

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.9【2010年3月分統計】

フィッシング詐欺サイトの傾向に変化、「Gumblar ウイルス」の攻撃手法との関連性も

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。

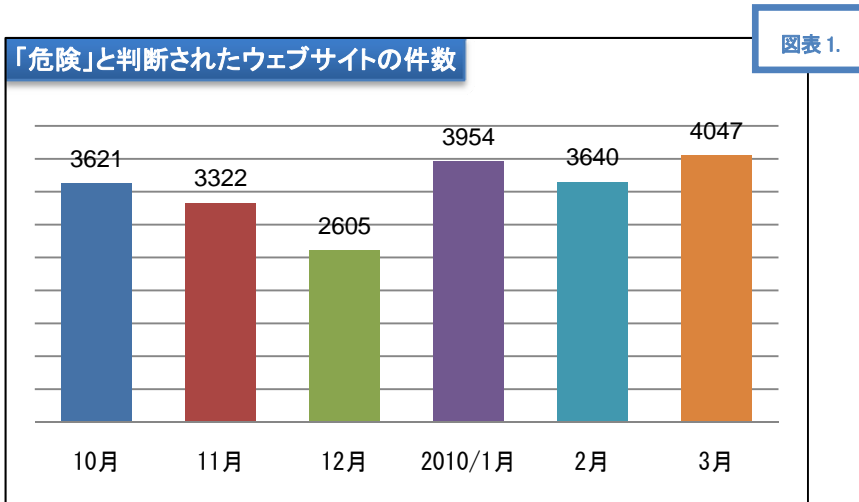
本レポートに含まれる内容

内容

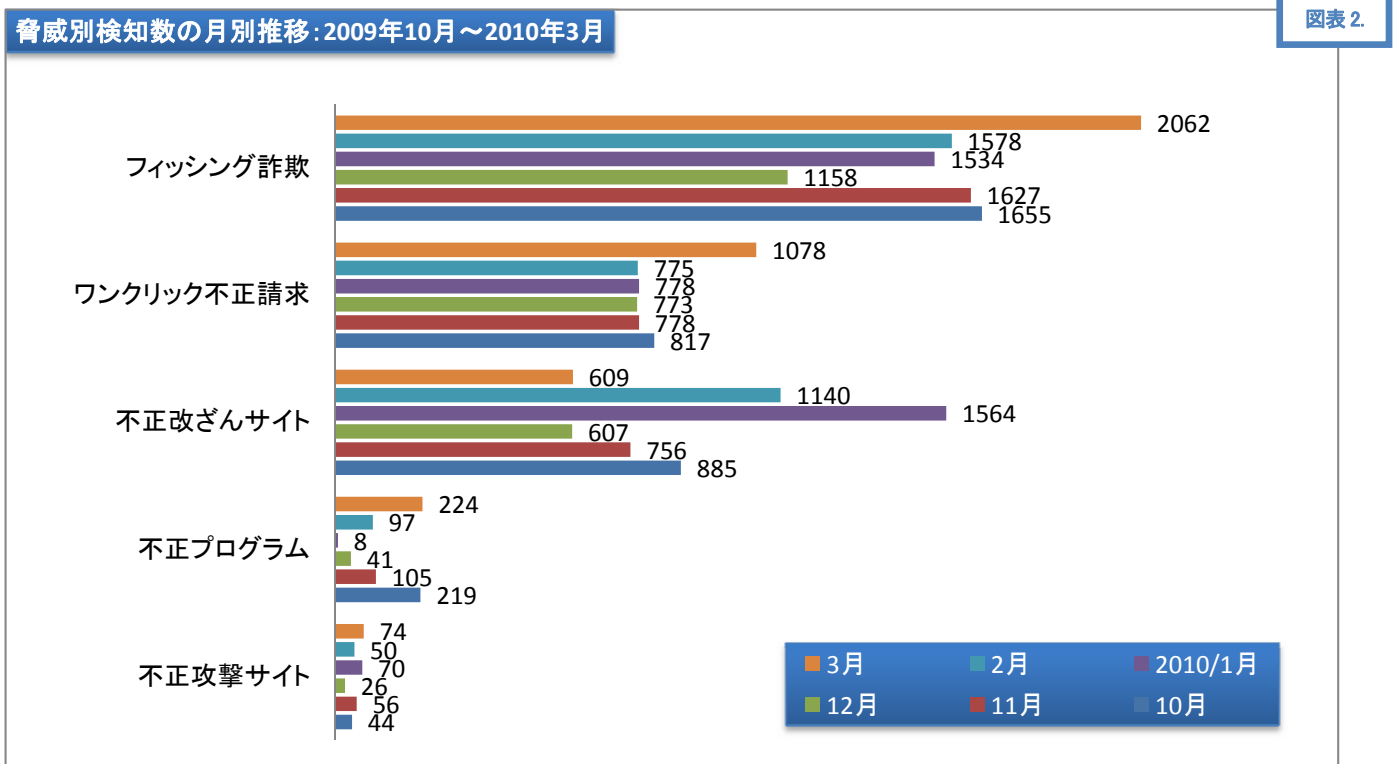
- 本レポートに含まれる内容..... 1
- 1 gred セキュリティレポート概要..... 2
 - 1.1 「危険」と判断されたウェブサイトの数(2010年3月):4,047件(図表1)..... 2
 - 1.2 「gred でチェック」で検知した脅威の月毎の推移(脅威別)(図表2)(単位:件)..... 2
 - 1.3 「gred でチェック」月別総利用数(2009/10月~2010/3月)..... 2
 - 1.4 「gred でチェック」のチェック結果に表示される脅威の説明..... 3
- 2 最新情報:フィッシング詐欺サイトの傾向に変化、「Gumblar ウイルス」の攻撃手法との関連性も..... 3
 - 2.1 フィッシング詐欺サイトの画面ショット(図表3-1)..... 4
 - 2.2 暗号化されたコンテンツ画面(図表3-2)..... 4
- 3 ウェブ改ざん被害は減少傾向だが、油断は大敵..... 5
 - 3.1 ウェブサイトのセキュリティ対策の総点検をこの時期に..... 5
 - 数値で見る「ウェブサイト改ざん被害」(図表4-1、4-2、4-3)..... 5
 - 3.2 ゴールデンウィーク前に、セキュリティ対策を再点検..... 7
- 4 詐欺サイトの検知数が急増..... 7
 - 4.1 詐欺サイト検知数の状況..... 7
 - 4.2 「個人情報を入力する手法」の傾向..... 8
 - 4.3 「詐欺サイト」の傾向とその対策における留意点..... 8
