

2012 年 1 月 6 日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

【報道資料】

チェック・ポイント 2012 年セキュリティ動向予測

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社(本社:東京都新宿区、代表取締役社長 藤岡健)は本日、チェック・ポイント独自の調査とお客様から寄せられたご意見に基づく、2012 年の注目すべきセキュリティ動向予測を発表しました。サイバー犯罪が次々とメディアの見出しを飾り、インターネットを利用した攻撃が複雑化の一途を辿る今日。規模の大小を問わず、すべての企業は、最新の技術動向やコンプライアンス要件に合わせたリスク管理戦略の見直しが求められています。

- **モバイル・デバイスを狙った攻撃の増加とその対策の強化**

モバイル・コンピューティングがビジネス・コミュニケーションの手段として急激に一般化したことに伴い、モバイル・デバイスの業務利用を認める IT 管理者も着実に増加しています。その一方で IT 管理者は、企業ネットワークに接続される大量のデバイスと多種多様なオペレーティング・システムをどう保護すべきか、モバイルおよびネットワーク・アクセス・ポリシーをどのような内容にすべきかといった課題に早急に取り組む必要に迫られています。チェック・ポイントが実施した調査では、回答者の 78%が 2 年前と比べて企業ネットワークに接続する個人所有のデバイスが 2 倍以上に増加したと答え、63%がセキュリティ・インシデントの増加はこの傾向と無縁ではないと答えています。

また、情報の搾取や機密情報への不正アクセスといった攻撃の対象として狙われるモバイル・デバイスが増加しています。適切なセキュリティ対策が講じられていない場合、トロイの木馬がインストールされ、例えば一定時間ごとに写真を撮られる、画面に表示された個人情報(SMS メッセージや電子メール、Web サイトの閲覧履歴、所在地情報など)がキャプチャされるなどの被害に遭うおそれがあります。モバイル・デバイスを狙うマルウェアの種類も倍増すると見込まれており、2012 年にはモバイルの脅威に対する一層の警戒とセキュリティ意識の向上が求められます。

- **QR コードの悪用**



昨今では、QR(Quick Response)コードを使用する小売業者や広告主が増えています。携帯電話で読み取るだけで商品などについての詳細情報が得られる二次元コードで、今後さらに普及すると見込まれます。それに伴い悪用事例の出現も予想されます。例えば QR コードを読み取らせ、不正な URL やファイル、アプリケーションへユーザを誘導するなどの手法が考えられます。

- **個人情報を利用したソーシャル・エンジニアリング攻撃が増加**

今日、オペレーティング・システム(OS)のセキュリティは成熟度を増しており、正しいセキュリティ戦略と対策により多くの脅威を阻むことが可能となっています。2012年には、それとは別の手段である「人」をターゲットに、つまり「ソーシャル・エンジニアリング」攻撃を使って不正な目的を達成しようとする攻撃者がさらに増加すると予想されます。

ソーシャル・エンジニアリング攻撃では通常、深い専門知識を持っている、あるいは機密情報にアクセスできる人物がターゲットにされます。さまざまなコミュニケーション・ツールが人気を得ている今日、ハッカーはこれらのツール上で一般公開されている情報から、ターゲットの詳細な人物像をいとも簡単に把握できます。例えば Facebook には氏名や誕生日、交友関係のある友人、Twitter には関心事やフォロワー、職務経歴や学歴が LinkedIn に、さらに FourSquare や Yelp ではチェックイン情報や所在地情報が公開されており、わずかな例を挙げるだけでもこれだけの情報を得ることが可能です。ソーシャル・エンジニアリング攻撃では、収集した情報を基にメールの文面がパーソナライズされるため、正規のメールであると思いついてしまうケースも珍しくありません。

チェック・ポイントの[調査](#)によると、ソーシャル・エンジニアリング攻撃の動機は「金銭的な利益」が51%で最も多く、次いで「知的財産へのアクセス」(46%)、「競合企業に対する優位性の確保」(40%)、「報復」(14%)となっています。また被害額はインシデント1件あたり2万5,000ドル~10万ドルに上ります。ソーシャル・エンジニアリング攻撃による被害を食い止めるには、テクノロジーの利用に加え、組織全体でユーザのセキュリティ意識を高める取り組みが欠かせません。

