[ポスター発表] 研究報告

Arkimeを用いた内部トラヒック調査に関する研究

中村 豊[1]　佐藤 彰洋[1]　福田 豊[1]　林 豊洋[1]　井上 純一[2]　岩崎 宣仁[2]　和田 数字郎[2]

Research of internal traffic investigation based on Arkime

1. はじめに

多くの企業・組織においてセキュリティ対策は喫緊の課題となっている．Emotet[1] の様なウイルスに組織内部の端末が感染すると，機微情報の漏洩，ランサムウェアの感染，他の内部端末への感染の伝搬，組織外へのウイルスメールの送信といった深刻な問題を発生させる．こうしたウイルスの主な侵入経路は標的型攻撃であるため，完全に防止することは不可能である．この様なウイルスでは内部への展開のために様々なボットをダウンロードし，ラテラルムーブメントと呼ばれる内部ネットワークの探索を行う．そこで本稿では，ラテラルムーブメントを追跡し，早期のダメージコントロールを実現するために，Arkime(旧 Moloch)[2] と呼ばれるパケットキャプチャツールを用いた実際のデータ取得と分析の結果について報告する．

2. 関連研究およびシステム構築

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．[3] では外部ネットワークから内部ネットワークへのダークネットを用いたスキャン通信の検知について研究されている．[4] ではスキャンを検知するために内部ネットワークにハニーポットを設置し，その通信を分析する手法が提案されている．またパケットをキャプチャし通信異常を検知するシステムやサービスは様々に存在する．特に NDR(Network Detection and Response) と呼ばれる製品 [5]，[6] 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，これらの製品の導入価格は 1 千万円を超えるため，簡単に導入することは困難である．ここでラテラルムーブメント通信は，送信元 IP アドレスが固定で宛先 IP が複数のセッションおよび，送信元・宛先 IP が固定で宛先ポートが複数のセッションが存在する，という特徴があり，急激なセッション数の増加が観測されると思われる．そこで，本稿ではこうしたトラヒックデータの蓄積・分析基盤を Arkime を用いてできるだけ安価に構築したので報告する．図 1 に本学で構築した内部トラヒック調査のためのネットワーク構成図を示す．図 1 に示す様にコアスイッチに各部局を収容するファイアーウォール (以下，FW) が接続されており，各部局の通信は対外ネットワークとの通信時に必ず FW を通過する．そこで内部通信を調査するために，この FW との接続点をモニタリングすることで，よりエンドユーザに近い位置での通信の調査が可能となる．

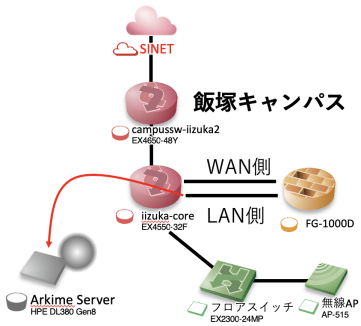

図 1　ネットワーク構成図

Arkime(旧 Moloch) は大規模パケットキャプチャ & フォレンジックツールであり，以下の 3 つのコンポーネントから構成される．

- moloch capture
  moloch capture はパケットキャプチャの本体である．このコンポーネントが NIC から取得したパケットを指定のディレクトリへ格納していく．また，セッション情報を elastic search へ転送する．
- moloch viewer
  moloch virewer は web ブラウザでの表示機能である．デフォルトでは 8005 ポートを用いており，アクセスする事でパケットキャプチャの状態を得る事ができ

[1] 九州工業大学 情報基盤センター / ネットワーク・セキュリティ基盤運用室
Kyushu Institute of Technology, Information Science and Technology Center / Network and Security Infrastructure Office
1-1 Sensui-cho, Tobata-ku, Kitakyushu, 804–8550, JAPAN
[2] 九州工業大学 飯塚キャンパス技術部 / ネットワーク・セキュリティ基盤運用室
Kyushu Institute of Technology, Iizuka Campus Technical Support Office / Network and Security Infrastructure Office
680-4 Kawazu, Iizuka-shi, Fukuoka, 820-8502, JAPAN

