

セキュアブレイン gred セキュリティレポート Vol.4【2009年10月】

再び猛威をふるう「Gumblar ウイルス」、被害サイトの53%は企業のウェブサイト フィッシング詐欺サイトでは「薬品の違法販売サイト」が台頭

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)」かを判断します。

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
- 1.2 「gred でチェック」で検知した脅威の月毎の推移
- 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

2 悪質サイトの傾向分析

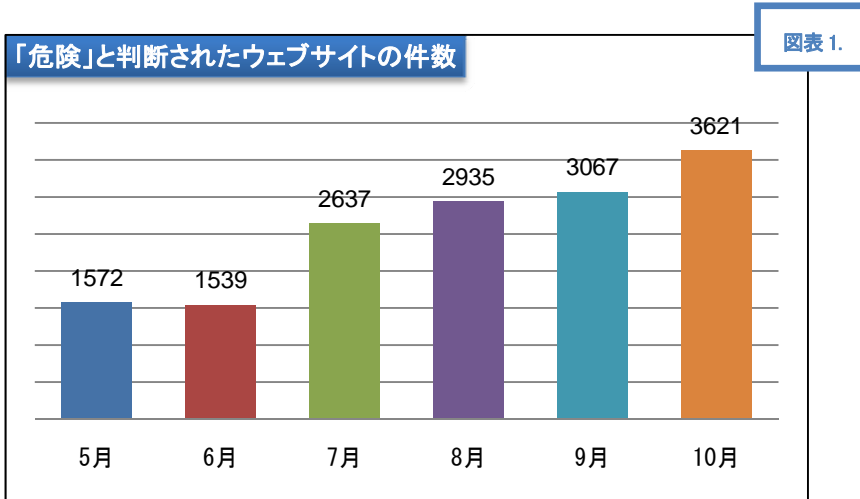
- 2.1 再び猛威を振るう「Gumblar ウイルス」、攻撃手法は複雑化
 - 2.1.1 新たに確認された「Gumblar ウイルス」の攻撃手法
 - 2.1.2 企業ウェブサイトの被害は引き続き深刻。ウェブサイトの監視等、速やかな対処が急務
- 2.2 薬品やサプリメントのネット販売を装い、クレジットカード番号等の個人情報を収集する、フィッシング詐欺サイトの一種に注意が必要

