DNS の不正使用手法に対抗するためのマトリックス

FIRST DNS Abuse Special Interest Group

https://www.first.org/global/sigs/dns

はじめに

本レポートは、FIRST の DNS Abuse SIG(Special Interest Group)によるもので、DNS の不正使用(DNS Abuse)を伴うインシデントに対応するインシデント対応チームに向けたアドバイスを提供する。何が DNS の不正使用で、何がそうでないかの境界を歯切れ良く定義することは難しい。多くの組織が DNS の不正使用の定義に関して、フィッシング、マルウェア、迷惑メール、ボットネット、詐欺の何らかの組み合わせに関するもの、あるいはこれらの不正使用方法の一部またはすべての組み合わせに関連するもの、などの議論を重ねてきた。FIRST DNS Abuse SIG は、これらの分類は実用的なアドバイスをインシデント対応者に与えてはいないと認識している。そこで本レポートは、インシデント対応者やセキュリティチームが目にするであろうインシデントで使用される手法の一般的な例を提示すること、また不正使用で使用される特定の手法をインシデント対応者が検知、緩和、抑止するうえで手助けとなりえるステークホルダーのリストを提供することにより、DNS の不正使用の調査・研究における既存の取組を補完することを目標とする。

現在、アドバイスは、特定のステークホルダーが特定の手法に関して直接支援できるかどうかを示すマトリックスの形で与えられる。ここでの「支援」とは、そのステークホルダーが不正使用手法を検知、緩和、抑止できる立場にあるかどうかを意味する。この情報を、インシデント対応行動(検知、緩和、抑止)を網羅する 3 つのスプレッドシートにまとめた。例えば、DNS キャッシュポイズニングを伴うインシデントの際、緩和のスプレッドシートに移動して DNS キャッシュポイズニングの行を参照すれば、インシデント緩和の支援を得るために連絡できるステークホルダーを見つけることができる。

DNS エコシステムは複雑で、多数のステークホルダーと運用モデルが存在する。リストに挙げられた不正使用手法の中には無害な使用法も存在するので、「これらの手法は絶対に許容されるべきではない」というほど単純なものではない。しかし、インシデント対応の文脈ではインシデントが発生しているという前提があるので、攻撃者がインシデントを仕掛けるまたは維持するために使用した手法が何であれ、それらは悪意あるものか、組織のセキュリティポリシーに違反するか、あるいはその両方にあてはまる。インシデント対応者は、権限範囲内で責任を持って証拠保全を行うということに徹するべきである。DNS Abuse SIG は、リストに挙げられた手法のいずれかが一般に DNS の不正使用にあたるものであるかどうかの判断は示さない。本レポートは、特定のインシデントにおいて、ある手法が悪意を持って使用されているとの前提で、インシデントを検知、緩和、抑止する行動ができるのは誰なのかを明らかにするという観点から構成されている。

DNS が関与する攻撃と並行して、いくつかの手法が使用される場合がある。例えば BGP ハイジャックや TLS 証明書のなりすましといったものである。これらの手法は対象範囲外とし、本文書は DNS の不正使用手法にだけ焦点を当てる。

本文書のこのバージョンには含まれていないが、インシデント対応の際に連絡可能な他のポリシー関連、政府、司法の関係組織があることに留意しておくと有用だろう。例えば、サイバー犯罪に関する条約や他の国際協定には、国境を越えた証拠の押収とインフラの一時停止をどちらも行える仕組みがある。外国の法執行機関の捜査官が行う作業の第 1 段階は、大抵の場合、正式な法(刑事共助条約)に基づく要請が保留されている間にデータが消失しないようにするための非公式な保全要請になるだろう。

用語

3 次元マトリックス(行動、手法、ステークホルダー)では、以下で定義する用語を使用する。

行動

以下の定義において、CSIRT が提供している可能性のあるサービスについては、FIRST CSIRT サービスフレームワーク v2.1 と連動している。

- **検知** – インシデントの可能性がある事象を特定する。サービス: 監視と検知、インシデント報告の受理。注: インシデント管理において、インシデント対応(IR)チームが追加の検知ツールやシグネチャの確認、収集を望む段階は、緩和段階であり検知段階ではない。検知行動は、インシデントの最初の検知のみに焦点を当てている。
- **緩和** – インシデントを封じ込め、安全な運用を回復させる。サービス: 緩和と復旧。
- **抑止** – DNS 固有の作業手順を適用し、将来におけるこの種のインシデントの発生確率を下げる。サービス: 知識の移転(組織内 IT チームへの移転も含む)、脆弱性対応。検知にも関連し(おそらくはシグネチャや検知ルールの更新)、復旧にも関連する(復旧作業時、再発防止のためにシステムを再設定する場合)。広範なマルウェア抑止は本文書の対象範囲外であることに注意して欲しい。もちろん、広範なマルウェア対策は誰もが行うべきである。例えば、M3AAWG によるベストプラクティスを参照。

