上半期レポート（2012 年 1 月 ～ 2012 年 6 月）

Global Phishing Survey:

Trends and Domain Name Use in 2012 年上半期

日本語版

本翻訳文書は、フィッシング対策協議会が、原書の著作権を保有する米国 APWG : Anti-Phishing Working Group の許諾を得て翻訳したものです。

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありませんので、必要に応じて APWG のホームページより原書"Global Phishing Survey: Trends and Domain Name Use in 1H2012" をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の APWG のホームページをご参照ください。
http://www.antiphishing.org/

目次

【Overview】概要

2012 年上半期に起きたフィッシングから、サイバー犯罪（e-crime: イークライム）には国境が無いことを再認識させられました。フィッシング攻撃は、国境を越えて国内外に対して行われました。大規模な攻撃を行う踏み台として、サーバに対してハッキングも行われました。また、様々なオンラインサービスを標的とし、適切な防御策を有していないサービスが不正利用されました。

本レポートは、フィッシングの傾向と深刻さを理解し、世界で起きているフィッシングの問題を定量化しました。また、本レポートでは、2012 年上半期（"2012 年上半期", 2012 年 1 月 1 日から 2012 年 6 月 30 日まで）に観測されたフィッシング攻撃を分析しています。データは、Anti－Phishing Working Group が収集したものに加え、他のフィードからのフィッシングデータや CNNIC、民間の情報源から集めたデータを使用しました。APWG が持つデータのリポジトリは、インターネット上において最も多くのフィッシングや E-mail 詐欺に関するはデータを有しています。

本レポートの主な成果は：

１．**2012 年上半期 のフィッシング攻撃の平均稼働時間は、2008 年に観測を始めて以来最短でした**(6 ページ)

２．**フィッシング攻撃の数が増加しました**（4-5 ページ）

３．**フィッシングを行う攻撃者は、通常のドメイン名よりサブドメイン名を多く登録しました。**（16 ページ）**また、ドメイン登録数は、2011 年初期に比べ半分になりました**（12-13 ページ）

４．**標的となる組織の数が減少しました；標的となる組織は大規模な組織や以前から標的となっている組織でした**（5 ページ）

５．**中国にある組織を標的とした悪意あるドメイン登録数は、世界中の 2/3 を占めました**（12 ページ）**レジストラは、中国内外のものを使用していますが、.CN のドメイン名を使用していません**（15 ページ）

６．**南アメリカドメイン名を保有しているウェブサーバに対するフィッシング攻撃が増加しました**（11 ページ）

【Basic Statistics】 統計データの概要

数百万件ものフィッシング URL が 2012 年上半期に報告されましたが、特定のフィッシング攻撃の数および攻撃をホストするドメイン名の数は、報告された URL の数よりも少ないことが判明しました。[1] 2012 上半期 で収集されたデータから以下の統計データを得ました：

－ **202 個の Top-level domain （TLD）で起きた特定のフィッシング攻撃の数は、最低でも 93,462 個ありました。**この数は、2011 年下半期に観測された 83,083 個を上回りました。この上昇は、複数のドメインに対し同時に攻撃を行うため、共有された仮想サーバを踏み台にしたフィッシング攻撃が増えたことに起因しています。"攻撃"は特定のブランドまたは団体を標的にしたフィッシングサイトと定義しています。例として、一つのドメイン名を使って、複数の銀行に対し、それぞれ固有の攻撃を仕掛けることが可能な事が挙げられます。

－ **観測された攻撃では、64,204 個の固有のドメイン名が使用されました。**[2] この数字も 2011 年下半期に観測された 50,298 個から増加し、世界にあるドメイン名の数は、2011 年 11 月時点の 226,500,000 個から 2012 年 5 月の 240,000,000 個に増えました。[3]

－ また、**2,410 個の攻撃は、1864 個の固有のドメイン名ではなく、IP アドレスから観測されました。**(例：http://79.173.233.18/paypal/.) IP アドレスを使用する攻撃の数はここ 2 年間でそれほど変動がありません。IPv6 アドレスを使用した攻撃はありませんでした。

－ 64,204 個のフィッシングドメインのうち、**7,712 個のドメインが悪意あるドメインとして登録されたものであると判断しました。**この数は、2011 年下半期の 12,895 個および 2011 年上半期の 14,650 個から大幅に減少しました。5,117 個（66%）は中国の標的を攻撃するために登録され、この数字も 2011 年下半期の 7,991 個から減少しました。残りの 56,492 個のドメインはウェブホスティングにおける脆弱性を使用してハッキングが行われたものが多かったです。

－ **フィッシング攻撃は、主に top-level domain で分散されていますが、悪意あるドメ**

---

1 これには、複数の要因があります：A) フィッシングの中には、カスタマイズされた攻撃で、ユニークな数字を URL に挿入することで、被害者をトラッキングしたり、スパムフィルタを通過したりするためのものがあります。一つのフィッシング攻撃が数千個の URL から一つのフィッシングサイトへ誘導されるものがあります。すべての URL を含めることで、数が水増しされます。本レポートだけでなく、我々が出すすべてのレポートでは数え方が統一されており、固有の攻撃をカウントするために重複したものを省いています。B) 攻撃者は、一つのドメイン名を使い、複数の標的に対して同時に攻撃を行うことがあります。攻撃者によって、登録したそれぞれのドメイン名に複数の異なるフィッシング攻撃を仕掛けることもあります。C) フィッシングサイトは複数のページを持つこともあり、それぞれが報告されるケースもあります。

2 ″ドメイン名″は second-level ドメイン名およびそのレジストリが提供していれば、 third-level ドメイン名を含めて定義しています。例として .CN（中国）のレジストリで、second-level 登録と third-level 登録（com.cn, gov.cn, zj.cn などのゾーンに対する）を提供しているものがあります。ただし、これらの数字が特定の TLD 内で実際に起きた攻撃の数より少ないケースがあることを ″サブドメインサービスを使用したフィッシング Subdomains Used for Phishing″ の項を読み、確認してください。

3 この調査では、ICANN.org の gTLD 数および ccTLD レジストリ管理者から提供されたデータをもとにしています。

イン登録の 90% は 3 つの TLD で行われました: .TK、.COM、.IN

－ 標的となった組織は 486 個で、2011 年下半期の 487 個とほぼ同じ数でしたが、2010 年下半期に観測された 587 個からは大幅に減少しています。標的は、銀行、e-commerce サイト、ソーシャルネットワーキングサービス、ISP、政府の主税局、オンラインゲームのサイト、郵便サービス、証券会社などの組織を含みます。

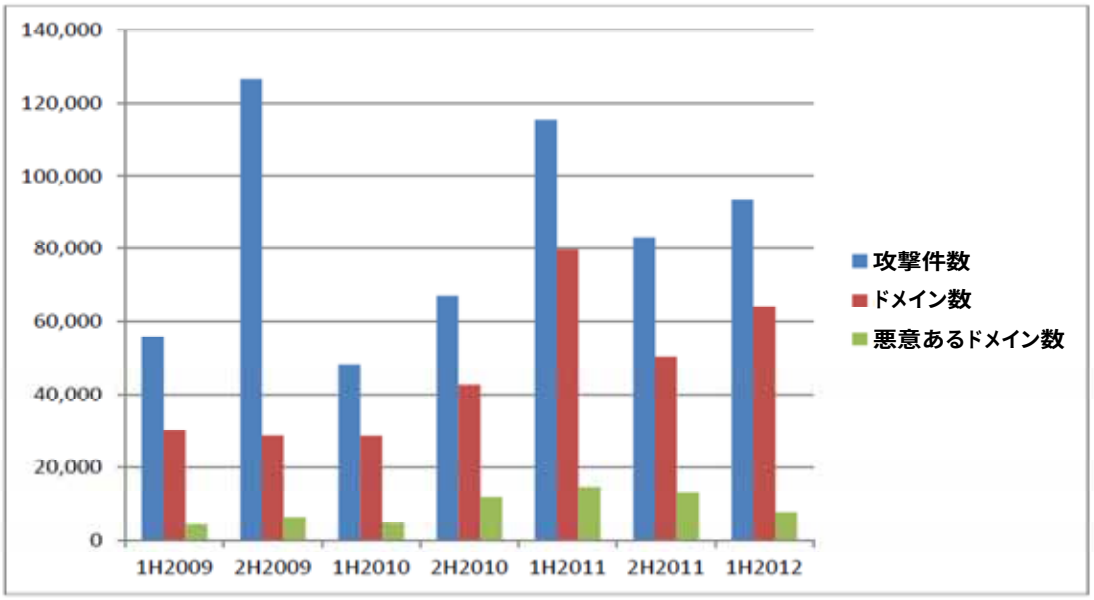
－ フィッシングで使用されたドメイン名のうち 2% がブランド名またはブランド名を変形させたものが使用されました（【Compromised Domains vs. Malicious Registrations】ハッキングされたドメイン vs 悪意ある登録 － を参照）

－ 64,204 個のドメインのうち、58 個が国際化ドメイン名（internationalized domain name - IDN）でした。尚、一つの地域のみを攻撃したものはありませんでした。

統計データ

	2012年上半期	2011年下半期	2011年上半期	2010年下半期	2010年上半期
フィッシング ドメイン名	64,204	50,298	79,753	42,624	28,646
攻撃件数	93,462	83,083	115,472	67,677	48,244
使用された TLD 数	202	200	200	183	177
IP によるフィッシングの件数 (固有 IP)	1,864	1,681	2,385	2,318	2,018
登録された悪意あるドメイン数	7,712	12,895	14,650	11,769	4,755
IDN ドメイン数	58	36	33	10	10
標的の数	486	487	520	587	568

攻撃者から標的とされる組織の数が減少し、大規模でかつ有名な組織に標的が絞られました。この傾向は、小さな組織を攻撃することによる金銭的な利益があまり無いからと考えます。攻撃者からすれば、有名な組織に関連する認証情報を売ることは容易です。また、スパムメールを送信するために Gmail, Hotmail, Yahoo! などのホワイトリストされているサービスの E-mail アカウント情報を取得する活動が増えています。



中国に存在する組織を標的とする攻撃は依然としてありますが、2011 年後半に比べ減少しています。中国の e-commerce サイトである Taobao.com が、攻撃件数が最も多いサイトから第 2 位になり、2012 年上半期 では、Paypal が再び攻撃件数の多いサイトとなりました。データを共有していただいた CNNIC および APAC に感謝申し上げます。