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？

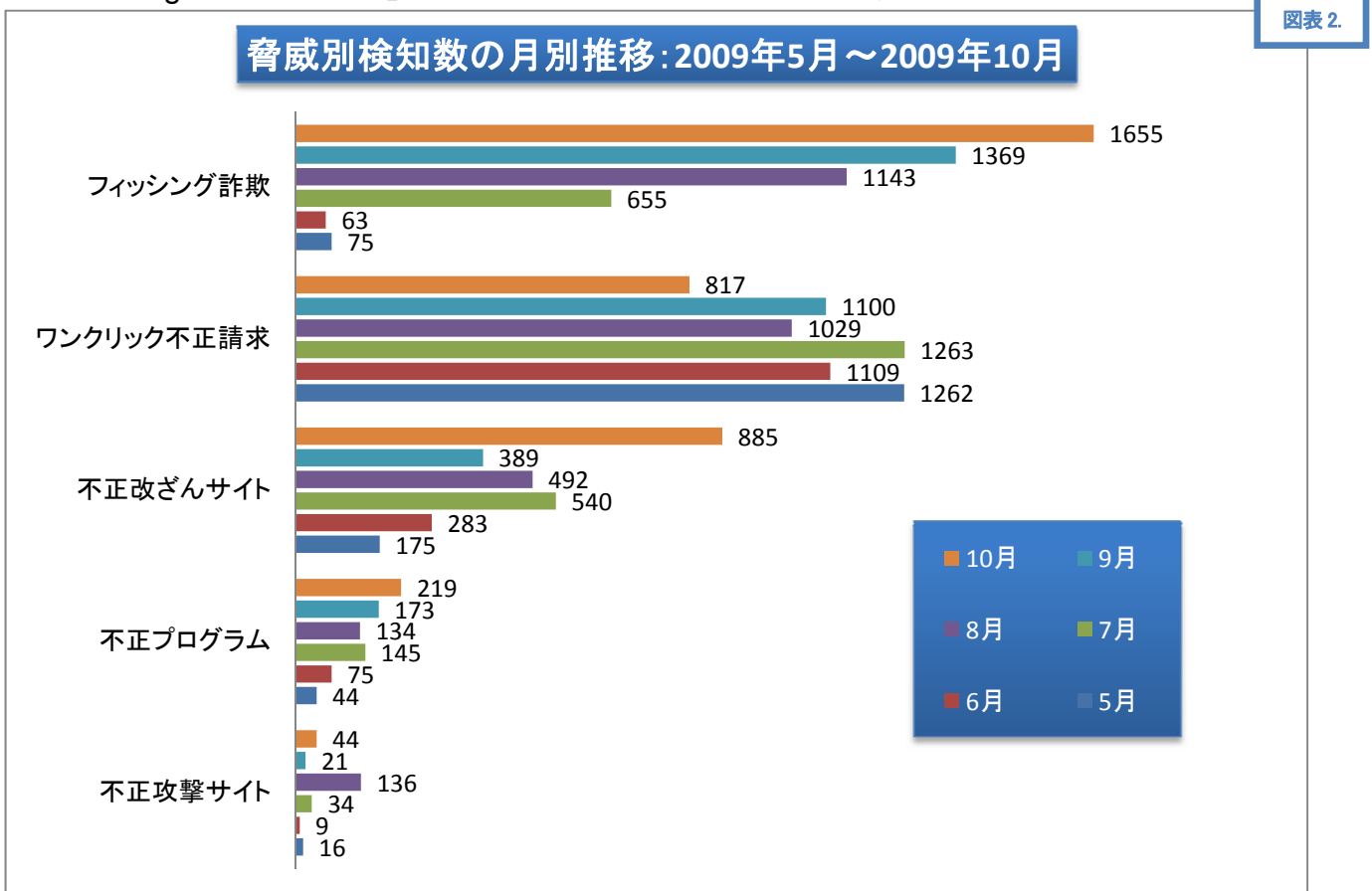
- 3.1 個人向けの対策:「gred でチェック」「Internet SagiWall(インターネット・サギウォール)」
- 3.2 企業向けの対策:「gred セキュリティサービス」

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10月）：3,621件（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）



- 「危険」と判断されたウェブサイトの件数は、3,621件で、統計開始後、6ヶ月連続で増加が続いています。（前月比 118.1%）（図表1参照）
- 2009年10月は、「フィッシング詐欺」（1,655件：前月比 121.0%）と「不正改ざんサイト」（885件：前月比 227.5%）、「不正プログラム」（219件：前月比 126.6%）の検出件数が、共に最高値を記録しています。（図表2参照）

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	本物そっくりで、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 再び猛威を振るう「Gumblar ウイルス」、攻撃手法は複雑化

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)の報告が急増しました。これは、「Gumblar ウイルス」が新たな手法を使い、攻撃を開始したことが原因と思われます。「Gumblar ウイルス」は、FTP サーバの ID・パスワードを収集・悪用することで、ウェブサイトの改ざんを行い、感染被害を拡大します。

