IRC プロトコルを利用した攻撃者と感染端末の探索手法

荒谷　光†　　本間　将紘†　　金井　敦†　　斉藤　典明††
†法政大学大学院　　††NTT セキュアプラットフォーム研究所

あらまし　近年増加している BOT による被害を減らすことが急務となっている. しかしながら，BOT の被害を防ぐ有効な手段は確立されていない．BOT の被害を防ぐには，攻撃者を突き止めるか，BOT Net を構成するコンピュータを減らす必要がある．本研究では、従来のトレースバック技術とは異なり，既存のプラットフォームに変更を加えず，BOT 感染時の脆弱性を利用して攻撃者を突き止める手法および IRC プロトコルの特徴を利用して感染コンピュータを探しだす新しい手法を提案する．ここでは，提案手法の有効性を確認するために MWS 2013 Datasets を調査し，IRC-BOT の擬似環境で検証を行い，有効性を示した.

Search approach of a herder and infected computers using IRC protocol

Akira Aratani†　Masahiro Homma†　Atsushi Kanai†　Noriaki Saitou††
†Hosei University Graduate School　††NTT Secure Platform Laboratories

Recently, it is urgent to reduce damage against BOT. However, there doesn't exist effective methods to prevent BOT damages. To prevent them, it is necessary to elucidate the herder or reduce the number of infected computers. In this paper, we propose new approach to identify the herder using the vulnerability of BOT infection without changing existing platforms and to search infected computers using features of IRC protocol. Furthermore, the proposed approach is evaluated using MWS 2013 Datasets.

1　はじめに

コンピュータとインターネットは我々の生活になくてはならない存在となっている. 価格の低下・容量の増加に伴って，一般家庭にも広く普及してきている．しかし，セキュリティに対する意識や知識が低い人は OS やソフトウェアの脆弱性を放置している場合が多く，BOT 等のマルウェアに感染してしまう.

BOT とは，マルウェアの一種で，インターネットを通じて感染したコンピュータを第三者から操作を可能にすることを目的に作成された悪性のプログラムである. 感染すると攻撃者からの指令受けるために C&C (Command & Control)サーバに接続して BOT Net と呼ばれるネットワークを構築する. 攻撃者は C&C サーバを介して BOT Net に接続している BOT に対して指令を下し実行させる. 現在 C&C サーバに IRC(Internet Relay Chat)サーバを利用している BOT も

少なくない．BOT Net の制御に IRC プロトコルを使用している BOT を以降では IRC-BOT と呼ぶ．IRC-BOT に感染したコンピュータは攻撃者からの指令を受けるために自動的に IRC サーバに接続し，特定のチャンネルに参加する．指令はユーザとして同じチャンネルに参加している攻撃者の発言として参加者全員に送信される．

IRC プロトコルとは，TCP/IP ネットワーク上でクライントとクライアントがサーバを経由してテキストデータを交換して会話をするプロトコルである．典型的な構成としては，クライアントの接続点の中心にメッセージの配信，多重配信などの機能を持つ IRC サーバを置き，メッセージの交換を行う．[1] C&C サーバに IRC サーバが多く使われる理由としてはメッセージの多重配信により，容易に多数の BOT に対して指令を出すことができるからである．

BOT に感染したコンピュータは感染前と同様にそのコンピュータを利用することができるため，ユーザは BOT に感染したことに気づかないことが多く感染者が後を絶たない．BOT に感染したコンピュータは外部からの司令で DDoS(Distributed Denial of Service)攻撃等を行うため 2 次的な被害も後を絶たない． しかし，現在 BOT に対する対策として，各個人が導入したウイルス対策ソフトの検出後に削除するという消極的な方法が中心で， BOT による被害を防ぐ有効な手段が確立されていない．BOT による被害を防ぐためには積極的に攻撃者を突き止めるか，BOT Net を構成するコンピュータを探索し．削除を促す必要があると考える．そこで，本稿では，IRC-BOT に焦点を当てて IRC プロトコルを利用して積極的に攻撃者を突き止める手法と BOT Net を構成する IRC-BOT に感染したコンピュータの IP アドレスを取得する手法を提案する．

