アンラボ・セキュリティレター

Press Ahn

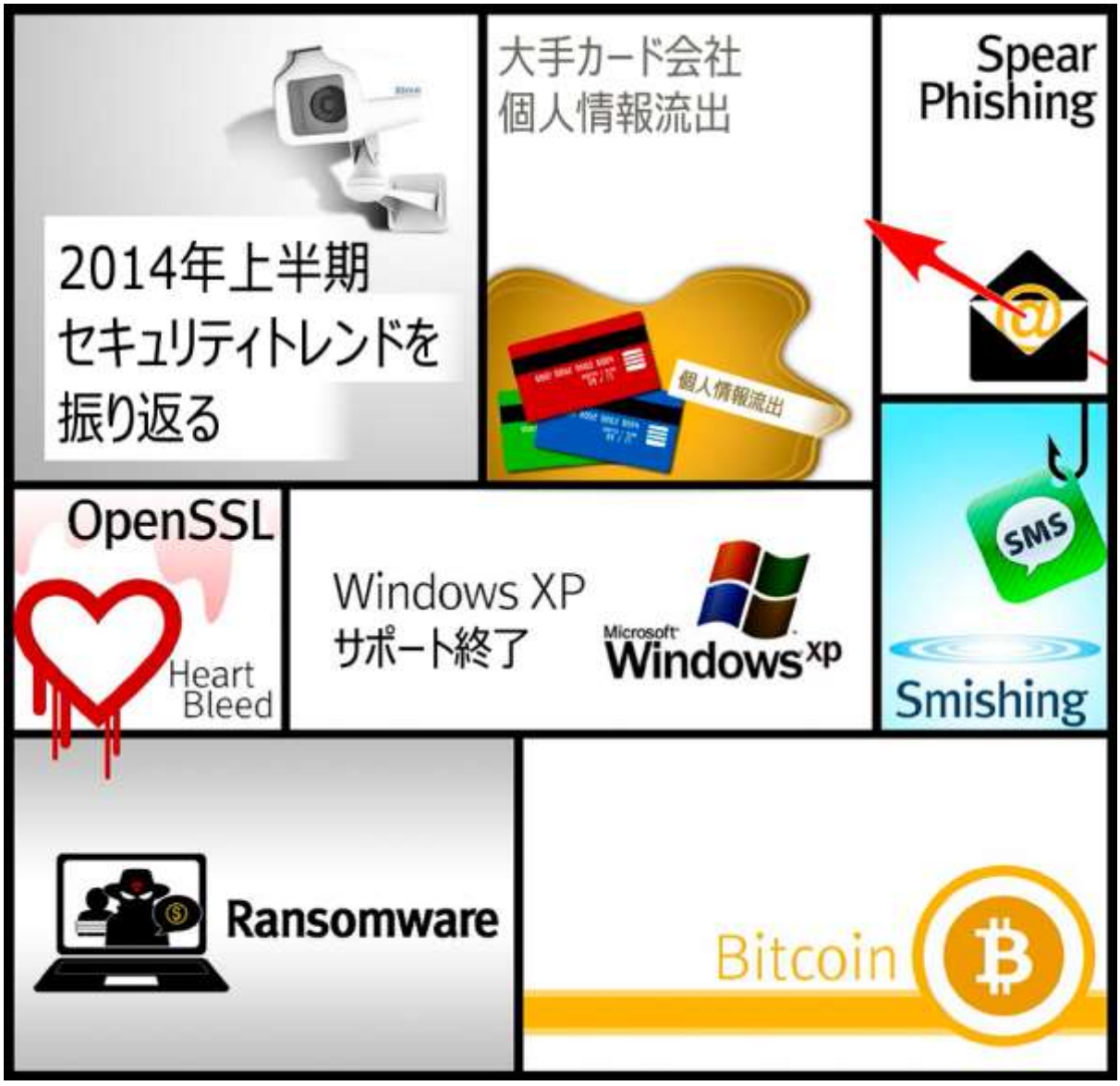
2014.7　Vol.07

2014 年上半期セキュリティトレンドを振り返る

2014 年上半期セキュリティトレンドを振り返る

2014年もすでに折り返し地点を過ぎ残り数ヶ月となりました。韓国は今年、大手カード会社で起こった大量の顧客情報流出という大事件からスタートし、Windows XPサポート終了、Open SSL脆弱性発見など、様々な問題がセキュリティ業界を緊張させました。さらにスピアフィッシング、スミッシング、ランサムウェアなどの脅威が具体化されることでこれらの用語も浸透しつつあります。特にこれらはスマートフォンのユーザーをターゲットにしている点で注目すべき脅威といえるでしょう。

