サブドメイン乗っ取り
脆弱性報告書

事業計画内容

グローバル企業は、ウェブページからEメール、認証、VoIPに至るまで、あらゆることをインターネットに依存しています。しかしそれは、外部からの攻撃を受ける組織のアタックサーフェス（攻撃対象領域）であり、サイバー犯罪の攻撃やフラウドを常に監視する必要があります。DNS（ドメイン名システム）は、簡単にいうとインターネット上の電話帳のような役割を果たすものであり、DNSレコードのハウスキープ処理は、最も管理が難しい作業の1つです。これはDNSの使用が始まってから 20年以上が経過し、これまで様々な所有者やポリシー、ベンダーの変遷があったからであり、また、アドミニストレータが不確実なものを削除することに不安があるという問題も存在しています。企業にとって、全てのデジタル資産を把握し、重要なものや現在運用しているもの、重複しているもの (つまり不要なもの) を認識することは非常に困難です。さらに恐ろしいことに、CSCが管理している数千ものドメインポートフォリオを見ると、5件に1件は、DNSレコードがサブドメインの乗っ取りに対して無防備な状態で放置されています

主なポイント

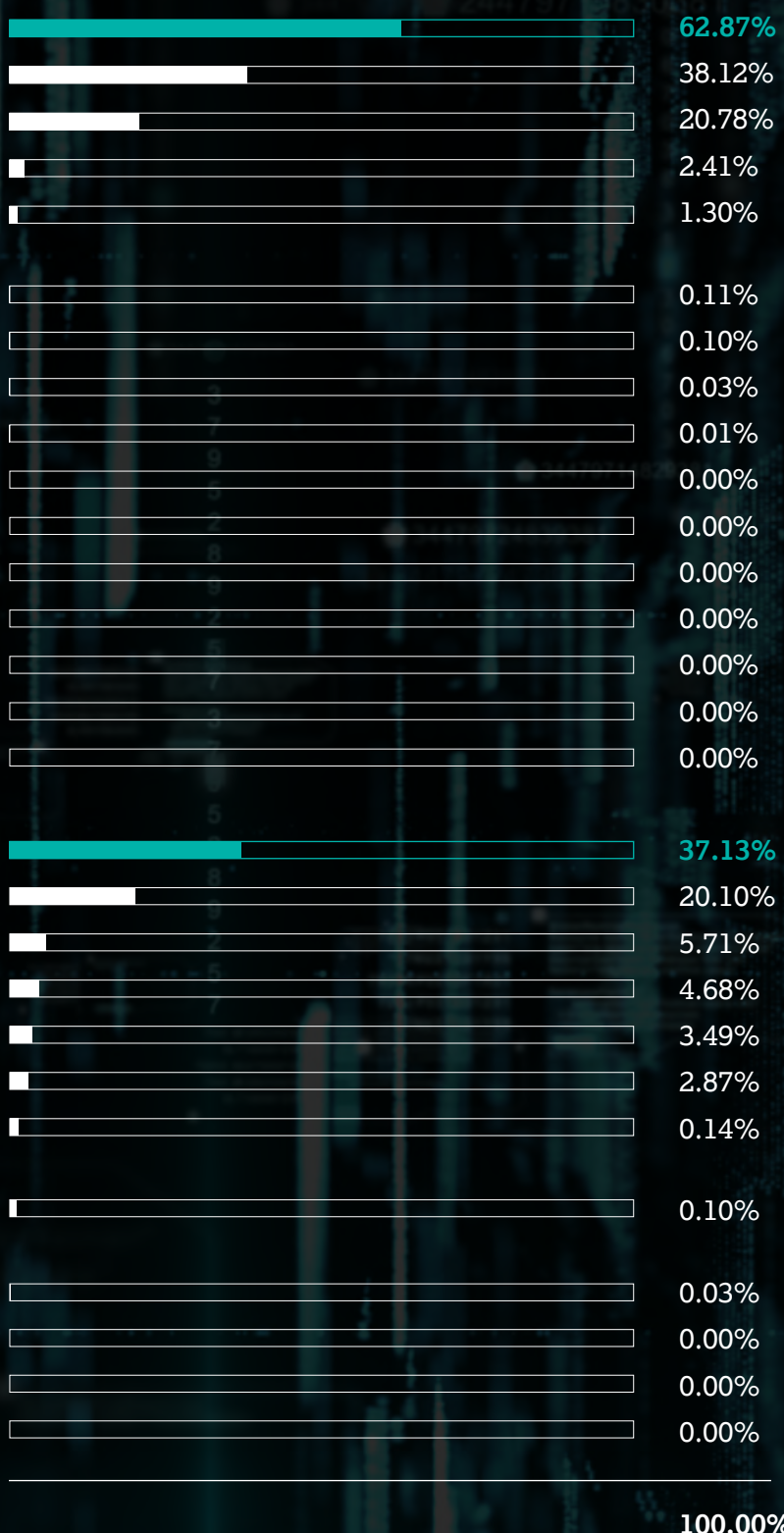
CSCは自社データベースから600万件を超えるDNSレコードを分析し、クラウドインフラストラクチャを指すAレコードとCNAMEを調べたところ、４４万件強のDNSレコードでサブドメインが乗っ取られる可能性があることがわかりました。これは、企業によるサブドメイン管理の現状を把握するために行ったもので、これら44万件のDNSレコードから、多くの企業がサブドメイン乗っ取りの被害の脅威にさらされていることが明らかになりました。