先端技術研究所が調査を行ったところ、以下のような攻撃手法が確認されています。

2.1.1 新たに確認された「Gumblar ウイルス」の攻撃手法

新たに確認された攻撃手法は、既存のウェブサイトに対して、大きく分けると 2 つの手法で改ざんを行います。

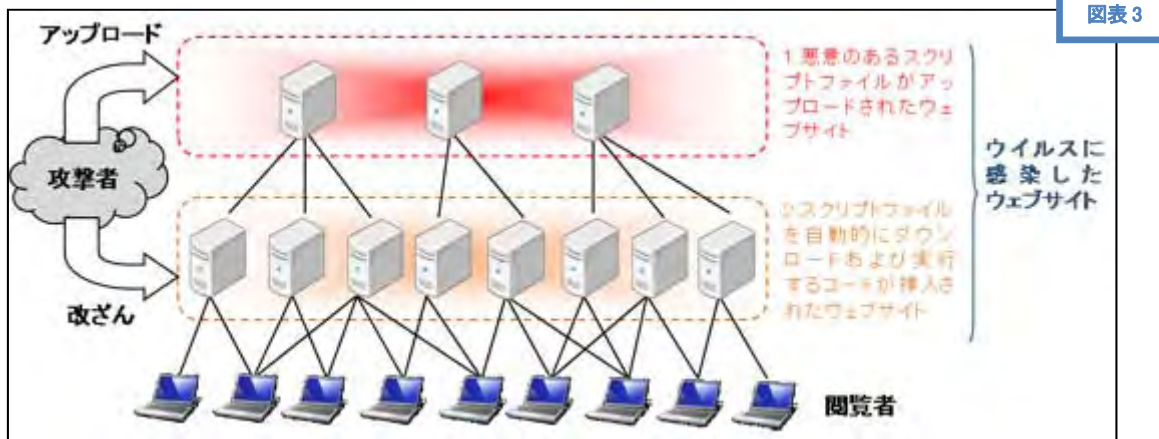
この改ざんは、別々のサイトに置かれていることが考えられますが、2 つの改ざんを 1 つのサーバに対して行われることがあることも確認しています。

1. ウイルスに感染させる機能を持たせるために、ウェブサイトに感染用の悪意のある、難読化されたスクリプトファイルがアップロードされます。

- 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。感染を検知するためには、ウェブサイト管理者が正常な状態のウェブサーバのファイル構成を把握しておき、不正なファイルが存在するか否か確認しなければなりません。
- スクリプトファイル名はソーシャルエンジニアリング的なテクニック(例えば、shopping_cart.php 等)を使ったものになっており、ファイル名からその成否を判断することが難しくなっています。また、スクリプトは難読化されており、その詳細を理解することは困難です。さらに、このスクリプトファイルが置かれている directory に、「/s」等のようなサブディレクトリを作成し、複数のファイルを作成していることも確認しています。

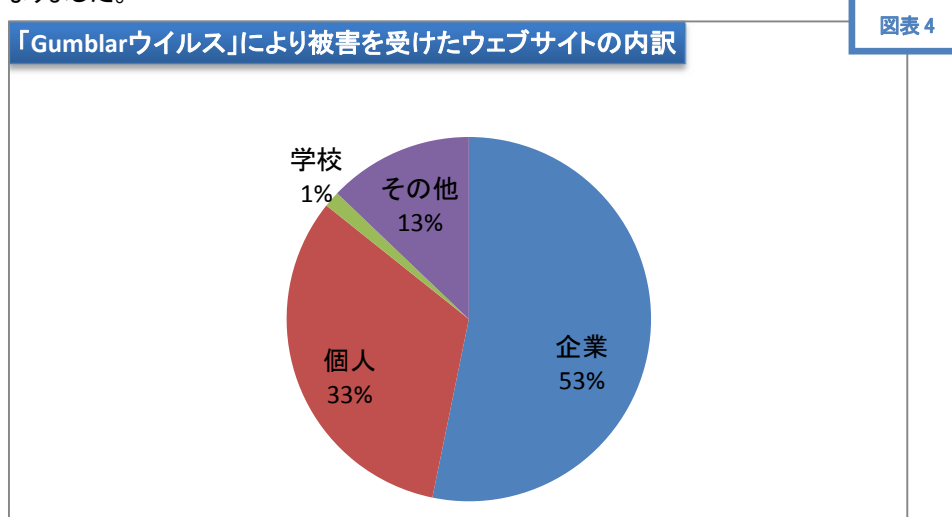
2. 「1」でアップロードされたスクリプトファイルを、自動的にダウンロードおよび実行させる機能です。

