

悪性 Botnet 包囲網におけるマイニングマルウェア検知のための 特徴抽出の試行

村上 順也¹ 山之上 卓¹

概要: マイニングマルウェアがマイニングを動作させたときの通信がマイニングウェアの通信と類似していると仮定し、マイニングの通信の性質を、Wireshark で観測することにより、抽出した。この性質を使って、現在開発中の悪性 Botnet 包囲網によるマイニングマルウェアの通信が検出できる可能性があることを確認した。ここで、悪性 Botnet 包囲網で得られたデータの解析に R を用いている。

キーワード: 双方向, デジタルサイネージ, スマートフォン

Experimental Feature Extraction for Detecting Mining Malware in the Botnet Detecting Infrastructure

Junya Murakami^{†1} Takashi Yamanoue^{†1}

Abstract: We discuss the possibility of detecting the mining malware communications using our botnet detecting infrastructure using beneficial botnet. We have used the features of mining malware communications for this detection. The features are collected by using Wireshark, by assuming that mining-malware communications are similar to the mining-malware communications.

Keywords: Intrusion detection, Mining malware, botnet

1. はじめに

2018 年からマイニングマルウェアが増加している[1]. マイニングマルウェアは他人のホストからバックグラウンドでマイニングプールに参加させ、CPU リソースを横取りして利益を攻撃者の口座に入るよう設定させ不利益を与える。暗号通貨の価格の上昇と比例してマイニングマルウェアが増加していることから、暗号通貨の価値の上昇に伴い、マイニングマルウェアを使用した攻撃がこれからも増加する可能性が高いと考えられる。さらに、セキュリティの甘い IoT デバイスを狙ったマイニングマルウェアも増加している。

2017 年に急増し、現在は減少傾向にあるランサムウェアと比較してマイニングマルウェアは低リスク、低コストで稼ぐことができることから攻撃者には都合がいい。感染ホストに不正マイニングを行って暗号通貨を稼ぐため、攻撃者はいかに見つからないことを目的とし攻撃手法を巧妙化させている。トレンドマイクロのセキュリティブログによると正規プロセスの中に不正なプロセスを入れ替えるプロセスハロウイングという手法と不正活動開始にコンポーネントファイルにコマンドライン引数を参照させる手法とを組み合わせる高度な検回避避手法が確認されている[2]. 引数が呼び出されなかったときは不正ファイルを見つけ出すことができないことで動的解析を困難化させている。この

ような攻撃手法でゼロデイ攻撃を受けた場合にウイルス対策ソフトでは検知できない可能性がある。我々は、不正マイニングをされているときの通信の特徴を用いて検知が可能と考え、その特徴をもとに検知するシステムを開発している。

我々は悪性 Botnet 包囲網を開発している。これは LAN の NAT の内側に設置する Agent Bot と、Agent Bot によって選択収集されたデータを解析する Analyzing Bot により構成された、良性 Bot のグループである[9][10][11][12][13].

本稿では、悪性 Botnet 包囲網の Agent Bot を使って収集したパケット情報を Wiki ページに書き込み、Wiki ページからパケット情報を Analyzing Bot の R に読み込ませて分析し、抽出したマイニングウェアの特徴をもとにマイニングの動作を検知できるのではないかと仮定し、その可能性の検証を行ったことについて述べる。

2. マイニングウェアの通信の特徴

マイニングウェア(MinerGate)が動作しているときの通信とマイニングマルウェアが不正マイニングしているときの通信は似た通信の観測結果になると仮定し、マイニングウェアである MinerGate が動作している通信と様々な場面での通信を Wireshark でパケットキャプチャし、それぞれの通信結果を比較してマイニングウェアが動作しているときの特徴の抽出を試みた。

¹ 福山大学
Fukuyama University

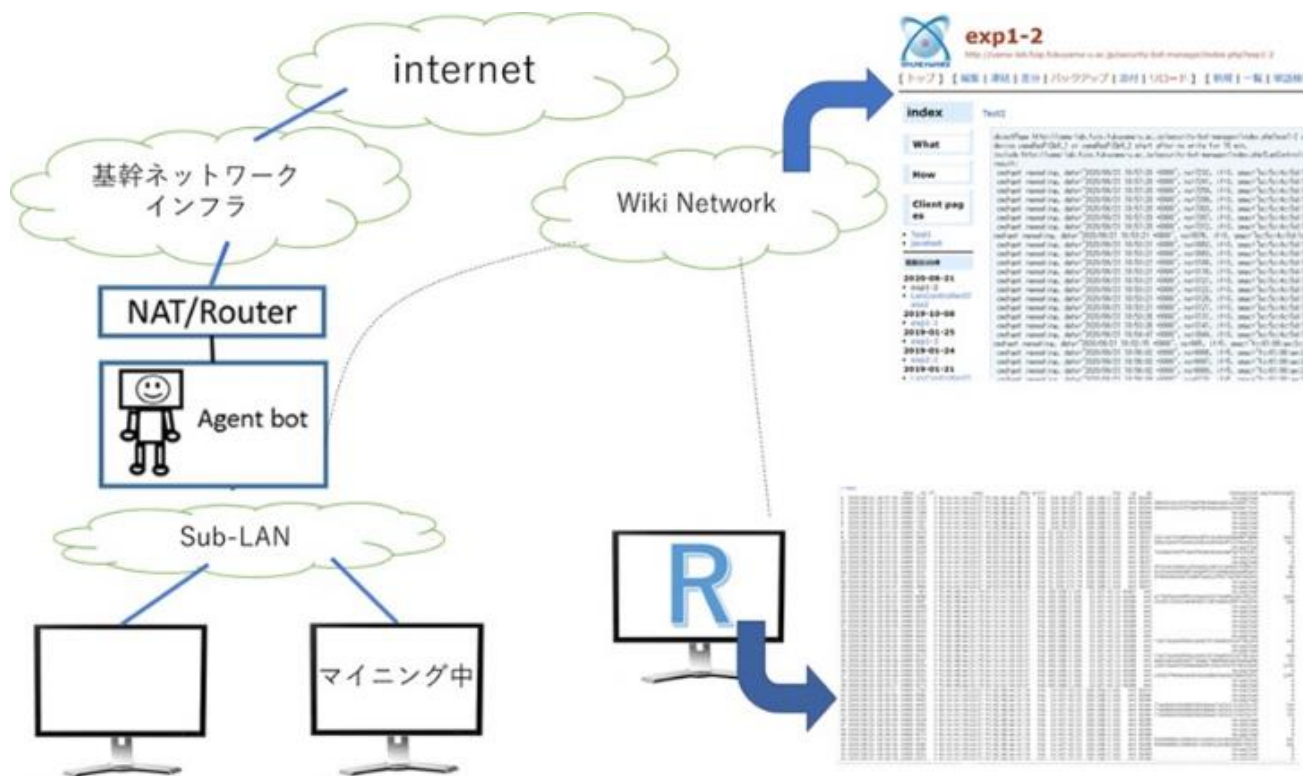


図 1 悪性 Botnet 包囲網を利用したマイニングウェアの検知システムの 構成

マイニングウェアは MinerGate の MinerGate Mobile Miner と呼ばれるアプリケーションを使用した[17]. MinerGate とは、様々な暗号通貨をマイニングできるマイニングプールである。MinerGate でマイニングする際の暗号通貨は Monero を選定した。Monero は匿名性が高く、2018 年ごろに価格が上昇したこともあり、攻撃者によって不正マイニングされやすい。paloalto NETWORKS によると、Monero はマイニングマルウェアの標的となる暗号通貨の中で大部分を占めていることが確認されている[8]。この原因として、マイニングする際に他の暗号通貨と比較して計算の難易度が低く、一般的な PC の CPU でもマイニング可能であることから不正マイニングされる暗号通貨の中で上位に位置付けられていると考えられる。

Wireshark でパケットキャプチャする時間は 256 秒前後で打ち切る。MinerGate でマイニングする際の設定は CPUcore 数が 3 で Reword method は PPS とする。また、MinerGate Mobile Miner はバージョン 1.6 で動作させる。ちなみに、マイニングウェアを動作させるホストのスペックは CPU が Intel®Core™i5-5200U@2.20GHz、メモリが 8.00GB、OS が Windows 10 Home である。

2.1 Miner Gate の通信

MinerGate によってマイニングされている通信を Wireshark で約 256 秒パケットキャプチャして、Wireshark の機能である対話表(図 2)や通信量の変化(図 3)などを見て

分析した結果、特徴になり得そうな点を以下に示す。

- MinerGate の IP アドレスからマイニングしているホストへのポート使用数が格段に多くなる時があること
- 単位時間あたり、同じパケット数を継続して確認できること
- MinerGate の IP アドレス側の 45700 ポートの通信が長時間継続して確認されやすいこと
- MinerGate とホストとの通信ストリームにおけるポートそれぞれの総バイト数の大きさ
- 双方向の通信のバイト数を合わせた大きさ

図 3 の横軸は継続時間を表している。Duration で 256 秒以上継続がみられる通信は全て MinerGate と MinerGate を動作させているホストとの通信であった。また、MinerGate の IP アドレスである 88.99.142.163 のみで表示させた入出力グラフでは複数の同バイト数が継続している通信を確認した。

2.2 Miner Gate 以外の通信との比較

日常で PC を使用しているときの PC の状況を再現した通信を Wireshark で約 256 秒間パケットキャプチャして比較した。再現状況として、4 つの状況を挙げる。

Ethernet - 1	IPv4 - 3	IPv6	TCP - 26		UDP													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A					
192.168.11.6	55665	136.243.102.154	443	22	8574	11	1662	11	6912	44.947236	1.8236	7291	30 k					
192.168.11.6	55670	136.243.102.154	443	20	8575	9	1422	11	7153	75.172388	2.0815	5465	27 k					
192.168.11.6	55666	136.243.102.154	443	15	2219	8	1453	7	766	46.509017	2.2772	5104	2691					
192.168.11.6	55169	88.99.142.163	443	10	674	5	342	5	332	24.650996	7.0791	386	375					
192.168.11.6	55669	136.243.102.154	443	43	14 k	21	2605	22	11 k	50.495411	7.1647	2908	13 k					
192.168.11.6	55171	136.243.102.154	443	9	624	6	399	3	225	16.594537	15.1441	210	118					
192.168.11.6	54982	136.243.102.154	443	9	624	6	399	3	225	14.522026	17.4524	182	103					
192.168.11.6	55168	136.243.102.154	443	8	570	5	345	3	225	6.522052	25.2088	109	71					
192.168.11.6	54980	136.243.102.154	443	9	624	6	399	3	225	6.521745	25.5563	124	70					
192.168.11.6	54981	136.243.102.167	443	14	965	7	450	7	515	0.911767	31.1714	115	132					
192.168.11.6	55662	136.243.102.154	443	20	8053	9	1141	11	6912	44.912327	60.8161	150	909					
192.168.11.6	55660	136.243.102.154	443	21	8834	9	1715	12	7119	44.584912	67.4285	203	844					
192.168.11.6	55677	136.243.102.154	443	15	2219	7	1399	8	820	131.591036	67.8755	164	96					
192.168.11.6	55659	136.243.102.154	443	30	14 k	13	2497	17	11 k	44.584287	67.9673	293	1363					
192.168.11.6	55658	136.243.102.154	443	28	10 k	13	2498	15	7531	44.583544	68.1641	293	883					
192.168.11.6	55667	136.243.102.154	443	15	2219	7	1399	8	820	48.525146	68.2662	163	96					
192.168.11.6	55678	136.243.102.154	443	53	16 k	23	2753	30	13 k	133.197691	76.4019	288	1458					
192.168.11.6	55668	88.99.142.163	45700	255	32 k	132	20 k	123	11 k	49.481922	160.8110	1039	562					
192.168.11.6	55663	136.243.102.154	443	40	10 k	17	2017	23	8160	44.936919	161.4898	99	404					
192.168.11.6	55664	136.243.102.154	443	38	10 k	16	1964	22	8360	44.937552	161.4943	97	414					
192.168.11.6	55023	136.243.102.154	443	21	1596	7	623	14	973	24.754560	181.8704	27	42					
192.168.11.6	55190	88.99.142.163	443	21	1596	7	623	14	973	24.555415	181.9766	27	42					
192.168.11.6	55197	88.99.142.163	443	25	1970	9	731	16	1239	24.156689	182.3733	32	54					
192.168.11.6	55020	136.243.102.154	443	25	1970	9	731	16	1239	24.059515	182.5628	32	54					
192.168.11.6	55504	136.243.102.154	443	62	13 k	26	1708	36	11 k	3.510756	206.0686	66	453					
192.168.11.6	55160	88.99.142.163	443	62	13 k	26	1708	36	11 k	3.512664	206.0870	66	453					

