経済レポート

経営者必読！

大規模サイバー攻撃「ランサム」で困る企業と困らない企業

テクニカルライター　井上孝司

猛威を振るう「Wanna Cry」

2017年5月の第2週頃から、まず欧米で、続いて日本でも、ランサムウェア「Wanna Cry」による大規模なサイバー攻撃の被害が続発している。欧州でルノーの工場が操業停止に追い込まれたと報じられた他、日本の大手企業でも感染事例がいくつか報告された。

2017年5月17日の時点で、感染したコンピューターの台数が、少なくとも34万台近くに達した、とする報道も出ている。

ランサムとは「身代金」のこと。悪意を持って作られたソフトウェアを総称して「マルウェア」と言うが、その内ランサムウェアは、感染対象になったコンピューター上にある文書データなどを勝手に暗号化してしまい、本来のユーザーがアクセスできない状態にしてしまう。そして、「データを読めるようにしてもらいたければ、身代金を支払え」と要求して来ることから、この名称がある。

しかし、実際にデータの暗号化が解除されるかどうかは、別の問題である。大規模感染が発生した「Wanna Cry」は、Windowsの脆弱性を突いて感染する。

ところで、「脆弱性を突いてウィルスが感染する」とは、どういう意味だろうか。ソフトの開発者は当然のことながら、さまざまな事態を考慮に入れて、セキュリティ上の不備が生じないソフトを開発するために努力している。しかしそれでも、特定の条件が揃った時に、セキュリティ上の問題が生じる事態まで、完全に阻止するのは容易ではない。

その「セキュリティ上の問題」の具体例としては、以下のものが挙げられる。

- **システムの動作に影響するため、本来はユーザーがアクセスできないようになっているファイルや設定項目が、アクセス可能になってしまう**
- **本来は実行できないようになっているはずのプログラムを実行できてしまう**
- **ソフトをインストールする際にユーザーに警告を出すのが本来の仕様だが、それが出ない**
- **本来は一般ユーザーとしてのアクセス（できることに制限がある）しか行なえないはずのプログラムや設定項目に対して、管理者とし**

てのアクセス（何でもできる）が可能になってしまう。いわゆる「特権の昇格」

誰かがこうした脆弱性を発見して、ソフトのメーカーに通報すると、メーカー側はそれを検証した上で、情報を公開すると共に、脆弱性を解消するためのセキュリティ修正プログラムをリリースする。

マイクロソフト（MS）が定期的に提供する「Windows Update」は、セキュリティ修正プログラムを導入する手段の典型である。

スマホやタブレットのオペレーティング・システム（OS）、あるいは各種のアプリケーション・ソフトについても同様に、脆弱性が見つかってセキュリティ修正プログラムがリリースされる場面は多い。

世界的な自動車メーカー、ルノーの工場も被害に

「著名人ゴシップ」は注意

マルウェアを作る側は、「どうやって感染させようか」と知恵を絞っている。ポピュラーな感染経路（アタック・ベクター）としては、電子メールの添付ファイル、あるいは攻撃者が設置したWebサイトへの誘導が挙げられる。

前者では「添付ファイルを開かせる」、後者では「リンクをクリックさせる」というアクションが必要だ。

添付ファイルが実行形式ファイル、つまり、プログラム本体であれば、ファイル名は「○○.EXE」となるから、ちょっと知識のあるユーザーであればたちまち警戒する。

そこで、普通の文書ファイルを利用するのは、相手の警戒心を緩めるための一つの手法だ。

リンクをクリックさせる手法の典型例としては、フィッシング詐欺がある。銀行やオンライン・ショップなどを装って「ユーザー認証システムが新しくなりました」とか、「パスワードの確認が必要です」といったメールを送りつける。

