C-14

TRAFL のデータベースを活用したトラフィック解析と可視化による暗号通貨のマイニングの検出支援の提案

龍　偉†　　川橋　裕‡

あらまし：和歌山大学の既存研究であるネットワークトラフィック監視システム TRAFL(TRAffic Flow Lagoon)のデータベースを活用し，ネットワークトラフィックの解析と可視化によるマイニングの検出を試みた．具体的には，マイニングを行った際の通信の特徴を考察し，それに応じた解析手法を考案した．学内外の間の通信記録を保存している TRAFL のデータベースに，提案手法を用いて問い合わせる．抽出した通信記録のグラフ化を行った結果，マイニングと疑われる通信の検出に成功した．

1. はじめに

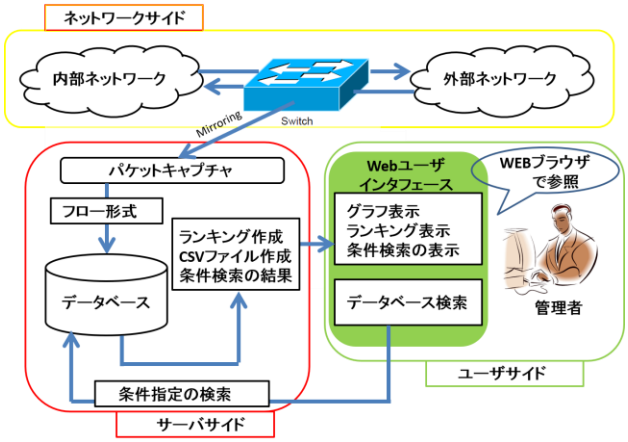
McAfee 社の 2018 年の調査によれば，PC や IoT などを含めたコンピュータを狙うマイニングツール，いわゆるコインマイナーのマルウェアの種類は１年間だけで 4000¥%以上増加している．また，企業や学校などの組織では，BYOD (Bring Your Own Device) や IoT (Internet of Thing) の導入により，持ち込み端末やセンサーなどにもインタネットの接続に対応する必要があるため，組織のネットワーク構成が膨張化している．その中，インタネットに接続した端末はウィルス対策がされていない場合，仮想通貨のマイニング（以下，マイニング）のマルウェアに感染されやすい．コストの削減や生産性の上昇を期待して BYOD を導入した組織では，持ち込み端末に OS の定期アップデートやセキュリティソフトウェアのインストールなどの安全対策を強要しにくい．実際に大学の場合では，大学 ICT 推進協議会の 2018 年の調査結果によると，日本の大学における持ち込みのモバイル端末は３割弱しかセキュリティソフトウェアを使用していないという．また，多くのメーカーは IoT 機器を設計する際に，電気消費や性能などに制約があるため，セキュリティの考慮が少ないと指摘されている．以上より，組織内におけるマイニングマルウェアの対策は個々の端末だけでは限界があり，ネットワーク全体の監視を行う必要があると考える．

2. 既存の検出手法と問題点

ネットワーク上を流れる通信から，マイニングの有無を検出する方法として， DNS サーバのログ分析や WAF (Web Application Firewall)のシグネチャー照合があり，いずれもパケットの中身を解析することになる．前者は組織外の DNS を使用した場合では調査できず，後者は新種のマルウェアに対応するシグネチャーが即座に生成されない問題がある．また BYOD (Bring Your Own Device) の導入や IoT (Internet of Thing) 機器の普及により，膨張化する組織ネットワークでは，パケットごとを解析する前述のような手法は非効率的だと考える．そこで，本研究は組織の内部と外部を流れる通信トラフィックを可視化し，そのグラフの特徴からマイニングの検出を試みる．

3. TRAFL について

現行 TRAFL のシステム構成は下図に示す．



TRAFL はネットワークサイド，サーバサイドおよびユーザサイトの３サイドで構成される．ネットワークサイドで流れる全パケットは，スイッチのポートミラーリング機能により複製されサーバサイトに伝送される．そして，サーバサイトのパケットキャプチャ部によりパケットを取得し，１分ごとにフロー形式で整形してからデータベースに挿入していく．管理者はユーザサイトの Web インタフェースでデータベースに格納している通信記録を検索し，その結果をリストやグラフで表示することができる．

4. 暗号通貨について

暗号通貨（英：cryptocurrency）は，原像計算困難性であるハッシュ関数による暗号化した仮想通貨（英：virtual currency）である．暗号通貨の取引履歴を記録した台帳は，中央管理サーバではなく，ブロックチェーンと P2P (Peer to Peer)の技術を用いて全世界のネットワーク上で分散して管理されている．

3.1 マイニングとマイニングプール

マイニングとは暗号通貨における新規取引の承認および，過去の取引履歴との統合性を図るための一連の作業のことであり，その中の重要な一環として，ハッシュ値の計算が必要である，マイニングでは特定のハッシュ値が算出するまでに計算が繰り返されるため，莫大な計算力が必要とな

†和歌山大学大学院

‡ 和歌山大学　学術情報センター

る．そのため，ハッシュ値の計算は世界中のマイニングの参加者たちに分配して分散する方法を取っている．また，全世界でいち早くマイニング作業を成功させた見返りとしては，新たに暗号通貨が発行され支払われる．このような仕組みでは，参加者たちは競って計算力を増やそうとするため，他人の計算資源でマイニングさせるマルウェアが増える理由の１つでもある．

