新たなサイバー攻撃への対抗策

木村尚亮

2011年の夏、国内の防衛関連企業に対してサイバー攻撃が仕掛けられる事件が起きた。海外でも大手ネット企業やセキュリティ関連企業、さらに原子力発電所の制御システムまでもがサイバー攻撃を受けた。これらの攻撃は、特定企業やシステムに的を絞り、標的組織からの重要情報の奪取を目的とすることが多い。攻撃には「マルウェア」が利用され、手口が巧妙であるため特効薬となる対策はない。マルウェアの感染を防ぐ「入口対策の強化」と、感染をいち早く検知して実害を防ぐ「出口対策」を組み合わせ、多層的な防御策でこれらの攻撃に立ち向かう必要がある。

新たなサイバー攻撃の手口

特定の企業や個人のパソコンをマルウェア（コンピュータウィルスなど悪意のある不正なプログラム）に感染させ、重要情報を盗み出す新たな手口のサイバー攻撃は、「標的型攻撃」や「APT」（Advanced Persistent Threat：持続的標的型攻撃）などと呼ばれている。

攻撃者の目的は、標的企業が持つ知的財産などの重要情報の取得であることが多い。攻撃の特徴として、

- マルウェアが利用されること
- 事前に情報収集をするなど手口が巧妙であること
- 攻撃が気づかれにくいため長期間にわたること

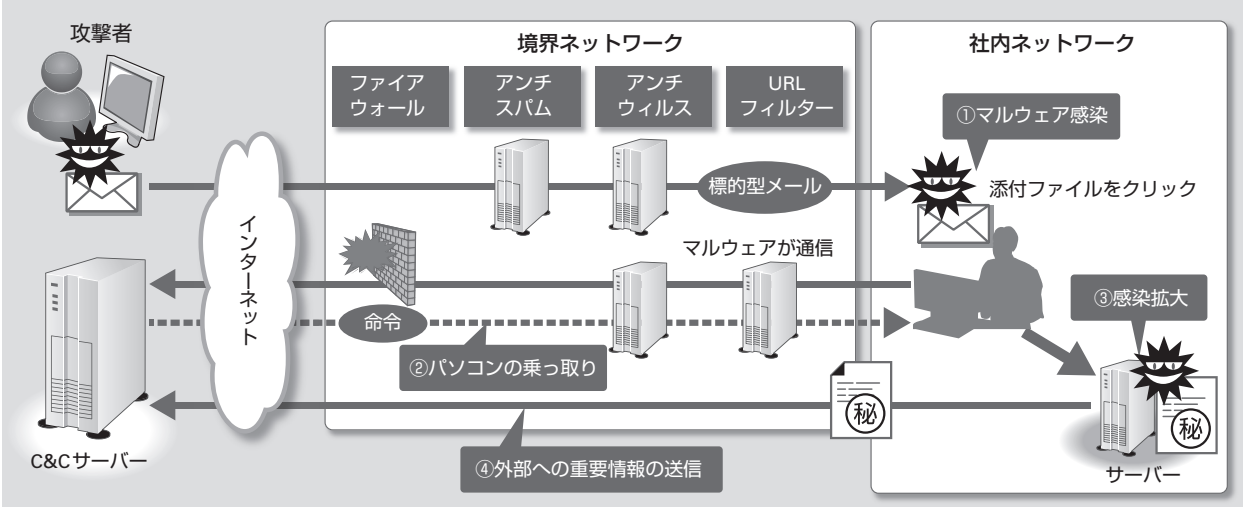
――が挙げられる。

このような攻撃は、一般に以下に示す段階を経る（図1）。

①マルウェア感染

攻撃者は、人事異動や打ち合わせ資料など、標的企業の受信者が興味を引く、または疑いを持ちにくい内容の電子メールを送付する。これにはウィルスを含むマイクロソフト・ワードや同エクセルの文書ファイル、PDFファイル

図1　標的型攻撃の代表的な手口



などが添付されており、ファイルを開くと受信者のパソコンがマルウェアに感染する。

②パソコンの乗っ取り

パソコンに入り込んだマルウェアがインターネット経由で通信を始める。通信先はコマンド&コントロール（C&C）サーバーと呼ばれる、攻撃者があらかじめ準備したサーバーである。攻撃者はC&Cサーバーを介してパソコンに命令を送ることができるようになり、パソコンは攻撃者に乗っ取られた状態となる。

