APIコール順序情報によるマルウェアの攻撃目的推定の研究

YAMAGUCHI, Yuka / 山口, 祐佳

(出版者 / Publisher)
法政大学大学院理工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学研究科編
(巻 / Volume)
64
(開始ページ / Start Page)
1
(終了ページ / End Page)
5
(発行年 / Year)
2023-03-24
(URL)
https://doi.org/10.15002/00026413

API コール順序情報による マルウェアの攻撃目的推定の研究

Malware Attack Objective Evaluation Based on API Calls Sequence Information

山口祐佳
Yuka YAMAGUCHI
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Cyber-attacks are increasing every year, and the scale of damage is also growing. Since malware is commonly used in cyber attacks, the number of malware detections is also on the rise. Since it is impossible to respond to malware by analyzing them one by one, many research efforts are being made to develop detection and classification methods that require as little manpower as possible. Malware analysis methods can be broadly classified into dynamic analysis and static analysis. In this study, we focus on dynamic analysis, which requires a relatively short analysis time and is suitable for processing a large number of malware compared to static analysis. We believe that if the purpose of an attack can be estimated using information on the names of API functions invoked by dynamic analysis, it can be used for damage assessment and recovery. In this study, we analyze the order information of API calls obtained from dynamic analysis to estimate the purpose of malware attacks. As a result, we show that the relationship between the order information of API calls and the attack objectives is characteristic.

***Key Words** : Malware, dynamic analysis, attack objective evaluation*

１．はじめに

サイバー攻撃は年々増加しており，被害規模も大きくなっている．また，明確な目的を持って計画的に犯行を行う場合も増えている．サイバー攻撃では目的達成のためにマルウェアが利用されることが多いため，サイバー攻撃の増加に伴ってマルウェアの検出数も増加傾向にある．キャノンマーケティングジャパン株式会社が発表しているサイバーセキュリティレポート[1]によると，ESET 製品が検出した直近 4 年間のマルウェアの検出数について，2018 年下半期と比べると近年は 2 倍近く検出されている．このように日々生成されるマルウェアを一つずつ解析していては対応が間に合わなくなるため，できる限り人手を使わずに検知や分類を行う手法の研究が多く行われている．

マルウェアの解析には大きく分けて動的解析と静的解析がある．動的解析は，マルウェアを実際に動作させて挙動から解析する手法である．一方，静的解析はマルウェアのファイルをリバースエンジニアリングして，プログラムのコードを読み解く手法である． 本研究では動的解析に着目した．静的解析と比べると解析時間が比較的短く，多くのマルウェアを処理するのに適しているためである．動的解析によって得ることができる情報のうち，呼び出された API 関数は，実際にマルウェアがどの様な動作を行おうとしたのかを知ることができる重要な情報であり，マルウェアの攻撃目的によって特徴が現れると考えられる．したがって，呼び出された API 関数名を用いて攻撃の目的を知ることができれば被害状況の調査や復旧にも活かすことができる．

本研究の目的は動的解析によって得られた API コールの順序情報からマルウェアの攻撃目的を推定することであり，そのための分析を行う．

以下，2 章では関連研究を紹介する．3 章では使用データや提案手法について述べる．4 章では実験結果と実験に対する評価を行い，5 章ではまとめと今後の課題について述べる．

２．関連研究

本章では，API コール情報を用いてマルウェアの検知・分類を行っている既存研究について述べる．また，攻撃目的の推定を行っている既存研究について述べる．

（１）API コール情報を用いたマルウェアの検知・分類

API コール情報を用いてマルウェアを検知・分類する

研究が行われている．

佐藤らは，API 呼び出しパターン，API 呼び出しによる経過時間とシステム負荷に関する特徴量を用いてマルウェアの検知を行う手法を提案した [1]．提案手法では，1 検体あたり 10 秒動作させ，その間に得られた API とそれに伴う経過時間とメモリ使用量を用いる．動的解析ログから，API 呼び出しとそれに伴う経過時間とメモリ使用量の情報を抽出し，マルウェアの特徴抽出を行い，機械学習アルゴリズムを用いてマルウェアか正規プログラムかの検知を行う．CCCDataset と正規プログラムを判別した実験と独自に収集したマルウェアと正規プログラムを判別した実験を行っており，特に CCCDataset2013 の方で高い精度の検知率となった．

