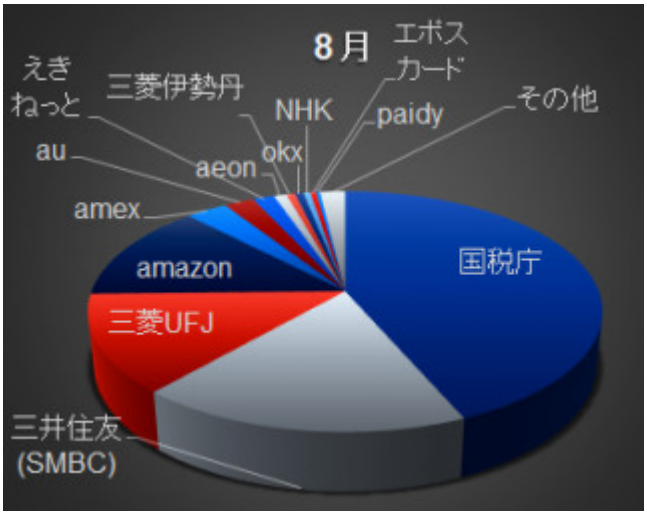
TwoFive、2022年6月～8月「フィッシングトレンド」を発表
フィッシングキャンペーン前のリソース準備段階のフィッシングサイトURLも検出



2022年10月5日

中国のカントリーコードTLD「.cn」に次いでフィッシングでの悪用が多い「.org」の大半は、国税庁のフィッシングサイトで使われた無料取得可能な「duckdns.org」

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、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調査を行っており、この度、2022年6月 ～8月の結果を「フィッシングトレンド」として発表しました。
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。
TwoFiveでは、今後も調査を継続して、定期的に「フィッシングトレンド」を発表してまいります。

※以下の結果をグラフでご覧いただけます。
https://www.twofive25.com/news/20221005_securityreport.html

● フィッシングに悪用されたブランド

クレジット、信販系では、三井住友(SMBC)カードの検出が多く、セゾンカード、ビューカードも検出されています。
ECサイトではAmazonの検出が多く、ヨドバシ・ドット・コムや楽天市場も検出されています。
携帯キャリアではauが多く検出されています。
主要ブランドは常に狙われていますが、攻撃対象は時期により変化していることがわかります。
また、8月には国税庁のe-Taxを語るフィッシングサイトが多数検出されました。
米国などではよくみられるフィッシングですが、日本ではやや珍しいと思えます。

● フィッシングに利用されているホスティング事業者

6月～8月を通して、Quadranet.com（米）を利用したフィッシングサイトの検出が最も多く、その他の事業者も、概して審査が甘く、安価なホスティングサービスが利用されやすい傾向にあります。
しかしながら、Google Cloud Platformを利用したサイトも少数ですが検出されています。

● フィッシングに利用されているTLD （Top Level Domain）

(6月～8月の合計)
中国のカントリーコードTLDである「.cn」が54%と最も多く検出されています。マルウェアを解析すると中国語が多いことからも、フィッシング攻撃者は中国系の比率が多いと推測されます。
特定の領域・分野ごとに割り当てられるgTLD（Generic
TLD）では、「.com」「.shop」「.top」「.ingo」「.net」などのメジャーなTLDが利用されています。

2番目に多く検出されたTLDは「.org」で、15%。このTLDは大半が「duckdns.org」でした。
「duckdns.org」は、Duck
DNSという無料のダイナミックDNSサービスを利用することで提供されますが、duckdns.orgのサブドメインを無料で取得できるためフィッシングサイトに利用されることが多いといえます。
国税庁をかたるフィッシングサイトでも、この「duckdns.org」が使われており、8月中旬から下旬にかけて件数が増加しました。

● フィッシングの検出時間帯（6月～8月の合計）

フィッシングサイトは、24時間まんべんなく作られていますが、深夜（22～24時）、および明け方（5～6時）の検知が多くなっています。検知を避けるために、この時間帯に作成されているのではないかと推測されます。
報告ベースの結果では、日中の発生が多いので深夜・明け方に作成して、日中に配布しているものが多いようです。

● フィッシング検出からソーシャルによる報告までの時間差

TwoFiveの調査で検出されたフィッシングが、実際にソーシャルで報告されるまでの時間差を見ると、検出から6時間以内に報告されるものが多く、長いものでは、検出から20日以上経って報告されるものもありました。

フィッシングサイトによってはサイト作成後ある程度時間が経ってから配布するものもあるようです。

● フィッシングに利用されている証明書

無料で作成できるSSL証明書の「Let's Encrypt」が最も多く使用されていました。
証明書内に別ドメインを記述できるSANs（Subject Alternative Names）は1件から数件が大半を占めますが、最大100件のものも検出され、接続先は同一になっているものが多く検出されました。攻撃者によっては、１つの証明書に複数のSANsで複数のドメインを登録して、それら全てを同じIPアドレスに紐づけることにより対象URLを変えるパターンも見られました。

■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