2018 年 6 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、サッカー・ワールドカップ人気に便乗した フィッシング・キャンペーンを確認

試合の日程や結果チェックのツールをダウンロードさせ、マルウェアに感染させる新たな攻撃が発生

カルフォルニア州 サン カルロス - 2018 年 6 月 18 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、先ごろ開幕したサッカーのFIFA ワールドカップに便乗するフィッシング・キャンペーンを発見したと発表しました。このキャンペーンでは、試合の日程や結果をチェックするツールをダウンロードさせ、マルウェアに感染させるという手口が用いられています。

フィッシング・メールに添付されたファイルを開くと、好ましくないプログラム（PUP）をダウンロードする既知のダウンローダ「DownloaderGuide」の亜種が実行されます。このダウンローダは、ツールバーやアドウェア、システム最適化ユーティリティなどのアプリケーションのインストーラとして広く使用されています。チェック・ポイントの研究者が確認したところによると、このキャンペーンでは、合計 9 種類の実行可能ファイルが使用されており、**「World_Cup_2018_Schedule_and_Scoresheet_V1.86_CB-DL-Manager」という件名の電子メールで送信**されています。

このキャンペーンは、2018 年 5 月 30 日に初めて観測され、6 月 5 日に最初のピークを迎えました。ただし、大会が開幕した先週から再び勢いを増し、新たな攻撃の発生が確認されています。

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、「大きな関心を集める一大イベントは、サイバー犯罪者にとって、新たなキャンペーンを展開する絶好の機会です。ワールドカップを巡ってさまざまな情報が行き交うこの時期、サイバー犯罪者は、メールや添付ファイルの開封に対するユーザの警戒心が緩むことを期待しています。このため企業では、攻撃による被害を防ぐためのベスト・プラクティスを改めて社員に周知する取り組みが重要となります」と述べています。

「あわせて、メール・ボックスに届く前の時点でフィッシング・メールをブロックする対策も大切です。例えば、既知のマルウェア・ファミリーによるサイバー攻撃と未知の脅威による攻撃の両方を阻止すると同時に、侵入を許した場合に備えて、ネットワーク内での感染拡大を防ぐことのできる、多層防御のセキュリティ戦略を導入する必要があります」（ホロウィッツ）

チェック・ポイントでは、1 か月にわたるワールドカップ期間中、さらに多くのオンライン詐欺やフィッシング攻撃が発生すると予測しています。この間、個人ユーザに対しては、サイバー攻撃から身を守る次の対策の実施を改めて推奨します。

■このサイバー攻撃で特に注意すべきこと

- **ソフトウェアを最新の状態に維持する** - PC をはじめとする各種デバイスのオペレーティング・システム、セキュリティ・ソフトウェア、アプリケーション、Web ブラウザをすべて最新のバージョンに更新します。これは、マルウェアやウイルスなど、オンラインの脅威に対する効果的な対策となります。
- **偽の Web サイトに注意する** - 過去に大きなイベントが開催されたときには、グッズ販売サイトやニュース・サイト、ライブ・ストリーミング・サイトなど、本物に見せかけたありとあらゆる偽サイトや偽ドメインが出現しました。このようなサイトは、マルウェアの配布や訪問者の機密情報の窃取に利用されます。
- **心当たりのない差出人からの電子メールに注意する** - サイバー犯罪者は、ワールドカップの大会期間中、抽選でチケットが当たるなどの内容の、さまざまなフィッシング・メールを送りつけてくると予想されます。このような攻撃では、ハイパーリンクや添付ファイルを介して、マルウェアをダウンロードさせたり、個人情報を窃取したりしようと試みます。心当たりのない差出人からの電子メールや添付ファイルは、開かないように心がけるのが効果的な対策となります。
- **Wi-Fi ホットスポットの使用に注意する** - ワールドカップでは 1 日を通して試合が行われるため、外出先で Wi-Fi ホットスポットに接続し、モバイル・デバイスで試合を観戦しようとする人も多数に上ると予想できます。しかし、セキュリティが不十分なホットスポットは、ハッカーの格好の標的でもあります。ホットスポットが乗っ取られていた場合、電子メールやパスワードなどの個人情報を盗み見られたり、マルウェアをインストールされる可能性があります。

本リリースは、米国時間 6 月 18 日に配信されたものの抄訳です。

リリース本文はこちらをご確認ください。

■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

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

