2017 年 6 月 29 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

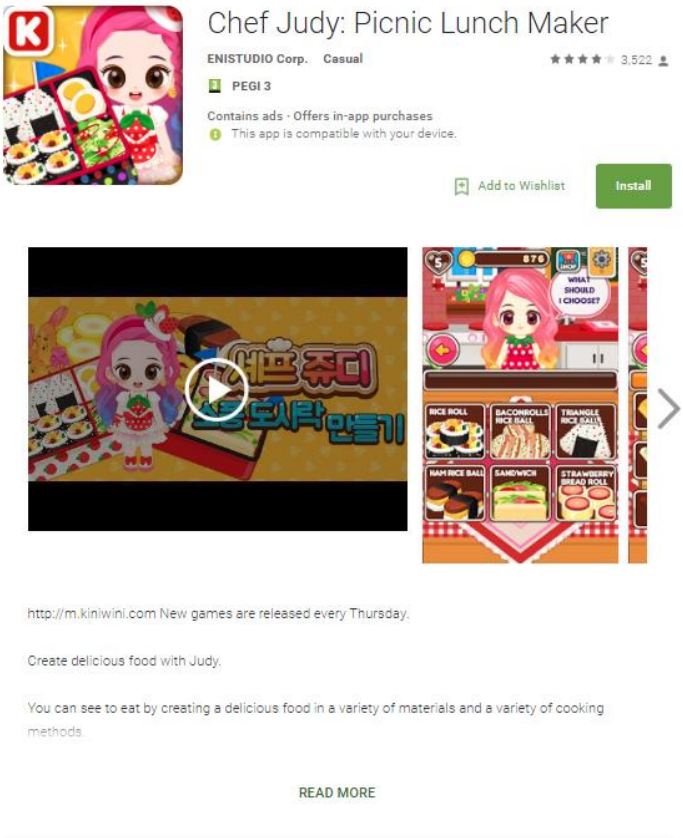
チェック・ポイント、Google Play に侵入した広告詐欺のマルウェア攻撃「Judy」を発見
～ 50 種以上の感染アプリダウンロード数は最大 1850 万件、3650 万人に拡散の可能性、Google Play は削除済み、高評価アプリも要対策～

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、Google の公式ストア Google Play に侵入した「Judy」と呼ばれる自動クリック・アドウェアによる、広範囲な広告詐欺のマルウェア攻撃を発見したことを発表しました。

Judy マルウェアは、韓国企業「Kiniwini」（Google Play 登録名は「ENISTUDIO corp」）が開発した 42 アプリに潜んでいました。他の複数の開発者が作成したものを含めると、 51 種の Judy マルウェア感染アプリが見つかっています。

Judy マルウェアは、感染したデバイスを利用して広告の不正クリックを大量に発生させ、加害者に不当な収益をもたらします。Judy マルウェアが潜む不正アプリのダウンロード数は少なく見積もって 450 万件、最大 1,850 万件に上り、計 850 万～3,650 万人のユーザに拡散している可能性があります。不正コードがいつ潜入したかは明らかでなく、拡散がどの程度進んでいるのかの実態は不明です。

図 1: Google Play で公開された不正な Judy アプリ



Judy アプリのうち Kiniwini 以外の開発者による最も古いものは最終更新が 2016 年 4 月だったため、この不正コードは少なくとも 1 年以上検出されずに Google Play に潜伏していたことが分かっています。

Judy も、以前 Google Play に侵入した FalseGuide や Skinner などのマルウェアと同様に、C&C サーバと連携して動作する仕組みになっています。チェック・ポイントの連絡を受け、Google Play ストアは該当するすべてのアプリを直ちに削除しました。

Judy はバナー広告を不正にクリックさせるだけでなく、場合によっては広告を大量に表示し、それを消すためにクリックし続けなければならない状況にユーザを追い込みます。関連するほとんどのアプリには高評価が付いていますが、DressCode など過去のマルウェア同様に、評価が高いからといって必ずしも安全に使えるわけではありません。ハッカーはアプリをユーザが高く評価するように誘導することもできます。公式のストアでもユーザの安全は担保されないため、未知のモバイル・マルウェアを検知し、ブロックできる高度なセキュリティ対策を導入する必要があります。

Judy の詳細、振る舞い、不正アプリのリスト、SHA256 のリストはブログ <http://www.checkpoint.co.jp/threat-cloud/2017/05/judy-malware-possibly-largest-malware-campaign-found-google-play.html>を参照ください。

■チェック・ポイントについて　　WELCOME TO THE FUTURE OF CYBER SECURITY

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　宮
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　花岡・上瀧
Tel: 03- 3571－5238 / Fax: 03- 3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

