2024 年 8 月 27 日
デジタルアーツ株式会社

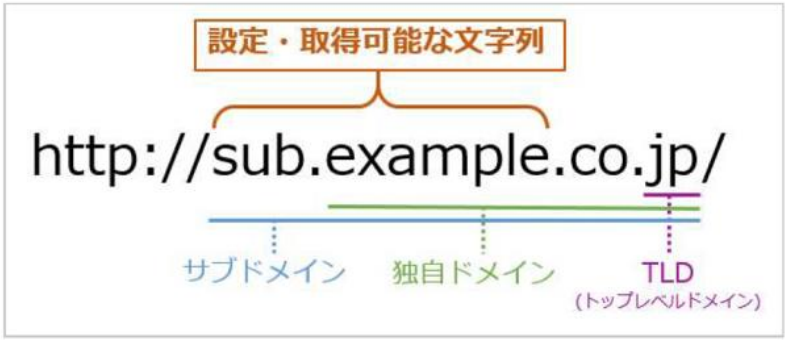
PRESS RELEASE

【セキュリティレポート】
2024 年上半期フィッシングサイトのドメインを独自に分析
低価格または無料で購入できるドメイン「.xyz」を悪用した攻撃が増加

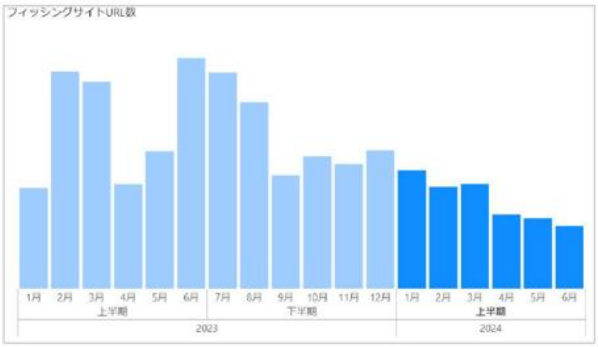
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、2024 年上半期に収集した国内外のフィッシングサイト URL のドメインを集計したレポートを公開したことを発表します。

URL 総数は下半期比約 4 割減、新たに TLD「.ly」「.cc」「.ci」の 3 つがランクイン

デジタルアーツでは、日々様々な Web サイトについて調査・収集を行っています。今回、デジタルアーツは、2024 年上半期(1 月～6 月)に確認した国内外のフィッシングサイト URL のドメインを集計しました(IP アドレス形式の URL は除く)。なお、本レポートで扱うドメインについては【図 1】のように定義しています。2024 年上半期のフィッシングサイト URL 総数は、2023 年下半期と比較すると約 4 割減という結果になりました。また、月別でみると 1 月が最多となり、3 月に再度増加しましたが 6 月にかけて徐々に減少しました。



【図1】ドメインについて



【図2】フィッシングサイトURL数

2024 年上半期のフィッシングサイト TLD(トップレベルドメイン)トップ 20 を集計した結果、「.com」が 36.91%と 2023 年下半期に比べシェアが減少したものの依然として首位に立っています。また、1 月の観測が最も多く、シェア全体の 8.77%を占めていることがわかりました。続いて、2 位が「.cn」の 12.12%、3 位が「.dev」の 8.77%という結果になり、順位が逆転しました。2023 年下半期に 8 位だった「.xyz」は、今期 4.76%増により 5 位にランクアップし、緩やかに増加しました。

他の TLD においては、新たに「.ly」「.cc」「.ci」の 3 つがランクインしました。「.ly」は「cutt.ly」という短縮 URL サービスで 9 割以上を占めていることがわかり、フィッシングサイトへの誘導を目的に悪用されていると推測できます。「.ci」も 9 割以上が「asso.si」という独自ドメインで占めており、**「hxxp://(4 桁の数字).(7 文字のランダム文字列).asso.si/」**といった形式のフィッシングサイト URL が多く見受けられました。また、「.cc」はオーストラリア領ココス(キーリング)諸島の ccTLD(国別コードトップレベルドメイン)であり、フィッシング詐欺で利用されやすい要因には、比較的低格価で簡単に取得できることや、登録・利用に関する規制が緩いことに加え、特定の国・地域に限定されないことから不正利用を目的とした登録が行いやすいという点が挙げられます。