以下本稿では， 2 章では，IRC プロトコルを利用して攻撃者を突き止める手法と BOT Net を構成する IRC-BOT に感染したコンピュータの IP アドレスを取得する手法をそれぞれ述べる．3 章では，CCC(Cyber Clean Center)が提供している BOT の検体のうち IRC-BOT の割合を調査し，提案手法の有効性を述べる．4 章では，提案手法のフィジビリティの検証を述べる．5 章で検証結果に対する考察を述べる．6 章では，本稿をまとめる．

2 提案手法

現在 BOT に対する対策として，各個人が導入したウイルス対策ソフトの検出後に削除するという消極的な方法が中心である．そこで，提案方式ではハニーポットを設置し BOT を収集して積極的に対策を行う．従来の消極的な対策と異なり，攻撃者の特定および BOT の感染端末の削減により BOT Net の機能を低下させることを目的としている積極的な対策である．本稿では，上記の目的を達成するために IRC プロトコルを利用して攻撃者を特定する手法と BOT 感染端末の IP アドレスを探索する手法を提案する．

取得した IP アドレスを基にネットワークの管理者に報告する等して削除を促す事を構想している．

各提案手法の概要を以下に示す．

・攻撃者の追跡

DDoS 攻撃は，攻撃発信元が偽装されている場合がほとんどである．そのため，DDoS 攻撃に対処するためには，攻撃の発信元が偽装されていても攻撃者を発見できるシステ

ムが必要となる．そこで，攻撃元が偽装されても攻撃元を発見できるシステムとして IP トレースバックシステムがいくつか研究されている．[2,3] しかしながら，今までのトレースバックの研究はいずれも既存のルーターや DNS のシステムに新たな機能を加えるためコストが高い．本方式では，既存のトレースバック方式とは異なり既存のルーター等に改変を加えず，大規模なシステム変更を必要としない BOT Net の特徴を利用した方法で DDoS 攻撃の攻撃者を探索する．

・BOT 感染端末の探索

BOT はユーザの目にとまるような表立った活動をしないため，感染していることに気が付きにくい．多くの人はアンチウイルスソフトを導入して対策を行なっているが，BOT は日々たくさんの新種が作成されているため頻繁にウイルスチェックソフトのウイルス定義ファイルの更新を行う必要がある．また，コンピュータの利便性を上げるために導入したアプリケーションにセキュリティホールが存在する場合があり，セキュリティホールに対するパッチを適用する必要がある．セキュリティに対する意識の低いユーザはそれらの行為を怠りがちなため，結果的に BOT に感染してしまう．そのために，気づかないうちに自身のコンピュータが踏み台にされサイバー犯罪の手助けをしてしまうことになる．本方式では，上記の作業を怠りがちなユーザに BOT に感染していることを通知し削除を促すことで BOT Net の機能を低下させる．

いずれの調査も IRC-BOT と同じ IRC サーバに接続し，同じチャンネルに参加する必要があるので共通するフェーズを第一フェーズとし BOT Net に参加する手法を述べる．第二フェーズに攻撃者の追跡，同一 BOT 感染端末の探索のそれぞれの方式を述べる．

2.1 BOT Net に参加

攻撃者と特定する手法と BOT 感染端末の IP アドレスを取得する手法において共通する IRC-BOT と同じ IRC サーバ内の同じチャンネルに参加する手法を以下に述べる．

IRC-BOT に感染したコンピュータは 攻撃者からの指令を受けるために IRC サーバに接続する．IRC サーバに接続する際に PASS, NIKC, USER コマンドを送信する．この時の通信を観察していれば IRC サーバの IP アドレスとパスワードが設定されて入ればパスワードを入手できるので第三者として IRC-BOT と同じ IRC サーバに接続することができる．