手法

1. DGA (ドメイン生成アルゴリズム) – 詳細については https://attack.mitre.org/techniques/T1568/002/ 参照。

2. ドメイン名の侵害 – ドメイン名の正当な保有者から管理権限を不当に奪う。侵害されたドメインは、さまざまな悪意ある行為、例えば SPAM の送信、フィッシング、マルウェアの配布、ボットネットのコマンド＆コントロール(C2)などに使用される可能性がある。詳細については https://www.icann.org/groups/ssac/documents/sac-007-en 参照。

3. lame delegation(レイムデレゲーション)– ネームサーバーのドメインの有効期限が切れると lame delegation が発生する。攻撃者は期限が切れたネームサーバーのドメインを再登録することにより、そのドメインの管理権限を得られる。詳細については https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/ 参照。

4. DNS キャッシュポイズニング – DNS スプーフィングとも呼ばれる。サイバー攻撃の一種で、攻撃者が偽の DNS レコードを注入することによって DNS リゾルバーのキャッシュを汚染し、攻撃者に制御されたレコードをリゾルバーに保存させる。詳細については https://capec.mitre.org/data/definitions/142.html 参照。

5. DNS リバインディング – 悪意ある Web サイトがクライアントをローカルネットワークアドレスに誘導し、攻撃者が同一生成元ポリシーを迂回して被害者のローカルリソースへのアクセスを得られるようにする。詳細については https://capec.mitre.org/data/definitions/275.html 参照。

6. DNS サーバーの侵害 – 攻撃者が、オープン再帰 DNS サーバー、権威 DNS サーバー、組織の再帰 DNS サーバー、ISP が運用する再帰 DNS サーバーなどの管理者権限を取得する。

7. スタブリゾルバーのハイジャック – 攻撃者が、DNS 問い合わせを傍受して不正な応答または悪意ある応答を返す悪意あるコードにより、コンピューターや携帯電話のオペレーティングシステムを侵害する。

8. ローカルな再帰リゾルバーのハイジャック – 家庭用ルーターなどの顧客構内設備(CPE)は、しばしばローカルネットワークに対して DNS 再帰検索サービスを提供する。CPE 機器が侵害されると、攻撃者は応答を改変するなどして再帰リゾルバーの振る舞いを変えられるようになる。

9. オンパス(on-path)の DNS 攻撃 – 攻撃者がユーザーと DNS サーバー間の通信を傍受し、悪意あるサイトを指し示す異なる宛先 IP アドレスを指定する。(https://www.imperva.com/learn/application-security/dns-hijacking-redirection/)

10. DNS に対する DoS – ターゲットの DNS サーバーに対して複数のシステムが悪意あるトラフィックを同時に送信する。

11. DoS を目的とした DNS サーバーの不正使用 – 攻撃者は、大量のネットワークトラフィックをターゲットに反射させることで、サービス妨害を引き起こそうと試みることがある。この種のネットワーク DoS は、サー

ビスをホストしており、偽装された送信元 IP アドレスに応答する第三者のサーバーを仲介者として利用する。このサーバーは、一般にリフレクターと呼ばれる。攻撃者は、被害者のアドレスに偽装されたパケットをリフレクターに送信することにより、リフレクション攻撃を達成する。反射・増幅・フラッドを可能にしたプロトコルでは、DNS と NTP の 2 つが突出しているが、他にもいくつかのプロトコルが実世界で使用されたと文書に記録されている。これらの反射や増幅によるフラッドを権威 DNS サーバーのような DNS の構成要素に誘導すれば、それらを応答不能にできる。(https://attack.mitre.org/techniques/T1498/002/)

12. 動的な DNS 解決による検知の難化 – 攻撃者は、一般的な検知・修正を回避するため、コマンド＆コントロールインフラへの接続を動的に確立する場合がある。これは、攻撃者がマルウェアからの通信を受信するために使用するインフラとマルウェアの間で、共通のアルゴリズムを使用することで達成できる。これらの演算を使用して、マルウェアがコマンド＆コントロールと通信するために使用するドメイン名、IP アドレス、ポート番号などを動的に調整することができる。(https://attack.mitre.org/techniques/T1568/)

13. 動的な DNS 解決(Fast flux)による隠ぺい – 攻撃者は、Fast flux DNS を使用して、単一のドメイン解決に割り当てられた素早く変化する多数の IP アドレス群の中にコマンド＆コントロールチャネルを隠ぺいする場合がある。この手法は、完全修飾ドメイン名(FQDN)と、そのドメイン名に割り当てられた複数の IP アドレスを使用する。これらの IP アドレスは、ラウンドロビン機能と DNS リソースレコードの短い TTL(Time-To-Live)を組み合わせることで、高い頻度で入れ替わっていく。
(https://attack.mitre.org/techniques/T1568/001/)

