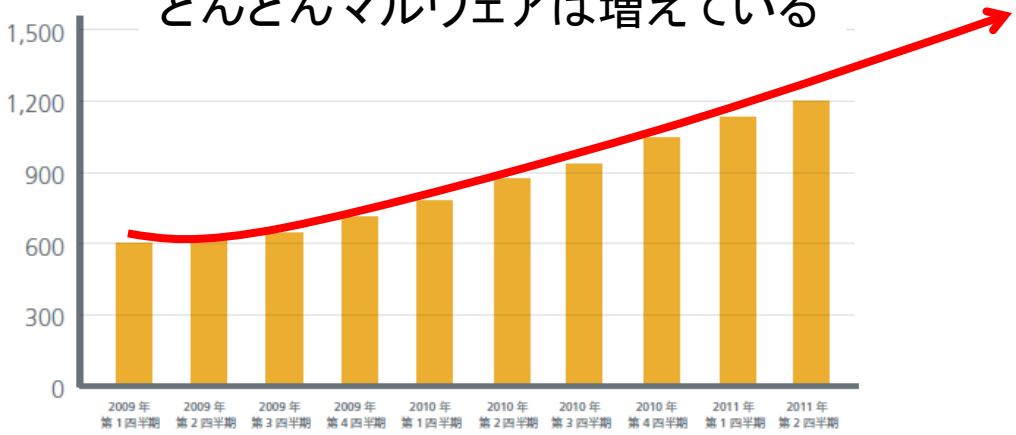
マルウェアはどんどん進化する！

- どんどんマルウェアの亜種ができる
  - Android 狙いのルートキット: DrdDream, DroidKungFu, DrdDreamLite
  - 一度の対策では不十分．ウィルス定義ファイルを更新しつづける
- マルウェアの進化
  - シグネチャによる検知をすり抜けるため，見た目を変える
    - 緑色のウィルスを少し変えて，黄緑色のウィルスにする
  - 攻撃方法を変える
    - OS などにパッチをあてても，別の方法で感染する
  - （亜種ではない）新種の出現

