OUCH! | 2016 年 08 月

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...

- CEO詐欺とは？
- 自身を守るために

ランサムウエアについて

ランサムウエアとは

ランサムウエアは、マルウエアの一種で、現在インターネット上で広く感染活動が行われており、被害者のコンピュータ内にあるドキュメントや他のファイルを破壊しようとします。マルウエアはソフトウエアでありーコンピュータ用プログラムーとして悪意ある行為を行うものです。ランサムウエアは、感染すると特定のファイルまたはハードディスク全体を暗号化しまうことから、システムにアクセスできない状態になったり、ドキュメントや画像など重要なファイルにアクセスできなくなったりするという点でマルウェアと似ています。しかし、ランサムウエアは、被害者に対して、ファイルを復号し、システムのリカバリを行うためには、サイバー犯罪者に対しランサム（脅迫金）を支払う方法しかないと通知することで（ランサムウエアと呼ばれる所以はここにあります）攻撃者に利益をもたらすことから広く一般にも知られるようになりました。多くの場合、ランサムは、Bitcoinのようなデジタル通貨で支払う必要があります。また、ランサムウエアは、他のマルウエアと同様に感染範囲を広げようとします。一番使われる手法は、被害者に対し悪意あるメールを送信するというもので、巧妙に細工された添付ファイルを開くよう促したり、攻撃者のサイトへと誘導するリンクをクリックさせたりします。

ゲストエディター

レニー・ゼルスター氏は、NCR Corp で顧客のIT 運用に関するセキュリティマネジメント業務を中心に活動していますが、SANS Institute でトレーニングも担当しています。レニーは、ツイッター（@lennyzeltser）や zelster.com にて情報を積極的に発信しています。

ランサムは支払うべきか？

これは、難しい質問です。問題として、感染した際にランサムを犯罪者に支払う人が多くなればなるほど、犯罪者は感染活動を広げるモチベーションが上がることにつながるからです。しかしながら、ファイルをリカバリするためには、支払うという選択肢しかない場合があるでしょう。また、注意しなければならないのは、ランサムを支払ってもファイルを完全にリカバリできない可能性があることです。犯罪者を相手にしているわけですから、ファイルを復号しなかったり、支払いと引き換えに復号用のツールや手法を提供しても復号中に何か起きたりする可能性があるだけでなく、コンピュータが新たなマルウエアに感染してしまう可能性もあります。

ファイルをバックアップしましょう

ランサムウエアによる感染からランサムを支払わずに復旧する手法として最も有効なのは、ファイルをバックアップから復元する方法です。こうすることで、ランサムウエアに感染してもコンピュータをリビルドまたはクリーンアップした後にファイルを復元する方法が残されています。感染したコンピュータからバックアップにアクセス可能な場合、ランサ

ランサムウエアについて

ムウエアによってバックアップファイルを削除されたり、暗号化されたりする可能性があることを肝に銘じておく必要があります。そのため、ファイルのバックアップは、評判の良いクラウドベースのサービスや日頃は接続していない外付けのハードディスクに保存することが重要です。さらに、バックアップに関して、一般的な間違いとして挙げられるのは、テストをせずにファイルを実際にリカバリできると想定してしまうことです。バックアップを定期的に確認し、実際にランサムウエアに感染してしまった時のために、ファイルをリカバリできるかどうかを事前にテストしてください。バックアップは重要であり、ファイルを誤って削除してしまったり、ハードドライブが故障してしまったりした際にもバックアップからファイルを復元できます。

ランサムウエアはマルウエアの一種で、コンピュータが感染してしまうと、コンピュータ上のファイルをすべて暗号化してしまうため、それらにアクセスすることができなくなってしまいます。

さらなる防御手法

それに加えて、他のマルウエアなどに感染しないための手法は、ランサムウエアに感染しないための防御としても有効です。まず、信頼できるベンダが提供するアンチウイルスソフトをインストールし、最新の状態にしてください。このようなツールは、アンチマルウエアソフトウエアとも呼ばれ、マルウエアを検知し、悪意ある活動を食い止めるために設計されています。しかし、アンチウイルスソフトウエアは、すべての不正なプログラムを防いだり、削除したりすることはできません。サイバー犯罪者は、常に進化しており、新たな高度なマルウエアを開発し、アンチウイルスソフトウエアによる検知を避けようとします。そして、アンチウイルスベンダは、常に製品を更新しており、マルウエアを検知するための新たな機能を追加しています。ある意味、激しい競争になっており、どちらもお互いを出し抜こうとしています。しかし、残念なことに、現在は犯罪者の方が一歩先を行っているため、ファイルをバックアップしたり、下記の防御策を適用したりすることが重要です：

- サイバー犯罪者は、コンピュータや他のデバイスを感染させるために、ソフトウエアの脆弱性を悪用することが多くあります。ソフトウエアが最新版に近ければ近いほど、既知の脆弱性が少なくなり、サイバー犯罪者による攻撃を受けたりマルウェアに感染する可能性は低くなります。そのため、オペレーティングシステムやアプリケーションが自動的に更新が適用されるようにデバイスに設定にしてください。
- コンピュータを普段使用する際には、「管理者」や「ROOT」権限を持ったアカウントでは無く、制限された権限でしか操作することができないアカウントを使うようにしてください。これは、多くの種類のマルウエアが自身をインストールできなくするための追加の防御策となります。
- 多くの場合、サイバー犯罪者は、自分の代わりにマルウエアをインストールさせるよう騙してきます。例えば、正規のメールと見せかけた添付ファイルまたはリンクが含まれるメールを送るというものです。このメールは、

ランサムウエアについて

銀行や友人から送られたかのように偽装されています。添付ファイルを開いたり、リンクをクリックしたりしてしまった場合は、悪意あるコードが実行され、マルウエアがシステム上にインストールされてしまいます。メールの文章が切迫感を作り出したり、分かりづらかったり、話が出来過ぎたり、言葉遣いが拙かったりした場合は、このような攻撃である可能性があります。疑念を抱くことは良い事です。多くの場合、一般常識が最大の防御となります。

メールの添付ファイルを開いたり、リンクをクリックする際は、注意を怠らず、ランサムウエアから自身を守ってください。また、アンチウイルスソフトウエアを最新の状態にし、バックアップを定期的に行い、それらからファイルを復元できることも定期的に確認してください。

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

日本語版翻訳ー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、国内最大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

フィッシングについて:	https://securingthehuman.sans.org//ouch/2015#december2015
マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
暗号について:	https://securingthehuman.sans.org/ouch/2016#june2016
バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoftの記事:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 コース - マルウエアのリバースエンジニアリング:	https://sans.org/for610

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