Empowered by Innovation NEC

資料8－4

# Malwareに関する調査研究2007年度

## Linuxシステムにおける
## Malwareの脅威に関する調査研究

# LinuxシステムとMalware

- Linuxシステムの増加
  - Webサーバ等、サーバシステムとしての利用に加え、クライアントシステムとしての利用も増加。
  - 数が増えれば攻撃ターゲットとしての旨みが増すため、攻撃が増える事が予想される。
- Linuxで動作するMalwareの実態
  - Windows向けMalwareについては実態調査が行われているが、Linux向けについては現状調査不十分。
  - Linux向けのMalwareをターゲットとしたAntiVirusは非常にマイナー。現在のWindows向けにあるような一般向けのAntiVirusソリューションが無い。
- Linuxのサーバ機能の悪用
  - フィッシングコンテンツやMpack等で作成された攻撃コードの設置。
  - C&Cサーバとして利用されているケースも。

# 調査対象

- 外部からのアクセス・侵入方式
- Malware等の設置・実行方式
- 設置されたMalwareの機能・種類

# 外部からのアクセス・侵入方式の調査

- 調査条件
  - IPアドレスは一般ユーザが利用する空間を利用。
  - １日毎にIPアドレスはリナンバする。固定にしない。
  - 基本的に、全ポート開放でアクセスチェック。一部一般的なサービスについては、サーバを起動し、アクセスログを採取。
  - 2007/10/01～2007/10/31のアクセスログから、アクセスを分類。

# 侵入方式調査(結果-サービス)

- サーバ系アクセス結果(非Windows固有)
  - sshアクセスが圧倒的に多い。ただし、アクセス自体はBruteForce(総当り攻撃)で同一IPからのものが多数のため、接続元IP数ではhttpアクセスと同等。
  - httpが次いで多いが、今回は脆弱性を設定していないので繰り返しのアクセスは無い。

| サービス(サーバ系) | Port番号 | 全アクセス数 | 接続元アドレス数 |
|---|---|---|---|
| ftp | 21 | 43 | 30 |
| ssh | 22 | 168298 | 364 |
| telnet | 23 | 34 | 13 |
| smtp | 25 | 143 | 61 |
| DNS | 53 | 32 | 26 |
| http | 80 | 347 | 303 |
| pop3 | 110 | 5 | 3 |
| sunrpc | 111 | 3 | 3 |
| https | 443 | 55 | 22 |
| Socks | 1080 | 43 | 19 |
| Proxy | 8080 | 268 | 41 |

# 侵入方式調査(結果-SSH BruteForce)

- SSH Brute Force の攻撃対象アカウント
  - rootアクセスが圧倒的多数。
  - それ以外はtest、admin、guest等、デフォルトでありそうなアカウントが試される。
  - 下表のアクセスは件数。

| アカウント | アクセス |
|---|---|
| root | 30927 |
| test | 2859 |
| admin | 2777 |
| guest | 1380 |
| user | 1292 |
| mysql | 899 |
| oracle | 789 |
| postgres | 757 |
| a | 750 |
| ftp | 646 |

| アカウント | アクセス |
|---|---|
| webmaster | 578 |
| adm | 523 |
| nobody | 497 |
| tester | 495 |
| info | 470 |
| web | 395 |
| student | 383 |
| testing | 382 |
| apache | 375 |
| amanda | 364 |

| アカウント | アクセス |
|---|---|
| sales | 357 |
| www | 353 |
| administrator | 320 |
| mail | 319 |
| postfix | 318 |
| cyrus | 314 |
| alex | 312 |
| sshd | 308 |
| paul | 307 |
| games | 307 |

# 侵入方式調査(結果-HTTP)

- HTTPアクセス
  - /(Root Dir)に対するアクセスが大半(非攻撃、サイトの死活監視)
  - XMLRPCの脆弱性を狙った侵入試行あり

| メソッド | アクセス先パス、URL | 回 | 推定されるアクセス対象、目的 |
|---|---|---|---|
| GET | /Ads/adxmlrpc.php | 2 | XMLRPCの脆弱性 |
| GET | /a1b2c3d4e5f6g7h8i9/nonexistentfile.php | 2 | |
| GET | /ads/adxmlrpc.php | 2 | |
| GET | /adserver/adxmlrpc.php | 2 | |
| GET | /adxmlrpc.php | 2 | |
| GET | /blog/xmlrpc.php | 1 | |
| GET | /drupal/xmlrpc.php | 1 | |
| GET | /phpAdsNew/adxmlrpc.php | 2 | |
| GET | /phpads/adxmlrpc.php | 2 | |
| GET | /phpadsnew/adxmlrpc.php | 2 | |
| GET | /xmlrpc.php | 2 | |
| GET | /xmlrpc/xmlrpc.php | 2 | |
| GET | /xmlsrv/xmlrpc.php | 2 | |

