一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SITE2021-59,IA2021-72(2022-03)

DGAベースのマルウェアが生成した不審なDoH通信の検知システムに関する一検討

三橋　力麻[†,††]　金　　勇[†††]　飯田　勝吉[††]　品川　高廣[††††]　高井　昌彰[††]

† 東京大学大学院情報理工学系研究科　〒113–8658 東京都文京区弥生 2–11–16
†† 北海道大学　〒060–0811 北海道札幌市北区北 11 条西 5 丁目
††† 東京工業大学　〒152–8550 東京都目黒区大岡山 2–12–1
†††† 東京大学　〒113–8658 東京都文京区弥生 2–11–16
E-mail: †mitsuhashi@os.ecc.u-tokyo.ac.jp, ††{iida,ytakai}@iic.hokudai.ac.jp, †††yongj@gsic.titech.ac.jp, ††††shina@ecc.u-tokyo.ac.jp

あらまし　DNS over HTTPS（DoH）プロトコルは, プライバシー保護や改ざん防止などが期待できる一方で, マルウェアによって生成された不審なドメイン名の検知が困難になる問題がある. 近年, OS レベルでの DoH サポートが普及しつつあるため, DGA ベースのマルウェアを用いたサイバー攻撃の早期発見が困難になることが予想される. 本研究では機械学習技術を用いた分類方法により, Web アクセスなど一般的な HTTPS トラフィックと, DGA ベースのマルウェアが生成した DoH トラフィックを分類するシステムを検討する.

キーワード　DNS over HTTPS, DoH, トラフィック分類, 機械学習, DGA ベースのマルウェア

A proposal of detection system for malicious DoH communication generated by DGA-based malware

Rikima MITSUHASHI[†,††], Yong JIN[†††], Katsuyoshi IIDA[††], Takahiro SHINAGAWA[††††], and Yoshiaki TAKAI[††]

† Graduate School of Information Science and Technology, the University of Tokyo　2–11–16 Yayoi, Bunkyo-ku, Tokyo, 113–8658 Japan
†† Hokkaido University　Kita11, Nishi5, Kita-ku, Sapporo, Hokkaido, 060–0811 Japan
††† Tokyo Institute of Technology　2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan
†††† The University of Tokyo　2–11–16 Yayoi, Bunkyo-ku, Tokyo, 113–8658 Japan
E-mail: †mitsuhashi@os.ecc.u-tokyo.ac.jp, ††{iida,ytakai}@iic.hokudai.ac.jp, †††yongj@gsic.titech.ac.jp, ††††shina@ecc.u-tokyo.ac.jp

Abstract　The DNS over HTTPS (DoH) protocol can provide privacy-protection and data-tampering for Internet users. However, DoH has a problem that makes it difficult for network administrators to detect malicious domain names generated by malware. Unfortunately, the widespread use of DoH support at the OS level is predicted to make early detection of cyber attacks using DGA-based malware more difficult. In this research, we propose a machine learning based system that filter the DoH traffic from the HTTPS traffic such as web access and then recognize the malicious DoH traffic generated by DGA-based malware.

Key words　DNS over HTTPS, DoH, Network traffic classification, Machine learning, DGA-based malware

1. はじめに

プライバシー保護や改ざん防止などを目的として, インターネット上の DNS トラフィックを暗号化するためのシステム環境整備が進んでいる. 暗号化の手法としては, HTTPS を介して DNS を送受信し, 443 ポートを使用する DNS over HTTPS（DoH）と, DNS クエリ／レスポンスを直接暗号化し, 853 ポートを使用する DNS over TLS（DoT）があるが, 既存のファイア

ウォールとの親和性が高いことなどから, DoH の普及が先行している. クライアントにおける DoH サポートは, これまで Chrome, Firefox, Edge などのブラウザが先行してきたが, 近年では OS レベルでの DoH サポートが進んできた. 例えば, 2021 年 10 月にリリースされた Windows 11 では, DoH による DNS 接続の暗号化機能を搭載した [1]. また, 2020 年 9 月にリリースされた MacOS 11 と iOS 14 では, DoH 接続のネットワーク設定を行うための NEDNSsettingsManager [2] の提供を開始した. 現在のところ, これらの OS で DoH 機能を使うためにはユーザが設定を有効にする必要があるが, 今後は標準設定になることが予想される. また, Linux では, DoH プロキシソフトウェアである DNS-over-HTTPS [3], DNSCrypt [4], doh-client [5] などを導入することで, OS レベルの DoH サポートと同等の機能を実現できる.