- 5 個人・企業それぞれに求められる、セキュリティ対策とは?..... 9
 - 5.1 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」 9
 - 5.2 企業向けの対策:「gred セキュリティサービス」..... 9

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(2010年3月):4,047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(脅威別)(図表2)(単位:件)



1.3 「gred でチェック」月別総利用数(2009/10月~2010/3月)

| 月 | 2009/10月 | 11月 | 12月 | 2010/1月 | 2月 | 3月 |
|------------------|----------|--------|--------|---------|--------|--------|
| 「gred でチェック」総利用数 | 39,569 | 39,330 | 40,697 | 70,999 | 55,927 | 54,995 |

- 「危険」と判断されたウェブサイトの件数は、4,047件(前月比111.2%)(図表1参照)。2009年5月の統計開始後の最高値です。
- 「不正改ざんサイト」の検知数は、前月より大幅に減少し609件(前月比53.4%)となっています。
- 「フィッシング詐欺」の検知数が、急激に増加しています。2010年3月の検知数2,062件(前月比130.7%)は統計開始後の最高値です。

- 「ワンクリック不正請求」の検知数が急増しています。2010年3月の検知数1,078件(前月比139.1%)は、過去6月間の最高値です。しかし、2009年5月～9月における「ワンクリック不正請求」の検知数の平均は1,152.6件ですので、その水準に戻ったと言えます。
- 「不正プログラム」の検知数も2010年2月から上昇傾向にあります。2010年3月の検知数224件(前月比231.0%)は統計開始後の最高値です。

