ご参考資料（ブログ）
報道関係者各位

2018 年 8 月 28 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 7 月のマルウェア・ランキング
IoT やネットワーク機器を狙う攻撃が 2018 年 5 月から倍増

米カルフォルニア州 サン カルロス - 2018 年 8 月 15 日

2018 年 5 月以降、Mirai および Reaper に関する脆弱性を狙った攻撃が倍増しており、7 月の脆弱性悪用ランキング上位 10 種では、IoT 関連の脆弱性が新たに 3 件ランクインしています。

2018 年 7 月は、脆弱性悪用ランキング上位 10 種に IoT 関連の脆弱性が新たに 3 件ランクインしました。MVPower DVR ルータにおけるリモート・コード実行の脆弱性が 5 位、D_Link DSL-2750B ルータにおけるリモート・コード実行の脆弱性が 7 位、Dasan GPON ルータにおける認証バイパスの脆弱性が 10 位です。このいずれかの脆弱性に対する攻撃を受けた組織の割合は、世界全体で 45%と、2018 年 6 月の 35%、2018 年 5 月の 21%から増加の一途を辿っています。これらの脆弱性を悪用すると、不正なコードを実行して標的のデバイスをリモートから制御できます。

サイバー犯罪者は、既知の脆弱性を悪用して難なく企業ネットワークに侵入し、さまざまな攻撃を仕掛けることができます。特に IoT 関連の脆弱性は、多くの場合、少ない労力で大きな成果を得ることが可能です。デバイスを 1 台侵害できれば、同じネットワークに接続する大量のデバイスにも容易に侵入できるからです。このため、IoT デバイスを運用する組織には、既知の脆弱性からネットワークを保護するため、公開されたパッチを速やかに適用することが求められます。

ただし、既知と未知の両方の脆弱性から組織を守るためには、既知のマルウェア・ファミリーによるサイバー攻撃とまったく新しい脅威の両者に対応できる多層防御のセキュリティ戦略が必要となります。
2018 年 7 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 19%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 7%の組織に影響を与えた Cryptoloot と Dorkbot がランクインしています。

2018 年 7 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. ↔ **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。
4. ↔ **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。
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. ↓ **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。
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. ↑ **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。
9. ↔ **Fireball** – フル機能のマルウェア・ダウンローダへと拡張可能なブラウザ・ハイジャッカーです。感染マシン上で任意のコードを実行できるため、認証情報の窃取から別のマルウェアのドロップまで、さまざまな活動を行うことができます。
10. ↔ **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。

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 Triada、Guerilla という順になっています。

2018 年 7 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. **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。
3. **Guerilla** – Android 向けの広告クリッカーで、リモートの指令（C&C）サーバと通信する、追加のプラグインをダウンロードする、ユーザに無断で勝手に広告をクリックするなどの機能を備えています。

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 42%に影響を与えた CVE-2017-5638、僅差で 41%に影響を与えた「OpenSSL TLS DTLS Heartbeat における情報漏洩の脆弱性」という順になっています。

2018 年 7 月の脆弱性上位 10 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。

2. ↑ **Apache Struts2 におけるコンテンツ・タイプを利用したリモート・コード実行（CVE-2017-5638）** – Jakarta マルチパート・パーサーを使用する Apache Struts2 に存在するリモート・コード実行の脆弱性です。攻撃者は、ファイル・アップロード・リクエストの一部として無効なコンテンツ・タイプを送信することで、この脆弱性を悪用できます。脆弱性を悪用された場合、問題のシステムで任意のコードを実行されるおそれがあります。

3. ↑ **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。

4. ↓ **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。

5. ↑ **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。

6. ↑ **PHP php-cgi におけるクエリ文字列パラメータによるコード実行（CVE-2012-1823、CVE-2012-2311、CVE-2012-2335、CVE-2012-2336、CVE-2013-4878）** – PHP にリモート・コード実行の脆弱性が見つかっています。この脆弱性は、PHP によるクエリ文字列の解析およびフィルタリングが不適切であることに起因しています。リモートの攻撃者は、細工を施した HTTP リクエストを送りつけることで、この脆弱性を悪用できます。脆弱性を悪用された場合、ターゲット上で任意のコードを実行されるおそれがあります。

