プレスリリース
報道関係者各位

2019 年 2 月 19 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 1 月の Global Threat Index を発表
深刻な新種脅威「SpeakUp」が出現

マイニング・ツールの XMRig を拡散する新たな Linux バックドア「SpeakUp」の検出数が急増

米カルフォルニア州サンカルロス ― 2019 年 2 月 13 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、2019 年 1 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、Linux サーバに感染し、マイニング・ツールの XMRig を拡散する新たなトロイの木馬が出現しています。SpeakUp と名付けられたこのマルウェアは、感染マシンに任意のペイロードをダウンロードして実行する機能を備えています。

SpeakUp は、現時点で全セキュリティ・ベンダーのアンチウイルス・ソフトウェアをすり抜けます。このトロイの木馬は、指令センターからの命令に従って一連の脆弱性（脆弱性悪用ランキング第 8 位の「HTTP 経由のコマンド・インジェクション」など）を悪用し、感染を広げています。チェック・ポイントの研究者は、あらゆるマルウェアのダウンロードと拡散に利用できる SpeakUp を深刻な脅威であると見ています。

2019 年 1 月のマルウェア・ファミリー上位 10 種では、1 位から 4 位までをマイニング・ツールが占めました。世界中の組織の 12%に影響を与えた Coinhive が引き続き第 1 位となっています。第 2 位には、8%の組織に影響を与えた XMRig が同じく前月に引き続きランクイン、第 3 位は、6%の組織に影響を与えた Cryptoloot となっています。1 月のランキングには、4 つのマイニング・ツールがランクインしていますが、トップ 10 のうち半数のマルウェアは、感染マシンに別のマルウェアをダウンロードする機能を備えています。

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、「1 月のランキングでは、世界中の組織を狙ったマルウェアの動向にほとんど変化がありません。しかしマルウェアの拡散手法に関しては、新たな方法が登場しつつあります。このような現象は、今後、より深刻な脅威が出現する前触れでもあります。SpeakUp のようなバックドアは、検出を免れたうえで、さらに危険性の高いマルウェアを感染マシンにダウンロードします。Linux は企業環境のサーバとして広く使用されているため、SpeakUp は今後さらに感染が増加し、深刻な被害をもたらすものと予想されます」と述べています。

2019 年 1 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. ↔ 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。

3. ↑ 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。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。

モバイル・マルウェア・ランキングでは、ダウンロードしたマルウェアに権限を付与する Android 向けのモジュール型バックドア Hiddad が、Triada に代わって第 1 位となりました。第 2 位には Lotoor がランクインし、Triada は第 3 位に順位を落としています。

2019 年 1 月のモバイル・マルウェア上位 3 種：

1. Hiddad： 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。
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 を偽装するタイプ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。第 1 位は、前月に引き続き、世界の 47%の組織に影響を与えた CVE-2017-7269 です。これに続いて、46%の組織に影響を与えた「Web サーバ上の Git リポジトリにおける情報漏洩」、45%の組織に影響した「OpenSSL TLS DTLS Heartbeat における情報漏洩」がそれぞれ僅差で第 2 位、第 3 位となっています。

2019 年 1 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. ↑ Web サーバ上の Git リポジトリにおける情報漏洩 – Git リポジトリに見つかった情報漏洩の脆弱性です。この脆弱性を悪用された場合、アカウント情報が意図せず漏洩する可能性があります。
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。

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。

1 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 2 月 13 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　横山
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

