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　６ 年　 ５ 月 ２９ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８８９

研究課題名（和文）パケットモニタリングを用いた感染端末検出のためのトラフィック分析に関する研究

研究課題名（英文）Study on Traffic Analysis for Detecting Infected Terminals Using Packet Monitoring

研究代表者
中村　豊（Nakamura, Yutaka）

九州工業大学・情報基盤センター・教授

研究者番号：４０３４６３１７

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究ではキャンパスネットワーク内においてラテラルムーブメントを検出するためのパケット計測基盤としてarkimeを用い，内部通信の監視を実施してきている。本学ではキャンパス内部においてもファイアーウォールを設置しており、その性能劣化が発生した際に、arkimeを用いたパケットキャプチャとファイアーウォールのインタフェース情報を組み合わせることで、ファイアーウォールのボトルネックポイントを見つけ出すことに成功した。これらの結果から、内部通信における異常検知はパケットキャプチャだけではなく、他のネットワーク機器からの情報との組み合わせが非常に重要であることが明らかとなった。

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を受けた一次被害端末の防御を100%実施できないことを前提に、ウイルス感染後通信挙動、具体的にはC&C通信、ボットダウンロード、ラテラルムーブメント等に着目し、それらを検出、分析するための手法を提案した。本手法の特徴は既存システムで検知可能な被害を受けた一次被害端末の特定ではなく、一次被害端末が生成する通信の特徴を分析することで二次被害端末の検出を可能とする、という点にある。また、分析の汎用性・可用性を高めるために、過去に蓄積したトラフィックデータも分析対象とした。これにより、自組織だけでなく様々な組織におけるトラフィックデータの分析が可能となりセキュリティ対策に貢献する。

研究成果の概要（英文）：In this research, we have been using arkime as a packet measurement platform for detecting lateral movement in the campus network and monitoring internal communications. Our University has a firewall on campus, and when its performance degraded, we succeeded in finding the bottleneck point of the firewall by combining the packet capture using arkime and the interface information of the firewall. . These results clearly show that anomaly detection in internal communication is not only based on packet capture, but also on the combination of information from other network devices, which is very important.

研究分野：情報セキュリティ関連

キーワード：パケットキャプチャ　ラテラルムーブメント

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

本研究では標的型攻撃を受けた一時被害端末の防御を 100%実施できないことを前提に、ウイルス感染後の通信挙動、具体的には C&C 通信、ボットダウンロード、ラテラルムーブメント等に着目しそれらを検出、分析するための手法を提案する。本手法の特徴は既存システムで検知可能な被害を受けた一次被害端末の特定ではなく、一時被害端末が生成する通信の特徴を分析することで二次被害端末の検出を可能とする点にある。また、分析の汎用性・可用性を高めるために、過去に蓄積したトラヒックデータも分析対象とする。これにより、自組織だけでなく様々な組織におけるトラヒックデータの分析が可能となり、セキュリティ対策に寄与すると考える。

２．研究の目的

本研究で提案する二次被害特定のためのトラヒック分析は我々独自の手法である。一次被害端末を検出するための製品やサービスはかず多く存在するが、一次被害端末が生成するトラヒックを分析し、二次被害端末の特定、調査を行う研究は行われていない。特に内部拡散に用いられているラテラルムーブメントにおいて内部ネットワークでどの端末が被害を受けたかを分析することはこれまで困難であった。これはラテラルムーブメントの通信を検知したとしても、その通信で内部拡散に成功したかどうかの成否を判定することが困難であったからである。また、内部ネットワークの計測自体が非常に高コストであるため困難であった。我々はこの問題を解決するために大規模環境向けフルパケットキャプチャツールである arkime[1]を用いることで、比較的低価格なサーバで内部ネットワークの計測環境を構築した。本研究では arkime が生成するセッション情報を分析することでラテラルムーブメント発生時の拡散の成否について判定する手法について検討する。

３．研究の方法

本学のキャンパスコアスイッチからミラーポートを出力し、arkime がインストールされたサーバを用いてパケットキャプチャを行う。そして arkime が管理しているセッション情報を定期的に取得し、内部ネットワークにおいてラテラルムーブメント通信が発生しているかどうかの分析を行う。

４．研究成果

(1) Arkime を用いた内部トラヒック調査に関する研究

ラテラルムーブメントの様なスキャン通信の検知はこれまで様々な研究が行われている。特に NDR(Network Detection and Response)と呼ばれる製品では、内部通信の異常を検出、通知する機能を有している。しかしながらこれらの製品導入は数千万円という単位になるため、簡単に導入することはできない。ラテラルムーブメント通信では、送信元 IP アドレスが固定で宛先 IP アドレスのセッションである場合、また送信元、宛先 IP アドレスが固定で宛先ポートが複数のセッションの２パターンが存在する。いずれも急激なセッション数の増加が観測されると思われる。