# 侵入方式調査(結果-HTTP続き)

- HTTPアクセス
  - Lotus Dominoの脆弱性チェックあり
  - それ以外はProxyアクセス、Robotによるチェックのみ

| メソッド | アクセス先パス、URL | 回 | 推定されるアクセス対象、目的 |
|---|---|---|---|
| GET | /webadmin.nsf | 2 | Lotus Domino webadmin.nsf の脆弱性 |
| POST | /manager/html | 1 | |
| CONNECT | msa.hinet.net:25 | 1 | Proxy(SMTPブリッジ)利用の可否 |
| GET | http://144.135.8.153/ | 1 | Proxy利用の可否 |
| GET | http://activate.qq.com/ | 1 | |
| GET | http://votdomain.com/scaner/test.txt | 1 | |
| GET | http://www.baidu.com/ | 1 | |
| GET | http://www.google.co.jp/ | 1 | |
| GET | /w00tw00t.at.ISC.SANS.DFind:) | 1 | ロボット |
| GET | /robots.txt | 1 | 百度ロボット |

# 転送・設置・実行方式調査

- 調査方式
  - 侵入方法調査でssh Brute Forceが多かったため、sshで侵入し易いようにシステムを調整。
    （ユーザ名＝パスワードで、sshアクセスの上位のアカウント100前後を作成しておく）
  - ホストIPSを利用して、侵入者の行動を制限しつつ、行動を観察。ファイルの転送や展開、実行等に関するログを採取。
- 結果
  - 2008/01/08～2008/01/18に侵入したユーザによるファイル転送を転送方式毎に集計
  - wgetによる転送多数。その他sftp-server、ftp-clientあり。

| 転送方式 | wget | ftp-client | sftpd-server |
|---|---|---|---|
| 試行回数 | 83 | 2 | 4 |