前田らは，マルウェアの動的解析の結果に含まれる LdrGetProcedureAddress の呼び出しログを用いてマルウェアの分類を行う手法を提案した [2]. 機械学習アルゴリズムには，決定木学習（CART）・ランダムフォレスト・SVM・ナイーブベイズの 4 種類を用いている．実験の結果，LdrGetProcedureAddress の呼び出し記録から得られる情報を用いたマルウェアの分類は，Cuckoo Sandbox が出力する動的解析ログをそのまま用いたときの分類性能に近い性能であった．また，提案手法と他のデータを組み合わせた実験では，それぞれのデータを単体で用いた場合よりも分類精度が向上した．これらの結果から LdrGetProcedureAddress の呼び出し記録はマルウェアの分類に有用であることを示している．

佐藤らは，マルウェアが呼び出す API 群およびその引数に着目し，それらを自然言語の一連の文章のように捉えて Paragraph Vector を作成することでマルウェアが指定の亜種であるかどうかを推定する手法を提案した[3]. 3 種類の手法で実験を行なっている．手法 1 は API 名のみを抽出したもの，手法 2 は API 名・引数名・引数値を抽出したもの，手法 3 は API 名・引数値の長さを抽出したものに、それぞれ提案手法を適用したものである．提案手法により，人手によらず自動的に特徴ベクトルを作成し，マルウェアの亜種判定が可能であることと API 引数も亜種判定に有用であることを示した．

これらの関連研究では API コール情報が検知や分類に有用であることが示されている．関連研究はファミリーや亜種ごとに分類をしているのに対し，本研究が攻撃目的の観点で分類をしている．

（２）マルウェアの目的の推定

マルウェアの目的を推定する研究が行われている．

鮫島らは，攻撃の目的推定という最終目標に向けての初期検討として，トラヒックデータと API ログを用いたマルウェアの目的の分析を行っている [4]. 分析から推測できたマルウェアの感染活動による目的を，各目的毎に統計的に分析し，考察を行った．その結果，マルウェアの感染活動による目的毎に，発生する API の属性やその回数，DNS クエリ等の外部との通信の有無に，傾向があることがわかった．

森らは，マルウェアの感染活動の目的を推定する目的で，動的解析ログから特徴的な挙動を分析し，挙動の推定も行っている [5]. 分析に関しては，各ラベル毎に特徴的な挙動を調べるために，決定木を作成しその木構造の可視化を行っている．また，挙動の推定に関してはログデータからマルウェアの挙動が推測できるか確認するために評価実験を行っている． その結果，70.5%の精度で挙動推定を行うことができている．

これらの関連研究では，本研究と同様に攻撃目的の観点で分析，分類を行っている． 分析を行った研究 [4]より，分析の結果，感染活動による目的毎に，発生する API の属性やその回数，DNS クエリ等の外部との通信の有無に，傾向があることが示されている．しかし，実際に分類を行ってはいない．分類を行った研究 [5]では，動的解析ログから単語を抽出し出現頻度を算出している．本研究では，API 関数はマルウェアの挙動を直接的に表している点や，他の関連研究で API コール情報の有効性が示されている点を考慮し，API 関数名を特徴量として用いている．

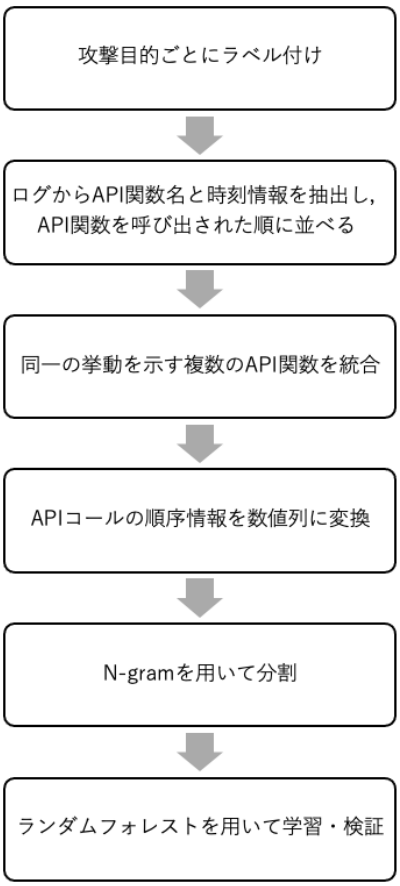

図 1　提案手法のフロー

表１　ラベル付けを行った検体数

ラベル名	検体数
ダウンロード	31
暗号化	7
マイニング	45
遠隔操作	37
広告表示	11

３．研究内容

本章では具体的な研究内容について述べる．

（１）使用データ

MWS Datasets 2019 [6]に含まれる Soliton Dataset 2019 の動的解析ログを用いた．Soliton Dataset 2019 は 2018 年 1 月から 2019 年 3 月までに話題になったマルウェアを収集しており，実行時間は 1 検体あたり 6 分を基本としている．EDR 製品である InfoTrace Mark Ⅱ for Cyber から取得したログと Cuckoo Sandbox [7]から取得したログが含まれている．本研究で使用したのは Cuckoo Sandbox から取得したログである．

（２）提案手法

提案手法のフローを図 1 に示す．まず，攻撃目的ごとに分類するためにラベル付けを行った．Soliton Dataset 2019に含まれているマルウェア一覧のリストにはハッシュ値や各セキュリティベンダが解析したマルウェア名が含まれている．これらを用いて検索し，挙動を調べることで攻撃目的を判断した．ラベル名とラベル付けを行った検体数を表 1 に示す．

Soliton Dataset 2019 の Cuckoo Sandbox から取得したログから呼び出された API 関数名と時刻情報を抜き出し，呼び出された順番に並べた．ログの一例を図 2 に示す．

次に前処理として，同一の挙動を示す複数の API 関数を 1 つに統合する．抽出した API 関数名の中には末尾を除いた名称が同一であるものが複数含まれていた．API 関数名の末尾の差異としては，A, W, Ex. ExA, ExW のいずれかが付属しているか否かである．Windows OS において, このパターンの API 関数は同一の挙動を示すか，一方の API 関数が他方の機能を内包している．よって，本実験ではそれらを 1 つに統合した．例えば，指定されたファイルまたはディレクトリの属性を取得する API 関数として，GetFileAttributesA と GetFileAttributesEx が存在するが，両者とも末尾の文字列を取り除き，GetFileAttributes として処理を行う．処理後の API コールの順序情報の関数名を対応する連番へ変換を行なった．そのようにして数値列に変換後, N-gram を用いて分割した．N-gram とは任意の文字列を連続した n 個の文字で分割するテキスト分割方法のことである．本研究では一つの API 関数を 1 文字と考え N-gram を適用した．具体


```
{
  "category": "process",
  "status": 1,
  "stacktrace": [],
  "api": "NtProtectVirtualMemory",
  "return_value": 0,
  "arguments": {
    "process_identifier": 3708,
    "stack_dep_bypass": 0,
    "stack_pivoted": 0,
    "heap_dep_bypass": 0,
    "length": 4096,
    "protection": 4,
    "process_handle": "0xffffffff",
    "base_address": "0x764a1000"
  },
  "time": 1553571043.0935,
  "tid": 2576,
  "flags": {
    "protection": "PAGE_READWRITE"
  }
},
```


図２　Soliton Dataset2019 のログの一例

表２　5 値分類の混合行列

		予測				
		A	B	C	D	E
実際	A	TA	FB_A	FC_A	FD_A	FE_A
	B	FA_B	TB	FC_B	FD_B	FE_B
	C	FA_C	FB_C	TC	FD_C	FE_C
	D	FA_D	FB_D	FC_D	TD	FE_D
	E	FA_E	FB_E	FC_E	FD_E	TE

表３　ラベル A に対する各評価指標の計算式

	計算式
正解率	$Accuracy = \frac{TA + TB + TC + TD + TE}{データ数}$
再現率	$R_A = \frac{TA}{TA + FB_A + FC_A + FD_A + FE_A}$
適合率	$P_A = \frac{TA}{TA + FA_B + FA_C + FA_D + FA_E}$
F 値	$F_A = \frac{2R_AP_A}{R_A + P_A}$

的には，3-gram，5-gram，7-gram の 3 種類で実験を行った. 分割後の数値列のうち半数は学習用, 残りの半数は検証用に無作為に分け，ランダムフォレストを用いて学習用の数値列で学習を行い，検証用の数値列でラベルの推定を行った．最後に推定を行った結果に対して評価を行った.

４．実験結果と評価

評価指標は正解率，再現率，適合率，F 値を用いる．正解率はすべての予測のうち正しく予測をすることができた割合で，再現率は実際に A ラベルの検体のうち A ラベルと予測できた割合，適合率は A ラベルと予測した検体のうち実際に A ラベルの検体の割合，F 値は再現率と適合率の調和平均である．これらの指標を用いた理由としては誤検知, 検知漏れの割合がわかりやすく, 正確さを評価することができると考えたためである．本研究のように 5 値分類の場合，各ラベルを A，B，C，D，E としたときの混合行列の値の定義を表 2 に示し，そのときのラベル A の各指標の計算式を一例として表 3 に示す.

3，5，7-gram のランダムフォレストの正解率を表 4 に示す．こちらの値は，実験を 3 回行い平均値の算出を行なっている．正解率に関しては API コールを分割する長さが長いほど高くなっている.

次に，3-gram の混合行列を表 5 に，5-gram の混合行列を表 6 に，7-gram の混合行列を表 7 に示す．これらから，ラベルごとにどのラベルに予測されやすかったのかがわかる．3-gram の場合，実際のラベルがダウンロードのものはマイニングと予測されることが一番多くなっている. 実際のラベルが暗号化のものは, 暗号化と予測されることが一番多いもののマイニングと予測されることも同程度ある結果となっている．実際のラベルがマイニング・遠隔操作のものは, それぞれ正しく予測できていることが多い．実際のラベルが広告表示のものは暗号化やマイニングと予測されることが多くなっている．全体的にマイニングと判定されることが多い結果となった．5-gram や 7-gram の場合も多少異なる部分はあるが 3-gram と似た結果となっている.

また，それぞれの混合行列から計算した再現率，適合率，F 値の値を表 8，表 9，表 10 に示す．再現率は正解があるラベルのもののうちどれだけそのラベルと予測できたかを表し，適合率はあるラベルと予測したもののうちどれだけ正解だったかを表す．F 値は再現率と適合率の調和平均である．表 7 をみると，マイニングと遠隔操作は再現率・適合率・F 値ともに比較的高い値となっている．分類に活用できる特徴が多く，API の順序情報と攻撃目的に関連があると考えられる．マイニングなどは繰り返し処理を行うため，よく特徴が現れたのではないかと考える．また, 検体数が比較的多く, 学習が十分にできていたことも関係している可能性がある. 暗号化と, 特に広告表示は再現率・適合率・F 値ともに比較的低い値となっている．API の順序情報から分類に活用できる特徴があまり得られなかったと考えられる. また, 検体数が少ないことも影響している可能性があるため，増やして検証をする必要がある. ダウンロードに関しても, 再現率・適合率・F 値ともに比較的低い値となっている. ダウンロードは他と比べて検体数が少ないわけではないため，API の順序情報からは分類に活用できる特徴があまり得られ

表 4　各分類方法の正解率

	正解率
3-gram	78.73
5-gram	79.56
7-gram	79.89

表 5　3-gram の混合行列

		予測				
		ダウンロード	暗号化	マイニング	遠隔操作	広告表示
実際	ダウンロード	41342	14894	126875	18684	704
	暗号化	22484	264513	214088	75857	20494
	マイニング	1764	108076	2123011	30398	6530
	遠隔操作	23797	131382	85582	1071818	1263
	広告表示	3350	30708	26544	2688	410

表 6　5-gram の混合行列

		予測				
		ダウンロード	暗号化	マイニング	遠隔操作	広告表示
実際	ダウンロード	38460	11557	124720	27084	648
	暗号化	23112	224559	251659	76730	21370
	マイニング	3159	46453	2191986	24304	3833
	遠隔操作	27758	120235	82114	1082585	1114
	広告表示	5951	30065	24086	3025	563

表 7　7-gram の混合行列

		予測				
		ダウンロード	暗号化	マイニング	遠隔操作	広告表示
実際	ダウンロード	31100	21293	122887	26517	642
	暗号化	27756	227315	241350	89888	11115
	マイニング	3811	39245	2200649	23255	2731
	遠隔操作	30468	110791	78911	1092573	1027
	広告表示	9877	28971	22265	1930	637

表 8　3-gram の結果（単位：%）

	再現率	適合率	F 値
ダウンロード	20.42	44.57	28.01
暗号化	44.27	48.13	46.12
マイニング	93.53	82.41	87.62
遠隔操作	81.58	89.36	85.29
広告表示	0.6436	1.395	0.8808

表 9　5-gram の結果（単位：%）

	再現率	適合率	F 値
ダウンロード	19.00	39.07	25.56
暗号化	37.59	51.88	43.59
マイニング	96.57	81.96	88.66
遠隔操作	82.40	89.20	85.66
広告表示	0.8840	2.045	1.234