14. DNS を介した情報の不正な持ち込みおよび持ち出し – DNS を介した不正な情報の持ち出しは、委任されたドメインを必要とする。パブリック DNS 内にドメインが存在しない場合は、ドメインのゾーンファイル情報があらかじめロードされており、侵害された機器が送信する問い合わせを受信して応答するように設定されたリゾルバーの運用が必要となる。

15. (実効的)セカンドレベルドメインの悪意ある登録 – 例えば、攻撃者が被害者を攻撃する前に、ターゲティング時に使用できるように、ICANN が認定したレジストラーからドメインを購入する、あるいはレジストラーにドメインを登録する。CAPEC-630 も参照。

16. ダイナミック DNS プロバイダーを介した悪意あるサブドメインの作成 – 攻撃者が被害者を攻撃する前に、レジストリやレジストラー以外で自分が保有、管理をしているドメイン下位のサブドメインを提供しているエンティティからドメインを購入する、あるいはそこでドメインを作成する。
https://en.wikipedia.org/wiki/Dynamic_DNS も参照。

17. DNS の不正使用を目的とした DNS 以外のサーバーの侵害 – インターネット攻撃のインフラは多岐にわたり、そこには DNS 以外のあらゆるサーバーが含まれる。侵害された多数のサーバー、例えば Web サーバーやメールサーバーなどは DNS とのやり取りを行っており、DNS の不正使用の実施に関与することがある。例えば、フィッシングメールの送信に使用される可能性がある方法の 1 つに、メールサーバーの侵害が挙げられる。

18. 未登録ドメイン名を介したなりすまし – ドメイン名が期待されるコンテキスト(メールの From ヘッダー、Web ページやメール本文に含まれる URL など)において、**攻撃者が管理しておらず、正当な登録者も管理していないまたは登録していないドメイン名**を指定する。

19. 登録されたドメイン名のなりすまし – ドメイン名が期待されるコンテキスト(メールの From ヘッダー、Web ページやメール本文に含まれる URL など)において、攻撃者は管理していないが、**実際に正当な登録者が管理しているかまたは登録したドメイン名**を指定する。

20. DNS トンネリング – DNS 上での他のプロトコルのトンネリング – DNS プロトコルは、コンピューターネットワークにおいて管理機能を提供しているため、環境の中では極めて一般的なものだろう。DNS トラフィックは、ネットワーク認証の完了前でも許可される場合がある。DNS パケットは多数のフィールドとヘッダーを含んでいるので、そこにデータを隠すことができる。しばしば DNS トンネリングとして知られるように、攻撃者は DNS を不正使用し、通常予期されるトラフィックに偽装して、被害者ネットワーク内にある攻撃者の管理下のシステムと通信する可能性がある。(https://attack.mitre.org/techniques/T1071/004/)

21. DNS ビーコン – C2 との通信 – データを不正に持ち出すか C2 からのさらなるコマンドを待機するため、コマンド＆コントロールサーバーに DNS 問い合わせを連続的または定期的に送信する。

ステークホルダー

多くの組織は、さまざまな状況に応じてそれぞれ異なるステークホルダーの役割を果たす場合がある。また中小規模の組織では、同じ個人がさまざまな状況で異なる役割を果たす場合がある。しかし、これらのさまざまなステークホルダーはそれぞれ異なる能力を保持することから、別個のものとして体系化した。ある組織が、それぞれ異なるステークホルダーの役割を果たすチームを複数保持する場合であっても、ステークホルダーの能力を実行するチームに連絡を試みることが有用だろう。

インシデント対応者は、すべてのステークホルダーが対応者のためを思ってくれるわけではないことに留意しておくことが重要である。連絡を受けたステークホルダーは、注意散漫であったり、未熟であったり、最悪の場合には不正使用をサポートするインフラを意図的に運用していたりするかもしれない。後者を行っている組織は、よくても連絡に対して受容的ではなく、最悪の場合は欺瞞に満ちたものになる。ステークホルダーとの連絡を進めるべきかどうか判断できない場合、同僚と一緒に確認することを勧める。

1. レジストラー – TLD 下位へのドメイン登録を許可する組織 – 詳細については https://www.icann.org/en/icann-acronyms-and-terms/registrar-en 参照。

2. レジストリ – TLD に関するドメインのデータベースを維持する責任を負う組織 – 詳細については https://www.icann.org/en/icann-acronyms-and-terms/registry-en 参照。

3. 権威 DNS サーバー運用者 – 詳細については https://www.icann.org/en/icann-acronyms-and-terms/authoritative-name-server-en 参照。

4. ドメイン名リセラー – 詳細については https://www.icann.org/resources/pages/reseller-2013-05-03-en 参照。

