クライアントアプリケーションの攻略

株式会社ラック
新井 悠
y.arai@lac.co.jp
http://www.lac.co.jp/security/

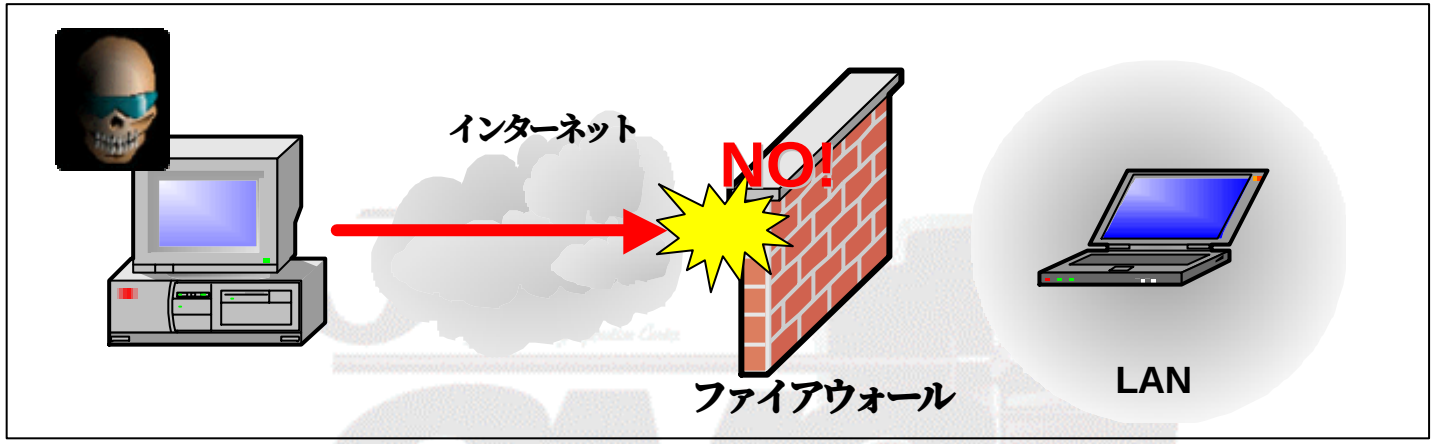
- クライアントアプリケーションの攻略とは？

  – クライアントNサーバ方式において、クライアントとして動作するアプリケーションを利用し、攻撃を発現させること

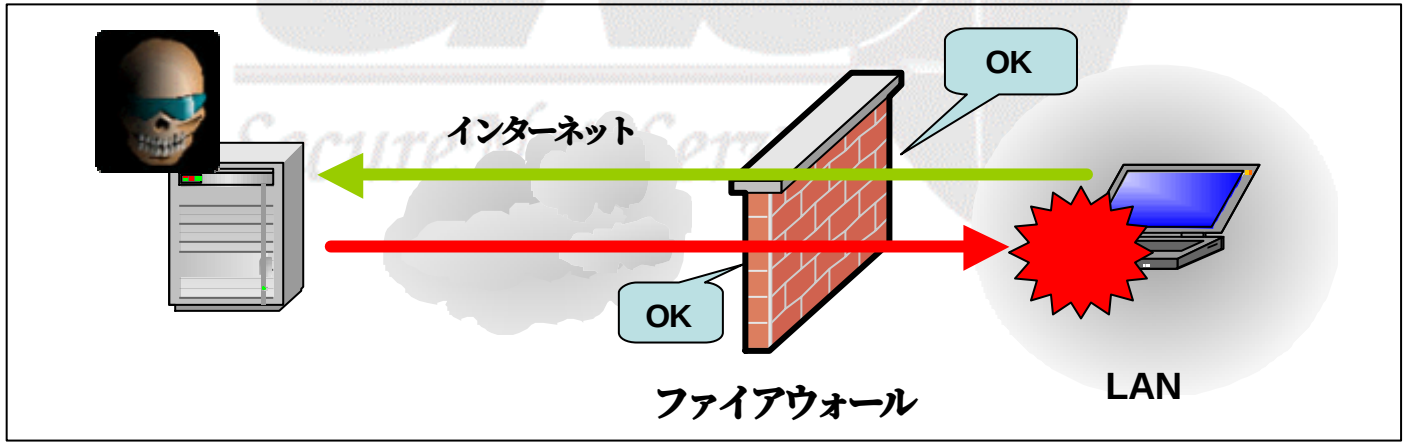
  – 標的となるのは、Webブラウザ、MUA、FTPクライアント、telnetクライアント、あるいはウイルス対策ソフトなど。。。

- どうやったらできるの？
  - 標的となるアプリケーションに悪意あるデータの送受信を行ってもらうこと(受動的な攻撃)
  - 悪意あるデータの送受信は、ユーザがなにげなく行ったことで引き起こされることが多い:
    - ハイパーリンクのクリック
    - サーバへの接続
    - 電子メールの受信
  - つまり、そうとは知らずに被害を受けてしまうことがあります!

