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

ドメインネームシステム (Domain Name System, DNS) は，ドメイン名 (E.g. www.example.com) をインターネット上でのノードの住所を表す IP アドレス (E.g. 93.184.216.34) に変換する機能を担っており，DNS を通じて特定した宛先に問い合わせることで我々はサービスにアクセスできている．現在のインターネットの利活用において，名前解決の仕組みは極めて重要な技術の一つである．しかし，性善説的な当時の設計に伴い生じた脆弱性を利用した攻撃がいくつか報告されている．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．その設計に起因する課題の内，DNS クエリのラベルおよびリソースレコード (Resource Record, RR) をデータ転送のメディアとする DNS Tunneling がある．

DNS Tunneling は，一般にフィルタリングされることが少ない DNS の特徴と DNS がデータ転送のメディアとして機能しているとは想像しない人の認知の隙間をついた手法であり，ファイヤー・ウォールや IDS/IPS といったセキュリティラインを突破するために使用される．このように本来の目的とは違う方法でデータを転送する手法は，一般に秘匿通信 (Covert Channel) と呼ばれる [3]．DNS Tunneling は，秘匿通信の代表例であり，マルウェアと C2(Command & Control) サーバとの通信の秘匿手法，または，ターゲットから取得したデータを外部に流出させるといった目的実行の手段として，実際のインシデントで広く利用されている [5, 6, 7, 8, 9, 10, 11, 12]．従来の DNS Tunnnling に対するアプローチには，検知による手法が採用されてきた．DNS Tunneling による DNS クエリは，以下 (1) に示すように，転送量に比例して長いラベルを持ち，ラベルとしての文字列制約を満たすためのエンコーディングによって高いエントロピーを示す特徴がある．

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

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．このような特徴に基づき，パターンマッチングや機械学習，文字列分布などのメソッドを用いた検知手法が過去に多数考案されてきた [13, 14, 15, 16, 17, 18]．それら検知手法は，かなり高い精度で分類を実現しているものがあるが，DNS Tunneling として検知する対象としているパケットには一般に利用することができる DNS Tunneling ツールキット [19, 20, 21] が使用され，それらは特に過剰な特徴量を示し，明らかに正規の DNS クエリと異なる特徴がある．高い精度を示す従来の検知手法だが，しかし，それらを迂回する手法として，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，また，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 手法があり，従来の検知手法では対応することが困難である．悪意を持つユーザの視点として，1bit でも転送できることは秘匿通信として利用することができるため，転送量の少なさは軽視されるべきではない．

他方で，DNS は初めに述べたように，現在のインターネットの根幹技術として根ざしており，抜本的な改変は期待されない．すなわち，既存の DNS による名前解決のメカニズムに大幅な改変を加えないという制約下で，Tunneling に対処することが現実的な最適解であると考える．

1.2 目的

本研究では，既存の DNS の名前解決メカニズムの大部分を流用することが一部の改変に留めながら，DNS を用いたデータ転送としての機能の排除を実現する次世代の名前解決メカニズムを提案する．

1.3 本論構成

本稿の構成は以下の通りである．まず第 2 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．第 3 章では，関連研究としてトラフィックおよびペイロード特徴に基づいた

検知手法を説明し，それら手法がLow Throughput 手法・Slow Tunneling 手法に対して検知が困難であることを説明する．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て議論する．最後に，第７章で結論と今後の課題について述べていく構成になっている．

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 プロトコル概要

DNS(Domain Name System) 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の IP アドレスを，人が認識しやすいドメイン名に変換するシステムである．元来，インターネット上でのホストの識別には IP アドレスが使用されてきた．しかし，32bit の名前空間で 10 進数表記の IPv4(E.g. “192.168.0.1”)，もしくは，128bit の名前空間で 16 進数表記の IPv6(E.g. “2001:200:16a:8::230”) は，人にとって認識しにくいものである．そのため，自然言語のようにアルファベットや数字で表記する方法が取られ，当初はその対応表である hosts.txt が中央集権的に管理されていたが，やがてホスト数の増大に伴い管理が困難になっていき，提案されたのが対応表を分散的に管理する DNS である．

DNS のシステムアーキテクチャは，クライアント・サーバ構成で成り立っている．一般に，クライアントがドメインを問い合わせた場合，サーバはドメインに対応づけている IP アドレスを応答することで，クライアントはドメインに対応づけられた IP アドレスを解決することができる．ドメインから IP アドレスの解決は正引きと呼ばれ，IP アドレスからドメインの解決を逆引きと呼ぶ．

ドメインは，数字とアルファベットおよびハイフン (“-”) の文字列で表記され，最大長は 63 オクテットと定義されている．また，ドメインはルートを頂点とする階層構造をとり，各階層にはドメインを管理する主体が存在し，管理主体を委譲することによって分散的にデータベースを管理する仕組みを取っている．