ここでは2014年上半期の代表的なセキュリティ案件をキーワードにまとめてみました。



カード会社の情報流出

1月、韓国では大手カード会社のK社から5,300万件、L社で2,600万件、N社2,500万件など計1億400万件もの個人情報が流出される前代未聞の事故が発生しました。これはプロジェクト開発のために派遣された信用評価会社の従業員が、これら3つのカード会社の顧客情報をUSBにコピーしてこっそり流出したことから起こりました。警察の調査結果、この派遣社員は持ち出した顧客の氏名、携帯番号、住所などの個人情報を融資広告業者とローン募集人に渡したことが明らかになりました。この事件の被害補償と責任者の懲戒処分などは、いまだ進行中です。この事件でカード会社3社を対象に出された訴訟額は、5月末を基準に1,068億~1,960億ウォンにのぼり、金融監督院はこれらのカード会社の最高経営責任者に解任勧告レベルの懲戒処分を通知しました。本件はカード会社のデータ暗号化、USB制御、外注スタッフ管理に関する強力な法令が設けられているにもかかわらず発生したことから、法のガイドラインと遵守との乖離を如実に現わしました。

スピアフィッシング

近年最大の脅威としてはAPT（Advanced Persistent Threat）があります。このAPT攻撃の主要手口こそスピアフィッシング（Spear phishing）なのです。スピアフィッシングとは、「spear：槍、刺す/phishing：受信者を騙す詐欺メールおよびその他の活動」の合成語で、訳すと「標的型悪意あるメール」になります。海外の統計によるとこれまでに明らかになったAPT性の標的型攻撃の90%以上がスピアフィッシングから誘発されたか、攻撃に使用されたとのことです。

スピアフィッシングと一般的なスパムメールの異なる点は、▲不特定多数を狙うのではなく、ハッカーがターゲットにした特定の機関や企業を狙う「標的性」、▲一般的な広告やアドウェアよりもはるかに深刻な情報流出を狙うマルウェアの「深刻性」、▲通常ファイルとして表示されたり、内容を疑う必要がないほど通常メールと同じ「精巧性」があります。

マルウェアを添付してユーザーを騙す内容のメールを送りつけることは非常に古典的な方法にもかかわらず、未だこの手法が十分通じています。「セキュリティにおける最大の脆弱性は、人に他ならない」という専門家らの指摘はまさにその通りなのです。

スミッシング

スマートフォンの時代が到来したことで最も厄介な脅威として浮上したのがスミッシング（Smishing）です。スミッシングは「SMSとフィッシング（Phishing）」の合成語であり、攻撃者がスマートフォンユーザーに有害なURLを含む文字メールを送信し、実行および有害アプリのインストールを誘導することによって、ユーザーの金融情報および個人情報を奪取する悪質な手法です。

初期のスミッシングは、流出された個人情報とスミッシングによって奪取した通信事業者情報、認証用の文字メールを結合させ、課金決済を誘導するタイプでした。しかし最近は専門家もすぐには区別できないほど高度化されたスミッシング手法を使用し、証明書、IDとパスワード、通信事業者情報、文字メールなどの金融取引および決済に必要なすべての情報を一度に奪取します。特にアドレス帳の情報までも奪取することで、スミッシングの受信が爆発的に増えています。

最近発見されたスミッシング文字に含まれているURLの有害サイトを分析した結果、▲キャプチャコード（CAPTCHA CODE）を使用し、▲フィッシングサイト内に一部正常サイトURLを挿入、▲偽サイトのデザインとフレーズの高度化などの特徴が際立ち、一層進化した様相を見せました。

アンラボの分析結果によると、今年1月から5月まで収集されたスミッシング・マルウェアは昨年同期比1,033個から約3.4倍増加した計3,558個でした。これは2012年同期比711.6倍増加した数値になります。

スミッシングはこのように各種の社会的な問題と高度化された手法を結合させ、常に別の形態に変貌しているためユーザの注意が求められています。

スミッシングを予防するためには、ソース不明の文字が含まれているURLをクリックせず、不審な文字はすぐに削除することが重要です。

Windows XP サポート中止

2014年は公式的にWindows XPのサポートが終了することから、セキュリティのブラックホール化することが懸念されていました。

Windows XPサポートの中止により、XPのためのPCセキュリティ、バグ修正、オンライン技術サポートなどは今後提供されず、XPユーザーはサポート終了日以降OSの致命的な脆弱性に対するセキュリティパッチを受けることができません。ユーザーがXPを使用し続ける場合、簡単に各種ウィルス、マルウェアやスパイウェア、ハッキングなどのセキュリティ上の脅威に晒されることになります。これにより個人情報の盗難など個人レベルの被害の危険性が高まり、ハードウェアの問題に起因するシステム障害や業務の中断など非常にリスクが高くなります。

