Press Release

2009 年 12 月 22 日

報道関係各位

株式会社セキュアブレイン

セキュアブレイン gred セキュリティレポート Vol.5【2009 年 11 月分統計】

「Gumblar ウイルス」は攻撃の変化により、その被害も増加/長期化傾向に

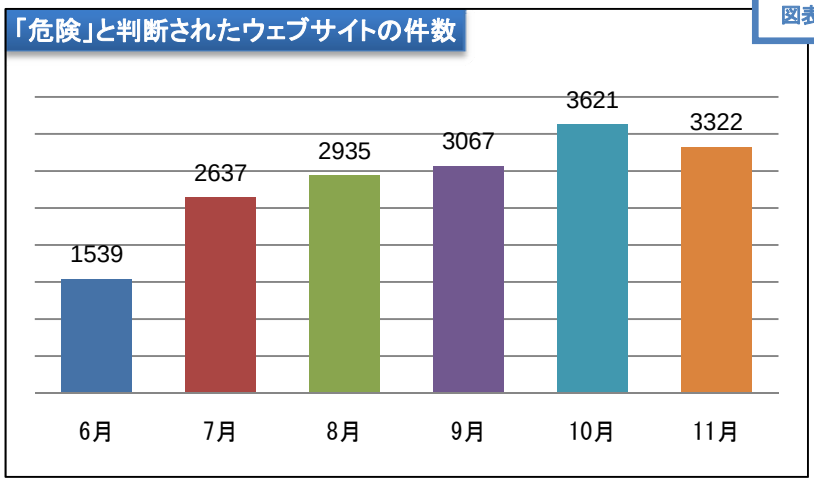
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解析エンジンが、ブラックリストを使用せず短時間で解析し、そのウェブサイトが「安全(Safe)」か「危険(Danger)」を判断します。

本レポートに含まれる内容

1　gred セキュリティレポート概要

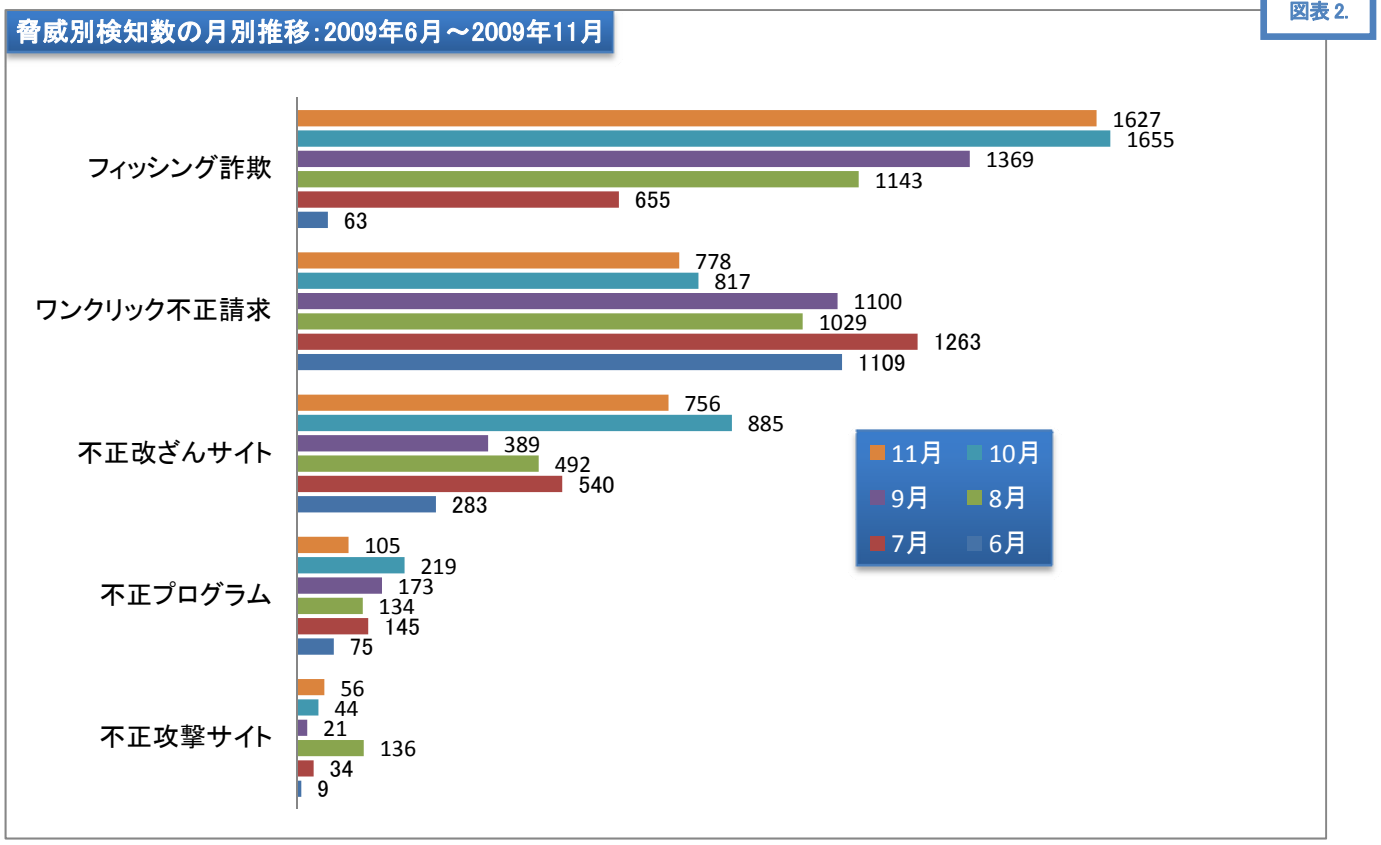
1.1　「危険」と判断されたウェブサイトの数（2009 年 11 月）：3,322 件（図表 1）

