全体発表 10/18

島本 大輔

2005年10月18日(火)

今回の発表内容

- 自分の研究
  - System Service 監視による Windows 用 IDS
- Google にインターンしてきました

これからのセキュリティ対策

- シグネチャのパターンマッチでは不十分
  - ゼロデイアタックを防げない
- シグネチャからビヘイビアへ
  - 「単純なパターンマッチ」ではなく、「妙な振る舞い」を検出
    - ファイル、レジストリの改変
  - SymantecのWhole Security買収
  - Panda Softwareの台頭

目標

- 『UNIX系OSにおける先進的なIDSの研究をWindowsへ応用』

既存のIDS

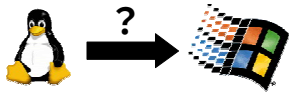
- UNIX系OSにおけるIDS
  - 様々な先進的な研究が多数
  - 現在も増殖中
- 既存のWindows用IDS
  - Signature based が主流＝新種への対応が困難
  - 研究は少数

UNIX系OSにおけるIDS

- プロセスの様々な情報を監視
  - [Forrest 96]
    - system call 列を監視
  - [Sekar 01]
    - プログラムカウンタを監視
  - [Feng 03]
    - スタックを監視

Windowsへの応用

- UNIXの技術をWindowsへ応用？
  ⇒ 困難
  - ブラックボックスな OS
  - 公式に提供されているモジュールでは不十分



目標

- 『UNIX系OSにおける先進的なIDSの研究をWindowsへ応用』

➡ Windowsでsystem callの情報を使って異常を検出

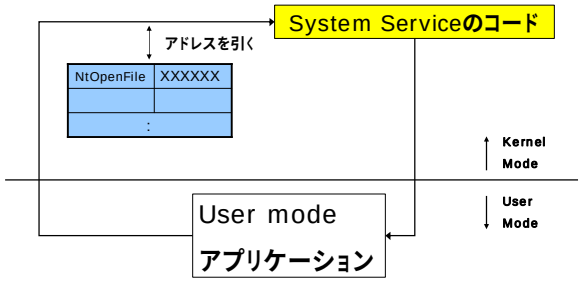
研究内容

- Windowsにおける先進的なIDS
  - System Service (Windows版system call) を利用して、異常を検知

System Service

- Windowsの根本的な機能を提供
  - ファイル、レジストリ、プロセス、スレッド
    タイマー、mutex、GDI
  - 例：NtWriteFile — ファイルへの書き込みは
    すべてこれを利用
- 数は非常に多い
  - 286個 (Windows 2000)
  - 991個 (〃 XP SP1)

System Serviceの動作



System Service Interception

- 2通りの手法が存在
  1. SSDT Patching
  2. Interrupt Hooking

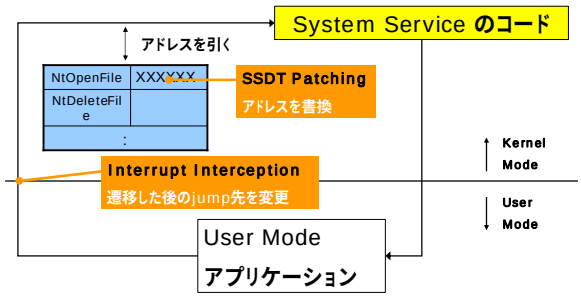
SSDT Patching

- System Serviceのアドレステーブル (System Service Descriptor Table) 内のリストを書き換え
- System call tableの書き換えと同様
- ただし、大量のコーディングが必要
  - System Service 1つあたり、1つの関数を定義

Interrupt Interception

- Kernel modeへ遷移する瞬間に intercept
  - Windows 2000以前ではソフトウェア割り込み (int 2e)
  - Windows XP以降はSYSENTER