DoH を用いて DNS トラフィックを暗号化すると, インターネットユーザは訪問したウェブサイト名を盗聴されるなどのリスク低減が期待できるが, ネットワーク管理者はマルウェア感染の早期発見を目的としたネットワークトラフィックの分析が困難になる問題がある. 従来は, マルウェアが DNS を使ってインターネット上の Command and Control(C&C) サーバのドメイン名解決を試みた場合, ドメイン名は平文でやり取りされていたため, ネットワーク管理者がドメイン名を分析することができた. 一方で, DoH を使ったドメイン名解決では, 暗号化によってドメイン名は隠ぺいされるため, マルウェアが行った名前解決の通信であるかどうかを判断することが難しくなる. しかしながら, ネットワークトラフィックを使ってマルウェア感染を早期発見することは, ネットワークのセキュリティレベルを維持するために重要である. マルウェアが生成した DoH トラフィックを検知し, 発信元のクライアントを特定することによって, ネットワーク管理者は, 1) クライアントから外部 Web サイトへ接続する通信を遮断すること, 2) クライアントの利用者に注意喚起すること, 3) マルウェア対策のセキュリティポリシーを改善すること, などが可能になる.

我々は不審な DoH トラフィックを生成するマルウェアとして, Domain Generation Algorithm (DGA) を使用する DGA ベースのマルウェアに着目した. DGA は大量でランダムなドメイン名（DGA ドメイン名）を自動生成するアルゴリズムである. DGA ベースのマルウェアは, 生成したドメイン名を使って C&C サーバに接続できるまで, 名前解決のためのクエリを送り続ける特徴がある. DoH による DGA ドメイン名の解決を図 1に示す. 感染したクライアント上でマルウェアが生成した DGA ドメイン名は, OS によって DNS から DoH に変換され, クライアントと DoH サーバとの間のトラフィックが暗号化される. また, DoH サーバはインターネット上の権威 DNS サーバとの間で従来の DNS プロトコルを使用してドメイン名解決を行う. DGA ベースのマルウェアを使った攻撃は最近も活発に行われている [6]. 先行研究では, DGA ベースのマルウェアが生成したドメイン名を分類・検知するための様々な手法が提案されている [7] [8] [9] [10]. しかし, それらの手法は, ドメイン名が平文で通信される従来の DNS 通信を前提としているため, DoH で暗

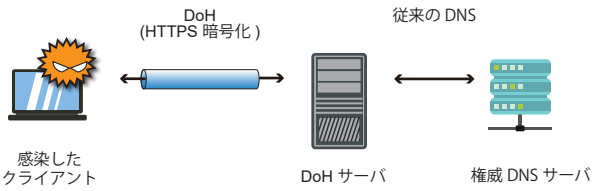

図 1　DoH による DGA ドメイン名の解決

号化されたドメイン名にそのまま適用することは難しい.

近年では, 暗号化されたネットワークトラフィックを機械学習で分類するための研究が多数報告されている [11]. しかし, DNS 暗号化技術は歴史が浅く, まだ完全には実用化されていないため, DoH トラフィックの分類に関する研究報告はそれほど多くない [12] [13]. DoH で暗号化された DGA ベースのマルウェアによる通信を機械学習で検知するためには, いくつかの課題がある. 一つ目に, マルウェアが生成した大量の名前解決の通信を DoH で暗号化する必要がある. 二つ目に, DGA ベースのマルウェアによる通信を検知するための特徴量は, パケットヘッダ, パケット番号, パケット長, パケット方向, パケット間の到着間隔など, DoH トラフィックの中から有効に機能するものを探し出す必要がある. 三つ目に, 高い分類精度を得るためには DGA ベースのマルウェアが発生した DoH 通信に合わせて, 適切な機械学習モデルを選択し、チューニングする必要がある. このように機械学習技術を用いて DGA ベースのマルウェアが生成した DoH 通信を検知するためには時間と手間がかかるが, ひとたび機械学習モデルが稼働すれば DoH トラフィックを自動的に解析することができる.

