

セキュリティ最前線 (2008年4月18日号)

目次:

- | | |
|-----------------------------------|-----|
| 1. スマートフォンへの新たな脅威 | P.1 |
| 2. 賢いユーザになるために—スマートフォンセキュリティ最初の一步 | P.3 |
| 3. モバイル機器が危ない | P.5 |

1. スマートフォンへの新たな脅威

スマートフォンの成長

携帯電話や小型コンピュータ (PDA)は、ますます洗練され機能も豊かで楽しく使えるようになってきています。スマートフォンの新種が人気上昇中の理由もここに 있습니다。スマートフォンの Motorola Q、Nokia E-シリーズ、Apple iPhone、HTC Touch 等は、携帯電話の完全な機能に加えて、コンピュータに類似した機能および情報処理能力を備えています。通話機能に加えて、ユーザは会社や家のネットワークおよびインターネット上のデータにアクセスしたり、データ保存、データ利用が可能です。スマートフォンはまた、音楽の再生、写真およびビデオの撮影、閲覧ができ、さらにいつでもどこでもインターネットを閲覧することができます。

スマートフォンは、ラップトップ PC やデスクトップコンピュータと同様に OS が必要です。最も一般的に使用されている OS は、Symbian (Nokia および Sony Ericsson)、Microsoft の Windows Mobile、Research In Motion Ltd. の Blackberry、Linux、Apple の iPhone、そして Palm OS です。今日の新しい携帯電話のほとんどは、10 年前のコンピュータと同じような機能を備えています。

生産性の向上でリスクも高まる

今日の携帯電話の機能により、企業で働く人々はより効率的に必要な情報を入手できるようになりました。しかし携帯電話が盗まれたり無くしたりした場合、組織の機密情報や個人情報漏えいという新たな危険もはらんでいます。さらに不正プログラムへの感染、スパムやハッキングなどの危険もあります。

トレンドマイクロの研究プロジェクトマネージャのジャムズ・ヤネザは次のように言います。「ポケ

ットの中の携帯電話は、小さくても一人前のコンピュータの機能を持っているということを認識している人はあまりいません。携帯電話がコンピュータと同じ機能を備えているなら、もちろん同じ危険も潜んでいます。」

企業の IT 部署は、組織における携帯電話の脅威に取り組み始めています。「Wall St. Journal」によると、従業員にパスワードの使用を義務付ける会社規定の履行がうまくいかず、多くの IT 部署では iPhone の利用を禁止しようとしています。またスマートフォンが紛失した場合、会社としては組織の機密データが流出してしまうのではないかと心配もあります。[*1]

携帯電話が紛失した場合、個人情報および企業情報が共に危険にさらされることになります。企業にとっては、対外的な評判が落ちるという懸念もあります。情報漏えいの問題に加えて、コンピュータと同様のデータ処理を行う携帯電話はまた、不正プログラムの作者やハッカーの標的にされると予測している専門家もいます。企業にとっては、業務停止時間、データ喪失、ウイルスへの感染、従業員の生産性低下、事件の後始末などが新たなコストとなる恐れがあります。消費者にとっても携帯電話が機能しなくなると、データの喪失、新たな費用および不便さという問題があります。

攻撃はどのように行われるか

携帯電話は比較的攻撃されやすく、多くの媒介を通じてアクセスされます。今日のスマートフォンの典型的な接続機能には音声、3G データ(EV-DO、HSDPA 等)、Wi-Fi、コンピュータケーブル、Bluetooth があります。加えて、SMS テキストメッセージおよび MMS マルチメディアテキスト機能があります。

侵入経路の一つとして、携帯電話がネットワークコンピュータにアドレス帳およびカレンダーを上書きするためやアプリケーションをダウンロードするためにケーブルで接続されている場合が挙げられます。アプリケーションやファイルが携帯電話にダウンロードされるのと同じ要領で、不正プログラムやウイルスも侵入します。RIM Blackberry や Apple iPhone のようなワイヤレスのデバイスは、不正プログラムが直にダウンロードされた際に感染します。

トレンドマイクロの専門家は、携帯電話への攻撃はまだ主流にはなっていないが将来的に増える可能性が大いにあると見ています。トレンドマイクロ インキューベーションマーケティングのシニアディレクター、トッド・ティエマンは次のように話しています。「コンピュータと同様の脅威がスマートフォンを襲うのは、もはや時間の問題です。不正プログラムの作者は、より多くの人々を標的にしたいと考えています。スマートフォンの成長とより速いデータ処理は、感染の可能性を著しく増加させます。明日の人気携帯電話が今日の最も強じんな不正プログラムに侵される日は近いと言えます。」

参考：

*1. Ben Worthen, Wall St. Journal, "Why IT Hates the iPhone,"

<http://online.wsj.com/public/article/SB120647580478363231.html?mod=blog>, March 31, 2008.