- **マルウェアの産業化**

ところでハッカーは「職業」として成り立っているのでしょうか。現代のサイバー犯罪はアマチュアによる単独行動ではなく、資金と動機、そして目標を持つテロリスト集団のように組織化されたグループによって行われています。相当なコストがかかるボットネットの構築と運営にサイバー犯罪者が多大な時間と知恵、労力を注ぎ込めるのは、単独犯ではなく組織犯罪だからです。多くの場合彼らは、時間をかける価値がないと判断したターゲットには攻撃を仕掛けません。金銭的利益が得られない攻撃は無駄な手間だからです。

一方、金銭に関する情報だけがサイバー犯罪者にとって価値があるとは限りません。彼らは特定の請求に関する情報やクレジット・カード情報よりも、一般的な顧客情報を重視する傾向にあります。後者のような情報を利用してソーシャル・エンジニアリング攻撃やスパム・メールをパーソナライズすると、より大きな成果を得られる可能性があるからです。また、クレジット・カード情報よりも社会的なアイデンティティ情報の方が重宝される場合もあります。8億人のユーザを擁し、そのほとんどが日常的にサービスを利用している Facebook などのソーシャル・ネットワーキング・サービス(SNS)サイトは、サイバー犯罪者にとって新たな攻撃材料と化していると言えます。

- **ボットネットが組織へのバックドアとして利用**

2012年には、組織にとってボットネットが最大のネットワーク・セキュリティ脅威の1つになると予想されます。数千台から、100万台以上のコンピュータで構成されるボットネットは、サイバー犯罪者がコンピュータを乗っ取り、さまざまな違法行為や不正行為を行うために使用されます。データの窃取やネットワーク・リソースへの不正アクセス、サービス妨害(DoS)攻撃の実行、スパム・メールの送信などがその一例です。

これまで、有名なボットネットの大半はWindowsマシンで構成されていると考えられていました。しかし現在では、LinuxやMacベースのシステムならボットと無縁と決め込むことはできなくなっています。2012年のボットネットは、ソーシャル・エンジニアリングとゼロデイ攻撃を組み合わせることでさらに進化し、普及が進むモバイル・デバイスやSNSサイトを利用するようになると予想されます。また複数のプラットフォームに加えて、iOS、Androidおよび、その他のモバイル・デバイスに対応するボットネットも登場すると見込まれ、3G回線やWi-Fiネットワーク経由で指令(C&C)サーバと通信するでしょう。

- **IPv6に移行する企業が急増**

2011年1月31日、ICANN Assigned Numbers Authority (IANA)によりIPv4アドレスの最終ブロックの割り当てが行われました。日本国内でもIPv4アドレスの枯渇問題は大きく報道されています。未割り当てのIPv4アドレスが残りわずかとなり、IPv4アドレス不足への対処が差し迫ってきたため、IPv6の導入が広範囲で始まりつつあります。IPv6には、プロトコルの一部がIPv4と違う点や、導入のために移行メカニズムが使用される点など、アーキテクチャに起因する固有のセキュリティ問題が存在します。それ以外にも、一部組織ではネットワーク管理者の知らないところでIPv6が導入され、ハッカーやボットネットの隠れ蓑として利用されている可能性も否定できません。2012年、IPv6への移行を計画している場合は、セキュリティが損なわれぬよう慎重に準備を進める必要があります。

- **セキュリティ対策としての仮想化技術の利用の増加**

当初、仮想化技術はサーバなどのITリソースを統合して、導入コストや設置スペース、電気料金を削減するために使用されるのが一般的でした。しかし最近では、この他にもさまざまな用途を担うようになっています。業界では、仮想化技術を追加のセキュリティ・レイヤとして活用する例が普及し始めています。例えば[Check Point Go](#)や[WebCheck](#)では、チェック・ポイント独自のブラウザ仮想化技術で企業データをインターネットから隔離して、ネットワークやエンドポイントを保護できます。ユーザは、ドライブバイ・ダウンロード(自動ダウンロード)やフィッシング、マルウェアなどを防御しながら安心してWebサイトを閲覧できるようになります。

