Press Release

2009 年 8 月 17 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.1【2009 年 7 月】

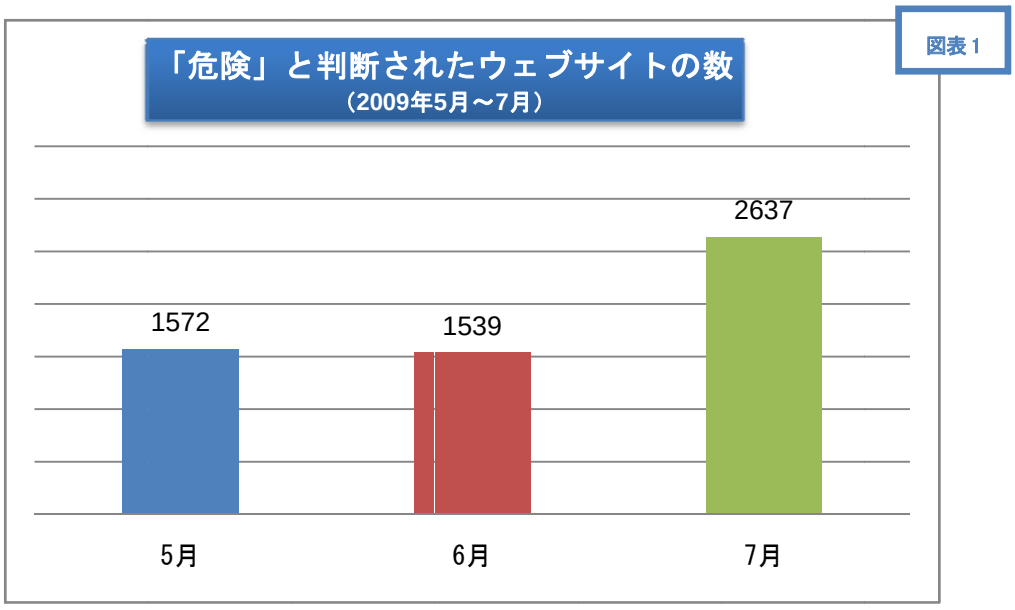
「大手検索エンジンを騙った、日本語フィッシング詐欺サイト」と「Gumbler/JSRedir-R ウイルス（通称 GENO ウイルス）により改ざんされたウェブサイト」が急増

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」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。