2. 賢いユーザになるためにースマートフォンセキュリティ最初の一步

トレンドマイクロ 研究プロジェクトマネージャのジャムズ・ヤネズは、次のように話しています。「携帯電話セキュリティにおける一番の問題は、認識の欠如です。携帯電話がコンピュータと同様にウイルスやその他脅威の標的となりうることを認識しているユーザは多くありません。」したがって、危険認識を高めるためのユーザ教育が最も大切な第一ステップです。トレンドマイクロのセキュリティ専門家はまた、スマートフォンおよびモバイル機器を安全に使用するために以下を心がけるよう提案しています。

電話をロックする

「最も簡単で基本的なセキュリティ機能は電話をロックすることですが、これはしばしば見過ごされています」とヤネズは言います。携帯電話はすべて、簡単なパスワードを使用することでロックおよびロック解除が可能です。電話をロックすることで、アドレスや電話番号等のデータが他人に盗まれることを防ぎ、スパイウェアその他悪意のあるアプリケーションのインストールが阻止されます。

Bluetooth の設定を変更する

Bluetooth を「接続不可（通信不可）モード」に設定し、携帯電話およびウイルスを蔓延させるデバイスに接続しないようにしておくことをお勧めします。（必要になれば、この「接続不可（通信不可）モード」設定は容易に解除できます。）また、Bluetooth 使用の際は、ウイルス感染等を防止するためにファイル受信は慎重に行う必要があります。万一携帯電話が感染した場合、すべての Bluetooth 機能をオフにして不正プログラムが新たな標的を見つけられないようにし、デバイスを再起動して標準設定に戻します。

送信者に注意を払う

いかに興味をそそられようとも、知らない人からのメッセージは削除することです。また、出所の不明なアプリケーションをインストールすることは控えるべきです。音楽やゲームは、合法で正規の Web サイトからのみダウンロードします。アプリケーションが万一感染した場合は、速やかにこれを削除します。

セキュリティソフトウェアをインストールする

トレンドマイクロでは、デスクトップやラップトップ用のウイルス対策アプリケーションと同様に携帯電話保護のソフトを開発してきました。現在、携帯電話保護の製品を二つ用意しています。個人ユーザ向けのスタンド・アローン・ソリューションと中小企業ユーザ向けの中央管理的なソリューションです。

トレンドマイクロのモバイルセキュリティは、データ喪失、ウイルス感染、その他攻撃からスマートフォンおよび小型コンピュータ（PDA）を保護します。暗号化と認証により、本体が紛失または盗まれた際にもデータが保護されます。ウイルス対策機能により、ウイルス、ワーム、トロイの木馬型不正プ

ログラム、SMS テキストメッセージスパムがブロックされます。さらに、内蔵のファイアウォールと検出システムにより、ハッカー、侵入者、DoS (Denial of Service：サービス拒否)攻撃からユーザを保護します。

職場で必要な規定

オフィス内でモバイル機器の使用を許可する場合、企業はしかるべき規定を設ける必要があります。規定作成には、企業内の IT、購買、人事、法務等の各部署が関わることを望ましいと言えます。セキュリティリスクを管理するために IT 部署では、モバイル機器の使用における明確な規定を設け、これらのデバイスを介してアクセスされる情報をコントロールします。第一ステップとして、組織内で使用されるデバイスの種類とモデルを把握し、企業の財産を保護するために適切で実行可能なセキュリティ規定を作成することが求められます。

データへのアクセスは慎重に

従業員が携帯電話やデバイスを社内のネットワーク機器につなぐことを許可する場合、会社はデータがアクセスされる前にユーザの認証を行うようにすべきです。またラップトップ PC におけるセキュリティ規定にならって、デバイスの盗難や紛失を防ぐための規定を設けます。さらに、社員が社内ネットワークから自身のデバイスにファイル等のデータを入手する際、必要なもののみコピーし、データ流出の危険を最小限に抑えることが重要です。また、データへのアクセスを必要な社員のみ限定することも大切です。