IRC-BOT は IRC サーバに接続した後，特定のチャンネルに参加する．チャンネルに参加するには JOIN コマンドを使ってチャンネル名とチャンネルに設定されたパスワードを送信する必要がある．ただし，チャンネルにパスワードが設定されていない場合はチャンネル名のみで良い．IRC サーバの接続と同様に通信から必要な情報を得ることが出来れば，第三者として IRC-BOT と同じチャンネルに参加することができる．

2.2 攻撃者の追跡

攻撃者は感染した BOT に対して各種機能を実行させるために自ら指令を送る必要がある．

・ステップ 1

IRC-BOT は攻撃者からの指令を IRC サーバ経由で受信するため，IRC-BOT が参加する IRC のチャンネルに入った後，チャンネルに入っているクライアントの発言を全て監視することで個々が発信する内容を確認することが出来る．通常は感染した IRC-BOT が自ら発信する機会は少なく，また発言した場合でも内容は感染端末の情報等に限られるため，DDoS 攻撃等の指令があれば，その指令発信者は攻撃者の可能性が高い．前述した IRC の特徴より同じチャンネル内に参加しているクライアントの一覧は確認することが可能なので攻撃者と思われるクライアントの IP アドレスを取得することが出来る．

・ステップ 2

ステップ 1 で取得した IP アドレスを元に攻撃者を追跡するが，特定を免れる為に攻撃者は直接 IRC チャンネルに接続せずにプロキシを介して指令を送信する．そのため，取得した IP アドレスは攻撃者では無い可能性があるのでハーダーとプロキシの判別をする必要がある．プロキシを介していた際，一般利用されているプロキシサーバで管理者が存在する場合は，管理者へログの確認をすれば良いが，プロキシには管理者が存在せず放置されているものや，感染端末と同様の BOT がプロキシとして動作しているものが多くある．本手法では管理者が存在しないプロキシを介していた場合は追跡する事が出来ない．

・ステップ 3

BOT に感染する端末は脆弱性を利用され侵入される．また自ら BOT を実行して，脆弱性から感染した場合でなくても攻撃者は BOT 感染端末へとバックドアを仕掛けるため BOT 感染端末には何らかの侵入手法が残される可能性が高い．

BOT がプロキシの役割として動作している場合は感染端末の脆弱性を利用することで BOT に感染しているプロキシに侵入してパケットを見ることで攻撃者の発信元 IP アドレスを取得し，追跡することが可能となる．

本手法では，ハーダー特定までステップ 2~3 を繰り返す事で攻撃者まで追跡を行う．

2.3 BOT 感染端末の探索

IRC-BOT に感染したコンピュータは攻撃者の指示を受けるために特定の IRC サーバに接続し，特定のチャンネルに参加する．つまり，同一の IRC-BOT 感染した全てのコンピュータは同じ IRC サーバの同じチャンネル参加しているということになる．

IRC プロトコルには同じチャンネルに参加している全てのユーザのニックネームを取得する NAMES コマンドとユーザのニックネームから IP アドレスを取得する WHOIS コマンドが用意されている．この 2 つのコマンドを組み合わせることで，チャンネルに参加している，つまり，IRC-BOT に感染している全てのコンピュータの IP アドレスを全て取得することができる．

3　MWS 2013 Datasets の調査

この章では, CCC が提供している BOT の検体の中に IRC-BOT が何割含まれているか調査を行い，IRC-BOT に焦点を当てた提案手法の有効性を検討する.

MWS 2013 Datasets のうちのマルウェアの検体 7201 件全てに対してカスペルスキーのウイルススキャンを行い．BOT と分類された全てのマルウェアについて調査を行った．BOT に分類されたマルウェアを表 1 に示す.