gred セキュリティレポート概要

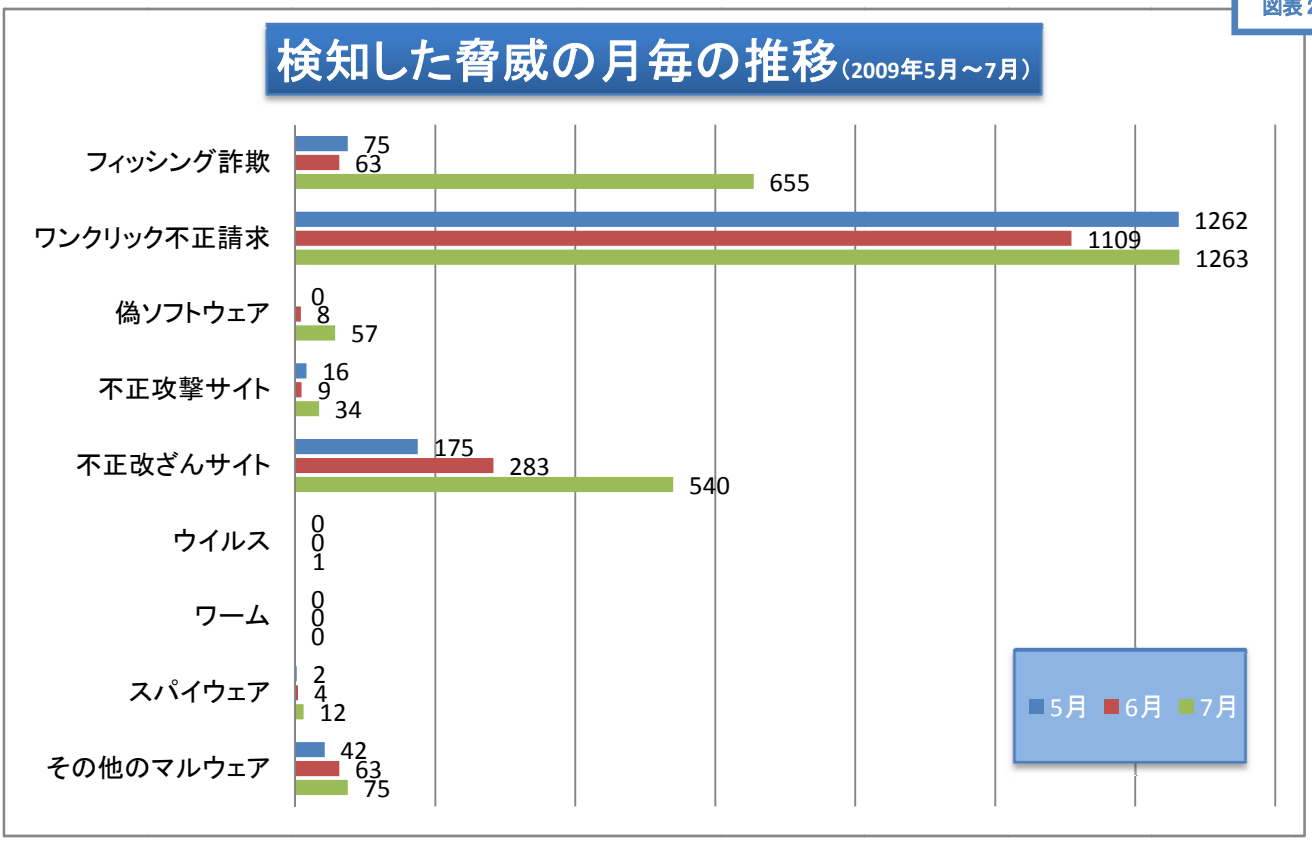
「危険」と判断されたウェブサイトの数（2009 年 7 月）：2,637 回



- 「危険」と判断されたウェブサイトの数は、大幅に増加しています。（前月比 183.6%）（図表 1 参照）
- 「gred でチェック」が「危険」と判断した場合には、そのウェブサイトにどのような脅威が存在しているかを、具体的に表示します。（内訳は図表 2 参照）

「gred でチェック」で検知した脅威の月毎の推移

図表 2



2009 年 7 月は、「大手検索エンジンを騙った、日本語フィッシング詐欺サイト」が大量に発生したことと、「通称 GENO ウイルス」による被害が急増したことにより、「フィッシング詐欺」「不正改ざんサイト」の数値が急増しています。