ドメイン名は，ドメインに相当するラベルをドット区切りで表され，最大長は 255 オクテットである．ドメイン名は右から順に階層序列が表現され，ドットで表現されるルートは一般には省略される．最も右に位置づくラベルが TLD(Top Level Domain) であり，その TLD から n 番目 ($n \mid n \in \mathbb{N}$) のラベルが第 n レベルドメインである．

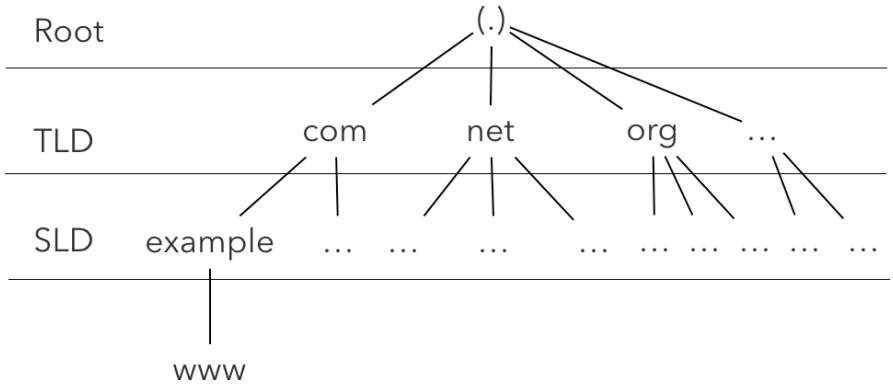

図 1 ドメインにおける名前空間

TLD を大別すると，“.com”や “.net”をはじめとした特定分野別の gTLD(global Top Level Domain)，“.jp”や “.ch”のような国ごとに割り当てられている ccTLD(Country Code Top Level Domain) の二つに分けられる．

2.1.1 ノードの種類

2.1.2 リソースレコード

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．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．

2.2 DNS Tunneling

DNS を利用して情報を外部に転送するには，初めにデータの宛先となるドメイン (E.g. exfil.com) を作成することになる．転送する際のキャリアとなる DNS クエリのラベルには，使用できる文字列は数字・アルファベット・ハイフン (“-”) である必要があるため，一般に Base32・64 を用いて転送したい情報をエンコーディングすることでこの制約条件を満たす．用意できた QNAME(E.g. arbitrary-string.exfil.com) について，例えば A のリソースレコードをクエリすると，サブ

ドメインの存在の有無に関わらず，宛先となるドメイン (exfil.com) に任意の情報を転送することができるという具合である．以下 3 に，DNS Exfiltration のメカニズムについて図解する．

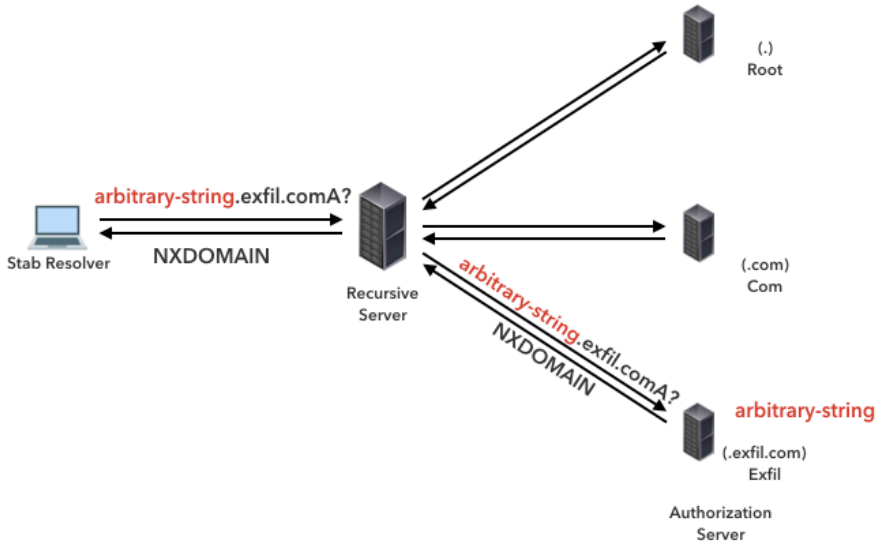

図 2　arbitrary-string という任意の文字列が，DNS クエリのラベル部を用いて，事前に用意した権威サーバ (exfil.com) に転送される様子．

また，管理する権威サーバのドメインに適当なホスト名 (E.g. www) を作成し，そのホスト名のリソースレコード (E.g. TXT) に情報を付与していた場合には，そのホストへの問い合わせを通じて逆方向，すなわち権威サーバから任意の情報を転送することができる．