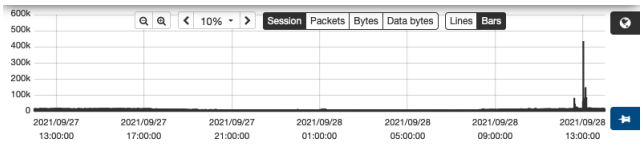

図 2 計測例 1

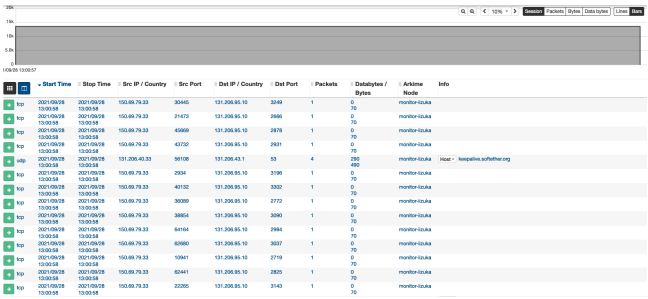

図 3 計測例 2

る．また，外部から 8005 ポートへ所定の API でアクセスすることで，json 形式でデータを取得することができる．

- elastic search
  moloch capture や moloch viewer の情報を一元管理しているサーバである．

図 1 で示した Arkime Server は HPE DL380 Gen8 で構成しており，HDD はパケット保存用に 8TB SATA HDD を 8 個挿入し，RAID6 でボリュームを構成し，データ保存用に 40TB のパーティションを設けている．図 1 での計測で 10 日程度で 10TB 程度のデータ量となっている．ただしネットワーク構成上，wifi 通信をキャプチャできていない．したがって，1 ヶ月程度の保存を目指すのであれば、もう少しストレージ容量が必要であると思われる．内部ネットワークにおける情報セキュリティ対策機器と価格を比較すると，最小構成価格で約 100 万程度から購入できる機材であり，価格は 1/10 程度になると考えられる．内部ネットワークの監視のためには Arkime が出力するトラヒックデータの定期的な分析が必要となる．次節に，Arkime を用いたトラヒック計測の結果について述べる．

3. 結果および考察

図 2 に実際の計測例を示す．図 2 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．当該時間帯を Arkime より詳細表示したものを図 3 に示す．図 3 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，moloch viewer では，ブラウザから検索機能を用いて特定の情報を抽出することができる．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」といった記述が可能である．moloch viewer でのセッション検索窓で以下の検索を実行したとする．

```
packets == 1 && ip.protocol == tcp && ip.src != 131.206.0.0/16 && ip.dst != 131.206.0.0/16
```

九州工業大飯塚キャンパスのグローバル IP アドレスは 131.206.0.0/16 であるので，この検索で出力が得られた場合，グローバル IP で通信している領域にプライベート IP アドレスの通信が紛れ込んでいることが想定される．この場合，通信を生成しているルータ等の設定不備が考えられる．さらに，Arkime には Web API[7] を用いて，データを取得することができる．例えば，以下の様にターミナルから入力すると，

```
% curl -vvv -i --anyauth 'http://[moloch viewer の ID]:[moloch viewer のパスワード]@[Arkime Server の IP]:8005/sessions.json'
```

4. まとめと今後の課題

本稿ではマルウェアの内部展開通信であるラテラルムーブメントを検出するための内部トラヒック調査のために，Arkime を用いた環境構築とその例について述べた．実際のラテラルムーブメント通信の検出には至っていないが，類似の通信である，脆弱性スキャナの通信を検出することができた．また，設定不備が考えられるルータの存在も検索により発見することができた．さらに，Web API を用いて Arkime が蓄積しているセッション情報を取得できることも確認できた．

今後は目視ではなく自動でこの様な異常な通信を検出するための分析手法について検討していく必要があると考えている．具体的には，Web API を用いて自動取得したセッション情報を統計的に分析することで，外れ値の検出ができないかと考えている．

謝辞 本研究は JSPS 科研費 JP21K11889 の助成を受けたものです．

参考文献

[1] 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて, https://www.ipa.go.jp/security/announce/20191202.html, (参照 2020 年 10 月 12 日)
[2] https://arkime.com/, (旧 Moloch), (参照 2021 年 9 月 28 日)
[3] ダークネットトラフィックの分析に基づく継続的な広域ネットワークスキャンの調査, 中 川 雄太, 韓 燦洙, 島村 隼平, 高橋 健志, 藤田 彬, 吉岡 克成, 井上 大介, コンピュータセキュリテ ィシンポジウム 2019 論文集, 2019 年
[4] 広域ネットワークスキャンに基づくオープンソースハニーポットの運用実態調査, 森 下 瞬, 上野 航, 田辺 瑠偉, カルロス ガニャン, ミシェル ファン イートゥン, 吉岡 克成, 松本 勉, 情報処理学会論文誌 61(9),1397-1413, 2020/9/15
[5] https://www.darktrace.com/ja/, (参照 2021 年 9 月 28 日)
[6] https://www.vectra.ai/jp/home, (参照 2021 年 9 月 28 日)
[7] https://arkime.com/apiv3,(参照 2021 年 10 月 5 日)