図表 1.



1.2　「gred でチェック」で検知した脅威の月毎の推移（図表 2）　（単位：件）

図表 2.



- 「危険」と判断されたウェブサイトの件数は、3,322 件で、統計開始後、初めて減少に転じました。（前月比 91.7%）（図表 1 参照）
- 2009 年 11 月は、「不正攻撃サイト」（56 件：前月比 127.3%）以外は、全ての項目の検知数が減少に転じています。

1.3 「gred でチェック」のチェック結果に表示される脅威の説明

表示される脅威の名称	説明
フィッシング詐欺	本物そっくりに、偽造されたウェブサイトです。ユーザの ID や、パスワード等の個人情報を不正に取得します。
ワンクリック不正請求	ウェブサイト上のボタン等をクリックしただけで、契約が成立したように見せかけ、料金を不当に請求する詐欺を行っているウェブサイトです。
偽ソフトウェア(不正プログラム)	不当に料金を請求する、実際には機能しない、偽物のソフトウェアを配布しているウェブサイトです。
不正攻撃サイト	他のコンピュータに存在する脆弱性を突いて、攻撃を行うことを目的として作成されたウェブサイトです。
不正改ざんサイト	攻撃者によって、不正に改ざんされてしまった状態になっているウェブサイトです。
ウイルス(不正プログラム)	ウイルスが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
ワーム(不正プログラム)	電子メールやネットワークを利用し自己増殖する、ワームが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
スパイウェア(不正プログラム)	個人情報等をコンピュータから盗む、スパイウェアが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
その他のマルウェア(不正プログラム)	ウイルス、ワーム、スパイウェア以外の不正プログラムが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。

2 悪質サイトの傾向分析

先端技術研究所では、「gred でチェック」で検出された結果について、詳細な分析・調査を行っています。この項では、それらの中から特に顕著に表れた傾向について、分析・調査結果を紹介します。

2.1 「Gumblar ウイルス」の脅威に晒される、企業ウェブサイト

2009 年下半期は、まさに「Gumblar ウイルス」が猛威をふるったと言えます。

2009 年 6 月にウェブサイトの改ざん被害が大量に発生した、「Gumblar/JSRedir-R ウイルス」(以下、Gumblar ウイルス)は、その後も攻撃手法を変えるなどして、攻撃を続けています

2.1.1 「Gumblar ウイルス」の攻撃手法の変遷

2009 年 5 月に確認された攻撃の概要

1. 「Gumblar ウイルス」により、悪意のある難読化されたスクリプトが埋め込まれたウェブサイトにアクセスした、「Adobe PDF」「Adobe Flash Player」の脆弱性を持つパソコンが「Gumblar ウイルス」に感染します。
2. 「Gumblar ウイルス」は、感染したパソコンから FTP のアカウント情報を収集します。
3. ウェブサイトの更新や管理を行っているパソコンが感染した場合、ウェブサイトが不正アクセスの被害に遭う可能性があります。
4. 閲覧者を「Gumblar ウイルス」の配布サイトに誘導する、難読化されたスクリプトをウェブサイトに埋め込みます。
5. 1-4 の活動が繰り返されることで、「Gumblar ウイルス」の被害が増大します。