- **ソーシャルボットが台頭**

ソーシャルボットは、特定の SNS サイトのアカウントを管理し、メッセージの投稿や友人申請の送信など基本的な操作を実行するソフトウェア・プログラムです。ソーシャルボットが増殖している理由は、その最大の特徴でもある「人間を模倣する能力」にあります。もしソーシャルボットからの友人申請を受け入れたなら、そのユーザは自身の交友関係や個人情報へのアクセスをソーシャルボットに認めたのも同然となり、なりすましなどの被害が発生するおそれがあります。インターネットに詳しいユーザが複数の SNS サイトのアカウントを同期している場合、ソーシャルボットは一度の攻撃で複数のアカウントに影響を及ぼすことができます。

- **大型イベントに便乗した不正な SEO がさらに増加**

2012 年も引き続き一般消費者や企業には、さまざまなブラックハット SEO(検索エンジン最適化)の影響が及ぶと予想されます。ブラックハット SEO とは検索エンジンでの検索結果を操作するハッキング行為で、自身の不正サイトを正規サイトよりも上位に表示させ、ユーザを不正サイトへ誘導します。米国の感謝祭明けに一斉に始まるオンラインセールや納税時期といった年に一度のイベントに関するキーワードをターゲットにして、不正サイトや詐欺サイトのリンクをクリックさせる仕掛けが定番の手口です。2012 年にニュースの見出しや広告を飾ると見込まれる大型イベントには、ロンドン五輪や米国の大統領選挙、第 46 回スーパーボウルなどがあります。例年同様、数多く検索されたり SNS サイトで広まったりする話題のキーワードには特に注意が必要です。企業の場合は、必要な注意喚起を行うと共に、URL フィルタリング・ソリューションやアプリケーション制御などのセキュリティ・ソリューションを導入してリスクを軽減する方策が有効となります。

従来型のインターネット脅威が依然として猛威を振るう中、Web 2.0 やモバイル・デバイス、クラウド・コンピューティングに関連する新しいセキュリティ問題が浮上してくるなど、CSO (Chief Security Officer = 最高セキュリティ責任者) が対処すべき課題は増加する一方です。これら複雑化する IT 環境へ適切に対処するには、セキュリティに対する考え方を見直し、ビジネス・ニーズに即した IT セキュリティを実現することが重要となります。

参考資料:

・- チェック・ポイント セキュリティ調査レポート -

欧米大企業の約半数がソーシャル・エンジニアリング攻撃の被害に

http://www.checkpoint.co.jp/pr/2011/20110928_social_engineering_survey.html

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド(www.checkpoint.com)は、インターネット・セキュリティにおけるトップ企業として、セキュリティの複雑さと総所有コスト(TCO)を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1 と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。チェック・ポイ

ントは、革新的セキュリティ技術である Software Blade アーキテクチャをベースとした一層の技術革新に努めています。Software Blade アーキテクチャは、導入先に合わせカスタマイズすることで、あらゆる組織のセキュリティ・ニーズにも的確に対応できる、柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、技術偏重から脱却してセキュリティをビジネス・プロセスの一環として定義する唯一のベンダーです。チェック・ポイント独自のビジョン 3D Security は、ポリシー、ユーザ、実施という3つの要素を統合して情報資産の保護を強化し、導入環境のニーズに合わせて高度なセキュリティを確保できるようにします。チェック・ポイントは、Fortune 100 社および Global 100 企業の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントの ZoneAlarm ソリューションは、世界中で何百万にも及ぶお客様の PC をハッカー、スパイウェア、および情報窃盗から未然に保護しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社は、1997年10月1日設立、東京都新宿区に拠点を置いています。

©2012 Check Point Software Technologies Ltd. All rights reserved

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
担当 マーケティング 溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行 株式会社プラップジャパン
担当 矢畑

Tel: 03-4570-3191/ Fax: 03-4570-3189

###