様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 １ 日現在

機関番号：２４４０５
研究種目：研究活動スタート支援
研究期間：2019～2022
課題番号：１９Ｋ２４３５１

研究課題名（和文）DNSトンネリング経由標的型攻撃に対する普遍的特徴量を用いた検知手法に関する研究

研究課題名（英文）A Study on Detection Methods Using Cache-Property-Aware Features Against Targeted Attacks Through DNS Tunneling

研究代表者
近藤　大嗣（Kondo, Daishi）

大阪公立大学・大学院情報学研究科　・助教

研究者番号：１０８４４１６０

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：標的型攻撃による情報漏洩問題は極めて深刻な社会問題であり、その中でもDNSトンネリングを利用した情報漏洩が確認されている。このDNSトンネリング自体の関連研究は複数存在し、有効な検知手法が提案されている。しかしこれらの手法は、特定マルウェアや特定トンネリングツールから得られる特徴量を元に構築されているため、攻撃者はこのような特徴量を生み出さないマルウェアを作成して、検知手法をバイパスすることは容易であると考える。本研究では、情報漏洩を実現するために必ずDNSキャッシュサーバ中に現れる普遍的な特徴量に注目して、汎用性のあるDNSトンネリング検知手法を提案した。

研究成果の学術的意義や社会的意義
本研究では標的型攻撃による情報漏洩を防止することを目指し、特定のDNSトンネリングトラフィックに依存しない汎用性のあるDNSトンネリング検知手法を提案した。そのためにDNSトンネリングトラフィックが発生したことによりDNSキャッシュサーバ中に現れる普遍的な特徴量であるキャッシュミスに注目した。研究代表者の調査によると、この特徴量を利用した関連研究は存在しなかった。そのため、新規性という観点から学術的意義があった。また、社会問題である標的型攻撃による情報漏洩問題に取り組んだ点から社会的意義もあった。

研究成果の概要（英文）：Many enterprises are under threat of targeted attacks aiming at data exfiltration. To launch such attacks, in recent years, attackers with their malware have exploited DNS tunneling. Although several research efforts have been made to detect DNS tunneling, the existing methods rely on features that advanced tunneling techniques can easily obfuscate by mimicking legitimate DNS clients. Such obfuscation would result in data leakage. To tackle this problem, we focused on a "trace" left by DNS tunneling that cannot be easily hidden. In the context of data exfiltration by DNS tunneling, the malware connects directly to the DNS cache server and the generated DNS tunneling queries produce cache misses with absolute certainty. In this study, we propose a DNS tunneling detection method based on the cache-property-aware features.

研究分野：コンピュータサイエンス

キーワード：ネットワークセキュリティ　DNSトンネリング　標的型攻撃

１．研究開始当初の背景

標的型攻撃による情報漏洩問題は極めて深刻な社会問題であり、その中でも Domain Name System (DNS)トンネリングを利用した情報漏洩が確認されている。DNS トンネリングとは、DNS クエリ中のドメイン名と対応する DNS レスポンスを利用することによって、データ等をトンネリングする技術である。この DNS トンネリング自体の関連研究は複数存在し、有効な検知手法が提案されている。しかしこれらの手法は、特定マルウェアや特定トンネリングツールから得られる特徴量を元に構築されているため、攻撃者はこのような特徴量を生み出さないマルウェア（例えば、一般ユーザの行動を模倣するマルウェア）を作成して、検知手法をバイパスすることは容易であると考える。そのため、様々な未知の DNS トンネリングトラフィックに対しては対処できないという根本的な問題が存在する。

２．研究の目的

特定の DNS トンネリングトラフィックに依存しない汎用性のある DNS トンネリング検知手法を設計し、標的型攻撃による情報漏洩を防止することを目指す。

３．研究の方法

DNS トンネリングトラフィックが発生したことにより DNS キャッシュサーバ中に必ず現れる普遍的な特徴量に注目する。その 1 つにキャッシュ特性がある。通常のインターネット利用を考えると Google 等のサーチエンジン経由で Web ページにアクセスを行い、アクセスした Web ページの IP アドレスは DNS キャッシュサーバにキャッシュされている可能性が高い。一方、DNS トンネリングを利用した場合、外部ネットワーク中の攻撃者に対して通信用の Fully Qualified Domain Name (FQDN)を新規作成するため、その FQDN を含む DNS クエリはキャッシュヒットを生み出さない。さもなければその DNS クエリは攻撃者まで届かず、マルウェアと攻撃者間で通信を行うことは不可能である。この特徴は特定マルウェアや特定ツールに依存しない普遍的なものであり、本研究代表者の調査によるとこのキャッシュ特性という特徴量を利用している関連研究は存在しない。

まず、本研究代表者の所属研究室から、通常ユーザとして集われた複数の被験者の通常 DNS トラフィックに加えて、マルウェアの DNS トラフィックの取得が困難であるため、代わりに DNS トンネリングツールを利用して発生させた DNS トラフィックを測定する。そして、その測定点において、DNS トラフィックに対するキャッシュ特性を時系列解析によって評価を行い、DNS トンネリングトラフィック発生時にてキャッシュ特性に変化があることを検証する。そしてその変化の検証後、時系列データの深層学習において有効性が確認されている Long Short-Term Memory (LSTM)を適用してフィルタを設計・作成する。

４．研究成果

(1) DNS トンネリング経由標的型攻撃に対する普遍的特徴量を用いた検知手法に関する研究

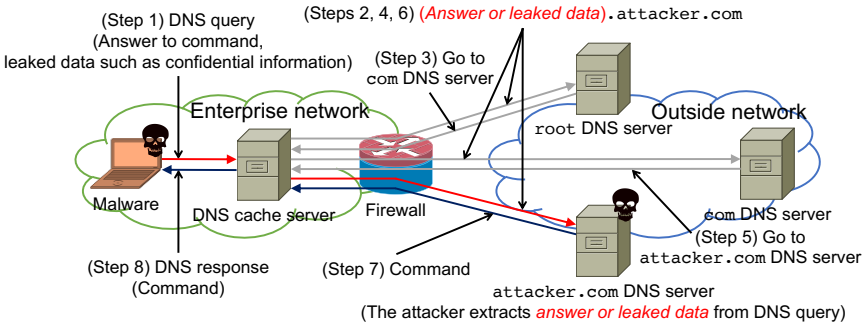

図 1：DNS トンネリングの概要

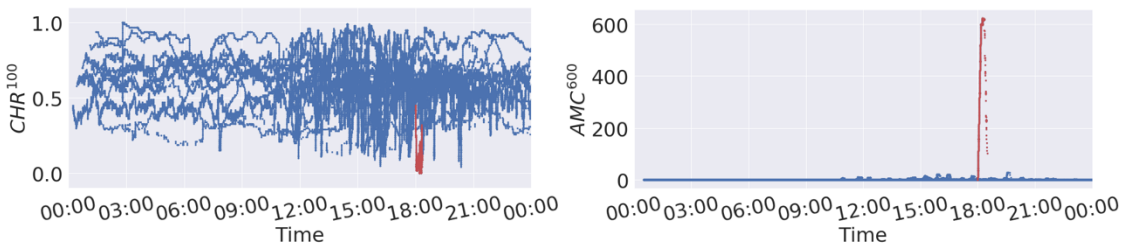

図 2：全クライアントのキャッシュヒット率 *CHR* とアクセスミスカウント *AMC*（赤線は DNS トンネリングトラフィックを示している）

DNS トンネリングトラフィックが発生する場合、生成された FQDN を含む DNS クエリはキャッシュヒットを生み出さない（図 1）。そこで、キャッシュ特性に基づく特徴量として、キャッシュヒット率（図 2 左グラフ）を計測した。DNS トンネリングによりキャッシュヒット率は低下すると予想したが、得られたキャッシュヒット率から、トンネリングトラフィックだけでなく、通常の DNS トラフィックによってもキャッシュヒット率が低下することが確認されたため、キャッシュヒット率による DNS トンネリング検知は困難であると考えた。そのため、通常のキャッシュミスによる影響を取り除くように改良した特徴量であるアクセスミスカウント（図 2 右グラフ）を提案し計測したところ、トンネリングトラフィックを特徴づけることに成功した。