2009 年 10 月に確認された攻撃の概要

◆ **攻撃 1:ウェブサーバへの不正なスクリプトのアップロード**

1. ウェブサイトの html コード(html コンテンツ)は改ざんされず、ウェブサーバ上に不正なスクリプトファイルがアップロードされます。
2. スクリプトの内容そのものは、難読化されています。

◆ **攻撃 2:不正なスクリプトへ誘導するリンクの埋め込み**

1. 別のウェブサイトの html コンテンツが改ざんされ、上記の「攻撃 1」でアップロードされたスクリプトファイルへのリンクが埋め込まれます。

2. 当該ウェブサイトが閲覧されると、「攻撃 1」でアップロードされたスクリプトファイルを自動的にダウンロード、および実行されます。

多くの場合、それぞれの攻撃で使用されるスクリプトは、別々のサーバに置かれており、いわゆる「クロスサイトスクリプト」として実行されます。
10 月に確認された攻撃手法は、5 月に確認されたものより手口が複雑化しています。その為企業のウェブサイトの管理者が、自社のウェブサイトが改ざんされていることに気づかず運用を続け、被害が拡大する可能性があります。
「Gumblar ウイルス」によって、不正なスクリプトが埋め込まれるウェブサイトは、一般のウェブサイトである場合がほとんどです。その為、「悪質サイトのブラックリスト」方式による検知は困難です。

「Gumblar ウイルス」被害の推移（2009 年 6 月～11 月）（図表 3）

「Gumblar ウイルス」により改ざん被害を受けたと思われるウェブサイトの数は、2009 年 6 月、7 月と、2009 年 10 月、11 月に確認されている数や発生期間に大きな違いがあります（図表 3 参照）。10 月は大量のウェブサイトが改ざん被害を受けていることが確認されています。また被害の発生期間も、6 月、7 月、10 月は 1 週間程度で終息していたましたが、11 月は、20 日以上の長期にわたっています。

これらの結果は、「Gumblar ウイルス」の新しい攻撃手法が、以前の攻撃手法に比べて、大きな影響力を持っていることが原因によるものと思われます。今後も攻撃手法の変化や、亜種の発生により、さらに被害が拡大、長期化する恐れがあります。

「Gumblar ウイルス」被害：ドメイン別集計（2009 年 6 月～11 月）（図表 4）

図表 4.

ドメイン	Total	企業・団体	個人	学校	その他
.co.jp	179	128	44	5	2
.ne.jp	207	28	161	0	18
.or.jp	57	10	47	0	0
.ac.jp	4	0	0	4	0
.jp	306	182	109	0	15
.com	493	257	135	0	101
.net	121	18	103	0	0
.info	84	0	59	0	25
その他	56	5	45	0	6
Total	1507	628	703	9	167

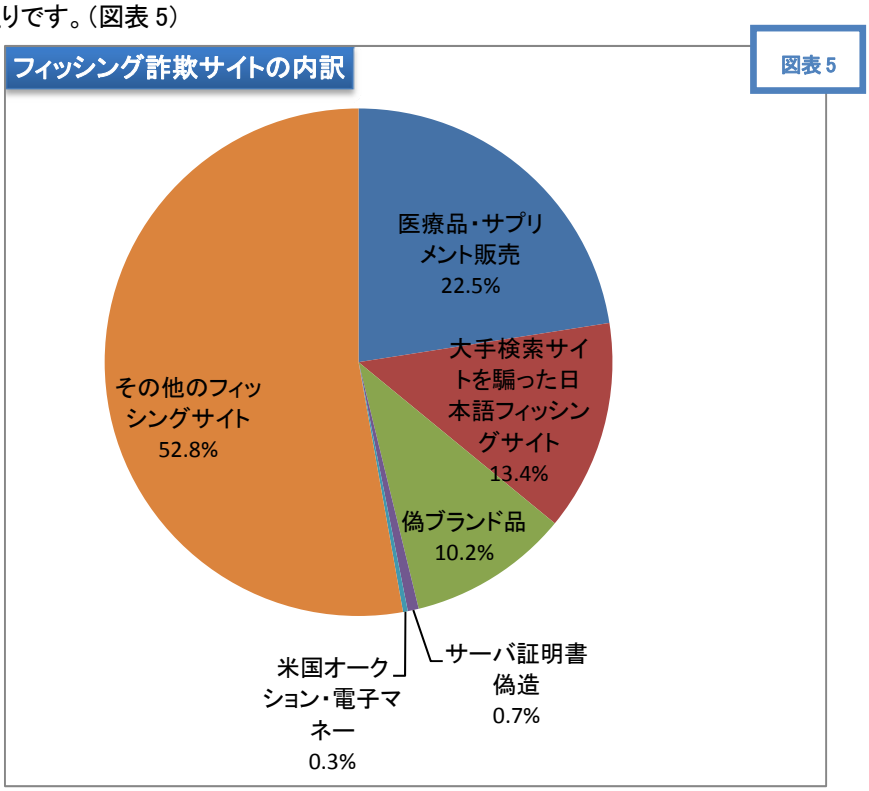
「gred でチェック」で収集された URL の中から、「Gumblar」ウイルスにより、改ざん被害を受けたウェブサイトを抽出し、コンテンツの詳細調査を行いました。被害に遭ったウェブサイトは、個人のウェブサイトと思われるものが、全体の 46.6%を占めていますが、企業のウェブサイトと思われるものも 41.7%。確認されています（図表 4）。また、該当する URL についてさらに調査を行ったところ、約 7.5%の URL は複数回改ざん被害に遭っていることが確認されました。

