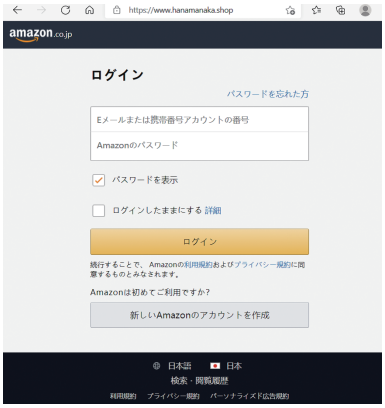
サイバー犯罪の犯人は、どこまで突き止められるか？

東京理科大学　創域理工学部　情報計算科学科　教授　明石（あかし）　重男（しげお）

メッセージに、「amazon の会費の不払いがあるのでログインするように」誘導する web サイトが送られてきました。そこで、クリックしてみると次のような画面が表示されました。まず最初に、見た目だけで確認可能な、「偽装と判断される根拠となる箇所」について解説します。



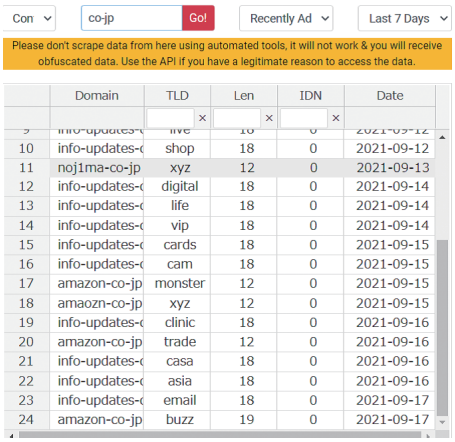
これから説明することですが、このサイトは、見た瞬間に「偽装」であることが分かります。そこで以下では、この web サイトに、複数個の無料で使えるツールを適用して、このようなサイバー犯罪について解析を試みます。最初に、この偽装サイトの URL は、

https://www.hanamanaka.shop

であり、

https://www.amazon.co.jp

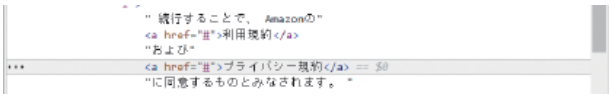
とは大きく異なっています。この点が、先程述べた「一目で見て偽装サイトと判別可能である」と述べた理由です。詐欺サイトのドメイン名が、一般的な .com や .jp 等でない理由としては、.xyz や .shop ドメインが安価に取得可能であるためと考えられます。一般的に、詐欺サイトや偽装サイトの寿命は短いです。長期にわたり偽装サイトを公開しておくと、捜査の対象となりやすく管理者の身元を追跡される可能性が高まるためです。そのため、詐欺サイト側にとって、ウェブサイト構築が安価であるということは、非常に重要な要素となっています。以上が、ドメイン名を確認することが、「詐欺サイトであるか否かを判別するのに効果がある」と考えられる理由です。しかし、詐欺サイト側も対策を行っており、co.jp と誤認させるために co-jp など類似している単語を URL に含めている場合が数多く存在します。そこで実際に、新規ドメイン名を検索するサイトである「DN Pedia」というウェブサイトを用いて、co-jp について検索を行ってみました。すると、以下のような結果が得られました。



	Domain	TLD	Len	IDN	Date
10	info-updates-(	shop	18	0	2021-09-12
11	noj1ma-co-jp	xyz	12	0	2021-09-13
12	info-updates-(	digital	18	0	2021-09-14
13	info-updates-(	life	18	0	2021-09-14
14	info-updates-(	vip	18	0	2021-09-14
15	info-updates-(	cards	18	0	2021-09-15
16	info-updates-(	cam	18	0	2021-09-15
17	amazon-co-jp	monster	12	0	2021-09-15
18	amaozn-co-jp	xyz	12	0	2021-09-15
19	info-updates-(	clinic	18	0	2021-09-16
20	amazon-co-jp	trade	12	0	2021-09-16
21	info-updates-(	casa	18	0	2021-09-16
22	info-updates-(	asia	18	0	2021-09-16
23	info-updates-(	email	18	0	2021-09-17
24	amazon-co-jp	buzz	19	0	2021-09-17

その結果、本物の amazon.co.jp に類似している amazonmazon-co-jp.xyz、amazonmazon-co-jp.trade 等を複数確認することができました。