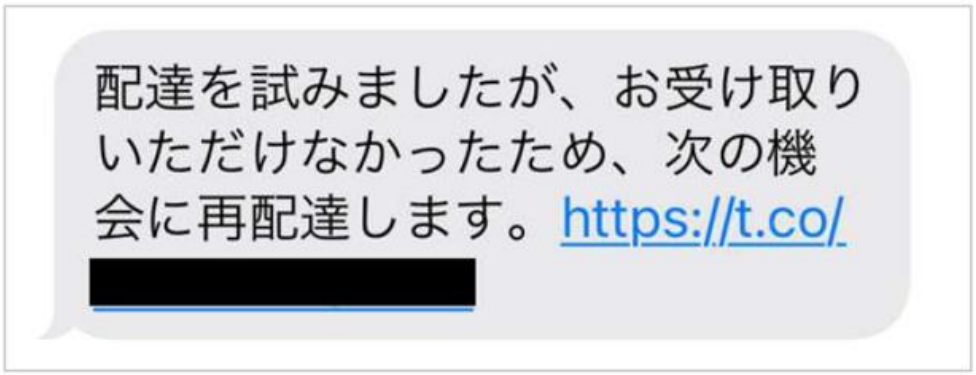
2024年上半期 フィッシングサイトTLDトップ20　※右表は昨年下半期

順位	TLD	シェア	順位	TLD	シェア
1	com	36.91%	1	com	44.99%
2	cn	12.12%	2	dev	7.26%
3	dev	8.77%	3	cn	5.28%
4	top	7.18%	4	app	3.78%
5	xyz	6.95%	5	io	3.24%
6	jp	4.11%	6	top	2.94%
7	io	2.69%	7	id	2.90%
8	id	2.23%	8	xyz	2.19%
9	org	1.95%	9	cfd	2.09%
10	app	1.86%	10	net	1.93%
11	net	1.67%	11	co	1.88%
12	me	1.33%	12	me	1.31%
13	shop	1.29%	13	org	1.18%
14	ly	1.07%	14	site	1.10%
15	ru	0.63%	15	pl	1.10%
16	site	0.52%	16	icu	0.99%
17	pl	0.47%	17	shop	0.92%
18	info	0.46%	18	ru	0.88%
19	cc	0.37%	19	info	0.81%
20	ci	0.35%	20	jp	0.78%

【図3】2024年上半期 フィッシングサイト TLDトップ20

今期 4.76%増した TLD「.xyz」の悪用方法に注目　宅配便を装った SMS に使用されるパターンが多い傾向に

「.xyz」を利用した独自ドメインは、「tbdym.xyz」「ppsed.xyz」「oqcey.xyz」「ibasv.xyz」の 5 つが突出して多く、これらには様々なサブドメインが利用されています。「.xyz」は、比較的低価格あるいは無料で取得できる TLD であることから、攻撃者はドメインを多数取得し、使い捨てていると考えられます。実際にこれらの独自ドメインは宅配便を装った SMS で使用されているパターンで見受けられ、「お客様がご不在で、荷物を一時的に持ち帰りました。こちらから詳細をご覧ください。」などの文面に加え、フィッシングサイトへの誘導先に X(旧 Twitter)の短縮 URL サービス「t.co」を経由して利用されていることを確認しました。



【図4】宅配便を装ったSMS例

フィッシング攻撃者は、多様な手法や規模でユーザーをフィッシングサイトに誘導しようと試みています。特に、短期間で使い捨てられるドメインや URL を利用したフィッシングサイトは、ブラックリストによる検出が難しいため、個別にリスト登録したとしても、いたちごっことなります。TLD やドメイン、一般的な文字列が変化するのと同様に、模倣されるブランドや攻撃手法も進化しており、フィッシング攻撃は依然として組織や個人に対する重大な脅威です。そのため、新たな攻撃手法に関する情報収集とセキュリティ対策がより一層重要になります。

2024 年上半期フィッシングサイト ドメイン集計のレポートはこちら
以下、弊社コーポレートサイト上にて公開しております。
https://www.daj.jp/security_reports/41/

◆デジタルアーツでは
▸受信したすべてのメールを開け、アクセスしたい Web をクリックできる。情報システム部門の運用負荷も削減できる。デジタルアーツの「ホワイト運用」がセキュアな世界を実現します。

「i-FILTER」
デジタルアーツでは日々様々な情報をもとにデータの収集を行っています。「i-FILTER」Ver.10 では、フィッシングサイト URL はフィルターデータベースへと迅速に配信され、[フィッシング詐欺]や[迷惑メールリンク]や[違法ソフト・反社会行為]カテゴリにてブロックが可能です。さらに、Web サービス制御機能においても、サービスごとの制御が可能です。

▸安全な Web セキュリティの新定番「ホワイト運用」とは
フィルターデータベースに反映されていない URL についても「ホワイト運用」を行うことで、デジタルアーツが安全を確認した URL にのみアクセスを許可し未知のフィッシングサイトや悪性 URL をブロックすることができます。

▸クレデンシャルプロテクション
「クレデンシャルプロテクション」機能では、正規のサイトと判別が困難な改ざんサイトに設置されたフィッシングサイトであっても、ユーザーが ID・パスワードを送信しようとした際にこれをブロックすることが可能です。

「m-FILTER」
「m-FILTER」は、送信元や添付ファイルの拡張子、メール本文中に含まれる URL の偽装判定などが行えるメールセキュリティ製品です。

▸「脅威 URL ブロック」オプション（※）
「i-FILTER」をお持ちでなくても「脅威 URL ブロック」オプションをご利用いただくことで、メールの本文と添付ファイル内の URL を、デジタルアーツが運用しているクラウド上のデータベースに問い合わせます。もしも危険な URL が記載されている場合は、メールをブロックします。
※本オプションは「i-FILTER」をお持ちでないユーザー様に向けた機能となります。
※インターネット接続が必要となります。オフライン環境ではご利用いただけませんのでご注意ください。

デジタルアーツ株式会社 概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、情報漏えい対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する最先端の製品を、企業・官公庁・学校・家庭向けに提供しています。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー14F ▸URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社 広報課 関・宮内 TEL : 03-5220-1670/ E-mail : press@daj.co.jp