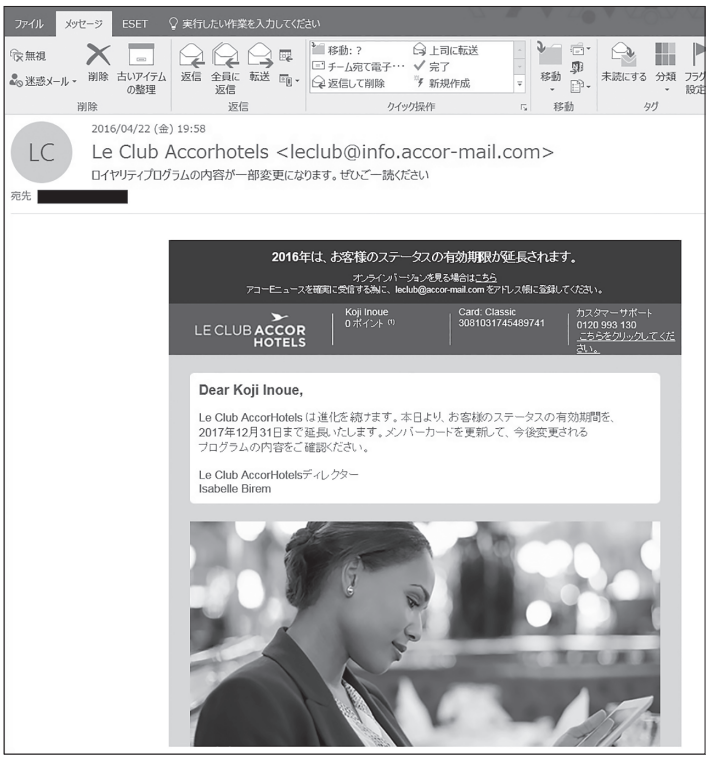
そして、メール本文中のURLをクリックさせて、攻撃者が設置したWebサイトに誘導する。そこでユーザー名、パスワード、銀行の口座番号やクレジットカードの番号などといった情報を入力させれば、それを利用した不正送金や資金の窃取に繋がる。

不特定多数を対象とする場合には、話題になっているニュースや著名人のゴシップなどを利用して受け手の興味をかきたてる手口が多い。

一方、ターゲットを特定の組織に絞り込んでいる場合には、業務上の連絡を装う手法が多用される。例えば、上司、同僚、あるいは取引先を騙ったメールを送って来る。

しかし、当節では、単に添付ファイルを開かせる、あるいはWebサイトに誘導するだけでは、マルウェアを送り込むのは難しい。そこで、実行形式ファイルではなく文書ファイルを利

フィッシング詐欺を企図したものと思われる不審なメールの一例。大抵はユーザー・アカウント情報の入力を求める内容なので一目瞭然だ。（筆者）



用したり、脆弱性を利用したりと、マルウェアを送り込むためにあの手この手という仕儀になる。

「業務に支障」で更新を躊躇

一般的にいって、マルウェアがもたらす被害は2種類ある。

1つは、それ自身が引き起こす被害で、「Wanna Cry」のように「貴重なデータが使用不可能になる」というものもあれば、「コンピューターが起動不可能になる」「コンピューターが過負荷になって使い物にならなくなる」といったものもある。

ところが、話はそれだけではない。もう1つの隠れた被害として、「マルウェアの発見・駆除のために多大な手間を要する」というものがある。マルウェアに感染したコンピューターが発見・駆除作業の対象になるのは当然だが、感染していないマシンであっても、安全を確認するために同様の手間がかかる。しかも、発見・駆除の作業を行なっている間は、当然のことながら、作業対象のコンピューターは使用不可能になり、結果的に業務を止めてしまう。それによる時間的・経済的損失は無視できない。

Windowsには、ファイル共有に使用する「SMBv1」という仕組みがある。LAN上にあるファイルサーバーや、ネットワーク接続型ハードディスク（NAS）に置かれているファイルを取り出したり、ファイルを書き込んだりする機能を実現するものだ。

この部分に脆弱性があり、「Wanna Cry」はそれを利用して感染する。

ところが実は、MSは「SMBv1」の脆弱性について、2017年3月に発表すると共に、セキュリティ修正プログラムもリリースしていた。その時点で、Windows Updateを実施したコンピューターであれば、「Wanna Cry」に感染することはなかったはずだ。

にもかかわらず、世界各地で感染事例が相次いでいるのはなぜか。

実は、過去に発生した大規模なマルウェア感染事案の多くは、すでにセキュリティ修正プログラムがリリースされているにもかかわらず、この適用を怠っていたマシンで発生している。つまり、ソフトウェアの更新を行なっていないユーザーが、世の中には案外と多いということだ。

これが、「セキュリティ修正プログラムの適用に手間がかかる」ということなら、まだ理解できなくもない。

確かに、個別に修正プログラムをダウンロードしてインストールしなければならないので面倒である。そういう手間をなくして、確実にセキュリティ修正プログラムを適用するために、Windows Updateのような仕組みが存在する。

