

プレスリリース
報道関係各位

2019 年 7 月 17 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・ポイントのリサーチ・チーム、2,500 万台のデバイスに 感染している新たなモバイル・マルウェアを発見

ユーザの同意や操作なしに、インストール済みのアプリを勝手に不正なバージョンに入れ替える
「Agent Smith」マルウェア

米カリフォルニア州サンカルロス — 2019 年 7 月 10 日--ゲートウェイからエンドポイントまで、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（Check Point® Software Technologies Ltd. NASDAQ: CHKP）の脅威情報部門である Check Point Research は本日、世界で 2,500 万台、インドだけで 1,500 万台のモバイル・デバイスに密かに感染している新たなモバイル・マルウェアを発見したと発表しました。Google 関連のアプリに偽装されたこのマルウェアは、Android OS に存在する既知の脆弱性を悪用し、ユーザの同意や操作を必要とすることなく、インストール済みのアプリを不正なバージョンに入れ替えます。

映画『マトリックス』にちなんで「Agent Smith」と名付けられた同マルウェアは、現在のところ、デバイスのリソースに対する広範なアクセス権を用いて詐欺的な広告を表示し、金銭的利益を得るために使用されていますが、銀行の認証情報の窃取や盗聴など、はるかに有害性の高い目的にも容易に転用できます。同マルウェアの活動は、[Gooligan](#)、[Hummingbad](#)、[CopyCat](#) などの過去のマルウェアにも似ています。

チェック・ポイントのモバイル脅威検出リサーチ担当責任者のジョナサン・シモノビッチ（Jonathan Shimonovich）は、「このマルウェアは、ユーザがインストールしたアプリを密かに攻撃するため、一般的な Android ユーザが自分で対処することは困難です。今回の Agent Smith のような侵略型のモバイル・マルウェア攻撃を防ぐには、デジタル資産を保護する十分な予防対策を講じたうえで、高度な脅威対策と脅威情報を組み合わせて活用するのが最も効果的です。また、アプリのダウンロードは、感染のリスクを軽減するため信頼できるアプリ・ストアからのみ行うように心がけることも重要です。サードパーティ・アプリ・ストアの多くは、アドウェアが組み込まれたアプリをブロックするためのセキュリティ対策が十分ではありません」と述べています。

Agent Smith の元々の感染源は、人気のサードパーティ・アプリ・ストア 9Apps であり、主にヒンディー語、アラビア語、ロシア語、インドネシア語を解するユーザを標的としています。これまでのところ、インドを中心に、パキスタンやバングラデシュなどのアジア諸国のユーザに被害が広がっています。また、英国やオーストラリア、米国でも、少なからず感染被害が確認されています。チェック・ポイントは Google と緊密に協力しており、本プレスリリースの公開時点で、Google Play ストアに不正なアプリは登録されていないことを確認しています。

このモバイル・マルウェアの詳細については、[Check Point Research のブログ](#)または[チェック・ポイントのコーポレート・ブログ](#)をご覧ください。

本リリースは、米国時間 7 月 10 日に配信されたものの抄訳です。

■ Check Point Research について

Check Point Research は、チェック・ポイントの顧客やインテリジェンス・コミュニティ全般に向けて、業界有数のサイバー脅威情報を提供しています。世界中で発生しているサイバー攻撃に関する情報を ThreatCloud に蓄積して分析し、ハッカーを追跡しながら、チェック・ポイントの各製品に搭載される最新の保護機能の開発に携わっています。Check Point Research は、セキュリティ・ベンダー各社や捜査当局、各種 CERT と協調する 100 人以上のアナリストと研究者で構成されています。

■ チェック・ポイントについて

チェック・ポイント・ソフトウェア・テクノロジーズ (<https://www.checkpoint.com/>) は、世界各国の政府機関や企業など、あらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供する大手プロバイダーです。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェア、高度な標的型の脅威などの多岐にわたる第 5 世代のサイバー攻撃から保護します。企業のクラウドやネットワーク、モバイル・デバイスを、今日の第 5 世代のサイバー攻撃を含めてあらゆる脅威から保護するため、第 5 世代の脅威に対応するマルチレベルのセキュリティ・アーキテクチャ「Infinity Total Protection」を備え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。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。

《本件に関するお問い合わせ先》

広報代行 共同ピーアール株式会社

担当 上瀧・花岡

Tel: 03-3571-5238 / Fax: 03-3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp