プレスリリース
報道関係各位

2019 年 6 月 17 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 5 月の Global Threat Index を発表
脆弱性「BlueKeep」の修正パッチの速やかな適用を呼びかけ

チェック・ポイントの研究者が、RDP の脆弱性「BlueKeep」をスキャンする複数の試みを世界規模で確認。
攻撃に備えた偵察活動の可能性

米カルフォルニア州サンカルロス ― 2019 年 6 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）の脅威情報部門である Check Point Research は本日、2019 年 5 月の『Global Threat Index（世界の脅威指標）』を発表しました。リサーチ・チームは、世界中の組織に対し、Microsoft の Windows 7 および Windows Server 2008 に発見された RDP の脆弱性「BlueKeep」（CVE-2019-0708）の影響を受けるシステムがないかどうかを早急に確認し、必要に応じてパッチを適用するように呼びかけています。修正しない場合、同脆弱性を悪用したランサムウェア攻撃やマイニング攻撃を受けるおそれがあります。

この脆弱性「BlueKeep」は、インターネットに直接接続された 100 万台近くのマシンに影響しますが、組織の内部ネットワークにはそれよりも多くの該当マシンが存在しています。同脆弱性が特に深刻であるのは、ユーザの介在なしで悪用できる点です。RDP は、すでに攻撃経路としてポピュラーな存在になっており、Samsam や Dharma などのマルウェアのインストールにも悪用されています。チェック・ポイントのリサーチ・チームは、この脆弱性の有無の確認を目的とした多数のスキャンが数か国から行われている事実を確認しています。このスキャンは、攻撃前の偵察活動として実行されている可能性があります。Microsoft は、すでに修正パッチを公開していますが、チェック・ポイントでも、ネットワーク向けとエンドポイント向けの保護機能を提供しています。

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、「BlueKeep は、5 月に出現した中で最も深刻な脅威です。この脆弱性を悪用する攻撃はまだ確認されていませんが、コンセプト実証を目的としたエクスプロイトはすでに複数開発されおり、攻撃対象を探す多数のスキャンが確認されています。Microsoft やサイバー・セキュリティ分野の有識者は、BlueKeep が悪用された場合、2017 年に発生した WannaCry や NotPetya による大規模攻撃キャンペーンに匹敵する規模のサイバー攻撃が発生する可能性があるとしていますが、私たちも同意見です。脆弱性の影響を受けるコンピュータがネットワークに 1 台でも存在していた場合、そのコンピュータが不正なペイロードの媒介となり、ネットワーク全体に感染が広がる可能性があります。そして、感染したコンピュータがインターネットに接続していた場合、世界中のコンピュータに感染が広がりかねません。感染は指数関数的に拡大し、それを止めることは極めて困難になるでしょう。自らの組織、そして他の組織を守るため、手遅れになる前に今すぐパッチを適用する必要があります」と述べています。

5 月に発生したその他の重大なマルウェア関連ニュースとしては、Ransomware-as-a-Service のアフィリエイト・プログラム「GandCrab」の開発元が、5 月 31 日に活動停止を発表したことが挙げられます。開発元は、プログラム利用者に対し、20 日以内にランサムウェアの配布を停止するよう求めています。同ランサムウェアの活動は 2018 年 1 月に始まり、それからわずか 2 か月で 5 万件以上の感染被害を出しました。開発元やプログラム利用者が得た収益は、数十億ドル

に上ると言われています。Global Threat Index の常連だった Gandcrab は頻繁にアップデートされており、検出を回避する新たな機能が次々と追加されていました。

2019 年 5 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。
今月のマルウェア・ランキングは、三大マイニング・ツールである Cryptoloot、XMRig、Jsecoin が引き続き上位を独占し、それぞれ世界の 4%の組織に影響を与えています。

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。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。

2019 年 5 月のモバイル・マルウェア上位 3 種：
モバイル・マルウェア・ランキングでは、4 月の第 2 位からランクアップした Lotoor が第 1 位となりました。第 1 位だった Triada は第 3 位にランクダウンし、第 3 位だった Hiddad が第 2 位にランクアップしています。

1. ↑ **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。
2. ↑ **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。
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。

2019 年 5 月の脆弱性上位 3 種：
5 月の脆弱性ランキングでは、比較的古い攻撃手法がカムバックを果たし、世界の 49%の組織に影響を与えた SQL インジェクション手法が第 1 位となりました（この動きには、マイニング・ツールの収益性低下が影響していると考えられます）。これに続いて、44%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」、41%の組織に影響した「OpenSSL TLS DTLS Heartbeat における情報漏洩」がそれぞれ第 2 位、第 3 位となっています。

1. ↑ **SQL インジェクション（複数の手法）**： 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、アプリケーションのソフトウェアに存在する脆弱性を悪用します。
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。

5 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。
https://blog.checkpoint.com/2019/06/13/may-2019-most-wanted-malware-bluekeep-microsoft-rdp-cryptocurrency-malware/

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 6 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》

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