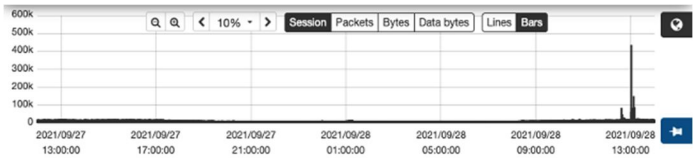

図１　計測例１

図 1 実際の計測例を示す。図 1 より 2021 年 9 月 28 日 13 時頃に急激なセッション数の増加が確認できる。これは当該時間帯を arkime により詳細表示したものを図２に示す。図２より、当該時間帯において、学内の脆弱性スキャナが学内のサーバに対してスキャンを実施していることが確認できた。スキャナの IP アドレスが学内のサーバの複数ポートへ接続を試みていることがわかる。また、arkime viewer ではブラウザからの検索機能を用いた特定の情報を抽出することが可能である。例えば「1 時間以内に送受信されたパケットが 1 つでプロトコルは TCP である」といった検索の場合、「packet == 1 && ip.protocol == tcp && ip.src != XXX.XXX.0.0/16 && ip.dst != XXX.XXX.0.0/16」といった

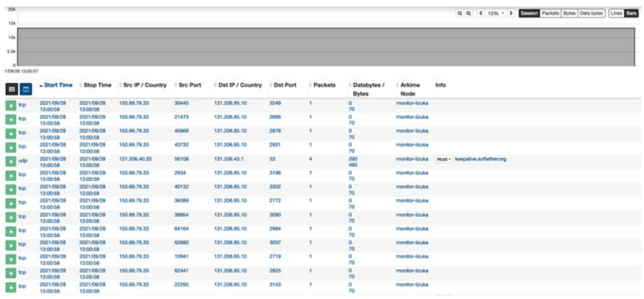

図２　計測例２

記述をすることで、XXX.XXX.0.0/16 以外の IP アドレスでの通信が紛れ込んでいることが分かる。具体て的には、プライベート IP アドレスが学内幹線に紛れ込んでいる場合に発見が可能となる。さらに arkime には Web API 機能を用いて、セッション情報を取得することができる。
% curl --anyauth ‘http://[arkime viewer の ID]:[arkime viewer のパスワード@[arkime viewer server の IP]:8005/sessions.json’
といったコマンドライン入力を行うと、図３の様な結果が得られる。


```
[yutaka-n@arkime-t ~]$ curl --anyauth 'http://admin:secnw2OI4@localhost:8005/session.json'
<!DOCTYPE html><html><head><base href="/"><meta charset=utf-8><meta name=referrer content=no-referrer><meta name=viewport content="width=device-width,initial-scale=1"><meta property=csp-nonce content="M2EyNmQ2OGYtMTFiNS00ODlkLTk5YWQtMTgwNWVhYjMwN2Mz"><link rel=stylesheet href=font-awesome/css/font-awesome.min.css><title>Arkime</title><link rel=stylesheet href=""><script nonce="M2EyNmQ2OGYtMTFiNS00ODlkLTk5YWQtMTgwNWVhYjMwN2Mz">const TITLE_CONFIG = 'opensearch - _page_ -_view_ -_expression_';
      const FOOTER_CONFIG = 'Arkime v5.1.2 | &lt;a href=&quot;https://arkime.com&quot;&gt;arkime.com&lt;/a&gt; | {{ responseTime | commaString }}ms';
      const DEMO_MODE = false;
      const VERSION = '5.1.2';
      const PATH = '/';
      const MULTIVIEWER = false;
      const HASUSERSES = false;
      const HUNTWARN = 100000;
      const HUNTLIMIT = 10000000;
      const ANONYMOUS_MODE = false;
      const BUSINESS_DAY_START = false;
      const BUSINESS_DAY_END = false;
      const BUSINESS_DAYS = '1,2,3,4,5';
      const TURN_OFF_GRAPH_DAYS = 30;
      const DISABLE_USER_PASSWORD_UI = true;
      const LOGOUT_URL = '';
      const DEFAULT_TIME_RANGE = '1';
      const SPIVIEW_CATEGORY_ORDER = '';</script><script defer=defer src=static/js/runtime.e11678a45ceaeccc44c3.js></script><script defer=defer src=static/js/app.748035673cc58b53c878.js></script><link href=static/css/app.748035673cc58b53c878.css rel=stylesheet></head><body class="default-theme"><div id="app" data-server-rendered="true"></div></body></html>[yutaka-n@arkime-t ~]$ curl --anyauth 'http://admin:secnw2OI4@localhost:8005/sessions.json'
{"data":[{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786427490,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NghUMSUfASBBEJAtsqb9R_CM"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786448164,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-Ngj1kcEb4z5FxJ4kwpVUDhHC"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786468859,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NghyAS-w56JIKav_N7BDiadz"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786406838,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NgixSScs_EJDNKKqdtV6U6hp"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786365547,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NghY1iAYEZBDmp4i7Ge3yJHb"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786386227,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NghUYz-bZllBIb6RaULJAHzo"},{"firstPacket":1716338215964,"rootId":"240522-NghdzKXvxdRLBaCyaYh9OOXN","totDataBytes":880000,"ipProtocol":17,"node":"arkime-t","lastPacket":1716786303573,"source":{"as":{},"geo":{},"packets":10000,"port":5353,"ip":"192.168.207.113","bytes":1340000},"destination":{"as":{},"geo":{},"port":5353,"ip":"224.0.0.251","packets":0,"bytes":0},"client":{"bytes":880000},"server":{"bytes":0},"network":{"packets":10000,"bytes":1340000},"id":"3@240527-NghDdUcsLbVLFK7iEBQepsQz"},{"firstPacket":1716338215964,"rootId":"2
```


図３　観測例３

図３の結果を定常的に収集し分析することで、なんらかの異常を検出することが可能となると思われる。

(2) IPv6 IPsec-VPN と VXLAN を用いたキャンパス間バックアップネットワークの構築

学内通信の異常検知を行うためには、学内ネットワークの安定的な運用が不可欠である。九州工業大学では３つのキャンパスの間と SINET への接続に関して、ダークファイバーを用いて接続している。これらの回線の安定運用のためにバックアップ回線も契約している。これは災害などによる回線切断のリスクがあるため、事業者の異なる回線をバックアップ回線として用いている。メインのダークファイバーは QTNet からの借料であるが、バックアップ回線は NTT 西が提供しているフレッツ光をアクセス線とした VPN 契約であった。本学では 2022 年 3 月に行われた SINET6 への移行に合わせて、フレッツで構築していたバックアップ回線の費用削減およびアクセス回線の増速を目指して、IPv6 IPsec VPN と VXLAN を組み合わせた構成へと更新した。九州工業大学では、キャンパス間で VLAN を多数延伸しているため、IPv6 上での VPN 接続に加えて、L2 延伸するために VXLAN を VPN 回線上に構築した。図４に更新後のバックアップネットワーク構成図を示す。図４に示す様に、nttgw-t(戸畑キャンパス)をハブとしたハブ&スポーク接続とした構成となっている。各拠点に fortigate を設置し、VPN ルータとして設定を投入している。現在導入している fortigate では VXLAN のオフロード機能が搭載されていなかったため、構成変更後のスループットの向上はほとんどなかった。しかしながら、費用面で大幅に削減することができた。

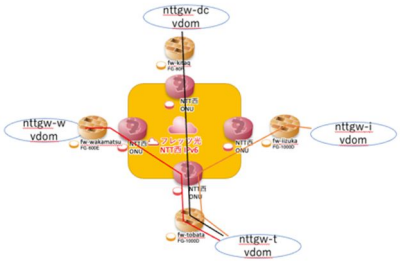

図４　ネットワーク構成図

(3) Arkime とファイアーウォール情報を用いたネットワーク機器のパフォーマンスチューニング

キャンパス内部に設置している arkime サーバによりパケットキャプチャは実施しているが、ラテラルムーブメント通信の検知・計測は十分に行うことができなかった。これは学内において、擬似的なスキャンを実施する脆弱性診断以外のラテラルムーブメント通信が生じていなかったことに起因している。しかしながら、部局を収容しているファイアーウォールの性能劣化が発生した際に arkime を用いたパケットキャプチャとファイアーウォール装置のインタフェース情報を組み合わせることで、ファイアーウォールのボトルネックポイントを見つけることに成功した。これらの結果から内部通信における異常検知はパケットキャプチャだけではなく、他のネットワーク機器からの情報との組み合わせが非常に重要であることが明らかとなった。またパケットキャプチャの問題点として、計測量が多すぎるため問題の通信の絞り込みが困難であることが挙げられる。この問題に対して、ファイアーウォール装置やネットワーク装置のインタフェース情報（パケットカウント）を広く収集することで、問題のネットワークセグメントを絞り込むことが可能となる。その後に詳細分析のために arkime を用いたパケット解析が有効であると考えられる。

[1] https://arkime.com/

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 中村豊，佐藤彰洋，福田豊
２．発表標題 IPv6IPsec VPNをVXLANを用いたキャンパス間バックアップネットワークの構築とその応用
３．学会等名 情報処理学会 IOTシンポジウム2022
４．発表年 2022年

１．発表者名 中村 豊，佐藤 彰洋，福田 豊，林 豊洋，井上 純一，岩崎 宣仁，和田 数字郎
２．発表標題 Arkime を用いた内部トラヒック調査に関する研究
３．学会等名 情報処理学会 IOTシンポジウム2021
４．発表年 2021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

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