5. 再帰リゾルバー運用者 – プライベート再帰リゾルバーまたはパブリック再帰リゾルバーを運用する組織。

6. ネットワーク運用者 – AS の運用組織。この能力を持つ組織は、再帰 DNS サーバーを稼働させていないものと想定する。この列は、ネットフローの情報(送信元/宛先 IP アドレス、L3 プロトコル、送信元/宛先ポート番号など)や BGP ルーティングデータを意味し、パッシブ DNS は除外する(明確化のため)。

7. アプリケーションサービスプロバイダー – (Google Docs のような)SaaS(Software as a Service)プロバイダー。SaaS の定義については https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en 参照。

8. ホスティングプロバイダー -インターネットホスティングサービスを提供する会社。インターネットホスティングサービスとは、インターネットに接続されたサーバーを運営し、組織や個人がインターネットに接続されたコンテンツを提供したり、サービスをホストしたりできるようにするサービスである。詳しくは、https://en.wikipedia.org/wiki/Internet_hosting_service 参照。

   留意:ホスティングプロバイダーが防弾ホスティングである場合や攻撃インフラの提供に加担している場合、連絡したとしても、よくて何も得るものはなく、最悪の場合チームが報復に晒されることになる。

9. 脅威インテリジェンスプロバイダー – 脅威インテリジェンスプロバイダーは、意思決定プロセスに必要なコンテキストを提供するため、インテリジェンスの集約、変換、分析、解釈、高品質化などを行う。サイバー脅威インテリジェンス(CTI)は共有と分析のみが行われるものとする。

10. 機器、OS、アプリケーションソフトウェアの開発者 – DNS リゾルバーソフトウェアのコードを書くまたは開発をしているソフトウェア開発者、またはソフトウェアプロジェクトにインポートされる DNS リゾルバーのバージョンを更新する責任を負う人。

11. ドメイン登録者 – ドメイン名を登録した個人またはエンティティ。詳細については https://www.icann.org/en/icann-acronyms-and-terms/registrant-en 参照。悪意ある登録の行におけるドメイン登録者の列では、このステークホルダーは、悪意ある登録を行った実在の人物としてモデル化されている。

12. エンドユーザー – インターネットを利用するすべての人々(列挙されている他のステークホルダーのいずれの能力も持たない人)。

13. 法執行機関および公安機関 – 法の執行または公益のために行動する権限を持つ政府組織。そのような組織が問題に気付くのは、通常、以下のような理由による。

a. 進行中の捜査において、法執行機関の手法により独自の洞察が得られる。

b. 被害者の告発が不正使用を示す情報を提供すると、大抵の場合、組織は技術的領域の専門家の協力を得てその証拠を理解する。

14. CSIRT / ISAC – コンピューターセキュリティインシデント対応チーム / 情報共有・分析センター。この列は、チームやセンターの能力だけをモデル化している。各 CSIRT や ISAC はサービスのエンドユーザーでもあり、ドメイン登録者でもあることに加えて、脅威インテリジェンスプロバイダーなどである場合もある。CSIRT や ISAC が(組織として)ステークホルダーの能力を提供している場合に、これらの列を使用する。

15. インシデント対応者 – 影響を受けている組織内部のコンピューターセキュリティインシデント対応チーム。

不正手法の例

SIG はさまざまな不正手法の例を収集し、FIRST.org の Web サイトの DNS Abuse SIG ホームページで閲覧可能になっている。

https://www.first.org/global/sigs/dns/dns-abuse-examples

手法の例のリストは、より多くの情報が収集、整理された段階で、継続的に更新されていく予定である。

JPCERT/CC は、ドメイン生成アルゴリズム(DGA)や、実効的 SLD の悪意ある登録などの手法例を実証するフィッシング URL のリストを公開している。

Nominet は、DNS の dangling エントリーがどのように lame delegation やオンパスの DNS 攻撃といった手法につながる脆弱性をもたらすかの解説を公開している。

米国歳入庁(IRS)は、攻撃対象の組織に関する悪意ある登録やなりすましを利用した SMS 詐欺に対する注意を公開している。

インシデント対応者へのアドバイス

以下のスプレッドシートは、さまざまな DNS の不正使用手法に対するさまざまなインシデント対応段階において、どのような組織に連絡するのが生産的かという点について我々のアドバイスを提示するものである。サイバー犯罪に関する条約や他のネットワークには、国境を越えた証拠の押収とインフラの一時停止をどちらも行える仕組みがある。条約は例えば、「外国の法執行機関の捜査官が行う作業の第 1 段階は、大抵の場合、正式な法(刑事共助条約)に基づく要請の保留中にデータが消失しないようにするための非公式な保全要請になる」といったことを期待している。