1.4 「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、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 最新情報: フィッシング詐欺サイトの傾向に変化、「Gumblar ウイルス」の攻撃手法との関連性も

2010年4月23日にクレジットカード会社を騙ったフィッシング詐欺サイトが報告されました。(図表 3-1)

一般のウェブサイトにもフィッシング詐欺のコンテンツが作られていました。対象となったウェブサイトのFTPのID、パスワードが漏えいし、不正アクセスと改ざんが行われた可能性が考えられます。

また、ウェブサイトの監視を行うセキュリティ管理者や監視ソフトからの検知を逃れるためにコンテンツが暗号化されていました。(図表 3-2)

1. FTPのID、パスワードの不正入手
2. 一般のウェブサイトへの不正アクセスと改ざん
3. 改ざんしたコンテンツの暗号化

上記の手法は、2010年1月に大量の改ざん被害を及ぼした「Gumblar ウイルス」の攻撃手法との関連性が見受けられます。また、このウェブサイト以外にも、同様の手法によるフィッシング詐欺サイトが多数発見されています。

一般のウェブサイトが改ざんされ、フィッシング詐欺サイトが作られた場合、ブラックリストによる迅速な対応が困難な場合があります。その理由としては、以下の通りです。

理由1. ブラックリストに登録されたドメイン全体が、「悪質サイト」としてみなされてしまう危険性

理由2. フィッシングコンテンツ削除後の、ブラックリストからの迅速な削除

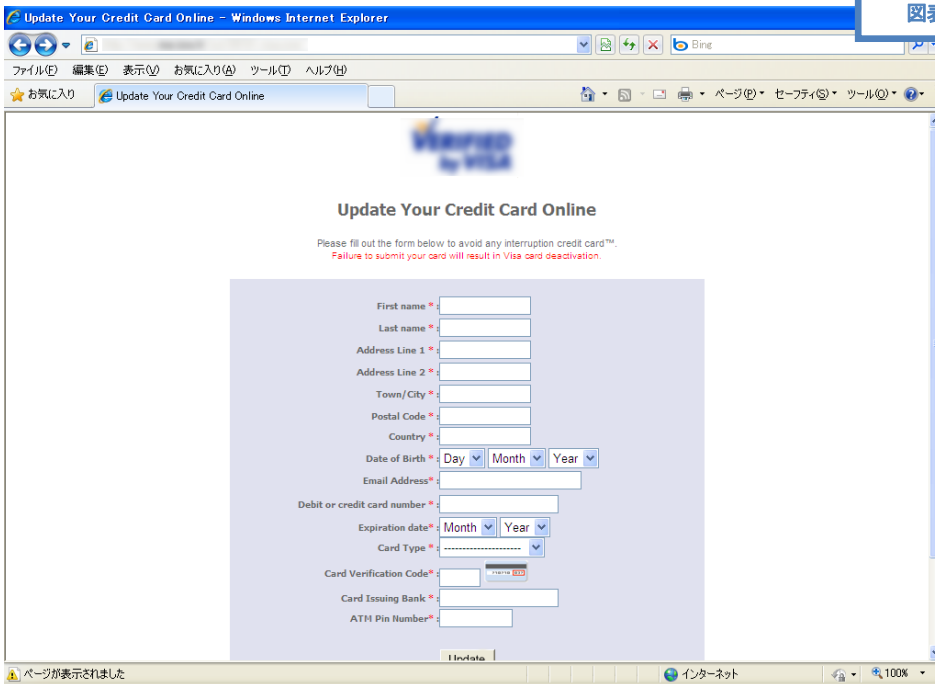
特に、理由2の問題に関しては、企業のビジネスに直結する問題でもあり、迅速な対応が求められます。しかし、一旦ブラックリストに登録されたURLが削除されるまでには、長い時間を要するのが現状です。