能動的な攻撃」はファイアウォールで遮断される公算が高い



受動的な攻撃」はファイアウォールを通過してしまう可能性がある



■攻撃の種類(1)

セキュリティホールを利用する

例:

- 不適切な MIME ヘッダーが原因で Internet Explorerが電子メールの添付ファイルを実行する (MS01-020)

  ⇒ “Klez”や”BugBear”,”Sobig”などのウイルスが利用

- 2002 年 2 月 11 日 Internet Explorer の累積的な修正プログラム (MS02-005)に含まれる:
  Document.Open機能による「フレームのドメイン照合」の変種

  ⇒ 2002年 2月”CoolNow”ウイルスが利用

■攻撃の種類(2)

機能や仕様を利用する

例:

- ActiveX コントロール

  •知らないうちにダイヤルアップネットワークの設定を書き換えられてしまい、高額な利用料金の請求が届いた、など。。。

攻撃の実例

-IE&WMP-

■ Windows Media Player(WMP)

- 最新版はバージョン９

  http://www.microsoft.com/japan/windows/windowsmedia/

- Windows 98, ME, 2000, XP に付属

- 動画や音楽の再生、インターネットラジオの受信などの用途

攻撃の実例 -IE&WMP-

■ ファイルが自動実行されるセキュリティホール

- www.malware.comの http-equiv (グループ名?)によって2002年の 8月に発見される
  - the!STENCH
    http://www.malware.com/stench.html
- (きっと)あまり知られていない。。。

攻撃の実例 -IE&WMP-

■攻撃の実際

1. Windows Media Download (WMD) Packagesファイルを利用

2. WMP 7.0 および 7.1 では、ダウンロードされた WMD ファイル(が解凍されたファイル)が設置されるパスが推測可能

3. IEにWebページを読み込ませ、OBJECTタグのCODEBASE属性に上記パスを指定させてファイルを実行させる

攻撃の実例 -IE&WMP-

■発見者に問い合わせてみたところ・・・

- 問題の根源はIEがOBJECTタグのCODEBASE属性に対して異常な解釈を行うところにある

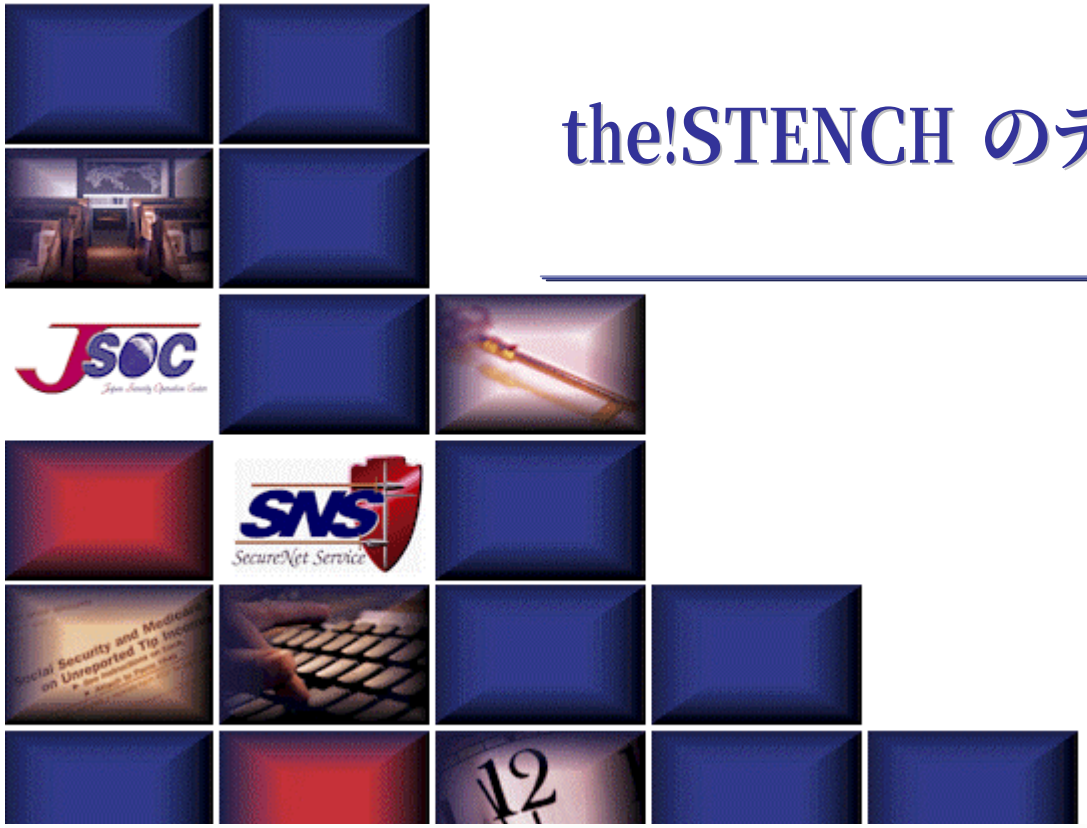
  過去、GreyMagic Software が報告した
  “GreyMagic Security Advisory GM#001-IE”が発端

  最近(2003年 2月)彼らが発表した
  ”Self-Executing HTML: Internet Explorer 5.5 and 6.0 Part II” も、この異常な解釈を利用している

攻撃の実例 -IE&WMP-

■影響を受ける環境(確認できたもの)

- Windows 2000 Pro. + SP3 + IE 5.5 SP2 + WMP 7.1 + パッチ全部
- Windows 2000 Pro. + SP3 + IE 6 SP1 + WMP 7.1 + パッチ全部



the!STENCH のデモンストレーション

■この問題への対策

- IEの[インターネットオプション]の設定から[アクティブスクリプト]を[無効]にする
- IEの[インターネットオプション]の設定から[ファイルのダウンロード]を無効にする
- WMP 9 へのアップグレード
  - WMD ファイルが格納されるディレクトリ名がランダムな8文字へと変更される
  - ただしhttp-equiv 曰く「根本的な解決ではないだろう」

クライアントコンピュータを守るために

クライアントコンピュータを守るために

- 脅威は、どんなソフトウェアにも潜んでいる
- Windows をご利用の皆さんは、WMP9へのアップグレードをお忘れずに。。。

参考文献

Unpatched IE security holes
http://www.pivx.com/larholm/unpatched/

malware.com
http://www.malware.com

GrayMagic Software
http://sec.greymagic.com/news/

謝辞

Thanks to:
http-equiv of malware.com