日本ネットワークセキュリティ協会技術部会

不正アクセス研究ワーキンググループ

２００１年度活動報告

日本ネットワークセキュリティ協会

WGのこれまでの活動

- 昨年度は「不正アクセス調査ワーキンググループ」として、不正アクセス手法や事例、動向などの調査を行ってきました。
- 今年度より「不正アクセス研究ワーキンググループ」として、テーマを絞ってより深く各種不正アクセス手法の調査研究を行っております。

WGのこれまでの活動

- 今年度はこれまで5回のミーティング（合宿含む）を実施、3つのテーマでの調査研究を行ってきました。
  - （1）バッファオーバーフロー攻撃
  - （2）セッションハイジャック
  - （3）IIS

WGの今後の活動

- 今後のテーマ（予定）
  - DDOS
  - ソーシャルエンジニアリング
  - トロイの木馬
  - スキャナー
  - 盗聴
- ミーティング（月1回ペース）、（合宿）

テーマ発表：IIS

- IISは危険であると言われていますが、いったい何がどう危険なのか？
- IISに関する不正アクセスの手口にはどんなものがあるのか？
  - Unicodeバグ
  - インターネットプリンターAPIバグ
  - Nimda
  - Code Red
  - Reverse telnet手法の取り込み

Unicode

- Unicodeは、全世界の文字を１６ビットでマッピングしたもの。
- WindowsのUnicodeがどのASCIIに対応しているか探す方法は
  - http://IIS_Server/A.ida/%2e.ida
    - 結果：“ファイル ..ida. 指定されたパスが見つかりません。”→“%2e” は “.”

IIS Unicodeバグ

- IISは “../” を指定すると上位ディレクトリへの移動を許可します (設定によって回避可能) 。
- ただ、URLに直接“/”を指定しても、“2f”にデコードされるだけです。
  - URLでUnicode “%c0%af” は “/” とデコードされます。
  - したがって、“..%c0%af” と記入すると、“../“ と解釈してしまいます。
- “%c0%af” 以外にも “/” にデコードされるものがあります。

Unicodeバグを利用した攻撃

- Unicodeを利用した攻撃は、ブラウザで次のようにURLを指定するだけです。
  - (1) “cmd.exe”のコピー
  - http://site/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+..¥..¥winnt¥system32¥cmd.exe+cmd1.exe
  - (2) ファイル内容の変更
  - http://site/scripts/..%c0%af../inetpub/scripts/cmd1.exe?/c+echo+abc+>aaa&dir&type+aaa

プリンターAPIのバグ

- Internet Services Application Programing Interface (ISAPI) **によってIISに拡張機能を提供する。**
- **IISがインストールされると、いくつかの**ISAPI**がエクステンションされるが、その中の**idq.dll、ida.dll**は、入力データのバウンドエラーや文字列長のチェックを行っていないため、オーバフローの脆弱性が存在する。**

プリンターAPIのバグ

- IIS 4.0 、IIS 5.0**のインストールで、** idq.dll **がインストールされるため、世の中の多くの** IIS 4.0 / 5.0 **に危険が存在すると考えられる。攻撃者は、**Web**セッションを確立できれば、この脆弱性を利用できるため、ファイアウォールでは防御できない。**

プリンターAPIのバグ：対処方法

- 攻撃者はターゲット上で意図するコードが実行できる。システム権限の奪取が可能であり、Webページ改ざんも容易である。CodeRedは、このセキュリティホールを利用していた。
- 修正プログラムの適用の他、.idq および .ida のスクリプトマッピングの削除、IISの稼働停止など。

nimda:感染方法

- Webブラウザを利用/電子メールを利用
  - 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)
- ネットワーク共有
- IISのunicode脆弱性を利用
  - 正規化エラーによる、ファイルへの誤ったアクセス権の適用 (MS00-057)
  - Web サーバー フォルダへの侵入 (MS00-078)
  - Web サーバーによるファイル要求の解析 (MS00-086)
  - 不要なデコーディング操作により IIS でコマンドが実行される (MS01-026)