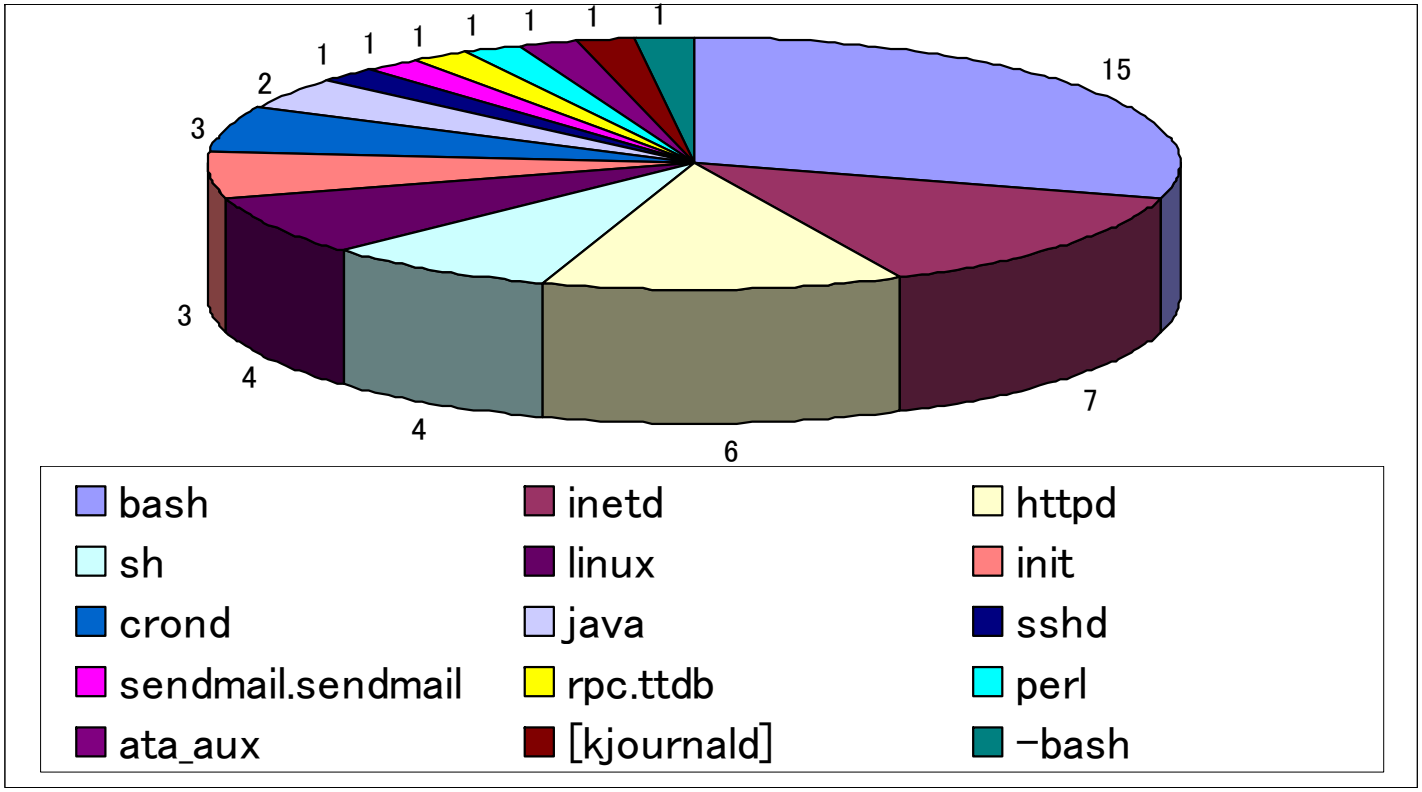
# Malware設置パス調査結果

- Malwareを転送、設置するパスをログから調査
  - /var/tmp、/tmpが多い。
  - 非表示、あるいは表示不正パスの利用がある。下表は利用された表示不正パス、あるいは不可視属性パスの一覧。
  - 表中の□は空白文字を表し、↲は改行コードを示す。

| ファイル転送先一覧（表示不正パス） | | |
|---|---|---|
| /home/a/.n | /tmp/□□ | /var/tmp/□□□□□□□□□□ |
| /home/apple/.ssh | /tmp/.□/.□ | /var/tmp/□/.a |
| /home/ftpuser/□ | /tmp/..□ | /var/tmp/.□ |
| /home/ftpuser/public_html/.□/ | /tmp/.ICE-unix | /var/tmp/..□ |
| /home/jimmy/□ | /tmp/.ICE-unix/.firewall | /var/tmp/..□.□↲ |
| /root/□ | /tmp/.font-unix | /var/tmp/... |
| /root/..□ | /tmp/.font-unix/.UNIX□ | /var/tmp/.o |
| /root/... | /tmp/.ssh | /var/tmp/.o/.sh |
| /root/.wim | /var/tmp/□ | /var/tmp/a/.scr |
| /tmp/□ | /var/tmp/□□ | /var/tmp/spool/app/□□ |

# Malware実行方式調査結果(プロセスの隠蔽)

- Malware転送後、実行時のexecveのログ確認
  - プロセス名をシステムプロセスに偽装するケースがある。
    下のグラフは偽装されたプロセス名の一覧