図 2. MinerGate の通信のみ継続の度合いが高いことを表した対話表

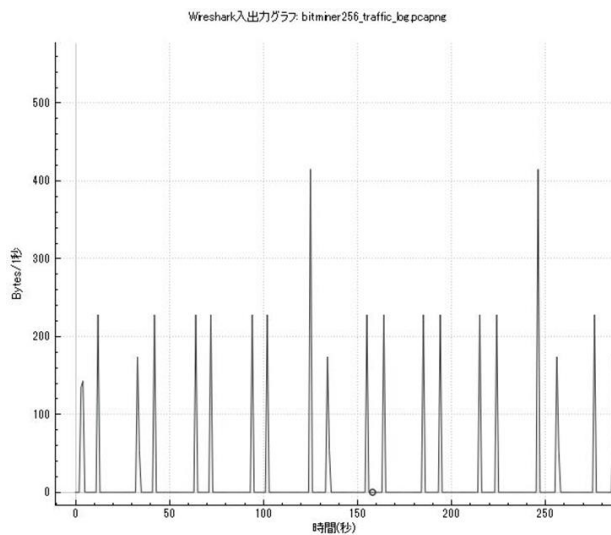


図 3 MinerGate の一部の通信量の変化

- Skype でマイク確認テストを数回行ったとき
- ネットサーフィンをしているとき
- Youtube を視聴しているとき
- 何もせず放置したとき

通信を取るホストのスペックは MinerGate の通信をパケットキャプチャしたときと同様で CPU が Intel®Core™i5-

5200U@2.20GHz, メモリが 8.00GB, OS が Windows 10 Home である。

Skype を使用した状況再現では Skype でのマイク確認テストを定期的に行うことにした。マイク確認テストは 1 分ほどで終わるので、何回も繰り返してマイク確認テストをした結果をパケットキャプチャした。