7. ↔ **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。

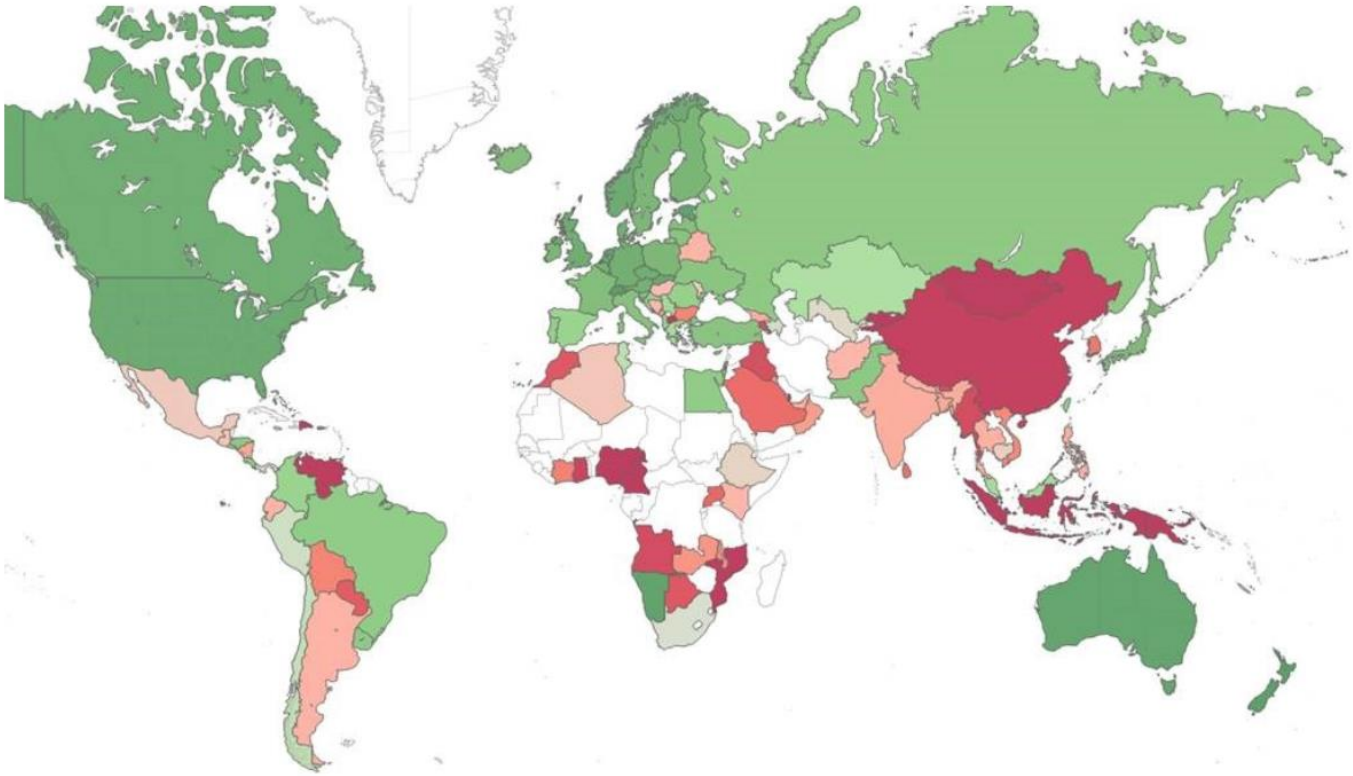
8. ↓ **Oracle WebLogic のコンポーネント WLS Security のリモート・コード実行（CVE-2017-10271）** – Oracle WebLogic のコンポーネントである WLS Security にはリモート・コード実行の脆弱性があります。これは Oracle WebLogic による xml のデコードの処理方法に起因するものです。この攻撃が成功した場合、リモートからコードを実行されるおそれがあります。

9. ↑ **OpenSSL tls_get_message_body 関数の init_msg 構造体における解放済みメモリ使用（CVE-2016-6309）** – OpenSSL の tls_get_message_body 関数に解放済みメモリ使用の脆弱性が見つかっています。認証を受けていないリモートの攻撃者は、特別な細工を施したメッセージを脆弱なサーバに送りつけることで、この脆弱性を悪用できます。脆弱性を悪用された場合、システム上で任意のコードを実行されるおそれがあります。

10. ↑ **Dasan GPON ルータにおける認証バイパス（CVE-2018-10561）** – Dasan GPON ルータには、認証バイパスの脆弱性が存在します。この脆弱性を悪用された場合、リモートから機密情報を窃取され、問

題のシステムに不正アクセスされる可能性があります。

次の地図は、世界各地のリスク指標を示しています（緑 - 低リスク、赤 - 高リスク、灰色 - データ不足）。特にリスクの高い地域やマルウェア感染が多数発生している地域を確認できます。



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 のセキュリティ情報です。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発見しています。

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 8 月 15 日に配信されたものの抄訳です。
米ブログ本文はこちらをご確認ください。
https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/
日本のブログ本文はこちらをご確認ください。
https://www.checkpoint.co.jp/threat-cloud/2018/08/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018.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