  - rootkit設置によるプロセス、ファイルの隠蔽もあり。

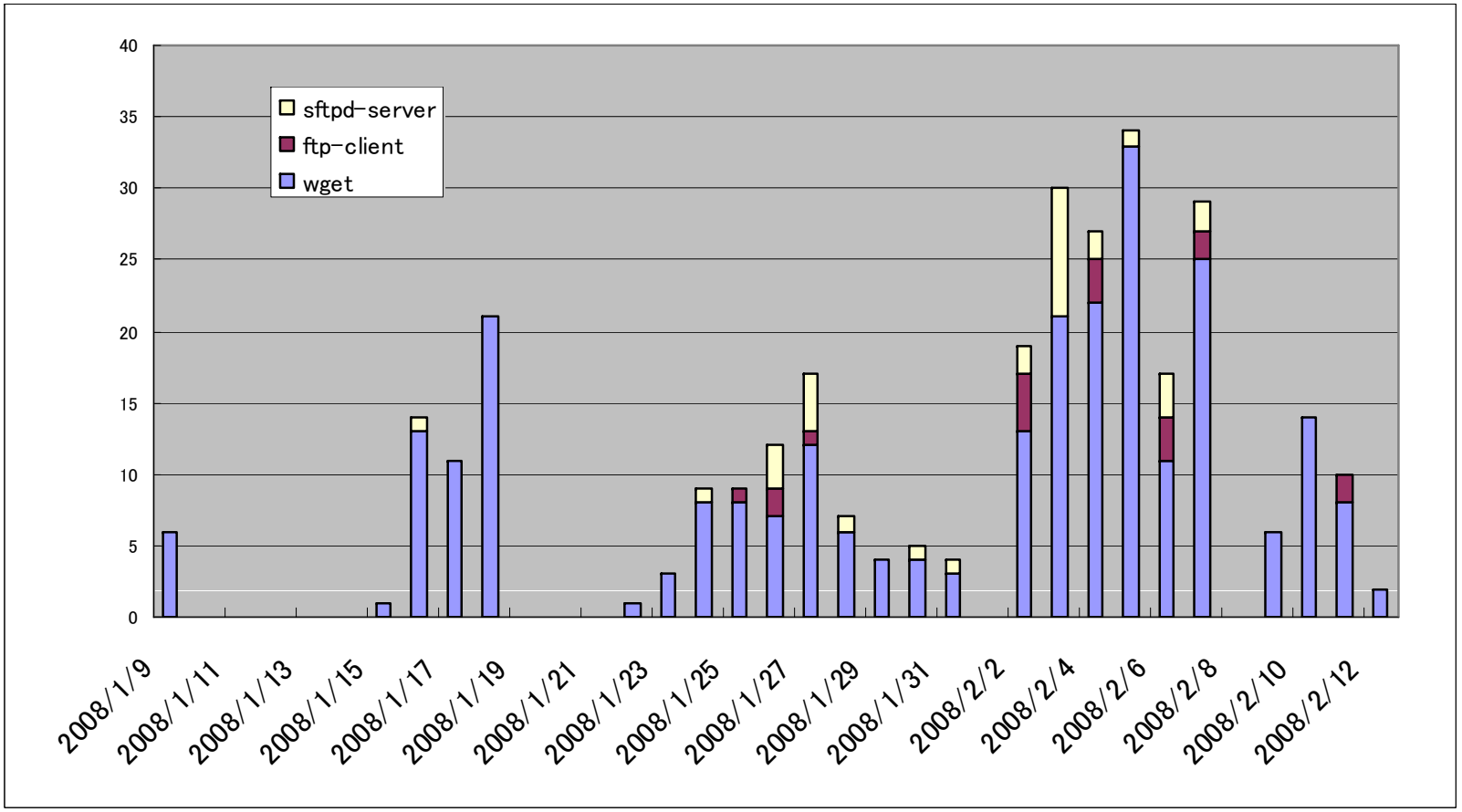
# Malwareの自動回収と分類

- 設置されたMalwareの自動回収
  - ここまでに判明した転送・設置・実行方式に該当する行為をホストIPSにて監視し、設置されたMalware等を自動回収するシステムを構築。
  - 2008/01/09～2008/01/25の２週間でホストIPSのルールを調整しながら試験運用。
  - 2008/01/28～2008/02/12でホストIPSのルールを固定して正式運用。

- Malwareの機能・種類を分類
  - 設置されたMalwareを分析、その機能や種類を分類する。

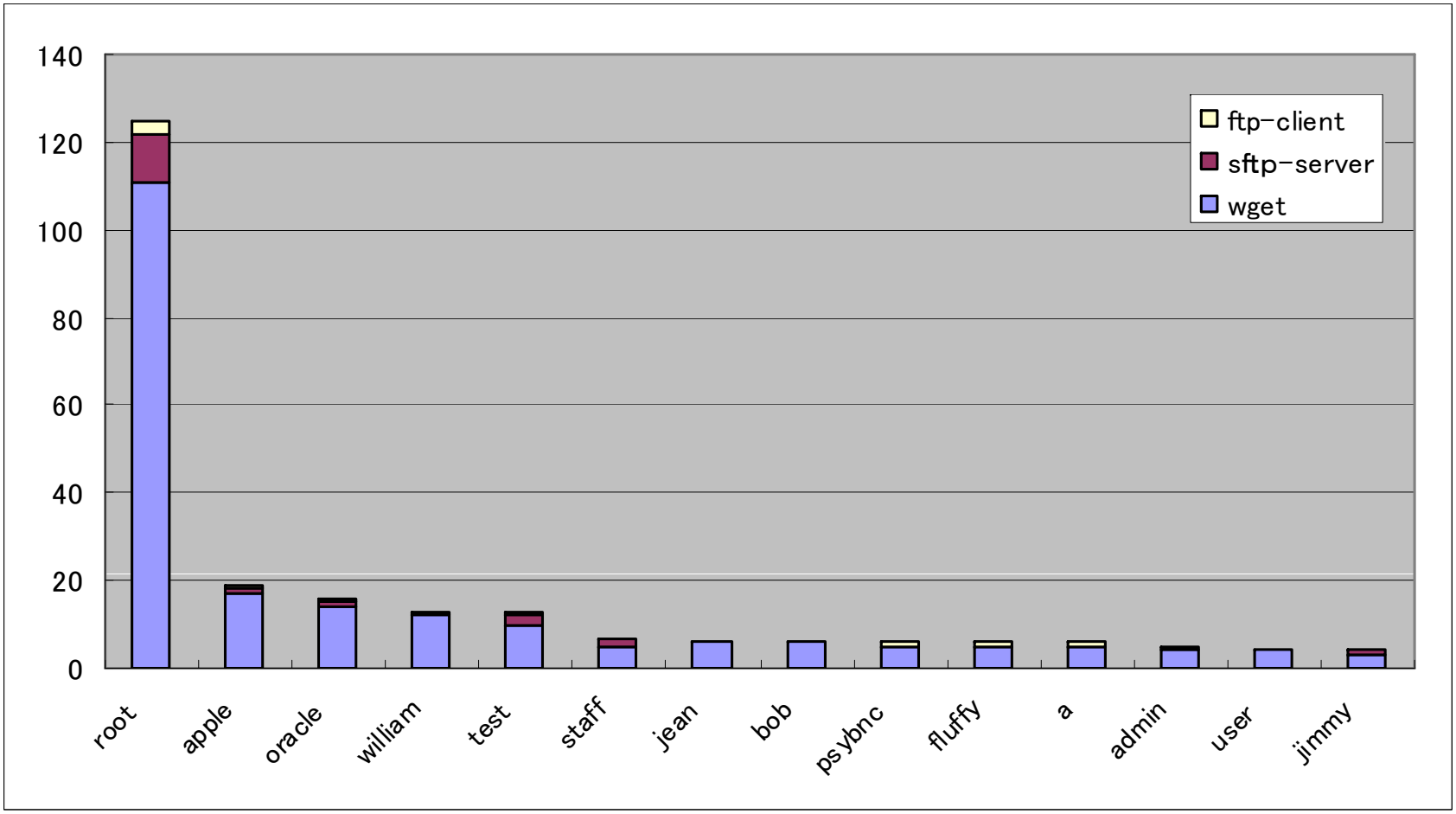
# Malware採取実験結果(日毎集計)

