DNSセキュリティイシューへの対応
DNS事業者(ドメイン名レジストリ)の視点

2014年11月20日

Internet Week 2014 DNS DAY

JPRS 米谷嘉朗

セキュリティイシューとは

- 何らかの脆弱性や脅威の存在が確認された状況
  - サーバーソフトウェアの脆弱性
  - サーバーの不適切な運用により攻撃の対象となってしまう脅威
  - など
- 具体的な攻撃事例(セキュリティインシデント)の発生は確認されていない状況
- セキュリティイシューを放置すると、セキュリティインシデントにつながるリスクが高まる

ドメイン名レジストリが対応するDNSセキュリティイシュー(1/4)

- DNSサーバーソフトウェアの不具合に起因する脆弱性
  - 具体例
    - BINDやNSD/Unboundなど
  - 対応例

(1) 自らが運用するDNSサーバーソフトウェアの更新

- ✓ サポート契約により脆弱性公開前に情報と対応策を入手

(2) 関係者への注意喚起

- ✓ 脆弱性の概要と対応をまとめた注意喚起を作成
- ✓ 指定事業者(レジストラ)やネットワークオペレーターへの連絡

ドメイン名レジストリが対応するDNSセキュリティイシュー(2/4)

- DNS運用に起因する問題
  - 具体例
    - オープンリゾルバー、キャッシュポイズニング、共用DNSサービス、権威とフルリゾルバーの分離、Lame Delegationによる問題など
  - 対応例

(1) 自らが運用するDNSサーバー設定の変更

- ✓ DNS RRLの導入、JPとDNS.JPのNSの分離など

(2) 関係者への注意喚起

- ✓ 脆弱性の概要と対応をまとめた注意喚起を作成
- ✓ 指定事業者(レジストラ)やネットワークオペレーターへの連絡

ドメイン名レジストリが対応するDNSセキュリティイシュー(3/4)

- OSの実装に起因する問題
  - 具体例
    - ➢WPAD、ISATAPにおけるサービス自動検索の問題
  - 対応例

(1) サービス自動検索に使われる名前の予約ドメイン名化

(2) 関係者への注意喚起

- ✓ 脆弱性の概要と対応をまとめた注意喚起を作成
- ✓ 指定事業者(レジストラ)やネットワークオペレーターへの連絡

ドメイン名レジストリが対応するDNSセキュリティイシュー(4/4)

- 登録情報の取り扱いに起因する問題
  - 具体例
    - 登録情報の不正書き換えによるドメイン名ハイジャック
  - 対応例

(1) 自らが運用しているシステムのセキュリティ対策
- ✓ 使用しているシステムのOS、ソフトウェア、設定に関する既知の脆弱性への対応

(2) 認証の強化
- ✓ 電子証明書認証の導入

(3) 関係者への注意喚起の実施と利用者(顧客)に対する周知の依頼
- ✓ 脆弱性の概要と対応をまとめた注意喚起を作成
- ✓ 指定事業者(レジストラ)やネットワークオペレーターへの連絡
- ✓ 指定事業者(レジストラ)へのシステムの再確認・電子証明書認証への移行・顧客への周知を依頼

現状における課題(1/2)

- 注意喚起(情報)の伝達範囲と伝えるべきチャネル
  - DNS利用者＝インターネット利用者
  - 1ドメイン名事業者がDNSセキュリティイシューの注意喚起を伝達できている範囲(チャネル)は限られている
  - 伝えられている(と考えている)チャネル
    - 指定事業者(レジストラ)、ネットワークオペレーター、専門系メディア
  - 伝えていきたい(と考えている)チャネル
    - 企業のシステム管理者、消費者向け製品開発者、一般マスコミ、一般利用者

現状における課題(2/2)

- 注意喚起をいつまで継続するかの判断
  - セキュリティイシューは一度注意喚起したら終わりというものではない
    - 対策が既知であっても、攻撃対象者がそれを知らずに(あるいは忘れていて)対策していなければ攻撃されてしまう
    - とはいえ、対策率を100%にすることは実質的に不可能
  - ドメイン名レジストリにできる注意喚起の効果測定は限定的
    - 例えばDNSクエリの分析や登録申請の利用状況など、自らのシステムで把握できるものに限られる
    - 消費者向け製品の対応状況や、一般利用者の対応状況まではカバーしきれない

有効な連携体制構築に向けて(1/2)

- 連携すべき人は誰か
  - 相互に補完し、より広い範囲へ効率的に注意喚起(情報)を伝達できることが重要
    - DNS専門家、セキュリティコーディネーター、公的情報セキュリティ対策機関、セキュリティ事業者、など

有効な連携体制構築に向けて(2/2)

- どのように情報を発信していくべきか
  - 情報の受信者から見た場合の見え方・見せ方の工夫
  - 複数のチャネルから情報を受け取ることがある
  - 連携しているという見え方・見せ方が大切
  - そのためには、情報発信側(組織間)が連携して背景や用語を揃え、タイミングを合わせて発信することが重要
- 他のセキュリティイシュー対応との違い
  - DNSは影響範囲が広い
  - そのために連携すべき組織数が多岐にわたる