3. モバイル機器が危ない

デスクトップやラップトップ PC におけるセキュリティ脅威のほとんどは、モバイル機器にも起こりうると言えます。以下にその主要なものを取り上げます。

スパイウェア

モバイルの世界でスパイウェアと言えば、ユーザの居所を探るためにモバイル機器にインストールされたアプリケーションを指します。おそらくこれは、放課後の子供の活動や浮気しているかもしれない配偶者の行き先を探るために用いられます。スパイウェアは、合法的なソフトウェアと違法不正プログラムの中間的存在で、ユーザの許可なしにスマートフォンの OS にダウンロードされます。そしてスパイウェアは、携帯電話内のテキストメッセージおよび通話履歴等の情報をスパイウェアサーバに送信し、オンラインでこれらの情報を閲覧できるようにします。スパイウェアはまた、機密情報を盗む目的でも使用され、組織にダメージを与えたり、ユーザの個人情報を漏えいさせたりします。トロイの木馬型不正プログラムやキーロガーは、コンピュータから情報収集するのと同様に、モバイル機器からも機密情報を盗むことが可能です。このようなスパイウェアのインストールは、モバイル機器への物理的なアクセスをもって行われます。

テキストメッセージスパム

テキストメッセージスパムは、電子メールスパムに類似しています。ただし、アメリカでは、スパムを受信したユーザに料金が課されます。(アメリカ以外の多くの国では、スパム送信者のみに料金が課され受信者には課されません。) NBC ニュースによると、昨年送信されたテキストメッセージスパムは 10 億通以上に上ります。[*2] アメリカ国外のユーザの方がより多くのテキストメッセージスパムを受信しているようです。これは、アメリカ国外の方がテキストメッセージ送信料が安いからでしょう。ここ数年のアジアにおけるテキストメッセージスパムの流行は、この事実を裏付けています。最近では、BBC ニュースが報道した中国でのテキストメッセージスパムがあります。中国当局では現在、移動体通信事業者である「China Mobile」を介して 2 億人以上の携帯電話ユーザに送信されたスパムを捜査中です。[*3] 電子メールスパムとは違いテキストメッセージスパムの受信者は、電話会社に連絡して返済を求めることができます。テキストメッセージスパムは違法行為です。

ワームとウイルス

モバイルワームやウイルスは、コンピュータに感染するそれらと類似しています。無害に見せかけたファイルをユーザが誤ってインストールし、そのファイルがデバイスに感染し、標的とする新たな携帯電話を探します。これにより、通常の電話機能が妨害されます。最初のモバイル攻撃は、キャビルまたはキャリベワームで、2004 年に Symbian OS で確認されました。

またファイル管理プログラムを装った「QDIAL.A」というウイルスが 2005 年に登場しました。この不正プログラムは、イギリス、ドイツ、オランダ、スイスから SMS メッセージを送信しました。

今年 1 月トレンドマイクロでは、マルチメディアファイルを装った不正プログラム「SYMBOS_BESELO.A」を発見しました。この不正プログラムは、Nokia の古いモデル用の Symbian OS をインストールした電話機に感染しました。この不正プログラムは、Bluetooth と MMS メッセージを使用して自身の頒布活動を行いました。トレンドマイクロ モバイルセキュリティ 3.0 または 5.0 をインストールしたユーザは、この攻撃から守られました。

最近では、Windows モバイルポケット PC を標的にした不正プログラムがトレンドマイクロで検出されました。「WINCE_INFOJACK.A」として検出されたこのワームは、Windows CE 環境で実行され、シリアル番号、OS バージョン、モデル、プラットフォーム、ホスト名等の情報を収集して不正プログラムの作者に送信しました。「WINCE_INFOJACK.A」はまた、感染した電話のセキュリティ設定を変更しました。このワームは、モバイルデバイス内の感染したメモ리카ードまたは SMS テキストメッセージを介して侵入しました。

ハッキング

モバイル機器はまた、ハッキングおよび DoS (Denial of Service: サービス拒否) 攻撃の標的とされます。例えば「Skulls」という不正プログラムは、モバイル機器のアプリケーションへのリンクをすべて無効にします。デバイスが感染すると、ユーザはメールやインスタントメッセージの送信できなくなり、カレンダー機能が停止します。さらに、電話のアイコンがすべて頭蓋骨 (skull) に変えられてしまいました。

参考:

*2. NBC11.com, "Silicon Valley Firms Battle Growing Text Message Spam Problem,"
<http://www.nbc11.com/technology/15635555/detail.html>, 3/18/08.

*3. BBC News, "Beijing investigates spam attack,"
<http://news.bbc.co.uk/2/hi/business/7311242.stm>, 3/24/08.

※ セキュリティ最前線は、米国トレンドマイクロで発行しているニュースレター「*First Line Of Defense (FLOD)*」(英語)を元に翻訳したものです。

※ お申し込み:「*F.L.O.D. Threat Watch Newsletter Signup*」(英語)
<<http://us.trendmicro.com/us/newsletter/>>