近年、「一般のウェブサイト」を改ざんし、不正なプログラムやコンテンツを仕掛ける事象が増えています。これらの事象が今後も増加した場合、ブラックリストによる対応は、その即時性と正確性が問われることとなります。

セキュアブレインでは、最新の脅威に対応可能な、ブラックリストを使わずに、「不正な改ざん」や「悪質なウェブサイト」を検知

する、セキュリティ対策製品やサービスを提供しています。ウェブサイトを運営する企業、インターネットを利用する個人のセキュリティ対策についての詳細は、本レポートの「5. 個人・企業それぞれに求められる、セキュリティ対策とは？」を参照してください。

2.1 フィッシング詐欺サイトの画面ショット(図表 3-1)



図表 3-1

2.2 暗号化されたコンテンツ画面(図表 3-2)



図表 3-2

暗号化されたコンテンツ

3 ウェブ改ざん被害は減少傾向だが、油断は大敵

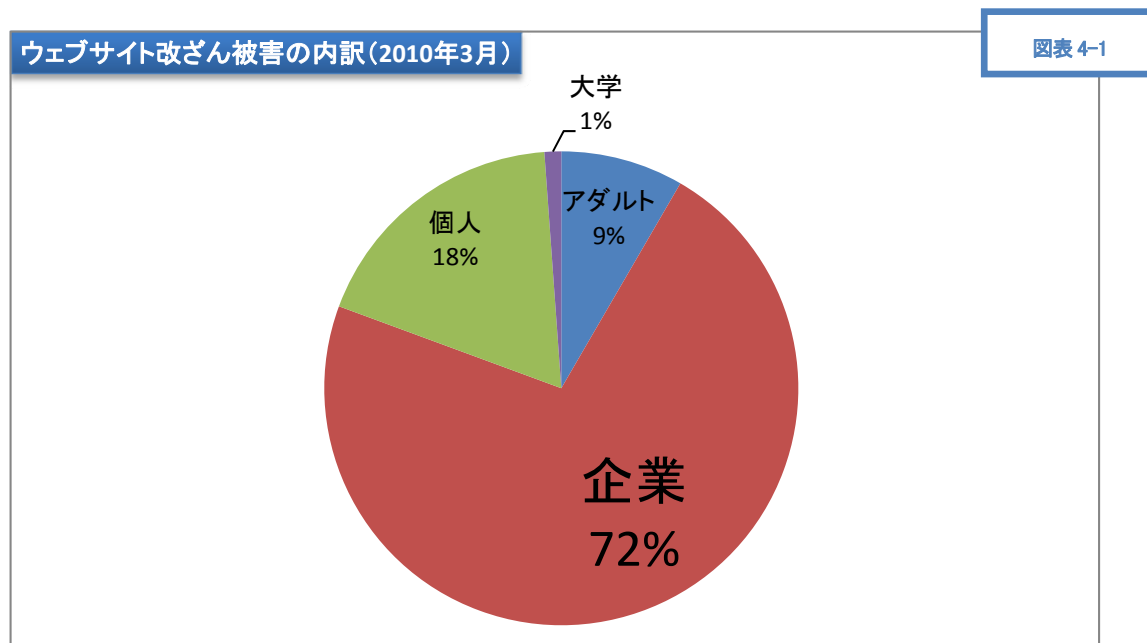
3.1 ウェブサイトのセキュリティ対策の総点検をこの時期に

2010年初頭から、「不正改ざんサイト」の検知数が急激に増加していましたが、2010年3月の統計では、大幅に検知数が減少しました。しかし、依然として、「不正改ざんサイト」に占める「企業のウェブサイト」の割合は高い数値を示しています(図表 4-1 参照)。企業のシステム管理者は、自社のウェブサイトの安全性を継続的に監視していく必要があります。また、『Gumblar』に代表される『Drive by Download タイプ』の攻撃(以下「Drive by Download タイプの攻撃」[※])による被害は、2010年1月、2月と比較すると数値は減少しているものの、依然として「不正改ざんサイト」の中で大きな割合を占めていることに変わりはありません(図表 4-2 参照)。全体の数値としては前月に比べ減少している為、被害事象は小康状態にあります。

このような状況ですが、「ウェブサイトの不正な改ざん攻撃」(以下「不正改ざん攻撃」)が終了したと考えることは危険です。下記のグラフ(図表 4-3)が示す通り、「不正改ざん攻撃」の大量発生は不定期に起きています。特にゴールデンウィークのような大型連休の際に被害が発生した場合には、ウェブサイトを運営している企業の対応が大幅に遅れる可能性があります。しかし、「Drive by Download タイプの攻撃」のように、ウェブサイトを閲覧したパソコンに不正プログラムを感染させる攻撃手法の場合には、一刻も早く、検知して修正を行わなければ被害が広範囲に拡大し、甚大な被害が発生する可能性があります。ゴールデンウィーク前に下記に紹介するような点に注意して、セキュリティ対策の総点検を行うことをお勧めします。

[※]セキュアブレインでは、「Gumblar」に代表される「ウェブサイトを不正に改ざんし、ウイルス等の不正なプログラムをウェブサイトの閲覧者のパソコンに感染させるような攻撃」を総称して、「Drive by Download タイプの攻撃」と呼んでいます。

● 数値で見る「ウェブサイト改ざん被害」(図表 4-1、4-2、4-3)



- 「不正改ざんサイト」における「企業」の割合は、依然として高くなっています。企業のウェブサイトが被害にあった場合、修復の為のコストはもちろんですが、顧客や取引先との信用問題に発展する可能性もあります。また、不特定対数のユーザが閲覧する為、「Drive by Download タイプの攻撃」を行うような改ざんが行われた場合、その被害が広範囲に及ぶ可能性があります。

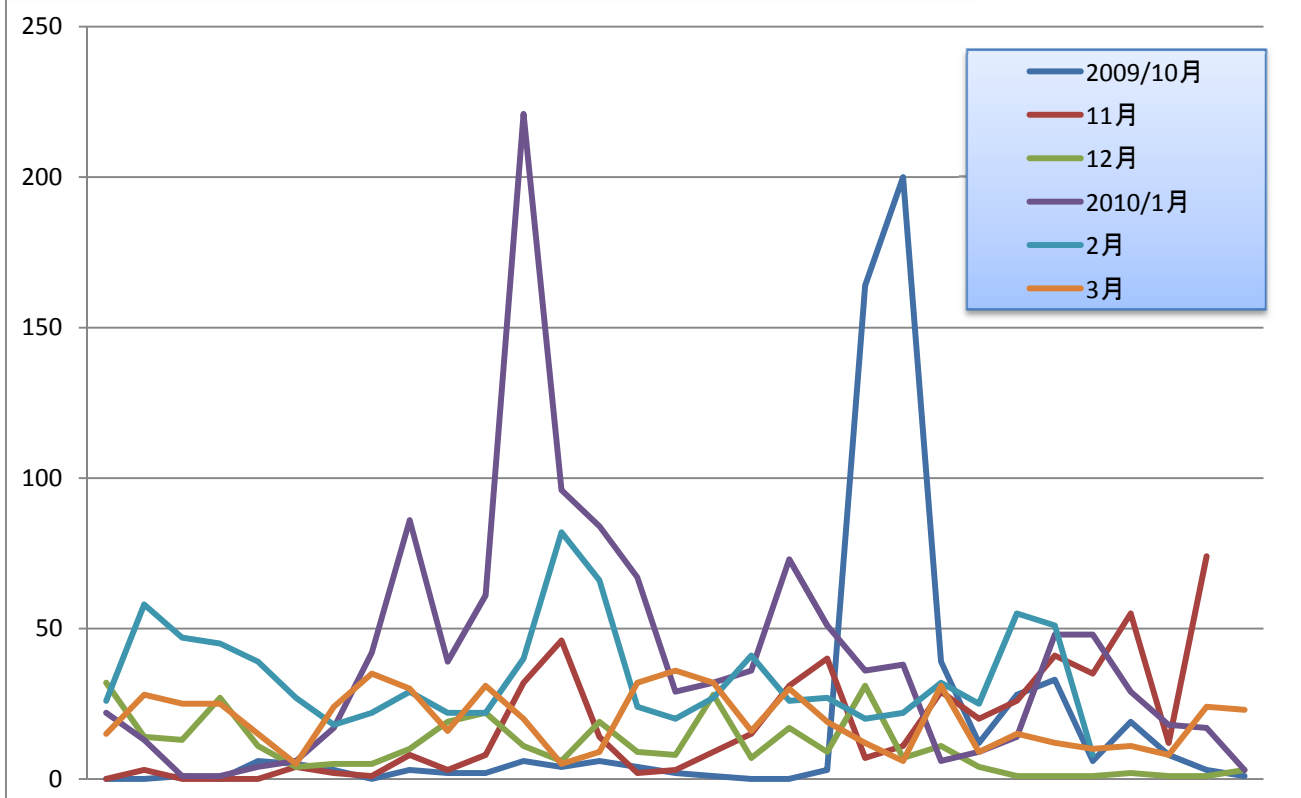
図表 4-2

| | 2010年3月 | 2010年2月 | 2010年1月 | 2009年12月 | 2009年10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 | 11.2% (453件/4,047件) | 25.3% (921件/3,640件) | 31.6% (1,248件/3,954件) | 12.9% (336件/2,605件) | 15.5% (562件/3,621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 | 74.4% (453件/609件) | 80.8% (921件/1,140件) | 79.8% (1,248件/1,564件) | 55.4% (336件/607件) | 63.2% (562件/889件) |
| 「Drive by Download タイプの攻撃」の中で、「企業ウェブサイト」が占める割合 | 76.2% (345件/453件) | 82.1% (756件/921件) | 80.9% (1,009件/1,248件) | 60.7% (204件/336件) | 53.2% (299件/562件) |

- 「Drive by Download タイプの攻撃」に関する数値は減少していますが、「ウェブサイトの不正改ざん」における攻撃手法の主役は、「Drive by Download タイプの攻撃」であることに変わりはありません。この攻撃は、自社のウェブサイトの改ざんにとどまらず、顧客や取引先、また自社のウェブサイトを閲覧したユーザへ被害が拡大します。その為、その修復に要する人員、時間、コストは図りしれません。また、この攻撃は、「セキュリティソフトによる検知が難しい」という特徴も併せ持っています。

「Drive by Downloadタイプの攻撃による被害」検知数の推移(2009/10月 - 2010/3月)

図表 4-3



- 「Drive by Download タイプの攻撃」による被害の検知数の増減を示しています。発生のピークの規模にばらつきがありますが、その発生時期についても周期性は確認できません。

