【米国報道発表資料抄訳】

2016 年 5 月 10 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

【メディアアラート】

チェック・ポイント調査の件数ランキングで「HummingBad」攻撃が急上昇、モバイル・マルウェアの脅威増加が引き続き顕著に

2016 年 3 月の脅威調査より、企業のネットワークやデバイスに対する攻撃において、
モバイル・マルウェアの利用が増えている事実が明らかに

2016 年 4 月 18 日（月）米国カリフォルニア州サンカルロスおよびフランス、ニース発 － 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.（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、お客様向けの年次イベントである「Check Point Experience（CPX）」において、2016 年 3 月の世界全体の組織のネットワークおよびモバイル・デバイスに対する攻撃において使用頻度の高いマルウェア・ファミリーを発表しました。

2016 年 3 月の全世界を対象とするマルウェア別攻撃件数ランキングでは、前月に初めてトップ 10 入りしたモバイル・マルウェアの HummingBad が第 6 位にまで順位を伸ばしました。しかも、チェック・ポイントの研究者により 2016 年 2 月に発見されたばかりであるにもかかわらず、すでに第 1 四半期全体のトップ 10 にも名を連ねています。この未知のマルウェア・ファミリーによる、Android 搭載デバイスを狙う攻撃が急増している傾向がうかがえます。

一方、チェック・ポイントが 3 月に検出したマルウェア・ファミリーは 1,300 種と、前月比で若干減少しています。この結果から、サイバー犯罪者が攻撃を実行する際には、完全に新規のマルウェア作成をもはや必要としていないという実態が読み取れます。攻撃者は、既存のファミリーにわずかな変更を加えるだけで、従来型のセキュリティ対策を回避する亜種を作成しているのです。同時に、チェック・ポイントの SandBlast や Mobile Threat Prevention など、感染前の段階でマルウェアを阻止する高度な脅威対策ソリューションを、ネットワークやエンドポイント、モバイル・デバイスに導入する必要性も浮き彫りになっています。

3 月のランキングで首位に立ったのは全体の 20%を占めた Conficker で、Sality（9.5%）、Cutwail（4%）がその後を追っています。トップ 10 入りしたファミリーを合わせると、検出された全攻撃の半分以上を占めています。

1. Conficker － 遠隔操作やマルウェアのダウンロードを可能にするワームです。感染したマシンはボットネットの一部として制御され、指令（C&C）サーバと通信して命令を受け取ります。
2. Sality － マルウェア管理者による感染システムの遠隔操作や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。システム内に残存し、遠隔制御やさらなるマルウェアのインストールを可能にする目的で利用されます。
3. Cutwail － スパム・メールの送信を中心に、一部の DDoS 攻撃でも使用されるボットネットです。ひとたびインストールされると、ボットは C&C サーバと直接通信し、送信すべき電子メールに関する命令を受け取ります。任務の完了後は、自身の活動に関する正確な情報をスパム業者に送り返します。

Android 搭載デバイスを狙うマルウェア・ファミリーの上位 3 種は以下のとおりです。

1. HummingBad － ターゲットのデバイスに対する永続的な rootkit の組み込みや、不正アプリ、キーロガーのインストールや認証情報の窃取、企業が使用する電子メール用の暗号化コンテナの回避など、さらなる不正活動を可能にする Android マルウェアです。
2. AndroRAT －ユーザが気付かない間にインストールされるよう自身と正規のモバイル・アプリをパッケージ化し、ハッカーによる Android 搭載デバイスの完全な遠隔操作を可能にするマルウェアです。

3. Iop – モバイル・デバイス上で root アクセスを使用し、アプリのインストールや過度の広告表示を行う Android マルウェアです。広告やインストールされているアプリが増えれば、ユーザのデバイス操作に支障が生じるようになります。

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、「HummingBad は 2016 年 2 月に世界全体のマルウェア・ファミリー上位 10 種に突如ランクインしました。その後、HummingBad を利用した攻撃は増加の一途を辿っています。すでに第 1 四半期全体のトップ 10 にも名を連ねており、この未知のモバイル・マルウェアが現実の脅威として急成長を遂げている実態がうかがえます。モバイル・デバイスを業務で利用する組織は日々増えていますが、モバイル・セキュリティは依然としてネットワーク・セキュリティに大きく遅れを取っているのが現状です。業務用のモバイル・デバイスへの効果的な保護機能の導入は、従来以上に急務となっています」と述べています。

チェック・ポイントの脅威インデックスは ThreatCloud World Cyber Map から得られた脅威情報に基づいています。この脅威マップは、全世界を対象としてサイバー攻撃が発生した経緯と場所をリアルタイムで追跡します。脅威マップの基盤となるのは、チェック・ポイントの ThreatCloudTM の情報データベースです。ThreatCloud は、サイバー犯罪阻止を目的とする業界最大規模の協調型ネットワークで、世界中に設置された脅威センサーのネットワークから収集した脅威情報や攻撃動向を配信しています。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、550 万件以上の不正サイトが登録されており、日々数百万種のマルウェアを検出しています。
チェック・ポイントの脅威対策に関する各種リソースについては、 /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