サイバー攻撃を仕掛ける「ブラック」サンタに注意を～G Data

G Data Software株式会社（本社：東京都千代田区、代表取締役社長：Jag
山本）は、毎年オンラインショッピングの繁忙期となる12月に、一般ユーザーが「ブラック」サンタによるサイバー攻撃にさらされる可能性が高いとみて、ここに手口の代表例と対策を紹介するとともに、警戒を呼び掛けます。

オンラインで買物や取引を行うインターネットユーザーの数は、ここ数年、増加傾向にあります。オンラインショッピングの年間売上は、経済産業省「平成21年消費者向け電子商取引実態調査」によれば、回答を得た2万7,558事業者の総計だけで、3兆円を超えています。もちろんそのなかで、クリスマスプレゼントや年末年始の買い物などが集中する12月の売上は、大きな比率を占めていると予測されます。場合によっては普段は利用していないユーザーも、この時期にはオンラインショッピングから購入する機会が増えるため、他の月以上に注意が必要です。そこでG Dataでは、サイバー犯罪者がよく用いる手口上位5パターンを紹介し、せっかくのクリスマスシーズンに嫌な思いをせず、また、損害なきよう、簡単なアドバイスを提供します。

クリスマスのオンラインショッピングに気をつけたい、5つのパターン
～「ブラック」サンタに騙されないために～

その1 ブランド品の大特価割引セール（メール）
大量に届くスパムメール。いつもならば開封もせずにゴミ箱に直行のはずが、有名ブランド品の特価提供といった内容が書かれているメールは、たとえそれが英文であっても、この季節になるとちょっと気になってしまうものです。高級腕時計、アクセサリー、バッグ、靴などが驚くほどの低価格で販売されているため、一度くらい試してみてみよう、という気持ちになるのも分からなくはありません。しかし、そもそも「偽ブランド品」は売るのはもちろん購入するのも違法行為ですので、お勧めできません。さらに、この種の内容のメール本文にあるリンクをクリックすると、多くの場合は、マルウェアを侵入させてしまうか、偽購入サイトに誘導されて個人情報とクレジットカードの番号などが奪われるばかりです。いつも利用しているショップやサイト以外からやってきたメールで、「Christmas Sale」というような件名、誰もが知っている有名ブランド、驚くほどの低価格、これらを含んだメールは、信用すべきではありません。

その2 送金未完了のお知らせ（メール）
クリスマスプレゼントをネットで購入する際に、オンラインバンキングからの振り込みをする場合が少なくありません。国内では大手銀行の名を騙ったフィッシング詐欺も多数発生しており、この手法は今、かなりポピュラーになっています。一般的な手口は、まず、送金未完了などの内容の偽メールが届くところからはじまります。質素な文面もあれば、HTML形式でロゴやデザインなどを本物のデータを借用したものもあります。一見するともっともらしい文面ですが、これは単に確率の問題で、メールを受け取った人の一定数はその銀行と口座を持っているであろうと予測したうえで送っているだけで、調査した結果をふまえて送っているのではありません。ここでメール本文にあるクリック先に飛ぶと、バンキング・トロージャンに感染し、口座情報を盗まれてしまいます。たまたま偶然にその銀行に口座があり、最近送金した記憶がある場合でも、要注意です。もし確認をしたいのであれば、メールにあるリンクをクリックするのではなく、いつも通りの手順でオンラインバンキングのサイトを開いてください。

その3 配送サービスからの通知（メール）
クリスマスプレゼントの場合、海外の通販サイトで購入する機会も増えます。しかも大変混み合

う時期なので、注文した品の配送ステータスを確認するメールが届いても、あまり違和感はありません。そこでサイバー犯罪者たちはメールを出荷確認や請求と思わせて無作為に送りつけます。多くの場合、明細が添付ファイルになっていて、その中身を確認するよう要求されます。しかしこの添付ファイルが危険で、開封するとともにキーロガーなどのマルウェアが侵入します。当然キーロガーでサイバー犯罪者が盗み出そうとしているのは、クレジットカードや銀行口座の情報であり個人情報です。また、メール文中にリンクと称して、偽リンクを用意しアカウントとパスワードを盗みだす手口も増加しています。

