7ZC-06

SDNに基づく欺瞞防御システム

陳　鑫†　　大久保　隆夫‡

情報セキュリティ大学院大学†　　情報セキュリティ大学院大学‡

1　はじめに

インターネット技術の発展に伴い、サイバー攻撃の技術も発達し、それによる被害が深刻な問題となっている。情報処理推進機構（IPA）[10]2022年3月に公開した2022年度「情報セキュリティ 10 大脅威」で、標的型攻撃はランキング第 2 位に上り、今最も重視すべき脅威の一つとなっている。

「法人組織のセキュリティ動向調査 2020 年版」によると、標的型攻撃は会社や業界に多大な経済損失をもたらす、そして、標的型攻撃の攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな攻撃手法を選択するため、いろいろな脆弱性や技術手段を用いて、攻撃を実現する。さらに、近年の攻撃手段は様々な隠蔽技術を利用し、検知も困難となっている。例えば、近年の攻撃は IDS や IPS などの検知を避けるため、DNS トンネルのような隠蔽技術を利用しているため、完全に防ぐことが困難である。この状況を対応するために、攻撃者を欺瞞し、セキュリティを確保することが有効な手段だと考えられる。

2　関連研究

Shimanaka ら[４]は、攻撃者に気付かれないように悪意のあるトラフィックを転送する欺瞞アーキテクチャを提案した。 Shimanaka らは実際に使用するネットワーク（Operation Network、略称 O-Net）とほとんど同じに見える欺瞞ネットワーク（Deception Network、略称 D-Net）を作成した。攻撃を検知した後に、侵入されたホストから O-Net へのすべての ARP 請求を SDN で処理し、D-Net へ転送する。この後の通信は mac address を書き換えることで、攻撃者を気づかれないように、パケットを D-Net に転送する。

Chiang ら[３]は、SDN を使用して、データパッチのヘッドフィールドを操作し、存在しない応答を偽造することで、ルーティング経路を模擬する。この手法によって、異なるホストからは、ネットワーク構造が完全に違うように見えることを実現する。また ARP、UDP、ping と traceroute の応答をただしく処理できる。

3　本研究のアプローチ

サイバーキルチェーンでは、攻撃者が最終目的を達成するための攻撃をいくつかの段階に分けている。各段階の行動を確保するため、情報収集は最優先の活動である。角丸らの研究[２]によって、侵入されたことを前提として、本研究はラテラルムーブメントの偵察段階に収集できる情報を中心として欺瞞防御を築く。

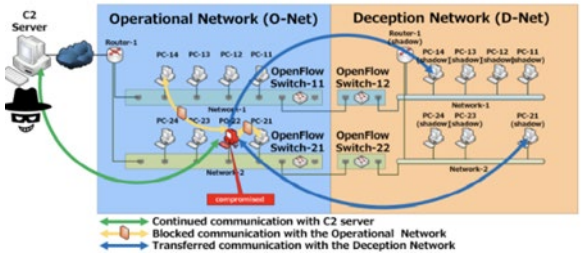

図 1 乗っ取ったホストからのトラフィックを偽りのネットワークに転送する[4]

本論文は OpenFlow でパケットのヘッダフィールダをマッチングし、特定ポート番号の通信を抽出し、Deception Server に転送する。Deception Server が受けたパケットの IP アドレスを事前に設定されたルールによって書き換える形で、重要のホストを攻撃者の視点から隠ぺいすることを考えられる。

4　実現手法

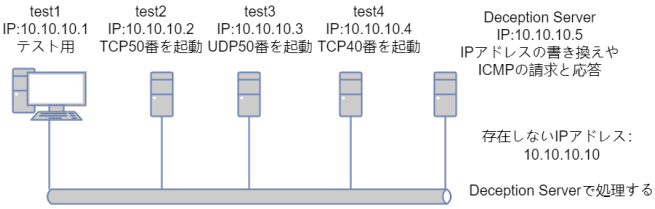

図 2 実験環境のテクノロジー

本研究は SDN の機能を利用し、パケットの通信先を書き換えることで、攻撃者に重要のホストを隠ぺいすることを考えた。だが、SDN コントローラーで IP アドレスを全部書き換えると、返信先の IP アドレスが確認できなくなる可能性がある。したがって、「請求」の宛先と「応答」の送信元の二つの部分を書き換える。

本論文の書き換えは Deception Server に処理

The research on deception defense using SDN

† CHEN XIN・Institute of Information Security

‡ Takao Okubo・Institute of Information Security

するものため、SDN switch に設定して必要なパケットを転送することが必須である。Deception Server が事前に設定した IP のパケットを受けたとき、設定情報によってパケットの IP と対応な MAC（Deception Server で自動請求）を書き換える。宛先は捏造された場合、Deception Server でその ARP 請求を応答する。もし捏造された IP へ設定外の番号に通信すると、Deception Server でたどり着けないに応答する。