本研究では, DoH トラフィックを分類する機械学習技術を用いて, DGA ベースのマルウェアによって生成された通信の検知システムを提案する. 図 2に示すように, 提案システムは階層的なネットワークトラフィックの分類を用いる. 第一段階で HTTPS から DoH を抽出し, 第二段階で不審な DoH 通信（Malicious DoH）を検知する. また, 各段階の分類に適した機械学習モデルを選択することによって, より高い精度での検知を目指す.

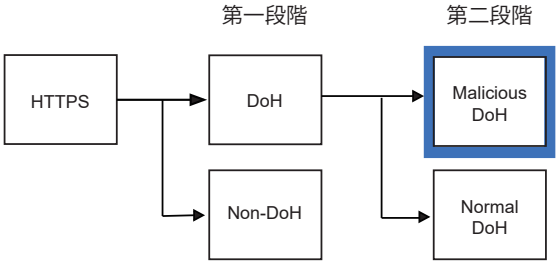

図 2　階層的なネットワークトラフィック分類の概要

2. 関 連 研 究

2.1 DGA によって生成されたドメイン名の検出

DGA によって生成されたドメインを検出するために様々な研究が提案されており, 近年では, 機械学習やディープラーニングを使った手法の提案が増えている [10]. 最近報告された DGA ドメイン名の検出に関する研究を見ると, Y. Zhang ら [14] は, クラスタリング手法を用いて, 同じ DGA ファミリーに属するドメイン名を集約した. 実験の結果, 22 種類の DGA ファミリーを分析し, 6 つに集約された DGA ファミリーを識別した. R.R. Curtin らは [15], DGA ドメイン名がどれだけ英単語に似ているかを測定するスマッシュワードスコアの概念を考案し, リカレント・ニューラル・ネットワーク・アーキテクチャとドメイン登録サイド情報を組み合わせたアプローチを用いて, matsnu, suppobox, rovnix などの DGA ファミリーを検出できることを示した. M.A. Ayub らは [16], DGA のデータセットに対して, Bigram モデルと Word2Vec モデルの特徴抽出法を用いて, 機械学習および深層学習に適用する手法を提案した. 84 種類の DGA ファミリーと辞書ベースの DGA ファミリーを分類した. Plohman らは [17], 43 種類の DGA ファミリーを分析し, DGA ドメイン名の発生状況を測定した.

これらの研究はいずれも DGA によって生成されたドメイン名を検出するために有効に機能しているが, ドメイン名が平文でやりとりされる従来の DNS を前提としているため, DoH によって暗号化されたドメイン名にそれらの手法をそのまま適用することは難しい問題がある.

2.2 暗号化ネットワークトラフィックの分類

暗号化ネットワークトラフィックの分類は，現在, 非常に活発な研究分野である [11]. しかし，DNS 暗号化技術は歴史が浅く, まだ完全には実用化されていないため，DoH のトラフィック分類に関する研究報告はそれほど多くない.

最近報告された DoH ネットワークの分類に関する研究を見ると, D. Vekshin ら [12] は, 機械学習を用いて HTTPS トラフィックを分類することで その中に含まれる DoH トラフィックを抽出した. また, DoH トラフィックを分類することで, Chrome, Firefox, Cloudflare などの DoH クライアントを特定した. 機械学習モデルには Ada-boost を使用し，99.9% の分類精度を得た. データセットには，Alexa [18] が提供する上位 100 万の Web サイトを使って, ドメイン名へのアクセスデータを収集した. M. MontazeriShatoori ら [13] は，機械学習技術を用いて HTTPS トラフィックから DoH トラフィックを抽出し，その後, DoH トラフィックを良性の DoH トラフィックと悪性の DoH トラフィックに分類する仕組みを提案した. この悪性の DoH トラフィックとは, DNS トンネルツールが生成したトラフィックである. R. Mitsuhashi ら [19] は，階層的なネットワークトラフィック分類を用いて, 悪意のある DNS トンネルツールの種類を識別した. データセットには CIRA-CIC-DoHBrw-2020 を用いた.

以上をまとめると, 我々が知る限り, DGA によって生成されたドメイン名の検出および暗号化ネットワークトラフィックの分類の研究分野ではいずれも, DoH 上で不審な DGA トラフィックを検知する手法については報告されていない. 我々は, 階層的なネットワークトラフィックの分類を用いて, DGA ベースのマルウェアが生成した不審な DoH トラフィックの検知を目指す.

