

平成 17 年上半期（1～6 月）における botnet 観測システム観測結果

注意 以下の観測結果は、サイバーフォースセンターの観測システムで把握した botnet について、その実態を示したものである。

上半期における観測結果の特徴

bot に感染したコンピュータ：主に日本を含む東アジアで約 5 割を占めている

bot に感染したコンピュータは、主に日本を含む中華人民共和国、大韓民国、香港、台湾などの東アジアが多かった。また、日本国内の bot に感染したコンピュータは、記録されているドメインから個人ユーザと推測されるものが多かった。

指令サーバ及び DoS 攻撃を受けた（対象）国：アメリカ合衆国が最も多い

最も指令サーバが多い国は、アメリカ合衆国で 234 アドレスあるが、日本の指令サーバも 93 アドレスとかなり多かった。また、日本国内の指令サーバは、記録されているドメインから個人ユーザと推測されるものが多かった。

DoS 攻撃を受けた（対象）国で最も多いのはアメリカ合衆国で、全体の 5 割を占めている。日本への攻撃は、3,531 件中、7 件とかなり少なかった。

bot の感染活動：Windows の DCOM 及び LSASS の脆弱性を突くものが圧倒的に多い

135/TCP へ DCOM の脆弱性を悪用して感染を拡大する命令が 65.3%で最も多く、次に多いのは 445/TCP へ LSASS の脆弱性を悪用して感染を拡大する命令で 7.7%であった。少数ではあるが、その他の感染手段も観測されており、今後更に新しい感染手段が実装されていくと思われる。

botnet 使用者による botnet 観測者対策が進んでいる

観測している botnet 指令サーバのうち、約 20 台が接続を拒否されている。これは、botnet 観測者対策として、不審な命令を発信する bot、命令への反応がない bot を、指令サーバで接続を拒否しているためと推測される。また、調査命令に対する反応がない指令サーバや、接続している bot のホスト名を表示しない指令サーバも増えてきている。これは、botnet に特化した専用の IRC サーバや IRC クライアントが使用されているためと推測される。

1 概要

サイバーフォースセンターでは、botnet の現状を把握するため、botnet 観測システムを構築し、平成 17 年 1 月から運用している。以下では、17 年上半期における観測結果を紹介するので、今後の botnet 対策の参考としていただきたい。

また、本観測期間中に、観測システムに対して必要な機能の追加等が継続的に行われていることから、本観測結果の一部については、上半期全期間にわたるデータが存在しないものがある。このため、各観測結果については、情報の取得期間を明記した。

なお、botnet の概要については、17 年 1 月 27 日から @police に掲載している「ボットネット(botnet)に注意」¹ を参照願いたい。

2 botnet 観測結果

(1) 接続 bot 数

観測期間	自 平成 17 年 1 月 1 日 至 平成 17 年 6 月 30 日
指令サーバ数	240 台
bot 数	1,285,247 台（日本は 144,512 台）

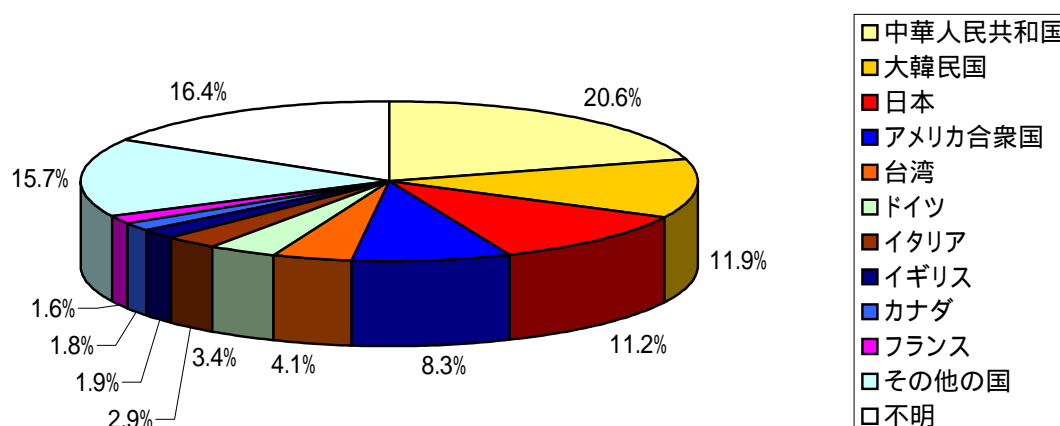


図 1 bot の国・地域別比率

¹ ボットネット(botnet)に注意 [PDF: 約 85KB]
http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf

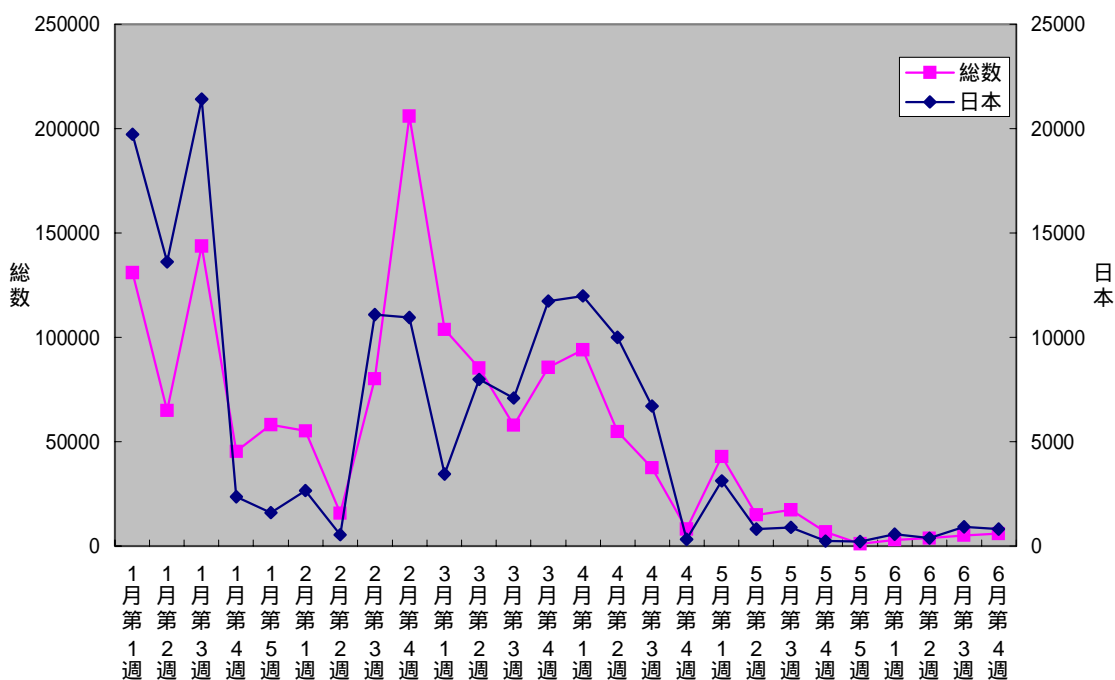


図2 bot 数の週別推移

図1及び2は観測している botnet に接続されたコンピュータのうち、IP アドレスが取得できたものについて集計したものである。bot に感染したコンピュータは、稼働状態になると、指令サーバに接続を試みる。このため、コンピュータの電源の on / off やインターネットの接続 / 切断によって botnet を構成するコンピュータの台数は時間とともに変化する。

観測期間中、bot に感染したと推定される IP アドレスは 1,285,247 アドレス存在し、そのうち国内が発信元と推定される件数は 144,512 アドレスであった。このように、国内でも数多くの bot に感染したコンピュータが存在していると考えられ、観測結果に記録されているドメイン名から、そのほとんどが個人ユーザの PC と推測される。

なお、個人ユーザの IP アドレスは接続する毎に変化する場合が多いため、この集計により正確な botnet の規模を把握することは困難ではあるが、おおよその接続 bot 数の目安になると思われる。

