

トランク接続方式を用いた複数の VLAN セグメントを流れる ARP リクエスト監視システムの構築

高台 典佳† 川橋 裕‡
Norika Kodai Yutaka Kawahashi

1. はじめに

近年、情報化社会の発展に伴い、様々な情報技術が社会全体に普及しており、我々の生活様式は多様化している。例として、企業や大学などの組織におけるクラウドサービスの利用の増加 [1] や、個人が所有する端末を業務に利用する BYOD の広がり [2][3] が挙げられる。さらに最近では、働き方改革や新型コロナウイルスの感染拡大の影響により、テレワークの実施が推進されている [4]。よって現在では、組織外で利用される端末が組織内部のネットワークへ接続することや、組織内の情報資産が組織外部で保管・利用される機会が増加している。しかしこれらの通信は、ファイアウォールを経由せずに行われるため、ネットワークの境界を監視する従来の防御方法だけでは、脅威の侵入が防ぎきれなくなっている。

加えて、境界型セキュリティでは、一度組織の内部に脅威が侵入してしまうと、発見するのが困難である。よって現状の環境では、ワームのような自己増殖するマルウェアの感染が、拡大する恐れがある。自己増殖マルウェアは、1 台の端末に感染すると、次の標的となる脆弱な端末を見つけるため、接続されている LAN 内の探索を行う。これにより感染を拡大させ、重要な情報を盗み出すなどさまざまな被害をもたらす。以上のような実情から、組織内のネットワークを監視し、脅威の侵入になるべく早く気付けるような環境を整備しておくことが求められる。

本研究では、和歌山大学の学内ネットワークにおいて、複数の VLAN セグメントを流れる ARP リクエストを監視するシステムを構築する。パケット数の増加を検出し、LAN 内にマルウェアが侵入している可能性があるかと判断することができる。

2. 関連研究

ARP に着目したマルウェア検出の関連研究 [5] では、ARP リクエストを取得・解析し、過去の傾向をもとに、マルウェア感染による LAN 内の異常を検知する手法が提案されている。

しかし、この手法では、1つのデバイスで1つのLANしか監視することができないため、複数のセグメントが整備された環境での運用には適していない。組織ネットワークは VLAN を利用して構築されることが多く、和歌山大学においても多数のセグメントが存在している。

3. 研究目的

本研究では、VLAN によって多数のセグメントが整備されている和歌山大学の学内ネットワークにおいて、複数セグメントを流れる ARP リクエストを 1 台で監視することができるシステムの構築を目的とする。LAN 内でブロードキャストされる ARP リクエストを日頃から取得し、その

数をグラフ化することで、パケット数の増加を検出することができる。これにより、LAN 内へのマルウェアの侵入を早期に発見することが可能である。

4. 提案手法

4.1 パケットキャプチャ

提案システムでは、監視対象となる L3 スイッチに設定された VLAN 内を流れる ARP リクエストパケットをキャプチャする。このとき、トランク接続方式を用いることで、1 台で複数の VLAN セグメントを監視することが可能である。

ARP パケットは、その性質から ARP スキャンに用いられているが、多くのマルウェアはこの手法を悪用して、次の感染相手を探索する。したがって、本研究では、ARP リクエストに着目することで、マルウェアの探索行為を検出することとする。

4.2 データベースへの記録

取得したパケットから得られる情報(送信元 IP アドレス、送信元 MAC アドレス、宛先 IP アドレス)と、パケットを取得した時刻をデータベースに記録する。

4.3 グラフおよびランキングの表示

データベースに記録したデータから、パケット数のグラフを作成し、Web ブラウザ上に表示する。グラフ化することで、数の増減が一目でわかるようになる。パケット数が急増した場合、LAN 内にマルウェアが侵入している可能性がある。

ただし、ARP リクエストの増加は正常な通信でも十分に起こり得るため、ARP の頻度順にパケットの送信元 IP アドレスのランキングを作成し、こちらもブラウザ上で参照できるようにする。仮に同じアドレスからの通信が多い場合は、その端末がマルウェアに感染している可能性が高いと判断することが可能である。

4.4 端末の部屋名の特定

和歌山大学では、MARS [6] という障害対応支援システムを運用している。MARS を利用することで、グラフの時刻とランキングの IP アドレスから、マルウェア感染の可能性のある端末が有線接続されている部屋名を特定することが可能である。

5. 実験・評価

5.1 実験概要

実験 1 多数の端末やネットワーク機器が接続されている環境において、提案システムの動作実験を行った。

†和歌山大学大学院 システム工学研究科

‡和歌山大学 学術情報センター

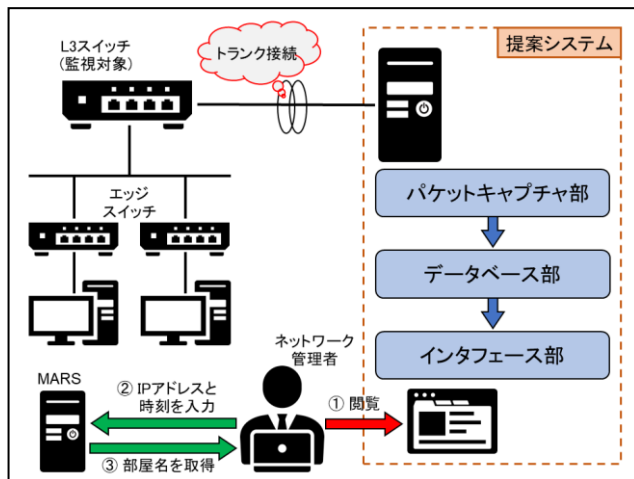


図1 提案システムの構成

提案システムを用いて、実験環境を 24 時間監視し、その間にネットワーク内の複数の端末から ARP スキャンを 3 回行った。なお本実験では、ネットワーク環境の都合上、L3 スイッチとのトランク接続ではなく、他の端末と同様に提案システムをエッジスイッチに接続した。

