マネージドセキュリティサービス 最前線
第2回 ― 実例ベースで考える ―

標的型攻撃への対策

NTTコミュニケーションズ（株）　経営企画部
マネージドセキュリティサービス推進室
室長 **与沢 和紀**／主査 **新夕 将史**

連載第２回となる今回は、実際に企業が直面したインシデント事例に基づき、
最新の攻撃の実態とセキュリティ対策について紹介していきたい。

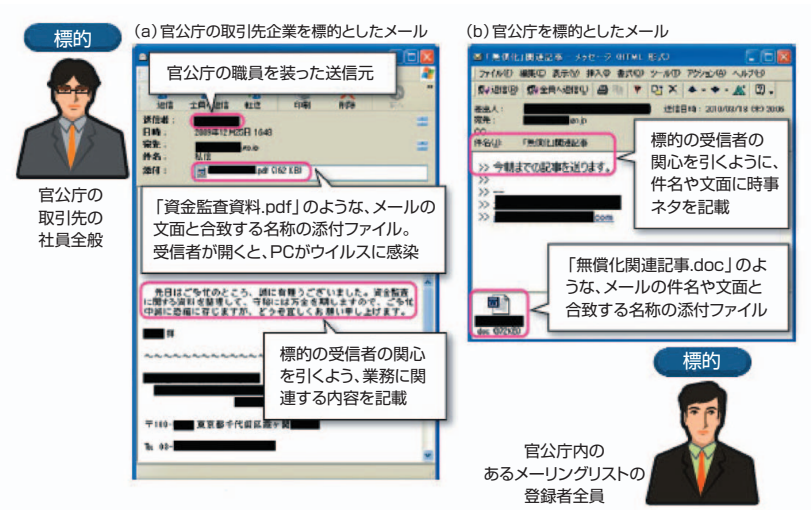
標的型メール攻撃の脅威

近年の攻撃手法の一つに標的型メール攻撃がある。攻撃対象を絞ってメールを送信し、受信者がマルウェア（不正プログラム）を仕込んだ添付ファイルを開封する、悪意あるWebサイト（マルウェアをダウンロードするしくみが埋め込まれている）にアクセスするなど誘導するものであることは前回触れた。

メールは対象者やその組織を研究し、内容に対象者が関心を抱かせるものを記載する、実在の組織のメールアドレスに偽装するなど、巧妙な形で送信される。このため受信者がメールを開封しないのは困難だ。実際に行われた標的型攻撃メール訓練で添付ファイルを開いてしまった割合は、巧妙なメールの場合30％に到達する（※1）。

マルウェアは企業内に侵入すると、攻撃者が遠隔操作を行うため設置したサーバー（C&Cサーバー）と通信を行い、さらに追加のマルウェアをダウンロードさせる。感染を拡大させて端末やサーバーから情報を入手したり、システムを停止するなどの不正行為が可能な状態になるのである。

なお、一般にマルウェア侵入の対策としては、アンチウイルス製品が想定されている。しかし現実的に実行されている標的型メールの場合、未知で新種のマルウェアが添付されていることが多い。実際にわれわれが既存のアンチウイルス製品で攻撃メールを駆除できるか試みたところ、感染チェックをすり抜けるマルウェアも多く見られた。それらのマルウェアにアンチウイルス製品のパターンファイルが対応するには１ヵ月



