IPA Technical Watch

2012年10月30日
独立行政法人情報処理推進機構

フリーメールからの送信が増加傾向に：最近の標的型攻撃メールの傾向と事例分析
～添付ファイルの詐称には手間をかけず、あえて exe ファイルのままの例も～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、IPAに情報提供のあった「特定の企業や組織、個人に特化した攻撃に使われる標的型攻撃メール」を分析した技術レポート（IPA テクニカルウォッチ 第11回）を公開しました。

標的型攻撃メールは、特定の企業や組織、個人に対して、だましのテクニックを使い添付ファイルを開かせたり、ウェブアクセスを誘うことでウイルスに感染させる攻撃の一つです。一見すると、普段からやり取りしている見慣れた文面で、更に詳しい内容を知るために、添付ファイルの開封を促すように書かれています。事実に即した内容を引用するなど文面が巧妙なため、メール本文の内容に意識が向き、差出人や添付ファイルの種類などを十分に注意せず、疑うことなく添付ファイルやウェブリンクを開いてしまうと考えられます。

IPAでは2011年10月から標的型サイバー攻撃の特別相談窓口で標的型攻撃メールの情報提供受付や相談受付を実施しています。
今回、IPAを対象にしたものを含む、2012年4月から2012年9月の間に入手した21件の標的型攻撃メールの分析を行いました。その結果から、最近の標的型攻撃メールの特徴は、無料で使えるウェブメールサービスを使ってメールを送ることや、exeファイルをアイコン偽装することなくそのまま添付するなど、メールの偽装に手間をかけていないという傾向を確認しました。

また、IPA宛に送り付けられた標的型攻撃メールの中には、実在の職員を詐称し、3分の間に19個のアドレスに対して送られたものがありました。それらのメールはいずれも同じメール本文と添付ファイルが使われ、だれかが添付ファイルを開くことを狙い、短時間に複数の宛先に集中して、送られていたと考えられます。

そのメールに添付されていた不審なファイルを検証環境で解析した結果、もしファイルを開いてウイルスに感染してしまうと、外部の攻撃者が用意する管理サーバと通信が行われ、パソコン利用者に気づかれることなく遠隔操作でパソコン画面の取得ができてしまうことが実証できました。
同じ解析を過去にIPA宛へ送られた他の標的型攻撃メールに対しても実施したところ、今回解析したメールと同じ管理サーバに接続するよう設定されていました。このことから、執拗に同一組織を狙う攻撃者の行動が確認できました。さらに、IPA以外へ宛てて送られた一部の標的型攻撃メールも同じ管理サーバに接続されるような設定があったことから、攻撃者は同一組織だけではなく複数の組織に対して並行して攻撃をしていることがわかりました。

本レポートでは、主な読者として企業や組織の情報システム部門の担当者を想定していますが、日常的にメールを業務で多用する一般社員にとっても、標的型攻撃メールの見分け方や、攻撃のからくりを知るうえで有益な情報です。IPAでは、このレポートが標的型攻撃メールに対する注意力や看破力を高める材料となって、被害の発生が少なくなることを期待します。

今後もIPAでは、標的型攻撃メールの情報提供の受付と相談対応を実施し、攻撃や脅威の発見、被害の予防、被害の拡大・再発防止を推進していきます。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター　青木／加賀谷
Tel: 03-5978-7591　Fax: 03-5978-7518　E-mail: isec-info@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ　横山／白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp