2018 年 8 月 21 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、6 月の Global Threat Index を発表
バンキング型トロイの木馬の影響が 50%拡大
マルウェア・ファミリー上位 10 種にバンキング型トロイの木馬がランクイン、
マイニング・マルウェアも上位を維持

米カルフォルニア州 サン カルロス - 2018 年 7 月 5 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、2018 年 6 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、バンキング型トロイの木馬の世界的な影響が過去 4 か月で 50%拡大し、このタイプのマルウェア・ファミリー2 種が新たにランキングのトップテン入りしています。

機密情報の窃取とサービス妨害攻撃を目的とするバンキング型トロイの木馬 Dorkbot は、2018 年 6 月に全世界の 7%の組織に感染。この影響の拡大により、チェック・ポイントのマルウェア・ランキングで 8 位から 3 位にランクアップしました。最近では被害者の銀行口座情報を窃取し、感染したマシンを踏み台にしてさらに感染を広げるバンキング型トロイの木馬 Emotet の出現も確認されています。この新種は 4 月のランキングでは 50 位でしたが、2 か月の間に急速に感染が広がり、最新版では 11 位までランクアップしています。銀行口座の情報や FTP のパスワードを窃取するバンキング型トロイの木馬 Ramnit も、Dorkbot と揃ってトップ 10 入りしました。

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、「忘れがちなことですが、サイバー犯罪のほとんどは金銭の窃取を目的としています。ハッカーたちは手っ取り早く金銭を獲得するというシンプルな目標を達成するため、さまざまなツールを活用しています」と述べています。「2017 年夏にも、バンキング型トロイの木馬を利用した攻撃の活発化が確認されています。サイバー犯罪者はおそらく、セキュリティ意識が低くなりがちな休暇中の旅行者を狙っているのでしょう。そうした旅行者は共用端末や安全性の低い接続を使ってオンライン・バンキングを利用する可能性があるためです。こうした事実から、金銭の窃取を狙う悪質なハッカーというのは実に戦略的であり、執拗でもあることがわかります」。

またホロウィッツは、「バンキング型トロイの木馬やその他の攻撃による被害を防ぐには、既存のマルウェア・ファミリーによるサイバー攻撃と最新の脅威のどちらにも対応できる多層防御のサイバー・セキュリティ戦略が欠かせません」とも述べています。

2018 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。

1 ↔ **Coinhive**： このマイニング・マルウェアはユーザが Web ページを訪れたときに、通知や同意を得たりすることなく、そのユーザのコンピュータ・リソースを利用して仮想通貨 Monero の採掘を行います。ページに埋め込まれている JavaScript がエンド・ユーザのマシンの処理能力を大量消費してコインを採掘するため、システムがクラッシュする場合もあります。

2 ↔ **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・マルウェアです。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、ウェブサイトからの収入の一部を窃取します。

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。タイプとしてはバンキング型のトロイの木馬であり、機密情報の窃取とサービス妨害攻撃の遂行を主な目的としています。

企業のモバイルの利用環境を攻撃するために使われたマルウェアの中で一番多かったものは、スーパーユーザ権限を付与できる Android 向けのモジュール型バックドア Triada です。これに 2 位の Lokibot と 3 位の The Truth Spy が続いています。

2018 年 6 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する Android 向けのモジュール型バックドア。システムのプロセスにマルウェアが埋め込まれます。Triada は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 **TheTruthSpy**： iPhone と Android 搭載端末に対応したスパイウェアであり、WhatsApp のメッセージ、Facebook のチャット、Web ページの閲覧など、スマートフォンで行われるあらゆる活動を監視します。

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。1 位は世界の 40%の組織が影響を受ける CVE-2017-7269。これに 35%の CVE-2017-10271 が続いています。3 位は世界の 15%の組織が影響を受ける SQL インジェクションです。

2018 年 6 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ー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 ↔ **Oracle WebLogic のコンポーネント WLS Security のリモート・コード実行（CVE-2017-10271）**： Oracle WebLogic のコンポーネントである WLS Security にはリモート・コード実行の脆弱性があります。これは Oracle WebLogic による xml のデコードの処理方法に起因するものです。この攻撃が成功すると、リモートからコードが実行されてしまいます。2017 年 10 月からパッチが提供されています。

3 ↔ **SQL インジェクション**：アプリケーションのソフトウェアにあるセキュリティの脆弱性を悪用するもので、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 クエリを挿入します。

このランキングを見ると、最新のテクニック（2017 年に見つかった 2 つの脆弱性）に限らず、古典的な攻撃経路（SQL インジェクションなど）もしっかり使われていることがわかります。

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。

6 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、www.checkpoint.com/threat-prevention-resources/をご覧ください。

本リリースは、米国時間 7 月 5 日に配信されたものの抄訳です。
翻訳リリース本文はこちらをご確認ください。
https://www.checkpoint.co.jp/press/2018/pressrelease_20180821.html

■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しています。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保護するマルチレベルのセキュリティ・アーキテクチャに加え、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。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（ http://www.checkpoint.co.jp/ ）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　広報代行　共同ピーアール株式会社

担当　マーケティング　横山

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

担当　上瀧・花岡

Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