- こちらのウェブサイトは、直接 html の内容が改ざんされています。一般ユーザが当該ウェブサイトを開くと同時にこのスクリプトが実行され、「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せます。また、改ざんされた html コードは、難読化されていません。
- 多くの場合、これらのスクリプトは他のサーバに置かれており、俗に言う「クロスサイトスクリプト」として実行されます。これらの不正なコードを仕掛けられた 2 種類のウェブサイトは、元は一般のウェブサイトなので、ブラックリスト方式による検知は難しくなります。



※以前の攻撃手法については、2009年6月12日の報道発表資料(http://www.securebrain.co.jp/news/090612_gred_gen0.html)をご確認ください。

2.1.2 企業ウェブサイトの被害は引続き深刻。ウェブサイトの監視等、速やかな対処が急務
 先端技術研究所が、「gred でチェック」で収集した情報の分析を行ったところ、被害を受けたウェブサイトの内訳は以下のようになりました。



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、再び悪意のあるスクリプトを埋め込ま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。

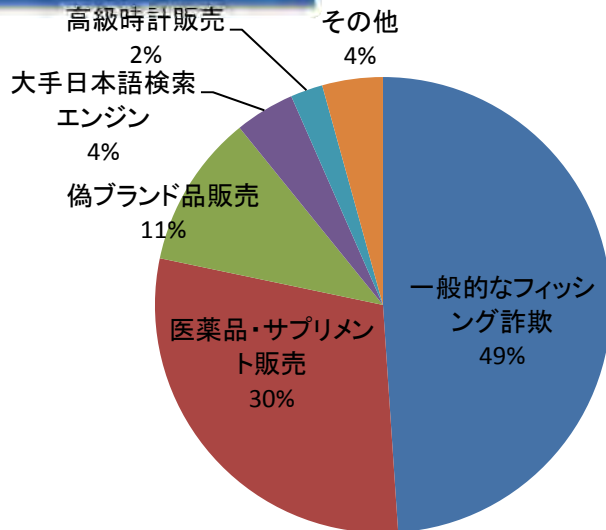
2.2 薬品やサプリメントのネット販売を装い、クレジットカード番号等の個人情報を収集する、フィッシング詐欺サイトの一種に注意が必要

2009年10月は、1,655件の「フィッシング詐欺」の報告がありました。2009年9月の1,369件に比べ、報告件数が急激に増加しました。

先端技術研究所が調査を行ったところ、医薬品・サプリメントの販売を行うように装い、情報を不正に取得しようとするウェブサイトの割合が増加していることがわかりました。(図表5参照)

図表 5

フィッシング詐欺サイトの種類 2009年10月



先端技術研究所では、その他、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。これらのウェブサイトは、英語によって記載されているものがほとんどです。興味本位での閲覧、購買には十分注意してください。

医薬品・サプリメント販売を装って個人情報を取得するウェブサイトの例

- ・ 医療従事者のモデル等を使ったデザインで安心感を演出するトップページ



- ・ 住所、氏名、クレジットカード番号などの情報を取得

Name	Price	Quantity	Sum
Viagra + Cialis (Generic) Viagra 100mg x 100mg + Cialis 10 pills x 20mg	\$69.99	1	\$69.99
Viagra(Generic) 4 pills x 100 mg	\$0.00	1	\$0.00
Delivery type Insurance Airmail			\$15.90
Total			\$85.89

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）」

インターネットユーザはウェブサイトを開覧する前に、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。

またセキュアブレインの、個人向けのセキュリティ対策ソフト「Internet SagiWall」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、その危険性を判断します。危険なウェブサイトを開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>

■「Internet SagiWall」の製品紹介 URL

<http://www.securebrain.co.jp/products/sagwall/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