nimda:感染方法

- Webブラウザを利用/電子メールを利用
  - Nimdaワームは感染した、IISサーバ上のページをReadme.emlファイルダウンロードするように改ざん（JavaScriptを追加する)
  - Readme.emlは添付ファイルつき電子メール(MIMEヘッダー＋Readme.exe)
  - MIMEヘッダーには、添付ファイルが音声ファイル(audio/x-wav)としてあるためブラウザが音声ファイルと認識し、Readme.exeを実行する。
  - Outlookのプレビュー機能はIEを使用しているため、上記の手法で可能

nimda:感染方法

- ネットワーク共有
  - 感染時には、%$ として各ドライブ (ネットワーク共有ドライブ含む) にコピーを作成しネットワーク共有させる。
- IISのunicode脆弱性を利用
  - 感染したコンピュータはIPアドレスをスキャンしてIISが実行されているサーバを検索(ランダムにHTTP Getリクエストを送信)
  - IISサーバを見つけたらunicode脆弱性を利用してTFTP.EXEを利用可能にしてワームをコピー
  - 同時にCodeRedが作成したバックドア利用も試みる。

Code Red

- Windows 2000シリーズで IIS(Internet Information Server) 5.0 (または4.0)を利用し、Indexing Serviceをインストールしているもののうち、MS01-033修正パッチを未適用Windows NT 4.0 + IIS 4.0 (または5.0)を利用し、Index Server 2.0をインストールしているもののうち、MS01-033修正パッチを未適用は影響を受けます。
  - Indexサービスを利用していなくても拡張子マッピングが生きていれば影響を受けてしまいます。

Code Red:攻撃パケット例

- "GET/default.ida?NNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNN%u9090%u6858%ucbd3%u7801%u909
0%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b
%u53ff%u0078%u0000%u00=a

Code Red：影響と手法

- Windows 2000 + IISの場合は、感染して自身を広めようする。Windows NT 4.0 + IIS等の場合は感染ではなくシステムないし IISをクラッシュ（システム変更がWindows 2000 用）
- cmd.exeをIISのスクリプト用ディレクトリなどにroot.exeとしてコピーする。また、c:\, d:\, \msadc, \Scriptsの各ドライブ、ディレクトリを読み込み・書き込みの可能(,,217)な仮想ルートとしてマップする。
  これがバックドアとなり、任意の侵入者が任意のコマンドを実行できる

Code Red：影響と手法

- c:\とd:\(存在する場合)にexplorer.exeというファイル名のトロイ の木馬を置き、上記の仮想ルートを設定し、かつ、それを継続的に維持しようとする。
- このトロイの木馬プログラムはまた、システムファイルの保護機能を無効にし、書き換えを可能にする。

Code Red：感染手順

- 感染したホストのIPアドレスを取得し、それを元に攻撃先IPの生成が行なわれる。
- 自己流布のために攻撃パケットを送信
- トロイの木馬を設置
- Code Red IIはメモリ上にあるため、リブートした時点で攻撃パケットの送信もなくなる。しかし、この時点で既にバックドアとトロイの木馬が設置されているため、システムは任意の侵入者が任意のコードを実行できる環境になっており、きわめて危険な状態である。再起動後、再びCode Red IIに感染する可能性が高い。

Code Red：自己流布

- 2分の1(4/8)の確率で、感染ホストと1オクテット目が同じIPアドレスをランダムに
- 8分の3の確率で、感染ホストと最初の2オクテットが同じIPアドレスをランダムに
- 8分の1の確率で、感染ホストのIPアドレスとは無関係にIPアドレスを生成するし、攻撃。
- この攻撃によって他ホストへの接続に成功すると、自身のコピーを送りつける。

Code Red：バックドア設置

- cmd.exeを次の2箇所にroot.exeとしてコピーする。
- c:￥inetpub￥scripts￥
- c:￥Program Files￥Common Files￥System￥MSADC￥
- c:\にexplorer.exeという名前のトロイの木馬を置く。これは保護されたシステムファイルとなっており、通常では表示されない。
- 上記をd:\ドライブに対しても繰り返す。d:\ドライブがなければただ失敗するだけ。