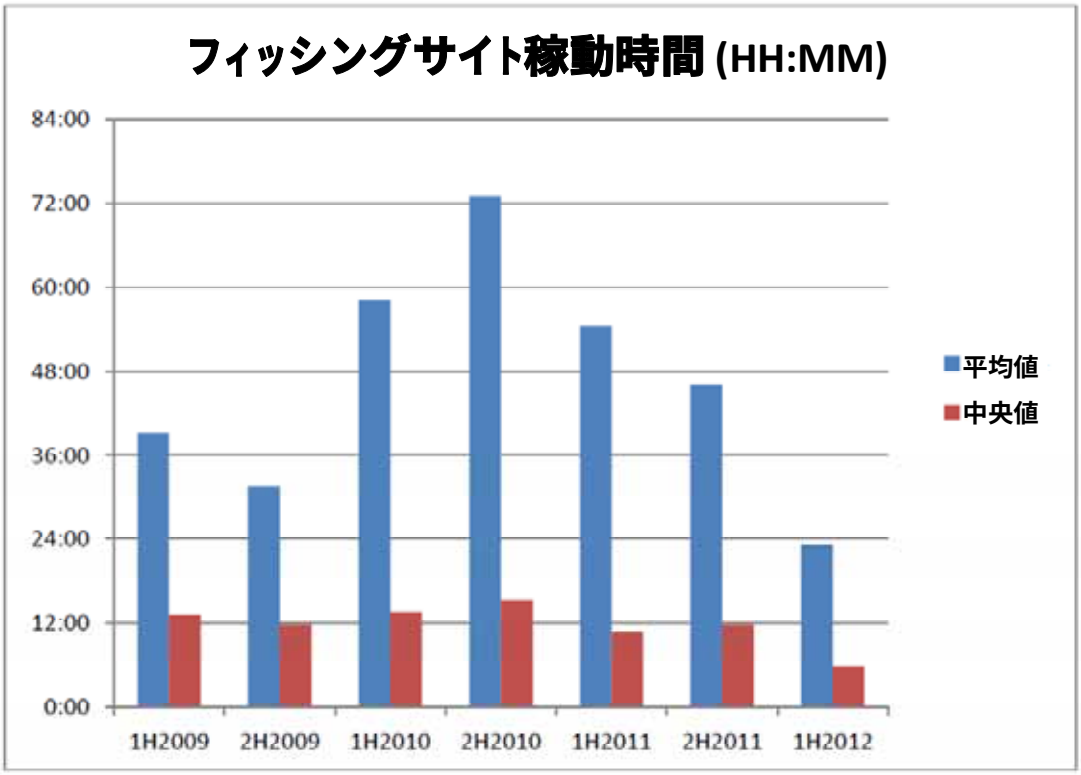
【Phishing by Uptime】稼働時間によるフィッシング

2012 年上半期 のフィッシング攻撃の平均稼働時間は、2008 年に観測を始めて以来最短でした。2012 年上半期 の平均稼働時間は、23 時間 10 分で、2012 年下半期 は 46 時間 3 分、最大値は、2010 年下期 の 73 時間でした。2012 年上半期 の中央値は、2012 年上半期 で 5 時間 45 分と、2012 年下半期 に観測された中央値の 11 時間 43 分の半分以下でした。

フィッシング攻撃における "稼働時間" または "活動している" 時間[4] は攻撃による損害を計るための重要な指針であると同時に対応がどのくらい成功したかの指針でもあります。フィッシング攻撃が稼動している時間が長ければ長いほど、標的となった組織および被害

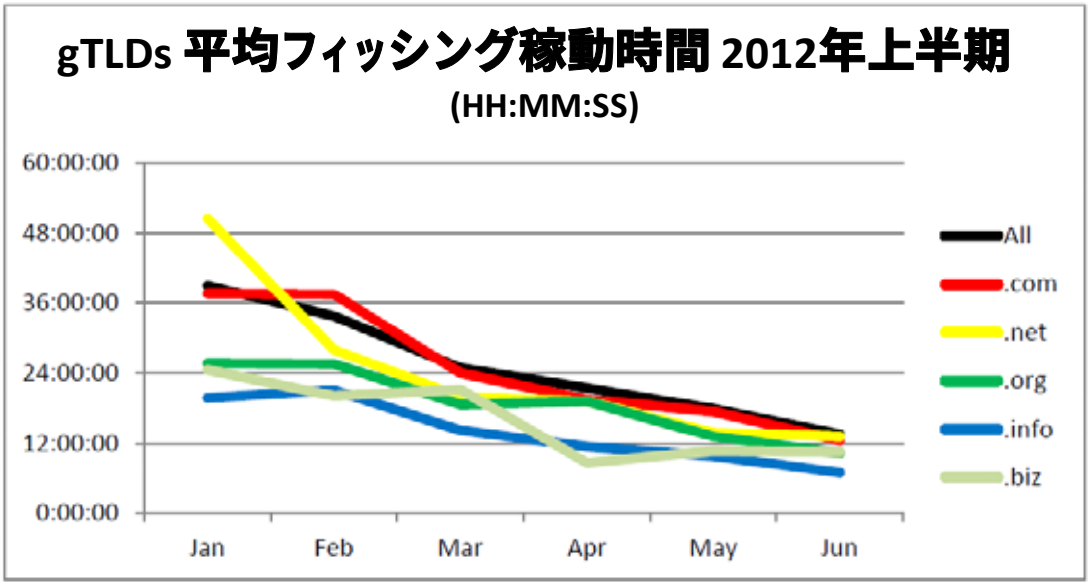
[4] 稼働時間を測定するためのシステムは、フィードまたはハニーポット経由でフィッシングが行われていることを確認次第、監視を自動的に開始します。それぞれのフィッシングサイトは一時間で数回確認され、″down″ されたと判定するには、一時間以上 ″down″ していることを確認する必要があります。(この要件はサイトによって、ボットネット上でホストされていることにより、毎回解決されることは無いが、サイトは生きていることがあるために採用された) この測定方法は、フィッシングサイトの稼働時間を実際の稼働時間より短く観測することがあります。その理由として、10%以上のサイトは、一時間 down した後に再稼動することがあるためです。ただし、インシデント間の比較や相対比較を行うための測定方法としては一貫性があります。

者の損害額が増えます。

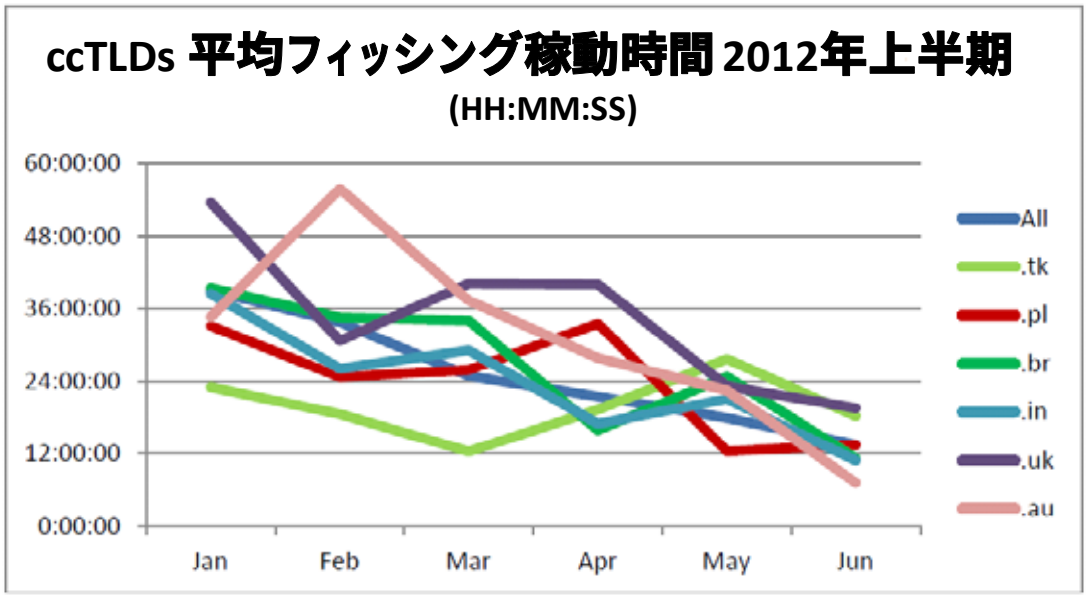


攻撃者にとって、攻撃を行う最初の２日間が最も金銭的な利益を得ることができるため、素早いテイクダウンが必須です。数週間や数ヶ月に渡る期間稼動している攻撃は、平均値に悪影響を及ぼすことがあるため、中央値の方が対応活動がいかに有効であったかを計る指標として使われます。ただし、CNNIC は、稼働時間を観測していなかったため、我々の稼働時間の統計には含まれていません。

大規模な gTLD の中では、.INFO、.BIZ と .ORG は稼動時間が最も短く、理由としてはレジストリ管理者の対応体制が確立されていることにあります:



6 月までに仮想サーバへのハッキング件数が上昇したことにより、gTLD 上での攻撃稼働時間が減少しました。仮想サーバに対する攻撃への対応は効率がよくーホスティングプロバイダへのクレームの上昇およびそれぞれの対応が複数のフィッシング攻撃をテイクダウンしました。大規模な ccTLD 上での攻撃稼動時間は様々でした：



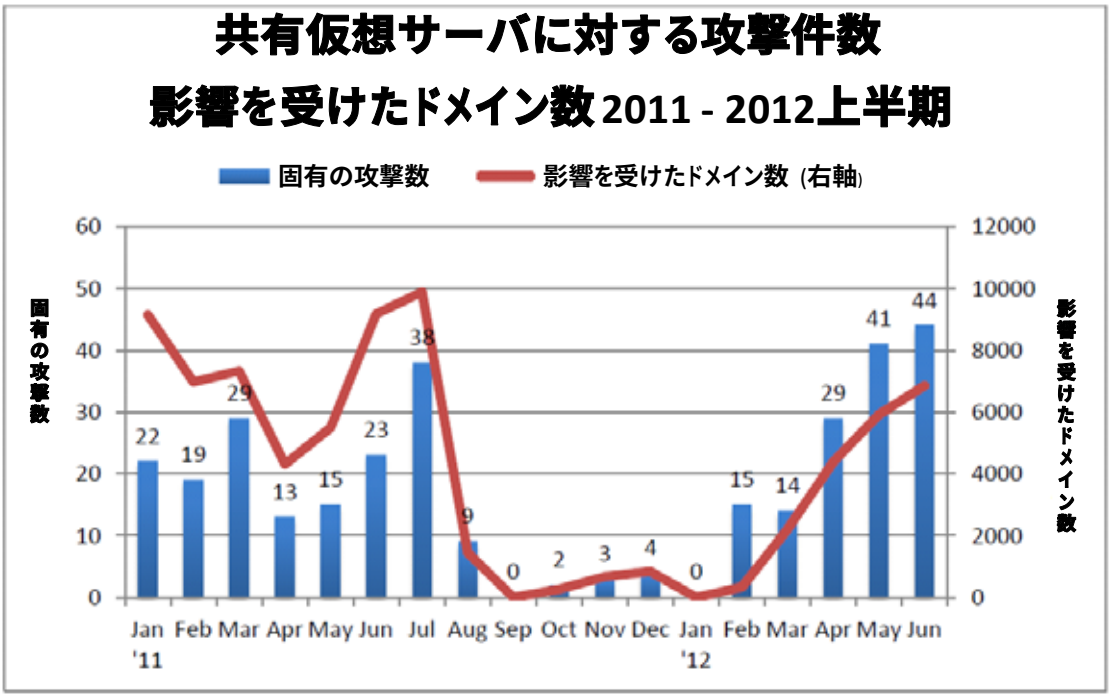
すべての top-level-domain における稼働時間につきましては、付録を確認してください。

【Attack Methods: Rise of Shared Virtual Server Hacking】攻撃手法： 仮想

サーバに対するハッキングが増加

2011 年上期 に始めて解説した傾向で、攻撃者が使用した特定の攻撃手法が、我々の統計データに大きな影響を与えました。この手法では、攻撃者は多数のドメインを管理するウェブサーバに侵入することを一業界内では"共有仮想サーバ"と呼んでいます。攻撃者はサーバへの侵入が成功すると、フィッシングコンテンツをアップロードします。その後、ウェブサーバの設定を変更し、そのコンテンツをウェブサーバ内に存在する「すべて」のホスト名に加えます。この変更により、サーバ内に存在するサイトが、細工されたディレクトリを作成し、フィッシングサイトを表示するようになります。

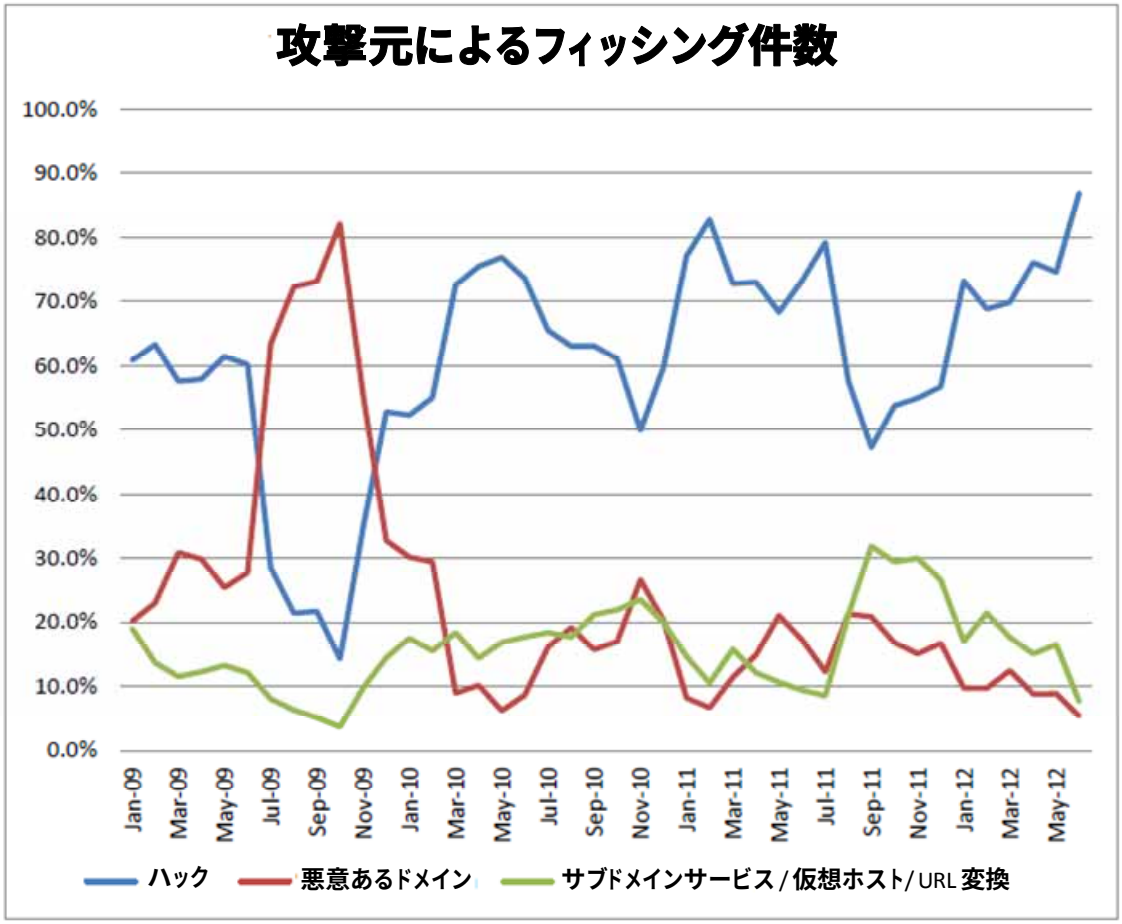
一つ一つのサイトをハッキングするのではなく、サーバによって、数百、数千のサイトを同時に攻撃することが可能です。2011 年上期 では、この手法を使った攻撃と特定できたもので 40,000 件を超えました。しかし、2011 年 7 月以降は、この手法を使った攻撃は激減し、2012 年 1 月には、1 件もありませんでした。2012 年 2 月に再び見られるようになり、2012 年 6 月には、44 個のサーバに対し、7,000 件の攻撃が観測されました。



-- 過去を振り返って　A Historical Retrospective --

このレポートを数年に渡り公表してきたことで、フィッシング攻撃の手法やリソースの傾向を分析できるようになりました。下のグラフでは、ドメインハッキング、悪意あるドメイン登録および共有された仮想ホストとサブドメインを使用したそれぞれの攻撃件数が占

める割合を記しています：



2009 年に悪意あるドメイン登録が多かったのは、Avalanche phishing gang によるものでした。一般的な攻撃者はサーバハッキングを使用することが多く、攻撃者が直接管理可能なリソース、例えばドメイン名などを使用することが減っている傾向があります。主な理由として reputation service が素早くドメインおよびサブドメインをブロックしている、ドメインレジストラやレジストリサービスによる悪意あるドメインへの対応強化、攻撃者は自動化スクリプトやサービスを使い、既知の脆弱性を抱えるウェブサーバを攻撃するようになったこと、WordPress や Joomla などの攻撃可能なウェブサービスが増えてきたことが挙げられます。

この目まぐるしい変化は、フィッシング対策を行うコミュニティが常に変化する状況に対応していかなければならないことを表しています。我々は今後もこのような攻撃を監視していく予定ですが、アンダーグランドで活動する一部のフィッシング団体が共有ウェブホスティングのプロバイダを狙っている為、特に注意が必要です。

【Prevalence of Phishing by Top-Leve Domain (TLD)】Top-Level Domain によるフィッシングのまん延

フィッシングドメインと攻撃を分析し、TLD 内でどのように分散されているのかを確認しました。依然として、大半のフィッシングは、数個の namespace の中で起きました。攻撃が頻繁に行われた .PL と .TK ドメインを除き、他のドメインは市場シェアに基づき攻撃頻度が分散されていました。**付録にある表にすべての数字が掲載されています。**

TLD 内でどの程度、フィッシングがまん延しているかをより正確に計るために、"10,000 ドメインあたりの"、"10,000 件ごとのフィッシング攻撃[5]" をそれぞれ計算し、測定しました。"10,000 個ごとのフィッシングドメイン"は、TLD 内でフィッシングに使われたドメインの数を同じ TLD 内で登録されたドメインの数で割ったものを割合（スコア）として算出したものです。この数値を使って、その TLD が他の TLD と比べてフィッシングがどのくらい発生しているかを確認します。

"10.00 件ごとのフィッシング攻撃"は、namespace 内でどの程度、フィッシングがまん延しているかを確認するための数値として有効です。サブドメインサービスを使用する攻撃者が主にどの TLD を不正利用しているか、また、一つのドメイン内で多くの攻撃が仕掛けられているドメインを確認することができます。

付録にある表にすべての数字が掲載されており、それぞれの TLD における測定値とフィッシング件数が含まれています。

－ **"10,000 ドメインあたりの" の中央値は、4.0 でした**

－ **世界で最も大規模な TLD、.COM の "10,000 ドメインあたりの" の値は、3.0 でした。**我々が収集したデータの中において、.COM は、48% のフィッシングドメインおよび 44% のドメインを有していました。

上記から、"10,000 ドメインあたりの" の数値が、.COM の 3.0 と 中央値である 4.0 の間を"中"程度と判断し、4.0 以上の TLD を、フィッシングが広くまん延していると判断しました。[6]

---

[5] スコア ＝（フィッシングドメインの数 / TLD 内のドメインの数）X 10,000

[6] 統計データに関して：

－ 小規模な TLD において、少数のフィッシング件数が大きな影響を与え、スコアを上昇させます。これにより、中央値が上昇します。TLD が大規模であればあるほど、1 件のフィッシングがスコアに与える影響は少ないです。

－ レジストリのスコアは、一人の攻撃者が多数の攻撃を仕掛ける場合、またはレジストラの不注意によ

下の表には、大きいスコアであった TLD を順番に掲載しています。

ドメインスコアが高い TLD、2012 年上半期

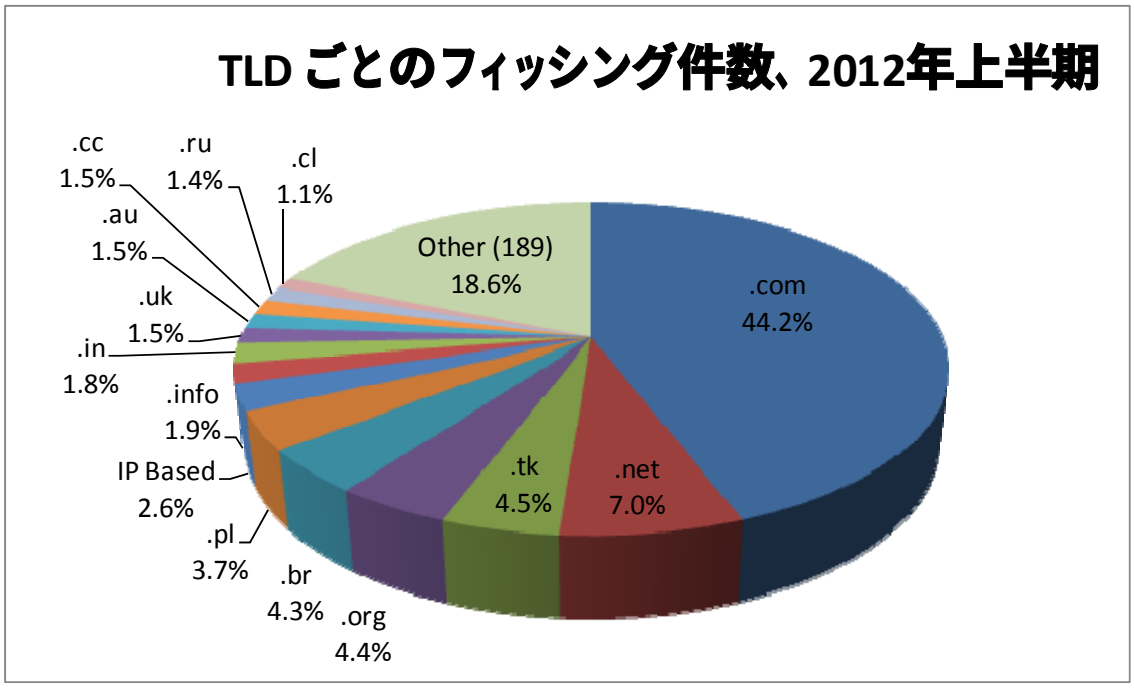
最低 25 個のフィッシングドメインおよびレジストリ内には最低 30,000 個のドメイン

順位	TLD	TLD 地域	2012年上半期 のフィッシング件数	2012年上半期 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 2011年下半期の10,000ドメインごとの攻撃件数
1	cl	Chile	1,024	831	383,100	21.7
2	pe	Peru	126	115	61,530	18.7
3	id	Indonesia	113	95	78,000	12.2
4	th	Thailand	122	77	69,490	11.1
5	br	Brazil	4,039	3,207	2,959,495	10.8
6	ec	Ecuador	36	31	30,001	10.3
7	ro	Romania	967	533	576,323	9.2
8	za	South Africa	764	644	779,500	8.3
9	in	India	1,690	1,351	1,674,552	8.1
10	uy	Uruguay	35	29	36,908	7.9

南アメリカのドメインにあるサーバが多数の攻撃を受けました。特に .CL ドメインが多数の攻撃を受け、2012 年下半期 のスコアが 7.2 だったのに対し、2012 年上半期 では 21.7 にまで上昇しました。ccTLD のうち、.PL (ペルー)、.BR (ブラジル)、.EC (エクアドル) と .UY (ウルグアイ) がドメインハッキングの被害を受けました。また、ここ数年もスコアが高いタイの .TH もスコアが高く、主に政府や大学などのウェブサーバが被害にあいました。

って上昇することがあります。

– TLD のスコアに影響を与えるその他の要因につきましては、過去のレポートにある "Factors Affecting Phishing Scores" を確認してください。



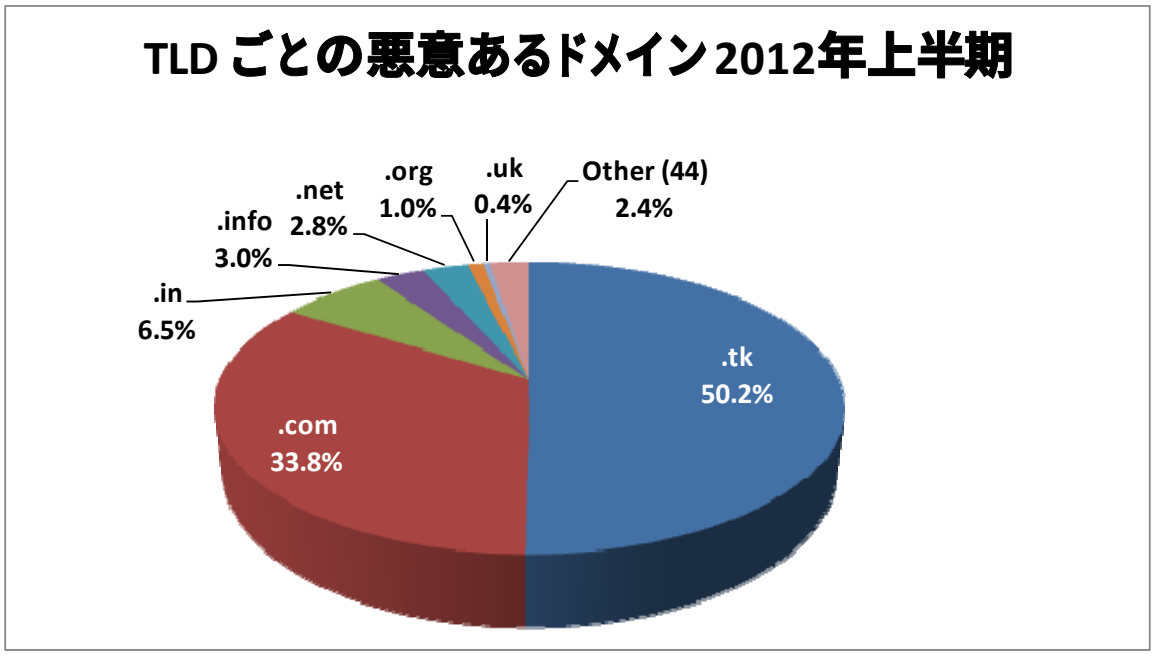
インドの .IN TLD が 2012 年下半期 時点で 2 位だったのが、9 位になりました。2012 年下半期 で .IN ドメインを使用した攻撃の半数以上が、ゲーミングサイト Battle.net のユーザを標的にしたものでした。2012 年上半期 では、.IN ドメインは 91 個の異なる標的がほぼ均等に攻撃されました。

【Compromised Domains vs. Malicious Registrations】ハッキングされたドメイン vs 悪意ある登録

攻撃者によって登録されたドメインの数と、ハッキングされたドメインで起きたフィッシングの数を比較し、分析しました。この分類は、インシデントレスポンスをする側から見て対応する手法が違うため、また攻撃者がどのようにして犯罪を犯しているかの実態が垣間見える為重要です。ドメインは登録されてから間もなくフィッシングドメインとして登録されたブランド名や、紛らわしい文字列を含む場合、またはまとめて登録された、あるいは登録方法に何らかの意図があり、一つの管理者に結びつけられた場合において悪意があると判断しました。

64,204 個のフィッシングドメインのうち、**7,712 個のドメインを攻撃者によって登録された悪意あるドメインと判定しました。**この数字は、2012 年下半期 の 12,895 個および 2011 上半期 の 14,650 個から大幅に減少しています。その他の 56,492 個のドメインのほとんどがハッキングされた、または脆弱なウェブホスト上にあり、被害を受けました。

登録された 7,712 個のドメインのうち、5,117 個（66%）のドメインは、中国にある標的を攻撃するために登録されました。この数字は、2012 年下半期 の 7,991 個から減少しました。中国を攻撃する者は、フィッシングのためにドメイン登録を続けており、ドメインをハッキングすることはほとんどありません。



悪意あるドメイン登録の半数が .TK TLD 内でありました。悪意あるドメイン登録数の 90% が 3 つの TLD 内でありました： .TK、.COM、.IN。

.TK ドメインは無料で配布されており、.TK のレジストリは、信頼あるパートナーに対し、フィッシングなどに不正利用されているドメインを停止するための API を提供しています。(これらのパートナーに、Facebook、Internet Identity、Anti-Phishing Alliance of China が含まれています) .TK のドメインを使用した攻撃で最も標的となったのは Taobao.com であり、中国を標的にする攻撃者が .TK ドメインを登録することを好んでいることが分かります。

その他の攻撃者は、TLD より防御が薄い、登録料が安い、または無料のサブドメインサービスに目をつけました。

登録された悪意あるドメインのうち、1,350 個がブランド名またはブランド名を変形させ

たもの（主にスペルの違い）が含まれていました[7]。この数字は、2012 年下半期 に観測された 2,232 より大幅に減りました。**この数字は期間内で観測されたフィッシングドメインのうち 2% を占めており、悪意あるドメインの登録数においては、17% を占めました。**

登録された悪意あるドメインの文字列には、被害者となるユーザを惑わすものは含まれていません。ドメイン名の中にブランド名またはブランド名を変形させたものを入れるのは手法として好まれていません。なぜなら、ブランド所有者は、これらの名前をインターネットゾーンのファイルから積極的に探しているからです。過去にも観測されましたが、**攻撃者にとってドメイン名はあまり関係なく、意味ある・無いに関わらず、どこかの TLD にあるドメインで良いのです。その代わり、攻撃者はブランド名をサブドメインまたはサブディレクトリに配置します。**これにより紛らわしい文字列を URL 内に存在させることで、被害者となるユーザがそれを閲覧し、騙されることがあります。一般的にインターネットのユーザは URL から"どの"ドメイン名が使用されているかを判断することができません。

【Registrars Used for Malicious Domain Registrations】悪意あるドメイン登録のために使われるレジストラ

本レポートでは、攻撃者がドメイン名を買うために使用したレジストラの分析を続けています。この分析は、ドメインが登録されてすぐに DomainTools.com からキャプチャした WHOIS データをもとに行われました。DomainTools の協力のおかげで、そこからのデータがフィッシングのために登録された 7,712 個の gTLD および ccTLD ドメインのうち、7,354 個（95%）のドメインを網羅できました。攻撃者は様々なレジストラを使って 2012 年上半期 に悪意あるドメインを取得しており、140 以上のレジストラが関与していました。

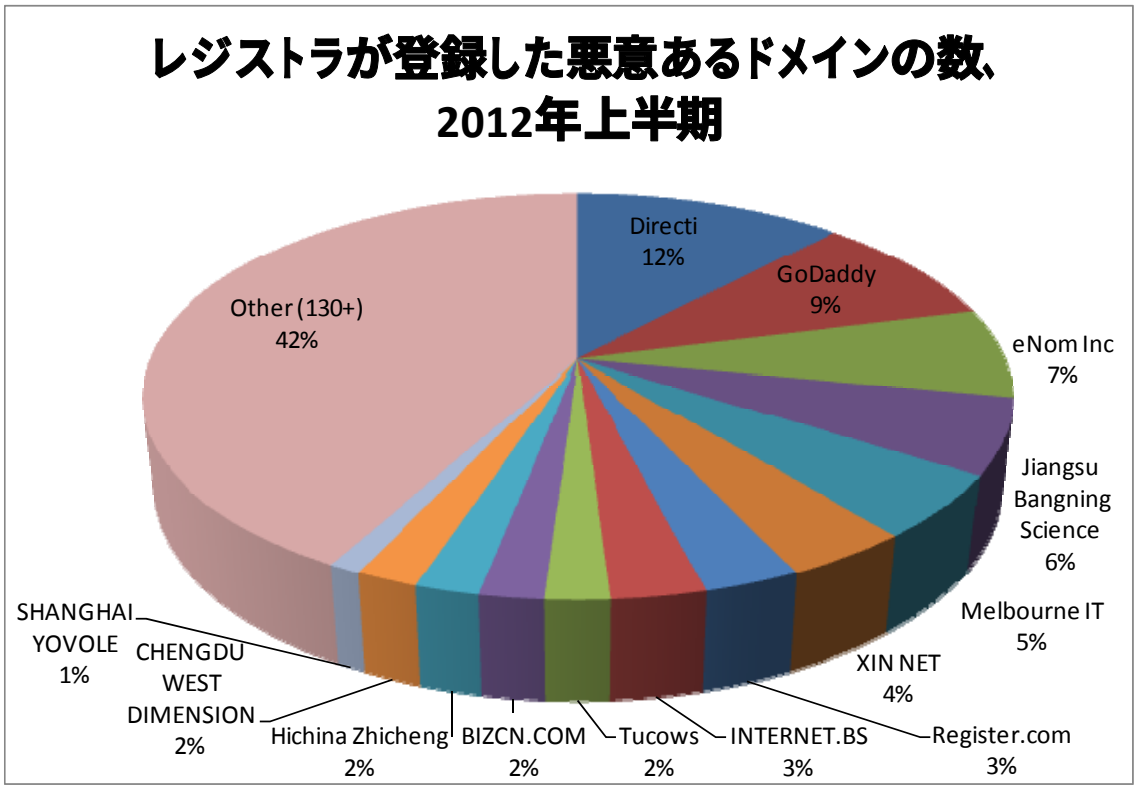
世界における半数以上の悪意あるドメインの登録は、.TK レジストリで行われ、さらに .TK がレジストラとしても記録されています。そのため、ここから先は、.TK ドメインを省き、3,773 個のドメインを分析しました。

レジストラの市場は多種多様です。主要事業者の GoDaddy は gTLD 市場の約半分を握っています。攻撃者は、GoDaddy の市場占有率に比べ、あまり GoDaddy を使用していなかったことが目立ちました。GoDaddy 以外には、20 社ほどの中規模から大規模な事業者がおり、そして多数の小規模な事業者がいます。

---

[7] ブランド名が含まれているドメイン名として判定されたものの中に： bid-pagz-yahoo.com（Yahoo!）、batteuswow.net（World of Warcraft）、ntwestsc.com（Natwest）と fbphonenumbers.tk（Facebook）が含まれていました。

大規模なレジストラーDirecti、eNorm、MelbourneIT、Register.com と Tucows は、誰もが想像できるように不正利用されたレジストラの上位に入りました。その理由として、各社の市場占有率が高いからです。レジストラの中には、代理店プログラムを持つものもあり、このプログラムの中で売られたドメインもありますが、転売した組織を特定することはできませんでした。今回の調査では、データの精度が高く、特に ccTLD 登録に関しては、140 のレジストラが最低一つの悪意あるドメインを登録したことが分かりました。



異なるレジストラを比較するために、TLD 同士を比較した際に使用した数値(スコア) と同じものを使用しました－管理下のドメインで 10,000 個の中で悪意あるドメインの割合。この数値を用い、レジストラの中で規模と比較し、攻撃を受けているかを確認しました。下記にある 21 のレジストラが、悪意あるドメイン登録数の 79% (2,991) を占めました。

トップ 11 のうち、7 つのレジストラが中国に存在しています。中国を標的にする攻撃者は、フィッシングのためにドメイン名の登録を行う傾向があり、ウェブサーバのハッキングはあまり行いません。攻撃者は、フィッシングのために 11 個の .CN ドメインしか登録せず、.TK、.IN、.COM、.INFO などの安いドメインを好んで購入していました。中国のレジストラで登録されたドメインは主に中国内にある組織を攻撃するためのものであり、Taobao.com、CCTV、China Construction Bank などが含まれます。しかしながら、

Facebook や Paypal などを攻撃するためにも使用されていました。中国を攻撃するために中国外のレジストラを使うこともあります。他のオンラインサービス同様、ドメイン登録には国境は無く、攻撃者は楽な方法でドメイン名を登録しています。

悪意あるドメインのスコアが高いレジストラ、2012 年下半期

25 件以上の悪意ある登録および 1,000 以上の gTLD ドメインを管理しているレジストラ

順位	レジストラ	2011年下半期で使用された悪意あるドメイン名の数	2012年3月時点でのgTLD ドメインの数[8]	スコア: 2011年下半期の 10,000 ドメインごとの攻撃件数
1	Shanghai Yovole	63	1,537	40.99
2	Chengdu West Dimension	88	3,177	27.7
3	Jiangsu Bangning Science	287	76,858	3.73
4	Internet.BS	118	89,402	1.32
5	Dynamic Network Services	28	58,555	0.48
6	EuroDNS	35	81,813	0.43
7	BIZCN.COM	97	278,109	0.35
8	Directi	558	1,724,071	0.32
9	XIN NET	184	980,268	0.19
10	Beijing Innovative	30	171,574	0.17
11	Hichina Zhicheng	97	751,285	0.13
12	Domainpeople	41	326,586	0.13
13	Register.com	146	1,911,337	0.08
14	Melbourne IT	237	3,128,559	0.08
15	Name.com	42	567,410	0.07
16	eNom Inc	333	7,830,968	0.04
17	Fastdomain	28	1,271,361	0.02
18	Tucows	106	6,447,422	0.02
19	GoDaddy	418	30,340,427	0.01
20	1 & 1 Internet	29	4,462,657	0.01
21	Network Solutions	26	5,542,203	0

2 つのレジストラ： Shanghai Yovole Networks Inc. (http://www.yovole.com/) と Chengdu WestDimension Digital Technology (http://west263.com/) が他社と比べ、特に目立ちました。この 2 社は、中国にある小さなレジストラで高いスコアとなりました。Chengdu West は、前回のレポートでも群を抜いてスコアが高く、問題が解決されていないことが伺われます。Chengdu West が提供しているドメインの中には、衣料品のブランド名が含まれるドメイン名を占拠し、偽造された製品を売っていると思われます。

一般的に見て、レジストラが悪意あるドメインの登録が多いか否かを判断する目安として、

[8] 情報源： Webhosting.info

10,000 個の管理下ドメインのうち、悪意あるものが 1 つ以上ある事です。今回のレポートでは、前回のレポートに比べ、レジストラ情報をより多く収集することができました。今後もデータを収集し、よりよい分析を行いたいと思います。

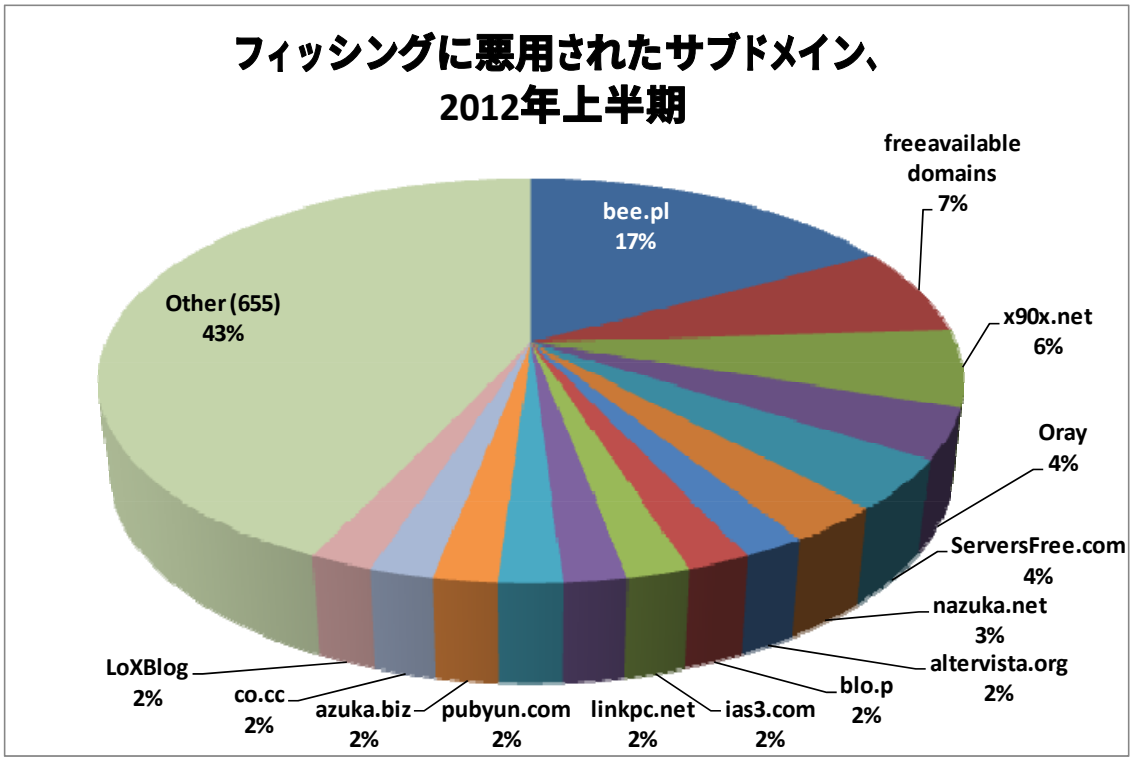
【Use of Subdomain Services for Phishing】サブドメインサービスを使用したフィッシング

サブドメインサービスを不正利用したフィッシングを引き続き観測しています。**以前からの傾向として、攻撃者によるサブドメインの登録数が "通常" ドメインの登録数を上回りました。しかし、サブドメインサービスを使用したフィッシングは、合計の 21% から 14% に減少しました。また、攻撃者は不正利用可能な新たなプロバイダを探しています。**

2012 年上半期 では、13,307 件のフィッシングがサブドメインサービス上で観測され、13,109 個の固有のサブドメインを使用していました。比較として、攻撃者は 7,712 個の "通常"ドメインを 2012 年上半期 に登録しました。この数字は、2012 年下半期 の 17,390 から 20% 減少しましたが、すべてのフィッシング件数の 14% を占めています。この割合は、2012 年下半期 の 21% から減少し、サブドメインサービスの中には、不正利用を未然に防いだり、検知したりするものも出てきたのではないかと推察しています。

"サブドメイン登録サービス" の定義は、プロバイダが管理するドメイン名の下にあるサブドメイン "ホスティングアカウント (hosting account)" を顧客に提供するサービスとしています。これらのサービスは、管理している DNS スペース内で "ドメイン名" を様々な用途のために提供し、無料で DNS 管理も提供することがあります。この場合、顧客が使用可能なホスト名・E-mail は以下のものになります：

<顧客契約期間>.<サービスプロバイダ_sld>.TLD



サブドメインサービスの不正利用は依然として対応が困難です[9]。理由として、多くのサービスが無料で提供され、匿名で登録可能、そしてサブドメインのプロバイダのみがフィッシングに対応可能だからです。多くのサービスはクレーム応じますが、未然にドメインが不正利用されないための対応はしていません。

ポーランドにあるサービス、bee.pl（または osa.pl）が、2012 年下半期 同様 2012 年上半期 も最も不正利用されたサービスでした。**サブドメインサービスを不正利用した攻撃のうち、17% が bee.pl を不正利用したものでした。**しかし、件数は 2012 年下半期 の 4,500 から 2012 年上半期 には 2,300 に減少していました。このプロバイダは色々な問題を抱えていることから、引き続き注意深く監視していきます。

新たなサブドメインサービスを不正利用されているケースを観測しました。**2012 年上半期では、50 個以上の新たなサブドメインサービスが不正利用され、これらのサービスは過去**

[9]通常のドメイン名レジストラまたはレジストリ管理者は、メインまたは"親" ドメインを停止することでフィッシングに対応できない事が多いです。理由として、その親ドメインの下にあるサブドメインが使用できなくなり、無実なユーザまでもがサービスが使用できなくなるからです。レジストラは、同じドメインに対して多くの報告を受けた場合、そのドメインに対するサービスを停止することもあります。このような事例は、数回観測されています。

のレポートでは観測されませんでした。これは、攻撃者が様々なところに手を出している証拠です。

2 番目に不正利用されたプロバイダ、freeavailabledomains.com では、1,000 個近くの不正利用されたドメインを観測しました。観測された数から、問題のあるサイトと推察できます。しかし、下記のスクリーンショットから "不正利用の報告（Report Abuse)" のリンクがあり、サブドメイン販売業者の中では大変良い傾向です。

freeavailabledomains.com のホームページ

最も不正利用されたサブドメインプロバイダの中で、多くのプロバイダは件数の大幅な増加または、過去にフィッシングを受けていません。今回のリストでは、トップ 10 のうち、8 つのサブドメインサービスは、過去にトップ 15 にすら掲載されておらず、始めてレポートに登場したサービスが多くありました。

朗報として、過去に多くの不正利用件数を受けていたサービスの中で、いくつかのサービスは、フィッシングを目的としたドメインが大幅に減少しました。常に問題を抱えていた、co.cc や cx.cc のサービスは、それぞれのドメイン上でのフィッシング件数に大幅の減少が見られました。過去 6 ヶ月監視していたサブドメインサービスの多くは、WHOIS サービスや不正利用報告（Report Abuse）のフォームを提供していました。過去から不正利用されていたサービスにおいて自然な行為ではありますが、他のサブドメインサービスも同様に、このようなサービスを提供することを推奨します。

我々は、750 個のサブドメイン登録サービスを特定しており、これらのサービスは 3,500

以上のドメイン名上でサービスを提供しています。この数は、それぞれのサブドメインサービスが "ドメインレジストリ" であるため、現在の Top-level ドメインスペースよりも多いです。サブドメインサービスには様々なビジネスモデルがあり、規制されていません。ただ、TLD レジストリサービスやレジストラの不正利用に対する対応体制が整っていくにつれ、攻撃者がサブドメインサービスの不正利用を行っていることに驚きはありません。サブドメインサービスの中で対応している組織があっても、不正利用が容易なサービスを提供するプロバイダがたくさんあります。

フィッシングに悪用されたサブドメインサービス、2012 年上半期

順位	攻撃件数	プロバイダ
1	2,290	bee.pl (osa.pl)
2	958	freeavailabledomains.com
3	799	x90x.net
4	548	Oray
5	541	ServersFree.com
6	326	nazuka.net
7	324	altervista.org
8	310	blo.pl
9	284	ias3.com
10	275	linkpc.net
11	247	pubyun.com
12	236	azuka.biz
13	225	co.cc
14	214	LoXBlog
15	191	cu.cc
16	190	1FreeHosting
17	154	r.gd
18	154	tripod.com
19	149	3owl.com
20	147	ce.ms

【Use of Internationalized Domain Names (IDNs)】国際化ドメイン名の使用

ここのところ、国際化ドメイン名（IDN）に対して関心が高まってきています。**データは、IDN 固有の特徴がフィッシングに使われていないことを証明しています。**

IDN は、1 つ以上の ASCII 文字ではない文字がドメイン名に含まれているものを指します。これらのドメイン名には、ä や ü などの発音区別符を含む文字や、アラビア文字、中国語、キリル文字やヒンディー文字などのラテン系でない活字から成り立つ事もあります。ここ 7 年間で IDN はドメイン名登録において 2nd レベルおよび 3rd レベルで提供されるようになっており、主にアジアで登録されています。IDN TLD は、TLD 拡張子を

含み、ドメイン名のすべてをラテン文字じゃない文字列で提供することが可能です。ICANN および IANA は 2010 年 5 月にはじめて IDN TLD を有効にし、執筆段階で 38 個の承認された IDN TLD があります。多くの IDN TLD は活動していませんが、ロシア連邦の .рф (.rf) には 830,000 個のドメインがあり、韓国の TLD . 한국 には、220,000 個のドメインがすぐに登録されました。

IDN homographic 攻撃は、インターネットのユーザが通常使う言語の文字と違う言語の文字を見分けにくい (または見分けられない) 事を不正利用する手法です。この手法を使った攻撃は、2007 年 1 月から 5 件しか観測されておらず、2012 年上半期 では 1 件も観測されませんでした。2012 年上半期 では、58 個の通常の 2nd レベル IDN が不正利用されました。

IDN が数年に渡り広く提供されていたことにも関わらず、攻撃者がなぜ IDN homographic 攻撃を行わないのでしょうか？

1. 攻撃者はこのような手法を使って攻撃をする必要が無い。本レポートにある通り、攻撃者にとって、ドメイン名は何でも良いのです。

2. ブラウザの中には、デフォルトでアドレスバー内でドメイン名を Punycode で表示 ("xn--hotmal-t9a.net") するようになっています。このようなブラウザを使用しているユーザはこの攻撃が見えません。

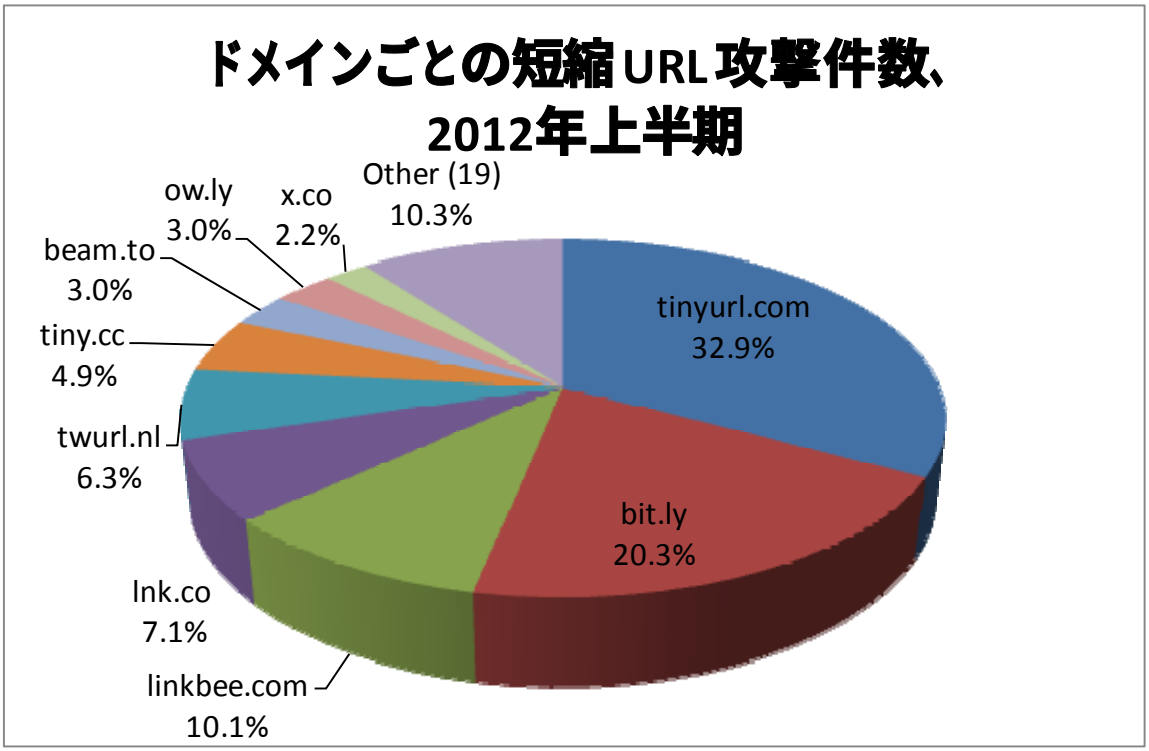
新しい IDN TLD レジストリは、現存する各国の ccTLD レジストリ管理者に割り当てられています。そのため、IDN TLD が他のドメインレジストリより攻撃を受ける事は無いと思います。

【Use of URL Shorteners for Phishing】短縮 URL を使用したフィッシング

攻撃者は、依然として "短縮 URL" サービスを使い、フィッシング URL を難読化しており、2012 年上半期 では、507 件しか観測されませんでしたが、2012 年下半期 で観測された 398 件よりも増加しました。これらのサービスを使うユーザは、入力文字数に限りがあるところに、サービスから得た短い URL を挿入し、被害者をより長い "隠れた" URL へ自動的にリダイレクトします。

メジャーな短縮 URL プロバイダは、積極的に悪意ある転送先をスクリーニングしており、サービスを不正利用されにくくするために規定を設けています。新たなベストプラクティスとして、多くのプロバイダは、転送先の URL を素早く特定するためのツールや、自動的に不正利用を報告する機能も提供しています。すべての短縮 URL プロバイダに似たような機能を提供することを推奨します。SURBL (http://www.surbl.org) は、無料で短縮

URL サービスの不正利用に関する情報を提供しています。すべてのサブドメイン代理店は、このフィードが提供する悪意のある URL リストを取得し、自サービス内で起きている不正防止に向け有効活用すべきだと思います。



犯罪者が攻撃のために、独自の短縮 URL サービスを作成している事も観測しています。ドメインのホームページは、通常の短縮 URL サービスと似ていますが、犯罪者はそのドメインを自分の私利私欲のために利用しているに過ぎません。これらのサイトを使ったフィッシングは悪意あるドメインとして判定しており、このカテゴリには、含まれていません。

【Conlusions】まとめ

攻撃者は利益のために、より効率的な手法にシフトしてきています。Top-level-domain の登録やセキュリティポリシーに関する変更や入手可能な自動的にハッキングツールの存在など様々な要因により、フィッシングをサイト改ざんや脆弱性のあるサービスへとシフトさせています。2012 年上半期 では、攻撃者がこれらの効率の良い手法を引き続き用い、多くの正規サーバや共有されたウェブホスティング環境を攻撃していることが判明しました。

また、攻撃者は収益につながる被害者に集中していたことも観測しました。中国人ユーザの中では、特に Taobao.com のユーザに対しフィッシング攻撃が成功しています。ウェブ

メールサービスに対する攻撃も増えました。表向きにはスパムを行うためにメールのアカウント情報に対する需要が増えたからです。一般的に、攻撃者は標的の数を絞りました。理由として小さな組織のユーザを狙うことで効率が落ちる、または特定の組織に関連したユーザ情報の方が高く売れるからだと我々は考えます。