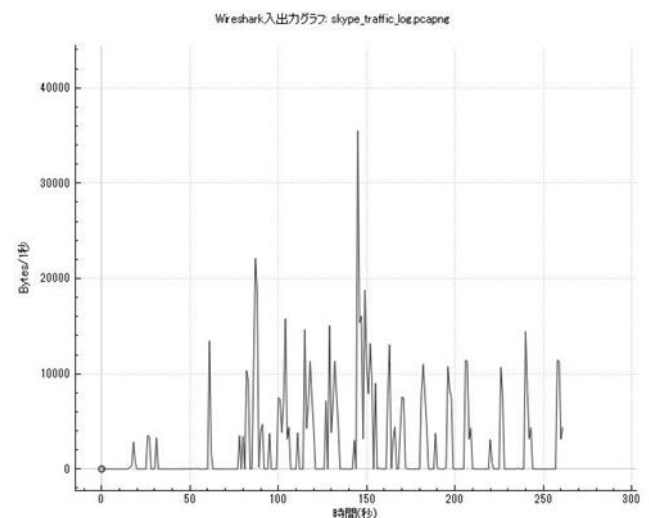


図 4 Skype のマイク確認テスト時の通信量の変化

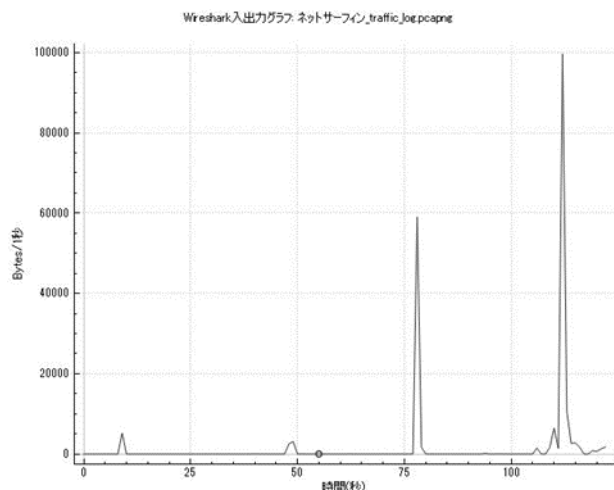


図 5 ネットサーフィン時の通信量の変化

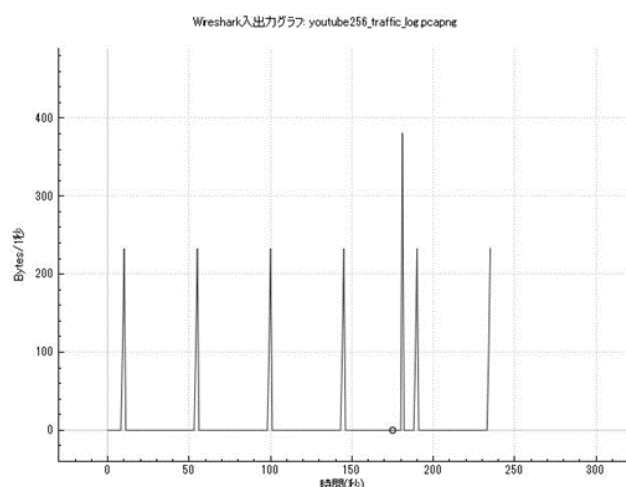


図 6 Youtube 視聴時の通信量の変化

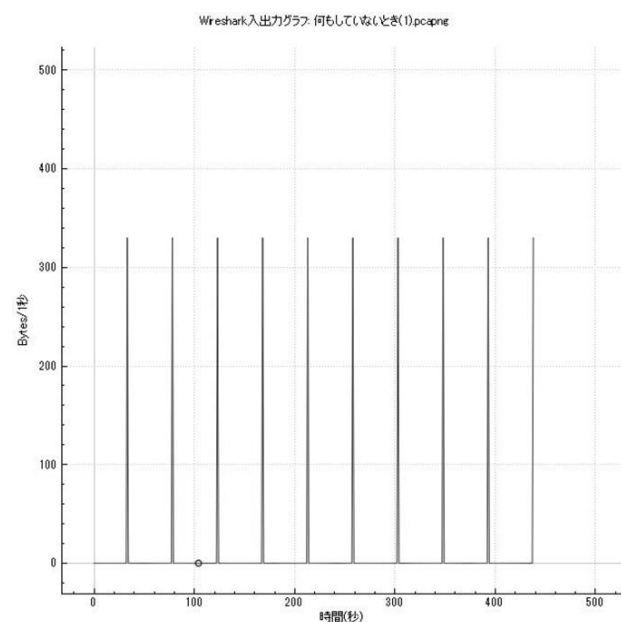


図 7 何もしていない時の通信量の変化

マイク確認テスト自体の継続された通信は取れる可能性が低い、宛先 IP アドレスは変わらないと考えているので、継続された通信が取れると考える。

ネットサーフィンをしているときはどんなサイトを閲覧するかは決めずにランダムで決めている。

Youtube を視聴しているときの通信では、視聴する動画はランダムで決めている。ただし 256 秒以上の動画を選定しており、動画が再生してからパケットキャプチャをしている。

何もせず放置したときの通信は何もアプリケーションを起動させずに通信をパケットキャプチャする。

2.2.1 MinerGate の通信と Skype を使用したとき通信の比較

Skype を使用すると必ず IP アドレス(20.189.78.37)を使用し、その IP アドレスは名前解決がされており、Google 関連の安全な IP アドレスであった。図 4 で示している一部の IP アドレスの入出力グラフは MinerGate の通信の特徴であるポート使用数と単位時間あたりに同じバイト数を継続して通信している箇所が所々にみられる。だが、ポートそれぞれのバイト数の偏りと双方向の通信を合わせたバイト数の大きさに差があることから区別できる。

2.2.2 MinerGate の通信とネットサーフィンをしたときの通信の比較

ネットサーフィンの通信は、図 5 で示した折れ線グラフのような通信ばかりであり、単位時間当たりの同じパケット数を継続して確認することはなかった。このことから、安全にネットサーフィンをすることができれば、MinerGate との通信の特徴は明白に区別できる。

2.2.3 MinerGate の通信と Youtube の動画を視聴したときの通信の比較

Youtube を視聴しているときの通信では MinerGate の通信と似た、継続している通信を 2 種類発見した。Google と Microsoft であり、(図 6)に示されたように継続はされている。しかし、パケット数が MinerGate と比べて小さいことから、区別することができる。

2.2.4 MinerGate の通信と何もしなかったときの通信の比較

何もせず放置した通信は何もしていないがたびたび通信があった(図 8)。IP アドレスをドメイン解決した結果 Microsoft 関連の通信であり、OS が通信をしていると考えられる。同バイト数の継続した通信がみられたが、パケット数が MinerGate の通信と比べて低かったことから、区別することができる。

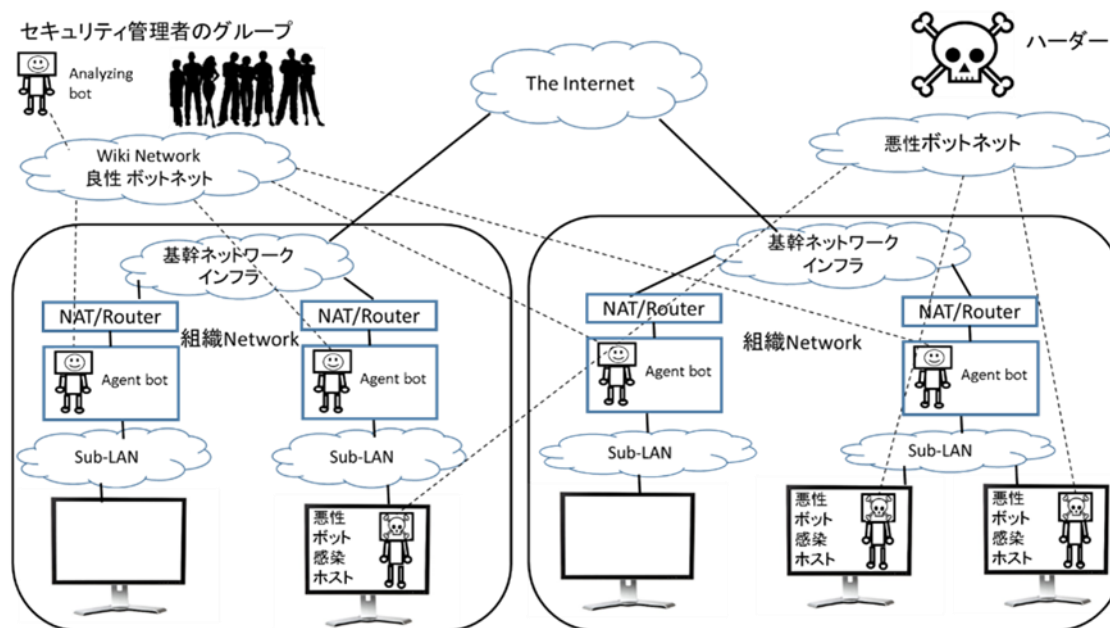


図 8 悪性 Botnet 包囲網の概要

4つの状況の通信は、抽出した MinerGate の通信の特徴と区別することができたことから有用性のある特徴とする。そこで、開発途中である悪性 Botnet 包囲網を使用して MinerGate の通信とその他の通信を区別できるかどうかの確認作業を行っている。3章で悪性 Botnet 包囲網の詳細について述べる。