3. 設　　計

2 節では, DGA が生成したドメイン名の検出に関する関連研究を紹介し, 暗号化ネットワークトラフィックの分類手法を調査した. 先に述べたとおり, ネットワーク管理者がネットワークセキュリティを維持するためには, DoH トラフィックの中から不審な DGA 通信を検知する必要がある. 本節では, 提案システムの設計について説明する.

3.1 システムの全体像

DoH トラフィックから不審な DGA トラフィックを検知するために，階層的な分類手法を導入する. 図 3にシステムの全体像を示す.

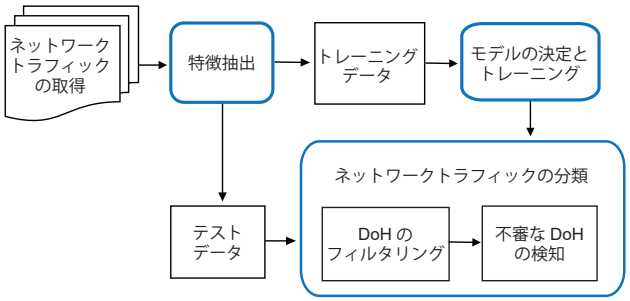

図 3　提案システムの全体像

3.2 ネットワークトラフィックの取得と特徴抽出

DoH は HTTPS を介して DNS トラフィックを送受信するため, 提案するシステムは HTTPS トラフィックを入力データとする. ネットワーク上には様々な種類のトラフィックが流れているが, パケットの送信元または送信先のポート番号から, HTTPS によって生成されたトラフィックであるかどうかを判定することができる. HTTPS トラフィックは図 4に示したポイントで収集する. クライアントが Web サーバに接続する目的は, web コンテンツを取得することである. また, クライアントはドメイン名を解決するために, DoH サーバを経由して通常の DNS サーバに接続する. クライアントに感染した DGA ベースのマルウェアは C&C サーバに接続するための IP アドレスを得るために, DoH サーバを経由してドメイン名解決を行う.

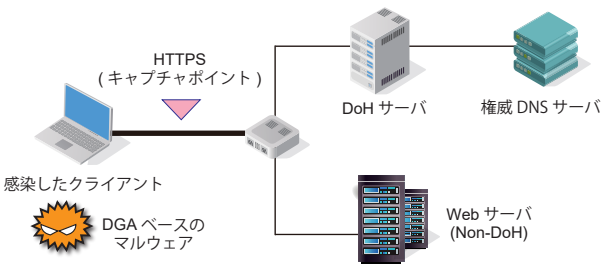

図 4　ネットワーク接続とキャプチャポイント

取得したネットワークトラフィックを機械学習モデルで分類するために，双方向通信の HTTPS トラフィックフローを定義する．トラフィックフローは，送信元 IP アドレス，送信先 IP アドレス，送信元ポート番号，送信先ポート番号で決定される．これらはパケットのヘッダに含まれている情報であり, 暗号化されていないため利用できる．トラフィックフローの統計的な特徴量は, 例えば, パケット数, パケットの方向, パケットの到着時間, パケットの長さなどから抽出する．ただし, パケットのペイロードは暗号化されているため, その内容は利用しない．

4. 評価の実施に向けた準備

DoH によって暗号化された DGA ドメイン名のトラフィック（Malicious DoH）を生成するために, DGA ベースのマルウェアをサンドボックス環境で稼働させる方法を検討している．ただし, 高度な機能を持つ DGA ベースのマルウェアは, サンドボックス環境（インターネットにつながっていない環境）を検知して, その動作を抑制する可能性がある．そのため, 疑似マルウェア作成することによってトラフィックを生成する方法も合わせて検討している．

DoH で暗号化された DGA を検知するためのネットワークトラフィック分類に適した機械学習モデルを今後選定する．また, 高い分類精度を得るために, 適切なパラメータチューニングを行うことを予定している．

ネットワークトラフィック分類の実施するためには, 一般的なウェブアクセスに伴う HTTPS コンテンツデータ（Non-DoH）と名前解決の DoH トラフィック（Normal DoH）を用意する必要がある．これらのデータは CIRA-CIC-DoHBrw-2020 データセット [20] から抽出することを想定している．