図1の bot の国・地域別比率では、上位には日本を含め東アジアの国々が非常に多く、全体の 5 割近くを占めている。「その他の国」とは、国が判別できた IP アドレスのうち、上位 11 位以下の合計である。「不明」とは、国が判別できない、または意図的に隠されている IP アドレスの合計である。この割合が多い理由としては、最近では botnet を観測する仕組み(システム)の存在が botnet 使用者の間で知られてきており、意図的に IP アドレスを隠すように bot が改良される場合が多くなってきているからで

ある。

図2のbot数の週別推移で4月第4週以降bot数が激減しているのは、観測していた幾つかの大規模なbotnetが観測者対策を施したことが原因である。当システムでは、bot数調査は指令サーバへ接続数を調査する命令を送信してその結果を集計している。しかし、最近では観測者対策として、指令サーバを改造することで調査命令の結果を返さない、又は、調査命令を受けた指令サーバは命令を送信した観測プログラムの接続を切断するなどの機能が実装されているため、今後のbot数調査は非常に困難になっていくと予想される。

(2) botnet 指令サーバ種別

観測期間	自平成17年2月28日 至平成17年6月30日
指令サーバ数	143ドメイン
指令サーバ IPアドレス数	664アドレス(うち、日本国内は93アドレス) 1ドメインに対してIPアドレスが複数設定されている場合が多いため、指令サーバ数とは異なる

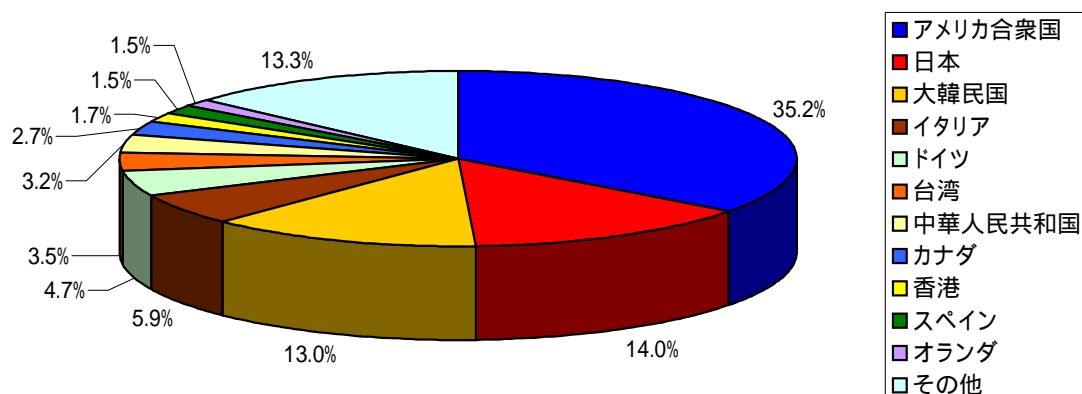


図3 指令サーバの国・地域別比率

図3は当システムで観測しているbotnet指令サーバのIPアドレスの国・地域別比率である。指令サーバに使用されているドメインは、複数のIPアドレスを割り当てているものも多く、一番多いもので1つのドメインに9アドレス割り当てているサーバも存在した。最もIPアドレスが多い国は、アメリカ合衆国で234アドレスであるが、日本のIPアドレスを使用している指令サーバも93アドレスとかなり多く、その93アドレス中84アドレスがDNSの逆引きをすると、国内プロバイダのADSL等でよく使用される形式(IPアドレス+ADSL等の文字+ドメイン名)のホスト名であったことから、個人ユーザのPCと推測される。

(3) botnet 指令サーバ接続情報ポート別

観測期間	自 平成 17 年 1 月 17 日 至 平成 17 年 6 月 30 日
観測指令サーバ 接続情報数	478 件 接続情報とは、指令サーバのドメイン名・ポート・ チャンネルの 3 つを 1 セットとしたものである