DNSレコードの21%が解決しないコンテンツを指定しています。これにより企業のサブドメインは乗っ取りに対して脆弱な状態になる可能性があります。

63%が、「404 not found」や「502 bad gateway」などのエラーを表示する。DNSレコードが設定されているドメイン名の多くが、不適切な応答を受け取っています。

38% という高い割合で「内部サーバーエラー」が表示されている。これは企業がDNSのハウスキープ処理とサイバーハイジーンを改善する必要があることを示しています。

分析したDNSレコード



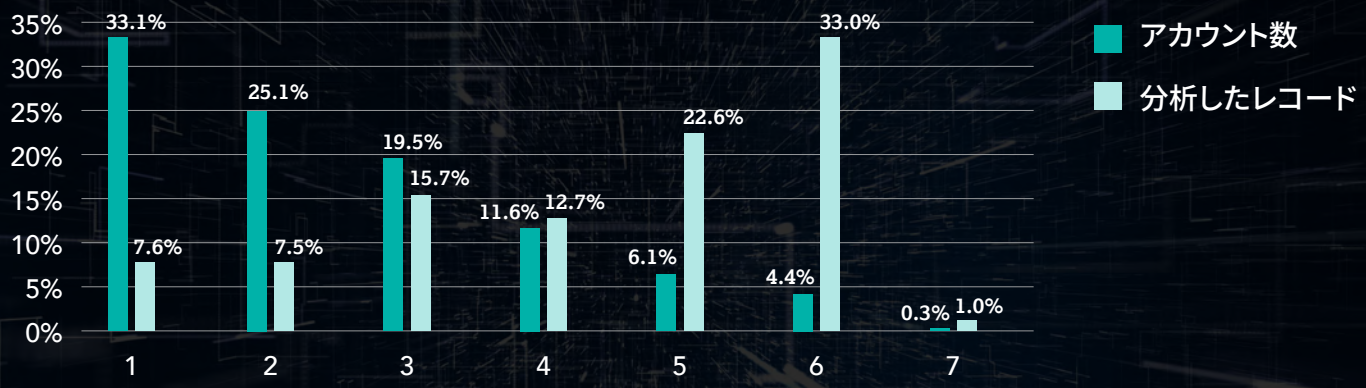
リスク要因:クラウドプロバイダ利用の普及

分析した全てのレコードのうち、**82% 以上**がクラウドプロバイダによってホストされていました。

このように高い割合となった背景には、ここ数年の間に、企業が従来の社内データセンタの利用から、クラウドプロバイダへの外注にシフトしているという状況があります。クラウドプロバイダを利用することで、新しいテクノロジーに簡単にアクセスし、アジャイルかつダイナミックに活動できるようになり、コスト効率も向上するからです。しかし、その一方で管理が必要なDNSレコードが大幅に増えることで、企業にとってはリスクも高まるのです。

リスク要因:大規模ポートフォリオを持つ企業におけるプロバイダ分散化

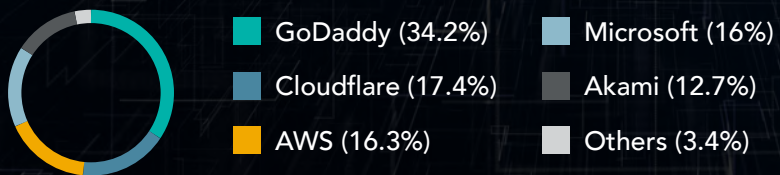
利用プロバイダ数



分析を行った企業のうち58%は、サブドメインを1〜2社のクラウドプロバイダに集約できているものの、それら企業は管理の利便性から、ポートフォリオを小規模にしている傾向があります。

