標的型攻撃による情報漏えいを未然に防ぐために

浜村 憲
株式会社日立ソリューションズ　ネットワークプロダクト部
ken.hamamura.uf@hitachi-solutions.com

概要：標的型サイバー攻撃で狙われているのは政府機関や大企業だけでなく、大学や研究機関もターゲットとなります。重要な情報を流出しないためにも、攻撃手法とそのリスクを把握し、複数のセキュリティ対策を組み合わせた多層防御の考え方が必要です。

キーワード：標的型サイバー攻撃、セキュリティ、ファイアウォール、情報漏えい対策

1. 標的型攻撃対策の考え方

昨今、政府機関や特定企業を狙った標的型攻撃による情報漏えい事故が相次いでいます。NPO 日本ネットワークセキュリティ協会（JNSA）の選考委員会が発表した「JNSA 2011 セキュリティ十大ニュース」では東日本大震災を抑えて標的型攻撃が第 1 位に選ばれています。この事は、標的型攻撃によるインシデント発生を機に、従来通りの定番のセキュリティ対策では不十分であり、見直しが必要な局面にきているという危機感を選考委員が示したいと思った表れであろうと思います。

標的型攻撃は特定組織をターゲットに、メールや外部メディアなどで組織の端末に入り込み、そこから更に組織の内部へ入り込んでいき、最終的に知的財産や個人情報などの組織にとって非常に重要な情報を組織に気が付かれることなく盗み出すというものです。

以下に標的型攻撃の流れをご説明します。

▶ 事前準備
標的型攻撃では標的の情報を盗む前の準備段階として標的の組織に関係のある組織へ攻撃を行います。その組織に実在する個人名や組織間でやり取りしたメールなどの情報を収集します。

▶ 初期潜入
準備段階で得られた情報を活用して組織内の特定のメールアドレスに対して関係者を装ったメールが送付されます。添付されているファイルがウイルスソフトで検知できないと感染してしまいます。

▶ バックドア通信確保
侵入したウイルスは攻撃者と通信できるような環境を構築します。具体的には組織の業務で行っている HTTP の通信を模倣してやり取りを行い攻撃者とウイルスが通信できるようにします。これがバックドア通信です。

▶ 潜入調査
侵入したウイルスは数週間から数カ月にわたり組織のシステムに存在し、攻撃者とのやり取りを繰り返しながら重要な情報を探し出します。

▶ 情報搾取
最後にバックドアを通じて重要な情報を攻撃者へ送付します。これで攻撃者の目的は達成ですが、更に情報を窃取するために再攻撃を行う事もあります。

従来から組織内にウイルスを“入れない”ための対策として、ファイアウォールや侵入検知システム、ウイルス対策ソフトの導入、パッチ適用による脆弱性対策などが行われています。しかし、このような対策では十分とは言えなくなってきているのが現状です。では組織は、どのような対策を行えばよいのでしょうか。全てのソフトウェアの脆弱性対策を実施する事は困難であり、全ての通信をシャットアウトする訳にもいきません。組織にとって最大の損失は重要な情報を搾取される事ですので、万が一、ウイルスが組織内に侵入したとしても、ウイルスを“早く見つける”ようにする事と、攻撃者との通信をブロックして重要な情報を“出さない”ようにする事で、最悪の事態は回避するという考え方が必要になってきています。

2. キャンパスネットワークに求められる対策

標的型攻撃は特定の大手企業や政府機関がターゲットになる事が多いですが、決して大学や研究機関などが対象外ではありません。今年に入ってからも、何者かによる攻撃を受けたとして被害報告を出している大学が相次いでいます。これらの攻撃は前述の標的型攻撃ではなく、SQL インジェクション等の Web アプリケーションの脆弱性を突いた攻撃のようですが、いずれにしても学生の個人情報が流失する被害を出してしまったのは事実です。

多くの大学が PC を利用した授業を取り入れ、学生それぞれに PC を用意し、キャンパス内から有線・無線で自由にインターネットへアクセスできる環境を提供しています。最近では Twitter、Facebook、mixi などの SNS アプリケーションや Web メール、Skype、Windows Live Messenger のような P2P 技術を利用したメッセージングアプリケーションが多様化し、多くの学生が利用しています。ところが標的型攻撃においては、これらのアプリケーションが利用されているケースもあります。

そのような環境の中で大学のネットワークでは、「安全かつ利便性の高いネットワーク」の構築が求められています。安全なネットワークの構築には、3 つのポイントがあると考えます。

- ✓ウイルスを“入れない”対策
- ✓侵入したウイルスを“早く見つける”対策
- ✓重要な情報を“出さない”対策

この 3 つのポイントをまとめていきます。

2.1 ウイルスを“入れない”対策

脅威：

最近 Twitter、Facebook、mixi、などの SNS アプリケーションは就職活動中の学生にとっては人事担当者や先輩社員に直接コンタクトできるなどのメリットがありますので利用している学生も多いかと思います。企業側も積極的に SNS を活用しているケースも多くなっていますので、SNS を活用する事が就職活動を成功させるカギとなるとも言われています。しかし、これらのアプリケーションを利用する事でウイルス感染を引き起こす可能性がありますので、大学側にとっては大きな脅威となります。

例えば、Facebook で対象となる大学名で検索すれば、その大学に在籍する学生や職員、教授などが実名で把握する事ができます。攻撃者は実在する学生もしくは卒業生になりすましてアカウントを作成し、友達リスエストを送信するのです。一見して不審者だと分かる場合は拒否すると思います。ところが攻撃者も巧妙なだましの手口を駆使しているので、偽物だと気が付かずに承認してしまう事があるようです。SNS アプリケーション上で友達になると、しばらくは、さりげないやり取りを行った後に、ウイルスを仕掛けたサイトへ誘導したり、直接ファイルを送りつけたりするのです。友達から送られてきたファイルは警戒することなく開いてしまうケースが多いようです。しかもそのファイルには、ウイルス対策ソフトベンダーさえ認識していない未知のウイルスが添付されているのです。

標的型攻撃においては、こうしたソーシャルエンジニアリング※を巧みに利用した手法が多く利用されています。もし、このような事が大学のネットワーク内で行われていたとすれば、ウイルス感染や、情報漏えいといった事故を招いてしまう可能性が多いにあります。

※ソーシャルエンジニアリング：人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のこと。

対策：

ネットワーク上の流れるアプリケーションを正しく把握する必要があります。大学のセキュリティポリシーに従ったルールを適用し、不正なアプリケーションの使用を制限する事が重要です。完全に禁止してしまうと利便性を損ないますので、例えば Twitter であれば“閲覧”は許可して“つぶやき”は禁止するなどの柔軟な対策をとる事で、安全性と利便性の両立ができます。

また、標的型攻撃で攻撃者が送りつけるウイルスは、従来通りのシグネチャーベースのパターンマッチングでは検出・駆除できない

可能性が高いです。攻撃者は主要なウイルス対策ソフトでは検知されない事を確認した上でウイルスを送りつけていると考えられます。このような未知のウイルスへの対策においては、クラウド型のウイルス検知サービスが有効です。これはファイアウォールが任意のアプリケーションから送られてきた未知の.EXE や .DLL ファイルを検出すると、そのファイルをクラウド上にある仮想サンドボックス環境で一旦実行してみて、挙動を明らかにする事により、未知のウイルスであっても検知するサービスです。検知後は迅速にシグネチャを自動生成する為、継続する攻撃に備えることもできます。

2.2 侵入したウイルスを“早く見つける”対策

脅威：
標的型攻撃により、学内のネットワークに侵入する事に成功したウイルスは攻撃者のサーバ（C&C サーバ）と通信が出来るような経路を開設します。この通信経路であるバックドアは職員もしくは学生の PC からインターネットにアクセスするのと同じ HTTP 通信です。そのため、既存の対策で検知し、通信を遮断する事は困難であると言えます。このバックドアを使って拡張機能がダウンロードされ、更に学内の深部へと侵入してきます。これ以降、攻撃者はシステム内容を調査、情報搾取のために執拗に侵入し続け、目的の情報に辿り着くまで調査範囲を広げます。

対策：
ウイルスに感染した PC を早期に発見し、バックドア通信を遮断する事が重要となります。そのためにはファイアウォールのログを分析する事が有効な対策となります。ログ分析で特徴的な通信の“振る舞い”から HTTP 通信を偽装したバックドア通信を見分ける事ができるのです。

バックドア通信を確保する際には特徴的な動きがあります。具体的には、HTTP 通信であっても IP アドレスベースの URL や DNS ドメインの URL、登録されたばかりのドメインの URL に定期的に、頻繁にアクセスするのが特徴です。例えば 1 日に数十回以上このような特徴的な URL にアクセスするような端末は、ウイルスに感染している疑いがあります。