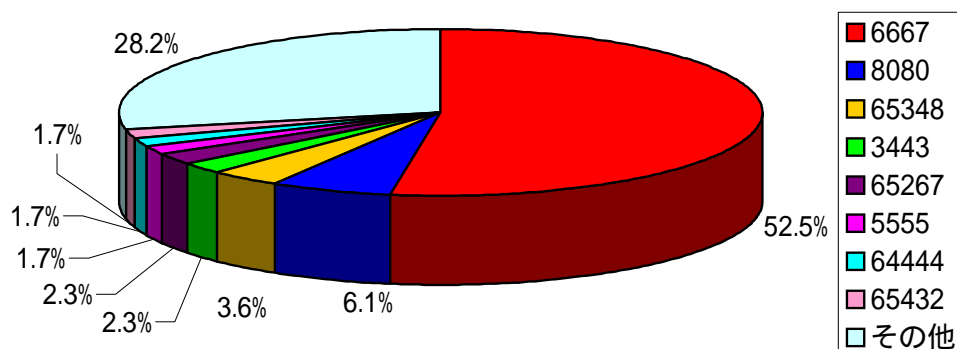


図 4 指令サーバの接続ポート別比率

図 4 は当システムで観測対象となった指令サーバの接続ポート別比率である。最も多かったポートは、一般的な IRC サーバで使用される 6667/TCP で全体の 5 割を占めている。次に多かったのがプロキシサーバで使用されている 8080/TCP で、その他としては、60000/TCP 以上、特に 65000 ~ 65535/TCP が比較的多い。

(4) 命令活動等種別

観測期間	自 平成 17 年 1 月 17 日 至 平成 17 年 6 月 30 日
観測指令サーバ 接続情報数	478 件 接続情報とは、指令サーバのドメイン名・ポート・ チャンネルの 3 つを 1 セットとしたものである
観測命令総数	126,103 件 命令実行結果の表示は除く (命令実行結果の合計は 866,624 件)

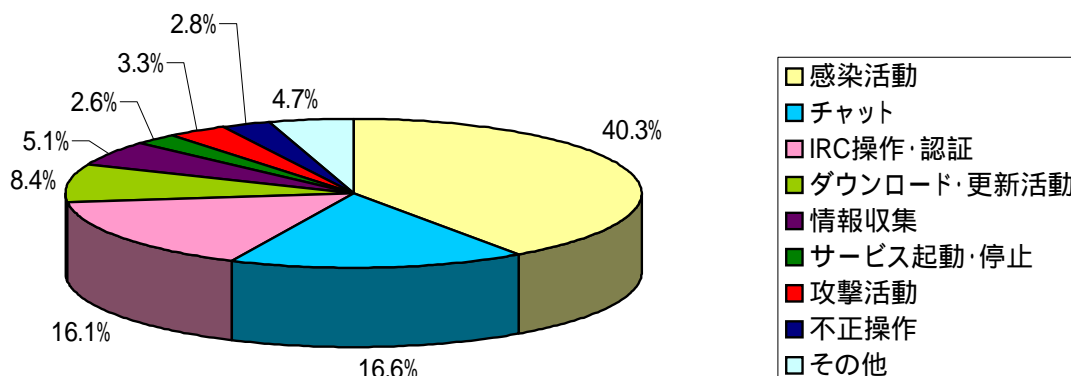


図 5 命令活動別比率

各命令の詳細は後述

図5は当システムで観測した命令等を種類別に分類したものである。最も多かったのは感染活動系の命令で、頻繁に観測されている。

なお、今回、命令実行結果を除外しているのは、指令サーバによって実行結果を表示しないもの（別チャンネルで表示など）が存在するためである。

ア 感染活動

観測期間	自平成17年1月17日 至平成17年6月30日
観測指令サーバ 接続情報数	478個 接続情報とは、指令サーバのドメイン名・ポート・ チャンネルの3つを1セットとしたものである
観測感染 命令総数	50,868件 命令実行結果の表示は除く