3. 悪性 Bot 包囲網

悪性 Botnet 包囲網は、従来の IDS や IPS の欠点を克服しようとするものである。図 8 に悪性 Botnet 包囲網の概要を示す。Agent Bot は Sub-LAN と NAT または Router の間に設置される。Agent Bot は Sub-LAN と Sub-LAN の外部との通信データを収集する。Analyzing Bot は Agent Bot が収集したデータを集めて解析し、sub-LAN 内に潜む Bot を検出する。すべての Agent Bot と Analyzing Bot はインターネット上の Wiki のページに書かれた script によって制御される。

3.1 Agent Bot

Agent Bot は”Traffic controller” (tcon) を備えた良性 Bot である。

tcon は2つの network interfaces とデータ取得ライブラリ (DAQ) と Filter/Controller と複数の Buffer を持っている。DAQ として Pcap4j を使っている。

この Bot の script interpreter は tcon の操作も行う。Bot は2つの interface の間の通信データを収集し、main wiki の script によってそのデータを main wiki のページに書きこ

む。2つの interfaces 間の通信の制御することもできる。Network interface の一つを NAT または router に接続し、もう一つを sub-LAN に接続することにより、sub-LAN と sub-LAN の外との間の通信のすべてを収集し、制御することができる。図 9 に Agent Bot の構造を示す。

tcon は以下の buffer を持つ。通信データはその種類によって分類され、これらの buffer に格納される。

□ Packet-history

この buffer は2つの interface 間で転送されるパケットの情報を格納する。この buffer は同じ source IP address と destination IP address のペア同士を格納するための sub buffer を持っている。Packet の payload の sha1 hash とその packet が転送された時間と packet の情報もペアと一緒に格納される。Sha1 の値は2つの異なる sub-LAN 間で行われる P2P 通信を検知するために使われる。Sub buffer があふれた時、古い情報が削除される。

□ MAC-list

この buffer は sub-LAN 内でやりとりされるすべての frame の MAC address を格納する。MAC address に対応付けられたすべての IP address も Mac address に関連付けて格納される。MAC list はこの sub-LAN に接続されているホストや、LAN 内の IP address を知るのに使うことができる。他よりも多くの IP アドレスが結び付けられている MAC address を見つけることにより、default gateway を特定することもできる。

□ Domain-list

この buffer は sub-LAN 内の DNS query をその query が行われた時間と一緒に格納する。Domain-list は sub-LAN のど

のホストが LAN 外のどのホストと通信したか知るために使うことができる。この list は DGA の利用を検知するためにも利用することができる。

□ Dhcp-list

この buffer は DHCP 通信の結果をそれが行われた時間と共に格納する。この list は DHCP spoofing や不正 DHCP サーバの検知を行うのに使うことができる。Default gateway を特定するのにも役立つ。

□ Arp-list

この buffer は Arp 通信をそれが行われた時間と共に格納する。Arp spoofing の検知に使うことができる。

Agent Bot はこれらの buffer から情報を得たり、操作したりするコマンドを実行できる。2 つのネットワーク間の通信を制御するコマンドも持っていて、このコマンドを使うことで悪性 Bot の通信を見つけた時、その通信を遮断することもできる。

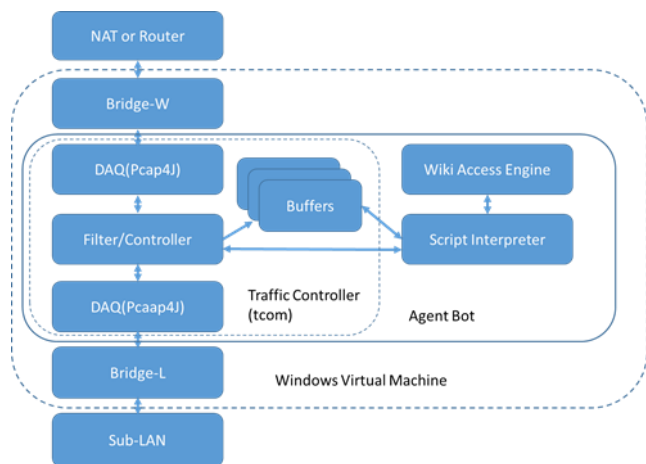


図 9 Agent Bot の構成

3.2 Analyzing Bot (R を使った解析部)

Analyzing Bot は各 Agent Bot で収集された情報を集め、それを解析する。

すべての良性 Bot の言語プロセッサは、comma separated value (CSV) parser と表操作/表計算関数を備えている。

Analyzing Bot はこれに加えて R 統計計算システムも備えている。Analyzing Bot の script の中に R のプログラムを埋め込むことができる。良性 Bot が元々備えている言語プロセッサと R 統計計算システムの間で値を交換する関数も使うことができる。

今回は R をインストールしたパソコンを Analyzing Bot の代わりに利用した。

4. 解析結果例

マイニングが動作しているときの通信の特徴が表れる以下の特徴を軸とした 3 次元散布図を作成し、解析した。

□ 単位時間当たりのパケット数

□ 継続している秒数

□ 単位時間当たりのバイト数の分散

バイト数の分散の算出の仕方は取得したパケット情報を収集する時間を、設定した値で分割し、分割した間隔ごとに間にあるパケットのバイト数を計算し、それぞれの間隔から算出されたバイト数を計算する。分散を使う理由として、複数の同じバイト数を長い時間継続しているマイニングの通信とそうでない通信を判別する際に、マイニングの通信は分散が低くなり、そうでない通信は分散が高くなると推測したからである。分割する値を設定する値は細かいほうが良いが、処理時間に関係するため、パケット取得数に適切な値を設定する。

図 10 に作成した 3 次元散布図を示す。図 10 の作成には shiny パッケージ[24]、ggplot2 パッケージ、plotly パッケージ[25]を使用した。

