※2016 年 5 月 17 日に米国シカゴで開催された Check Point Experience (CPX)で発表されたプレスリリースの抄訳です。

2016 年 5 月 25 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・ポイントの調査で、モバイル・マルウェア被害の深刻化が明らかに

ネットワークやデバイスに対するマルウェア攻撃の発生状況を示す「Check Point Threat Index」2016 年 4 月版で、iOS 搭載デバイスを狙ったモバイル・マルウェアの検出数が 50%増加

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 Check Point® Software Technologies Ltd.（NASDAQ: CHKP、インターナショナル本社：イスラエル、会長兼 CEO：ギル・シュエッド）は、組織のネットワークやモバイル・デバイスの攻撃に使用されたマルウェア・ファミリーの世界的な拡散状況を示す「Threat Index（脅威指標）」2016 年 4 月版を発表しました。

4 月の Threat Index では、2,000 種類のマルウェア・ファミリーが確認されました。前月比で 50%以上の増加となっていることからも、組織のネットワークは多種多様な脅威にさらされているだけでなく、重要なビジネス情報を保護するために対処すべき課題の規模が明らかになっています。2016 年 4 月の Threat Index の特徴は次のとおりです。

- iOS のアプリ開発プラットフォーム Xcode の改変版「XcodeGhost」で開発されたアプリが、組織のモバイル・デバイスにとっていまだに深刻なリスクとなっています。同プラットフォームで開発されたアプリは、2015 年 9 月に Apple App Store からすべて排除されました。しかし、今回また、iOS 搭載デバイスを攻撃するマルウェアが史上初めてモバイル・マルウェア・ランキングのトップ 3 にランクインしています。
- Android マルウェアの HummingBad が、全プラットフォーム、全世界を対象にした総合ランキングで引き続きトップ 10 にランクインしています。今年 2 月にチェック・ポイントの研究者が発見して以来、同マルウェアは急速に感染を拡大しており、攻撃者にとって Android 搭載デバイスは、企業のセキュリティを侵害する格好の弱点であり、見返りの大きいターゲットという位置付けになっていることがうかがえます。

チェック・ポイントのモバイル製品管理担当責任者であるマイケル・シャウロフ（Michael Shaulov）は、「ビジネスにおけるモバイル・デバイスの重要性は高まる一方です。モバイル・マルウェアの増加を示す今回の Threat Index は、サイバー犯罪者にとって、モバイル・デバイスが企業のセキュリティを攻略する最大の弱点になっているという事実を示唆しています。さらに今回明らかになったのは、高度な脅威対策の重要性です。マルウェアを未然に検出し防御するためには、ネットワークに加え、すべてのエンドポイントおよびモバイル・デバイスに高度な脅威対策を導入する必要があります」と述べています。

4 月の総合ランキングで最も検出数が多かったマルウェア・ファミリーは Conficker で、全体の 17%を占めています。第 2 位は Sality で全体の 12%、第 3 位は Zeroaccess で全体の 6%という結果になっています。検出されたマルウェア・ファミリーの内訳を見ると、トップ 10 にランクインしたファミリーが全体の半数以上を占めています。

- **Conficker** - 感染マシンの遠隔操作とマルウェアの追加ダウンロードを可能にするワームです。Conficker の感染マシンはボットネットの一部となり、指令（C&C）サーバから命令を受け取ります。
- **Sality** – 感染マシンの遠隔操作とマルウェアの追加ダウンロードを可能にするウイルスです。主な目的は、感染マシンに常駐して、攻撃者による遠隔操作と別のマルウェアのインストールを可能にすることです。
- **Zeroaccess** – Windows プラットフォームに感染するワームで、感染マシンの遠隔操作とマルウェアの追加ダウンロードを可能にします。ピアツーピア（P2P）プロトコルを使用して、リモートのピアから追加のマルウェア・コンポーネントやアップデートをダウンロードします。

4 月に検出されたモバイル・マルウェア・ファミリーのトップ 3 は次のとおりです。

- **HummingBad** - モバイル・デバイスに永続的な rootkit を組み込み、詐欺的なアプリをインストールする Android マルウェアです。キーロガーのインストールや認証情報の窃取、ユーザが導入した電子メール暗号化機能の回避といった追加機能を備える亜種も存在します。
- **Iop** – モバイル・デバイスの root アクセスを使用し、アプリをインストールしたり大量の広告を表示したりする Android マルウェアです。大量の広告やアプリによって、デバイスの使い勝手が大幅に低下します。
- **XcodeGhost** – iOS のアプリ開発プラットフォーム Xcode を改ざんしたプログラムです。XcodeGhost を使用して開発、コンパイルされたアプリには不正なコードが挿入され、このコードが C&C サーバにアプリ情報を送信します。アプリはデバイスのクリップボードの内容を読み取るなどの不正な活動を行います。

Check Point Threat Index について

Check Point Threat Index は、世界各地におけるリアルタイムのサイバー攻撃発生状況を追跡する ThreatCloud World Cyber Threat Map の脅威情報に基づいて算出されています。Threat Map のベースとなるのは、サイバー犯罪阻止を目的とした業界最大規模の協調型ネットワーク Check Point ThreatCloud です。世界規模の脅威センサー・ネットワークから収集された脅威情報や攻撃動向を配信する ThreatCloud のデータベースには、ボット発見を目的として分析された 2 億 5,000 万件以上のアドレスや、1,100 万件以上のマルウェア・シグネチャ、5,500 万件以上の不正サイトの情報が登録されています。ThreatCloud は、1 日あたり数百万種類のマルウェアを発見しています。

セキュリティ脅威や脅威対策の最新情報については、/threat-prevention-resources/index.html をご覧ください。

■チェック・ポイントについて　　WE SECURE THE FUTURE.

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　石黒佐知子
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行　株式会社プラップジャパン
担当　高橋・南宮
Tel: 03-4580-9109 / Fax: 03-4580-9135
Email: CheckPoint_pr@ml.prap.co.jp

©2016 Check Point Software Technologies Ltd. All rights reserved