3.2 ゴールデンウィーク前に、セキュリティ対策を再点検

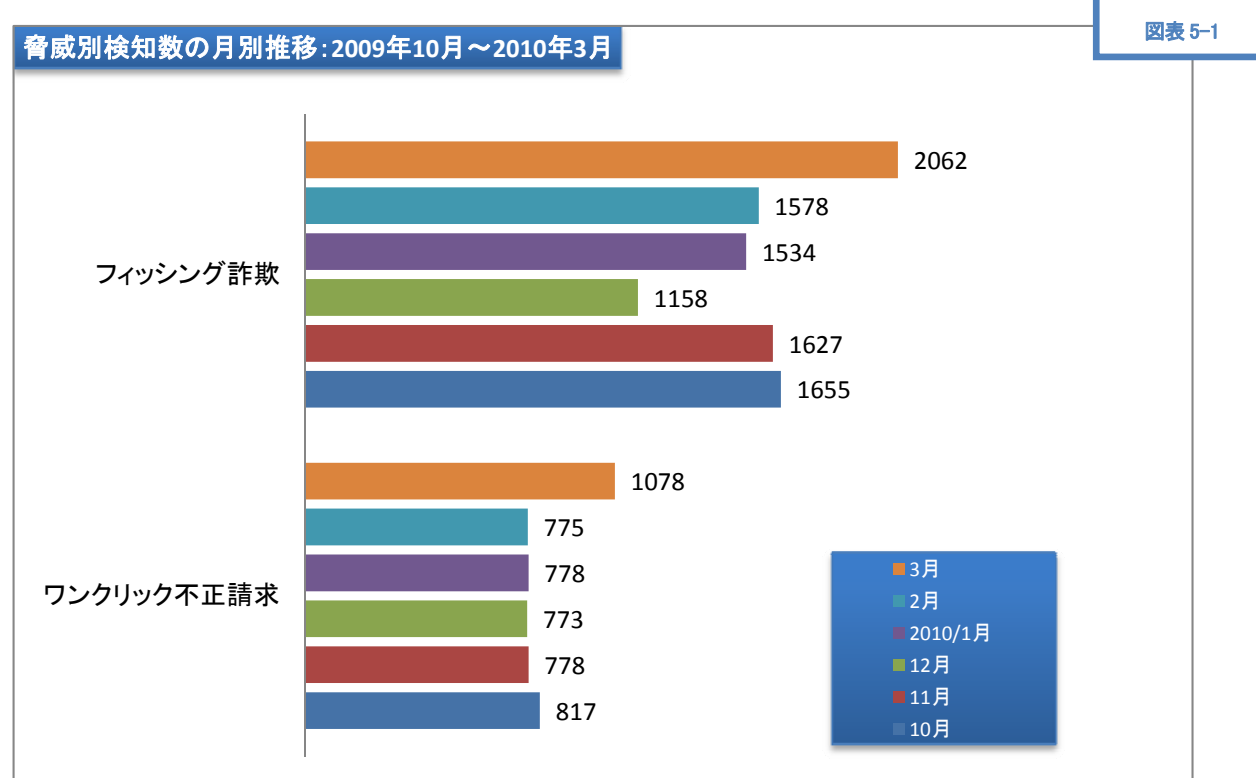
ゴールデンウィーク等の長期休暇期間は、過去にも大規模なセキュリティ被害が発生しています。企業では、システム管理者を中心として、以下の点に注意して、セキュリティ対策を再点検することをお勧めします。

| ゴールデンウィーク等、長期休暇に際して特に注意すべき7つの項目 | |
|---------------------------------|--|
| 1 | OSのサービスパック、修正プログラム、アンチウイルス製品のパターンファイル等の更新が必要なものを確認 |
| 2 | ウェブサイト等、外部に公開しているコンテンツの安全性のチェックと監視体制の確認 |
| 3 | 社内で管理している機密情報の確認、取り扱いルールの確認、不要な情報の削除等 |
| 4 | ノートPCやUSBメディアの外部持ち出しに関するルールの確認と徹底 |
| 5 | ゴールデンウィーク終了後に、外部持ち出しから戻ってくる機材を、社内に持ち込む際の安全性の確認 |
| 6 | セキュリティ被害発生時の対応マニュアルの準備と確認 |
| 7 | データのバックアップ等、被害発生時に備えた取り組み |

ショッピングサイト、オークションを運営するウェブサイトは長期休暇中でも多くのユーザが閲覧します。「Drive by Downloadタイプの攻撃」をはじめとした「不正な改ざん攻撃」に備え、監視・対応体制を整え、問題発生時に迅速な対応するための、準備を行ってください。