分散が低く、継続時間の長さの値が高く、パケットが多数みられる場所がマイニングウェアの通信が行われている疑いを持つ範囲であるが、この範囲は Agent Bot の IP アドレスごとに取得するパケットの数の上限の設定によって変化する。分散を X 軸、継続時間の長さが Y 軸、パケット数が Z 軸で表している。右側に通信ストリーム先が記載されている。

図 10 の 3 次元散布図は回転させることができる。また、点にマウスカーソルを持っていくと XYZ の値、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号が記載されたツールチップが表示される。

Mining Ware の通信の分散は少ないと仮定したが、一部分分散が大きい場合が存在した。しかしながら、分割する値によっては判断材料になりえる可能性がある。分析項目に加えるかどうかは今後の課題とする。

抽出した特徴から推測した疑いを持っている範囲に MinerGate の通信が確認できることから、Agent Bot のパケット数の取得の上限設定と Wiki ページに記録する行数に応じた閾値を決めて範囲指定をすれば、範囲に入っている示された IP アドレスとポート番号の通信がマイニングの通信であると疑いを持つことができ、検知できる可能性がある。

4.1 主成分分析

3 つの特徴による特徴空間を使って判別する手法ではパケット数、継続した秒数、バイト数の分散の 3 つの情報を使用したが、3 つの情報に相関性があるかどうか確認するため R で主成分分析を用いた。

軸の間に強い相関があった場合は、必要のない軸があることになる。主成分分析の結果を図 11 と図 12 に示す。図 11 の PC1 は第一主成分、PC2 は第二主成分、数字はパケット情報、赤の矢印は向きが 2 つの主成分に対する各変数の方向を表し、長さは各変数が各主成分とどれだけ相関が強いを表す。

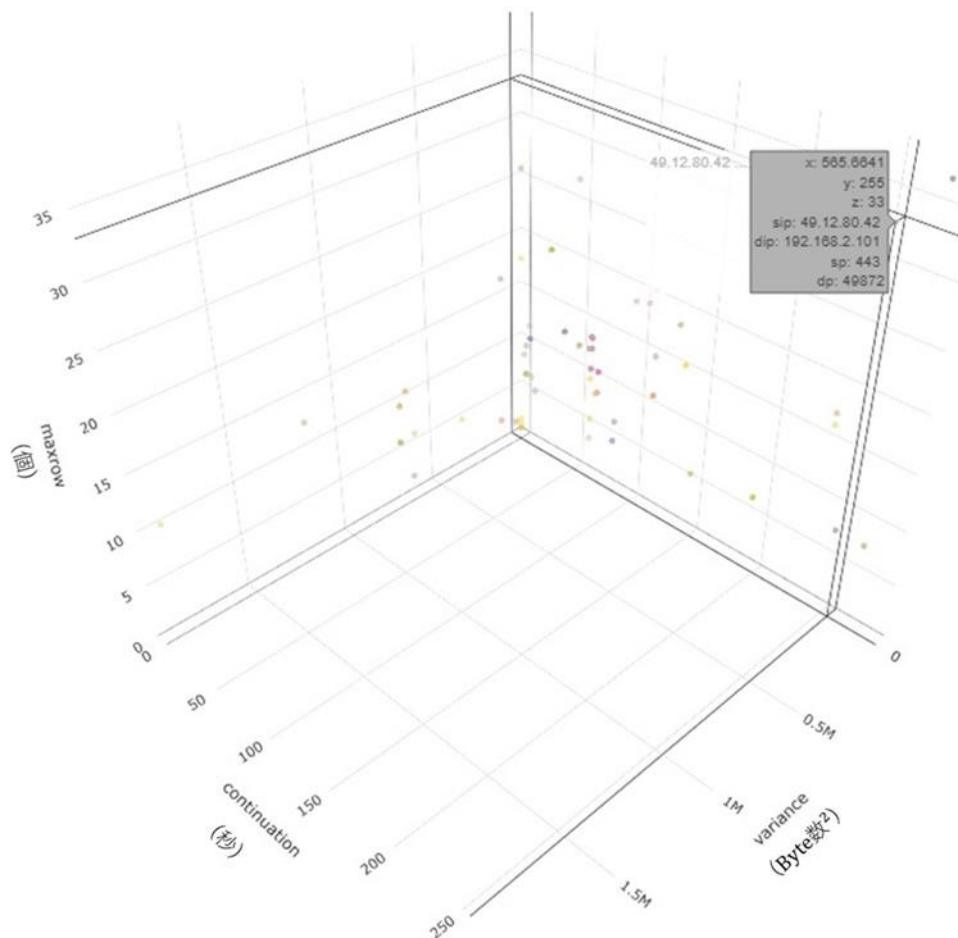


図 10. 単位時間当たりのパケット数, 継続秒数, 単位時間当たりの分散を軸とした散布図

図 12 の Standard deviation は標準偏差, Proportion of variance は寄与率, Cumulative Proportion は累積寄与率, PC1 は第一主成分, PC2 は第二主成分, PC3 は第三主成分を表す. 図 11 からそれぞれのデータが第一主成分と第二主成分の方向に縮退していないことから, 相関性はないと考える. 図 12 で示されている寄与率から第二主成分で十分情報が示されているが, バイト数の分散である variance の値は分割する値で変わり, 主成分分析で得た情報が変わる. パケット情報を収集する環境でも変わり, 今後データの収集次第で相関性が変わってくると考える. しかし, パケット数と継続時間とバイト数の分散の特徴は Wireshark でパケット情報を見た限り, 相関性はないと推測しており, これらの特徴は必要であると考えている. 双方向の通信のバイト数の偏りとポート使用数に関しても同様の理由で相関性はないと推測している. このことから, 分析項目に挙げている特徴は全てマイニングマルウェアの判別に有効であると

考える.

主成分分析をして得た図 11 からマイニングが動作しているときの通信とその他の通信を判別できる可能性があると考えている.

5. 関連研究

5.1 Detection of Bitcoin miners from network measurements

Zayuelas I Muñoz は CISCO 社のネットワークトラフィックを分析するルータ機能である Netflow を使用してキャプチャした情報の特徴を機械学習によって学習させ, マイニングしている通信の検知を行った[3]. 機械学習を用いて検知はできているが, 通信そのものがどのような特徴を検出して検知しているのかどうか判断することができない.

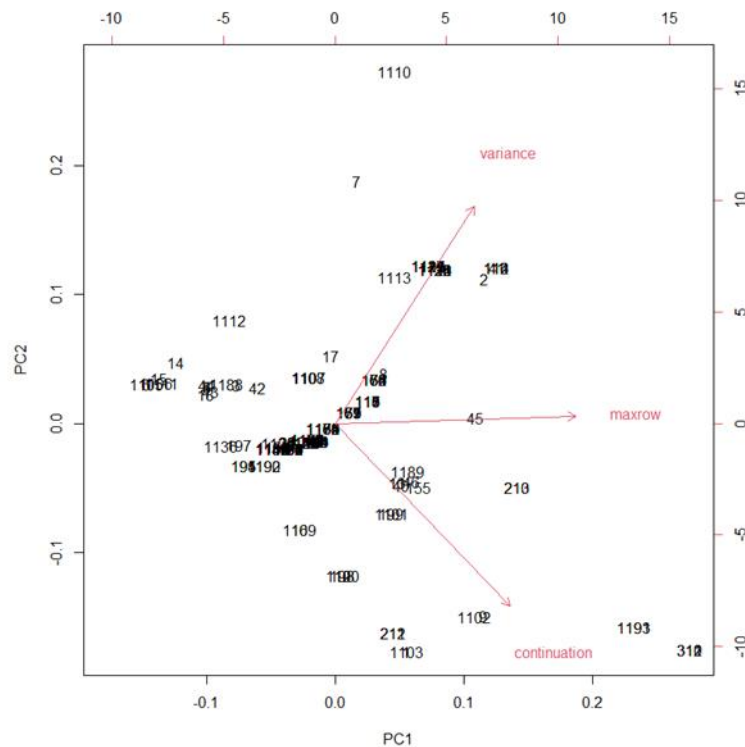


図 11 第一主成分と第二主成分で示された 2 次元の図

	PC1	PC2	PC3
Standard deviation	1.197	1.0340	0.7050
Proportion of Variance	0.478	0.3564	0.1656
Cumulative Proportion	0.478	0.8344	1.0000

図 12 標準偏差，寄与率，累積寄与率が示された表

我々の手法においては、マイニングウェアでマイニングしている通信を Wireshark でキャプチャし、パケットの毎秒の通信量などから特徴を抽出し、その特徴を明らかにしようとしている。

5.2 Fine-Grain Feature Extraction from Malware from Malware’s Scan Behavior Based on Spectrum Analysis

江藤らはパケットの宛先 IP アドレスの振動から SPpectrum Analysis for Distinction and Extraction of malware features (SPADE) によって離散フーリエ変換し、マルウェアの特徴を抽出するスペクトラム分析手法を提案した[4]。マルウェアの特徴を抽出する部分で類似している。我々の研究では、宛先 IP アドレスの毎秒の通信量をグラフ化した結果自体を扱い、特徴の抽出を試みている。我々の研究でもマイニングウェアが動作している通信をキャプチャし、プール先の宛先 IP アドレスの毎秒の通信量をグラフ化した結果を離散フーリエ変換して特徴抽出を試みたが、有用性のある特徴を見つけることができなかった。

5.3 Using R for Anomaly Detection in Network Traffic

Denis Hock らはデータの事前処理、分析操作、異常の実際の検出など、ネットワーク異常の検出に必要なすべての操作を R で実行できる異常検知システムの評価を行った[5]。さまざまなトラフィック機能から計算されたメトリックの統計的特性に基づいてトラフィック異常を検知しているが、我々の研究では、マイニングマルウェアに目標を絞り、マイニングウェアの通信の特徴をもとに検知を試みている。

6. おわりに

本研究ではマイニングの通信から特徴抽出をして、現在開発中の悪性 Botnet 包囲網でマイニングの通信とそれ以外の通信を分別できる可能性を示した。MinerGate が動作しているときの通信とマイニングマルウェアが不正マイニングしているときの通信は似た通信の観測結果になると仮定しているが、マルウェアが何らかの方法でウイルス対策ソ

フトを回避するための工夫をしている場合は検知が難しくなる可能性がある。しかし、正規のマイニングウェアをダウンロードさせてウイルス対策ソフトを回避するようなマルウェアが行うマイニングの通信は検知できる可能性がある。本研究で述べた手法のみで新種のマイニングマルウェアを検知することは難しいが、全ての新種のマルウェアについては様々なアプローチ方法で検知することが重要であるため、多層的に検知を試みる必要がある。多層的にセキュアな環境を構築したとしても、各層の対策を見破られた場合、攻撃者からの攻撃を防ぐことが難しくなる。

悪性 Botnet 包囲網の Agent Bot については設置する数が増えるとパケットを取得する数も増える。今回は R によって膨大な量のパケットの処理を行うことについては考慮していないが、膨大な量のパケットを扱う場合は処理に時間が掛かる可能性がある。IP アドレスごとのパケット取得に上限があることについても Sub-LAN 内のホストの数が増えると一度に Wiki ページに記録できる数も減ってしまうため、今後検討する必要がある。

マイニングが動作しているときの通信の特徴の抽出や R で通信を分析する際、ディープラーニングを使うと透明性が低くなる[26]ことから手動で行った。ブラックボックスになっているところを明白にするため、R で可視化などを試みた。しかし、特徴の抽出や特徴の選択、マルウェアの検知率に関しては、今のところディープラーニングで行ったほうが正確である。

本研究で扱ったマイニングが動作しているときの通信とその他の通信のパケット情報、その他の通信における環境の種類のこれらはデータを今後も増やしていく必要がある。

謝辞 本研究の一部は JSPS 科研費 16K00197 の助成を受けたものです。

参考文献

[1] 行正和義, “仮想通貨マイニングマルウェアが 71%増, マカフィー2018 年第 3 四半期の脅威レポート,” 角川アスキー総合研究所, 16 1 2019. [オンライン]. Available: <https://ascii.jp/elem/000/001/798/1798580/>.

