コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- はじめに
- パッチの適用
- バックアップについて
- フィッシングについて

WannaCryから学んだ教訓

はじめに

最近ニュースでも大きな話題になった「WannaCry」と呼ばれるサイバー攻撃を聞いたことがあるでしょうか。「WannaCry」は、20万台以上のパソコンに感染し、英国にある病院などではデータにアクセスできなくなってしまっています。この攻撃が大きな話題となったのには、いくつか理由があります。まず、パソコンからパソコンへの感染が早く、Windowsに存在する既知の問題を悪用していたこと。次に、この攻撃は、「ランサムウエア」という種類のマルウエアを使っており、感染してしまうと、パソコン上のファイルを暗号されてしまうため、自身のデータにアクセスできなくなる状態になってしまうということです。データを復元するためには、バックアップからの復元か攻撃者に身代金$300を支払い、データを復号してもらうしか方法はありません。そして、最後に一番重要なことですが、この攻撃はそもそも起きるべきではなかったということです。「WannaCry」が標的にしていたWindowsの脆弱性は、Microsoftによって知られているものであり、数か月前に修正パッチもリリースされていたものです。しかし、多くの企業では修正を適用していない、パッチが配布されなかった古いバージョンのOS、例えばWindows XPをまだ利用しているのが現状でした。以下に、「WannaCry」のような攻撃による感染を受けないためにできる3つのことをご紹介します。

ゲストエディタ

ヨハネス・ウルリッヒ博士は、SANS Technology Instituteの研究学部長であり、DShield.orgの創設者である。また、サイバーセキュリティ脅威を監視する**SANS Internet Storm Center**も運用しているほか、Web Application Security (**DEV522**)、Intrusion Detection (**SEC503**)およびIPv6 (**SEC546**)のコースを教えている。

パッチの適用

最初に、そして一番重要なことは、パソコン、モバイル機器、アプリケーション、そしてインターネットに接続しているすべてのデバイスを、常に最新の状態に保ってください。サイバー犯罪者は、利用されているソフトウエアに存在する新たな脆弱性を探しています。脆弱性を発見すると、特殊なプログラムを使い、利用している機器をハッキングし、侵入します。これらと並行して、ソフトウエアを開発した企業は、脆弱性を修正するためのアップデートを一生懸命開発しているのですから、パソコンやモバイル機器にこれらのアップデートを適用させることで、ハッキングされる可能性を低くすることができます。WannaCryの感染拡大において、残念なのはここです。この攻撃を防ぐためのアップデートは、マイクロソフトから2か月前に公開されていたもので、企業によってパソコンが最新の状態に保たれていれば、この攻撃は成功しなかったのです。機器を最新の状態に保つためには、自動で更新を行う設定にしてください。これは、ネットワークに接続されているすべての機器に当てはまります。パソコンやモバイル機器だけでなく、インターネットに接続されているテレビ、家庭用ルータ、ゲーム機器、そして車が当てはまる日も来るでしょう。Windows XPのようにオペレーティングシステムや機器が古すぎて、セキュリティアップデートの提供を受けることができないのであれば、サポートされているバージョンへアップグレードするようにしてください。

WannaCryから学んだ教訓

バックアップ

ランサムウエアのようなサイバー攻撃では、システムが最新の状態であっても感染してしまう可能性があります。自分を保護するためにできる二つ目のことは、データのバックアップを取ることです。バックアップは、自分のパソコンやモバイル機器以外に保存されている情報のコピーです。重要な情報を失ってしまった際には、バックアップからデータを復元できます。しかし、簡単でコストもそれほどかからないというのに、多くの人は定期的にバックアップを取ることをしていないのです。データのバックアップを取る方法は二つあります：物理的なメディアとクラウドストレージです。どちらのアプローチにも長所と短所があります。迷った場合は、両方使うという方法もあります。

WannaCryなどの攻撃から自身を守るためにできる3つのことは；パソコンを最新の状態に保つ、フィッシング攻撃に気をつける、およびシステムのバックアップを取ることです。

物理的なメディアとは、管理下にある外部接続のUSBドライブまたは自宅や社内のネットワークに接続されているドライブです。自身の物理メディアを使う利点として、大量のデータを素早くバックアップ、復元できることにあります。欠点は、ランサムウエアのようなマルウエアに感染してしまった場合、バックアップにも感染が拡大してしまう可能性があることです。バックアップに物理的なメディアを使う場合、外部の安全な場所にバックアップを保管してください。そして、保管するバックアップには適切なラベルを貼ってください。クラウドベースのソリューションは、インターネット上にバックアップを取ることで、ファイルを保管してくれるオンラインサービスです。多くの場合、プログラムをパソコンにインストールすると、後は勝手にやってくれます。クラウドソリューションの利点は、とにかく簡単であることです。また、ランサムウエアに感染してしまった場合であっても、クラウド上のバックアップにまでアクセスして悪影響を及ぼすことはほとんどありません。欠点として、大量データのバックアップ、復元には時間がかかることです。また、クラウドバックアップのプライバシーやセキュリティに関しても入念に調べてください。バックアップサービスは、例えば、データの暗号化や強い認証などの強度なセキュリティを提供しているかどうか、などがあるでしょう。

フィッシング

最後に、攻撃者は常に攻撃手法を更新、変更しています。サイバー犯罪者は、フィッシングと呼ばれる攻撃手法を使って被害者を感染させようとすることが多いです。フィッシングでは、サイバー犯罪者からメールが送られ、感染している添付ファイルの開封や悪意あるウェブサイトにアクセスさせようとします。どちらか一方でも行ってしまった場合、パソコンが感染してしまいます。「WannaCry」では、この手法は使われませんでしたが、他の攻撃ではよく使われている手法で、ランサムウエアの感染でもよく見られます。WannaCryを開発したサイバー犯罪者やグループは、いずれ攻撃手法を変え、フィッシングなどの手法を使って感染を拡大させようとするでしょう。メールによる攻撃から自身を守るためにできることは、常識に頼ることです。メールの内容が怪しい、出来すぎた話であった場合、攻撃である確率が高いと考えてください。

WannaCryから学んだ教訓

手本となるように

最後に忘れてならないのは、親として手本を示すことです。子供が話しかけてきた際には、モバイル機器を置き、目を見て話してください。食事中をしながらモバイル機器を利用したり、運転中しながら機器の操作は行わないでください。また、子供が過ちを犯してしまった場合には、それぞれを教育の場として扱うようにし、すぐに何かの処分を下さないようにしてください。毎回、「なぜ」ということを伝えた上で、見えない脅威から保護しようとしているということも念押ししてください。インターネット上で何か不快なことがあれば、いつでも相談しても良いということも一緒に伝えてください。その際には、スクリーンショットを取って見せるようにしてもらうと良いでしょう。大事なのは、何か過ちを犯してしまった場合には、いつでも相談できる雰囲気を作ることです。常にコミュニケーションを取れる状態にしておくことが、子供を現在のデジタルな世界での安全を保つ、最良の方法なのです。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内でも有数の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションなどの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。http://www.nri-secure.co.jp

リソース

マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
ランサムウエアについて:	https://securingthehuman.sans.org/ouch/2016#august2016
バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015
フィッシングについて:	https://securingthehuman.sans.org/ouch/2015#december2015
クラウドを安全に利用するには:	https://securingthehuman.sans.org/ouch/2016#november2016

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Translated By: 内山　貴之, 時田　剛