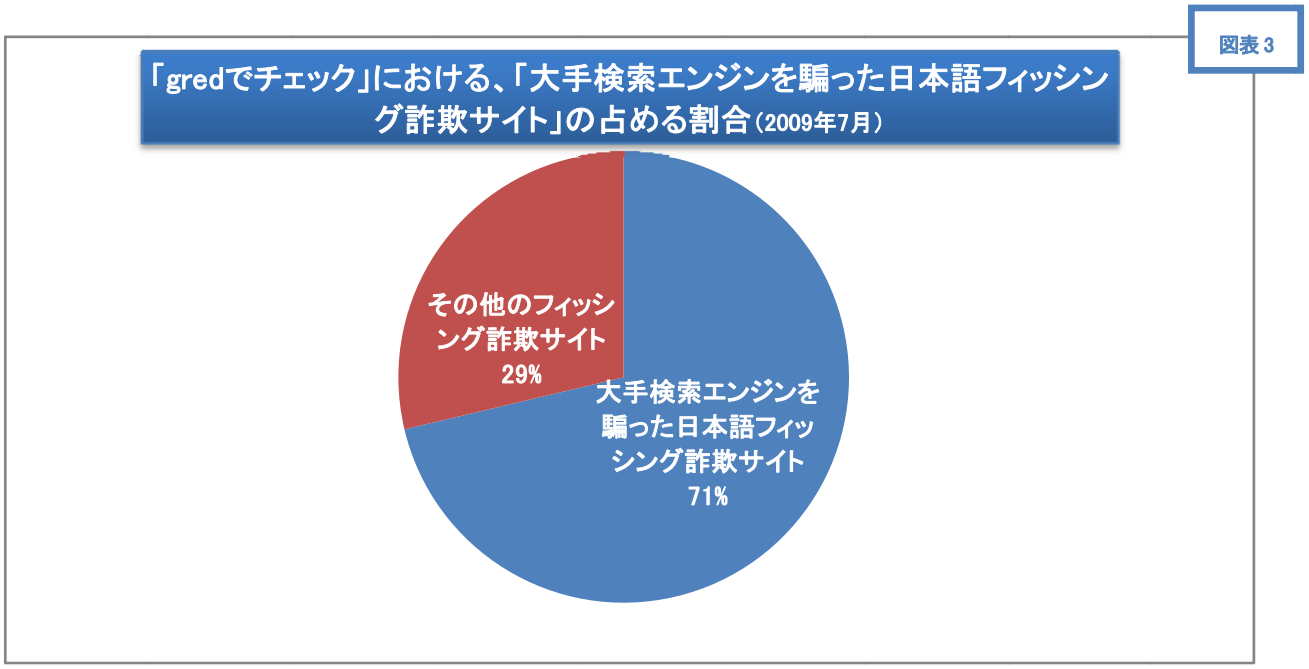
「gred でチェック」のチェック結果に表示される脅威の説明

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攻撃を行う事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	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	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	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	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。

複数の URL を使い、大量の個人情報を取得する「大手検索エンジンを騙った日本語のフィッシング詐欺サイト」が急増

「gred でチェック」で検知したフィッシング詐欺の総数 655 件のうち、「大手検索エンジンを騙った日本語フィッシングサイト」は、467 件（全体の 71%）でした。

図表 3



以下は、全て「大手検索エンジンを騙った日本語フィッシング詐欺サイト」の URL です。日時は、当該 URL が最初に「gred でチェック」で解析された日時です。

図表 4

7/17（金）21:47	http://****-up-grade.com/login-id-center/
7/18（土）00:23	http;//****amer-srvice.fc2rs.com
7/18（土）15:20	http://****teproceduresupport.com/account-web-up-load/
7/19（日）09:24	http://****rmationupdate.info/user-account-id/
7/20（月）23:01	http://****tesupportcenter.com/account-login-user-date/
7/21（火）04:25	http://****ntesenter.blackapplehost.com/yahoo-auction.acounte/
7/24（金）20:26	http://****yaloginuser.com/account-login-user-date-web/
7/25（土）04:56	http://****domainname.com/id-update-login-url/
7/25（土）07:43	http://****account.biz/your-account-id-uplode/
7/26（日）00:50	http://****downcenter.powweb.com/login-user-account-id/
7/27（月）13:33	http://****esenter.blackapplehost.com/yahoo-auction.acounte