表 1　BOT の検体

BOT 名称	検出数
Backdoor.Win32.Rbot.adpd	8
Backdoor.Win32.Rbot.aftu	18
Backdoor.Win32.Rbot.bni	2
Backdoor.Win32.Agbot.nq	1
Backdoor.Win32.IRC-BOT.oib	1
Backdoor.Win32.IRC-BOT.rwv	1
Backdoor.Win32.IRC-BOT.sad	1
Backdoor.Win32.kbot.s	1
Backdoor.Win32.SdBot.vxf	1
Trojan-Spy.Win32.Zbot.apbg	1
Trojan-Spy.Win32.Zbot.cati	1
Trojan-Spy.Win32.Zbot.gen	1
Trojan-Spy.Win32.Zbot.tej	1
Worm.Win32.Bgrbot.byu	1
合計	39

次に，BOT の通信を監視し，IRC プロトコルを利用していた場合 IRC-BOT であると判断する．IRC プロトコルは通常 6667~6669 番ポートを利用して通信を行なっているが, 設置する攻撃者によってポートは自由に変えることができるので判断基準としては不十分である．そこで，IRC-BOT が IRC サーバに接続する際に IRC プロトコルで定められたコマンドを送信する特徴を利用して判定を行うことにする.

IRC プロトコルのインタフェースにはユーザコマンドが用意されていて, IRC サーバに接続する際には PASS，NICK，USER コマンドの 3 つを送信し, この 3 つの全てが受理されなければ IRC サーバに接続することはできない．NICK，USER コマンドについては順序不同で構わないが，PASS コマンドは必ず最初に送信しなければならない. ただし, IRC サーバにパスワードが設定されていない場合送信しなくても良い．　従って，NICK,USER コマンドの両方が通信から確認できれば IRC-BOT であると判断できる.

調査の結果を図 1 に示す. 全 39 個の BOT の内 17 個が IRC-BOT, 6 個がその他の BOT, 16 個が起動できないものであった．調査の結果から IRC-BOT は全体の約 4 割を占めており，IRC-BOT に焦点を当てた提案手法は充分に有効であると考えられる.

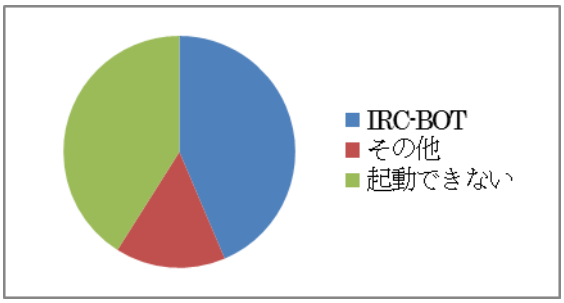

図 1　BOT の調査

4　検証

この章では, 各フェーズの手法のフィジビリティを検証する. 通常攻撃者は追跡を逃れる為，BOT への指令に使われる C&C サーバは短い期間で入れ替わる．2013/07/24 に MWS 2013 Datasets を調査したが 2013/02/28 以前に収集された検体に実際に IRC サーバに接続可能な IRC-BOT は存在しなかった．そのため，第一フェーズは Linux で擬似 IRC サーバを構築し検証を行った．第二フェーズにおいては IRC-BOT として広

く利用されている rBOT をソースからコンパイルし BOT を作成して独自に BOT Net を構築し検証を行った.

4.1 BOT Net に参加可能性検証

BOT Net に参加可能か検証を行うために BOT 感染端末，IRC サーバ，調査端末の計 3 台の PC を利用して検証を行った．検証を行った環境を表 2 に示す.