実は、ソフト・メーカーがセキュリティ修正プログラムをリリースする際には、「こういう脆弱性があるので、修正プログラムをリリースします」という形になる。

その時点で、脆弱性の存在は一般のユーザーだけでなく、攻撃者にも知られてしまうのだ。だから、新しい脆弱性と、それに対応するセキュリティ修正プログラムがリリースされるとたちまち、脆弱性を利用して攻撃を仕掛けるプログラムの例、つまり実証コードが出回るのが普通だ。

つまり、セキュリティ修正プログラムのリリースは「安全性を高める」という一面と、「攻撃を誘発する」という一面がある。

もちろん、同プログラムを適用しなくていいということにはならない。攻撃を防ぐ手段が提供されているのだから、それを適用する方が好ましいのは当然である。

セキュリティ修正プログラムを適用した後で、システムの再起動を要する（つまり仕事が止まる）場面が多いことから、そのことを面倒に感じるのはありそうな話だが、話はそれだけではない。

企業ユーザーでしばしば耳にするのは、「Windows Updateの適用によって、社内で使用している業務用ソフトが動かなくなるのは困る」というものだ。筆者が日常的に利用している市販のアプリケーション・ソフトなどが、これによって動作しなくなった経験は皆無といっていい。だが、OSを構成するソフトが書き換わる以上、あらゆるソフトが影響を受けないと断言することはできない。

そして、自社のためだけに費用をかけて開発した業務用ソフトが使えなくなると、原因究明や改良版ソフトの開発・配布など、多大な手間と費用を要する。

しかし、だからといってWindows Updateの適用を怠れば、今回の「WannaCry」のような騒ぎに巻き込まれてしまう。

実は、アンチウィルス・ソフトについても同様の課題がある。実際、筆者が使用しているノートPCで、某社の同ソフトを導入したところ、メモリ

カード・スロットが使えなくなるトラブルが発生して、別の製品に切り替えた経験がある。

マネージメントとしての心得

前述したような事情があるので、セキュリティ修正プログラムの適用を遅滞なく行なうだけでも、被害の多くは防止できる。

そして、セキュリティ修正プログラムの適用や、アンチウィルス・ソフトの常時稼動によって、自分のコンピューターを安全な状態に保つことは、自分だけでなく、他のユーザーに迷惑を及ぼさないという観点からいっても必要なことである。

しかし、業務用ソフトが動かなくなるリスクを完全に否定できないのも事実だ。かと言って、それを理由にしてセキュリティ修正プログラムの適用を怠れば、結果としてさらに大きい損失に直面する可能性がある。

トレンドマイクロなど大手ネットセキュリティ企業は、「ランサム」に関してかなり以前から注意を喚起していた

では、企業を初めとするさまざまな組織のマネージメントを担当する立場、あるいは情報システムを管理・運用する立場としては、どう向き合っていけばよいのだろうか。

まず譲れない一線は、「セキュリティ修正プログラムの適用は不可欠」ということだ。

ソフト・ベンダー各社は、脆弱性に関する情報のリリースや、セキュリティ修正プログラムの配布・インストールを容易にするための仕組みをいろいろと整備しているから、それは活用する必要がある。

そして、社内情報システムを開発・整備する際には、同プログラムの適用による影響を受けない、あるいは影響を受けにくいような形で実現していくことを考慮する必要がある。

例えば、OSを構成する特定のファイルが、特定のバージョンのものでなければ動作しない業務用ソフトは、セキュリティ修正プログラムの適用によって影響を受ける可能性が高い。そういう事態を避ける配慮が必要だ。

また、新しい同プログラムのリリース、あるいはアンチウィルス・ソフトの導入に際して、社内の業務システムなどに影響が生じないかどうかを検証する体制も必要になる。問題がなければ、可及的速やかに導入するということでもある。

さらに、社員・職員に対する注意喚起も必要だ。近年のマルウェア感染事案の多くは、まず攻撃者から電子メールが送られてくるところからスタートしている。そのメールを見て「何か怪しい」と勘を働かせることができるかどうかだ。

実際、数年前に日本の防衛関連企業を狙って攻撃が仕掛けられた時、メールに不審を抱いて無視したために、攻撃回避に成功したメーカーの事例があったと聞く。

人間は最大の脆弱性になり得る存在だが、攻撃を阻止する際の砦でもある。なぜなら、コンピューターには「勘を働かせる」とか「ピンと来る」といった芸当はできないからだ。

そして、データの多重化を確実に行なうこと。もしも、ランサムウェアのようなマルウェアに感染してデータが使えなくなってしまったとしても、別のところにバックアップがあれば、データを回復させることはできる。

ただし、マルウェアの駆除を並行して行なわなければならないのは言うまでもない。