PRESS RELEASE

2009 年 12 月 25 日

報道関係各位

株式会社セキュアブレイン

年末年始における個人のインターネット利用、

企業のウェブサイトの改ざん被害に関する注意喚起

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 25 日、年末年始のインターネット利用、企業のウェブサイトの安全性監視について、注意喚起を行いました。

年末から年始にかけては、インターネットの利用が急増します。同時に、悪質なウェブサイトによる、オンライン詐欺や、ウェブサイトの改ざん、ウイルス等不正プログラムの大量配布が行われ、それによる被害も多発します。

インターネットを利用する個人ユーザは、使用しているセキュリティ対策ソフトが最新の状態に保たれているか、また設定は正しく行われているか等を確認すると同時に、下記に示す基本的なセキュリティ対策を行う必要があります。

また、ウェブサイトを運営する企業では、自社のネットワークや外部に公開しているウェブサイトの安全性を確認する必要があります。特に 2009 年 5 月以降は、企業のウェブサイトが「Gumblar ウイルス」により、改ざんされる事件が多発しています。「Gumblar ウイルス」はウェブサイトに脆弱性等の問題が無くても、改ざんを行うことが可能な為、企業はウェブサイトの監視を強化する必要があります。

改ざんに気付かず放置してしまうと、ウェブサイトを閲覧したユーザが「Gumblar ウイルス」に感染する等の被害を受け、さらに被害が拡大する恐れがあります。

個人のインターネット利用についての注意喚起

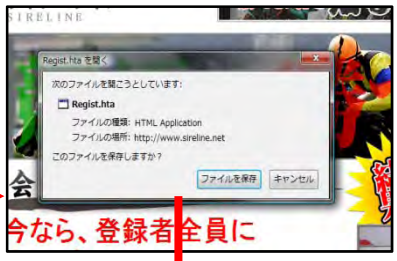
■ワンクリック/ツークリック詐欺のコンテンツが多様化。競馬等のギャンブル情報、マルチ商法を騙ったウェブサイトも登場

ワンクリック/ツークリック詐欺のコンテンツに変化が見られます。従来はアダルト情報が主流でしたが、競馬やパチンコなどの攻略情報サイトや、「金儲け」「マルチ商法」を騙ったウェブサイトが確認されています。

これらのウェブサイトでは、上記に関連する「お得」な情報を提供すると見せかけて誘導し、ある程度画面が進んだところで、「料金請求」の画面を出します。

競馬情報サイトの画面

「登録するボタン」を 2 回クリックすると、「regist.hta」というファイルをダウンロードさせようとします。



「regist.hta」を展開すると、下記の画面を表示させます。一度表示された後は、起動時には、毎回この画面が表示されます。

このように、オンライン詐欺の手口は多様化が進んでいます。年末年始はインターネットを利用する機会の増加に伴い、上記のような不正に料金を請求するウェブサイトや、個人情報を詐取や、ウイルス等の不正プログラムの配布を目的とした悪質なウェブサイトが増加することが予想されます。

インターネットを利用する際には以下の項目に特に注意して利用してください。

1. ウイルス感染やスパイウェアによる情報漏えい防止のためセキュリティ対策ソフトを必ず使用してください。
2. 暗証番号、パスワード、また個人情報を他人に教えたり、不特定多数の人が閲覧する掲示板等に公開することは避けてください。
3. インターネット上には、悪意のあるウェブサイトも存在します。情報の発信元、ウェブサイトの運営者、及び内容などを充分にチェックしてください。同時に、危険なウェブサイトを検知するセキュリティ対策ソフトウェアや、閲覧しようとしているウェブサイトを事前にチェックするサービス等を利用してください。

同時に、セキュアブレインでは、個人のお客様を、インターネット上の脅威から守る為に、以下のセキュリティ対策ソフトおよびサービスを提供していますので、ぜひご活用ください。

1. オンライン詐欺/危険なウェブサイトブロック「Internet SagiWall」
   （ https://www.securebrain.co.jp/products/sagiwall/trial.html）
2. 無料のウェブ診断サービス「gred でチェック！」（http://www.gred.jp/）
3. 無料でウイルス対策を強化する「gred AV アクセラレータ」（https://www.gred.jp/avx/download.html）

企業のウェブサイト改ざん被害についての注意喚起

■依然猛威を振るう「Gumblar ウイルス」、攻撃手法は複雑化

2009 年 5 月から 12 月にかけて、「Gumblar ウイルス」によるウェブサイトの改ざん事件が後を絶ちません。特に企業ウェブサイトの改ざん被害は深刻です。Gumblar ウイルスは感染したパソコンからウェブサーバの FTP の ID やパスワードを盗みとり、不正アクセスを行います。

不正アクセスの結果、ウェブサイトのコンテンツの改ざんや、不正なファイルの設置、また情報漏えいにまで発展するケースが報告されています。また、「Gumblar ウイルス」は、正規の FTP の ID やパスワードを使いアクセスを行う為、ウェブサーバに脆弱性等の問題が無くても改ざんが可能になる為、未然に防ぐことが非常に困難です。企業ではウェブサイトの監視を強化する必要があります。

「Gumblar ウイルス」は 2009 年 5 月に日本国内で初めて大量に被害が発生しましたが、その後のセキュアブレインの調査によれば、2009 年 10 月に Gumblar ウイルスの新たな攻撃手法を確認しています。新たな攻撃手法は、より手口が複雑化しているため、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。

セキュアブレインの調査では、Gumblar ウイルスにより改ざんされたウェブサイトの中で 41.7%は企業のサイトです。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。

過去に「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を行ってください。

「Gumblar ウイルス」被害の集計（2009 年 6 月～11 月）

Total	*企業・団体*	*個人*	*学校*	*その他*
1507	628	703	9	167

Gumblar ウイルスの攻撃手法については、セキュアブレイン gred セキュリティレポート Vol.5 をご覧ください。
http://www.securebrain.co.jp/about/news/2009/12/gred-report5.html

年末年始の休暇中は、企業ウェブサイトの監視も十分に行われない可能性があります。その為、改ざんによる被害

が発生しても対応が遅れ、被害が拡大する恐れがあります。企業はウェブサイトの監視体制を十分に行うと共に、感染が発生した場合に、いち早くそれを検知し、報告を行う体制を整える必要があります。

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。

◆ 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)

電子メール: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