不正使用手法に対抗するためのマトリックス

記号一覧

✅ : エンティティは脅威を**検知/緩和/抑止**する能力を保持している
❌ : エンティティは脅威を**検知/緩和/抑止**する能力が無い

- **DGA**: ドメイン生成アルゴリズム
- **eSLD**: 実効的セカンドレベルドメイン
- **pDNS**: パッシブ DNS

検知

✅ : エンティティは検知する能力を保持している
❌ : エンティティは検知する能力が無い

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DGA (ドメイン生成アルゴリズム)	✅ (eSLD のみ。ドメイン作成時点および存在中に分析を行っている場合)	✅ (eSLD のみ)	✅ (eSLD のみ。顧客のドメインの分析を行っている場合)	✅ (eSLD のみ)	✅ (再帰リゾルバーでロギングまたは pDNS によるロギングと分析を行っている場合)	❌	✅	❌	✅	❌	該当なし (登録者が脅威アクターそのもの)	❌	✅ (レジストリか、PSWG および GAC のどちらかあるいは両方に関与を要請可能)	❌	✅ (送出される問合わせがロギングされている場合)
ドメイン名の侵害	✅	✅	❌	✅	✅ (DNS RPZ を使用し、脅威インテリジェンスを反映している場合)	❌	❌	❌	✅	❌	✅ (事前防御的監視を行っている場合)	❌	✅	❌	❌ (組織外のドメインを想定)
lame delegation (レイムデレゲーション)	❌	✅	❌	❌	✅	❌	❌	❌	✅	❌	✅ (事前防御的監視を行っている場合)	❌	❌	❌	❌ (組織外のドメインを想定)
DNS キャッシュポイズニング	❌	❌	❌	❌	✅ (再帰リゾルバーで DNSSEC 署名検証を行い RFC 8914 規定の拡張エラーを有効にしている場合)	✅ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	❌	❌	✅	❌	✅ (事前防御的監視を行っている場合)	❌	❌	❌	❌ (外部のリゾルバーが汚染されたと想定)
DNS リバインディング	❌	❌	❌	❌	✅ (pDNS 分析により、パブリック IP アドレスから RFC 1918 アドレスに変化した DNS 応答を検知可能)	✅ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	❌	❌	✅	❌	✅ (事前防御的監視を行っている場合)	❌	❌	❌	✅

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DNS サーバーの侵害	✗	✗	✓ (権威サーバーが侵害された場合)	✗	✓ (再帰リゾルバー自身が侵害された場合)	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗ (侵害前の pDNS ログが存在しない場合)
スタブリゾルバーのハイジャック	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓ (おそらくはアンチウイルスソフトウェア次第)	✗	✗	✓
ローカルな再帰リゾルバーのハイジャック	✗	✗	✗	✗	✗	✓ (NetFlow/Zeek 等によるトラフィック分析を行い、脅威インテリジェンスの提供を受けている場合)	✗	✗	✓	✓	✗	✓ (ホームルーターのビルトインセキュリティ機能により検知可能)	✗	✗	✓
オンパス(on-path)の DNS 攻撃	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓ (pDNS がロギングしており、解決パスが検査可能な場合のみ)
DNS に対する DoS	✗	✗	✓ (攻撃が権威サーバーに対するものである場合)	✗	✓ (攻撃が再帰リゾルバーまたは権威サーバーに対するもので、かつロギング、NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✗	✗	✗	✗	✓	✗	✓
DoS を目的とした DNS サーバーの不正使用	✗	✗	✓ (攻撃が権威サーバーの応答を利用している場合)	✗	✓ (攻撃が再帰リゾルバーまたは権威サーバーに対するもので、かつロギング、NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✗	✓	✗	✗	✓	✗	✓

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
動的な DNS 解決による検知の難化	✗	✓ (eSLD のみ)	✗	✗	✓	✗	✗	✗	✓	✗	該当なし (登録者が脅威アクターそのもの)	✓ (アンチウイルスソフトウェアで検知可能)	✓	✗	✓ (pDNS がロギングしているか、この攻撃手法が健在で解決が進行していると想定)
動的な DNS 解決 (Fast flux)による隠ぺい	✗	✓ (eSLD のみ)	✓ (eSLD のみ。短い TTL にフラグを設定して詳細な分析を行っている場合)	✗	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗ (pDNS が無ければ検知不可)	✗	✗	✓	✗	該当なし (登録者が脅威アクターそのもの)	✓ (アンチウイルスソフトウェアで検知可能)	✓	✗	✓ (pDNS がロギングしているか、この攻撃手法が健在で解決が進行していると想定)
DNS を介した情報の不正な持ち込みおよび持ち出し	✗	✗	✗	✗	✗	✗ (トラフィック分析を行っていない場合は検知不可)	✗	✗	✓	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓	✗	✓ (pDNS がロギングしていると想定)
(実効的)セカンドレベルドメインの悪意ある登録	✓ (eSLD のみ。ドメイン作成時点および存在中に分析を行っている場合)	✓	✓ (登録された文字列による)	✓	✓ (pDNS 分析を行っている場合)	✗	✓	✗	✓	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓ (レジストラーに連絡し、レジストリへのエスカレーションを要請)	✗	✗ (登録の検知はできない)
ダイナミック DNS プロバイダーを介した悪意あるサブドメインの作成	✗	✗	✓	✗	✓ (DNS RPZ を使用し、脅威インテリジェンスを反映している場合)	✗	✓	✗	✓	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓	✗	✗ (名前の作成は検知できない)
DNS の不正使用を目的とした DNS 以外のサーバーの侵害	✗	✗	✗	✗	✗	✗	✗	✓ (防弾ホスティングでない場合)	✓	✗	✗	✗	✓	✗	✓

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
未登録ドメイン名を介したなりすまし	✗	✗	✓	✗	✓ (DNS ログ分析や NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✓ (防弾ホスティングでない場合)	✓	✗	✗		✓	✗	✓
登録されたドメイン名のなりすまし	✗	✓	✗	✗	✓ (DNS 応答の分析を行い RFC 8914 規定の拡張エラーを有効にしている場合)	✗	✓	✓ (防弾ホスティングでない場合)	✓	✗	✗ (DMARC を使用していない場合)	✗	✓	✗	✓ (DMARC を使用しているか、pDNS による分析を行っていると想定)
DNS トンネリング	✗	✗	✗	✗	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗ (トラフィック分析を行っていない場合)	✗	✗	✓	✗	✗	✗	✗	✗	✗ (pDNS は理論上これを検知できるが、極めて困難)
DNS ビーコン	✗	✓	✗	✗	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓ (C2 チャネルを使用する機器があると認識している場合、pDNS を使用する)

緩和

✅ : エンティティは緩和する能力を保持している
❌ : エンティティは緩和する能力が無い

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DGA (ドメイン生成アルゴリズム)	✅ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✅	❌	✅ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✅ (DNS RPZ を使用する)	❌	❌	❌	❌	❌	該当なし (登録者が脅威アクターそのもの)	❌	✅ (防衛的登録。ドメインを生成し複数レジストリで同じものを登録する)	❌	✅ (ブロッキングを行う)
ドメイン名の侵害	✅ (侵害がレジストラレベルで行われている場合)	✅	✅	✅ (侵害がリセラーレベルで行われている場合)	✅	❌	❌	❌	❌	❌	✅ (適切に不正を排除する)	❌	❌	❌	✅ (ブロッキングを行う)
lame delegation (レイムデレゲーション)	❌	❌	❌	❌	❌	❌	❌	❌	❌		✅ (ネームサーバーを更新する)	❌	❌	❌	❌ レジストラーなどに連絡を推奨
DNS キャッシュポイズニング	❌	❌	✅	❌	✅ (DNSSEC 署名検証を行う)	✅	❌	❌	❌	❌	❌	❌	❌	❌	❌ (権威サーバー運用者などに連絡を推奨
DNS リバインディング	❌	✅	❌	❌	❌	✅ (BCP38 を適用する、攻撃者の IP ネットブロックを BGP でブラックホールに吸い込む)	❌	❌	❌	❌	❌	❌	❌	❌	✅

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DNS サーバーの侵害	✗	✗	✓	✗	✓ (再帰リゾルバー自身を自分達で運用している場合のみ)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
スタブリゾルバーのハイジャック	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓ (アンチウイルスソフトウェアで PC をスキャンする)	✗	✗	✓
ローカルな再帰リゾルバーのハイジャック	✗	✗	✗	✗	✗	✓ (悪意ある DNS サーバー宛の送出トラフィックをブロックする)	✗	✗	✗	✗	✗	✓ (ホームルーターをリブートまたは初期化する)	✗	✗	✓
オンパス(on-path)の DNS 攻撃	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗ (ネットワーク運用者などに連絡を推奨
DNS に対する DoS	✗	✓	✗	✗	✗	✓ (攻撃者の IP ネットブロックを BGP でブラックホールに吸い込む)	✗	✗	✗	✗	✗	✗	✗	✗	✓
DoS を目的とした DNS サーバーの不正使用	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
動的な DNS 解決による検知の難化	✗ (eSLD の登録サービスを提供しているに過ぎないため)	✗	✗	✗	✓	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✗	✗	✓ (詳細が特定できているならブロッキングを行う)

