プレスリリース
報道関係各位

2019 年 9 月 19 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 8 月の Global Threat Index を発表
Echobot が IoT デバイスを狙った大規模攻撃を実施

チェック・ポイントの研究者は、Emotet ボットネットの活動再開も指摘

米カルフォルニア州サンカルロス ― 2019 年 9 月 12 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、2019 年 8 月の『Global Threat Index（世界の脅威指標）』を発表しました。研究チームは、IoT ボットネット Mirai の新亜種である Echobot が多様な IoT デバイスに対する大規模攻撃を開始したと注意を呼びかけています。Echobot は、2019 年 5 月の登場以来、50 種類以上の脆弱性を悪用しており、特に「HTTP 経由のコマンド・インジェクション」攻撃は急増しており、世界の 34%の組織が影響を受けています。

8 月はこのほかにも、大規模ボットネット・インフラストラクチャの Emotet が、サービス停止から 3 か月ぶりに活動を再開しています。Emotet は、2019 年上半期に活動が確認された中で最も規模の大きいボットネットです。活動再開後、現時点ではまだ大規模なキャンペーンは確認されていませんが、近日中にスパム・キャンペーンが開始されるものと予想されます。

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、「5 月中旬に出現した Echobot は、悪名高い IoT ボットネット Mirai の新亜種です。50 種類以上の脆弱性を悪用しており、このところ攻撃件数が急増しています。Echobot は、世界中の 34%の組織に影響を与えていますが、この事実は、ネットワークやソフトウェア、IoT デバイスにパッチとアップデートを確実に適用することがいかに重要であるかを示しています」と述べています。

2019 年 8 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。
今月のランキングでは、XMRig が第 1 位の座を維持し、次いで JSEcoin が第 2 位という結果になりました。どちらも世界の 7%の組織に影響を与えています。第 3 位には、6%の組織に影響を与えた Dorkbot が続いています。

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。広告の非表示やゲーム内通貨の提供などのメリットをユーザにもたらす代わりに、ブラウザで直接マイニング・ツールを実行します。
3. ↔ **Dorkbot**：Dorkbot は、リモート・コード実行や、感染したシステムへのマルウェアのダウンロードを可能にする IRC ベースのワームです。

2019 年 8 月のモバイル・マルウェア上位 3 種：
8 月のモバイル・マルウェア・ランキングでは、Lotoor が第 1 位、次いで AndroidBauts と Triada がそれぞれ第 2 位、第 3 位という結果になりました。

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. **AndroidBauts**：Android ユーザを標的とするアドウェアで、IMEI、IMSI、GPS の位置情報などデバイスの情報を外部に送信します。モバイル・デバイスへのサードパーティ・アプリのインストールやショートカットの設置も可能となります。
3. **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。

2019 年 8 月の脆弱性上位 3 種：
脆弱性悪用ランキングでは、前月に引き続き SQL インジェクションが第 1 位となり、僅差で「OpenSSL TLS DTLS Heartbeat における情報漏洩」が第 2 位となっています。どちらも 39%の組織に影響を与えています。第 3 位には、38%の組織に影響を与えた「MVPower DVR におけるリモート・コード実行」が続いています。

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. ↔ **MVPower DVR におけるリモート・コード実行**：MVPower DVR デバイスにリモート・コード実行の脆弱性が存在します。リモートの攻撃者は、細工を施したリクエストを送りつけてこの脆弱性を悪用し、問題のルータ上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。

2019 年 8 月のマルウェア・ファミリー上位 10 種の詳細なリストは、チェック・ポイントのブログでご確認ください。

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、http://www.checkpoint.com/threat-prevention-resources/index.html をご覧ください。

本リリースは、米国時間 9 月 12 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