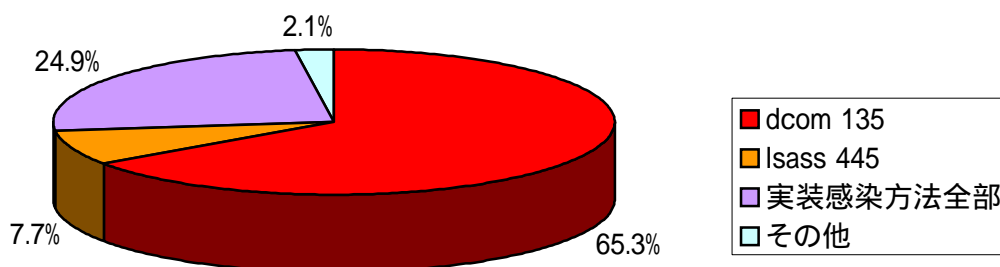


図6 感染活動命令手段別比率

図6は当システムで観測した感染活動命令の手段別比率である。botは、感染したbotを増やすために他のコンピュータへ感染活動を行う機能が実装されていることが多い。脆弱性を突く攻撃やパスワード攻撃などにより、感染を拡大させている。

dcom135

135/TCPを対象にMS03-026,039(DCOM)の脆弱性を悪用して感染を拡大する命令である。2003年に報告されている古い脆弱性ではあるが、最も多く見られる感染活動であり、この脆弱性はBlasterワームなどで利用されている。バリエーションとして、445/TCPや1025/TCPを対象とするdcom感染命令も観測されている。

lsass445

445/TCPを対象にMS04-011(LSASS)の脆弱性を悪用して感染を拡大する命令である。これもかなり古い脆弱性ではあるが、Sassarワームなどで利用されている。バリエーションとして、135/TCPや139/TCPを対象とするlsass感染命令も観測されている。

その他

以下にその他の観測された感染手段を示す。

- ・ 445/TCP へ Windows ネットワーク共有の脆弱なパスワードを標的にして感染
- ・ 139/TCP へ Windows ネットワーク共有の脆弱なパスワードを標的にして感染
- ・ 1433/TCP へ MS SQL Server の脆弱なパスワードを標的にして感染
- ・ 6129/TCP へ DameWareMiniRemoteControl の脆弱性を標的にして感染
- ・ 135/TCP へメッセンジャサービスの脆弱性を標的にして感染
- ・ 6101/TCP へ VeritasBackupExec の脆弱性を標的に感染
- ・ 443/TCP へ IIS5.0 の脆弱性を標的に感染
- ・ 80/TCP へ WevDav の脆弱性を標的に感染
- ・ ウイルス・ワームに感染してバックドアが存在するコンピュータを標的に感染
(mydoom-3127/TCP、kuang-17300/TCP、sub7-27374/TCP、netdevil-901/TCP、
beagle-2745/TCP、optix-3410/TCP、sassar-5554/TCP など)
- ・ 実装している全ての手段で感染拡大
- ・ 以上のような手段により、ネットワーク範囲を指定して感染

イ 攻撃活動

観測期間	自 平成 17 年 1 月 17 日 至 平成 17 年 6 月 30 日
観測指令サーバ 接続情報数	478 個 接続情報とは、指令サーバのドメイン名・ポート・ チャンネルの 3 つを 1 セットとしたものである
観測攻撃 命令総数	4,180 件 命令実行結果の表示は除く うち、攻撃先が特定できるもの 3,531 件中、 日本対象の IP は 7 件

