修士論文

DNS Exfiltrationの緩和を目的とした Non-Transparent DNS(NTDNS)の提案

高須賀 昌烈

2020年3月15日

奈良先端科学技術大学院大学
先端科学技術研究科

本論文は奈良先端科学技術大学院大学先端科学技術研究科に
修士 (工学) 授与の要件として提出した修士論文である。

高須賀 昌烈

審査委員：

門林 雄基 教授　（主指導教員）
笠原 正治 教授　（副指導教員）
林 優一 教授　（副指導教員）
妙中 雄三 准教授　（副指導教員）

DNS Exfiltrationの緩和を目的とした Non-Transparent DNS(NTDNS)の提案*

高須賀 昌烈

内容梗概

キーワード

情報流出，秘匿通信，Domain Name System，DNSセキュリティ，DNS Exfiltration，分散ハッシュテーブル

*奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 2020年3月15日.

Proposal for Non-Transparent DNS(NTDNS) to Mitigate DNS Exfiltration*

Shoretsu Takasuka

Abstract

Keywords:

DNS Exfiltration, Covert Channel, Hash Function, Recursive Name Resolution

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2020.

目 次

図 目 次

表 目 次

1. 序論

1.1 研究背景

インターネットの利活用において，おおよそ全ての通信はドメインネームシステム (Domain Name System, DNS) による名前解決をきっかけにサービスは開始される．DNS の機能のおかげで，インターネット利用者は，人が覚えにくいインターネット上でのノードの住所を意味する IP アドレス (E.g. 203.10.23.86) ではなく，人が認識しやすいドメイン名 (E.g. www.example.com) を使用することができる，など現在のインターネットの利便性を実現する上で極めて重要な技術の一つである．1987 年にそのコンセプト [1, 2] が公開されて以降，採用されている名前解決の仕組みは公開当時と変わることなく現在も使用されている．

しかし，プライバシーやセキュリティの観点が現在ほど議論されていない当時の設計が原因で，第三者からのトランザクションを覗く脅威や偽の応答パケットによるキャッシュの毒入れの脅威など，多数の課題が浮き彫りになってきている．例えば，IDS・IPS やファイヤーウォールなどのセキュリティラインが引かれているネットワークにおいて，悪意のユーザがなんらかの方法でマルウェアを潜伏させた後，機密情報等を外部へ持ち出す際のデータ転送ベクターに，DNS の名前解決の仕組みを利用することで，そのようなセキュリティラインを迂回できてしまうことが明らかになっている．この DNS Tunneling と呼ばれる DNS をデータ転送メディアとする手法は，大規模な影響をもたらしたクレジットカード情報流出のサイバー犯罪 [3] に使用される POS システムを狙った大規模なクレジットカード情報流出事件をこの手法は，DNS Tunneling と呼称され，2014 年のアメリカで発生した

しかし，DNS の名前解決の仕組みは，任意の文字列を転送するためのキャリア (媒体) として機能する意図しない設計になっている．

この設計の不備は，DNS Tunneling と呼称され，データ流出や C2 通信などの攻撃ベクターとして都合がよく，事実，クレジットカードの大規模流出事件に使用されるなどしている．従来の DNS Tunneling 対策アプローチは，検知に焦点が当てられ，QNAME の長さやエントロピーの特徴を利用するペイロードベース検

知およびトラフィック頻度を特徴量とするトラフィックベース検知手法が提案されてきた.

しかし，これまでの検知アプローチは，提案手法に対する検知対象がツールキットによって生成される顕著な特徴を有するパケットであることが多く，1 回あたりの転送データ量を少なくしたり，パケット間のインターバルを数日・数ヶ月と長期化させるといった Low Throughput や Slow なバイパス手法への対応が困難であるという課題がある.

少ない転送量だからと軽視されるべきではなく，攻撃者にとって，1bit でも複数組み合わせることで多種多様な情報量を持たせ得る可能性があるため，

たとえ，転送されるデータ量が少なかったとしても，このような既存の DNS Tunneling 通信の検知迂回手法に対応させることが考えた場合，高い誤検知もしくは大量のログファイルの発生が予想されるなど難しさが残っている.

