プレスリリース
報道関係者各位

2019 年 5 月 22 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 4 月の Global Threat Index を発表
バンキング・マルウェアの「Trickbots」が久々のランクイン

多目的のバンキング型トロイの木馬 Trickbot が 2 年ぶりにマルウェア・ファミリー上位 10 種に登場

米カルフォルニア州サンカルロス ― 2019 年 5 月 14 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 4 月の『Global Threat Index（世界の脅威指標）』を発表しました。今月のランキングでは、バンキング型トロイの木馬 Trickbot が、約 2 年ぶりにトップ 10 への返り咲きを果たしています。

Trickbot に代表される多目的のバンキング型トロイの木馬は、金銭的利益を目的とするサイバー犯罪者の間で広く使用されてきました。Trickbot を使用したキャンペーンは 4 月に入って急増しており、間もなく期限を迎える米国の個人確定申告に便乗したスパム・キャンペーンが複数確認されています。これらのスパム・キャンペーンで拡散している電子メールには、感染先のコンピュータに Trickbot をダウンロードする Excel ファイルが添付されています。Trickbot はネットワーク全体に感染を広げ、銀行の口座情報を収集するほか、詐欺に利用できる税務書類の窃取を試みる場合もあります。

4 月のランキング・トップ 10 のうち、トップ 3 はマイニング・ツールでしたが、残り 7 つはすべて多目的型のトロイの木馬でした。この結果は、複数の主要マイニング・サービスの閉鎖やここ 1 年間における仮想通貨の価値下落に伴い、より大きな金銭的利益を見込める攻撃手法にサイバー犯罪者が移行している可能性を示しています。

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、「今月のランキングでは、Trickbot と Emotet の両方がトップ 10 入りを果たしました。この動きが懸念されるのは、両者共に個人情報や認証情報を窃取するだけでなく、Ryuk ランサムウェアを拡散するように進化を遂げているためです。Ryuk は、データベースやバックアップ・サーバなどのシステムのデータを暗号化して、最高で 100 万ドルを超える身代金を要求します。これらのマルウェアは常に進化を遂げているため、高度な脅威対策ソリューションを導入して、感染被害を防ぐ強固な防御体制を構築することが重要となります」と述べています。

2019 年 4 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. ↑ **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・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。元々は 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。
2. ↑ **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。
3. ↑ **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。

モバイル・マルウェア・ランキングでは、Hiddad に代わって Triada が第 1 位となりました。第 2 位は前月に引き続き Lootor が入り、Hiddad は第 3 位に順位を落としています。

2019 年 4 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 を偽装するタイプも確認されています。
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. **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、世界の 44%の組織に影響を与えた「OpenSSL TLS DTLS Heartbeat における情報漏洩」です。第 2 位は、1 年ぶりにトップから陥落した CVE-2017-7269、第 3 位は CVE-2017-5638 となっています。それぞれ、40%の組織、38%の組織に影響を与えています。

2019 年 4 月の脆弱性上位 3 種：

1. ↑ **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。
2. ↓ **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。
3. ↑ **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・パーサを使用する Apache Struts2 に見つかったリモート・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。

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。

4 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 5 月 14 日に配信されたものの抄訳です。

■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（ 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
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

（参考資料）

2019 年 5 月 22 日

チェック・ポイント、2019 年 4 月の Global Threat Index
日本国内のランキング

Find top 10 per country			
Malware_Family_Name	**Description**	**Global Impact**	**Japan Impact**
Babilon		0.56%	0.94%
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。	1.72%	0.82%
DeceptPCClean		0.27%	0.81%
Sality	感染マシンの遠隔操作とマルウェアの追加ダウンロードを可能にするウイルスです。主な目的は、感染マシンに常駐して、攻撃者による遠隔操作と別のマルウェアのインストールを可能にすることです。–感染マシンの遠隔操作とマルウェアの追加ダウンロードを可能にするウイルスです。主な目的は、感染マシンに常駐して、攻撃者による遠隔操作と別のマルウェアのインストールを可能にすることです。	1.87%	0.75%
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・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。元々は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。	5.49%	0.40%
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。	0.40%	0.29%
DLBoost		0.04%	0.28%
Sload		0.59%	0.24%
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。	4.08%	0.19%
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。	3.93%	0.15%