続いて、ウェブサイトを構築する際に必ず行う「デバック」（＝ウェブサイト閲覧時に発生するエラーの事前除去作業）機能を持つ開発者ツールを使用して、この詐欺サイトを眺めた結果を以下に示します。

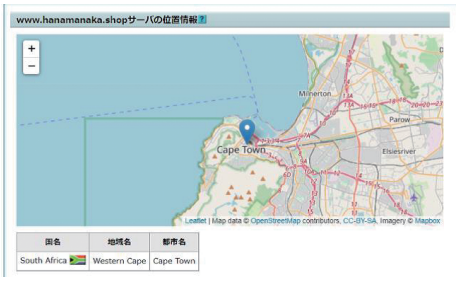


この画像は、正規ウェブサイトでは、法的に明記しなければいけない利用規約やプライバシー規約などを省略していることを示しています。正規ウェブサイトでは、これらの規約が改ざんされることを回避するため、別のページにリンクを張って、トップページには設定しないのが普通ですが、このサイトは、それを省略していることがわかります。本来、このようなサイトは、「クレジットカード番号等の情報を抜き取る」ことが目的ですから、実際に全くでたらめな email

アドレスとパスワードを使用して、ログインを実行してみましょう。すると、以下の様な本物の amazon ウェブサイトに移動させられることが分かりました。

上記表示は、この amazon 偽装サイトは、amazon アカウント情報に加えて、amazon アカウント保持者が持つクレジットカード情報までも抜き取り、更に amazon アカウント情報抜き取り終了後は、アカウント保持者に悟られないように本物の web サイトへ誘導するような悪意ある設定をしていることを示しています。当然ですが、偽装サイトの管理者が、クレジットカード情報を確認するサーバからの接続を許可してくれるはずはありません。従って、ここだけは、正規ウェブサイトに依存せざるを得ないことになります。しかし、被害者となっているクライアントと正規ウェブサイトを提供するサーバが、直接接続されていたのでは、クレジットカード番号を抜き取ることが不可能になってしまいます。従って、このような状況では、必ず悪意あるサーバが、正規クライアントと正規サーバとの間に、情報を抜き取る中間者として存在するはずです。

最後に、偽装サイトを提供するサーバの地理的情報を「aguse.jp」を使用して調べてみます。



この結果より、偽装ウェブサイトを公開するサーバは、南アフリカ共和国に存在することが分かりました。一方、比較対象として本物の amazon のウェブサーバ情報も調べてみました。

この結果より、本物の amazon ウェブサイトはアメリカ合衆国に存在することが分かりました。

組織名	Amazon, Inc.
ドメイン名	AMAZON.CO.JP
組織種別	Foreign Company
登録担当者	JC076JP
技術連絡担当者	IK4644JP
ネームサーバ	ns1.p31.dynect.net ns2.p31.dynect.net pdns1.ultradns.net pdns6.ultradns.co.uk
登録年月日	2002/11/21
最終更新日	2020/12/01 01:02:13 (JST)
接続年月日	2002/11/21

このような情報から判断すると、大手の正規ウェブサイトは、ドメイン名や組織名をそのまま用いていることが多いので、偽装サイトとの識別には、有効性を発揮していると考えられます。更に、今まで述べてきたように、1 つだけの識別要素ではなく、複数の識別要素から偽装サイトか否かを見分ける必要があることが分かりました。今回は、紹介しませんでしたが、偽装サーバの地理的位置だけでなく、サーバ管理者の連絡先までを表示する「Who is lookup」というツールがあります。しかしこれらのツールを使って偽装サイトを提供するサーバの身元を特定しても、「サーバ管理者と連絡がとれない」状況、もしくは、「サーバ管理者がレンタルサーバ会社であっても、個人情報保護という名目で、身元を教えてくれない」ため、残念なことに、個人レベルでの犯人追及は、困難な場合が多いのが現状です。

以上のように、犯人追跡の可能性について述べてきましたが、注意して頂きたいのは、「サイバー犯罪者は、個人を特定して犯罪を仕掛けてきているのではない」ということです。このような観点から、「スマホによる『見覚えのないウェブサイトなどへのアクセス』を実行しない」、「どうしても確認したい場合は、パソコン経由でインターネットを使って調べる」という作業が重要であることが分かります。