出典:ITPro（http://itpro.nikkeibp.co.jp/article/COLUMN/20120617/403226/）

図１　標的型攻撃で使われるメールの例

【Sandboxとは】

・シグネチャベースで検知できないマルウェアを発見するための技術

・社内ネットワークとは切り離した仮想環境に閉じ込めて、プログラムを実行

・プログラムを実行し、その挙動を監視することで、マルウェアかどうかを判定

・プログラムを複数の種類・バージョンのOS・ソフトウェアで実行

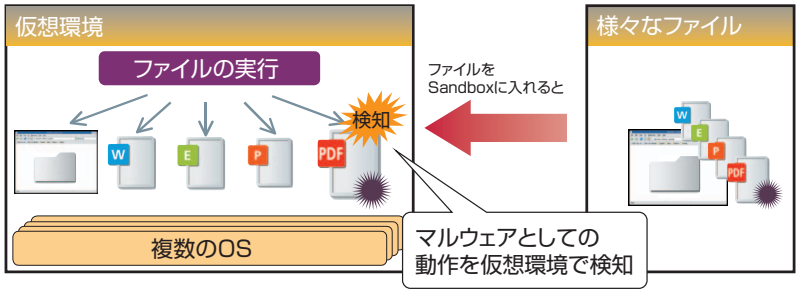


図２　Sandbox 技術

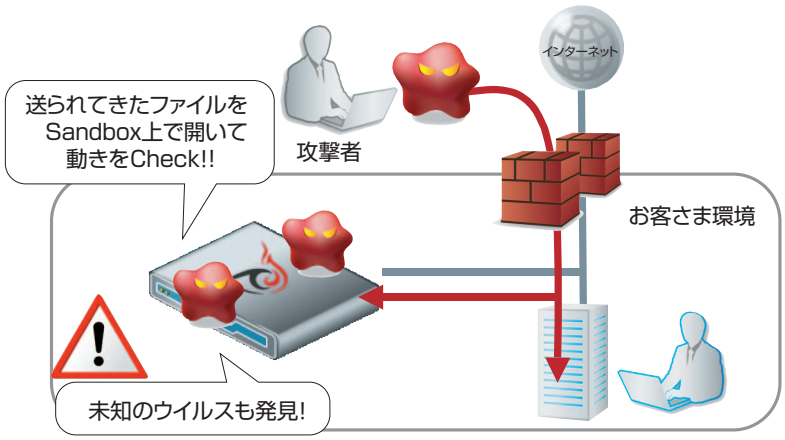


図３　リアルタイムマルウェア検知サービス

以上かかることもあり、既存の対策だけでは不十分であると言わざるを得ない。

攻撃による被害の実例と対策の導入

われわれが対策に関わった標的型メール攻撃による被害の事例としては、情報サービス関連企業のA社がある。A社では攻撃を受けたことにより、不幸にして機密情報が漏えいしてしまう結果となった。

A社は技術情報や取引先に関する情報が攻撃者にとって非常に価値のあるものとして狙われたと考えられる。

その発見は偶然であった。たまたまサーバーの異常値が検出されたのをきっかけに、不審に思った関係者が調査したところ、サーバー内にマルウェアが侵入していることと情報が漏えいしていた痕跡を見つけたのである。しかし、各種ログの調査により検知時点で最初の侵入から既に数か月以上が経過していた。

その後A社では、各機器のログを詳細分析してウイルス感染の被疑端末を特定し、該当端末をフォーマットするなどの対処を実施した。

われわれは被害に遭ったA社に対し今後、未知のマルウェアを用いた攻撃があっても、インシデントの再発を防止できるよう新たなタイプの対策の導入を行った。その内容をご覧いただこう。今回導入を進めたのはリアルタイムマルウェア検知とネットワーク／アプリケーションプロファイリングの各マネージドセキュリティサービスであり、標的型攻撃を早期に検知し情報漏洩等に至る前に対処するための策である。

リアルタイムマルウェア検知（RTMD）〜サンドボックスで未知の脅威を検出〜

RTMDが通常のアンチウイルス製品と異なるのは、Webアクセスやメールなどの通信を監視し、疑わしいファイルについては仮想環境（Sandbox：サンドボックス）で実際に開封・実行させることである。実行結果を解析することでファイルが不正なものかを判定するため、パターンファイルがなくてもマルウェア検知が可能である。

標的型メール攻撃の場合では、メールに添付されたり、メールに記載されたURLよりダウンロードされたりするマルウェアが、未知のものでも検知し被害の発生を防ぐ。また万一社内に侵入されても、C&Cサーバーとの通信や追加ファイルのダウンロードを検出することが可能である。