表 2　BOTNet に参加の実験環境

役割	OS	使用ソフト
BOT 感染端末 (挙動観察)	WindowsXP 32bit	Wireshark
IRC サーバ	Ubuntu12.4 32bit	Ircd-hybrid (IRC サーバ)
調査端末 (第三者)	Windows7 64bit	Lime Chat (IRC クライアント)

MWS 2013 Datasets に含まれる IRC-BOT を実際にコンピュータ上で動作させて， Wireshark を用いて通信の様子を観察した．通信パケットの中から NICK，USER，PASS コマンドを抽出して，IRC サーバに接続する際に必要な情報を確認することができた．また，各コマンドの送信先 IP アドレスから IRC サーバの IP アドレスを取得できた．上記の情報を元の Linux 上に IRC サーバを構築して実際に IRC-BOT を接続させた. その時の通信パケットからチャンネル名を取得することができた. 上記の全ての情報を元に IRC-BOT と同じ IRC サーバの同じチャンネルに調査端末から LimeChat を利用して接続を試みたところ，同じチャンネル内に IRC-BOT と同じニックネームの参加者を確認する事ができた. IRC サーバについては, 攻撃者が追跡を逃れるためすでに使えない状態であったため我々で用意したもので擬似的な環境で行ったが第三者として BOT Net に参加することは可能であることがわかった.

4.2 攻撃者の追跡は可能性検証

攻撃者の特定が可能か検証を行うために BOT 感染端末，攻撃者，プロキシ，IRC サーバ，侵入用 PC，チャンネル監視用 PC の計 6 台の PC を使用して実験を行った. 実験を行った環境を表 3 に示す.

表 3　攻撃者特定の実験環境

役割	OS	使用ソフト
BOT 感染端末 (挙動観察)	Windows7 64bit	—
攻撃者端末	Windows7 64bit	Lime Chat (IRC クライアント)
調査端末 (第三者)	Windows7 64bit	Lime Chat (IRC クライアント)
IRC サーバ	Ubuntu12.4 32bit	Ircd-hybrid (IRC サーバ)
Proxy サーバ (BOT)	Windows XP Service Pack2 32bit	—
Cracker	Back Track R3 32bit	Metasploit Nmap

第一フェーズと同様に rBOT 感染端末の通信を観察し, IRC サーバに接続するために必要な情報とチャンネルに参加するために必要な情報を取得した後，調査端末から LimeChat を利用して IRC-BOT と同じ IRC サーバの同じチャンネルに参加して攻撃者から BOT 感染端末に指令を出す様子を観察した.

今回は実験用の攻撃者端末から rBOT に感染しているプロキシ用の端末を介して指令を送信する. そうすることでチャンネル内に表示される指令の送信元はプロキシ用の BOT になる．チャンネルに侵入している端末からは指令の送信元を取得出来るため, クラック用端末でプロキシへと侵入する. 今回

は Windows XP の脆弱性を利用してプロキシ内に侵入を試みた．侵入に成功した後，通信ログを得るため，Metasploit で用意されているパケットキャプチャのツールを使用してパケットのログを見る．パケットのログを観察すると攻撃者から IRC サーバ宛に送信されている中継パケットを発見することが出来るため攻撃者を特定することが可能となる．また，MWS 2013 Datasets に含まれている IRC-BOT を実行し， Linux で擬似 IRC サーバを構築した後，パケットから読み取った接続先を用意した擬似 IRC サーバへと変更すると IRC-BOT に感染した端末は IRC サーバ上のチャンネルへと参加した．IRC の仕組みからチャンネルに参加した IRC-BOT は第三者の立場から確認することが出来るので，IRC-BOT に感染した接続先の IP アドレスを知ることが可能であった．

4.3 BOT 感染端末の探索可能性検証

BOT 感染端末の探索が可能か検証を行うために挙動観察用ではない BOT 感染端末 2 台，観察対象の BOT 感染端末，IRC サーバ，調査端末の計 5 台の PC を使用して実験を行った．実験を行った環境を表 4 に示す．

表 4　BOT 感染端末探索の実験環境

役割	OS	使用ソフト
BOT 感染端末 (非挙動観察)*2	Windows7 64bit	—
BOT 感染端末 (挙動観察)	Windows7 64bit	—
IRC サーバ	Ubuntu12.4 32bit	Ircd-hybrid (IRC サーバ)
調査端末 (第三者)	Windows7 64bit	Lime Chat (IRC クライアント)