多 ↕ 稀

- マルウェアの進化に対応するには？
  - 出現頻度の高い亜種: 新規対策不要であるべき
  - 出現頻度の低い本当の新種: このときだけ新規対策が必要

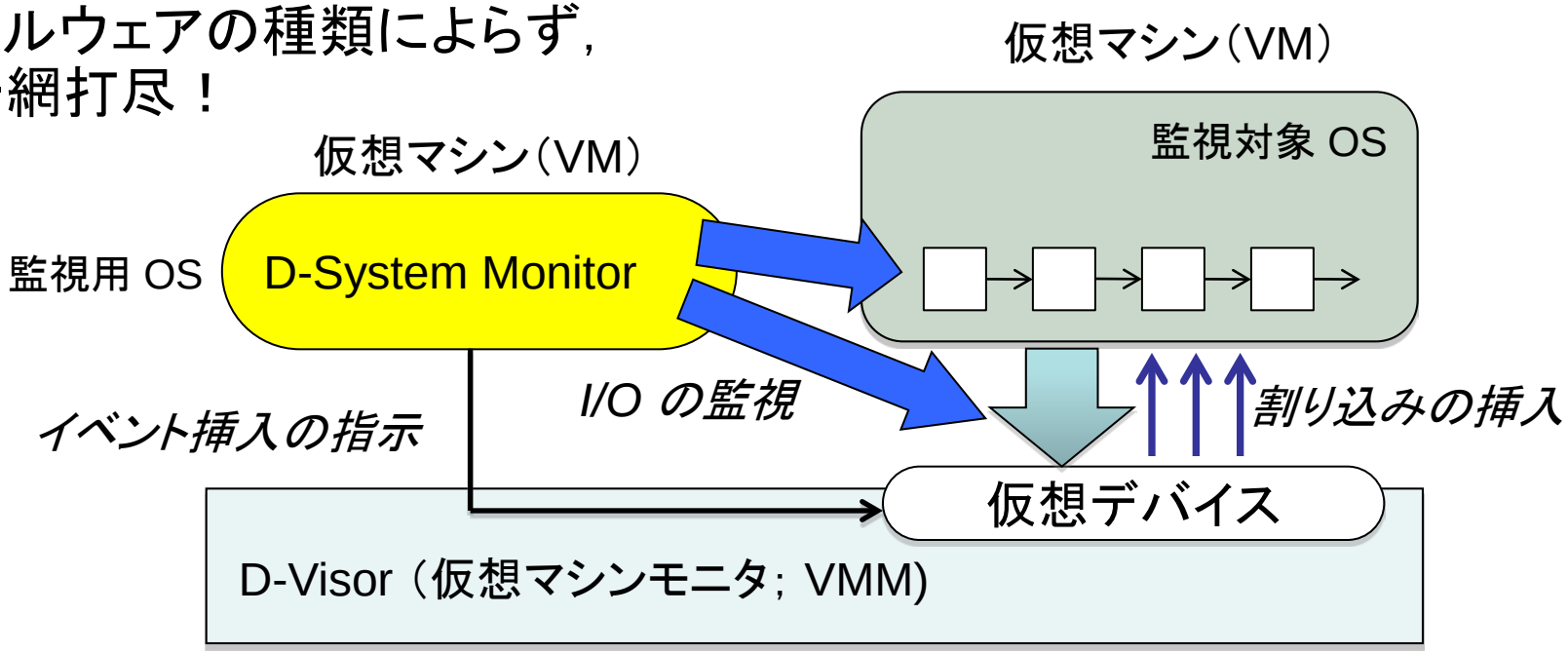
携帯端末向けに限っても
どんどんマルウェアは増えている



McAfee 脅威レポート 2011年第2四半期より

進化に強いマルウェア検知基盤

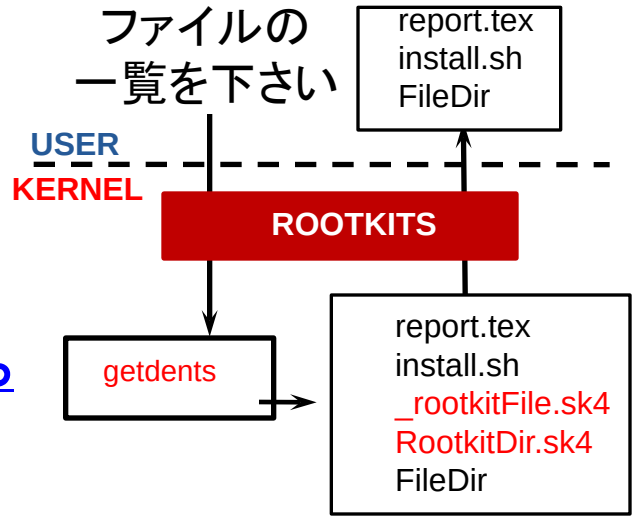
- 着眼点：
  - マルウェアに感染した OS の“振る舞い”は何か違うはず
    - 振る舞いにまったく違いがなければ，感染していないのと同じ
- アプローチ：
  - 仮想マシン技術により監視対象 OS の“振る舞い”を監視する
  - 健全な OS の“振る舞い”と何か違えば，
    マルウェアの種類によらず，
    一網打尽！