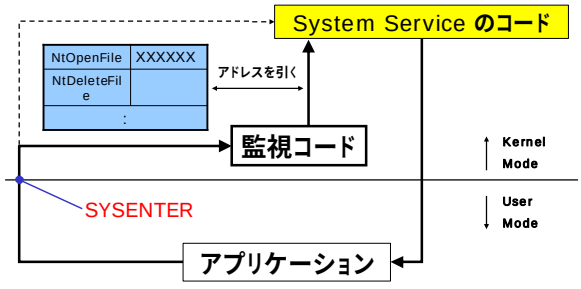
System Service Interception



System Service Interception

- Interrupt Interception を採用
  - 既存研究が少数
  - 1ヵ所において監視可能
    - SSDT patchingでは監視コードが散在
  - 監視する System Service の追加･削除が容易

System Service の Interception



実装内容

- デバイスドライバ部分
  - Interception コードの挿入･取り外しを担当
  - Kernel mode で動作
- GUI プログラム
  - デバイスドライバの操作を担当
  - User mode で動作

デバイスドライバ部分

- 基本的にC言語で記述
  - SYSENTER_EIP_MSRの書き換えは インラインアセンブリ
- 挿入するコードもデバイスドライバの 中に存在
  - Kernel内なので、コードのアドレスはどこでも 同じ

GUIプログラム

- デバイスドライバの操作
  - 挿入、削除
- デバイスドライバとの通信
  - ログをデバイスドライバから読み出し、出力
  - InterceptするSystem Serviceの変更を デバイスドライバに伝達

問題点

- Interrupt Hooking の弱点
  - Kernel mode内からのSystem Serviceの 呼び出しを監視不可能

→
- SSDT patchingの導入？
- ターゲットをUser modeプログラムに限定？

まとめ

- モチベーション
  - Windows における先進的なIDSの実装
- 研究内容
  - Interception の手法を調査･実装
  - ウィルスなどのパターンを取得

質疑応答1

今回の発表内容

- 自分の研究
  - System Service 監視による Windows 用 IDS
- Google にインターンしてきました

Google

- 1998 年スタート（今年7年目）
- No.1 とされている検索サイト
  - 中国では baidu.com の方が上
  - 日本では Yahoo! Japan の方が上
- 去年のIPOと先月の新株発行で資金は豊富

最近のGoogle(1)

- Sun と提携
  - 単純にソフトの相互リンク？
- NASA と提携
  - 土地を間借り
- AOL 買収？？
  - ユーザー数の獲得
- Google.org
  - Google の寄付団体

最近のGoogle(2)

- 製品
  - Blog Search
    - http://blogsearch.google.com/
  - Google Desktop 2
    - http://desktop.google.com/
  - Google Talk
    - http://www.google.com/talk/
  - Personalized Homepage
    - http://www.google.com/ig/

環境

- 食事
  - 1日3食
  - 土日も軽食あり
  - スナックコーナー
- 生活面
  - ジム、マッサージ、（無限）プール付き
  - 洗濯・乾燥機あり
  - 医者、床屋、オイル交換、自転車改良
  - San Francisco と San Jose からの専用バス

文化

- （中では）オープン
  - 外に情報を出さない
- 雰囲気を重視
  - Offsite（課外イベント）
  - その他のイベント
- 人種・年齢・性別など関係なし
  - アメリカ全体に言えることかも

開発状況

- 発言についてはNDAで厳しく制限
  - 自分のプロジェクトについて話せません
- 小さいプロジェクトが多数
  - 各プロジェクトが5〜8人
- 全員が同一のレポジトリ
  - 他プロジェクトのソースコードへアクセス可
  - インターンですらほぼアクセス可

Googleの問題点

- とにかく人が多い
  - 週50～90人ペースで増殖
  - スペースのクレームが多数
  - レポジトリがゴチャゴチャ
- バブル状態
  - どんどん膨らんでいる
  - 周りには破裂した企業もたくさん……
- 日本を軽視している感が…

Googleのこれから

- Webのすべてをインデックス化
- すべてをWebで
  - クライアントPCは端末化
  - ブラウザの機能拡張に意欲的

インターンシップ

- プロジェクトに放り込まれる
  - 文字通り「放り込まれる」
  - 自分から動かないと何も始まらない
- 内容
  - Windowsのクライアント作成
  - 詳しくは製品が出てから…

感想

- いい経験
  - 企業の中を知ることができた
  - 様々な人との交流
  - 仕事としての開発
  - アメリカの生活を知ることができた

質疑応答2