【Appendix】付録

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
ac	Ascension Island	1	1	16,000	0.6	0.6	7:51:23	7:51:23	0	0.0
ad	Andorra	1	1	1,450	6.9	6.9	239:36:55	239:36:55	0	0.0
ae	United Arab Emirates	29	21	94,000	2.2	3.1	54:09:35	6:52:32	0	0.0
aero	sponsored TLD	3	3	7,980	3.8	3.8	23:16:24	12:08:09	0	0.0
af	Afghanistan	2	2				2:20:27	2:20:27	0	
ag	Antigua and Barbuda	2	2	19,524	1	1	7:48:58	7:48:59	0	0.0
ai	Anguilla	11	2	3,300	6.1	33.3	3:58:06	3:58:07	0	0.0
al	Albania	5	5	7,500	6.7	6.7	5:31:40	2:04:07	0	0.0
am	Armenia	21	8	19,900	4	10.6	15:43:52	2:12:25	0	0.0
an	Netherlands Antilles	0	0	900					0	
ao	Angola	0	0	250					0	
ar	Argentina	499	412	2,437,500	1.7	2	8:53:26	8:53:26	2	0.0
arpa	Advanced Research Project Agency	0	0						0	
as	American Samoa	4	4				8:26:20	8:23:46	0	
asia	sponsored TLD	18	14	197,864	0.7	0.9	24:01:18	5:19:42	0	0.0
at	Austria	94	67	1,133,707	0.6	0.8	49:50:36	18:37:30	0	0.0
au	Australia	1,383	1,101	1,731,128	6.4	8	24:58:02	5:03:41	2	0.0
aw	Aruba	0	0	600					0	
az	Azerbaijan	5	5	13,831	3.6	3.6	16:58:06	12:49:55	0	0.0
ba	Bosnia and Herzegovina	17		13,500	11.1	12.6	18:55:19	11:02:36	0	0.0
bd	Bangladesh	12		4,950	18.2	24.2	13:34:28	10:13:22	0	0.0
be	Belgium	536		1,292,600	3.7	4.1	13:11:39	1:32:22	12	0.1
bf	Burkina Faso	1					29:11:44	29:11:45	0	
bg	Bulgaria	19		24,400	5.3	7.8	22:05:54	5:43:00	0	0.0
bh	Bahrain	1					1:03:33	1:03:34	0	
biz	generic TLD	877		2,296,289	1.4	3.8	14:40:24	3:28:11	5	0.0
bm	Bermuda	3		7,900	2.5	3.8	5:29:11	7:43:09	0	0.0

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
bn	Brunei Darussalam	1	1	1,150	8.7	8.7	4:29:35	4:29:35	0	0.0
bo	Bolivia	22	18	8,200	22	26.8	10:40:43	6:13:23	0	0.0
br	Brazil	4,039	3,207	2,959,495	10.8	13.6	22:02:59	6:18:34	24	0.1
bs	Bahamas	0	0	2,300					0	
bt	Bhutan	6	6				22:32:13	3:08:00	0	
bw	Botswana	0	0						0	
by	Belarus	43	25				43:26:03	13:50:50	0	
bz	Belize	9	7	48,066	1.5	1.9	57:42:53	4:57:19	2	0.4
ca	Canada	632	521	1,926,000	2.7	3.3	28:42:33	5:32:05	5	0.0
cat	sponsored TLD	16	14	53,817	2.6	3	18:47:28	17:21:16	0	0.0
cc	Cocos (Keeling) Islands *(estimated)*	1,373	75	900,000	0.8	15.3	16:44:43	7:53:53	3	0.0
cd	Congo, Democratic Repub.	3	2	5,200	3.8	5.8	10:27:29	8:17:57	0	0.0
cg	Congo	1	1				18:49:05	18:49:06	0	
Ch	Switzerland	348	308	1,700,985	1.8	2	18:44:25	2:03:46	0	0.0
ci	Côte d'Ivoire	3	2	2,100	9.5	14.3	361:45:33	314:40:56	0	0.0
cl	Chile	1,024	831	383,100	21.7	26.7	30:10:45	8:44:08	1	0.0
cm	Cameroon	20	11	12,000	9.2	16.7	25:29:19	16:51:22	0	0.0
cn	China	156	120	3,502,064	0.3	0.4	24:05:44	0.538888889	11	0.0
co	Colombia	354	269	1,250,856	2.2	2.8	15:50:11	8:11:03	11	0.1
com	generic TLD	41,265	31,228	105,601,144	3	3.9	23:04:36	5:25:59	2,588	0.2
coop	sponsored TLD	2	2	14,729	1.4	1.4	9:47:00	9:47:00	0	0.0
cr	Costa Rica	26	24	14,200	16.9	18.3	10:46:10	0:37:32	0	0.0
cu	Cuba	1	1	2,250	4.4	4.4	50:44:57	50:44:58	0	0.0
cx	Christmas Island	18	9	5,225	17.2	34.4	43:21:32	17:53:51	0	0.0
cy	Cyprus	6	6	9,950	6	6	23:31:58	8:50:04	0	0.0
cz	Czech Republic	170	107	948,871	1.1	1.8.	39:41:14	8:50:04	0	0.0
de	Germany	849	573	15,069,393	0.4	0.6	32:35:26	12:36:49	6	0.0
dj	Djibouti	0	0						0	
dk	Denmark	263	209	1,185,409	1.8	2.2	31:40:57	11:29:15	0	0.0
dm	Dominica	1	1	14,500	0.7	0.7	0:30:18	0:30:18	0	0.0

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
do	Dominican Republic	13	12				21:06:58	4:05:23	0	
dz	Algeria	2	2	4,366	4.6	4.6	118:06:17	118:06:18	0	0.0
ec	Ecuador	36	31	30,001	10.3	12	24:26:59	8:42:35	0	0.0
edu	U.S. higher education	36	31	7,588	40.9	47.4	36:08:56	10:16:40	0	0.0
ee	Estonia	28	21	65,635	3.2	4.3	31:21:34	19:38:18	0	0.0
eg	Egypt	10	8	6,000	13.3	16.7	60:31:57	7:37:09	0	0.0
er	Eritrea	0	0						0	
es	Spain	381	288	1,548,844	1.9	2.5	29:40:55	12:10:00	2	0.0
et	Ethiopia	1	1	1,000	10	10	88:18:20	88:18:20	0	0.0
eu	European Union	347	276	3,592,000	0.8	1	20:22:28	7:30:20	7	0.0
fi	Finland	26	23	290,801	0.8	0.9	43:34:52	10:06:39	0	0.0
fj	Fiji	0	0	4,000					0	
fk	Falkland Islands	0	0	100					0	
fm	Micronesia, Fed. States	7	6				9:09:21	3:01:51	0	
fo	Faroe Islands	2	2				1:47:29	1:47:29	0	
fr	France	703	502	2,339,564	2.1	3	31:15:25	13:08:43	2	0.0
gd	Grenada	156	2	4,300	4.7	362.8	16:05:25	12:43:28	0	0.0
ge	Georgia	289	277	18,400	150.5	157.1	3:55:44	0:59:35	0	0.0
gg	Guernsey	45	5				35:25:41	33:05:06	0	
gh	Ghana	2	2				21:01:55	21:01:56	0	
gi	Gibraltar	0	0	1,896					0	
gl	Greenland	22	5	4,600	10.9	47.8	18:47:58	3:48:19	0	0.0
gov	U.S. government	3	3	5,000	6	6	23:44:24	4:53:26	0	0.0
gp	Guadeloupe	20	15	1,475	101.7	135.6	20:14:43	8:01:45	1	6.8
gr	Greece *(estimated)*	267	212	450,000	4.7	5.9	23:16:18	7:58:39	0	0.0
gs	South Georgia & Sandwich Is.	2	2	8,160	2.5	2.5	0:10:00	0:10:00	1	1.2
gt	Guatemala	12	9	10,820	8.3	11.1	17:21:35	4:55:05	0	0.0
gy	Guyana	2	2	2,050	9.8	9.8	38:58:14	38:58:15	0	0.0
hk	Hong Kong	31	23	233,562	1	1.3	23:51:38	10:14:51	0	0.0
hm	Heard and McDonald Is.	3	1				19:44:16	19:44:16	0	
hn	Honduras	6	6	6,256	9.6	9.6	10:40:44	6:11:28	0	0.0

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
hr	Croatia	40	35	79,224	4.4	5	20:04:22	11:20:28	0	0.0
ht	Haiti	4	3				26:24:15	25:55:04	0	
hu	Hungary	176	126	620,111	2	2.8	63:27:19	18:35:39	0	0.0
id	Indonesia	113	95	78,000	12.2	14.5	20:32:33	6:45:08	0	0.0
ie	Ireland	77	55	179,731	3.1	4.3	30:11:30	12:35:53	0	0.0
il	Israel	89	65	230,100	2.8	3.9	48:37:04	14:32:19	1	0.0
im	Isle of Man	19	8				18:57:46	8:41:03	2	
in	India	1,690	1,351	1,674,552	8.1	10.1	23:27:07	7:57:25	474	2.8
info	generic TLD	1,764	1,514	8,153,167	1.9	2.2	12:32:24	4:01:44	231	0.3
int	sponsored TLD	2	1						0	
io	British Indian Ocean Terr.	0	0						0	
IP address	(no domain name used)	2,410							0	
iq	Iraq	0	0						0	
ir	Iran	276	138	267,226	5.2	10.3	15:59:50	3:46:09	0	0.0
is	Iceland	20	17	38,900	4.4	5.1	189:38:15	75:28:39	1	0.3
it	Italy	454	339	2,403,000	1.4	1.9	47:52:27	15:26:47	1	0.0
je	Jersey	11	5				16:39:44	8:59:43	0	
jm	Jamaica	1	1	6,400	1.6	1.6	156:53:45	156:53:46	0	0.0
jo	Jordan	2	1	4,200	2.4	4.8	8:32:48	8:32:49	0	0.0
jobs	sponsored TLD	0	0	41,700					0	
jp	Japan	183	110	1,291,433	0.9	1.4	58:29:11	27:14:11	1	0.0
ke	Kenya	16	15	22,000	6.8	7.3	29:28:49	17:26:20	0	0.0
kg	Kyrgyzstan	62	4	5,300	7.5	117	4:07:23	0:21:15	0	0.0
kh	Cambodia	4	2	1,550	12.9	25.8	3:30:13	3:28:15	0	0.0
ki	Kiribati	0	0						0	
kr	Korea	550	357	1,095,127	3.3	5	25:00:27	11:20:10	1	0.0
kw	Kuwait	3	3	3,181	9.4	9.4	0:10:00	0:10:00	0	0.0
ky	Cayman Islands	1	1				1:03:39	1:03:40	0	
kz	Kazakhstan	57	44	73,050	6	7.8	47:41:20	21:56:30	1	0.1
la	Lao People's Demo. Rep. *(domains estimated)*	45	10	9,500	10.5	47.4	27:02:04	9:37:09	1	1.1

