2016 年 11 月 30 日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

ソーシャル・メディア上で画像ファイルを通じてマルウェアを配付する新たな手口

「ImageGate」を発見

ソーシャル・メディアを利用した最近のランサムウェア攻撃で用いられた手法

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社（本社：東京都、代表取締役社長：ピーター・ハレット、以下チェック・ポイント）は、ImageGate と名付けられた新たな攻撃ベクトルが当社のセキュリティ調査により発見されたことを発表しました。

サイバー犯罪者は、悪質なコードを埋め込んだ画像ファイルをソーシャル・メディア・サイトにアップロードし、設定上の問題に起因するインフラの脆弱性を利用して攻撃対象のユーザーにファイルをダウンロードさせることができます。ユーザーがダウンロードされたファイルをクリックすると、デバイスがマルウェアに感染します。

Facebook をはじめとするソーシャル・メディアを通じてランサムウェア Locky を拡散する大規模な攻撃キャンペーンを、セキュリティ業界全体が注視しています。このキャンペーンが実現するに至った経緯についてはこれまで謎に包まれていましたが、チェック・ポイントの調査員らは今回新たに発見された ImageGate がこの謎を紐解く手掛かりになるとの確信を強めています。

チェック・ポイントは、全世界のソーシャル・ネットワークや主要ウェブサイトへの影響を防ぐため、9 月初めに Facebook と LinkedIn に情報提供を行っています。

「ImageGate」攻撃の流れは https://youtu.be/sGlrLFo43pY のデモでご覧いただけます。

ランサムウェア Locky の場合、マルウェアを含むファイルをユーザがダウンロードして開くと、デバイス上の全てのファイルが自動的に暗号化され、身代金を支払わなければファイルにアクセスすることができません。このセキュリティ攻撃は現在も拡がっており、被害者の数は増えていると見られています。

デバイスの保護対策

チェック・ポイントでは以下の予防措置を推奨しています。

1. SNS サイトでは通常、画像を表示するのにファイルをダウンロードする必要はありません。画像をクリックしてすぐにブラウザがファイルのダウンロードを始めたら、そのファイルは開かないようにしてください。
2. 見慣れない拡張子（SVG、JS、HTA など）が付いた画像ファイルは開かないようにしてください。

本攻撃に関する詳細な技術情報が攻撃者に悪用されるのを防ぐため、チェック・ポイントは、影響を受ける可能性がある主要ウェブサイトの脆弱性が修正された後に公開する予定です。

チェック・ポイントの製品脆弱性調査部門責任者のオーデッド・ヴァヌヌ（Oded Vanunu）は次のように述べています。「SNS サイトの利用者が増えるなか、ハッカーはこうしたプラットフォームに侵入する方法の発見に力を入れています。SNS サイトは通常、利用制限の対象外とされるホワイトリストに登録されているので、サイバー犯罪者は攻撃活動の拠点として利用する新たな手口を常に探しています。最新の脅威からユーザーを保護するため、チェック・ポイントは、攻撃者の次なる標的を特定すべく全力を挙げています。」

■チェック･ポイントについて　　ONE STEP AHEAD

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（ http://www.checkpoint.co.jp/ ）は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
担当　マーケティング　石黒・溝口
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行　共同ピーアール株式会社
担当　中村・小林・上瀧
Tel: 03- 3571－5238 / Fax: 03- 3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp