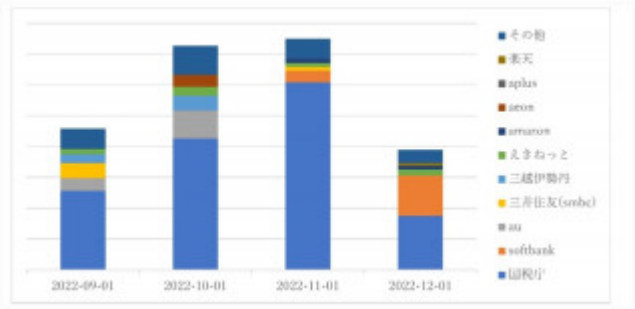
TwoFive、「フィッシングトレンド」レポート最新版を発表 2022年9月～12月 調査結果



2023年2月27日

急増したソフトバンクのフィッシングと国税庁のフィッシングは同一犯の可能性も
中国系フィッシング攻撃者は「.cn」を使わず別のTLDに移行
ドメインのブラックリスト登録回避のため同一ホストで複数ドメインを割り当てる傾向

メッセージングセキュリティのリーディングカンパニーである株式会社TwoFive（本社：東京都中央区、代表取締役 末政 延浩）は、「フィッシングトレンド」レポートの2022年9月～12月版を発表しました。
同レポートは、SSL証明書発行情報、ドメイン登録情報、ソーシャル情報、マルウェアなど複数のデータソースから独自のアルゴリズムにより、国内のフィッシングサイトについて多角的に独自に調査し、メッセージングセキュリティの専門ベンダーとして長年培った経験に基づく知見により分析・判定して検知した結果をまとめたもので定期的に公開しています。

※本文中の図(グラフ)は、以下でご覧ください
https://www.twofive25.com/news/20230227_securityreport.html

◆ 国税庁のフィッシンググループが、標的をソフトバンクに変更

前回の調査（2022年6月～8月）で、国税庁のフィッシングサイトで使われたダイナミックDNSサービスは「duckdns.org」で、8月中旬から下旬にかけて件数が増加しました。
今回の調査期間で、この「duckdns.org」を使ったフィッシングの攻撃ブランド（図1）では、11月～12月にかけて、国税庁が減り、ソフトバンクが増加しています。
日単位で動きをとらえてみると、ソフトバンクを騙るフィッシングサイトが検出されている期間が、国税庁を騙るフィッシングサイト数が落ち着いている期間と一致し、フィッシングの成果を検証しているかのような動きが見られることから、国税庁をターゲットとした攻撃者が、攻撃対象をソフトバンクに切り替えた可能性が考えられます。

◆ フィッシングに悪用されたブランド

前回の調査結果（2022年6月 ～8月）に引き続き、国税庁のe-Tax
を騙るフィッシングサイトは11月まで増加し続けて大量に検出されましたが、12月は11月の1/3以下に減少しました。
携帯キャリア系を騙るフィッシングサイトで多く検出されたのは、9月～10月がauブランドを狙ったもの、11月～12月はソフトバンクユーザーを狙ったフィッシングサイトでした。
クレジット・信販系では、全体的にサイト数は少ないですが三井住友（SMBC）カード、VISAカード、イオンカード、アメックスカードなどを狙ったフィッシングサイトが各月で検出されました。

◆ フィッシングに利用されているTLD （duckdns.orgを除く）

中国のカントリーコードTLD （ccTLD）である「.cn」を利用するフィッシングサイトは、前回（2022年6月 ～8月の合計）は全体の54%と最も多く検出されていましたが、今回（2022年9月 ～12月の合計）は19%と減少傾向にあります。
しかしながら、「.cn」以外を利用するフィッシングサイトの本文やHTMLコメント内の一部に、中国語が混じっている例が依然として多く散見され、中国系のフィッシング攻撃数が減少しているのではなく、警戒されがちな「.cn」ではなく、別のTLDに変えたと考えられます。

国税庁、ソフトバンクのフィッシングサイトで使われている「duckdns.org」以外の状況をみると（図3）、「.cn」のフィッシングサイトが減った一方で、特定の領域・分野ごとに割り当てられるGeneric TLD
（gTLD）である「.com」と「.shop」を利用するフィッシングサイトが増加傾向にあります。gTLDでは他にも「.top」や「.xyz」や「.club」などのドメインが多く見られます。
全体的に、ccTLDよりgTLDを利用するドメインの比率が上がってきています。

◆ フィッシングに利用されているホスティング事業者

前回の調査結果（2022年6月
～8月）で全体の半数近くを占めていたQuadranet.comの利用が減っている一方で、DediPathを利用したフィッシングサイトが増え、半数以上を占めています。
9月～10月にはColoCrossingを利用したフィッシングサイト、11月にはSun Network Company Limitedを利用したフィッシングサイトが見られました。
何れも米国のホスティング事業者ですが、料金が安価であることに加えて、利用に際しての審査が甘く、支払い方法において足が付かないホスティングサービスが狙われているのではないかと考えられます。
数は少ないですが、Google
CloudやAWS等のメジャーなクラウド・ホスティング事業者を利用したフィッシングサイトも検知されています。

◆ フィッシングに利用されたIP数とドメイン数

フィッシングサイトでは、ドメインのブラックリスト登録を回避するために、同一IPアドレスに対して複数のドメインを割り当てる傾向にあります。今回の集計期間では、1つのIPアドレスに対して平均16個のドメインが割り当てられていました。
「duckdns.org」を使って、国税庁、ソフトバンクを標的にしたフィッシングサイトでも、1つのI

Pで複数ドメインを運用していると考えられます。

◆ フィッシングに利用されている証明書

フィッシングサイトに利用されている証明書は、99.8%がLet’s Encryptにて取得されたものです。
数は少ないですが、cPanelやTrustAsia Technologies、Sectigoなどで取得されたものも見られました。
証明書内のSubject Alternative Name（SAN）の数は1件、2件のものが85%以上を占めますが、50件又は100件のものも5%くらいあり、ドメインごとに証明書を取るものと大量のドメインに同一の証明書を使用する２パターンがある傾向が見られ、大量に取得する場合は機械的に取得していると想定され、切りの良い50又は100件が選ばれるようです。

◆ TwoFiveの「フィッシングトレンド」調査について

SSL証明書発行情報、ドメイン登録情報、ソーシャル情報、マルウェアなど複数のデータソースから独自のアルゴリズムにより、国内のフィッシングサイトについて多角的に独自に調査しています。
TwoFiveもメンバーであるフィッシング対策協議会が定期的に発表する報告件数に基づく「フィッシング報告状況」とは、件数、内容などが異なります。
また、攻撃者は、IDの盗用やクレジットカードを不正利用するために、メールやSMSで詐欺メッセージを配信しフィッシングキャンペーンを実行する前に、予備調査により詐取方法や対象を検討して、ドメイン確保やDNS設定、Webサーバー構築やフィッシングコンテンツの設定、SSL証明書やドメインなどのリソースを準備します。TwoFiveの調査では、フィッシングキャンペーンの実行前の準備段階を含めて情報を収集し、メッセージングセキュリティの専門ベンダーとして長年培った経験に基づく知見により分析・判定して検知するのが特長です。

■株式会社TwoFiveについて

https://www.twofive25.com/
株式会社TwoFiveは、大手ISP、ASP、携帯事業者の電子メールシステムインフラで長年経験をつんだメールシステムの技術者集団により2014年に設立されました。日本の電子メール環境を向上させることを使命としてベンダーニュートラルな立場で最適な技術とサービスを組み合わせ、メールシステムの設計・構築、電子セキュリティなどについてコンサルティング、ならびに各種レピュテーションデータを提供しています。

Generated by ぷれりりプレスリリース
https://www.prerele.com