以前「Gumblar ウイルス」による改ざん被害を受けたウェブサイトが、FTP サーバの ID・パスワードを変更していないなど、適切な対処を行わなかった場合、再び攻撃に晒される可能性があります。ウェブサイトを運営している企業では、細心の注意を払って、自社ウェブサイトの検査と継続的な監視等、速やかに対策を行う必要があります。

2.2　フィッシングサイトの出現周期

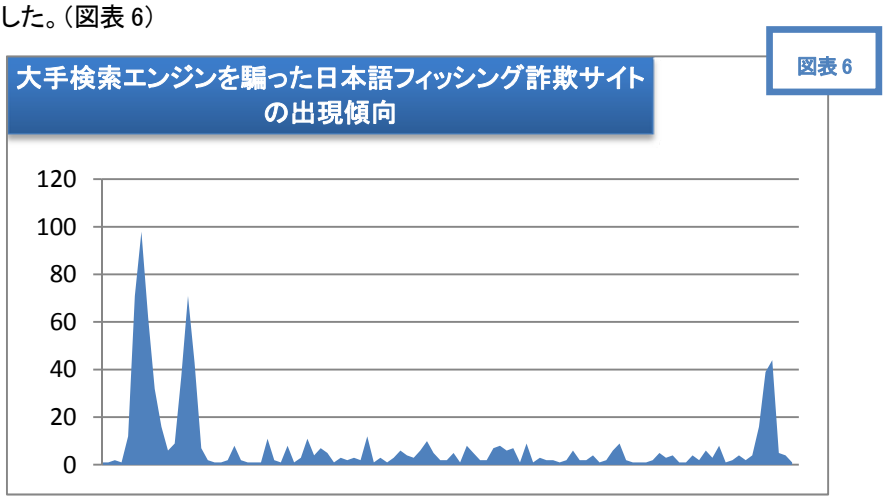
2.2.1 フィッシング詐欺サイトの内訳

gred セキュリティレポートの統計開始後（2009 年 6 月～11 月）、6,587 件のフィッシングサイトを検知しています。内訳は以下の通りです。（図表 5）