実験 2 実験用にネットワーク環境を構築し、トランク接続によって複数の VLAN セグメントの監視を行った。実験環境の L3 スイッチには、2 つの VLAN を設定し、それぞれに端末を接続した。そして、2 台の端末から同時に、2 回 ARP スキャンを行った。

5.2 実験結果

実験 1 の結果のグラフを図 2 に示す。ARP スキャンを行った時刻が含まれる、グラフ上の各点を(1), (2), (3)としている。ARP スキャンを行った時間帯にパケット数が増加していることを、グラフから読み取ることができた。



図2 実験結果のグラフ

さらに、(1), (2), (3)の時間帯のランキングを確認したところ、他の時間帯に比べてパケット数が急増したアドレスが存在した。それらのアドレスは、ARP スキャンを行った端末のアドレスと一致しており、スキャンを行った端末の IP アドレスが特定できたと言える。(1)のランキングを図 3 に示す。

実験 2 では、2 台の端末が ARP スキャンを行った時刻のパケット数が、両 VLAN のグラフ表示ページにきちんと反映された。さらに、各 VLAN のランキングには、スキャンを行った端末の IP アドレスが正しく表示された。よって提案システムは、トランク接続によって複数の VLAN セグメントを監視できることが確認できた。

2021-01-28 12:15:00~12:20:00

src IP Address	Number of packets
133	724
254	521
209	459
250	87
251	45
207	5

図3 (1)のランキング

5.3 評価

既存研究では、1 つのデバイスで 1 つの LAN しか監視することができなかった。そのため、和歌山大学の学内ネットワークのように VLAN によって多数のセグメントが整備された環境での運用には適していない。これに対して、本研究の提案システムでは、トランク接続方式を用いることで、1 台で複数の VLAN セグメントを監視することを可能にした。よって、大規模なネットワークで運用する場合、既存研究よりも有用なシステムであると言える。

さらに、提案システムを用いることで、現行の和歌山大学のネットワーク環境では発見が困難であった、マルウェアの侵入を検出できるようになった。現在運用している MARS は、「どの IP アドレスがどの端末によって、いつどこで使用されているか」を管理するシステムであり、LAN 内の通信の監視は行っていない。しかし、本システムで得られる情報を用いると、MARS を利用して端末の接続場所を特定することができる。よって本システムは、早期にマルウェアへの対策を講じるために、MARS を手助けするような役割を担っていると言える。

6. 今後の課題

本研究では、VLAN によって多数のセグメントが整備されている環境において、複数セグメントを流れる ARP リクエストを 1 台で監視することができるシステムを構築した。LAN 内でブロードキャストされる ARP リクエストを日頃から取得し、その数をグラフ化することで、パケット数の増加の検出を可能にした。これにより、LAN 内へのマルウェアの侵入を早期に発見することができる。

提案システムは、現在、送信元 IP アドレスのランキングしか表示していないため、今後は、Web インタフェースで参照できる情報量を増やし、機能を拡張したいと考えている。さらに、和歌山大学において実際に運用し、ネットワーク管理者のインシデント対応を支援できるよう努めていきたい。本システムを学内ネットワークへ導入する場合、監視を行う VLAN の数や通信量は膨大なものとなる。したがって、本システムへの負荷も大きくなると予想され、動作の効率化が求められる。さらに、動作実験の環境では MARS の運用を行っていなかったため、実環境に導入する際は、MARS のデータベースへのアクセス方法について検討する必要がある。

参考文献

[1] 総務省

“令和 02 年版 情報通信白書 第 5 章第 2 節 1(4)企業におけるクラウドサービスの利用動向” (2020)

<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252140.html>

[2] 株式会社 NTT データ経営研究所

“私用端末の業務利用(BYOD)動向調査” (2013)

<https://www.nttdata-strategy.com/archives/survey/goo/pdf/20131211.pdf>

[3] AXIES 大学 ICT 推進協議会

“BYOD を活用した教育改善に関する調査研究” (2018)

https://axies.jp/_files/report/ict_survey/2016survey/byod_report_2016.pdf

[4] 総務省

“令和 02 年版 情報通信白書 第 2 章第 3 節 2(1)テレワークの推進” (2020)

<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd123210.html>

[5] 松藤 央

“ARP リクエスト監視に基づく LAN 内異常検知”

2019 年度修士論文 東京大学大学院情報理工学系研究科

[6] 吉田 祐亮

“ネットワーク接続監視システム MARS の構築”

2012 年度修士論文 和歌山大学大学院システム工学研究科