企業ネットワークセキュリティにおける情報漏えいの対策に関する研究

大阪公立大学　博士後期課程　情報学研究科　基幹情報学専攻　システム情報学分野　石倉　直武

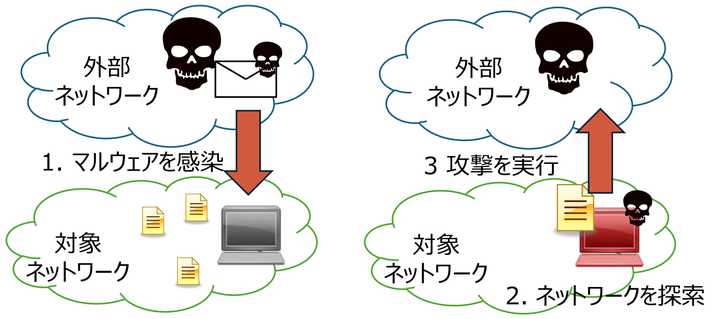
研究背景

- 組織に対する10大セキュリティ脅威 [1]のうち，標的型攻撃はこの数年常に上位に位置付けられている
- 攻撃者は**あらゆる脆弱性**を利用して対象ネットワークへの侵入，通信チャネルの確立及び目的達成を図る

[1]情報セキュリティ10大脅威2023, https://www.ipa.go.jp/security/vuln/10threats2023.html

❖企業ネットワークに対する攻撃の手順

1. Eメール等を介して対象ネットワークのPCにマルウェアを感染
2. 攻撃者は秘密裏に通信チャネルを確立して対象ネットワークを探索
3. 攻撃を実行 (機密情報の窃取や身代金の要求等)



❖標的型攻撃に対する企業の対策

- 社員に疑わしいメディアにアクセスしないよう訓練する　→ ヒューマンエラを完全に消すことはできない

❖生成Artifical Intelligence (AI)による攻撃の高度化

- マルウェアを忍ばせたメール内容の巧妙化
- 生成AIによる未知のマルウェア作成
- 生成AIでマルウェアのふるまいを通常クライアントに似せて従来の検知を回避

[2] Emotet 感染の被害にあった企業事例一覧【2022 年更新版】, https://cybersecurityinfo.com/column/who-hacked-by-emotet/
[3] ランサムウェア攻撃による情報漏洩に関するお知らせとお詫び, https://tp.kadokawa.co.jp/.assets/240628_release_f1wyy3RN.pdf
[4] JAXAに複数回サイバー攻撃 情報が漏えいした可能性, https://www3.nhk.or.jp/news/html/20240621/k10014487721000.html

❖攻撃事例

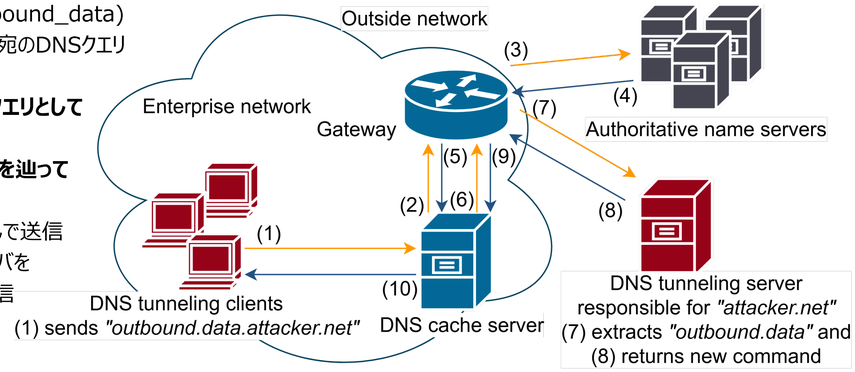
- Emotetが国内で**150組織以上で感染が確認**されている[2]
- KADOKAWA[3]、JAXA[4]に対してサイバー攻撃が確認されている

感染後の継続的な出口対策が必須

DNSトンネリングを用いた情報漏えい

- 企業ネットワークでは不要な通信ポートやプロトコルを制限する
- しかし，DNSで利用されるポートやプロトコルを制限することは難しい
- DNSトンネリングによる攻撃は正常なDNS通信とみなされて攻撃が長期的に継続する可能性がある

(1) 侵入したマルウェアが送信データ(outbound_data)をFQDNに埋め込み，attacker.net宛のDNSクエリを社内DNSキャッシュサーバに送信
(2) DNSキャッシュサーバが**通常のDNSクエリとして反復問い合わせを開始**
(3) – (7) **通常のDNSクエリと同じ経路を辿って** DNSトンネリングサーバに到達
(8) DNSレスポンスに次の命令を埋め込んで送信
(9) (10) ゲートウェイ・DNSキャッシュサーバを通過し，マルウェアが命令を受信

