サイバーセキュリティレポート

2019 年 6 月

ケン・リンスコット（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

クイン・タガート（Quinn Taggart） シニアドメインプロダクトマネージャー

レティシア・ティアン（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。

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。

この号では、メディア産業を取り扱います。技術が変化し、オンデマンドコンテンツを利用する顧客が増えていることから、メディアの従来の形態はデジタルおよびモバイル形式に替わりました。例えば、ソーシャルメディア、オンラインストリーミング、インターネット広告などは、この変化の時代の過去 25 年間に生まれました。多くのメディアブランドがオンラインプレゼンスを有し、多くの顧客データを収集しています。会社がログインおよび決済情報を収集していることに加えて、メディア配信経路がサイバー攻撃によって遮断されたり、ハイジャックされる可能性もあります。ブランドは、ブランドと顧客を攻撃と侵害から保護する措置を直ちに施すことが不可欠です。

世界中の最大手メディア・コングロマリット数社とそのエンティティ、広告、出版、テレビ、ラジオなど経路全体のブランド、および、オンラインだけのブランドを分析し、メディア産業がドメインセキュリティをどのように取り入れているかを調査しました。

ドメインセキュリティと観察の動向

120 のメディアブランドに基づきます。

CSC の最後のレポートでは、金融および保険セクターを取り扱いました。今回は、メディアに焦点を当てて、それぞれのセクターがドメインセキュリティのさまざまなエレメントをどのように重視しているかを調査します。すべてのセキュリティ対策に多額の費用が掛かる訳ではありません。特に、1 度侵害された場合に要する費用と比較すると多くありません。しかしながら、依然として、基本的なセキュリティエレメントで、年間を通してサイバー脅威が増加したにもかかわらず、期待される導入レベルに達していません。厄介なのは、ドメインセキュリティ全体およびユーザー信頼度に対応する最も簡単なセキュリティテクニックの導入が企業にとって最も難しいことです。

レジストラプロバイダー

78% コーポレートレジストラ

22% 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

メディア産業の 78% はコーポレートレジストラを使用しています。
基本レベルのドメインセキュリティを評価する際には、ロック、電子メール、ドメインネームシステム（DNS）、セキュアソケットレイヤー（SSL）などいくつかのキーエレメントを精査する必要があります。勿論、ドメインポートフォリオ全体を信頼できるコーポレートレジストラが管理すれば、リテイルレジストラと比較して、これらのエレメントのいくつかは大変容易に導入できます。これが、メディア産業がコーポレートレジストラを使用してドメインポートフォリオを管理している理由であると考えられます。

レジストリロック

43% レジストリロックオン

37% レジストリロックオフ

20% *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

43% がレジストリロックを導入しています。
これらのロックは、DNS に不正な変更が加えられて、サイトがオフラインになったり、ユーザーが悪意のあるコンテンツに誘導されることを防止するので、人気が高まっています。

DNS プロバイダー

25% 内部 DNS

55% コーポレートまたはエンタープライズ DNS

20% 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以外のレベルの DNS プロバイダーは、潜在的なセキュリティの脅威（DDoS 攻撃など）を引き起こし、ダウンタイム（停止時間）や収益損失につながります。

常時 SSL

78% 常時 SSL、採用

22% 常時 SSL、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。

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。

観測結果

55% 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。

コーポレートレジストラの選択が、エンタープライズレベル DNS プロバイダーの選択につながっているようです。メディアブランドのおよそ半数が、エンタープライズレベル DNS プロバイダーを使用しています。およそ 25% が自社の DNS アーキテクチャーを使用しており、20% がリテイルプロバイダーを使用しています。DNS は企業が品質と信頼性について節約してはならない領域の 1 つであることは確かです。DNS はオンラインプレゼンスの後ろにあるエンジンです。DNSSEC は、ユーザーとウェブプロパティの間の通信全体を保護するもう 1 つの方法ですが、DNSSEC の採用率は大変低くわずか 3% です。

SSL タイプ（EV、OV、または、DV）

2% EV

74% OV

24% 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

74% が OV 証明書を使用していますが、依然として 24% は DV 証明書を使用しています。

DNS と同様に、デジタル証明書を節約することは賢明ではありません。DNS が家に入る扉だとしたら、SSL は鍵です。扉がどんなに堅牢でも、鍵がしっかりしていなければ意味がありません。主なリスク要因は SSL が検証される方法にあります。最も低いレベルの検証が必要なドメイン検証は、メディアブランドの 24% で使用されています。これは、もしもハッカーが内部電子メールにアクセスすれば、悪意のある目的のために、会社所有のドメイン上にある SSL を簡単に検証できることを意味します。これが、リテイルレジストラ GoDaddy® 経由の最近のハッキングの理由でした。

電子メール認証

27% DMARC

79% SPF

6% 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

27% 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

フィッシング詐欺 と電子メール詐欺

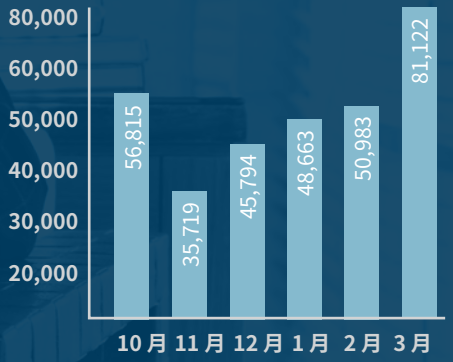
年間を通してのフィッシング詐欺サイトの急増

2019 年第 1 四半期には、フィッシング詐欺サイトの約 58% が SSL 証明書を使用していました。これは、前四半期比 46% 増という大幅な増加でした。2016 年年末に SSL 証明書を使用しているフィッシング詐欺サイトは 5% 未満でした。この増加の考えられる理由は 2 つあります。まず、攻撃者は自由に利用できるドメイン検証済みの証明書を作成できます。次に、一般に、SSL を使用するウェブサイトが増えており、ハッキングされた正規のサイト上でホストされたフィッシング詐欺、SSL を使用するフィッシング詐欺サイトの数も増えました。フィッシング詐欺サイトは「HTTPS」があるとより合法的に見えるので、インターネットユーザーをだまし、インターネットセキュリティ機能で消費者が保護されないようにして、悪者が個人の識別データやアカウントのクレデンシャル情報を盗むことができるようにします。

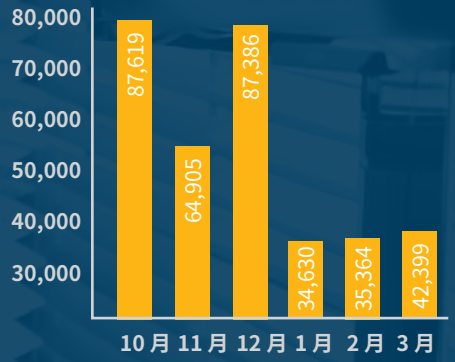
フィッシング詐欺攻撃

2019 年第 1 四半期のフィッシング詐欺サイトの数は 180,768 であり、前四半期比で 31% 増加しました。

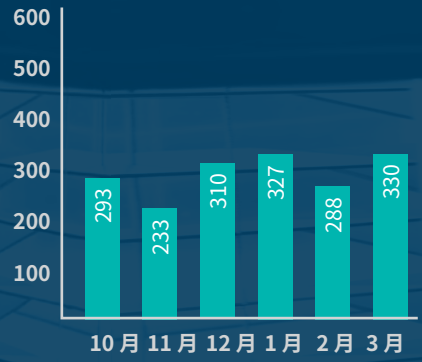
固有のフィッシング詐欺サイト



固有のフィッシング詐欺電子メール



標的にされたブランドの数



最も標的にされてる業種

初めて、ソフトウェア・アズ・ア・サービス（SaaS）とウェブメールのカテゴリが 、フィッシング詐欺の最も標的にされた業種になりました。オンライン決済と金融機関は、引き続き、2019 年第 1 四半期にフィッシング詐欺の最も標的にされたトップ 3 の業種でした。

出典: 2019 年第 1 四半期のフィッシング対策実務者グループ（APWG）
フィッシング詐欺動向レポート（Phishing Activity Trends Report）

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。

TLD のタイプ:

レガシー gTLD　ccTLD　新 gTLD

.com #1 • ドメイン数 2,098	.pw #2 • ドメイン数 374	.net #3 • ドメイン数 175	.org #4 • ドメイン数 154
.uk #5 • ドメイン数 121	.cf #6 • ドメイン数 84	.info #7 • ドメイン数 83	.br #8 • ドメイン数 82
.ml #9 • ドメイン数 78	.ga #10 • ドメイン数 68	.in #11 • ドメイン数 58	.us #12 • ドメイン数 45
.ru #13 • ドメイン数 44	.tk #14 • ドメイン数 40	.gq #15 • ドメイン数 37	.it #16 • ドメイン数 37
.xyz #17 • ドメイン数 37	.online #18 • ドメイン数 33	.pl #19 • ドメイン数 28	.ca #20 • ドメイン数 26

出典: 2018 年第 4 四半期のフィッシング対策実務者グループ（APWG）フィッシング詐欺動向レポート（Phishing Activity Trends Report）

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

米国の大手新聞社が Ryuk ランサムウェア攻撃で壊滅的な影響を受けました。

ランサムウェアが大手新聞社のインフラストラクチャを無効にして、出版および印刷新聞の配達に影響を及ぼしました。

csoonline.com/article/3330645/major-us-newspapers-crippled-by-ryuk-ransomware-attack.html

米国

Newsquest のウェブサイトがセキュリティ侵害の危険にさらされました。

メディアグループのウェブサイトの何百というタイトルがマルウェア（悪意のある不正ソフトウェア）に感染しました。このマルウェアは、ユーザーがローカルニュースへのアクセスを試みると、モバイルおよびウェブブラウザーをハイジャックして、“賞品を獲得するチャンス”という内容の無関係なウェブサイトにユーザーを誘導しました。

uknip.co.uk/2019/02/newsquest-websites-compromised-by-security-breach/

フランス

ビデオシェアリンクプラットフォームが クレデンシャルスタッフィング攻撃の標的になりました。

サイバー犯罪者がビデオシェアリングプラットフォームをクレデンシャルスタッフィング攻撃（または、ブルートフォースアタック（総当たり攻撃））の標的にしました。ブルートフォースアタック（総当たり攻撃）とは、データ侵害から得たパスワードを推測したり再使用して、ユーザーのアカウントをハイジャックする攻撃手法です。

securityboulevard.com/2019/01/video-sharing-platform-targeted-by-credential-stuffing-attacks/

フィリピン

大規模な資金力のあるテックチームがPH オルタナティブ・メディアのウェブサイトを攻撃しました。

政治的な動機に基づくハクティビストが、フィリピンのメディアウェブサイトを標的にして、毎週最大 40 の攻撃を開始して、通常のトラフィックの 40,000 倍のサイズの DDoS 攻撃を行いました。

news.abs-cbn.com/news/02/07/19/big-rich-tech-teams-attack-ph-alternative-media-websites

米国

新しい Mirai マルウェア亜種が Signs TV と Presentation Systems を標的にしました。

研究者は、エンタープライズ IoT デバイスを標的とする Mirai ボットネットの新種が、2016 年の DNS プロバイダーに対する Mirai 攻撃と同様の大規模な DDoS 攻撃を開始する可能性があることを発見しました。2016 年の DNS プロバイダーに対する Mirai 攻撃では、北米および欧州の主なウェブサイトおよびインターネットサービスが中断しました。

zdnet.com/article/new-mirai-malware-variant-targets-signage-tvs-and-presentation-systems/

推奨事項

1.ドメインを自動更新する

リテイルレジストラの場合は、ファイル上のクレジットカードの有効期限が切れたりキャンセルされても、自動更新は決定されていないので、ドメインがオフラインになり、悪くすると、ドメインが削除されます。コーポレートレジストラと提携すれば、企業が特定のドメインを更新しないことを明示的に指示しない限り、ドメイン は自動的に更新されるので、ドメインがドロップする心配がありません。

cscdigitalbrand.services/blog/an-abandoned-domain-name-could-hurt-you/

2.重要なドメインをロックする

コーポレートレジストラと提携するもう 1 つの理由は、サポート構成です。つまり、技術と産業を知る専門家の組み合わせのバランスです。重要なドメインをロックするために、企業は、どのドメインが重要であるか、どのドメインが明らかでない可能性があるかを知る必要があります。CSC Security CenterSM は、重要なドメインを特定して、トラフィック以外のことも調べ、レイヤーセキュリティの複数のベクトルを分析する技術を提供します。

cscglobal.com/service/csc/press-csc-alerts-companies-to-increased-dns-hijacking/

3.ドメインセキュリティ措置を施す

しっかりとした基盤がなければ、要塞は崩れます。コーポレートドメインレジストラと提携すれば、ドメインポートフォリオを丁寧に検査して、保護措置が取られているかどうかを確認します。セキュリティ・ランドスケープは絶え間なく変化しています。戦略を発案するために、専門の信頼できるパートナーが不可欠です。セキュリティは一度対応すればそれで終わりというものではありません。サイバー犯罪者も新しい攻撃テクニックを開発しているので、 周期的に対応しなければなりません。

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-5/

4.その他の関係者が関与する

ドメインセキュリティとポートフォリオ管理は 1 人が担当する仕事ではありません。マーケティング、法務、ブランド管理、IT などの関係者に関わることです。ドメインポートフォリオの管理については、皆の意見が重要です。セキュリティは皆に関わることです。CSC は、企業がドメイン評議会を設置することを推奨します 。

5.取締役会が DNS リスクを知る

世界的な攻撃や規模の大きい侵害が増加していることから、法規制の遵守に加えて、サイバーセキュリティは取締役会にとって最優先課題になっています。Business Continuity Institute Horizon Scan Report で特定されたリスクのうち、DNS がトップ 10 リスク中の 4 つのリスクの寄与因子です。

cscdigitalbrand.services/blog/dns-the-neglected-building-block-part-6/

CSC は、クライアント企業がオンラインで成功するお手伝いをします。CSC は、クライアントの価値あるブランド資産を効率的に管理、促進し、オンライン世界の脅威から保護するお手伝いをします。CSC® は、Interbrand® 100 ベストグローバルブランドの 65% を超える企業など、多数の大手企業からパートナーとして信頼されてきました。最新の技術を採用したデジタルブランドサービス（Digital Brand Services）は、独自のアカウント管理システムで素晴らしい成果をお届けします。CSC の専門家と専門チームが、21 世紀に成功を収めるために貴社のブランドが必要とする強さを確固たるものにするサービスをご提供します。CSC は、貴社のブランドを統合、保護、監視、権利行使、最適化、促進し、デジタルプレゼンスを最大化して、デジタル時代の知的資産を保護し、コストを削減するお手伝いをします。

cscdigitalbrand.services/jp