ウイルスもすぐに重要な情報に辿りつけるものではなく、数週間から数カ月にわたり長い期間で、攻撃者とのやり取りを繰り返しながら重要な情報を探し出します。ですから定期的にログを分析し、早期に感染した疑いのある PC を割り出す事で最悪の事態（知的財産や個人情報などの情報漏えい）を未然に防ぐ事ができます。

2.3 重要な情報を“出さない”対策

脅威：
攻撃者は重要な情報を、バックドアを通して攻撃者のサーバ（C&C サーバ）に送信します。
これで攻撃者にとっては目標を達成した事になりますが、入手した情報にはシステム管理者のログインパスワードなども含まれますので、これらの情報を基に再度攻撃を仕掛けてくる場合もあります。このように一度、学内のネットワークに攻撃基盤を構築してしまえば何度も侵入を繰り返して、更なる情報搾取されてしまいますので被害が拡大してしまいます。

対策：
2.1 ウイルスを“入れない”対策でも書きましたが、ネットワークを流れるアプリケーションを正しく把握し、不正なアプリケーションの使用を制限する事は、情報漏えいを未然に防ぐ対策としても有効です。

標的型攻撃の被害事例を見てみると攻撃者のサーバ（C&C サーバ）は海外に設置してある事が多いです。侵入したウイルスは指定された C&C サーバと通信してバックドアを確保しようと試みますので、標的型攻撃でよく利用される特定国への通信を排除する事ができればバックドア通信を遮断する対策にもなります。国別の IP アドレスを保持しているデータベースを利用し、特定国との不要な通信を遮断する設定が可能なファイアウォールであれば有効な対策ができます。仮にその国に姉妹校がある場合には、その姉妹校との通信だけは許可する事も可能です。

3. まとめ

標的型攻撃への対策を考えるにあたっては

「外部からの攻撃は完全に防げないので万が一、ウイルスに感染しても、重要な情報の流出を未然に防ぐ事で被害を最小限に抑える」という考え方が重要です。それを実現するためには、多層防御の考え方が必要です。つまり、何枚もの防衛壁を設置するように複数のセキュリティ保護対策を組み合わせて実施するという事です。今回は標的型攻撃の対策として“入れない”“早く見つける”“出さない”という3つの対策を紹介してきました。簡単にまとめると以下のようになります。

① ウイルスを“入れない”対策
ネットワークを流れるトラフィックをアプリケーションで識別し、不正な目的で利用されるSNSアプリケーションを制御する必要があります。仮に未知のウイルスが添付されたファイルを開いても検知・駆除できる対策をしておくことも重要です。

② 侵入したウイルスを“早く見つける”対策
ファイアウォールのログを解析する事でウイルスに感染した疑いのある端末を早期に発見する事が重要です。侵入したウイルスは、C&Cサーバとのバックドアを確保しようと試みますので、その振る舞いを検知する事ができれば、ウイルスが拡大する前に対策を打つ事ができます。

③ 重要な情報を“出さない”対策
ネットワークを流れるアプリケーションを制限する事と、標的型攻撃でよく利用される特定国への通信をシャットアウトする事で、バックドア通信を遮断できます。大学にとって最大の損失は重要な情報が流出する事だという事を再認識する必要があります。

安全なネットワークの構築には、利用されるアプリケーションの制御、利用できるユーザの制限に加えて、バックドア通信を遮断する事が必要です。ここで誤解をしないでいただきたいのは「アプリケーションの制御とはSNSアプリケーションは危険なので全て禁止にしてしまう」という事でありません。
先に述べました通り、就職活動中の学生にとっては活用すべきアプリケーションですので、利用方法と利用者を制限したうえで許可する必要があります。このように大学のネットワーク構築には、安全性と利便性の両立を考えて、柔軟に対応できるようなセキュリティポリシー策定が求められています。

今回ご紹介した対策のようにファイアウォールの導入は非常に大きな効果があります。ただし、ファイアウォールを導入すれば、対策は万全という訳ではありません。導入したファイアウォールを大学内で定めたセキュリティポリシーに沿って運用することも重要です。更には、標的型攻撃の始まりがソーシャルエンジニアリングである事を考えれば、だましの手口に引っかからない為に、学生や職員を対象にしたセキュリティ教育を実施する事も必要である事を忘れてはいけません。

〈参考文献〉

- 独立行政法人情報処理推進機構セキュリティセンター「新しいタイプの攻撃」の対策に向けた設計・運用ガイド　改訂第2版　2011年11月
- NPO日本ネットワークセキュリティ協会「JNSA2011セキュリティ十大ニュース」2011年12月