1.2 脅威モデル

そこで本研究では，脅威モデルは，〜である.

1.3 研究目的

1.4 アプローチ

2. 準備

本章では，本論において使用する用語及び技術について説明する．

2.1 DNS

2.1.1 プロトコル概要

インターネットの利活用において，おおよそ全ての通信はドメインネームシステム (Domain Name System, DNS)[1, 2] による名前解決をきっかけにサービスは開始される．すなわち，DNS は，人が覚えにくいインターネット上のでノードの住所を表す IP アドレス (E.g. 203.10.23.86) を，人が認識しやすいドメイン名に変換する機能を提供しており，この機能は現在のインターネットの利便性を実現する上で欠かすことの出来ない根幹技術の一つである．

ドメインネームシステムは，IP アドレスで表現されるインターネット上のノードの住所について，人が認識しやすいドメイン名に変換する名前解決機能を提供しており，インターネットの利便性を実現する根幹技術の一つである．

DNS は，各権威サーバが固有のゾーンを管理することによる階層型分散データベースとして機能させている．ドメインは通常，複数のラベルで構成されており，ラベルの区切り文字にはドットが使用されている．階層の最上位に位置するルートはラベルを持たず，最も右に位置するラベルが TLD である．最も一般的なレコードは，A レコードであり，FQDN を IPv4 アドレスにマッピングする．ゾーンは，管理者が管轄するべき名前空間を意味する．権威は，サブドメインへ委譲することが可能である．この機能は，NS レコードによって実現される．

2.1.2 DNS Tunneling

2.2 暗号学的ハッシュ関数

2.2.1 定義

2.2.2 性質

3. 先行研究

3.1 トラフィック特徴に基づいた悪性DNSトランザクションの検知

3.1.1 同一ドメインあたりのクエリ頻度

3.2 ペイロード特徴に基づいた悪性DNSクエリの検知

3.2.1 文字列分布特徴

3.2.2 ペイロード特徴

3.3 ポストDNSプロトコルによる悪性DNSクエリの発生緩和

4. 提案手法

4.1 分散データベースを用いた再起問い合わせにおけるハッシュ関数の適用

5. 評価

5.1 シミュレーションによるパフォーマンス実験

5.2 結果

5.3 課題

6. 議論

6.1 DNS を用いた秘匿流入通信対策

6.1.1 リソースレコード

6.1.2 ポリシー

6.2 既存アプローチとの比較

7. 結論

7.1 貢献

透過性への対策 スタブリゾルバからの名前解決クエリは，分散データベースにのみ転送されるため，従来権威サーバで受け取れていたDNSクエリパケットの到達性を改善することができる．

秘匿性の実現 フルリゾルバとデータベース間の通信において，クエリの内容はハッシュ化されたQnameとリソースレコードであり，第三者からのスプーティング忍耐して，意味抽出を無効化することが期待される．

7.2 総括

謝辞

ご指導ご鞭撻賜りありがとうございました.

参考文献

[1] P.V. Mockapetris. “Domain names - concepts and facilities. RFC 1034 (INTERNET STANDARD),” November 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[2] P.V. Mockapetris. “Domain names - implementation and specifica- tion. RFC 1035 (INTERNET STANDARD),” November 1987. Up- dated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604.”

[3] KrebsonSecurity. “Deconstructing the 2014 Sally Beauty Breach,” May 2015. https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/. Novemver 2019 Accessed.

付録

A. 発表リスト (国内研究会)

1. 高須賀 昌烈, 妙中 雄三, 門林 雄基, “非実在ドメインに対するネガティブキャッシュの拡張と再帰問い合わせハッシュ化の提案”, 電子情報通信学会情報ネットワーク研究会, 2019-10-ICTSSL-IN, 2019 年 10 月.