- 回収されたMalwareと転送方式の集計
  - 1日平均10検体程度採取。
  - 検体の設置にはwgetの利用が大半。次いでsftp-server



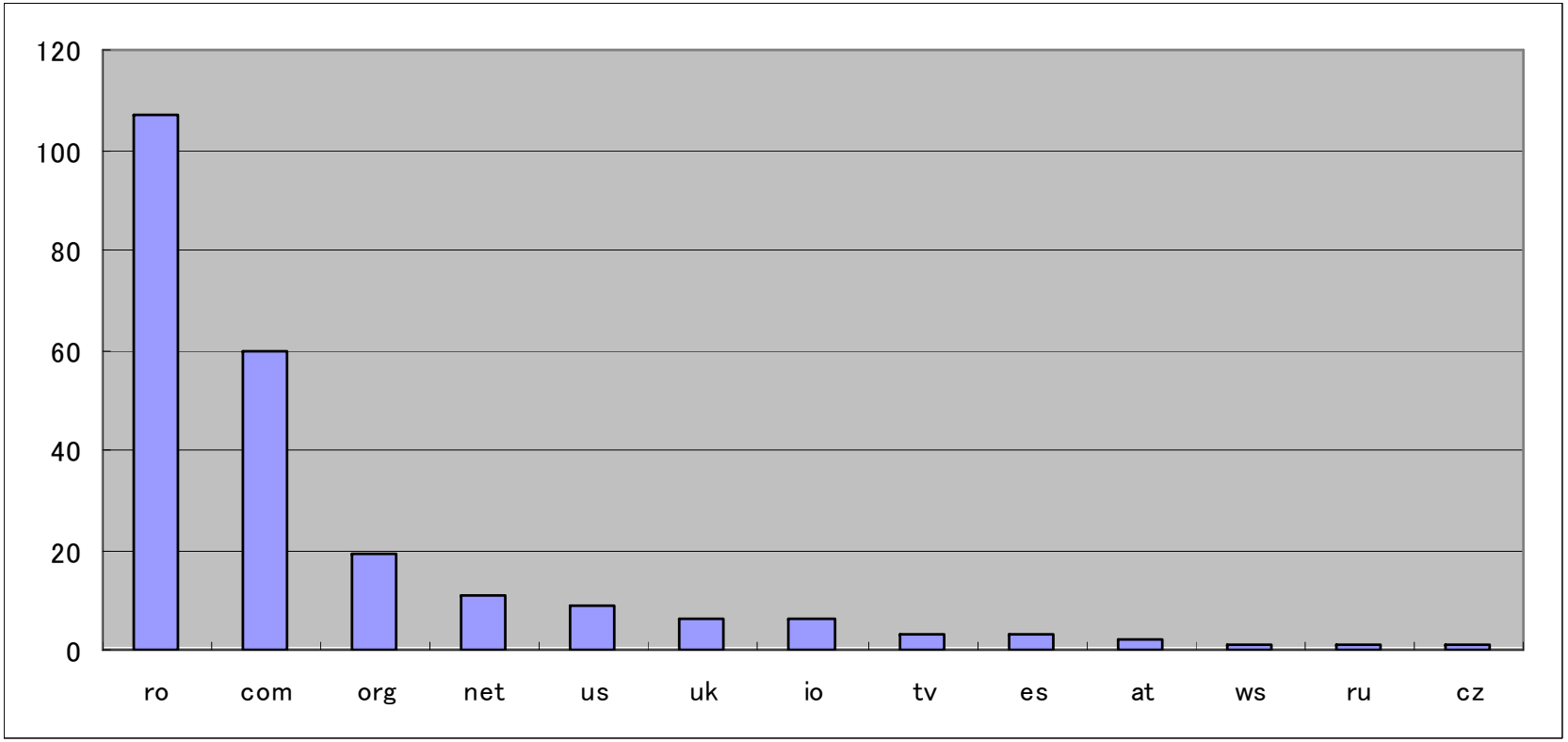
# Malware転送アカウント

- 転送方式と利用アカウント(転送数は延べ数)
  - wgetによる転送多数。その他sftp-server、ftp-clientあり。
  - アカウントはrootの利用が大半。



