サイバーセキュリティレポート

2019年10月

Vincent D' Angelo *グローバルディレクター、コーポレートデベロップメントおよびストラテジーアライアンス*

Quinn Taggart *シニアドメインプロダクトマネージャー*

Ken Linscott *プロダクトディレクター、ドメインおよびセキュリティ*

Letitia Thian *マーケティング担当マネージャー*

CSC による調査と解説

この CSC サイバーセキュリティレポートは、サイバー犯罪とサイバーセキュリティに関する最も重要なすべての情報を抜粋して、包括的に解説します。1 つの報告書で最新情報を提供するので、お客様とお客様のブランドにとって重要なニュースに素早く目を通すことができます。今回の特集では、グローバルな防衛産業におけるドメイン名セキュリティ制御の採用に焦点を当てています。

ドメインセキュリティ

CSC は、65%以上のトップグローバルブランドを管理しています

CSC は、65%以上のトップグローバルブランド を(Interbrand®)管理しています。独自開発ツールを使用して、CSC は、企業のお客様のドメインポートフォリオでのセキュリティギャップとビジネスチャンスを明らかにするお手伝いをします。同様の方法で、ドメインセキュリティについてどのように対処しているかを知るために、世界中の組織のメインドメイン名を分析しました。

今回の特集では、グローバルな政府防衛請負業者に焦点を当てています。違反につながる政府機関や請負業者への継続的な攻撃は[1]、国家と国民の安全に影響を与える可能性があり、したがって、これらの問題の共有は絶対的に不可欠です。ドメイン名、DNSや証明書は、インターネットのインフラストラクチャを強化するものであり、適切な防衛で保護されていない場合、このインフラストラクチャに依存する機密性の高いアプリケーション、ツール、システムや情報は、悪意ある機関の手にわたる可能性があります[2]。

当社は24か国におよぶ大手グローバル防衛請負業者を分析し、この業界がドメインセキュリティ制御をどのように採用しているかを分析しました。

ドメインセキュリティと観察の動向

トップ100グローバル防衛請負業者のデータをベースに

DNSハイジャックの背景

当社の2019年は、米国サイバーセキュリティ・インフラストラクチャ庁からのDNSハイジャック警告[3]から始まりました。それ以降、ブライアン・クレブス氏[4]といった業界専門家や、英国のサイバーセキュリティセンター・NSCS[5]などの世界的政府機関から関連する警告が発せられました。これらの警告は、金融およびメディアセクター[6]に関するCSCのサイバーセキュリティレポートが示すように、DNSおよびドメイン名のハイジャック発生という進行中のリスクへの認識を高めました。

これらの攻撃の標的は、特定の業界、規模、または地理的位置の企業に限定されません。例えば、カリフォルニアに拠点を置く病院は最近、ドメイン名が盗まれ[7]、ウェブサイト、Eメール、アプリ、そして関連情報へのアクセスが遮断されました。

レジストラプロバイダー

29% コーポレートレジストラ

71% リテイルレジストラ

リスク

これまで、リテイルレジストラは頻繁にサイバー攻撃の標的になっています。特にコアドメイン向けには、企業は、技術レベルのセキュリティ、警戒の企業価値を浸透させるなど、従業員のトレーニングに多額の投資をし、悪意のあるコンテンツを識別する方法を知っているレジストラと提携する必要があります。

観測結果

13% はエンタープライズレベル DNS プロバイダーを使用しており、3% は DNSSEC を使用しています。

ドメイン名、電子メール、DNS、およびデジタル証明書に対する悪意のある攻撃が増加しています。したがって、評判の高いコーポレートレジストラとリテイルレジストラによるドメイン名ポートフォリオ全体の管理こそが、ドメイン名セキュリティの導入と監視をはるかに容易なものとします。更に、ドメイン名レジストラの制御、プロセス、ツール、およびセキュリティの定期的な評価は、組織のサイバーセキュリティ体制を前進させる重要な要素となります。

レジストリロック

13% レジストリロックオン

65% レジストリロックオフ

22% *レジストリロックなし

リスク

ロック解除されたドメインは、ソーシャルエンジニアリング攻撃を受けやすくなり、不正な DNS 変更につながることがあります。世界各地のレジストリにはロックサービスを提供していないレジストリもあるので、ドメインがロック解除されたままになることがあります*。

観測結果

13% がレジストリロックを導入しています。

レジストリロックは、ドメイン名の乗っ取りや、サイトをオフラインにしたり、ユーザーを悪意のあるコンテンツにリダイレクトしたりするDNSへの不正な変更を防ぎます。政府および重要な産業に対する継続的なDNSハイジャックリスクに基づき、防衛請負業者によるこの制御の採用は非常に低いものでした。

驚いたことに、コアウェブサイト、電子メール、DNSに同じドメイン名を使用し、レジストリロックの対象でもあった企業の69%はロックされていませんでした。

ドメインセキュリティと観察の動向

DNS プロバイダー

32% 内部DNS

13% コーポレートまたはエンタープライズ DNS

55% その他（ホスティングまたはリテイル DNS）

リスク

エンタープライズレベルではないDNSプロバイダーを使用すると、分散型サービス拒否（DDoS）攻撃、ダウンタイム、収益の損失などの潜在的なセキュリティ上の脅威が生じます。

DNSSEC

3% DNSSEC オン

97% DNSSEC オフ

リスク

ドメインネームシステムのセキュリティ拡張（DNSSEC）は最も費用対効果の高いセキュリティプロトコルの 1 つです。DNSSEC を導入しないことは、DNS の脆弱性につながります。例えば、攻撃者が DNS ルックアッププロセスのステップをハイジャックすると、ハッカーがインターネット閲覧セッションをコントロールして、ユーザーを詐欺サイトに誘導することができます。

HTTPS everywhere

77% HTTPS everywhere、採用

23% HTTPS everywhere、採用

リスク

安全な暗号化をすべてのオンライン取引処理で採用することにより、サイバー犯罪者が個人情報を盗んだり、あるいは、ユーザーのデバイス上にマルウェア（悪意のあるソフトウェア）をインストールするために、ウェブセッションをハイジャックすることや、ハッカーが情報漏洩につながるようなウェブ通信侵害すること、顧客データの窃盗、DDoS 攻撃、また、ウェブサイトの改ざん等のリスクを軽減することができます。

観測結果

13% はエンタープライズレベル DNS プロバイダーを使用しており、3% は DNSSEC を使用しています。

防衛請負業者がリテイルドメイン名レジストラの使用を好む傾向は、エンタープライズレベルではないDNSホスティングの使用によって拡大され、これによりDDoSおよび関連リスクへの露出が増加しています。当社の調査によると、防衛請負業者の13%がエンタープライズレベルのDNSプロバイダーを好み、32%近くが独自のDNSアーキテクチャを採用しており、55%がリテイルレベルのプロバイダーを採用しているようです。DNSSECは、ユーザーとウェブプロパティ間の全体的な通信を保護するもう1つの方法ですが、DNSSECの採用率は非常に低く、わずか3%でした。

デジタル認証の種類

4% EV

84% OV

12% DV

リスク

企業認証（OV、Organization Validation）および EV 認証（EV、Extended Validation） などの追加認証が必要な SSL タイプは、ドメイン認証（DV、Domain Validation）よりも危険にさらされる可能性が低くなります。

観測結果

84% が OV 証明書を使用していますが、依然として 12% は DV 証明書を使用しています。DNS と同様に、デジタル証

DNSがホームへの扉である場合、デジタル証明書が鍵を握ります。ロックが弱い場合、ドアがどれだけしっかりしているかは関係ありません。重要なリスク要因は、デジタル証明書の検証方法にあります。防衛請負業者の12%が最低レベルの検証が必要なドメイン検証（DV）を使用しています。つまり、ハッカーが内部電子メールにアクセスした場合、悪意ある目的で企業所有ドメインのデジタル証明書を簡単に有効にすることができます。

电子邮箱认证

25% DMARC

85% SPF

3% DKIM

リスク

ドメインベースのメッセージ認証、報告、適合（DMARC）、センダー・ポリシー・フレームワーク（SPF）、または、ドメインキー識別メール（DKIM）で電子メールチャンネルを認証して、電子メールスプーフィング詐欺と潜在的なフィッシング詐欺のインシデンスを最小限に抑えます。

観測結果

25% が DMARC を使用

DMARC は、会社の電子メールドメインが電子メールスプーフィング、フィッシングスカム、その他のサイバー犯罪で使用されないように保護する電子メール検証システムです。何百万というユーザーと通信する企業の採用率が低いことは驚きです。一部政府8ではDMARCの採用が義務付けられているため、防衛請負業者によるこのコントロールの採用を増やすことが推奨されており、これは電子メール通信に対する脅威に対処するのに役立ちます。

CAA レコード

4% CAAレコード採用

96% CAA レコード不採用

リスク

認証局認可（Certificate Authority Authorization、CAA）レコードは、ゾーンファイルにあるリソースレコードです。これを使用して、ドメイン所有者は、該当するドメイン名の証明書の発行を許可する認証局（CA）を指定できます。CAA レコードを追加することで、会社が使用する認証局（CA）を制御できます。CAA レコードを追加することで、会社が使用する認証局（CA）を制御できます。選択したプロバイダーのみがドメイン名の証明書を発行できることを保証し、ポリシーの実施とハイジャックされたサブドメインのHTTPSフィッシングなどのサイバー脅威の緩和を可能にする重要な技術的制御です。

観測結果

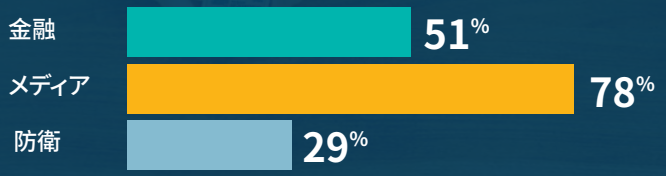
4%がCAAレコードを採用

防衛産業のCAAレコードを見ると、これら企業の4%しか採用していません。うち、半分に当たる企業はエンタープライズレベルではないリテイルベンダーによる証明書の発行を許可していました。これは、グローバルな公開企業を観察する際、CAAレコード採用率3%と比較することができます。

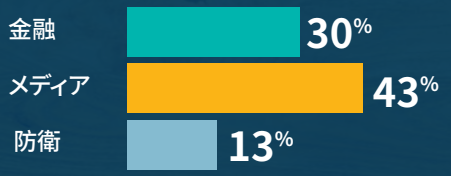
ドメイン名のセキュリティ管理: 防衛 vs メディア vs 金融

CSCの最後の2つのレポートは、金融およびメディアセクターに焦点を当てています。今回、グローバルな防衛請負業者に焦点を当てると、ドメイン名セキュリティのさまざまな要素、特にレジストリロック、企業ドメインレジストラの採用、エンタープライズDNSホスティングプロバイダー、およびDMARCの採用が遅れていることがわかります。CSCで以前説明したように、これらの制御の多くは業界のリーダーから推奨されています。

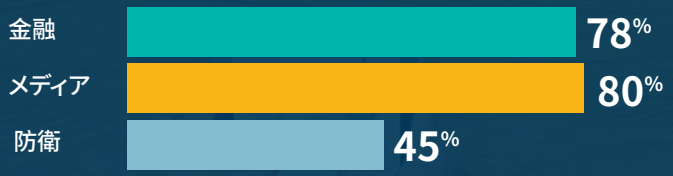
企業ドメインレジストラ



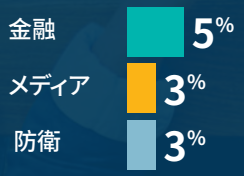
レジストリロックオン



エンタープライズまたは内部DNS



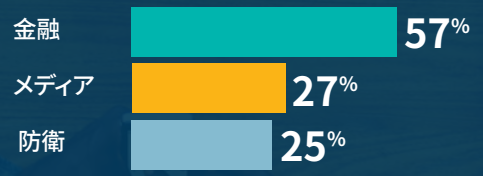
DNSSECオン



HTTPS EVERYWHERE

デジタル認証の種類(EV または OV)

DMARCオン



さらに、すべてのセキュリティ対策、特に単一侵害のコストに比べて多くのコストを要するわけではないものの、基本的なセキュリティ要素は、サイバー脅威の年毎の増加から予想される防衛部門による採用レベルに達していないことが依然としてわかります。厄介な点は、ドメイン全体のセキュリティとユーザーの信頼に対処する最も簡単なセキュリティ手法が、企業にとって実装が最も難しいと思われることです。

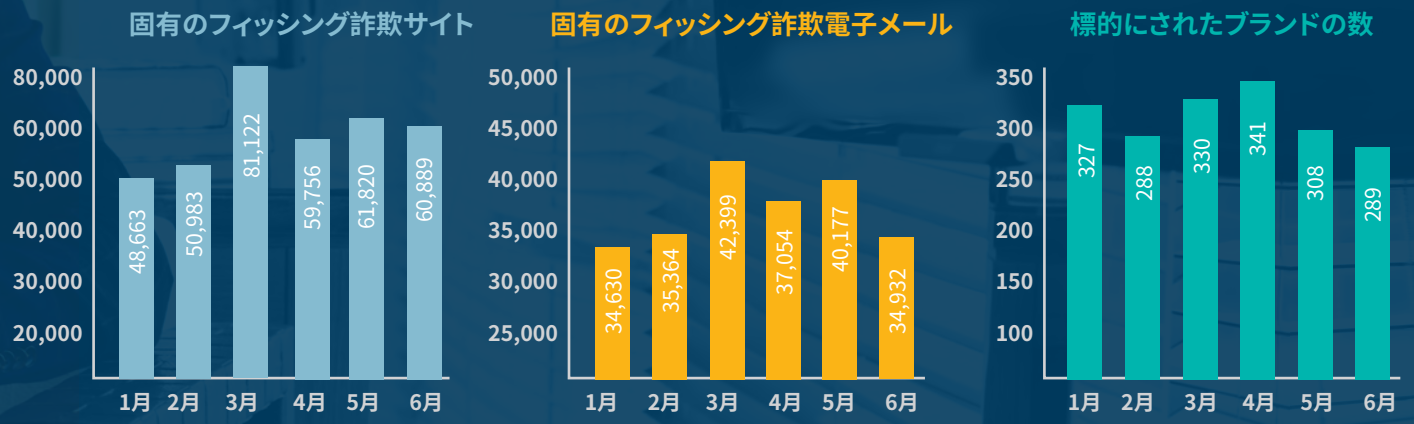
フィッシング詐欺 と電子メール詐欺

年間を通してのフィッシング詐欺サイトの急増

2019年第2四半期までに、フィッシング詐欺サイトの55%以上にデジタル証明書を有しており、ユーザーが安全なウェブサイトにアクセスしているかどうかを示す効果を無効なものとしました。フィッシング詐欺サイトは「HTTPS」でより正当化され、インターネットユーザーを騙し、消費者に対しインターネットセキュリティ機能が有効であるかのように見せかけ、個人のIDデータやアカウント資格情報が悪意をもって盗まれる事態をもたらしています。

フィッシング詐欺攻撃

2019年第2四半期のフィッシング詐欺サイト数は182,465で、前四半期からわずかに増加しました。ただし、2019年上半期の攻撃数は、2018年下半期よりも25%増加しました。



最も標的にされる業種

Software as a Service（SaaS）およびウェブメール、オンライン決済サービス、銀行および金融機関が、依然として2019年第2四半期のフィッシングの標的にされる業種トップ3となりました。

出典: APWG Phishing Activity Trends Report, 2nd Quarter 2019

フィッシング詐欺 サイトで最も使用されているトップレベルドメイン（TLD）

レガシー TLD — かなり前に多数のウェブサイトで確立された TLD です。多くのフィッシング詐欺をホストする傾向があります。しかしながら、再購入された国別コード TLD、および、しばしば低コストで提供される新しいジェネリック TLD も、他の世界中のすべてのドメインと比較して、大量のフィッシング詐欺をホストするのに使われています。

Type of TLD:

Legacy gTLD　ccTLD　New gTLD

↑ / ↓ 順位の変動　　+ / - 規模の変動

.com +714 → #1 • ドメイン数 2,812	.net +33 ランキング 3位から ↑ #2 • ドメイン数 208	.br +64 ランキング 8位から ↑ #3 • ドメイン数 146	.org -9 → #4 • ドメイン数 145
.uk +16 → .#5 • ドメイン数 137	.top #6 • ドメイン数 120	.info +36 → #7 • ドメイン数 119	.in +47 ランキング 11位から ↑ #8 • ドメイン数 105
.au #9 • ドメイン数 80	.xyz +26 ランキング 17位から ↑ #10 • ドメイン数 63	.icu #11 • 59 domains	.cl #12 • ドメイン数 47
.ga -21 ランキング 10位から ↓ #13 • ドメイン数 47	.ml -35 ランキング 9位から ↓ #14 • ドメイン数 43	.cf -43 ランキング 6位から ↓ #15 • 41 domains	.co #16 • ドメイン数 41
.ru -6 ランキング 13位から ↓ #17 • ドメイン数 38	.pl +9 ランキング 19位から ↑ #18 • ドメイン数 37	.id #19 • ドメイン数 36	.it -1 ランキング 16位から ↓ #20 • ドメイン数 36

出典: APWG Phishing Activity Trends Report, 2nd Quarter 2019

すべての組織が危険にさらされています

報道に見る事例

米国

DNSインフラストラクチャの改ざんを緩和

米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁は、一連の改竄事件を追跡し、DNSレコードの監査、およびDNSハイジャックを緩和するためのポータルアクセスの保護などの必要なアクションを採用するために、連邦政府機関に緊急指令を発令しました。

cyber.dhs.gov/ed/19-01/

メインネームシステムに対する攻撃の公開レポートに関する警告

ICANN（The Internet Corporation for Assigned Names and Numbers）は、DNSSECなどのベストプラクティスと対策、およびDNSを対象とする悪意のあるアクティビティからシステムを保護するレジストリロックを実装するよう組織に警告を発しました。

icann.org/news/announcement-2019-02-15-en

最近の広範囲にわたるDNSハイジャック攻撃の詳細

KrebsOnSecurityは、複雑で広範囲にわたるDNSハイジャック攻撃を調査し、その起源と範囲を分析し、主要なインターネットインフラストラクチャプロバイダーの侵害により世界中の政府が影響を受けていることを表明しました。

krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

シークレットサービスが米国政府IT請負業者の侵害情況を調査

20社以上の連邦政府機関のIT請負業者が、電子メールの添付ファイルからのマルウェアにより、影響を受けた機関のデータベースへのアクセスを許可する可能性のある電子メール通信と資格情報への侵害を受けました

krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

英国

継続的なDNSハイジャックと緩和へのアドバイス

英国国立サイバーセキュリティセンターは、大規模なグローバルDNSハイジャックキャンペーンで、引き続き複数の地域やセクターに影響を与える活動についての勧告を発表し、レジストラ、ネームサーバー、およびウェブアプリケーションセキュリティに関する緩和へのアドバイスを提供しました

ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

ブルガリア

国全体がハッキングされる

ブルガリア国税庁がハッキングされ、700万人の人口を持つ国において500万人もの個人データと財務記録が侵害されました

edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/

エクアドル

エクアドルのほぼ全国民がデータ侵害被害に

大統領を含むエクアドルの約2,000万件の詳細な個人情報が、政府レジストリやその他組織からのデータとともに、地元の請負業者のサーバーに公開されたままとなっていました。

engadget.com/2019/09/17/ecuador-data-breach-20-million-citizens/

オーストラリア

ACSC、政府の重要インフラストラクチャに保護DNSサービスを展開

オーストラリアのサイバーセキュリティセンターは、地方自治体および重要なインフラストラクチャで採用される保護DNSサービスを試験的に実施しています。

itnews.com.au/news/acsc-to-deploy-protective-dns-service-for-govt-critical-infrastructure-520138