マネージドセキュリティサービス 最前線

第2回 ― 実例ベースで考える ―

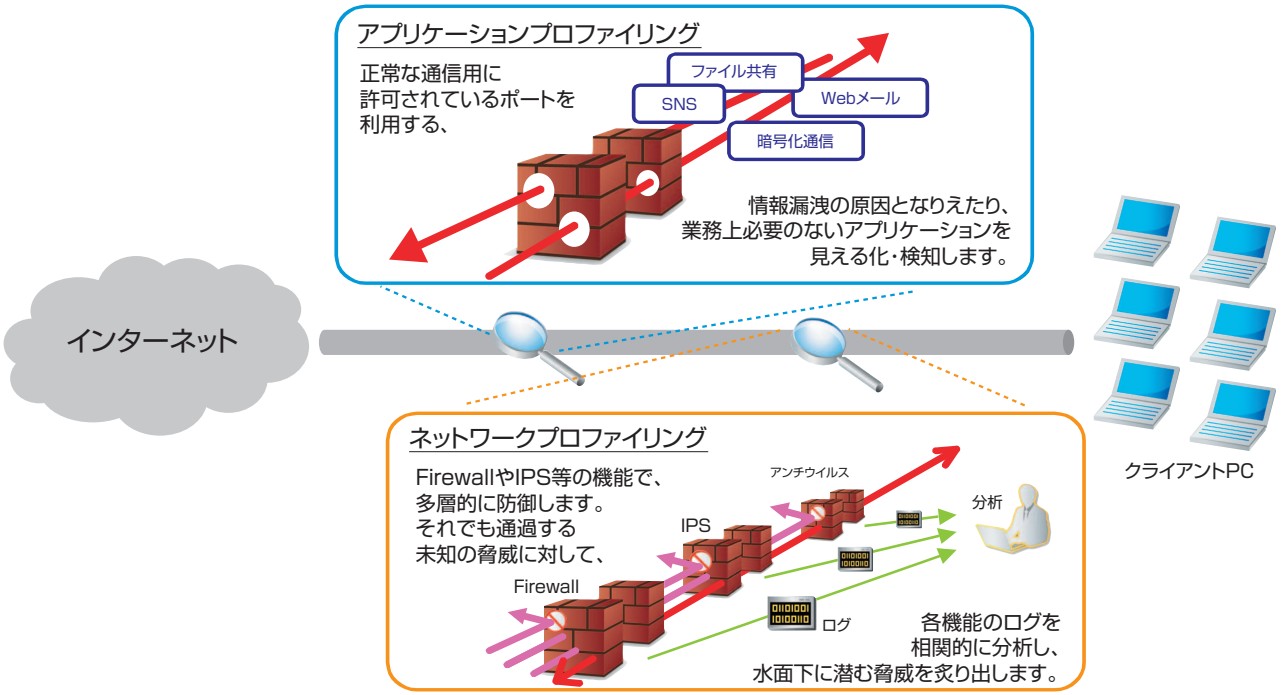


図4　ネットワーク／アプリケーションプロファイリング

ネットワーク／アプリケーションプロファイリング ～内部に潜む未知のリスクを可視化～

ネットワークプロファイリングでは、IPS/IDS、アンチウイルス、FW、URL filtering等の各種ログ情報からセキュリティエンジニアが独自に相関的に分析を行うことによりNW内のエンドポイントデバイスにおける不審な動作や、情報入手のためのサーバーへの異常なアクセスなどの潜在脅威を可視化し、通常気がつきにくい感染後の問題発見を可能とする。

またアプリケーションプロファイリングは、情報漏えいにつながるリスクのあるアプリケーションを可視化するものだ。例えばP2PファイルやWebメール、オンラインでのファイル共有サービスの利用など、管理者が許諾していない、ユーザーのアプリケーション利用を発見することができる。これにより、マルウェアの動作状況のみならず、セキュリティポリシー違反やコンプライアンス違反の通信活動などの検知も可能となる。

A社に対してこれらの対策の導入を進めた結果、管理者の目が行き届かず脆弱な状態のまま運用されている開発用サーバーが存在し、そこに攻撃の準備につながる外部からの調査行為がしかけられていたことをネットワークプロファイリングの手法で発見することができた。新たな被害が生じる可能性を未然に防ぐことができたのである。

まとめ

標的型メール攻撃は決してA社のような一部の企業だけの脅威ではない。いつ、どの企業が標的になってもおかしくはないものだ。それを回避するには、アンチウイルスなど既存のセキュリティ対策だけでなく、新たな対策が求められている。

もしあなたの属する企業や組織が、こうした攻撃の標的にならないか心配なら、あるいは既に不審な兆候が見られているのなら、ただちにわれわれに連絡をしてほしい。

（※1）弊社内で実施した標的型攻撃メール訓練の実例

お問い合わせ先
NTTコミュニケーションズ㈱
経営企画部 マネージドセキュリティサービス推進室
E-mail：mss-sp-cp@ntt.com