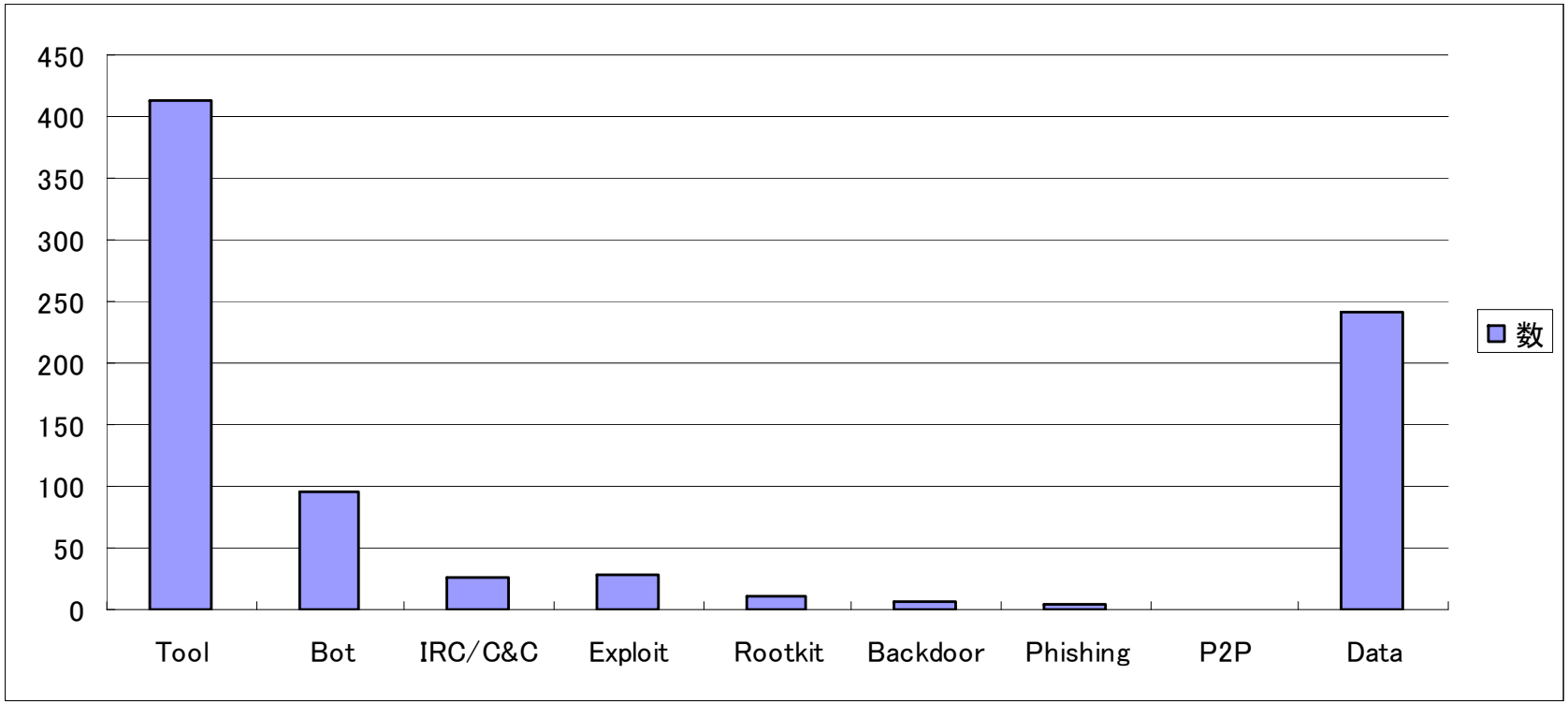
# Malware採取実験結果(ドメイン毎集計/TLD)

- 回収されたMalwareの転送元サイトのTLDでの集計
  - ルーマニア(.ro)が最多。
  - その他、com/org/netが比較的多い。
  - サイト単位では1サイトあたり20個が最大(調査期間の累計で)



# Malware採取実験結果(種類)

- 回収検体の分類
  - Toolには、多種のツールが纏まっている為、数が多く見えている。別途Tool内の分類集計を行う。
  - 1つの転送アーカイブ(tar.gz等)に複数種類が含まれるケースがあるため、回収数はそれらを重複カウントした延べ数になっている。
  - DataはMalwareではなく、Malwareで利用するためのファイルを指す。(BruteForceの辞書やボットの設定ファイルなど)



# Malware採取実験結果(Tool詳細-１)

- Toolを更に区分
  - 全般的にScan系が多い。
  - 汎用ポートスキャナは、純粋にTCPのConnectチェック用
  - ブルートフォーススキャナはパスワードチェックまで行う。

| Type | Target | 説明 | 数 |
|---|---|---|---|
| Scan | Generic Port | 汎用のポートスキャナ | 128 |
| | ssh | ssh のブルートフォーススキャナ | 108 |
| | SYN | TCP SYN スキャナ | 23 |
| | UDP | UDPスキャナ(ICMP Port Unreachableを利用) | 5 |
| | ICMP | Ping broadcastによるアドレススキャナ | 3 |
| | samba | samba(smb) スキャナ | 2 |
| | http | http スキャナ | 2 |
| | ftp | ftp スキャナ | 1 |
| Attack | UDP-Flood | UDP DoS 攻撃ツール | 22 |
| | TCP-Flood | TCP SYN FLOOD 攻撃ツール | 10 |
| | smurf | smurf 攻撃ツール | 5 |
| | IRC Flood | mirkforce IRC Clone Floodツール | 6 |

# Malware採取実験結果(Tool詳細-2)

- Toolを更に区分
  - SPYツールはpcapを利用したスニファ、もしくはそれらの出力から必要なデータを再構築して盗む比較的高度なものがある
  - エディタやコンソールも人気。ログイン後の手作業に利用。

| Type | Target | 説明 | 数 |
|---|---|---|---|
| SPY | SniffAnalyzer | プロミスキャストモードによるスニファ(盗聴)ツール | 11 |
| | User/Password | 各種プロトコルのログイン情報を上記スニファと組み合わせて盗む | 2 |
| | ssh | sshのコマンドを置き換えてログイン情報を盗む | 2 |
| Crack | Password Cracker | ローカルパスワードに対するクラッカー | 5 |
| | Log Cleanup | ログイン等の痕跡を消すLog Cleaner | 3 |
| Other | Editor | pico フルスクリーンエディタ | 43 |
| | Console | screen マルチスクリーンターミナルサーバ | 33 |
| | identd/oidentd | リモートからのidentに応答するサービス | 6 |

# Malware採取実験結果（Rootkit）

- 複数のタイプのRootkitを検出
  - カーネルドライバタイプのRootkitと、ライブラリやコマンド置換によるものがある。
  - adoreを設置した侵入者は、専用のスクリプトを利用して、カーネルモジュールのコンパイルとインストールを行い、再起動までする。

| Tootkit | 説明 | 数 |
|---|---|---|
| shv4/shv5 | ユーザランドrootkit | 6 |
| adore | カーネルモジュール rootkit | 4 |

注）Rootkit:
Malwareのプロセスやファイルをシステムから隠蔽する機能、もしくはモジュールを指す。

# Malware採取実験結果（Exploit）

- 外部からの進入用と侵入後の権限昇格用を確認
  - 侵入用のRemote Exploitについては、その種類（攻撃対象）で分類。
  - root取得用のLocal Exploitは多数確認されたが、数が多いため詳細な分類（何の脆弱性を攻撃するかについての分類）はしていない。
  - 基本的にはToolの類だが、ここではToolとは分けて集計している。

| Exploit | local Exploit | Remote Exploit | | | |
|---|---|---|---|---|---|
| | | samba | xmlrpc | webmin | webmail |
| 数 | 23 | 3 | 1 | 1 | 1 |

注）Exploit:
プログラムやシステムの脆弱性を検証するためのプログラム。本報告書ではそれらを利用した侵入、あるいは権限昇格を行うツール、もしくはプログラムを指す。

# Malware採取実験結果（Bot）

- 採取されたBotの一覧
  - EnergyMech多数。マルチプラットフォームバイナリ、ソースあり。
  - Perlのボットはperlb0t以外は正式名称不明なため、スクリプト中にて自称している名称を記載。perlで記述されているため、ある意味マルチプラットフォーム。
  - オフィシャルサイトあり（GPL配布）は別途URLを記載。

| ボット | Platform | 数 | ボット | Platform | 数 |
|---|---|---|---|---|---|
| EnergyMech | Linux | 88 | eggdrop | Linux/src | 2 |
| | FreeBSD | 15 | Perlb0t | Perl | 1 |
| | Mac-OS | 16 | The Best Scanner | Perl | 1 |
| | src | 14 | RoScan 5.5x | Perl | 1 |

| Bot | 配布URL |
|---|---|
| EnergyMech | http://www.energymech.net/ |
| eggdrop | http://www.eggheads.org/ |