推奨事項

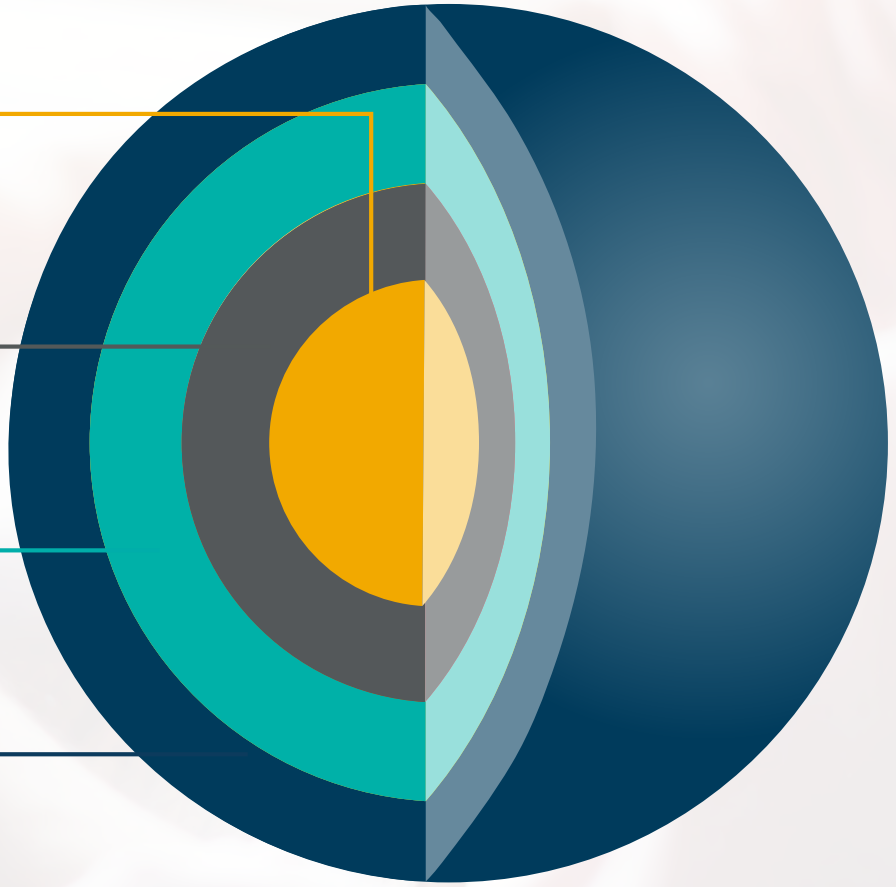
多層防御(DiD)アプローチ

ビジネスクリティカルドメイン向けの高度なセキュリティ機能を採用
マルチロック、DNSSEC、HTTPS、DMARC、CAAレコード

ユーザー権限の制御
昇格アクセス許可と通知の可視性

安全なポータルアクセス
IP検証、2要素認証、フェデレーションID

エンタープライズクラスプロバイダー
システム、スタッフ、ポリシー、プロセス



CSC は、ドメイン名、DNS、デジタル証明書などの基本的なインターネット資産内に存在する盲点を開示することにより、セキュリティ体制に多大な投資を行っている企業をサポートします。CSCは独自のセキュリティソリューションを活用することで、企業をサイバー資産からのデジタル資産への脅威から保護し、GDPRなどのポリシーにより、収益の損失、ブランドへの中傷、重大な経済的ペナルティを回避します。CSCは、インターネット資産と共に、偽造サイト、詐欺、IP侵害を介して悪用されるオンラインブランドを保護、監視および緩和し、多くの世界最大手ブランドの保護およびアドバイザリーサービスを提供しています。詳細につきましては、*cscdigitalbrand.services/jp*をご覧ください。

参照

1.krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

2.cscglobal.com/cscglobal/pdfs/DBS/Digital-Asset-Security-Checklist-EN.pdf

3.us-cert.gov/ncas/alerts/AA19-024A

4.krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-DNS-hijacking-attacks/

5.ncsc.gov.uk/news/ongoing-DNS-hijacking-and-mitigation-advice

6.cscglobal.com/cscglobal/pdfs/DBS/Cyber-Security-Report-June-2019-EN.pdf

7.beckershospitalreview.com/cybersecurity/hackers-steal-california-hospital-s-website-domain-email-addresses.html

8.eweek.com/security/dmarc-email-security-adoption-soars-as-us-government-deadline-hits