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
動的な DNS 解決 (Fast flux)による隠ぺい	✓ (十分迅速に行動できる場合)	✓ (十分迅速に行動できる場合)	✗	✓ (十分迅速に行動できる場合)	✓	✓	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✗	✗	✓
DNS を介した情報の不正な持ち込みおよび持ち出し	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✗	✗	✓
(実効的)セカンドレベルドメインの悪意ある登録	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓	✗	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓ (レジストラー/レジストリへの通知、(法執行機関による)ドメインの押収)	✗	✗ (登録それ自体には対処できない)
ダイナミック DNS プロバイダーを介した悪意あるサブドメインの作成	✗ (eSLD の登録サービスを提供しているに過ぎないため)	✗	✓	✗	✓	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✗	✗	✗ (作成それ自体には対処できない)
DNS の不正使用を目的とした DNS 以外のサーバーの侵害	✗	✗	✗	✗	✗	✗	✓	✓ (防弾ホスティングでない場合)	✗	✗	✗	✗	✗	✗	✓ (サーバーの修正がチームの職責範囲である場合)
未登録ドメイン名を介したなりすまし	✗	✗	✓	✗	✓	✗	✗	✓ (防弾ホスティングでない場合)	✗	✗	✗	✗	✗	✗	✗
登録されたドメイン名のなりすまし	✓ (ドメイン作成時点または存在中に分析を行っている場合)	✗	✗	✓ (ドメイン作成時点または存在中に分析を行っている場合)	✓	✗	✗	✓ (防弾ホスティングでない場合)	✗	✗	✓ (状況に応じて通報するか、UDRP または URS を申し立てる)	✗	✗	✗	✗ (DMARC を適用していても、なりすましは止められない)

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DNS トンネリング	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	該当なし （登録者が脅威アクターそのもの）	✗	✗	✗	✓
DNS ビーコン	✗ （C2 ドメインはインフラに過ぎないため）	✗	✗	✓ （C2 ドメインはインフラに過ぎないため）	✓	✗	✗	✗	✗	✗	該当なし （登録者が脅威アクターそのもの）	✗	✓	✗	✓

抑止

✅ : エンティティは抑止する能力を保持している
⛔ : エンティティは抑止する能力が無い

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DGA (ドメイン生成アルゴリズム)	✅ (eSLD のみ。ドメイン作成時点および存在中に分析を行う)	✅ (eSLD のみ)	✅ (DGA が既知の場合)	✅ (eSLD のみ。ドメイン作成時点および存在中に分析を行う)	✅ (DGA が既知であれば、DNS RPZ を使用し脅威インテリジェンスを反映する)	✅ (DGA が既知の場合)	⛔	⛔	⛔	⛔	該当なし (登録者が脅威アクターそのもの)	⛔	✅	✅ (DGA の調査)	⛔
ドメイン名の侵害	✅ (登録者アカウントの侵害を抑止する対策を講じる)	⛔	⛔	✅ (登録者アカウントの侵害を抑止する対策を講じる)	⛔	⛔	⛔	⛔	⛔	⛔	✅ (登録者アカウントの侵害を抑止する事前防御策を講じる)	⛔	✅	✅ (関連するステークホルダーに連絡する)	⛔
lame delegation (レイムデレゲーション)	⛔	✅	⛔	⛔	⛔	⛔	⛔	⛔	⛔	⛔	✅ (ドメインポートフォリオを管理するための優れた実践を導入する)	⛔	✅	✅ (関連するステークホルダーに連絡する)	⛔
DNS キャッシュポイズニング	⛔	⛔	⛔	⛔	✅ (再帰リゾルバーで DNSSEC 署名検証を有効にする)	⛔	⛔	⛔	⛔	⛔	⛔	⛔	✅	✅ (再帰リゾルバー運用者またはネットワーク運用者に連絡し、キャッシュのクリア/リフレッシュを確認)	⛔ (キャッシュは組織外にあると想定)

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DNS リバインディング	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓ (ホームルーターに強力なパスワードを設定するか、ブラウザーのセキュリティ機能に頼る)	✓	✓ (脆弱な/改ざんされた Web サイトについて調整を行う)	✓
DNS サーバーの侵害	✗	✗	✓ (権威サーバーが侵害された場合)	✗	✓ (再帰リゾルバー自身が侵害された場合)	✗	✗	✗	✗	✗	✗	✗	✓	✓ (関連するステークホルダーに連絡する)	✗ (サーバーは組織外にあると想定)
スタブリゾルバーのハイジャック	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓ (ブラウザーやアドオンツール等を最新の状態に保つ)	✓	✓ (エンドユーザーの注意を喚起する)	✓
ローカルな再帰リゾルバーのハイジャック	✗	✗	✗	✗	✗	✓ (NetFlow/Zeek によるトラフィック分析を行い、脅威インテリジェンスの提供を受ける)	✗	✗	✗	✓	✗	✓ (ソフトウェアを最新の状態に保ち、強力なパスワードを設定するなど)	✓	✓ (エンドユーザーの注意を喚起する)	✓
オンパス(on-path)の DNS 攻撃	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓ (情報を共有し関心を高める)	✓ (DNSSEC 署名検証を有効にする)