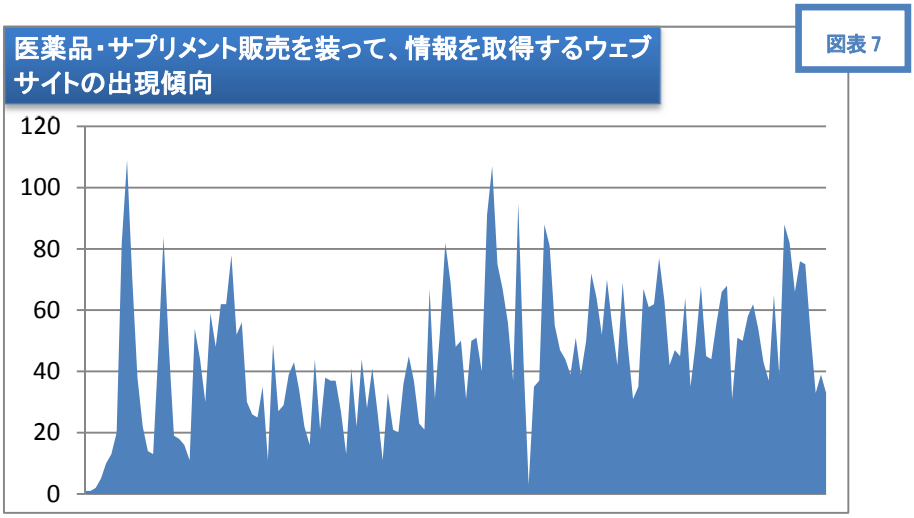
2.2.2 フィッシング詐欺サイトの出現傾向

先端技術研究所が調査を行ったところ、フィッシングサイトの種類によって、その出現傾向に大きな違いがあることが確認されました。（図表 6）



上記（図表 6）の例では、実在する会社のウェブサイトを偽装しています。当該企業がフィッシング詐欺サイトの閉鎖を積極的に行っている為、比較的短い期間で閉鎖されています。その為、一時的に報告件数は急増するものの、沈静化も早い傾向にあります。出現時期についての周期性は無いものの、そのコンテンツはどの時期のものも酷似しています。フィッシング詐欺サイト作成の為の「キット」が出回っている可能性があります。このようなキットが広く流通すると、フィッシング詐欺サイトの出現周期の短期化やウェブサイト数の増大により、被害が増加する可能性があります。

図表 7



上記（図表 7）の例では、実在の企業を偽装していません。ウェブサイトの閉鎖を積極的に進める企業が存在しない為、常に情報を取得する為のウェブサイトが存在するという状態になっています。「医薬品・サプリメント」を紹介する手口の他に、偽ブランド品や高級腕時計の販売を行うウェブサイトを装って、クレジットカード番号をはじめとするいわゆる「個人情報」の取得を試みるウェブサイトの存在が確認されています。

これらの手口のウェブサイトは、インターネット上に常設されているような状態になっています。閉鎖もされず、ユーザが遭遇する率も高いため、情報取得が効率よく行える為、フィッシング詐欺サイトよりも多く報告されています。

3　個人・企業それぞれに求められる、セキュリティ対策とは？

3.1　個人向けの対策：「gred でチェック」「Internet SagiWall（インターネット・サギウォール）」「gred AntiVirus アクセラレータ」

インターネットユーザはウェブサイトを閲覧する前に、その安全性を確認する必要があります。セキュアブレインでは、無料でご利用いただけるウェブセキュリティサービス「gred でチェック」（http://www.gred.jp）を提供しています。

また、ウイルス対策を無料で強化する、コミュニティ型ウイルス対策製品「gred AntiVirus アクセラレータ」（http://www.securebrain.co.jp/products/gredavx/index.html）もダウンロード提供を行っています。

オンライン詐欺対策ソフトとしては、閲覧するウェブサイトのコンテンツやリンク先等複数の要素を解析し、その危険性を判断する「Internet SagiWall」（http://www.securebrain.co.jp/products/sagiwall/index.html）を提供しています。危険なウェブサイトを閲覧してしまった場合でも、瞬時に画面を遮断し警告画面を表示します。

■「gred でチェック」URL

http://www.gred.jp

■「gred AV アクセラレータ」URL

http://www.securebrain.co.jp/products/gredavx/index.html

■「Internet SagiWall」の製品紹介 URL

http://www.securebrain.co.jp/products/sagiwall/index.html

3.2　企業向けの対策：「gred セキュリティサービス」

企業のウェブサイトの管理者は、自社のウェブサイトの安全性を、自動で定期的に監視するソリューションが必要です。セキュアブレインでは、企業のウェブサイトが不正に改ざんされていないかを定期的に監視し、問題が発見された場合には、即座に管理者に通知する、SaaS 型セキュリティサービス「gred セキュリティサービス」をご提供しています。

「gred セキュリティサービス」では、「30 日無償トライアル版」を用意しています。「無償トライアル版」は、自社のウェブサイトのURL、アラートメール送信先等の情報を登録するだけで、すぐにサービスを利用開始することができます。「gred セキュリティサービス」は、検査対象となるウェブサイトのコンテンツを、ダウンロードして検査を行いますので、ウェブサイトへの負荷はほとんどかかりません。

■「gred セキュリティサービス」30 日間無償トライアルお申込み URL

http://www.securebrain.co.jp/products/gred/trial.html

■「gred セキュリティサービス」の機能詳細説明 URL

http://www.securebrain.co.jp/products/gred/function.html

以上

セキュアブレインについて:

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する日本発のセキュリティの専門企業です。詳細は、www.securebrain.co.jp をご覧ください。

◆ gred セキュリティサービスに関するお問い合わせ先 ◆

gred セキュリティサービス　カスタマーサービスセンター

e-mail：tech_support@securebrain.co.jp

電話：0120-988-131

※ダイヤル後、アナウンスに従い『1』を押してください。

営業時間　月～金、9:00-12:00 13:00-17:00　土日祝祭日を除く

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン　広報担当：丸山　芳生（まるやま　よしお）

e-mail：info@securebrain.co.jp

電話：03-3234-3001、FAX：03-3234-3002　〒102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F