マイニングの参加者は主に前述のハッシュ値の計算を行うが，一般的にその元となるデータの取得先は，マイニングプールと呼ばれるサーバ（群）である．また，算出したハッシュ値はマイニングプールに送り，値の有効性が判断される．一般的に，一種の仮想通貨におけるマイニングプールは複数あり，それぞれは異なるドメインに所有される．

3.2　マイニング通信の特徴

マイニングを行う際に発生する通信は，コインマイナーとマイニングプールの間の通信であり，本論文ではマイニング通信と呼ぶ．マイニング通信のトラフィックは以下のような２つの特徴がある．

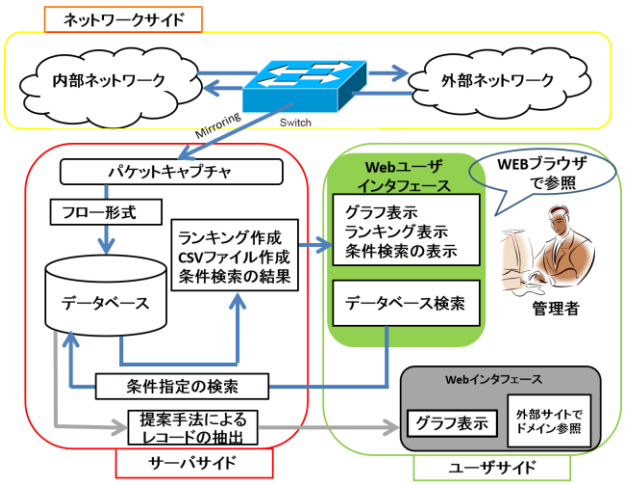
1) 1000 個のコインマイナーを用いた実験の結果によると，１個のコインマイナーを稼働するために，帯域幅は 1Mbps でも過大だという．

2) 暗号通貨の仕組み上，参加者は利益を得るためにできるだけコインマイナーを稼働するため，マイニング通信は長引く傾向にあると考える．

5.　研究目的

本研究は，マイニング通信の特徴に応じ，TRAFL のデータベースの操作手法を考案した．それを用いてデータベースからマイニング通信のフローを抽出し，グラフ表示ができるようにした．管理者にトラフィックグラフを提示することより，マイニング通信の調査支援をしたい．

6.　提案システムの概要



上図のように，本研究は現行の TRAFL をそのまま利用し，提案手法の有効性を検証する．システムの構築にあたり，提案手法の SQL やコマンドによるデータベースの操作は，python のプログラムを用いて簡易化にした．また，グラフの出力は JavaScript のライブラリである Highcharts を利用した．管理者の調査を支援するために，生成されたトラフィックグラフにマウスで左クリックすれば，自動的に外部サイトの virustotal.com で，宛先 IP アドレスのドメイン等の検索ができるようにした．

7.　実験と評価

本研究は二段階に分けて実験を行う．第一段階では提案手法の精度を上げるため，データベースを操作する際に用いるパラメータを変更し，誤検出の件数の変化を観測する．第二段階では改善した提案手法を用いて異なる状況での有効性を検証する．ただし，誤検出とは，提案手法を用いてデータベースから抽出したフロー群の中に，本研究で稼働したコインマイナーとマイニングプールの間の通信以外のフローを指す．

下図は実験の結果の一例である．



8.　今後の課題

提案手法の課題として，以下のようなである．

- well-known ports に対応できない
- 数時間しかマイニングを行った場合では検出できない
- DHCP を利用している端末は IP アドレスが変わりやすいため，検出できない可能性がある

提案手法で well-known ports を除外しないようにすると，誤検出を含むトラフィックグラフは 40 個ぐらい生成されるため，グラフの確認は管理者の負担になる．また，本研究の実験は１日マイニングを行った場合のみ考慮したため，数時間だけのマイニングが行われたら，誤検出の影響で提案手法による検出は困難である．さらに，DHCP により IP アドレスを取得しているモバイル端末は，随時に IP アドレスが変更する可能性があるため，検出されない可能性がある．以上の課題は誤検出の検出を減少できれば，解消されることになるため，本研究における一番の課題は誤検出であると考える．

9. 参考

[1] 陰地 健太 “トラフィックとフロー数の検索情報に基づいたネットワーク障害の調査支援するための TRAFL の拡張”

[2] “BYOD を活用した教育改善に関する調査研究 結果報告書”
https://axies.jp/ja/ict/2017axies_byod_report

[3] McAfee “Labs Threats Report” (December 2018)
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

[4] “IoT マルウェア攻撃の徹底調査 ”https://www.ibm.com/developerworks/jp/iot/library/iot-anatomy-iot-malware-attack/index.html

[5] “How to detect Cryptocurrency Mining Activity on Your Network”
httpswww.netfort.com/blog/detect-cryptocurrency-mining-activity/

[6] “We answer how much bandwidth crypto mining uses with 1000 miners”
https://www.servethehome.com/answer-much-bandwidth-crypto-mining-uses-1000-miners/

[7] 大塚　雄介”いまさら聞けないビットコインとブロックチェーン” FIT2012（第 11 回情報科学技術フォーラム）, 2012 年 9 月

[8] 総務省 “平成 29 年版 情報通信白書｜爆発的に増加する IoT デバイス”
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc133100.html