修士論文

DNS Exfiltration 対策を目的としたスーパーノード型 P2P ネットワークに基づく名前解決システムの提案

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 対策を目的としたスーパーノード型 P2P ネットワークに基づく名前解決システムの提案*

高須賀 昌烈

内容梗概

キーワード

ネットワークセキュリティ，ドメインネームシステム，秘匿通信，分散ハッシュテーブル，スーパーノード型ピアツーピア

*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 Name Resolution System based on Supernode in P2P Networks against DNS Exfiltration*

Shoretsu Takasuka

Abstract

Keywords:

Network Security, Domain Name System(DNS), Covert Channel, Distributed Hash Table(DHT), Supernode in Peer-to-Peer

*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 背景

インターネットの利活用において，サービス通信の開始は，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としている．インターネット利用者は，DNS の名前解決の機能を通じて，インターネット上でのノードの住所を意味する人にとっては覚えにくい IP アドレス (E.g. 93.184.216.34) ではなく，人が認識しやすいドメイン名 (E.g. www.example.com) を使用してサービスを利用することができている．このように現在のインターネットの利便性を実現する上で，DNS は極めて重要な技術の一つである．

1987 年に RFC1034, RFC1035([1, 2]) として公開された DNS のコンセプトは，現在もなお本質的な仕組みは変更されることなく適用されている．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には，第三者からのトランザクションを覗く脅威やフルサービスリゾルバ (キャッシュサーバ) に対して偽の応答パケットをキャッシュすることで任意のページにユーザを誘導させる脅威などが問題になるなど，設計の不備に起因する問題が山積している状態にある．

1.2 課題

本研究では，DNS における課題の内，DNS をデータ転送のメディアとして利用することでファイヤー・ウォールや IDS/IPS などのセキュリティラインを迂回する DNS Tunneling 手法に焦点を当てている．DNS Tunneling は，2014 年に発生した大規模なクレジットカード情報流出事件 [3] や最近では 2019 年に発生した APT グループ (通称,OilRig) による中東政府を標的とするサイバー攻撃の C2 通信 [4] といった実際の攻撃ベクターにデータ転送フェーズに使用されることが明らかになっている．上記以外にも，Tunneling メソッドを使用したマルウェアによるインシデントは多数報告されている [5, 6, 7, 8, 9, 10]．

Tunneling のメカニズムは，すなわち，現在の DNS のメカニズム，スタブリゾ

ルバがフルリゾルバを介在してコンテンツを所有する権威サーバへ問い合わせる仕組みには，本質的にデータ転送の機能としての側面があり，名前解決を実現するにあたり副次的に発生した設計上の脆弱であると考えることができる．この脆弱な設計により，悪意を持つユーザによって正規の利用方法な DNS Tunneling を用いることで容易にセキュリティラインを突破されるという具合である．

この DNS Tunneling に対して，従来の対策アプローチは，そのほとんどが検知に焦点が当てられてきた．DNS Tunneling を用いた場合の QNAME は，以下 (1) に示すように，一回あたりに転送するデータ量に比例して長いラベルを持つ特徴が現れる．

$$\begin{aligned} &obqxg43xmqytcmjr.exfil.com \\ &base32(password1111) = obqxg43xmqytcmjr \end{aligned} \tag{1}$$

また，インタラクティブなシェルなど双方向の通信を DNS Tunneling で実現しようとする場合，時間あたりに高頻度なトラフィックが発生するという特徴が現れることもある．これまでの既存の検知アプローチでは，上記のような特徴に基づいて以上のような特徴から，従来の検知アプローチは，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手法と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に大別することができる．

しかし，これら検知に基づくアプローチをバイパスする手法として，1 回あたりの転送データ量を少なくすることで特徴量を減らす Low Throughput なバイパス手法や，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ことでファイル肥大から一定期間しか保存されることがないログ管理の隙間を突いた Slow な Tunenling 手法が提案されており，これらを利用することで既存の検知手法をバイパスされるリスクが残留している．

転送量が少ないとして軽視されるべきではなく，1bit でも複数組み合わせる事などによって多種多様な情報量を送受信できることを踏まえると，脅威である．そこで，本研究では，従来の検知手法ベースの DNS Tunneling 対策では対策することが困難な Low Throughput および SLow な Tunneling 手法によるデータ流出を緩和するために，DNS Tunneling が発生しない新しい名前解決メカニズムを提

案する．

1.3 目的

背景で示すように，DNS にはラベルをデータ転送のキャリアとする Exfiltration のリスクがあり，なおかつ従来の検知による対策がバイパスされる潜在的な設計の脆弱性がある．本研究の目的は，DNS における Exfiltration の発生を防止である．これを実現するために，選抜的ノードに基づく P2P アーキテクチャによる情報流出に対応する名前解決システムを提案する．

1.4 貢献点

1.5 本論構成

本稿の構成は以下の通りである．まず第 1 章で，準備として，DNS プロトコル・秘匿通信・Tunneling メカニズム・分散データベースの 4 点について説明する．次に第 2 章で，先行研究が採用する検知アプローチにおける Low Throughput 手法・Slow Tunneling 手法に対する課題を説明する．第 4 章で提案手法とその実装について述べ，第 5 章で提案手法の性能評価と考察行い，第 6 章で残留する脅威モデルについ議論する．最後に，第 7 章で結論と今後の課題について述べる．

2. 準備

本章は第 3 章以降の要素補足を目的に，本論において核となる技術内容・特徴およびそのメカニズムについて説明する．

2.1 DNS

2.1.1 プロトコル概要

DNS は，インターネットに接続された無数のコンピュータを一意に識別するために，IP アドレスを人が認識しやすいドメイン名に変換する機能を担うネットワークプロトコルスタックの一つである．

IP アドレスは，現在 IP アドレスには，32bit の名前空間を持つ 10 進数で構成される IPv4(E.g. “192.168.0.1”) と，128bit の名前空間を持つ 16 進数で構成される IPv6(E.g. “2001:200:16a:8::230”) がある．このような 10・16 進数で構成される IP アドレスについて，コンピュータはそれらをバイナリで解釈するため都合がよい一方で，一般に人には記憶・認識することが困難である．IP アドレスのこのような文字列の側面における特性に対して，より人が認識しやすいよう ASCII コードで構成されるドメイン名という仕組みがある．DNS が担う役割は，IP アドレスをドメインに対応づける機能である．ドメイン名は，ルートを頂点として，63 文字と

にツリー構造をとり，ドット区切りで各ドメインが表現される．

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 メカニズム

2.1.3 DNS Tunneling 特徴

2.2 分散ハッシュテーブル

2.2.1 アルゴリズム

2.2.2 暗号学的ハッシュ関数

2.3 P2P

2.3.1 アーキテクチャ

3. 先行研究

3.1 検知アプローチ

3.1.1 パターンマッチング

3.1.2 同一ドメインあたりのクエリ頻度

3.1.3 Qname における文字列分布

3.1.4 Qname における長さとエントロピー

3.1.5 Low Throughput な Tunneling に対する検知手法

3.2 DNS アーキテクチャに基づく緩和アプローチ

3.2.1 Blockchain ベース - Namecoin, Blockstack

3.2.2 P2P ベース - GNS(Gnu Name System)

4. スーパーノード型P2Pに基づく名前解決システム

4.1 設計

4.2 アーキテクチャ

5. 評価

5.1 DNS Exfiltrationに対する定性評価

5.2 シミュレーション実験に基づく定量評価

5.2.1 シミュレーション実験構成

5.2.2 肥大化したリクエストペイロードサイズ

5.2.3 分析

5.2.4 RTT

5.2.5 分析

5.2.6 トラフィック量

5.2.7 分析

6. 議論

6.1 最適なハッシュ計算ノード

6.2 流入通信に対するリソースレコード

7. 結論

7.1 まとめ

7.2 今後の課題

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 specification. RFC 1035 (INTERNET STANDARD),” November 1987. Updated 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/. (accessd 2019-11-30).

[4] IronNet. “Chirp of the PoisonFrog,” February 2019. https://ironnet.com/blog/chirp-of-the-poisonfrog/. (accessd 2019-11-30).

[5] Nick Hoffman. “BernhardPOS,” July 2015. https://securitykitten.github.io/2015/07/14/bernhardpos.html. (accessd 2019-11-30).

[6] Fireeye. “MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry,” April 2016. https://www.fieeye.com/blog/threat-research/2016/04/multigrain_pointo.html. (accessd 2019-11-30).

[7] Palo alto Networks. “New Wekby Attacks Use DNS Requests As Command and Control Mechanism,” May 2016. https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/. (accessd 2019-11-30).

[8] Kaspersky. “Use of DNS Tunneling for C&C Communications,” April 2017. https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/. (accessd 2019-11-30).

[9] CISCO Talos. “Spoofed SEC Emails Distribute Evolved DNSMessenger,” October 2017. https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html. (accessd 2019-11-30).

[10] Cylance. “Threat Spotlight: Inside UDPoS Malware,” Febrary 27 2018. https://threatvector.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html. (accessd 2019-11-30).

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.