このような DNS を用いて双方向な通信手法が DNS Tunneling である．

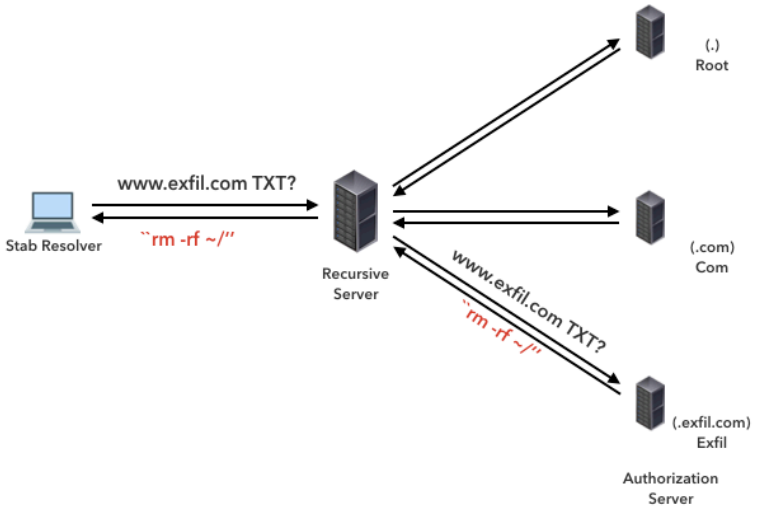

図 3 事前に TXT レコードに登録された情報を問い合わせることで，権威サーバからの命令情報を取得している様子．

3. 関連研究

本章では，これまでに提案されてきた検知手法について説明し，その課題を明らかにする．また，次世代 DNS として議論されている名前解決システムのアーキテクチャを説明し，Tunneling に対する課題を明らかにする．最後に，既存の検知手法および次世代名前解決システムの課題から，既存のシステムに迎合しながら DNS Tunneling を緩和する名前解決システムの必要性を明らかにする．

3.1 DNS Tunneling 検知に関する研究

これまで，DNS Tunneling に対する検知手法は数多く提案されてきたが，それらを分類すると，統計ベース・機械学習ベース多クラス・機械学習ベースバイナリクラスに区別することができる．

4. 提案手法

4.1 スーパーノード型 P2P に基づく名前解決システム

4.1.1 QNAME と RR を引数とするハッシュ値をキーとするクエリ

4.1.2 選抜ノードによる分散データベースの管理

4.1.3 選抜ノードをルートとするツリー構造

4.1.4 プロトコル

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 RTT(Round Trip Time)

5.2.4 トラフィック量

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] ICANN, “What Is an Internet Covert Channel?, ” August 2016. https://www.icann.org/news/blog/what-is-an-internet-covert-channel

[4] S. Bortzmeyer. “DNS Privacy Considerations, ” August 2015.

[5] KrebsonSecurity. “Deconstructing the 2014 Sally Beauty Breach,” May 2015. https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/. (accessd 2019-11-30).

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

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

[8] 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).

[9] 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).

[10] 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).

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

[12] 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).

[13] K. Born and D. Gustafson, "NgViz: detecting DNS tunnels through n-gram visualization and quantitative analysis," Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee, 2010, pp. 1-4.

[14] Cheng Qi, Xiaojun Chen, Cui Xu, Jinqiao Shi, Peipeng Liu, "A Bigram based Real Time DNS Tunnel Detection Approach," Procedia Computer Science, Volume 17, 2013, Pages 852-860.

[15] J. Liu, S. Li, Y. Zhang, J. Xiao, P. Chang and C. Peng, "Detecting DNS Tunnel through Binary-Classification Based on Behavior Features," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, pp. 339-346.

[16] Asaf Nadler, Avi Aminov, Asaf Shabtai, "Detection of malicious and low throughput data exfiltration over the DNS protocol," Computers & Security, Volume 80, 2019, Pages 36-53.

[17] J. Steadman and S. Scott-Hayward, "DNSxD: Detecting Data Exfiltration Over DNS," 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Verona, Italy, 2018, pp. 1-6.

[18] J. Ahmed, H. H. Gharakheili, Q. Raza, C. Russell and V. Sivaraman, "Monitoring Enterprise DNS Queries for Detecting Data Exfiltration from Internal Hosts," in IEEE Transactions on Network and Service Management.

[19] "OzymanDNS - Tunneling SSH over DNS," https://room362.com/post/2009/2009310ozymandns-tunneling-ssh-over-dns-html/, accessed: 2019-11-20.

[20] "iodine," http://code.kryo.se/iodine/, accessd: 2019-11-20.

[21] "DNScat2," https://github.com/iagox86/dnscat2, accessed: 2019-11-20.

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.