ご参考資料（ブログ）
報道関係者各位

2018 年 11 月 29 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、10 月の Global Threat Index を発表
リモート・アクセス型トロイの木馬（RAT）が初のトップテン入り

RAT が初のトップテン入りの一方、引き続きマイニング・ツールが上位を占める

米カルフォルニア州サンカルロス ― 2018 年 11 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）は本日、2018 年 10 月の『Global Threat Index（世界の脅威指標）』を発表しました。この最新のレポートによると、引き続きマイニング・ツールが上位を占める一方、リモート・アクセス型トロイの木馬（RAT）が初のトップテン入りしています。

この 10 月は、コンピュータの乗っ取りとデータの窃取を目的とした RAT「FlawedAmmyy」を拡散する大規模なマルウェア・キャンペーンが発生しました。同じ RAT を拡散するキャンペーンはこのところ多発していましたが、その最新版である 10 月のキャンペーンは過去最大の規模でした。この RAT は、感染マシンのカメラやマイクへのフルアクセス、スクリーンショットの収集、認証情報や機密ファイルの窃取、ユーザの行動の監視などの機能を備えています。

FlawedAmmyy は、Global Threat Index のランキングでトップテン入りを果たした初の RAT です。

一方、ランキングの上位は引き続きマイニング・ツールが占めており、世界の 18%の組織に影響した Coinhive が第 1 位、8%の組織に影響した Cryptoloot がランクアップの形で第 2 位に入っています。

チェック・ポイントの脅威情報グループ・マネージャを務めるマヤ・ホロウィッツ（Maya Horowitz）は、「今月は、ランキング史上初めて RAT がトップテン入りを果たしました。このところ、FlawedAmmyy RAT を拡散するキャンペーンは複数発生していましたが、この最新のキャンペーンは明らかに過去最大規模であり、広範囲に影響を及ぼしています。ランキングの上位は依然としてマイニング・ツールが占めているものの、FlawedAmmyy のトップテン入りは、ログイン認証情報や機密ファイル、金融情報/決済情報などのデータが、今もサイバー犯罪者にとって実入りのよいターゲットになっている可能性を示唆しています」と述べています。

2018 年 10 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。

1. ↔ **Coinhive** – このマイニング・ツールはユーザが Web ページを訪れたときに、通知したり同意を得たりすることなく、そのユーザのリソースを利用して仮想通貨 Monero の採掘を行います。埋め込ま

れた JavaScript により、エンドユーザの大量のコンピューティング・リソースを利用してマイニングを実施し、システムのパフォーマンスに悪影響を及ぼします。
2. ↑ **Cryptoloot** – 被害者の CPU や GPU の処理能力に加え、既存の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。
3. ↓ **Dorkbot** – 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。

モバイル・マルウェア・ランキングでは、Android を標的とするモジュール型バックドア Triada が第 1 位となりました。前回の第 1 位だった、情報の窃取を目的とする Android 向けのバンキング型トロイの木馬 Lokibot は、第 2 位にランクダウンしています。第 3 位には、ランキングへのカムバックを果たした Hiddad が入りました。

2018 年 10 月のモバイル・マルウェア上位 3 種：

1. **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 を偽装する動作も確認されています。
2. **Lokibot** – 情報の窃取を目的とする Android 向けのバンキング型トロイの木馬ですが、管理者権限を取得できない場合はランサムウェアとなってスマートフォンをロックします。
3. **Hiddad** - 正規のアプリを再パッケージしてサードパーティ・アプリ・ストアで公開する Android マルウェアです。主な機能は広告の表示ですが、OS に組み込まれた重要なセキュリティ情報にアクセスできるため、機密性の高いユーザ・データを窃取されるおそれがあります。

チェック・ポイントの研究者は最も悪用されている脆弱性も調査しています。第 1 位は前月に引き続き世界の 48%の組織が影響を受ける CVE-2017-7269。これに 46%の OpenSSL TLS DTLS Heartbeat における情報漏洩が続いています。3 位は世界の 42%の組織が影響を受ける Web サーバの PHPMyAdmin の設定ミスに起因するコード・インジェクションです。

2018 年 10 月の脆弱性上位 3 種：

1. ↔ **Microsoft IIS WebDAV サービスの ScStoragePathFromUrl 関数のバッファ・オーバーフロー（CVE-2017-7269）** – Microsoft Internet Information Services 6.0 を使ってネットワーク経由で Microsoft Windows Server 2003 R2 に細工したリクエストを送信することにより、攻撃者がリモートから任意のコードを実行したり、ターゲットのサーバにサービス妨害攻撃を仕掛けたりできるようになります。これは HTTP リクエストの長いヘッダの検証不備に起因するバッファ・オーバーフローの脆弱性が主な原因です。2017 年 3 月からパッチが提供されています。
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. ↑ **Web サーバの PHPMyAdmin の設定ミスに起因するコード・インジェクション** – PHPMyAdmin に見つかったコード・インジェクションの脆弱性です。この脆弱性は、PHPMyAdmin の設定ミスに起因しています。リモートの攻撃者は、特別な細工を施した HTTP リクエストをターゲットに送りつけることで、この脆弱性を悪用できます。

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。

10 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、こちらをご覧ください。

本リリースは、米国時間 11 月 12 日に配信されたものの抄訳です。
英文オリジナルはこちら:
https://www.checkpoint.com/press/2018/october-2018s-most-wanted-malware-for-the-first-time-remote-access-trojan-reaches-global-threat-indexs-top-10/

■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》

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　横山
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: marketing_jp@checkpoint.com

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