※2016 年 6 月 21 日（火）に米国で発表されたプレスリリースの抄訳です。

2016 年 7 月 14 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、企業ネットワークを狙うマルウェア・ファミリーの増加傾向が明らかに

「Check Point Threat Index」の 2016 年 5 月版では、バンキング型マルウェアなど、
企業ネットワークを攻撃するマルウェア・ファミリーが引き続き増加

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）は本日、「Threat Index（脅威指標）」の 2016 年 5 月版を発表しました。この最新の Threat Index により、世界全体のアクティブなマルウェア・ファミリーが 15%増加している事実が明らかになりました。同月には、企業ネットワークを攻撃する 2,300 種類のアクティブなマルウェア・ファミリーが確認され、これで、50%の増加が報告された 3～4 月に引き続き、2 か月連続でマルウェア・ファミリーの種類が増加したことになります。アクティブなマルウェアの亜種が継続的に増えていることからも、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 5 月の Threat Index の特徴は次のとおりです。

- 5 月に最も広く利用されたマルウェアは引き続き Conficker でしたが、第 2 位にはバンキング型トロイの木馬の Tinba が入りました。このマルウェアは、ユーザが銀行の Web サイトにログインしているときに活動を開始し、Web インジェクションによる認証情報の窃取を可能にします。
- 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るなど、モバイル・デバイスに対する攻撃も継続して確認されています。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・ポイントの脅威対策部門責任者であるネイサン・シューカミ（Nathan Shuchami）は、「企業ネットワークを標的とする、アクティブなマルウェア・ファミリー種の大幅な増加が引き続き確認されています。攻撃者は日々新しいゼロデイの脅威を産みだしており、サイバー攻撃からネットワークを保護するために対処すべき課題が山積しています。最新の脅威にも効果的に対処できるよう、組織は高度な脅威対策の導入を検討する必要があります。ネットワーク、エンドポイント、モバイル・デバイスに高度な脅威対策を導入すれば、マルウェアを未然に検出し、防御できます」と述べています。5 月の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 14%を占めています。次いで、それぞれ約 9%を占めた Tinba と Sality が続きました。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 60%を占めています。

1. ↔ **Conficker** – Microsoft Windows システムのセキュリティ・サービスを無効にして、感染マシンの遠隔操作やマルウェアの追加ダウンロード、認証情報の窃取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。
2. ↑ **Tinba** – Tiny Banker や Zusy としても知られ、Web インジェクションによりユーザの認証情報を窃取するバンキング型トロイの木馬です。ユーザが銀行の Web サイトにログインすると、活動を開始します。
3. ↓ **Sality** – Microsoft Windows システムに感染し、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。その複雑さと適応能力から、史上最強のマルウェアの 1 つであると見なされています。

5 月に入ってからも、モバイル・マルウェアファミリーは企業のモバイル・デバイスを深刻なリスクにさらしており、ランキングでもトップ 100 内に 6 種が名を連ねています。そのほとんどが Android を標的としていますが、4 月以降は iOS を狙う数種も確認されています。5 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。

1. ↔ **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などの追加機能を備える亜種も存在します。
2. ↔ **Iop** – モバイル・デバイスの root アクセスを使用し、アプリのインストールや大量の広告を表示する 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。
3. ↔ **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である、チェック・ポイントの ThreatCloud™ です。世界規模の脅威センサー・ネットワークから脅威情報を収集し、攻撃動向を配信する ThreatCloud のデータベースには、ボットの検出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、550 万件以上の不正サイトの情報が登録されています。また 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、http://www.checkpoint.com/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