その4 オンライン決済の確認（メール）
「あなたのアカウントが何らかのトラブルで使用できなくなっていますので、ご確認のうえ、再設定してください」――こういった内容のメールがオンライン決済サービス業者から届いた場合も、要注意です。このメールにもリンクが貼ってあり、クリックすると、口座情報や個人情報を入力するよう求められるサイトに飛びます。このサイトを開いただけでマルウェアに感染する場合もあれば、情報を入力させて盗む出す方に力点がある場合もあります。

その5 クリスマスカード（メール）
キリスト教文化圏では年賀状よりもクリスマスカードがポピュラーな挨拶状です。最近では郵送や印刷物ではなくオンラインによるEカードが増えています。しかし「ブラック」サンタが送りつけるのは偽物のカードです。このありがたくない贈り物は、添付ファイルになっている場合もあれば、メール本文にリンクが貼ってある場合もあります。いずれもマルウェアに感染させて金銭につながる情報を盗み出すのが目的です。日本の場合は、メールで届く年賀状にも、引き続き注意すべきです。

さて、以上の5点にわたる危険性の高い「ブラック」サンタからマルウェアという嫌な贈り物を受け取らないために、以下の8項目のTIPSを是非とも実行しましょう。

オンラインでクリスマスプレゼントを安心して購入するための8つのTIPS

1 統合セキュリティソフトを正しく使う
ウイルス対策だけではなく、スパムやフィッシングなどの対策機能をもったインターネットセキュリティソフトウェアを導入し、アップデートや更新などを正しく行いましょう。また、契約期日がすぎたら、すみやかに更新しましょう。

2 OS／ソフトのアップデートを実行
脆弱性を放置すると致命的なダメージを被ります。OSや基本ソフトウェアのアップデートは必ず実行しましょう。

3 スパムメールは、読まずに削除
おかしなメール、怪しいメールは、中身を読んだり、添付ファイルを開いたりせずに、即刻ゴミ箱に移動しましょう。もちろん文面に貼ってあるリンクもクリックしないようにしましょう。

4 信用のないオンラインショップは利用しない
はじめて利用するショップやモールは、できるだけサイトにある関連情報を読んでから購入手続きなどを行いましょう。配送料や支払い方法、返品方法などの記載内容や個人情報保護方針などをしっかり読むのが理想です。

5 自分のパソコン以外は使わない

ネットカフェでは、クッキーなどのユーザーに関連するログ情報がインターネット閲覧後もコンピュータに残り、後でコンピュータを利用する別のユーザーがそのデータを閲覧され、不正利用される可能性があります。また、公衆WLANも安全性が高いとは言えないので避けるべきでしょう。

6 ブラウザの「安全」表示を確認
ユーザーログインが必要なサイトでは、URLをマニュアルで入力、もしくはサイトをブラウザのお気に入り機能に登録して、お気に入りから選択するようにしてください。

7 パスワードの見直し
パスワードを定期的に変更しましょう。また、すぐに分かる文字列は避け、なるべく長めに、数字と文字などを組み合わせて作成しましょう。大文字や特殊文字を混ぜるだけで大幅に安全性が高まります。

8 ショップの信頼性の確認
利用規約や個人情報保護方針があるか、サイト運営責任者が怪しくないか、送料や追加費用が発生するかどうかなど、はじめて利用するサイトの場合は特に確認を必要とします。

ジーデータソフトウェアとは
G Data Softwareは、1985年に創業し、1987年に世界最初の個人向けウイルス対策ソフトを発売した、ドイツのセキュリティソフトウェア会社です。
EUを中心に、個人向け・法人向け製品を展開しています。日本法人は2007年に設立しました。最大の特徴は、ダブルエンジンによる世界最高位のウイルス検出率です。また、新種や未知ウイルスへの防御、フィッシング対策、迷惑メールへの外国語フィルターなど、インターネットやメール環境を安全・快適にする機能を豊富に搭載しています。その結果G Dataのセキュリティ製品群は、マルウェアやフィッシング詐欺サイトを常に高検出することに定評があり、過去5年間以上にわたって、第三者機関・雑誌における受賞獲得数は他社の追随を許しません。2011年にはアンドロイド端末向けのセキュリティアプリも発売しました。

＊本リリースに記載されている各種名称、会社名、商品名などは各社の商標または登録商標です。

【本リリースに関する問合せ先】
G Data Software株式会社
101-0042 東京都千代田区神田東松下町48 ヤマダビル6F
窓口： 瀧本往人
E-mail: gdata_japan_info@gdatasoftware.com
URL： http://www.gdata.co.jp/