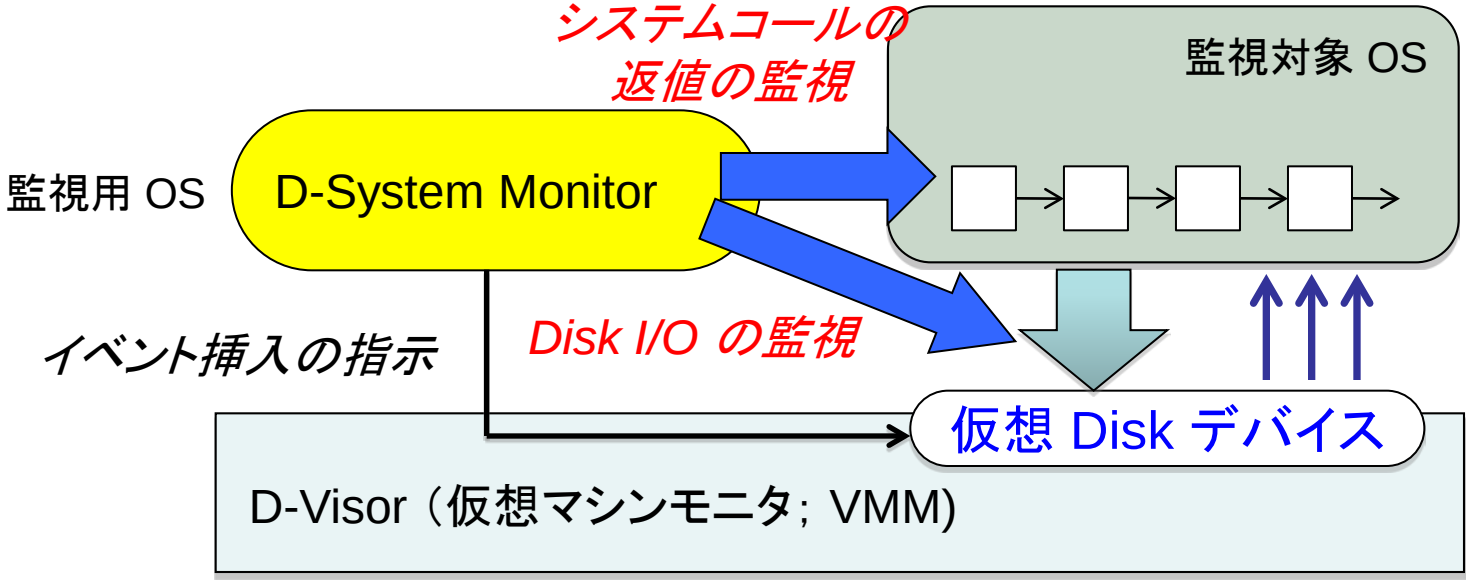


“振る舞い”監視の例（その1）

- ファイル隠蔽型ルートキット:
  - 隠蔽したいファイルを一覧から削除する
    - 攻撃方法だけでも多様:
      - Replace/redirect system calls,
      - Patch Kernel Text, Modify Jump tables, ...
- 監視する“振る舞い”
  - システムコールの返値
  - ディスク I/O の内容

一致しなかったら
異常動作





なぜマルウェアの進化に強いのか？

- マルウェア特有の“振る舞い”を監視しているため
  - シグネチャ不要
  -
- フ
  - たったひとつの仕組みで多様な検体をすべて検知！
    - 攻撃ベクタ，攻撃対象が異なる 8 つの検体

Rootkit	Attack Vector	Target	Detected
adore – 0.42	LKM	Sys. Call Table	Yes
rial	LKM	Sys. Call Table	Yes
enyelkm	LKM	Kernel Text	Yes
override	LKM	Sys. Call Table	Yes
adore-ng0.56	LKM	Virt. File System	Yes
mood-nt	Raw mem. access	Sys. Call Table	Yes
superkit	Raw mem. access	Kernel Text	Yes
suckit2priv	Raw mem. access	Kernel Text	Yes