③感染拡大

攻撃者は、パソコンに格納されている情報（受信メール、Webブラウザーのアクセス履歴、認証情報など）や通信を盗み見して得られた情報を使い、重要情報が格納されている企業のサーバーやドメインコントローラー（ユーザー情報の管理や認証を司るコンピュータ）へ侵入する。

④外部への重要情報の送信

FTP（ファイル転送プロトコル）やHTTP（Webサーバーとクライアント間のデータ転送プロトコル）など、企業から外部へ向けて許可されている通信を使い、企業の重要情報をC&Cサーバーに送信する。

表1　企業が実施している入口対策と標的型攻撃に対する有効性

入口対策	特徴
ファイアウォール	標的型攻撃の電子メールは、通常空いているSMTPポート（TCP25番）宛ての通信なので遮断できない。マルウェアからC&Cサーバーへの通信は、通常のWebブラウジングと同じHTTP（HTTPS）ポートが利用されることが多く遮断できない
スパムメール対策	広く出回っている広告目的などのスパム（迷惑）メールではなく、特定企業をターゲットにするために文面が考えられており、スパムメールと判定するのは困難
ウィルス対策ソフト	特定企業をターゲットに作成されたマルウェアであるため、パターンマッチング型のウィルス対策ソフトでは検知が困難。攻撃者は事前に主要なウィルス対策ソフトで検知されないことを確認してから電子メールを送付してくることもある
従業員教育	不審な添付ファイルやURLはクリックしないことなどについて従業員に注意を喚起し教育していても、攻撃者は事前に情報を収集してできるだけ不審に思われないような電子メールを送付してくるため、警戒せずにクリックしてしまうおそれがある
URLフィルター（HTTPプロキシー）	業務外利用や情報漏えい対策を目的とした製品であるため、マルウェア対策は範囲外であることが多い。対応する場合でも、マルウェアが通信するC&CサーバーのURLは短期間で変化し続けていくため、URLフィルターのデータベースに取り込むことは容易ではない

防ぎにくい標的型攻撃

これまで企業ではマルウェアを社内に入れない、もしくはマルウェア感染を防ぐことを目的とした「入口対策」が重点的に実施されてきた。

表1は、現在多くの企業で実施されている対策と、標的型攻撃に対する有効性についてまとめたものである。これらの対策は、標的を定めない不特定多数をターゲットにした攻撃には効果がある。しかし標的型攻撃の場合、攻撃者は標的企業の内部情報を事前に収集するなど周到な準備をしており、従来の対策では防ぐことが難しい。

現状では攻撃者側が優位であり、いったん標的にされてしまうと、情報セキュリティ対策を実施している企業でも被害に遭ってしまう。

入口対策の強化を

このように、従来型の入口対策では防ぐことが難しいため、標的型攻撃の対策としては、後述する「出口対策」に焦点が当たっている。しかし、マルウェア侵入を「やむをえない」と諦めるわけにはいかないし、入口対策には改善の余地がまだ残されている。

従来の対策のうち、多くの企業で十分ではないのがパッチ（修正プログラム）のマネジメントである。管理対象がマイクロソフト製品以外のソフトウェア（アドビシステムズ製品やJava〈ジャバ〉など）にも広がってきたことや、脆弱性が発見される頻度が高くなっていることから、アップデート（パッチの適用）が追いついていない企業が多い。

アップデートが追いつかない場合は、攻撃を受けた際の影響を緩和する対策を検討すべきであろう。アドビ・フラッシュやJavaに関しては、業務上必須でなければアンインストールすればよい。あるいは、通常利用するWebブラウザーでは無効化しておき、それが必要なWebサイトは別のWebブラウザーで有効化して利用するなどの使い分けが考えられる。アドビ・リーダーに関しては、攻撃で頻繁に利用されるJavascriptは無効化しておくべきである。あまり攻撃の対象とならない別のPDF閲覧ソフトを利用するという方法もある。