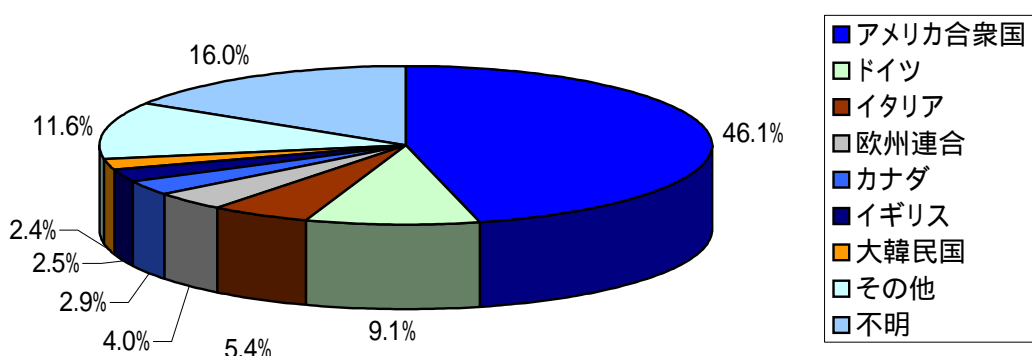


図 7 攻撃活動命令攻撃先国・地域別比率

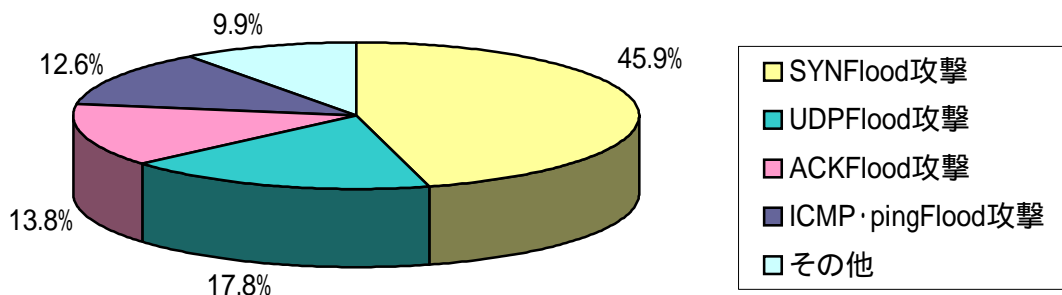


図 8 攻撃活動命令手段別比率

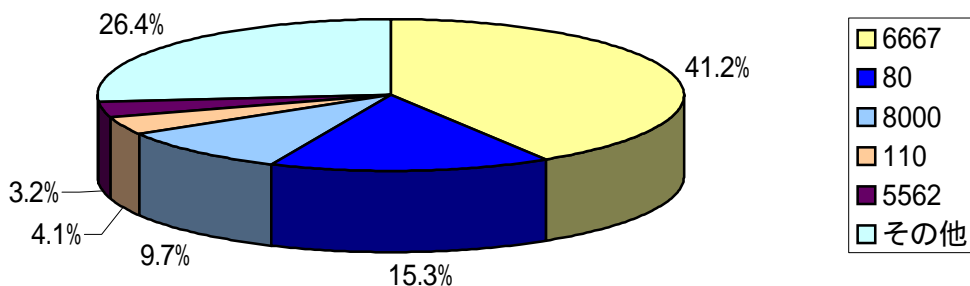


図 9 攻撃活動命令ポート別比率 (SYNFlood 攻撃のみ対象)

図 7 は当システムで観測した攻撃活動命令の攻撃先国・地域別比率である。最も多いのはアメリカ合衆国で、全体の 5 割を占めている。日本への攻撃は、3,531 件中、7 件とかなり少ない。

図 8 は、当システムで観測した攻撃活動命令の手段別比率である。SYNFlood 攻撃が最も多く、UDPFlood、PINGFlood など一般的に行われている DoS 攻撃がほとんどである。その他として、TCP パケットをランダムに出す攻撃や bot 毎のオリジナルの攻撃と推測されるものなども観測されている。

図 9 は、当システムで観測した攻撃活動命令 (SYNFlood 攻撃のみ) の宛先ポート別比率である。6667/TCP が最も多く、考えられる理由としては botnet 構築者同士の争いから、他の botnet の指令サーバを妨害する目的で攻撃しているものと推測される。次に多いのは 80/TCP で、web サービスを狙った攻撃によりホームページを閲覧困難にさせるのが目的と思われる。