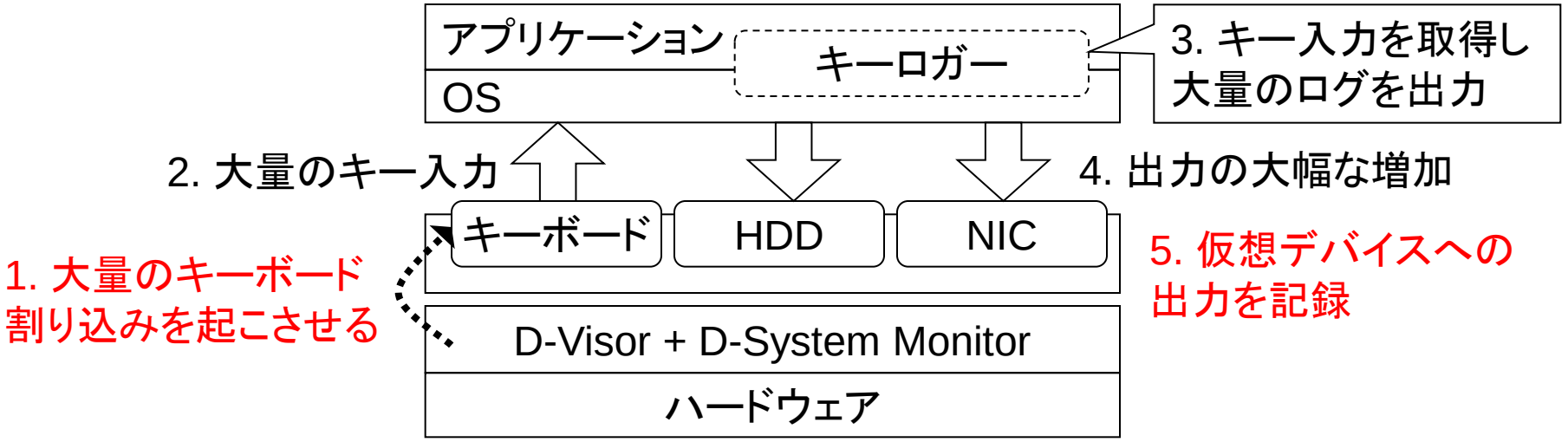
“振る舞い” 監視の例：キーロガー

sslab system software

- キーロガーとは？
  - キー入力の記録を目的とした悪意あるプログラム
    - 情報漏洩を目的としたスパイウェアの一種
    - ログをディスクに保存したり，ネットワークに送信する機能を持つ
    - パスワードやクレジットカード番号などを漏洩させる
    - 多大な被害を与える可能性がある
  - 自身の存在を隠蔽する
    - ユーザに気づかれずに動作する
    - カーネルレベルに存在することで OS をのっとる
    - キーロガー検知システムを不能にする

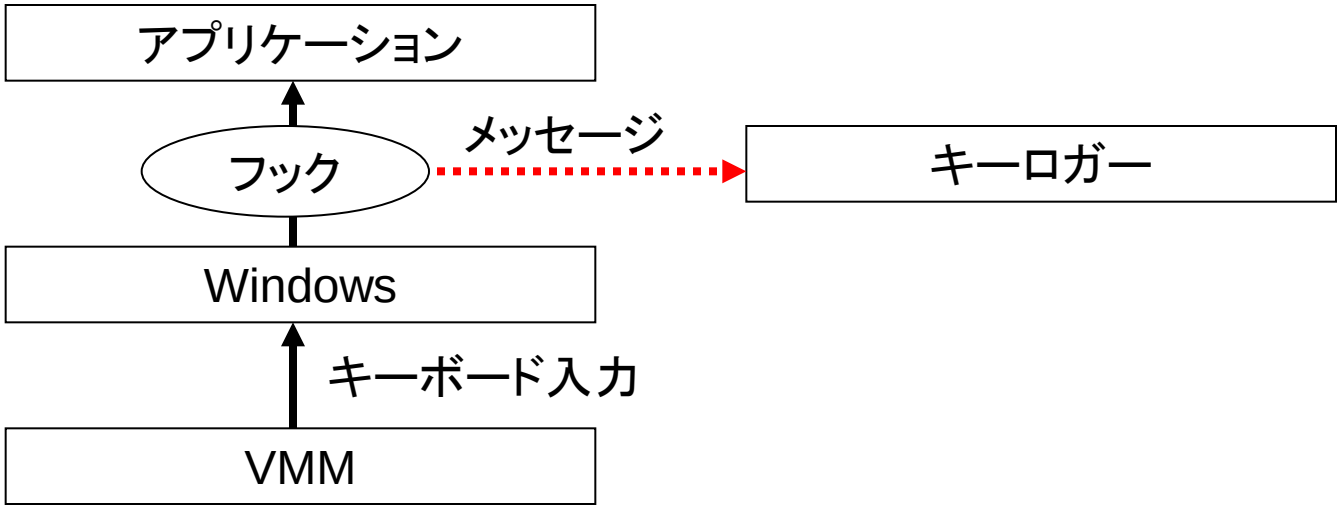
FoxyKBD

- 手動では不可能なほど大量のキー入力を与える
  - VM 上で検証対象システムを動作させる
  - VMM は VM に大量のキーボード割り込みを起こす
  - 仮想デバイスの出力量の変化を解析する
    - キーロガーが存在する場合大量のログが仮想デバイスに出力される
    - 出力が大幅に増加した場合キーロガーが存在すると判断する