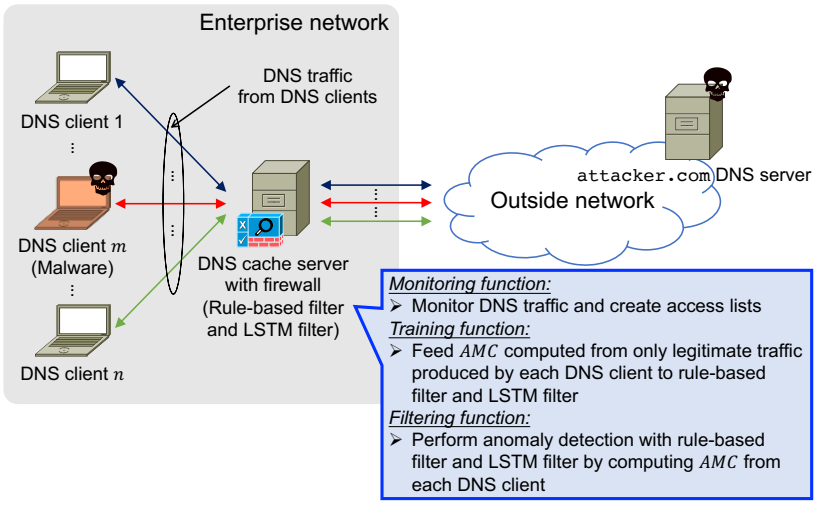

図 3：モニタリング及びフィルタリングシステムの設計概要

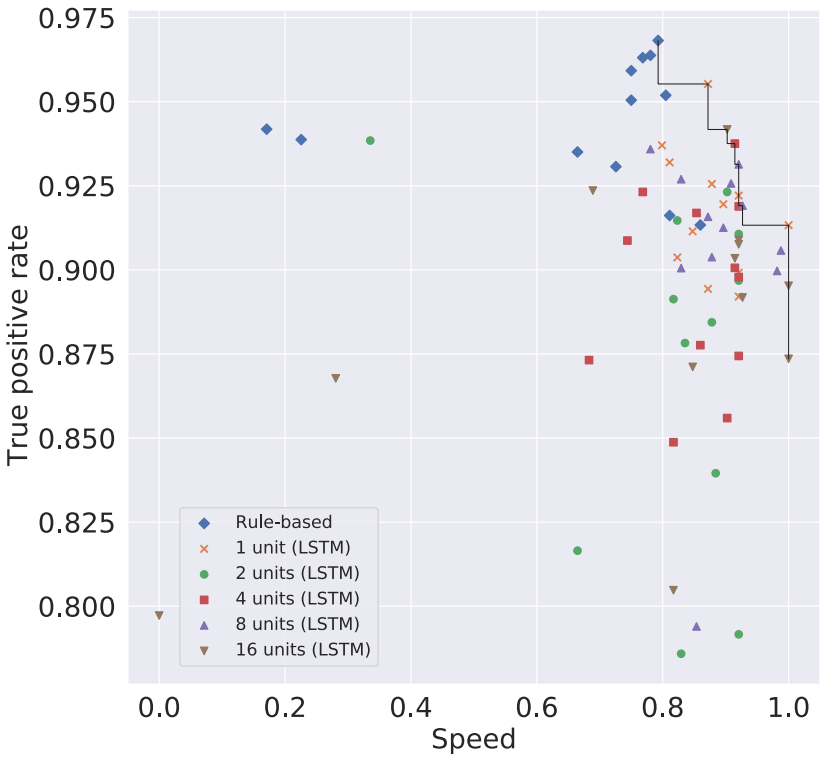

図 4：偽陽性率が 0.025 におけるパレートフロント

このアクセスミスカウントを利用して検知フィルタを作成するため、LSTM を利用した。また、図 2 右グラフからトンネリングトラフィックをアクセスミスカウントの閾値によって検知可能と考えたため、ルールベースのフィルタも作成した。図 3 は提案するモニタリング及びフィルタチングシステムの設計概要を示している。図 4 に真陽性率と攻撃検知スピードに基づいたパレートフロントを示している。この図から、ルールベースフィルタは LSTM フィルタよりも高い真陽性率を示す傾向であることがわかった。一方、LSTM フィルタはルールベースフィルタよりもより早く攻撃を検知する傾向であることがわかった。これは、LSTM フィルタが時系列データを予測することにより、早い攻撃検知を実現したと考えられる。つまり、LSTM フィルタで早期に

攻撃を検知して異常なクライアントを特定し、その後ルールベースフィルタを用いてそのクライアントを隔離するかを決定するようなフィルタ運用を実行することができる。

本研究で提案したキャッシュ特性に基づく特徴量は、低スループットで DNS トンネリングトラフィックが生成された場合、その特徴が顕著に現れない。そこで今後の展開として、このような低スループットで情報漏洩を行なう攻撃を検知するための提案を行なう。また、攻撃者としては生成 AI のような技術を利用して、通常クライアントによるトラフィック生成を模倣したマルウェアを作成するような事例が登場する可能性がある。低スループットの攻撃だけでなく、生成 AI ベースの攻撃も視野にいれ、そのような攻撃が実行された場合の漏洩データ量の評価を行なう。

(2) Web ブラウザから 1 語の検索クエリが DNS に漏れる問題の実態調査と利用者の興味関心漏れによるプライバシー侵害の評価に関する研究

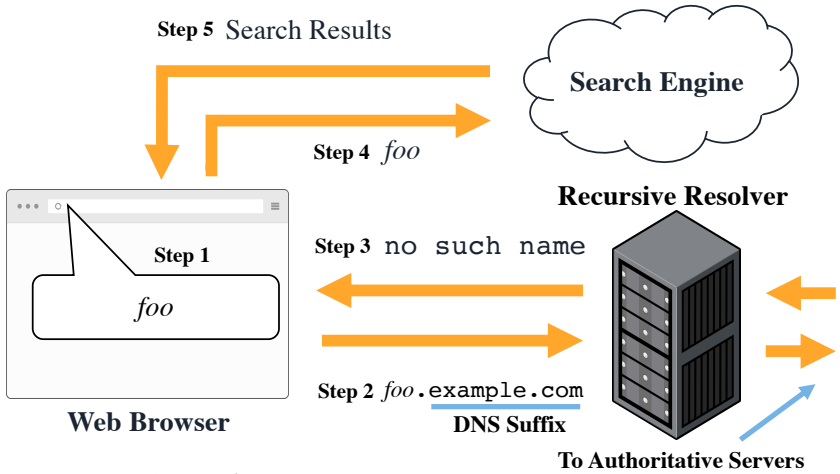

図 5：Web ブラウザから 1 語の検索クエリが DNS に漏れる問題の概要

本研究を通して、Web ブラウザから 1 語の検索クエリが DNS に漏れる問題（図 5）を発見し、調査を行なった。コンピュータ端末で利用される Web ブラウザの中には、検索バーに入力された検索クエリのうち、1 語（空白や特定の種類の記号を含まない語）のクエリを、検索エンジンに送る前に DNS キャッシュサーバに解決すべきドメイン名として DNS リクエストの形態で送信する仕様をもつものがある。利用者はこの仕様を想定しておらず、その利用者の興味関心漏れによるプライバシー侵害への懸念が報告されている。

そこで、その仕様と関連するプライバシーへの懸念を検索クエリ漏れ問題と定義し、この問題の発生環境や条件について調査した。その上で、DNS キャッシュサーバ上で取得した DNS トラフィックデータセットを分析し、相当数の検索クエリが実際に漏れていることを実証した。さらに、この問題が発生することが利用者のプライバシーにどの程度影響を与えるのかを単語の分散表現とクラスタリングを元に評価する手法を提案し、それにより、利用者の興味関心の傾向を推測することができることを示した。さらに、利用者側で検索クエリ漏れ問題を防止する方法についても調査し、利用者側で対処できる解決策は、高度な設定に触れるか、検索毎に所定の操作をする必要があるため、一般的な利用者にとってハードルが高いと考えた。そのため、ブラウザ開発者には、1 語のクエリを名前解決させない設定をデフォルトにするなどして、利用者の知らない間にクエリが漏れることが無いようにすることが求められると結論づけた。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Ishikura Naotake、Kondo Daishi、Vassiliades Vassilis、Iordanov Iordan、Tode Hideki	４．巻 18
２．論文標題 DNS Tunneling Detection by Cache-Property-Aware Features	５．発行年 2021年
３．雑誌名 IEEE Transactions on Network and Service Management	６．最初と最後の頁 1203～1217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TNSM.2021.3078428	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Isobe Katsuki、Kondo Daishi、Tode Hideki	４．巻 4
２．論文標題 Privacy Concerns From Single-Word Search Query Leakage From Web Browsers Through DNS	５．発行年 2022年
３．雑誌名 IEEE Networking Letters	６．最初と最後の頁 48～52
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LNET.2021.3117600	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 磯部克貴，近藤大嗣，戸出英樹
２．発表標題 Webブラウザから1語の検索クエリがDomain Name Systemに漏れる問題の実態調査と利用者の興味関心漏れによるプライバシー侵害の評価
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2021年

１．発表者名 石倉直武，近藤大嗣，戸出英樹
２．発表標題 DNSトンネリング検知のためのキャッシュ特性に基づく特徴量
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2019年

１．発表者名 N. Ishikura, D. Kondo, I. Iordanov, V. Vassiliades, and H. Tode
２．発表標題 Cache-Property-Aware Features for DNS Tunneling Detection
３．学会等名 ICIN（国際学会）
４．発表年 2020年

１．発表者名 石倉直武，近藤大嗣，戸出英樹
２．発表標題 DNSトンネリングに関する攻撃手法と防御手法の分類
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	戸出　英樹 (Tode Hideki)		
研究協力者	バシリアデス　バシリス (Vassiliades Vassilis)		
研究協力者	ヨルダノフ　ヨルダン (Iordanov Iordan)		

6．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	石倉　直武 (Ishikura Naotake)		
研究協力者	磯部　克貴 (Isobe Katsuki)		

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
キプロス	CYENS Centre of Excellence			