[2] “巧妙な検出回避手法「プロセスハロウイング」を使用する不正コインマイナー攻撃,” Trend Micro, 27 12 2019. [オンライン]. Available: <https://blog.trendmicro.co.jp/archives/23376>.

[3] J. Z. I. Muñoz, “Detection of Bitcoin miners from network measurements,” Universitat Politècnica de Catalunya, 2019.

[4] Masashi ETO, Kotaro SONODA, Daisuke INOUE, Katsunari YOSHIHOKA, and Koji NAKAO, “Fine-Grain Feature Extraction from Malware’s Scan Behavior Based on Spectrum Analysis,” IEICE transactions on information and systems 93(5), 1106-1116, MAY 2010.

[5] M. K. Denis Hock, “Using R for Anomaly Detection in Network Traffic,” Fifth International Conference on Internet Technologies & Applications At: Wrexham, North Wales, UK, DOI: 10.13140/2.1.1400.0002, September 2013.

[6] 株式会社デライトチューブ, “仮想通貨のマイニングとは? 仕組み, やり方, 稼ぎ方, マイニングにおすすめな仮想通貨は?”, 株式会社デライトチューブ, 29 2019. [オンライン]. Available: <https://bitdays.jp/blockchain/mining/>.

[7] 山之上 卓, 村上 順也, “マイニングマルウェアの通信の特徴抽出の試行,” 情報処理学会研究報告, インターネットと運用技術 (IOT), vol. 2020-IOT-48, No. 6, pp. 1 - 6, 2020-02-24.

[8] “最もマイニングされた仮想通貨は? 攻撃者が稼いだ額は?-仮想通貨マイニングマルウェアの最新動向” paloalto NETWORKS, 14 6 2018. [オンライン]. Available: <https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-rise-cryptocurrency-miners>

[9] Yamanoue, T., Oda, K., Shimozono, K., “Capturing Malicious Bots using a Beneficial Bot and Wiki”, 2012, In Proceedings of the 40th annual ACM SIGUCCS conference on User services (Memphis, Tennessee, USA. 15-19 Oct. 2012). ACM, New York, NY, 91-96. DOI=<https://doi.org/10.1145/2382456.2382477>

[10] Takashi Yamanoue, Kentaro Oda, Koichi Shimozono. “A Malicious Bot Capturing System using a Beneficial Bot and Wiki,” 2013, Journal of Information Processing (JIP), vol.21, No.2, pp.237-245.

[11] Yamanoue, T., Oda, K., Shimozono, K. 2013. “An Inter-Wiki Page Data Processor for a M2M System,” 2013, In Proceedings of the 4th International Conference on E-Service and Knowledge Management (ESKM 2013), Advanced Applied Informatics (IIAIAAI), 2013 IIAI International Conference on (Matsue, Shimane, Japan, 31 Aug- 4 Sep. 2013) IEEE, Los Alamitos, CA. 45-50. DOI=<https://doi.org/10.1109/IIAIAAI.2013.48>

[12] Yamanoue, T., Oda, K., Shimozono, K., “Experimental Implementation of a M2M System Controlled by a Wiki Network,” 2014, In Applied Computing and Information Technology, Studies in Computational Intelligence, Springer, Vol.553, 121-136.

[13] Yamanoue, T., “Monitoring Servers, With a Little Help from my Bots,” 2017, In Proceedings of the 45th annual ACM SIGUCCS conference on User services (Seattle, Washington, USA. 01-04 Oct. 2017). ACM, New York, NY, 173-180. DOI=<https://doi.org/10.1145/3123458.3123461>

[14] 青木繁伸, R による統計解析, 株式会社オーム社, 2009 年 4 月 15 日.

[15] G. G. Hadley Wickham, R では始めるデータサイエンス, 株式会社オーム社, 2017 年 10 月 24 日.

[16] 村上 順也, 山之上 卓: “R を使ったマイニングマルウェアの特徴検知の試行”, 第 22 回 IEEE 広島支部学生シンポジウム (22th HISS) 論文集, (2020.12)

[17] “How to mining Monero” MinerGate, 7,9,2016. [オンライン]. Available: <https://minergate.com/blog/how-to-mine-monero/>

[18] “The R Manuals” R Development Core Team, 10,10,2020. [オンライン]. Available: <https://cran.r-project.org/doc/manuals/r-release/fullrefman.pdf>

[19] “gt package -Rstudio”, Richard Iannone, Joe Cheng, Barret Schloerke, [オンライン]. Available: <https://gt.rstudio.com/>

[20] “Function reference • ggplot2”, Hadley Wickham, Winston Chang, Lionel Henry, Thomas Lin Pedersen, Kohske Takahashi, Claus Wilke, Kara Woo, Hiroaki Yutani, Dewey Dunnington, [オンライン]. Available: <https://ggplot2.tidyverse.org/reference/>

[21] “Package ‘ggsci’”, Nan Xiao, 14,5,2018, [オンライン], Available: <https://cran.r-project.org/web/packages/ggsci/ggsci.pdf>

[22] “Package ‘rvest’”, Hadley Wickham, 25.7.2020, [オンライン], Available: <https://cran.r-project.org/web/packages/rvest/rvest.pdf>

[23] “A Grammar of Data Manipulation • dplyr”, Hadley Wickham,

Romain François, Lionel Henry, Kirill Müller,[オンライン].Available: <https://dplyr.tidyverse.org/>

[24]“Tutorial-R Shiny-Rstudio”, Shiny app developer community, [オンライン], Available: <https://shiny.rstudio.com/tutorial/>

[25]“Package‘plotly’”, Carson Sievert, 10,1,2021,[オンライン].Available: <https://cran.r-project.org/web/packages/plotly/plotly.pdf>

[26]“活用広がる AI と「ブラックボックス」の実情(前編)-(page3)”, Charles McLellan, 9.12.2016,[オンライン].Available: <https://japan.zdnet.com/article/35093175/3/>