幸いにも当初の懸念とは異なり、まだWindows XPサポート中止により大きな問題は発生していませんが、今後もXPを使用することは非常にリスクが大きいため、OSの変更やアップグレードなど根本的な解決策が必要です。

ハートブリードとオープンSSL

4月には全世界で最も多く使用される暗号化プロトコル・オープンSSLのハートブリード（HeartBleed）バグが発見されました。一部のセキュリティ専門家やマスコミは「インターネット史上最悪の脆弱性」と表現するなど、世界的に大きな波紋を起こしました。

オープンSSLは、インターネットでデータを送受信する際に元の内容を暗号化する方法（プロトコル）です。今回問題となったハートブリードはオープンSSLであり、クライアント（PC）とWebサーバ間の暗号化通信が正常に行われているかどうかを確認するために使用されるプロトコル「ハートビート（HeartBeat）」で発見された脆弱性でした。

これは、ハートビートというプロトコルでクライアントの要求メッセージを処理する際、データの長さの検証を実行せずにシステムメモリに保存された64KBサイズのデータを、外部から何ら制限なく奪取できるというものです。ハートブリードという用語は、通信プロトコルのハートビートから発見された欠陥として命名されました。「心臓の出血」を意味するハートブリード（HeartBleed）は、ハッキングにより心臓の出血のようにデータが少しずつ外部に持ち出されることで、致命的な個人情報流出に繋がる可能性があるということを意味します。

以来6月には中間者攻撃（Man In The Middle、MITM）に悪用される可能性がある脆弱性（CVE-2014-0224）が登場するなど計6つのオープンSSL脆弱性が追加で発見されました。 2014年の上半期に相次いで発見されたオープンSSLの脆弱性により、インターネット企業、ネットワーク・アプライアンスメーカー、セキュリティベンダーは製品のパッチ作業のために奔走しました。

ランサムウェア

ランサムウェアは既におなじみの用語ですが、スマートフォンへの拡大、ビットコイン決済など様々な問題が浮き彫りになっている点で注目されています。ランサムウェアとはransom（身代金）とware（製品）の合成語で、ユーザーの重要な資産を人質にして金銭的な要求をする悪質なプログラムのことを指します。最近ではAndroidを狙ったランサムウェアが登場し、スマートフォン端末そのものを人質にとるのが特徴的です。つまりAndroidランサムウェアは既存のマルウェアとは異なり、感染する場合は機器そのものが制御不能状態に陥るため携帯電話の重要情報を正常に使用できなくなるのです。

他にもクリプトロッカー（CryptoLocker）のようなランサムウェアは、ユーザーのコンピュータファイルを暗号化し、ビットコインや現金決済などでお金を払わなければ解除しないと脅迫することもあります。ランサムウェアは重要な文書を暗号化した後で解除の対価を要求しますが、一度暗号化されてしまうと要求に応じない限り復元することは非常に難しいといえます。

また身代金を支払うとしてすべてのファイルを復元するという保証もありません。よってランサムウェアを予防するためには、ソース不明の電子メールに添付されたファイルやURLはクリックしないようにし、PCとスマートフォンに保存された重要な文書やファイルは、普段からバックアップしておく習慣が必要です。ランサムウェアに感染しても、復元ポイントを設定しておくかファイルをバックアップしておけば、その時点に戻って復元することができます。

ビットコイン

ビットコイン（Bitcoin）は、昨年から世界のメディアに度々登場している魅力的な用語の一つです。これは仮想通貨の一種であり、利用者間のP2P（ファイル共有システム）をベースに通貨の発行および取引が行われる特徴を持っています。ビットコインは他の仮想通貨とは異なり、一般通貨のようにオフラインでも商品やサービスを購入することができます。また民間市場でドルやユーロなど、既存の通貨に簡単に変えることもできます。

セキュリティの観点からビットコインを注目するのは、昨年下半期からビットコインの価値が上昇し、これを奪取するためのマルウェアも増加しているということです。最も一般的な形態のビットコイン・マルウェアは、ビットコインの確認と転送に使用される暗号化キーを保存・作成するソフトウェア「財布（Wallets）」を攻撃するとして知られています。海外のメディアによると2月のゾンビウイルス・ポニー（Pony）によって85個の電子財布が被害を被り、盗まれた金額は20万ドル（約2億1,400万ウォン）にのぼると報告されました。

これまでビットコインは議論の対象でしたが、6月Appleがビットコインで取引するアプリを承認したことからさらに関心が高まると予想されます。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)

© 2014 AhnLab, Inc. All rights reserved.