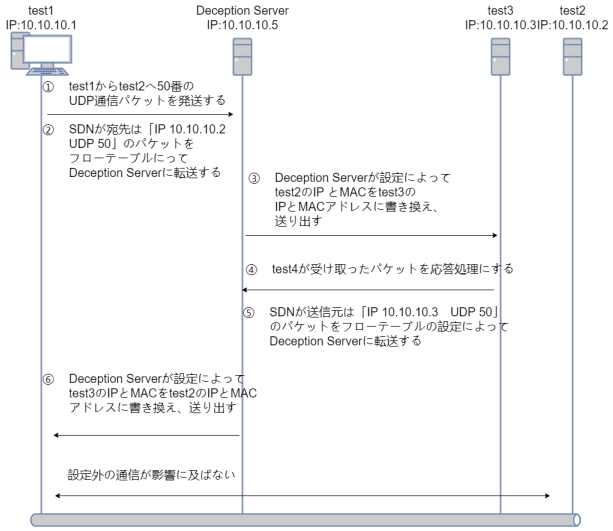

図 3 IP を書き換える過程

5 現時点の問題

Deception Server で処理した通信に関して、全体的に大きな遅延がある。同時に UDP はコネクションレス型のプロトコルで、その通信の安定性が保証できなくなり、通信内容が乱れる可能性が高い。

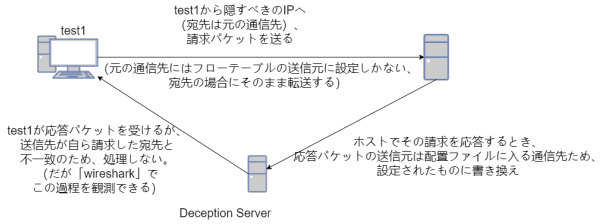

図 4 元 IP への通信を遮断できない

元 IP への通信を遮断できないことも、現時点の問題の一つである。本当の通信先は攻撃者の判断を歪めるため、偽の通信先に書き換えていたが、元通信に請求を発送することも可能である。元の通信先へ請求しても応答をもらっている、しかし受け取った応答が送信元の情報は SDN に設定されたものから、その送信元の情報書き換えていたため、応答を処理した。普通に見るとただタイムアウトに感じられるかも 、だが「tcpdump」や「wireshark」などツールを利用して調べると、すぐに攻撃者に偽装が発覚する可能性が高い。

また、IP の書き換えについて、現在は Deception Server に処理することが、実際に OpenFlow に書き換えることも可能である。OpenFlow のアクションに「Mod」という指定のフィールドを書き換える機能が存在している。この機能を利用すると、上記の遅延と安定性の問題を大半に解決できる。しかし、フローテーブルの設定には、転送のため出口を指定しなければならない。その場合、「応答」パケットを書き換えるとき、宛先によって出口を指定する必要である。ならば、SDNコントローラーで自動的に設定する必要である。

6 まとめと今後

本研究は、標的型攻撃のラテラルムーブメントにおいて用いられる「netstat」などの偵察コマンドに対し、通信先情報の書き換えに通じて誤った通信情報を出すことを確認した。このため、とある程度に侵入者の偵察を影響し、判断を歪め、攻撃の遅延やコストを上げることになると考えられる。

本研究は、Ryu コントローラーを用いて、フローテーブルを設定することを予想していた。しかし、今回の研究においてそれは、実現に至らなかったため、現時点でフローテーブルの設定は Open vSwitch のコマンドで実現することしかできない。今後はフローテーブルの設定や IP の書き換えを SDN コントローラーに移行することを次の課題と考えられる。

参考文献

[1]角丸貴洋，島成佳 ，渡部正文，吉岡克成（2014）： 標的型攻撃対策に向けた欺瞞機構を用いた防御アーキテクチャ（情報通信システムセキュリティ）
[2]角丸貴洋，島成佳 ，吉岡克成（2014）： 組織ネットワークにおける内部攻撃に対する模擬的欺瞞方式（computer security symposium）
[3]C. -Y. J. Chiang et al., "ACyDS: An adaptive cyber deception system," MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 800-805, doi: 10.1109/MILCOM.2016.7795427.
[4]Toru Shimanaka, Ryusuke Masuoka, Brian Hay “Cyber Deception Architecture: Covert Attack Reconnaissance Using a Safe SDN Approach” Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019