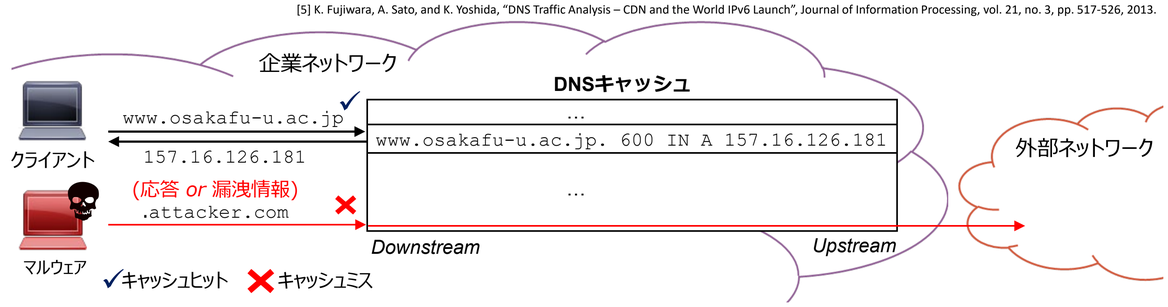


DNSトンネリングによる情報漏えいフロー

DNSキャッシュの特性

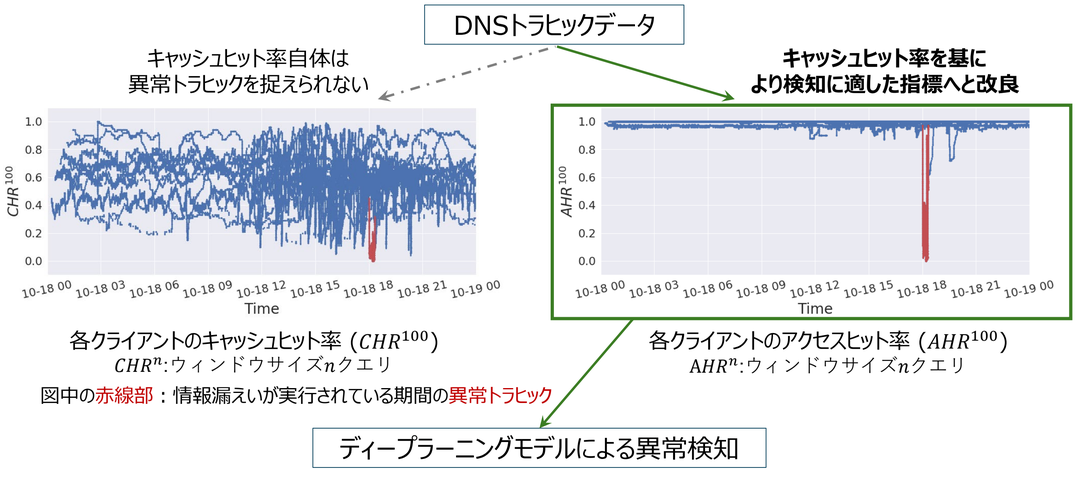
- Domain Name System (DNS)通信はコンテンツ配信を含む多くのサービス実現に必須
- 攻撃者は管理が手薄なDNS通信を悪用し、秘密裏に通信チャネルを確立して情報漏えいを達成可能
- DNSキャッシュは問い合わせ結果を一時的に保管することでDNS通信の効率化を図るための機能
  - 通常クライアントの利用ではキャッシュヒットが頻繁に発生する [5]
  - マルウェアが外部に情報を送信するにはDNSクエリが外部に送信されなければならない
    →キャッシュヒットしたDNSクエリは外部ネットワークに送信されないため
    外部と通信をするためにはDNSクエリをキャッシュミスさせなければならない

[5] K. Fujiwara, A. Sato, and K. Yoshida, "DNS Traffic Analysis – CDN and the World IPv6 Launch", Journal of Information Processing, vol. 21, no. 3, pp. 517-526, 2013.



実験結果 – DNSトンネリングによる情報漏えいの特徴量

- 未知のマルウェアや通常クライアントのふるまいを模倣する高度な攻撃にも有効な検知手法の確立を目指す
- **情報漏えいを達成するうえで必ず痕跡として残る指標を抽出（特徴量エンジニアリング）**
- 抽出した指標に合わせて異常検知可能なディープラーニングモデルを実装



まとめと今後の課題

- 検知が難しい高度なDNSトンネリングによる情報漏えいに対して，攻撃者にとって隠蔽困難な痕跡の抽出に成功した
- 今後，DNSトンネリングの通信特性に応じて最適な異常検知モデルを構築し，企業ネットワークで発生したDNSトンネリングによる情報漏えいの早期検知を目指す