今回の実験は 3 台の rBOT 感染端末を利用して小規模の BOT Net を構築して行った．第一フェーズと同様に rBOT 感染端末の通信を観察し，IRC サーバに接続するために必要な情報とチャンネルに参加するために必要な情報を取得した後，調査端末から Lime Chat を利用して IRC-BOT と同じ IRC サーバの同じチャンネルに参加した．

初めに，チャンネル名を引数に渡すとそのチャンネルに参加している全てのユーザのニックネームを取得できる NAMES コマンドを使用して同じチャンネルに参加している全員のニックネームを取得した．続いて，取得した全てのニックネームに対してニックネームを引数に渡すとユーザの詳細情報を取得できる WHOIS コマンドを使用して IP アドレスを取得した．いずれも BOT 感染端末に設定された IP アドレスを正しく取得することができた．

4.4 検証結果

独自に構築した BOT Net 擬似環境を利用して検証を行った結果，提案手法の目的を達成させるために必要な情報が取得可能であったため提案手法の実現性が充分にあることを確認することができた．

5　考察

この章では，4 章の検証結果について考察する．

5.1 BOT Net に参加について

CCC が提供する BOT の検体を実際に動作させて通信を観察することで，接続先の IRC サーバの IP アドレスとパスワードを取得することができた．また，チャンネルに参加するために必要なチャンネル名とパスワードを取得することができた．しかし，CCC が BOT の検体を提供する際には収集してから配布するまでに準備期間が必要なため，短

期間で C&C サーバを切り替える BOT などは配布されてからも活動を続けているものがない．そのため，BOT Net の参加についてはMWS 2013 Datasets の検体を使用しているが, IRC サーバは独自に構築したものを利用している．そのため，実際の BOT Net とは環境が多少異なるので，実際の BOT Net で実行可能か検証していく必要がある．

5.2 攻撃者の追跡について

攻撃者の追跡についても BOT Net に参加と同様に実際の BOT Net でも実行可能か検証していく必要がある．

本稿では, ハーダー追跡のステップでプロキシが BOT 感染端末の場合に管理者が存在しない場合は無断で感染端末へ攻撃をしかけ，侵入する手法をとっている．そのためコンプライアンス等を定めハーダー探索以外の用途で悪用をしないことを明記する必要がある．また，ハーダーを特定する際にプロキシサーバとハーダーの判別が曖昧な為，ハーダーの判別手法を検討する．

5.3 BOT 感染端末の探索について

BOT 感染端末の探索についても BOT Net に参加と同様に実際の BOTNet でも実行可能か検証していく必要がある．また，収集した IP アドレスを基に BOT 感染端末の所有者に対してどのようにして BOT に感染しているか通知をする手法についても検討していく必要がある．

6 まとめ

本研究では IRC プロトコルを利用した攻撃者の追跡と BOT の感染端末の探索する手法についてフィジビリティを検証した. 提案手法の第一フェーズにおいて実際の BOT の検体から IRC サーバに接続に必要な情報およびチャンネルに参加するために必要な情報を取得することができた. IRC サーバは独自に用意したものを利用したが, 実際の環境においても実行可能であると考えられる．

今後は，独自にハニーポットを設置し，活動中の BOT について調査を行う予定である．

参考文献

[1] 東角 芳樹 武仲 正彦(富士通研), “ネットワーク挙動に基づく Bot 検知手法の提案”情報処理学会シンポジウム論文集 巻：2007 号：10 ページ：85-90.

[2] 竹森 敬祐，藤長 昌彦，西垣 正勝(KDDI 研，静岡大学), “DNS ログに注目した詐称 IP 探索”情報処理学会研究報告 巻：2008 号：21(DPS-134 CSEC-40) ページ：61-66.

[3] 播磨 宏和，渡邊 晃，竹尾大輔(名城大), “MAC アドレスを用いた IP トレースバック技術の提案”情報処理学会全国大会講演論文集 巻：67th 号：3 ページ：573-574.