Code Red：侵入後の動作

- c:\explorer.exeならびにd:\explorer.exeとして作成されたトロイの木馬プログラムは次のような条件で動作する。
- システムがリブートされるまでは実行されない。
- リブート後も、Administratorないしそのグループに所属するユーザがログオンするまで実行されない。
- SP2がインストールされておらず、MS00-052で提供される修正パッチも適用されていない(MS00-052の修正パッチはWindows 2000 SP2に含まれている) 場合しか実行されない。これはこうした修正モジュールが適用されている場合は、explorer.exeが必ず、本来の場所にあるものが優先的に起動されるのに対して、こうした修正モジュールが適用されていない場合は、トロイの木馬であるc:\またはd:\のexploer.exeが先に実行されるためである。

Code Red：侵入後の動作

- このトロイの木馬のexplorer.exeが実行されると、次のような活動を無限に繰り返す
- このレジストリ項目の値を 0FFFFFF9Dh に設定する。これにより、システムファイル保護機能 (WFP, Windows File Protection) が無効となり、書き換えの監視が行なわれていたはずのシステムファイルも書き換えが可能になる。
  - SOFTWARE￥MicrosoftWindows NT￥CurrentVersion￥Winlogon￥SFCDisable

Code Red：侵入後の動作

- 次の4つのレジストリ項目(がなければ作成され)の値が217に設定される。
  - SYSTEM￥CurrentControlSet￥Services￥W3SVC￥Parameters￥VirtualRoots￥Scripts
  - SYSTEM￥CurrentControlSet￥Services￥W3SVC￥Parameters￥VirtualRoots￥msadc
  - SYSTEM￥CurrentControlSet￥Services￥W3SVC￥Parameters￥VirtualRoots￥c
  - SYSTEM￥CurrentControlSet￥Services￥W3SVC￥Parameters￥VirtualRoots￥d
- ここで指定された.\scripts, .\msadc, c:\, d:\の各ディレクトリ、ドライブが仮想ドライブとしてネットワーク上に公開され、217は読み込み、書き込み、実行を許可している。
- 10分間休眠し、その後、同じ活動を永遠に繰り返す。

Code Red：対処方法

- c:￥explorer.exe、c:￥inetpub￥scripts￥root.exeやc:￥Program Files￥Common Files￥System￥MSADC￥root.exeがあれば確実に感染している。
- 感染を確認したら、いったんインターネット/ネットワークから切り離し、OSから再インストールする以外対処方法は無い。バックアップもいつの時点から感染したか特定できない限り信用できないものと考えるべきである。

reverse telnet

- **通常telnetは接続したい側（クライアント）からサーバーに接続します**
- **reverse telnetと呼ばれる接続方法はサーバーからクライアントに接続させる手法です**
- **接続方法を逆にすることで、ファイアウォールのフィルタルールをかいくぐることができます**

reverse telnet

- IISのセキュリティホールを突くプログラムのなかにも、このreverse telnet的手法を取り入れているコードがあります
- 最近発表されたjim.cというプログラムは、この手法を使ってIISサーバーに侵入するものです

Jim.c

- Jim.cが利用するのは、IISのサーバーサイドインクルードの機能です
- サーバーサイドインクルードの機能とは、サーバーの内部コマンドなどを使いながら、動的にWebコンテンツを作成するものです。一般的にインターネットでは危険であると言われています

Jim.c

- Jim.cはiis.shtmlというファイルを作成します。このファイルはサーバーサイドインクルード機能を呼び出すものですが、そこに攻撃者のマシンと攻撃者側の待ち受けポートの情報が埋め込まれています。そのファイルを何か別の手段（笑）でIISサーバーに送り込み、ブラウザからそのファイルを呼び出すことで初めて侵入できるようになるわけです。

Jim.c

- **したがって攻撃者がわは待ち受け用通信ポートを開けて待っている必要があります。**
- **待ち受けには**netcat**を使います。**
  - nc -l -p <attacker port> -vv

Jill.c

- Jill.cというプログラムはインターネットプリンターサービスを利用するプログラムです
- Jim.cと異なり、インターネットプリンターサービスに対し直接攻撃コードを送り込みますので、iis.shtmlのようなファイルをIISサーバーにコピーする必要はありません
- 待ちうけにはjim.cと同様にnetcatを使います。