5. おわりに

DoH は, DNS トラフィックを暗号化することで, インターネットユーザにセキュリティとプライバシーを提供するために開発された．しかし, DoH には, ネットワーク管理者がネットワークセキュリティを確保するためのトラフィック分析が困難になる問題がある．DGA ベースのマルウェアが生成したドメイン名の検出や, 暗号化されたネットワークトラフィックの分類に関する研究は数多く報告されているが, DoH は新しいプロトコルであるため, これまでの研究成果をそのまま適用することは難しい状況にある．

本報告では, DGA ベースのマルウェアが生成した不審な DoH トラフィックを特定する方法を検討した．DoH トラフィックのペイロードは暗号化されているため, パケットペイロードに依らない統計的な特徴量を利用してトラフィックを詳細に分析する方法を提案した．また, 評価の実施に向けた準備について述べた．

文　献

[1] “How to Enable DNS Over HTTPS on Windows 11”. https://www.howtogeek.com/765940/how-to-enable-dns-over-https-on-windows-11/.

[2] “DNS on IOS v14 in Apple Developer Forums”. https://developer.apple.com/forums/thread/663371.

[3] “DNS-over-HTTPS”. https://github.com/m13253/dns-over-https.

[4] “DNSCrypt”. https://github.com/DNSCrypt.

[5] “doh-client”. https://docs.rs/crate/doh-client/1.1.5.

[6] Paloalto, “Newly Registered Domains: Malicious Abuse by Bad Actors”. https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/.

[7] H. Ichise, Y. Jin, and K. Iida, “Analysis of DNS TXT Record Usage and Consideration of Botnet Communication Detection,” IEICE Transactions on Communications, vol.E101, no.1, pp.70–79, 2018.

[8] H. Ichise, Y. Jin, K. Iida, and Y. Takai, “NS record History Based Abnormal DNS traffic Detection Considering Adaptive Botnet Communication Blocking,” IPSJ Journal of Information Processing, vol.28, pp.112–122, 2020.

[9] Y. Iuchi, Y. Jin, H. Ichise, K. Iida, and Y. Takai, “Detection and Blocking of DGA-based Bot Infected Computers by Monitoring NXDOMAIN Responses,” Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp.82–87, 2020.

[10] S. Ajmera and T.R Pattanshetti, “A Survey Report on Identifying Different Machine Learning Algorithms in Detecting Domain Generation Algorithms within Enterprise Network,” Proceedings of 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp.1–5, 2020.

[11] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, “Mobile Encrypted Traffic Classification Using Deep Learning: Experimental Evaluation, Lessons Learned, and Challenges,” IEEE Transactions on Network and Service Management, vol.16, no.2, pp.445–458, 2019.

[12] D. Vekshin, K. Hynek, and T. Cejka, “DoH Insight: Detecting DNS over HTTPS by Machine Learning,” Proceedings of the 15th International Conference on Availability, Reliability and Security, pp.••–••, ARES ’20, 2020.

[13] M. MontazeriShatoori, L. Davidson, G. Kaur, and A. Habibi Lashkari, “Detection of DoH Tunnels using Time-series Classification of Encrypted Traffic,” Proceedings of 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp.63–70, 2020.

[14] Y. Zhang, Y. Wu, and S. Jin, “Which DGA Family does A Malicious Domain Name Belong To,” Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), pp.53–60, July 2020.

[15] R.R. Curtin, A.B. Gardner, S. Grzonkowski, A. Kleymenov, and A. Mosquera, “Detecting DGA Domains with Recurrent Neural Networks and Side Information,” Proceedings of the 14th International Conference on Availability, Reliability and Security, pp.••–••, ARES ’19, 2019.

[16] M.A. Ayub, S. Smith, A. Siraj, and P. Tinker, “Domain Generating Algorithm based Malicious Domains Detection,” Proceedings of the 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp.77–82, June 2021.

[17] D. Plohmann, K. Yakdan, M. Klatt, J. Bader, and E. Gerhards-Padilla, “A comprehensive measurement study of domain generating malware,” Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), pp.263–278, 2016.

[18] “Amazon Alexa Voice AI”. https://developer.amazon.com/en-US/alexa/.

[19] R. Mitsuhashi, A. Satoh, Y. Jin, K. Iida, T. Shinagawa, and Y. Takai, “Identifying Malicious DNS Tunnel Tools from DoH Traffic Using Hierarchical Machine Learning Classification,” Information Security, pp.238–256, 2021.

[20] “CIRA-CIC-DoHBrw-2020”. https://www.unb.ca/cic/datasets/dohbrw-2020.html.