ご参考資料（ブログ）
報道関係者各位

2018 年 9 月 27 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、2018 年 8 月のマルウェア・ランキング
バンキング型トロイの木馬による攻撃が急増
Ramnit による大規模キャンペーンの被害が拡大

チェック・ポイントの最新の Global Threat Index に基づく 8 月のマルウェア・ランキングでは、バンキング型トロイの木馬 Ramnit を利用した攻撃が急増していることが報告されています。2018 年 8 月の Threat Index では、Ramnit が第 6 位に急上昇しています。2018 年 6 月から、バンキング型トロイの木馬が倍増する中でも、Ramnit は最も検出数の多い存在となっています。

Ramnit のグローバルでの検出数は、この数か月間で倍増していますが、その背景には、感染マシンをプロキシ・サーバとして悪用する大規模キャンペーンの存在があります（詳細については、チェック・ポイントのリサーチ・ブログをご覧ください。）

手っ取り早く金銭的利益を得るためにバンキング型トロイの木馬を使う攻撃が夏に急増するのは、これで 2 年連続となります。偶然と思われるかもしれませんが、このような傾向は決して無視できません。ハッカーは、その時々でどのような攻撃が最も効果的かを正確に把握しているのです。つまり攻撃者は、夏の間のインターネット・ユーザの動向から、「この時期はこの攻撃手法が有効」と判断したと考えられるのです。この事実は、金銭的利益を狙うハッカーの執拗さ、巧妙さを明確に示しています。

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、有名なマルウェア・ファミリーの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必要不可欠です。

2018 年 8 月のマルウェア・ファミリー上位 10 種では、世界中の組織の 17%に影響を与えた Coinhive が前月に引き続き第 1 位となっています。第 2 位と第 3 位には、それぞれ 6%の組織に影響を与えた Dorkbot と Andromeda がランクインしています。

2018 年 8 月のマルウェア・ファミリー上位 10 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.↑ 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。

3.↑ Andromeda – 主にバックドアとして使用されるモジュール型のボットです。感染ホストに追加のマルウェアをダウンロードしますが、さまざまなタイプのボットネットを構築するように改変することも可能です。

4.↓ 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。

5.↔ 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。

6.↑ Ramnit – バンキング型トロイの木馬です。銀行の認証情報や FTP のパスワード、セッション cookie、個人情報を窃取します。

7.↔ XMRig – XMRig は、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。

8.↓ Roughted – 不正なインターネット広告キャンペーンを大規模展開する RoughTed は、各種の不正な Web サイトの構築やペイロード（詐欺ツール、アドウェア、エクスプロイト・キット、ランサムウェア）の配信に使用されています。標的のプラットフォームやオペレーティング・システムを問わずに使用できるほか、広告ブロッカーのバイパスやフィンガープリンティングによって、標的に最適な攻撃を実行します。

9.↓ 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。

10.↑ Nivdort – パスワードの収集、システム設定の改変、追加マルウェアのダウンロードなどに使用される多目的ボットです（別名 Bayrob）。通常はスパム・メール経由で拡散しますが、受信者のアドレスがバイナリにエンコードされているため、各ファイルは一意となっています。

組織のモバイル資産を狙った攻撃では、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 が最も多く検出され、次いで Lotoor、Triada という順になっています。

2018 年 8 月のモバイル・マルウェア上位 3 種：

1.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。

2.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。

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 を偽装する動作も確認されています。

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。その中で最も悪用件数が多かったのは CVE-2017-7269 で、世界の組織の 47%に影響を与えています。次いで 41%に影響を与えた「OpenSSL TLS DTLS Heartbeat における情報漏洩の脆弱性」、36%に影響を与えた CVE-2017-5638 という順になっています。

2018 年 8 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。

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.↑ D-Link DSL-2750B におけるリモート・コード実行 – D-Link DSL-2750B ルータにリモート・コード実行の脆弱性が見つかっています。脆弱性を悪用された場合、問題のデバイス上で任意のコードを実行されるおそれがあります。

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を観測、認識しています。

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、次の URL をご覧ください。
https://www.checkpoint.com/threat-prevention-resources/

本ブログは、米国時間 9 月 6 日に配信されたものの抄訳です。
本文はこちらをご覧ください。
https://blog.checkpoint.com/2018/09/11/augusts-most-wanted-malware-banking-trojan-attacks-turn-up-the-heat/

■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

