KASPERSKY lab

カスペルスキー クリプトマルウェア対策
サブシステムでユーザーデータを保護

サイバー犯罪者は、現実世界の犯罪者が編み出した手口をすぐに取り入れます。金銭をゆすりとる手口もその 1 つです。ランサムウェア攻撃で最も多い手口は、ユーザーのデータを暗号化してから身代金を要求するというものです。ユーザーにとってデータの価値は高いため、その大切なファイルを取り戻そうとして、多くのユーザーが金銭を払おうとします。しかし、身代金を払うのは賢明な選択ではありません。主な理由は、破壊されたデータを復号化できる保証がまったくないからです。しかも、最近のクリプトマルウェアは、以前なら解読不可能と思えた暗号化手法を用いるため、被害者の選択肢は身代金の支払要求に応じるか、ファイルを失うかの二択でした。もちろん、コンピューターに信頼できるインターネットセキュリティソフトウェアをインストールしていれば、不正な活動を検知できるでしょう。しかし、たとえ優れたアンチマルウェア製品であっても、新たに開発されたクリプトマルウェアを検知できるのはデータの破壊が始まった後です。したがって、これまで発見されておらず、データベースに登録されていないマルウェアが、無効化される前に一部のファイルを暗号化してしまう場合もあります。この問題を解決するため、Kaspersky Lab はクリプトマルウェア対策サブシステムを開発しました。

クリプトマルウェアの脅威

クリプトマルウェアは一般的に、文書ファイルに見せかけた実行ファイルとして、スパムメッセージに添付されて配布されますが、これ以外の方法で感染することもあります。たとえば、トロイの木馬 ZeuS/Zbot ファミリーなど、別のマルウェアによってインストールされるという実例も確認されています。

クリプトマルウェアの脅威は増大しています。Kaspersky Security Network では、2013 年に 280 万件のクリプトマルウェア攻撃を記録しており、その数は 2012 年の 9 倍以上に及びます。身代金の要求に応じる人がいまだに多いことからも、被害件数のさらなる増加が予測されます。ケント大学のサイバーセキュリティ学際研究センター（Interdisciplinary Research Centre in Cyber Security）が 2014 年 2 月に実施した調査によると、Cryptolocker の被害者のうち 40 % 以上が支払いに応じたといいます。さらに、Dell SecureWorks のレポートでも、Cryptolocker は 100 日ごとに最大 3000 万ドルを奪い取っていることが判明しています。

さらに、最新のマルウェアによって暗号化されたファイルを復号化できないことは、偽の修復方法という新たな脅威を招きます。ファイルを失って取り乱したユーザーが、解決方法を求めてインターネットを検索すると、暗号化データを「修復」できるというソフトウェアに行き当たることがあります。こうしたソフトウェアが、役に立たない「ソリューション」を売りつける詐欺だったというケースは、まだ救いがある方で、最悪の場合、さらなるマルウェア感染の可能性もあります。

暗号化マルウェアの進化

犯罪者の手口は年々巧妙化しています。初期のクリプトマルウェアは、暗号化と復号化に同じ鍵を使用する共通鍵暗号方式を採用していました。この場合は通常、アンチマルウェアベンダーのサポートを受けることで、破壊された情報を復号化することができました。しかしその後、サイバー犯罪者は公開鍵暗号化方式を採用するようになります。これは、ファイルの暗号化に使用する公開鍵と、復号化に必要な秘密鍵の、2 種類の鍵を使う方式です。実用化された公開鍵暗号化方式のうち、サイバー犯罪者が最初に採用したのは、RSA（この方式を発表した Ron Rivest 氏、Adi Shamir 氏、Leonard Adleman 氏の頭文字）でした。2008 年、Kaspersky Lab のエキスパートはトロイの木馬 GP

Code が使用していた 660 ビット RSA 鍵の解読に成功しましたが、鍵はすぐに 1024 ビットにアップグレードされ、復号化がさらに困難になりました。

最近の最も危険なクリプトマルウェアの 1 つが、先述のトロイの木馬 Cryptolocker で、これも公開鍵暗号化方式を採用しています。コンピューターに感染すると、指揮統制（C&C）サーバーに接続して公開鍵をダウンロードします。これは、もう 1 つの鍵である秘密鍵に Cryptolocker の作成者しかアクセスできないようにするためです。一般的に、身代金の支払期限は 72 時間以内に設定され、これを過ぎると秘密鍵が永遠に削除されてしまいます。この鍵がなければ、どんなファイルも復号化することはできません。カスペルスキー製品はこのトロイの木馬を検知できますが、システムがすでに感染している場合、破損したファイルを元に戻す方法はありません。