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DNS に対する DoS	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓ (オープンリゾルバーおよび感染した機器について調整を行う)	⊗ (BCP 38 は IR の職責範囲ではないと想定)
DoS を目的とした DNS サーバーの不正使用	⊗	⊗	✓ (攻撃が権威サーバーの応答を利用している場合)	⊗	✓ (ACL やレート制限などを適用する)	⊗	⊗	⊗	⊗	✓	⊗	✓ (ファームウェアを最新の状態に保ち、適切な設定を行うなど)	✓ (踏み台となっている DNS サーバーを特定するためナショナルレベルの CERT に関与を要請)	✓ (オープンリゾルバーおよび感染した機器について調整を行う)	✓ (感染した機器をクリーンアップする)
動的な DNS 解決による検知の難化	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓ (関連するステークホルダーに連絡する)	⊗
動的な DNS 解決 (Fast flux)による隠ぺい	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓ (関連するステークホルダーに連絡する)	⊗
DNS を介した情報の不正な持ち込みおよび持ち出し	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓ (情報を共有し関心を高める)	✓
(実効的)セカンドレベルドメインの悪意ある登録	✓ (eSLD のみ。ドメイン作成時に分析を行う)	✓	⊗	✓ (eSLD のみ。ドメイン作成時に分析を行う)	⊗	⊗	⊗	⊗	⊗	✓	該当なし (登録者が脅威アクターそのもの)	⊗	✓ (レジストラーに通知し、レジストリへのエスカレーションを要請)	✓ (関連するステークホルダーに連絡する)	⊗

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
ダイナミック DNS プロバイダーを介した悪意あるサブドメインの作成	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	該当なし （登録者が脅威アクターそのもの）	⊗	✓	✓（関連するステークホルダーに連絡する）	⊗
DNS の不正使用を目的とした DNS 以外のサーバーの侵害	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓（防弾ホスティングでない場合）	⊗	⊗	⊗	⊗	✓	✓（情報を共有し関心を高める）	✓（パッチ管理などを行う）
未登録ドメイン名を介したなりすまし	⊗	✓	⊗	⊗	⊗	⊗	⊗	✓（防弾ホスティングでない場合）	⊗	⊗	⊗	⊗	✓	✓（情報を共有し関心を高める）	⊗
登録されたドメイン名のなりすまし	✓（eSLD のみ。ドメイン生成時に分析を行う）	⊗	✓（偽装ドメインがサービス対象となり解決が行われるのを防止する）	✓（eSLD のみ。ドメイン生成時に分析を行う）	⊗	⊗	⊗	✓（防弾ホスティングでない場合）	⊗	✓	該当なし （登録者が脅威アクターそのもの）	⊗	✓	✓（情報を共有し関心を高める）	⊗
DNS トンネリング	⊗	⊗	⊗	⊗	✓（JA3、JA3S による TLS フィンガープリント採取、NetFlow/Zeek 等によるトラフィック分析を行う）	✓（NetFlow/ Zeek によるトラフィック分析を行い、脅威インテリジェンスの提供を受ける）	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓（感染した機器のクリーンアップおよびマルウェアの分析を行う）	⊗（ファイアウォールのルール管理はは IR の職責範囲ではないと想定）
DNS ビーコン	⊗	⊗	⊗	⊗	✓（NetFlow/ Zeek によるトラフィック分析を行う）	✓（NetFlow/ Zeek によるトラフィック分析を行い、脅威インテリジェン	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓（感染した機器のクリーンアップおよびマルウェアの分析を行う）	⊗

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
						スの提供を受ける）									

Acknowledgements

SIG members

Andrey Meshkov (AdGuard)

Ángel González (INCIBE-CERT)

Angela Matlapeng (bwCSIRT)

Benedict Addis (Shadowserver)

Brett Carr (Nominet)

Carlos Alvarez (ICANN; founding member)

David Ruefenacht (Infoguard)

Gabriel Andrews (FBI)

John Todd (Quad9; current co-chair of DNS Abuse SIG)

Jonathan Matkowsky (RiskIQ / Microsoft; former co-chair)

Jonathan Spring (CISA; current co-chair of DNS Abuse SIG)

Mark Henderson (IRS)

Mark Svancarek (Microsoft)

Merike Kaeo (Double Shot Security)

Michael Hausding (SWITCH-CERT; former co-chair, current FIRST board member)

Peter Lowe (current co-chair of DNS Abuse SIG)

Shoko Nakai (JPCERT/CC)

Swapneel Patnekar (Shreshta IT)

Trey Darley (FIRST board; founding member)

SIG chairs

Current: Jonathan Spring, John Todd, Peter Lowe

Former: Michael Hausding, Jonathan Matkowsky

Special Thanks

To Carlos Alvarez (ICANN) for an initial start on the abuse technique types matrix.

Translation: Professionally outsourced
Review: Shoko Nakai, Yukako Uchida, JPCERT/CC, (and volunteers from DNSOPS.JP)