一方、分析した企業の11%が5社を超えるクラウドプロバイダを利用していました。分析対象のDNSレコードの半数以上をこれらの企業が占めており、レコード数が数千という大規模ポートフォリオを保有している企業もあります。このような分析から、大規模ポートフォリオを保有する企業は、クラウドプロバイダの一元管理ができていない可能性があり、DNSレコードすべてを十分に監視することが困難になっています。

利用しているクラウドプロバイダの分布



分析した全DNSレコードの96%以上が、5大クラウドプロバイダ、すなわちGoDaddy®、Cloudflare®、AWS、Microsoft®、Akamai を利用しています。

サブドメインのモニタリングによりサイバー脅威を低減

様々なブランドのポートフォリオを保有し、グローバルにに事業を展開する大企業は、自社のデジタルフットプリントの規模を把握できていないことも多々あります。デジタルレコードは時間とともに蓄積され続けるため、サイバーハイジーンの維持は極めて困難です。

デジタルレコードと管理を適切に監視していなければ、「ノイズ」が蓄積され、シンプルだったはずのサイバーハイジーンとハウスキープ処理が複雑になり、サイバー犯罪者に安易に悪用される結果になりかねません。コンテンツを指していない非アクティブなゾーンの蓄積は「ダングリングDNS」と呼ばれ、サブドメインが乗っ取られる危険にさらされます。これによりフィッシング、マルウェア、ランサムウェアなど、その他のサイバー攻撃の脅威を招き入れることになり、ブランド評判に傷をつけ、消費者からの信頼喪失、さらに深刻なデータやセキュリティ侵害につながる恐れがあります。ドメインの履歴を知らないアドミニストレータは、これら残されたレコードが重要なインフラストラクチャと紐づいており、うっかり削除すると業務を停止させてしまうかもしれないとの不安から、削除をためらってしまうのです。

企業にとって、すべてのデジタル資産を把握し、重要なものや現在運用しているもの、重複しているもの (つまり不要なもの) を認識することはとても困難です。、20年以上の間に所有者、ポリシー、プロバイダの変遷や、アドミニストレータがよく分からないものを削除することに不安があることなどから、DNSレコードのハウスキープ処理は最も管理が難しい作業の1つなのです。

サブドメイン乗っ取りは、ドメインやDNSのハイジャック、ドメインシャドウイング、キャッシュポイズニングなど、ドメインセキュリティに対して、現在存在している多くの脅威の1つに過ぎません。これらの脅威は、さらに悪質なフィッシングやランサムウェア攻撃、BEC(ビジネスメール詐欺)、なりすましメール、さらにはデータ漏えいなどを可能にするための攻撃であることが多いのです。

CSCは、DNSレコードの変更が検出されたときにアラートを通知するだけでなく、サブドメイン乗っ取りを防止するために、情報に基づいた適切な判断と対応ができるよう、状況をお知らせするサブドメインモニタリングソリューションをすべての企業が導入することをお勧めしています。

CSCのサブドメインモニタリングソリューションの詳細についてはこちらをご覧ください。

CSC

CSCは企業向けドメイン名、ドメイン名システム（DNS）、デジタル証明書管理、デジタルブランド保護・詐欺防止サービスのプロバイダーとして、フォーブス誌「グローバル2000」や「世界で最も価値の高いブランド100　社」®に名前を連ねる多くの企業に選ばれています。グローバル企業はセキュリティ体制に多額の投資を行っており、CSCは、現在ある既知のサイバーセキュリティの脆弱性を把握し、企業のオンラインデジタル資産とブランドの保護を支援します。CSC　独自のテクノロジーを活用することで、企業はセキュリティ体制を強化することができ、オンライン資産とブランドの評判をターゲットとするサイバー脅威ベクトルから保護し、一般データ保護規則（GDPR）のような規制による甚大な収益の損失や多額の罰金を回避することができます。当社は、オンラインブランドモニタリングと保護活動を組み合わせたオンラインブランド保護、そしてフィッシング対策としてフラウド保護を提供するなど、デジタル資産保護に向けた総合的なサービスを展開しています。CSCは、1899年創業以来、米国デラウェア州ウィルミントンに本社を置き、米国、カナダ、ヨーロッパ、およびアジア太平洋地域にオフィスを構えています。CSCは、クライアントがどこにいてもビジネスを行うことができるグローバル企業です。また、CSCは、当社がサービスを提供しているすべての事業で専門家を雇用することでそれを実現しています。詳しくはcscdbs.com/jpをご覧ください。

DBS04052023