図 1：Cryptolocker の身代金要求画面

Kaspersky Lab のクリプトマルウェア対策サブシステム

最新のクリプトマルウェアで暗号化されたファイルを復号化することは、現時点では不可能です。そのため、データを守るための唯一の対策は、ファイルのバックアップとなります。ただし、一般的なバックアップでは（定期バックアップも）、最近更新されたファイルを守れないことから、十分ではありません。そこで、Kaspersky Lab は システムウォッチャーモジュールを基に、新たな対策機能を開発しました。

カスペルスキー システムウォッチャーは、ファイルの変更に関する情報など、最も関連性の高いシステムイベントデータを分析します。不審なアプリケーションがユーザーの個人ファイルを開こうとしているところを検知すると、ローカルで保護されたバックアップコピーをすぐに作成します。そのアプリケーションがマルウェアと判定された場合、システムウォッチャーは改ざんされたファイルを自動的にロールバックします。そのため、ユーザーはクリプトマルウェアに関して何もする必要はありません。保護プロセスの進捗状況の通知を受け取るだけです。

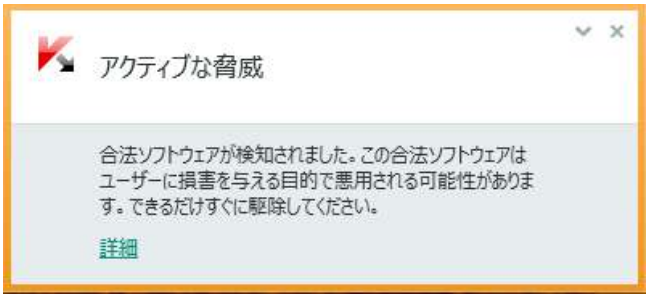

図 2: システムウォッチャーは、ファイルに対して不審な変更を行うアプリケーションを検知し、ユーザーに警告します。この時点で、ファイルの保護されたバックアップコピーを作成し、変更の性質を分析します

図 3: アプリケーションがマルウェアと判定された場合、そのマルウェアが含まれるファイルは削除されます。影響を受けたファイルは、暗号化されたままになります

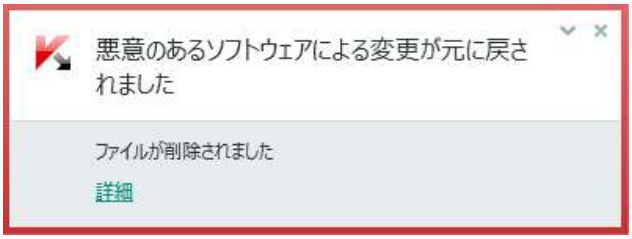

図 4: システムウォッチャーは、クリプトマルウェアの問題がすべて排除されたのち、暗号化されたファイルをバックアップコピーに置き換えて、不正なアクションがすべて取り消されたことを通知します

したがって、新たに開発されたクリプトマルウェアがゼロデイぜい弱性を悪用し、あらゆるセキュリティシステムを回避できたとしても、いかなる変更も自動的にロールバックされるため、実際の被害

は発生しません。言い換えれば、クリプトマルウェア対策サブシステムはユーザーのデータを保護すると同時に、サイバー犯罪者への間接的な資金提供を防ぐということです。身代金を支払うということは、犯罪者の活動を継続させ、悪意あるソフトウェアの開発を手助けすることにほかなりません。

搭載製品

クリプトマルウェア対策サブシステムは、以下の個人向け製品と法人向け製品に、システムウォッチャーコンポーネントの一部として搭載されています。

個人向け製品

- カスペルスキー インターネット セキュリティ
- カスペルスキー アンチウイルス

法人向け製品

- Kaspersky Endpoint Security for Business
- カスペルスキー スモール オフィス セキュリティ