ホスト名の一部を「*」でマスクしています

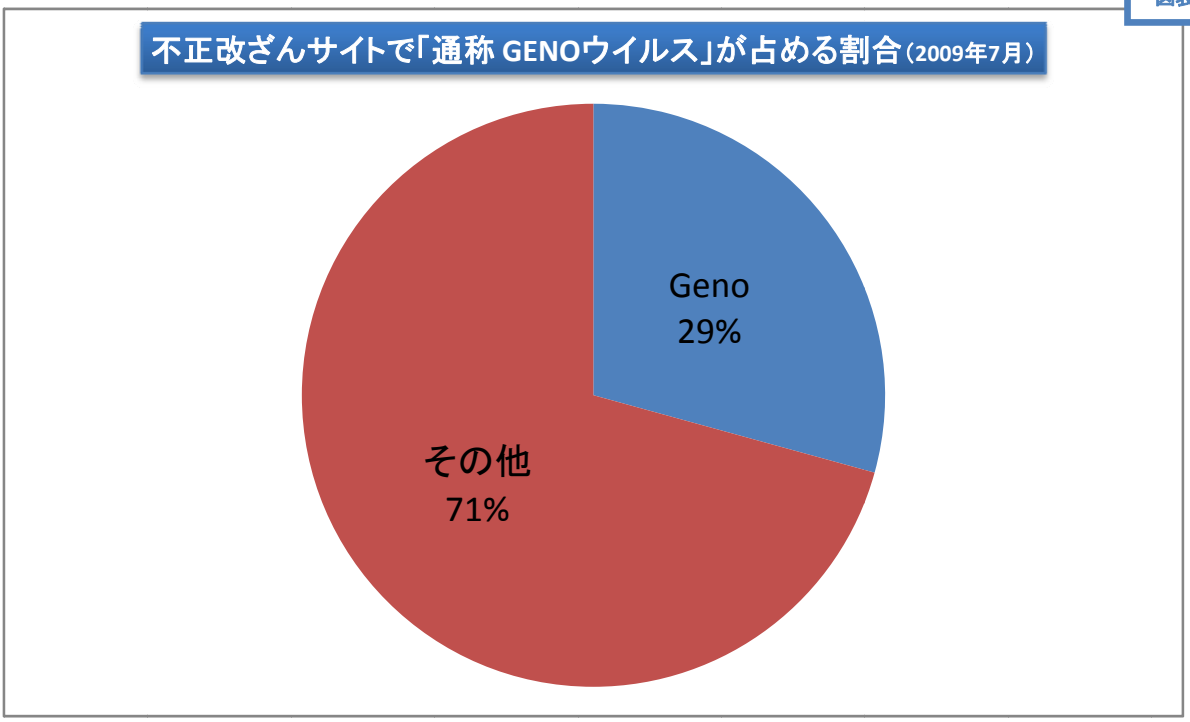
2009 年 7 月 17 日以降、ほぼ毎日のように新しい URL のフィッシング詐欺サイトが出現しています（図表 4 参照）。今後も日本のインターネットユーザを狙った、日本語のフィッシング詐欺サイトが増加する可能性がある為、十分な注意が必要です。

ウェブサイト上で個人情報の入力を要求された場合には、念のため「gred でチェック」を利用し、そのウェブサイトの安全性を確認することを推奨します。また、危険なウェブサイトを自動でブロックする機能を持った、セキュアブレインのセキュリティ対策ソフト「Internet SagiWall」は、フィッシング詐欺サイトをはじめとした、危険なウェブサイトへのアクセスを未然に防止します。

依然として続く、「通称 GENO ウイルス」による改ざん被害

「gred でチェック」で検知した「不正改ざんサイト」（総数 540 件）のうち、「通称 GENO ウイルス」によって不正に改ざんされたウェブサイトは、157 件（全体の 29%）でした。

図表 5



不正改ざんサイトの閲覧者は、ウイルス等のマルウェアに感染し、個人情報の漏えいの被害等を受ける場合があります。「通称 GENO ウイルス」は、ユーザが使用する、パソコンの脆弱性を利用して、感染を広げていきます。その為、ウェブサイトに脆弱性が無くても、感染したパソコンから漏えいした情報が悪用され、ウェブサイトが改ざんされてしまう場合があります。セキュリティソフトが「危険なウェブサイト」を検知できずに、ユーザが気づかないうちにウイルスに感染し、さらに別のウェブサイトが改ざんされるという被害連鎖が発生しています。

閲覧者が個人情報漏えい等の被害を受けた場合、ウェブサイトが不正改ざんされた企業は、被害者であると同時に、情報漏えいの原因を作った加害者として見られる可能性があり、企業のブランドイメージや取引における信頼性等、企業活動に甚大な影響を及ぼすことが考えられます。

個人・企業それぞれに求められる、セキュリティ対策とは？

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

■「Internet SagiWall」の製品紹介 URL

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

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:tec_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