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
lb	Lebanon	2	2	3,500	5.7	5.7	0:28:59	0:28:59	0	0.0
lc	St. Lucia	31	23	3,115	73.8	99.5	8:06:24	3:31:07	0	0.0
li	Liechtenstein	10	8	68,500	1.2	1.5	20:11:52	6:14:52	0	0.0
lk	Sri Lanka	11	8	8,490	9.4	13	14:49:00	6:54:11	0	0.0
ls	Lesotho	0	0						0	
lt	Lithuania	44	35	145,550	2.4	3	32:43:32	14:34:48	0	0.0
lu	Luxembourg	6	5	68,549	0.7	0.9	10:49:33	3:33:21	0	0.0
lv	Latvia	35	28	100,060	2.8	3.5	57:46:36	25:47:17	0	0.0
ly	Libya	133	10	12,400	8.1	107.3	24:09:25	9:24:32	0	0.0
ma	Morocco	22	17	42,354	4	5.2	21:32:01	10:39:05	0	0.0
mc	Monaco	1	1				0:27:16	0:27:17	0	
md	Moldova	12	9	20,697	4.3	5.8	18:46:03	16:24:53	0	0.0
me	Montenegro	168	117	637,940	1.8	2.6	27:30:46	4:39:13	4	0.1
mg	Madagascar	2	2				19:11:20	19:11:21	0	
mk	Macedonia	15	10				47:27:52	14:28:35	0	
ml	Mali	0	0						0	
mn	Mongolia	214	197	12,967	151.9	165	6:08:53	0:15:05	0	0.0
mo	Macao	0	0	300					0	
mobi	sponsored TLD	25	23	1,047,487	0.2	0.2	14:50:31	6:40:15	1	0.0
mp	Northern Mariana Islands	5	4				11:10:55	15:35:37	0	
mr	Mauritania	0	0						0	
ms	Montserrat	271	13	9,800	13.3	276.5	33:15:37	14:36:20	5	5.1
mt	Malta	2	2	6,200	3.2	3.2	1:23:04	1:23:04	0	0.0
mu	Mauritius	12	8	7,500	10.7	16	20:38:27	9:48:49	0	0.0
museum	sponsored TLD	0	0	440					0	
mv	Maldives	1	1						0	
mw	Malawi	1	1						0	
mx	Mexico	328	248	568,577	4.4	5.8	31:28:35	11:35:45	1	0.0
my	Malaysia	155	121	194,365	6.2	8	27:25:57	12:02:27	0	0.0
mz	Mozambique	0	0	1,885					0	
na	Namibia	1	1	220	45.5	45.5	126:37:37	126:37:38	0	0.0
name	generic TLD	19	18	230,572	0.8	0.8	8:13:40	3:00:13	0	0.0

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
nc	New Caledonia	0	0						0	
ne	Niger	0	0	140					0	
net	generic TLD	6,518	3,515	15,097,524	2.3	4.3	22:26:22	5:19:49	208	0.1
nf	Norfolk Island	3	2	1,600	12.5	18.8	48:58:58	54:17:14	0	0.0
ng	Nigeria	26	22	35,000	6.3	7.4	19:19:05	4:09:45	0	0.0
ni	Nicaragua	10	7	6,400	10.9	15.6	10:07:54	3:59:02	0	0.0
nl	Netherlands	936	776	4,956,736	1.6	1.9	21:09:11	6:02:27	1	0.0
no	Norway	89	67	558,004	1.2	1.6	47:35:42	18:28:04	0	0.0
np	Nepal	67	55	29,280	18.8	22.9	33:47:18	11:24:17	0	0.0
nr	Nauru	1	1				0:40:41	0:40:42	0	
nu	Niue *(domains estimated)*	136	39	100,000	3.9	13.6 s	26:44:36	9:22:42	1	0.1
nz	New Zealand	110	93	485,358	1.9	2.3	34:03:28	11:01:09	1	0.0
om	Oman	0	0						0	
org	generic TLD	4,147	2,870	9,957,774	2.9	4.2	18:17:27	5:58:01	78	0.1
pa	Panam	3	3	7,112	4.2	4.2	16:07:12	14:33:48	0	0.0
pe	Peru	126	115	61,530	18.7	20.5	16:24:47	3:15:38	0	0.0
pf	French Polynesia	0	0						0	
pg	Papua New Guinea	1	1						0	
ph	Philippines *(domains estimated)*	46	35				23:34:05	4:35:12	1	
pk	Pakistan (domains estimated)	58	51	18,000	28.3	32.2	17:05:05	4:16:48	1	0.6
pl	Poland	3,453	565	2,311,649	2.4	14.9	24:21:38	11:53:54	2	0.0
pn	Pitcairn	4	3				29:39:08	36:20:56	0	
post	sponsored TLD	0	0	0					0	
pro	sponsored TLD	13	12	154,664	0.8	0.8	23:18:41	16:14:02	0	0.0
ps	Palestinian Territory	12	9	7,660	11.7	15.7	47:02:52	8:04:40	0	0.0
pt	Portugal	74	57	235,091	2.4	3.1	35:52:02	8:08:15	0	0.0
py	Paraguay	41	39	14,500	26.9	28.3	2:38:26	1:06:30	0	0.0
qa	Qatar	2	2	13,866 s	1.4	1.4	7:57:11	7:57:11	1	0.7
re	Réunion	7	6	16,510	3.6	4.2	24:17:10	8:32:16	0	0.0
ro	Romania	967	533	576,323	9.2	16.8	21:59:25	5:31:48 s	0	0.0

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
rs	Serbia	89	54	74,000	7.3	12	64:41:43	18:56:25	0	0.0
ru	Russian Fed.	1,304	829	3,860,995	2.1	3.4	39:31:53	13:02:11	8	0.0
rw	Rwanda	2	2				1:44:02	1:44:03	0	
sa	Saudi Arabia	11	9	28,458	3.2	3.9	13:33:24	12:10:46	0	0.0
sc	Seychelles	2	2	4,778	4.2	4.2	6:58:45	6:58:45	0	0.0
sd	Sudan	6	6				0:49:23	0:45:05	0	
se	Sweden	216	156	1,210,031	1.3	1.8	42:11:58	18:53:13	0	0.0
sg	Singapore	89	66	140,107	4.7	6.4	55:29:05	17:18:39	0	0.0
sh	Saint Helena	1	1	2,999	3.3	3.3	14:10:36	14:10:37	0	0.0
si	Slovenia	61	55	103,202	5.3	5.9	49:52:26	15:08:51	0	0.0
sk	Slovakia	66	34	274,360	1.2	2.4	17:47:19	9:42:18	0	0.0
Sl	Sierra Leone	0	0						0	
sm	San Marino	0	0	1,900					0	
sn	Senegal	1	1	3,500	2.9	2.9	66:42:35	66:42:36	0	0.0
so	Somalia	24	4						1	
st	Sao Tome and Principe	6	4				6:11:54	5:03:01	0	
su	Soviet Union	37	24	104,544	2.3	3.5	32:42:01	11:44:31	0	0.0
sv	El Salvador	9	5	5,400	9.3	16.7	18:44:26	14:24:46	0	0.0
sy	Syria	2	2				18:47:45	18:47:45	0	
sz	Swaziland	0	0						0	
tc	Turks and Caicos	39	13				10:52:51	7:46:43	0	
tel	generic TLD	0	0	264,241					0	
tf	French Southern Territories	62	7	1,550	45.2	400	12:39:35	8:06:47	0	0.0
tg	Togo	2	2				24:22:37	24:22:38	0	
th	Thailand	122	77	69,490	11.1	17.6	29:16:33	13:18:19	0	0.0
tj	Tajikistan	1	1	18,800	0.5	0.5	0:23:14	0:23:15	0	0.0
tk	Tokelau	4,197	3,939	8,994,000	4.4	4.7	19:20:38	10:49:40	3,939	4.4
tl	Timor-Leste	11	7				12:44:02	10:15:51	0	
tm	Turkmenistan	3	1	3,775	2.6	7.9	11:22:39	6:15:07	0	0.0
tn	Tunisia	6	6	14,860	4	4	6:16:17	0:26:53	0	0.0
to	Tonga	71	16	15,000	10.7	47.3	17:38:53	8:03:27	1	0.7

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意あるドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
tp	Portuguese Timor	0	0						0	
tr	Turkey	170	138	302,008	4.6	5.6	30:33:06	10:58:56	2	0.1
travel	sponsored TLD	4	4	24,120	1.7	1.7	39:52:25	11:43:25	0	0.0
tt	Trinidad and Tobago	2	1	2,500	4	8	17:03:07	17:03:07	0	0.0
tv	Tuvalu *(domains estimated)*	133	106	200,000	5.3	6.7	28:19:07	10:30:25	4	0.2
tw	Taiwan	176	123	508,089	2.4	3.5	26:42:05	9:38:24	4	0.1
tz	Tanzania	5	4	5,200	7.7	9.6	53:47:35	29:23:53	0	0.0
ua	Ukraine	253	185	619,517	3	4.1	28:54:29	14:48:42	2	0.0
ug	Uganda	5	3	3,200	9.4	15.6	32:58:35	27:18:32	0	0.0
uk	United Kingdom	1,433	1,190	10,131,000	1.2	1.4	33:54:15	10:42:50	28	0.0
us	United States	626	303	1,784,000	1.7	3.5	15:14:37	2:54:22	20	0.1
uy	Uruguay	35	29	36,908	7.9	9.5	53:12:33	6:18:15	0	0.0
uz	Uzbekistan	10	7	14,703	4.8	6.8	25:48:26	10:22:36	0	0.0
vc	St. Vincent and Grenadines	4	4	8,196	4.9	4.9	8:10:17	8:10:18	0	0.0
ve	Venezuela	61	44	213,000	2.1	2.9	38:51:03	15:35:49	0	0.0
vg	British Virgin Islands	1	1	8,300	1.2	1.2	0:36:19	0:36:19	0	0.0
vi	Virgin Islands	0	0	8,300					0	
vn	Vietnam	136	105	300,343	3.5	4.5	44:14:26	15:22:23	1	0.0
vu	Vanuatu	16	5				23:33:33	7:46:20	0	
ws	Samoa	69	44	543,500	0.8	1.3	16:34:01	5:23:45	3	0.1
xn--3e0b707	.한국 (KR IDN)	0	0	220,250					0	
xn--90a3ac	.СРБ (Serbia IDN)	0	0	3,600					0	
xn—fzc2c9e2c	.ලංකා ලංකා (Sri Lanka IDN)	0	0	150					0	
xn—mgberp4a5d4a	.السعودية (Saudi Arabia IDN)	0	0	1,800					0	

TLD	TLD Location	1H2012 のフィッシング件数	1H2012 のフィッシングで使用されたドメイン名の数	2012年5月時点でのドメイン数	スコア: 1H2012 の 10,000 ドメインごとのフィッシングドメイン数	スコア: 1H2012の 10,000 ドメインごとの攻撃件数	1H2012 の平均稼働時間 (hh:mm:ss)	1H2012 の稼働時間中央値 (hh:mm:ss)	1H2012 の悪意ある ドメイン登録数	悪意ある登録スコア / レジストリ内の 10,000 ドメイン
xn--o3cw4h	.ไทย (.TH IDN)	0	0	1,000					0	
xn--p1ai	.рф (Russian Federation IDN)	1	1	830,689	0	0			0	0.0
xn—xkc2al3hye2a	.இலங்கை (Sri Lanka IDN)	0	0	80					0	
xxx	sponsored TLD	0	0	136,632					0	
ye	Yemen	0	0	800					0	
yu	Yugoslavia *(TLD deprecated March 2010)*	0	0	0					0	
za	South Africa	763	644	779,500	8.3	9.8	21:57:53	5:08:33	2	0.0
zm	Zambia	3	3				24:13:19	25:57:05	0	
zw	Zimbabwe	24	21				4:19:08	4:05:16	0	
	TOTALS	**93,462**	**64,204**	**240,418,900**					**7,719**	