2016 年 12 月 1 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

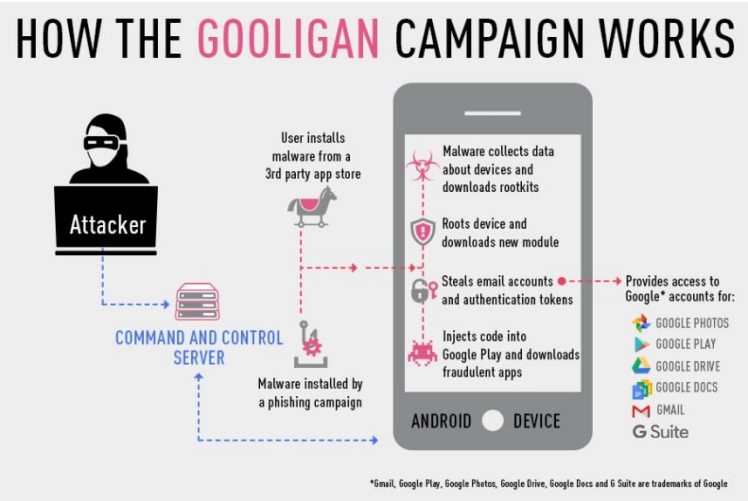
新たな Android マルウェア・キャンペーン「Gooligan」を発見
100 万件以上の Google アカウントに大規模セキュリティ侵害が発生

1 日当たり 1 万 3,000 台以上のデバイスに感染

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、新たな Android マルウェアにより、100 万件以上の Google アカウントがセキュリティ侵害を受けていることが判明したと発表しました。「Gooligan」と名付けられたこのマルウェア・キャンペーンでは、Android 搭載デバイスが root 化され、デバイスに保存されている電子メール・アドレスと認証トークンが窃取されます。攻撃者がこれらの情報を入手した場合、各種 Google サービス（Gmail、Google フォト、Google ドキュメント、Google Play、Google ドライブ、G Suite）の重要情報に不正アクセスされる恐れがあります。

攻撃の概要：

- このマルウェアで **1 日あたり 1 万 3,000 台**のデバイスが感染しています。100 万台以上のデバイスが root 化された事例は、今回の攻撃キャンペーンが初めてです。
- 窃取された電子メール・アドレスのうち数百件は、世界各国の企業で使われているアドレスです。
- 今回の攻撃キャンペーンが標的としているのは、Android 4（Jelly Bean、KitKat）および Android 5（Lollipop）です。両バージョンのシェアは、**現在使用されている Android 搭載デバイス全体の 74%近く**を占めています。
- デバイスを侵害した攻撃者は、Google Play のアプリを不正にインストールし、デバイス所有者を装いアプリを評価することによって、収益を得ています。
- この攻撃キャンペーンでは、1 日当たり **3 万以上のアプリ**が不正にインストールされて、キャンペーン開始以降のインストール数は 200 万を超えます。



チェック・ポイントは、この攻撃キャンペーンを発見後、直ちに Google のセキュリティ・チームに情報提供しました。チェック・ポイントでは、Google アカウントが侵害されているかどうかをチェックするオンライン・ツールを無償提供しています。

Google の Android セキュリティ担当責任者、エイドリアン・ラドウィッグ（Adrian Ludwig）氏は、次のように述べています。
「チェック・ポイントの、問題の把握と対策の実施への協力に感謝しています。Google では、Ghost Push マルウェア・ファミリーからユーザを保護する継続的な取り組みの一環として、Android エコシステム全体のセキュリティを強化するさまざまな対策を実施しています。」

Google は、被害を受けたユーザへの通知、トークンの無効化、Ghost Push ファミリーに関連するアプリの Google Play からの排除、Android のセキュリティ機構「Verify Apps」への機能追加などの措置を講じています。

チェック・ポイントのモバイル・リサーチ・チームが Gooligan のコードを最初に発見したのは、昨年、不正な SnapPea アプリを調査していたときです。その後 2016 年 8 月になって同マルウェアの新たな亜種が出現し、それ以降、1 日当たり 1 万 3,000 台以上のデバイスが感染被害を受けています。**感染デバイスの約 57%はアジア諸国**、約 9%はヨーロッパ諸国で使用されています。窃取された電子メール・アドレスのうち数百件は、世界各国の企業で使われているアドレスです。脆弱性のある Android 搭載デバイスに Gooligan 感染アプリをダウンロードしてインストールするか、フィッシングを目的とするテキスト・メッセージの不正なリンクをクリックすると、感染プロセスが開始します。

チェック・ポイントのモバイル製品担当責任者であるマイケル・シャウロフ（Michael Shaulov）は、次のように述べています。「詳細な Google アカウント情報が 100 万件以上窃取された今回の事件は、非常に深刻な事態であり、サイバー攻撃が次なるステージへと突入した事実を示すものです。攻撃者はこれまでの戦略を転換し、モバイル・デバイスに保存された重要情報に狙いを定めています。」

Google アカウントの侵害の有無を確認する Gooligan チェッカーはこちら(https://gooligan.checkpoint.com/)をご利用ください。

また、シャウロフは感染したデバイスの対応について以下を推奨しています。
「アカウントが侵害されていた場合は、Android 搭載デバイスのオペレーティング・システムをクリーン・インストールする必要があります。デバイスの電源をオフにし、クリーン・インストールに不明点がある場合は、デバイスのメーカーまたはモバイル通信事業者へ確認することをお勧めします。」

■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