4 詐欺サイトの検知数が急増

4.1 詐欺サイト検知数の状況

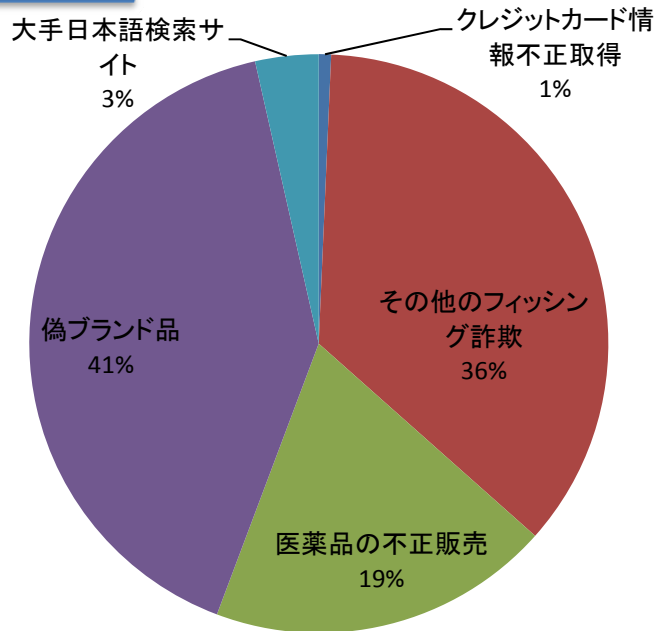


- 「フィッシング詐欺」の検知数が、急激に増加しています。2010年3月の検知数2,062件(前月比130.7%)は統計開始後の最高値です。
- 「ワンクリック不正請求」の検知数が急増しています。2010年3月の検知数1,078件(前月比139.1%)は、過去6月間の最高値です。しかし、2009年5月～9月における「ワンクリック不正請求」の検知数の平均は1,152.6件ですので、その水準に戻ったと言えます。

4.2 「個人情報を入力する手法」の傾向

図表 5-2

フィッシング詐欺サイト内訳(2010年3月)



個人情報を入力する手法の傾向としては、「実在する企業のウェブサイトを模倣」する「一般的なフィッシングサイト」ではなく、「ブランド品の販売」、「医薬品の販売」を装って「個人情報の収集」を行うウェブサイトが主流です。

これらのウェブサイトは「不正な販売行為」である可能性も高く、情報漏えい以外のトラブルに巻き込まれる可能性もあります。

4.3 「詐欺サイト」の傾向とその対策における留意点

| | 誘導手法 | コンテンツ | 対策における留意点 |
|------------|-----------------------------|---|--|
| フィッシング詐欺 | 電子メール | 実在する企業の偽サイト | <ul style="list-style-type: none"> 怪しいメールは開かない 文中の URL はむやみにクリックしない 閲覧しているウェブサイトの URL を確認 知らない人からの「友達リクエスト」や「メッセージ」に対して反応しない セキュリティ対策ソフトの導入 |
| | ↓ 手法の変化 ↓ | | |
| | SNS(mixi, Facebook 等) | ブランド品・医薬品の販売サイト | |
| | メッセージングサービス (Yahoo、Skype 等) | 架空の消費者金融による審査を装ったサイト | |
| ワンクリック不正請求 | 攻撃対象が若年層に拡大している | | <ul style="list-style-type: none"> インターネットの利用者年齢が下がってきています。自己防衛のみならず、詐欺サイトの情報、または「危険・悪質なウェブサイト」を閲覧することの危険性を家庭内でも共有する必要があります。 |
| | アダルトコンテンツ等を閲覧する中高年男性 | パソコンを使い始めた小・中・高生が興味本位でサイトを閲覧し、「不正請求被害」に遭う事例が報告されている | |

詐欺サイトの攻撃手法、攻撃対象に変化が見られます。それぞれの攻撃手法に応じた対策をとる必要があります。

5 個人・企業それぞれに求められる、セキュリティ対策とは？

5.1 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」

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。

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。

また、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、オンライン詐欺サイトや不正プログラム等を配布している危険サイトをブラックリストを使わずに検知する「Internet SagiWall」(<http://www.securebrain.co.jp/products/sagiwall/index.html>)も提供しています。危険なウェブサイトを閲覧してしまった場合、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>

■「gred AV アクセラレータ」URL

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

5.2 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」は、ブラックリストを使わずに、ウェブサイトの「今の状態」をリアルタイムに判断します。

「gred セキュリティサービス」の「無償トライアル版」は、自社ウェブサイトの 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」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