表 10　7-gram の結果（単位：%）

	再現率	適合率	F 値
ダウンロード	15.36	30.19	20.36
暗号化	38.05	53.16	44.35
マイニング	96.96	82.54	89.17
遠隔操作	83.16	88.53	85.76
広告表示	1.000	3.944	1.596

なかったと考えられる．他のラベルとの差がどのような部分に現れるのかを調査し特徴量を検討する必要がある．

また，API コールの分割方法の観点で結果を考察する．分類の精度が比較的高いマイニングと遠隔操作は API コールの分割方法が長いほど F 値が高くなっており，API コール列が長いほど他のラベルと分類に活用できる特徴が得られやすかったと考えられる．ダウンロードは分割方法が長いほど F 値が低くなっている．この結果から，特徴的な挙動は 3 連鎖以下の API コール列から得られ，長くしても精度は向上しないことが推測できる．暗号化は API コールを分割する長さによる影響は見られなかった．広告表示に関しては分割方法が長いほど F 値が高くなっていることから，特徴的な挙動を示す API コール列が長い傾向にあると考えられる．

より精度をあげるための方法を考察する．一つの処理が完了する API コール列の長さを調べ，N-gram に適用することで，より正確に特徴を捉えることができると考える．また，本研究では処理速度の関係でランダムフォレストを用いたが，他の機械学習で分類する実験を試し最適な方法を探ることも必要である．

５．まとめ

本研究では，マルウェアの攻撃目的の推定を行うため，API コールの順序データを用いて目的ごとに分類を行った．実験の結果，API コールの順序情報と攻撃目的の関係に特徴が見られた．本研究で提案した手法が有効であるラベルと不十分な精度となるラベルが存在している．具体的には，マイニングや遠隔操作には有効な手法であり，ダウンロードや広告表示では良い値が得られなかった．繰り返し同じ処理を行うようなラベルには有効な手法であると考えられる．

今後の課題として，まず検体数を十分に増やす必要があると考えている．機械学習では一般的に検体数を増やすことで十分な学習を行うことができ精度が向上する可能性がある．特に暗号化と広告表示の結果関しては検体数が少ないことも影響している可能性があるため，増やして再度検証を行う必要がある．また，今回は処理速度の関係でランダムフォレストを用いたが，今後は他の方法で分類する実験を行い最適な方法を探っていく予定である．さらに，分割した API コール列で評価を行うだけでなく，検体ごとに一番割合が多いラベルを予測値として正しく分類できたのかも確認することも，本手法が有効であるかを評価する上でひとつの基準になると考えている．

謝辞：本研究を進めるにあたり，ご指導して頂いた指導教員の金井敦教授に感謝致します．また，助教の呉謙先生，ご協力頂いた皆様，研究室の方々に厚く感謝を申し上げます．

参考文献

1) キャノンマーケティングジャパン株式会社．“サイバーセキュリティレポート 2022 上半期”．https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/CybersecurityReport_2022FirstHalf.pdf（参照：2023/2/7）
2) 佐藤 順子，花田 真樹，面 和成，山口 崇志，鈴木 英男，布広 永示，折田 彰，関口 竜也“API 呼び出しとそれに伴う経過時間とシステム負荷を用いたマルウェア検知手法，” Computer Security Symposium 2017
3) 前田 優人，大山 恵弘“動的な関数アドレス解決 API の呼び出しログを用いたマルウェア分類，” Computer Security Symposium 2018
4) 佐藤 拓未，後藤 滋樹，武部 嵩礼，“Paragraph Vector を用いたマルウェアの亜種推定法，” Computer Security Symposium 2016
5) 鮫島 礼佳，村上 純一，吉浦 裕，市野 将嗣，“マルウェアによる感染活動の目的推定のためのトラヒックデータと API ログに基づく分析，” Computer Security Symposium 2016
6) 森 優輝，金居 良治，吉浦 裕，市野 将嗣，“マルウェアによる感染活動の目的推定に向けた動的解析ログに基づく分析，” Computer Security Symposium 2018
7) 荒木 粧子，笠間 貴弘，押場 博光，畑田 充弘，寺田 真敏，“マルウェア対策のための研究用データセット ~MWS Datasets 2019~，” 情報処理学会研究報告
8) “Cuckoo Sandbox – Automated Malware Analysis”．https://cuckoosandbox.org (参照：2023/2/7)