セキュリティ

ITマネジメント（内部統制）

「私は無害です」とサイバー攻撃者は欺く

組織から個人情報が盗み出される手口とは

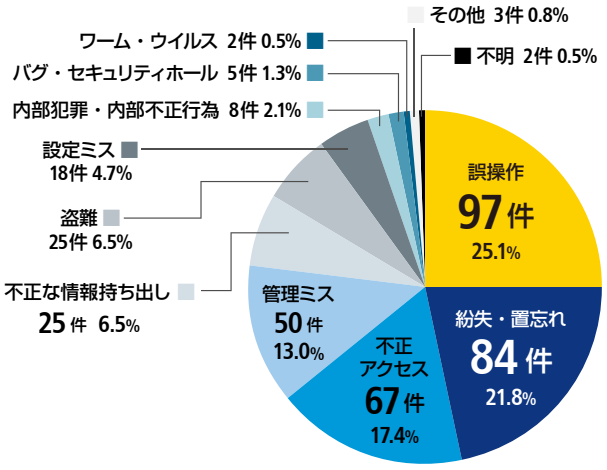
企業や団体、自治体などからの個人情報の漏えい事件が後を絶ちません。しかも、そのほとんどが攻撃を受けた組織ではなく、第三者からの指摘による発覚です。なぜサイバー攻撃者はデータを気づかれることなく盗み出すことができるのでしょうか。典型的な個人情報漏えい事件を例に、その手法について解説します。

標的型攻撃の拡大が情報漏えいを気づきにくくする

しばしば新聞紙面をにぎわせている個人情報の漏えい事件。JNSA(日本ネットワークセキュリティ協会)の調査によれば、2017年の情報漏えい件数は386件で、2016年の468件からやや減少しています。しかし、この調査はあくまで新聞などのメディアで報道された事件のみをカウントしているものであり、公表されないケースが少なからず存在することを考えると、実際にはもっと多くの情報漏えいが発生しているとJNSAではみています。

同調査によると、情報漏えいの原因はメール誤送信などの「誤操作」が全体の25.1%を占めており、次いで「紛失・置き忘れ」(21.8%)、「不正アクセス」(17.4%)と続きます。中でも不正アクセスは犯罪性が高く、その特徴は組織が自ら検知したのではなく、第三者からの指摘による発覚が多い点が特徴です。これは、標的型攻撃の手法が広く使用されるようになったためと考えられています。

標的型攻撃はAPT攻撃とも呼ばれ、非常に高度なサイバー攻撃です。攻撃者はターゲットに対しじっくりと時間をかけて調査し、巧妙な文面のメールを作成。添付ファイルやURLをクリックさせることでマルウェアに感染させ、気づかれないよう組織内で感染を拡大。最終的に個人情報など重要なデータを盗み出します。サイバー攻撃者は国家や企業に依頼を受けて攻撃を行うこともあり、潤沢なスタッフや予算を抱えている組織もあるといいます。



JNSA「2017年 情報セキュリティインシデントに関する調査報告書【速報版】」より

誰にも気づかれずデータを盗む、標的型攻撃の進化

一般に標的型攻撃は「事前調査」「マルウェア感染」「C&C(コマンド&コントロール)サーバとの通信確立」「内部移動」「情報の盗み出し」「痕跡の消去」といった手順を踏みますが、この際サイバー攻撃者は標的に気づかれないことに最大の注意を払います。

事前調査では、ターゲットの企業や従業員について調査を行います。まずSNSなどを活用し人間関係や趣味嗜好を把握、そして企業や個人が使用しているソフトウェアなどの情報も入手します。脆弱性のあるグループウェアやクラウドサービスなど、社外からアクセス可能なソフトウェアがあるかどうかを調べるためです。特にクラウドサービスは従業員が個人で利用しているケースも多く、侵入の糸口となりえます。

サイバー攻撃者はこれらの調査をした上で、ターゲットとなる従業員を絞り込み、添付ファイルを開きたくなるような、巧妙な文面のウイルスメールを送ります。使用されるマルウェアは、攻撃だけのために作られた「新種」であるため、ウイルス対策ソフトの検知をすり抜ける可能性が高くなっています。添付ファイル自体は普通に開くことができるため、従業員は不審を抱くことがありません。しかし裏ではマルウェアの活動が始まっており、感染を拡大させるとともに、パソコンにバックドアを開きC&Cサーバと通信を行います。

C&Cサーバはサイバー攻撃者がマルウェアに指令を出したり、盗み出した情報を受け取ったりするためのサーバです。サイバー攻撃者はC&Cサーバから次々にマルウェアを送り込み、感染したパソコン内で活動させます。そしてマルウェアは社内を移動し、重要な情報のある場所を突き止め、タイミングを見計らって盗み、C&Cサーバへと送信します。必要な情報をすべて盗み出したところで、サイバー攻撃者は活動の痕跡を消去し、証拠を隠滅します。

攻撃に気づかれないよう、サイバー犯罪者はさまざまな工夫を行います。たとえば、マルウェアとC&Cサーバの通信には、http(インターネットを利用する際に使用するプロトコル)を使います。これは、情報を盗み出す際の通信も同様です。また、重要な情報にアクセスする際も、従業員が業務でアクセスするタイミングに合わせて行うことで、発見される可能性を低くしています。さらに、その際に記録されるログも書き換えてしまいます。

近年では、他のサイバー攻撃も標的型攻撃の手法を取り入れるようになりました。感染に気づかれにくいマルウェアの採用や、C&Cサーバの使用、通信にhttpを使用することなどです。たとえば、ランサムウェアがファイルを暗号化する際の「鍵」をC&Cサーバに保存するケースも報告されています。そんなこともあり、サイバー攻撃の検知はますます難しくなっているのです。

関連サービス

マルウェア不正通信ブロック	NTTコミュニケーションズがDNSサーバーを提供するインターネット接続サービスにおいて、不正送金や個人情報漏えいなどによるお客さまの被害防止のために、悪意ある第三者が管理するC&Cサーバーとの通信を自動的にブロックします。
WideAngle マネージドセキュリティサービス	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが、ICT環境を24時間365日サポート。高度なセキュリティ監視により、実在するリスクと潜在リスクを可視化します。 また、「NWセキュリティ」をはじめとするセキュリティ対策パックメニューや、「リアルタイムマルウェア検知」などの機能をご用意、様々なご要望に応じて総合的なセキュリティソリューションを提供します。
WideAngle マネージドセキュリティサービス NWセキュリティ	ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。 セキュリティ運用基盤(SIEM)とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。
WideAngle マネージドセキュリティサービス リアルタイムマルウェア検知	アンチウイルスなど、従来のセキュリティ対策では検知できない、メールの添付ファイルやWebサイトに潜む未知の脅威を検知します。