次に検討が必要なのは、アプリケーションソフトの「ホワイトリスト」化である。実行を許可してよいアプリケーションソフトを管理者がホワイトリストに登録し、マルウェアのような許可されていないプログラムが実行されることを防ぐ対策である。

ホワイトリストができれば、マイクロソフトから提供されている「ソフトウェア制限ポリシー」や「AppLocker（アップロッカー）」（Windows 7 UltimateとEnterprise、Windows Server 2008 R2で利用可能）などの機能を使ってアプリケーションソフトの実行を制限できるようになる。特に、AppLockerは実行ファイルの電子署名を判定条件に利用できるため、たとえば「アドビ・フラッシュ・アップデートのインストーラーは実行を許可する」というポリシーを定義すれば、アップデートの都度ホワイトリストを更新する必要がない。

一方で、標的型攻撃の被害拡大を受け、新たなソリューションやサービスも出てきている。技術的対策で最も注目されているのが「振る舞い検知型」のマルウェア対策ソフトである。既存のマルウェア対策ソフトはパターンマッチング型が主流であるが、振る舞い検知型は、ファイルを仮想環境で実際に実行させてマルウェア固有の動作をするかどうかを検知するロジックを組み込んでおり、既知・未知に関係なくマルウェアを検出できる。

人的な対策では、標的型攻撃の電子メールへの訓練が挙げられる。従業員に対して人事異動表などを装う訓練メールを送信し、本来自分に届くことが不自然な電子メールを受信させ、添付ファイルをクリックするかどうか判断することを実体験させる。従業員は訓練を通じて、標的型攻撃を身近な脅威として認識する。

訓練と併せて教育を実施することで、セキュリティ意識を向上させることも期待できる。また標的型攻撃の電子メールを受信した場合のエスカレーション（上司などへの報告）も併せて訓練しておくことで、組織としての対策の実効性を向上させる効果も見込める。

標的型攻撃の増加を受けて、内閣官房など12の政府機関が2011年10～12月に大規模な訓練を実施した。訓練は比較的短期間で実施できるため、標的型攻撃には即効性のある対策といえる。

出口対策のポイント

標的型攻撃に対する出口対策は、社内に入り込んだマルウェアや攻撃の兆候をいち早く発見し、

標的型攻撃の後続ステップである「パソコンの乗っ取り」「感染拡大」「外部への重要情報の送信」へと進ませないようにするための対策である。

出口対策では、認証つきプロキシー（プロキシーサーバーを使ったWebアクセスの際に認証を必要とする仕組み）を導入してマルウェアが外部向けに通信する際のハードルを高くしたり、マルウェアの外部向け通信を各種セキュリティ機器のログ（履歴）を監視して検知したりする方法がある。

しかしこれで万全というわけではなく、ログ監視にも問題点がある。たとえば従業員がプログラムを自由にインストールできるパソコンでは、ソフトウェアのアップデートのような正常の通信がログ監視によってアクセス違反として検知されてしまう。そのため、前述したアプリケーションソフトのホワイトリスト化などの対策を併用することによって実行可能なプログラムを制限し、管理可能な正常状態をつくり上げることで、監視精度を高めることが必要である。

感染が疑われる動作のアラート（警告）を検知した際には、実際にマルウェアに感染しているかどうかを短時間で切り分ける必要がある。これにより感染が発覚した場合は、迅速かつ適切な一次対処が求められる。さらに、被害状況を把握するために、何をするマルウェアなのかを素早く解析する必要もある。これらの対応は、情報セキュリティ対策のなかでも特に専門知識が要求される領域である。そのため、セキュリティログの監視を外部委託する場合には、上述のような対応が可能かどうかを確認する必要がある。

重要な「多層防御」の対策

情報セキュリティの基本は多層防御だといわれる。標的型攻撃には特効薬がなく、特に多層防御が重要となる。そのため、本稿で紹介した入口対策や出口対策を組み合わせた対策の検討が必要である。情報処理推進機構（IPA）から提供されている情報（www.ipa.go.jp/security/keihatsu/pr2012/general/02_targeted_attack.html）も併せて参照されることをお勧めしたい。

『ITソリューションフロンティア』2012年6月号より転載

木村尚亮（きむらたかあき）
MSS事業二部ITセキュリティアナリスト