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、2019 年 6 月の Global Threat Index を発表
Emotet が活動を停止するも、一時的な休止に過ぎない可能性

Emotet ボットネットのインフラストラクチャは、6 月のほとんどの期間、活動を停止。ただし専門家は、新機能の追加に伴う一時的な休止と分析

カリフォルニア州サンカルロス – 2019 年 7 月 9 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、2019 年 6 月の『Global Threat Index（世界の脅威指標）』を発表しました。同チームによると、現在活動している中では最大規模のボットネットである Emotet は、6 月のほとんどの期間、活動を停止し、新たなキャンペーンを展開していませんでした。Emotet は、2019 年上半期を通じてマルウェア・グローバル・ランキングのトップ 5 にランクインし続け、大規模スパム・キャンペーンで拡散されていました。

リサーチ・チームの分析によると、Emotet が活動を停止しているのは、メンテナンスおよびアップグレードのためにインフラストラクチャをオフラインにしていることが理由と考えられます。この分析が正しければ、インフラストラクチャの準備が整い次第、強力な新機能を備えた Emotet が活動を再開することになります。

チェック・ポイントの脅威情報およびリサーチ担当ディレクターを務めるマヤ・ホロウィッツ（Maya Horowitz）は、「Emotet は、2014 年の登場以来、しばらくの間はトロイの木馬として活動していましたが、2018 年以降は、大規模なマルウェア・スパム・キャンペーンで他のマルウェアを拡散させるボットネットとして使用されるようになっています。Emotet は、6 月のほとんどの期間、活動を停止していたにもかかわらず、今回もマルウェア・グローバル・ランキングの第 5 位にランクインしています。この点からも、同マルウェアが極めて広範囲に感染を広げている事実がうかがえます。Emotet はおそらく、新機能を携えて再登場することになるでしょう」と述べています。

「コンピュータにインストールされた Emotet は、さらなるスパム・キャンペーンで自身を拡散させるほか、Trickbot などのマルウェアをダウンロードしてネットワーク内の他のシステムに感染を広げます。なお、この Trickbot は、特に悪質なことで知られるランサムウェアの Ryuk をネットワーク全体に感染させるという活動を展開します」（ホロウィッツ）

2019 年 6 月のマルウェア・ファミリー上位 3 種：
*矢印は前月からのランキングの変動を表しています。
2019 年 6 月のランキング上位は、引き続き 3 大マイニング・ツールが占めています。世界の 4%の組織に影響を与えた XMRig が第 1 位、次いで 3%の組織に影響を与えた Jsecoin と Cryptoloot が僅差の第 2 位と第 3 位に入っています。

1. ↑ **XMRig**： 仮想通貨 Monero の採掘に使用されるオープンソースの CPU マイニング・ソフトウェアで、2017 年 5 月に初めて確認されました。

2. ↑ **JSEcoin**： Web サイトに埋め込み可能な JavaScript によるマイニング・ツールです。JSEcoin では、ブラウザで直接マイニング・ツールを実行する代わりに、広告の非表示やゲーム内通貨の提供などのメリットが得られます。

3. ↓ **Cryptoloot**： 被害者の CPU や GPU の処理能力に加え、既存のコンピュータ・リソースも活用して仮想通貨の採掘を行うマイニング・ツールです。ブロックチェーンにトランザクションを追加し、新しい通貨を発行します。Coinhive と競合するツールであり、Web サイトで生じた収益から差し引く手数料を抑える戦略で優位に立とうとしています。

2019 年 6 月のモバイル・マルウェア上位 3 種：

モバイル・マルウェア・ランキングは、前月に続き Lotoor が第 1 位となり、Triada が第 2 位、そして初のランクインとなる Ztorg が第 3 位という結果になっています。

1. **Lotoor**： Android オペレーティング・システムの脆弱性を悪用し、感染モバイル・デバイスの root 権限を取得するハッキング・ツールです。
2. **Triada**： ダウンロードしたマルウェアにスーパーユーザ権限を付与し、システム・プロセスへの埋め込みを可能にする Android 向けのモジュール型バックドアです。ブラウザに読み込まれる URL を偽装するタイプも確認されています。
3. **Ztorg**： Android デバイスで権限を昇格させ、システム・ディレクトリに自身を組み込む Ztorg ファミリーのトロイの木馬です。感染デバイス上に別のアプリケーションをインストールする機能を備えています。

2019 年 6 月の脆弱性上位 3 種：

2019 年 6 月は、前月に引き続き、世界の 52%の組織に影響を与えた SQL インジェクションが第 1 位となっています。続いて、43%の組織に影響を与えた「OpenSSL TLS DTLS Heartbeat における情報漏洩」が第 2 位、41%に影響を与えた CVE-2015-8562 が僅差の第 3 位となっています。

1. ↑ **SQL インジェクション（複数の手法）**： クライアントからアプリケーションへの入力データに SQL クエリを挿入し、アプリケーションのソフトウェアに存在する脆弱性を悪用します。

2. ↑ **OpenSSL TLS DTLS Heartbeat における情報漏洩（CVE-2014-0160、CVE-2014-0346）**：
OpenSSL に存在する情報漏洩の脆弱性です。この脆弱性は、TLS/DTLS Heartbeat のパケット処理時のエラーに起因しています。攻撃者は、この脆弱性を悪用して、接続しているクライアントまたはサーバのメモリの内容を入手できます。

3. ↑ **Joomla におけるオブジェクト・インジェクションによるリモート・コマンド実行（CVE-2015-8562）**：
Joomla プラットフォームに発見されたリモート・コマンド実行の脆弱性です。この脆弱性の原因は、入力オブジェクトに対する検証が行われない点にあり、悪用された場合はリモートでコードを実行されるおそれがあります。リモートの攻撃者は、不正なリクエストを標的に送りつけることで、この脆弱性を悪用できます。脆弱性の悪用に成功した場合、標的のユーザのコンテキストで任意のコードを実行できます。

チェック・ポイントの Global Threat Impact Index と ThreatCloud Map の基盤となるのは、チェック・ポイントが運用している ThreatCloud 脅威インテリジェンスの情報です。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観測、認識しています。

本リリースは、米国時間 7 月 9 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（ 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のほかモバイル・デバイスに保存されている情報を、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