ウ ダウンロード・更新命令

bot は、機能追加や接続する指令サーバ変更など行うため、botnet の指令サーバから命令を受けて、特定のサイトからダウンロードし、ファイルを蔵置又は自分自身を更新する。

当システムで観測した更新命令で指定されているファイルをダウンロードして、あるウイルス対策ソフトで検査したところ、1965 件中 292 件しかウイルスとして検出されなかった。これは、検査対象となったファイルが bot 本体ではなく、単体動作しない一部機能追加用ファイルが多かったためとは推測されるが、検出されないものもかなりあると思われる。

エ 情報収集命令

以下に観測された主な情報収集命令の内容と観測例を示す。

bot に感染しているコンピュータの LAN 情報やダイヤルアップ情報を表示

- ・ 実行結果表示例

```
:LamE CoMp: [Type]: LAN (LAN Connection). [IP Address]: 192.168.1.1.
```

```
[Hostname]: host
```

```
:[NETINFO]: [Type]: Dial-up (yahoo). [IP Address]: 192.168.1.1.
```

```
[Hostname]: host.
```

bot に感染しているコンピュータの OS、CPU の種類、ユーザ名などを表示

- ・ 実行結果表示例

```
:hot Computer @_@ [CPU]: 2600MHz. [RAM]: 256,000KB total, 200,000KB free.
```

```
[Disk]: 20,000,000KB total, 10,000,000KB free.
```

```
[OS]:WindowsXP(ServicePack1)(5.1,Build2600).
```

```
[Sysdir]:C:¥WINDOWS¥System32.[Hostname]:host(192.168.1.1).
```

```
[CurrentUser]:user. [Date]: 01:01:2005. [Time]: 01:01:01.
```

```
[Uptime]: 0d 0h 3m.
```

bot に感染しているコンピュータの稼働時間を表示 (例は省略)

bot に感染しているコンピュータの OS の Product ID などの CD-KEY を表示

- ・ 実行結果表示例

```
:Microsoft Windows Product ID CD Key: (XXXXXX-XXX-XXXXXXXX-XXXXX).
```

キーロガーを動作

- ・ 実行結果表示例

: [KEYLOG]: abcd [CTRL]efgh (Return) (XXX - Microsoft Internet Explorer)

ネットワーク盗聴 (スニッフィング)

- ・ 実行結果表示例

: [PSNIFF]: Suspicious BOT packet from: 192.168.1.1:3590
- GET /xxx.jp/xxx/xx.txt HTTP/1.1

画面キャプチャをファイル保存

- ・ 実行結果表示例

: [Capture]: Screen capture saved to: c:\¥xxx.jpg.

オ チャット

本来 botnet は、IRC サーバを bot に指令を送るために使用しているが、IRC は、本来チャット (キーボードを介した会話) のためのシステムであることから、いわゆるチャットにも使用可能である。ここで交わされる内容は、主に botnet 使用者同士が情報交換のために会話しているものと推測される。当システムでは、英語やイタリア語、フランス語、オランダ語、ベトナム語等が観測されている。

チャット例 1 (元は英語)

- > どれくらいの bot の数か?
- > 現時点ではおよそ 300
- > rxbot か?
- > そうだ
- > まだ拡大するか?
- > そうだ
- > あなたは、ソースを持っているのか?
- > いや、私は既存の exe ファイルを...

チャット例 2 (元は英語)

- > ダウンロード命令を知っているか?
- > 知らない
- > 他のボットのためか?
- > ダウンロード命令も更新命令も知らない
- > 他のチャンネルで話せ

カ その他の命令

以下に少数ではあるが、観測されたその他の命令で主なものを示す。

bot に感染しているコンピュータのシステムログを消去

他のウイルス・ワームの感染を防ぐために、特定のサービスを終了

プロキシサーバを起動

HTTP サービスを起動

リモートコンソールでコマンド実行

3 おわりに

今後の botnet 観測は、botnet 観測者対策により今まで以上に困難になると考えられるが、サイバーフォースセンターでは引き続き、国内外の関係各機関との連携強化を含め、botnet の活動の把握に努めていく。