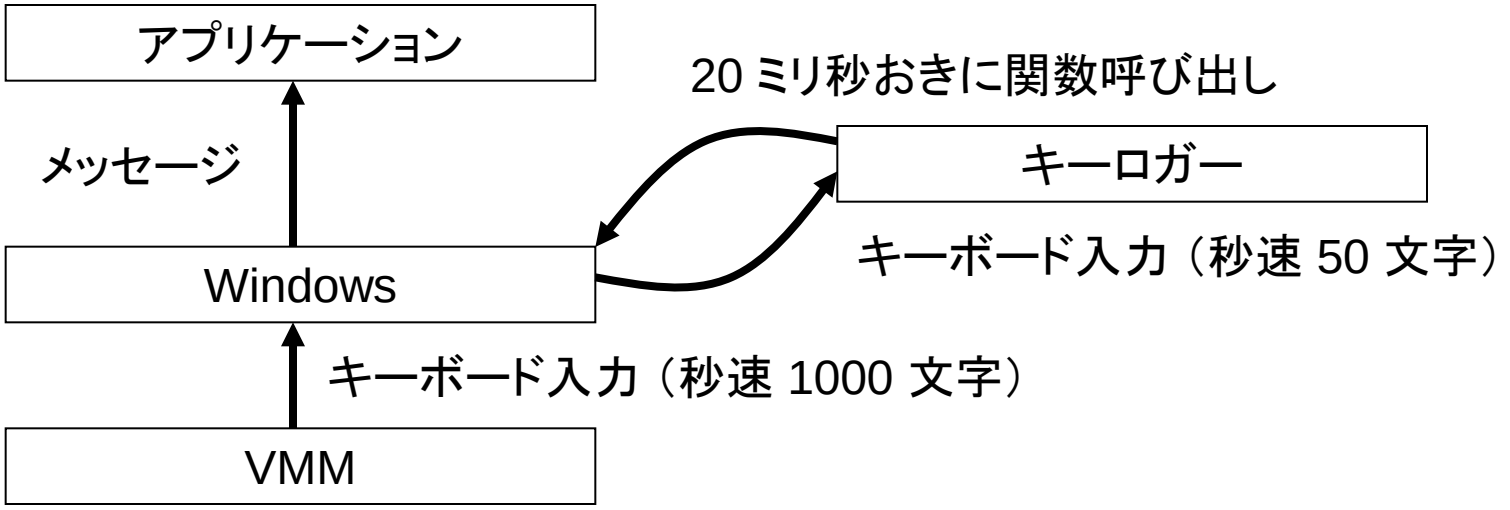
検知が容易なキーロガーのタイプ

- フックを利用してキーボード入力を取得するタイプ
  - SetWindowsHookEx(), フィルタドライバを利用して実装
  - VMMが与えたキーボード入力を全て取得する
  - 大量のキーボード入力を与えられる
  - 例：Family KGB Keylogger Ver. 1.8, All In-One Spy Ver. 2.0, Spy Agent 6.01, Active Key Logger Ver. 3.7.3