# Malware採取実験結果（Backdoor/Trojan）

- バックドア系
  - HTTPサーバに設置して、別途専用のクライアントでHTTPサーバにアクセスし、サーバ上で任意のコマンドを実行するものがある。これはクライアントとSSIがセット。
  - IRC Proxyはperlで記述されている。

| Backdoor/Trojan | 説明 | 数 |
|---|---|---|
| HTTP/PHP Command | SSIとして動作するHTTP経由のコマンド実行ツール | 4 |
| IRC Proxy/Command | IRCをDelegateする機能を持つリモートコマンド実行サービス | 2 |

# Malware採取実験結果（その他）

- Malwareかどうか微妙なもの。
  - 単なる転送テスト？（Linux/W2KSP3）
  - IRC Server は恐らくC&Cサーバとして利用される。
  - P2P Hub は、設置された当初何か分からず、別途個別のファイルを調査して判明。

| Module | 説明 | 数 |
|---|---|---|
| IRC Server | C&Cサーバ用のフリーのIRCサーバ。オフィシャルURLは http://www.psybnc.at/ | 27 |
| P2P Hub | 実験的P2Pファイル共有HUBサーバ。オフィシャルURLは http://aquila.berlios.de/index.php/Aquila_Homepage | 1 |
| W2KSP3 | Windows2000 Service Pack 3。オフィシャルから取得 | 1 |
| Linux | Linux kernel 2.6.9 のソースコード。オフィシャルから取得 | 1 |

# Malware採取実験結果(Phishing関連)

- Phishingコンテンツ他
  - Phishing誘導用Mail Launcher(PHP)
  - Phishingコンテンツ、複数あり。ディレクトリツリー毎sftpでまとめて転送されるケースが多い。
  - イタリア郵便局は別バージョンあり。
  - コンテンツには、盗んだカード情報等を転送する先のメールアドレス等がハードコードされている。ただし難読化されていてそのままでは読めない。

| Type | 偽装対象サイト・偽装送信元 |
|---|---|
| Contents | JPモルガン・チェース(コンテンツ内の記述はチェース・マンハッタン)銀行のオンラインサイト |
| | イタリア郵便局のオンラインサイト |
| | PayPalオンライン決済サイト |
| Mail Launcher | Bank of America のオンラインサイト |
| | eBay オークション出品者 |

# 侵入者のアクセス元について

- 同一ユーザが複数の踏み台を持つ可能性
  - 異なるアドレスから侵入したユーザが同一の検体をダウンロードする。
  - これが、同一侵入者によるものであれば、侵入者は多数の踏み台ホストを持っていることになる。
  - 下記は5箇所から侵入したユーザが同一検体をダウンロードしたケースの例

| 対象検体: http://y2khom3.evonet.ro/unixcod.tar.gz | | | | |
|---|---|---|---|---|
| 89.42.126.198 | 89.131.182.123 | 78.96.12.207 | 89.136.243.148 | 85.186.195.200 |

# 総括

- LinuxシステムのMalware/悪用に関する現実
  - 一旦何らかの方法で侵入されると、やられ放題。
  - ホスティング等で、脆弱なアカウントが1つでもあると、侵入され、その後Local Exploitや、パスワードクラッカー等でroot権限が取られる。取られなくてもボットは動く。
  - 場合により、他サイト攻撃の踏み台に。
- 悪用に対する対策は？
  - 侵入されないための対策と侵入された後の悪用に対する対策それぞれについて、下記の様な情勢を鑑み、考える必要がある。
    - OLPC（One Laptop Per Child）や、OSP(Open School Platform)等の取り組みにより、クライアント数は増加中だが。。。
    - 高校・大学等の学術機関で、外部からアクセス可能なLinuxの対策は？

# 侵入されないために

- 不要なサービスの停止、OSの更新
  - 基本的なお約束。
- ssh Brute Force対策
  - sshのポートを変えるか、公開鍵以外による認証を切る。
    - 辞書は1ファイルで100万エントリ等、ほぼ単語として考えられるものは（例え日本語であっても）アウト。
    - Brute Force検知でポートをブロックするものもあるが、複数の踏み台を利用されると厳しい。
- その他、侵入の検知
  - ホストIDS等で侵入やMalwareの設置を確認。
    - 気づいた時には手遅れの可能性もありますが、無いよりまし。

# 侵入されてしまったら

- 外部に迷惑をかけない
  - ホスト→外部へのアクセスもFirewall（出来れば外部の）で不要なものはガードしておき、ログを採取すべき。
  - VMを使って同一ホスト上に別のVMとしてIDS/FWを設置するなどにより、感染チェックを行う当で対策する手もある。
    - が、、、一般の人に出来るかというと難しいところ。
- その他、検知、駆除など。。
  - Linuxへの侵入/Linux向けMalwareをReal-Time検知出来るAntiVirus等があればそれらを利用すべきだが、、、
    - OSに標準的なチェック用のAPIで使えるものが無いので、ディストリビューションによって対応してなかったり、、、
    - そもそも一般ユーザが利用するにはハードルが高い。

Empowered by Innovation