修士論文

ペイロード特徴に基づいた Incoming DNS Tunneling 検知

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）

ペイロード特徴に基づいたIncoming DNS Tunneling検知*

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，Domain Name System(DNS)，秘匿通信，Tunneling，機械学習

*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.

Detecting Incoming DNS Tunneling Based on Payload Features*

Shoretsu Takasuka

Abstract

Keywords:

Network Security, Domain Name System(DNS), Covert Channel, Machine Learning

*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，おおよそ全てのサービスの通信は，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として開始される．DNS の名前解決の機能を通じて，インターネット利用者は，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，そのコンセプトとなる RFC1034, RFC1035([1, 2]) が公開されて以降なお現在まで，当時採用された名前解決の根幹の仕組みは変わることなく使用されている．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

1.4 貢献点

- 侵入通信を目的とする DNS Tunneling に対するリアルタイム検知アルゴリズムの提案
- 既存対策アプローチと DNS の潜在的データ転送脅威モデルの検討

1.5 本論構成

本論の構成は，次の通りに構成されている．第二章では，本論の内容への準備として，DNS プロトコル，Tunneling メカニズム，秘匿通信，オンライン機械学習などの核となる技術要素について説明する．第三章では，DNS Tunneling に対する検知アプローチおよびセキュリティドリブンな次世代 DNS プロトコルに関する先行研究を説明する．第四章では，提案手法について説明する．第五章では，提案手法の効果測定について，またその結果について説明する．第六章では，提案手法および既存研究で対処しきれていない残留する脅威モデルについてまとめ，さらに DNS プロトコルにおけるリソースレコードの現状の使用方法の課題について説明する．最後に，第七章にて結論を述べる．

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 プロトコル解説

インターネットの利活用において，おおよそ全てのサービスの通信は，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として開始される．DNS の名前解決の機能を通じて，インターネット利用者は，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．

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 リソースレコード (RR)

2.1.3 Tunneling メカニズム

2.2 秘匿通信

秘匿通信 (英 Covert Channel) とは，情報転送を実現するにあたり，データの転送を本来の設計としていないプロトコルにそのデータを注入する手法である．

2.2.1 ステガノグラフィ

2.2.2 代替プロトコル

2.3 機械学習

2.3.1 概要

2.3.2 ランダムフォレスト

2.3.3 SVM

2.3.4 ロジスティック回帰

2.3.5 ニューラルネットワーク

3. 先行研究

3.1 パターンマッチングによる検知

3.2 トラフィック特徴に基づいた悪性 DNS クエリの検知

3.2.1 同一ドメインあたりのクエリ頻度

3.3 ペイロード特徴に基づいた悪性 DNS クエリの検知

3.3.1 Qname における文字列分布

3.3.2 Qname における長さとエントロピー

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

3.4 次世代 DNS による緩和

3.4.1 分散ハッシュテーブルベース - GNS(Gnu Name System)

3.4.2 Blockchain ベース - Namecoin, Blockstack

4. 機械学習によるリアルタイム検知モデル

4.1 概要

4.2 本研究の位置づけ

4.3 特徴量分析

4.4 データセット

4.5 分類アルゴリズム

5. 評価

5.1 実験概要

5.2 データセット

5.3 DNS Tunneling ツールキット

5.4 結果

5.5 課題

6. 議論

6.1 脅威となるバイパス手法

6.1.1 1パケットあたりの転送量の削減

6.1.2 同一ドメインに対する時間あたりのパケット頻度

6.1.3 一般的ラベルへのマッピング

6.2 データ転送キャリアとして脅威なリソースレコード

6.2.1 CNAME, MX

6.2.2 DNSKEY - 公開鍵検証

6.2.3 TXT - ドメイン検証

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.