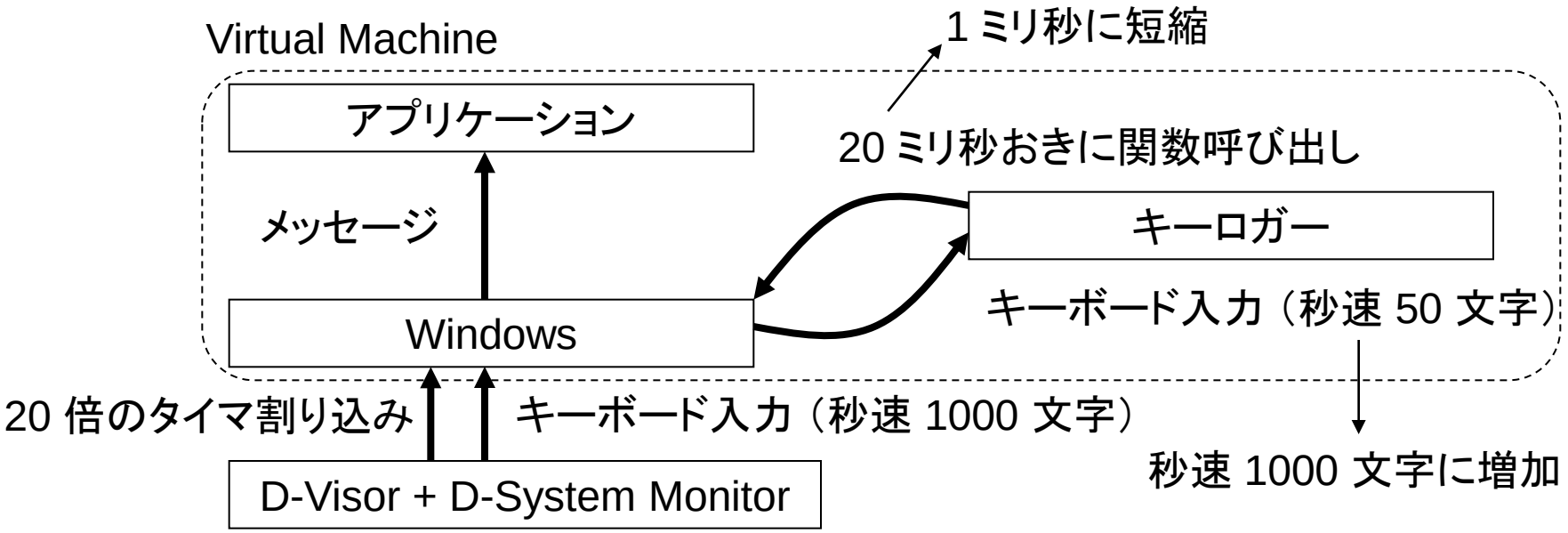
検知が難しいキーロガーのタイプ

- 反復的にキーボード状態を取得するタイプ
  - GetAsyncKeyState() を利用して実装
    - 関数呼び出し時に指定したキーが押されているかがわかる
    - 一定時間おきに関数呼び出しを行う
  - 関数の呼び出し回数がキーボード入力の取得数の上限
    - 関数呼び出しされた瞬間以外の入力は取得されない
  - 検知に十分な入力を与えられない可能性がある
  - 例：All In One Keylogger Ver. 2.8, LoggerA, キーロガー Ver. 1.5.0



解決手法

- 監視対象 OS の内部時刻を加速する
  - VM のタイマ割り込み間隔を短縮する
  - 関数呼び出し間隔が短縮される
    - 単位時間あたりのキーボード入力の取得数が増える
    - VM の外側から見たとき，取得数と出力の増加が期待できる



実験

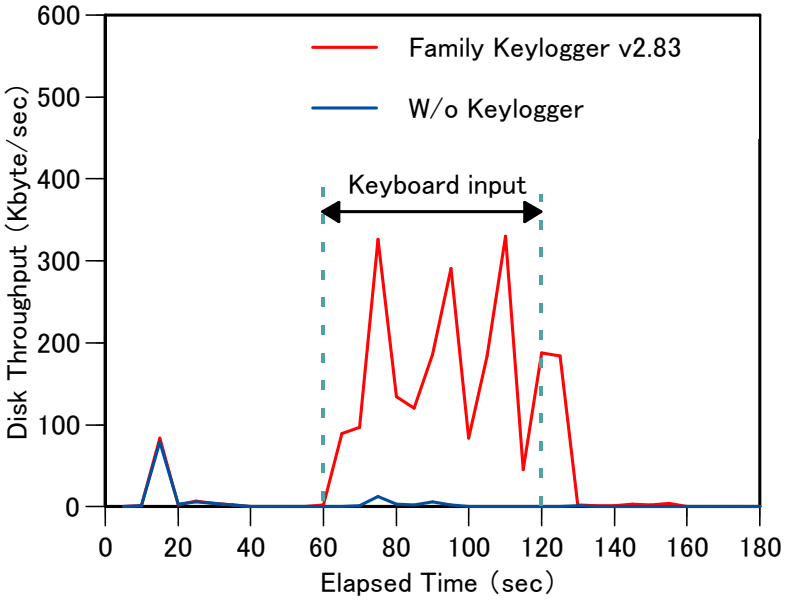
- 検知精度の評価
  - 56 種類の実際のキーロガーと 8 種類のキーボードユーティリティに対して実験
    - 全て常駐してキーボード入力を取得する機能を持つ
  - 提案システムを用いて 60 秒間に約 3 万文字を入力

- 実験環境
  - CPU　Core2Duo 1.8GHz
  - 物理メモリ　2GB
  - ホストOS　Linux 2.6.19
  - ゲストOS　Windows XP
  - ゲストメモリ　128MB

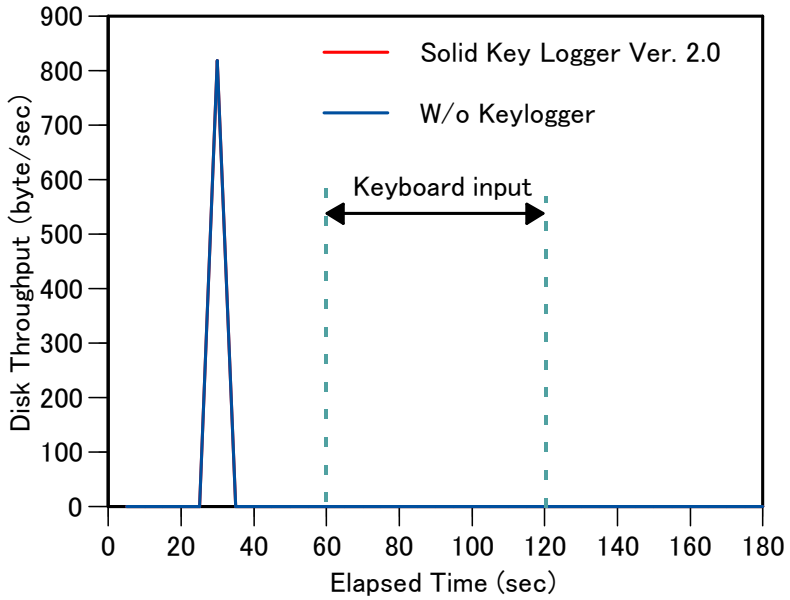
実験結果

- 55 種類のキーロガーを検知した
  - ファイルにログを保存しないキーロガーを検知できなかった
- False positive 無し
  - キーボードユーティリティはほとんど出力しないため誤検知されなかった
- ネットワーク出力は計測されなかった
  - 取得した情報を直ちにネットワークに送信する仕様ではないため

検知できたキーロガー

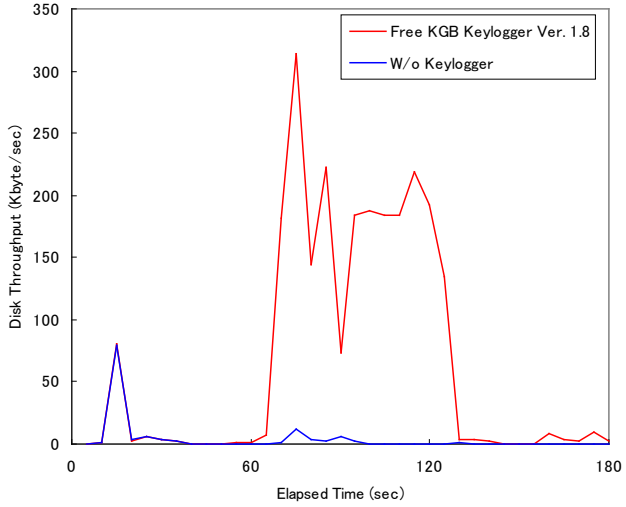


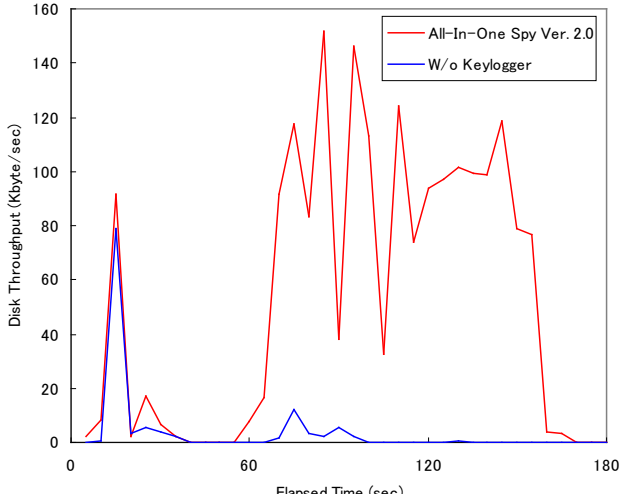
検知できなかったキーロガー

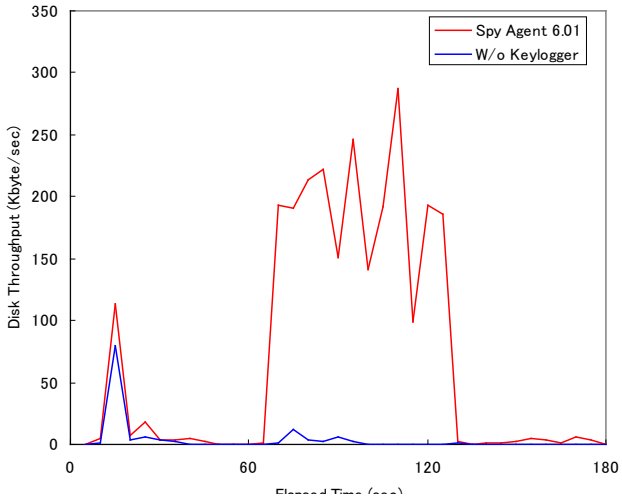


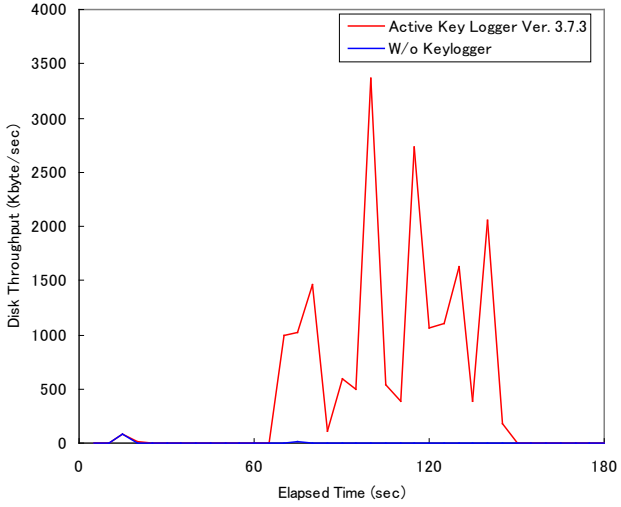
検知できたキーロガーの例

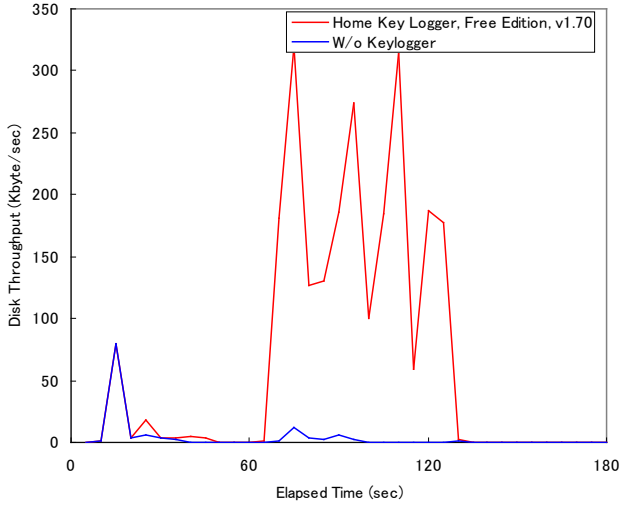
sslab system software

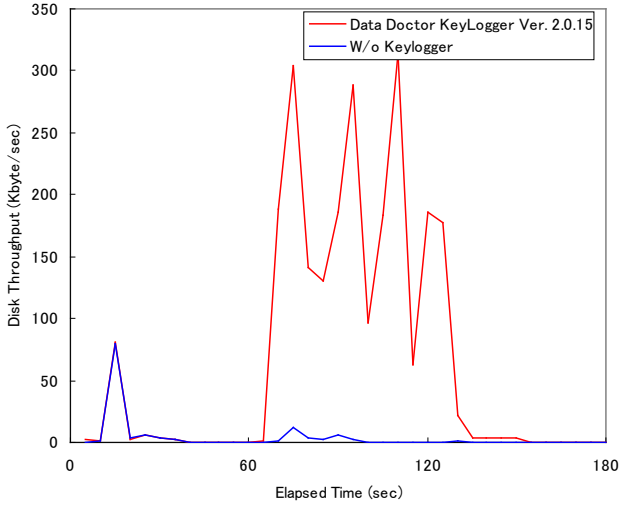












まとめ

- 進化するマルウェアへの仮想マシンからの挑戦
  - マルウェアの“振る舞い”に着目
    - 感染したOSの“振る舞い”は健全な振る舞いとは違うはず
    - 振る舞いがまったく変わらなければ，感染していないのと同じ
  - 仮想マシンによりOSの“振る舞い”を監視
    - 健全な振る舞いとは違う“振る舞い”を発見する
- これまでの成果
  - ファイル隠蔽，キーロガーが検知できる
  - 他にも，
    C&C型のボット，アドウェア，偽アンチウィルス，・・・
    などが検出可能