動的解析時の画面から取得可能な情報の調査と応用可能性の検討

塙 剛生[1,a)]　山岸 伶[1]　藤井 翔太[1]

概要：マルウェアを実行し，挙動を分析する動的解析では，画面キャプチャを用いることで解析環境に表示される画面（解析画面）を取得できる．解析画面から起動されたアプリケーションやユーザを欺く手口等のマルウェアの挙動に関する情報が取得可能なため，解析の効率化に寄与する動的解析システムの拡張やユーザのセキュリティ意識の向上に寄与する教育に解析画面を応用できる可能性がある．一方で，解析画面から取得可能な情報について体系的な調査が実施されておらず，解析画面の応用可能性が具体的に示されていない．そこで本研究では，解析画面から取得可能な情報の整理を目的として，合計 93 ファミリを対象とした 213 件のレポートに含まれる 3,598 枚の解析画面について質的コーディングによる調査を実施した．調査の結果，解析画面から取得できるマルウェアの情報およびユーザ欺瞞の工夫点を明らかにした．また，従来のログと比較して，解析画面から容易に取得できる情報があることを明らかにし，解析画面の応用可能性について検討した．これらの本研究の成果は，今後の動的解析に関わるシステム開発の検討やユーザに対する教育指針の検討の一助になるものと考えられる．

Survey of Obtained Information from Screens during Dynamic Malware Analysis and Consideration of Potential Applications

Goki Hanawa[1,a)]　Rei Yamagishi[1]　Shota Fujii[1]

Abstract: In dynamic malware analysis, screen captures are used to obtain the display of the analysis environment (analysis screen). Since it is expected that information about malware behavior can be obtained from these analysis screens, there is potential for these screens to be used to enhance dynamic malware analysis systems, aimed at sophistication of analysis. However, no research has been conducted on the information that can be extracted from analysis screens, and the applicability of these screens has not been concretely demonstrated. In this study, we conducted a qualitative coding analysis of 3,598 analysis screens with the aim of organizing the information that can be obtained from analysis screens. As a result of this research, we organized the information extractable from the analysis screens and discussed their applicability.

1. はじめに

サイバー攻撃の増加に伴い，攻撃に用いられるマルウェアの数や種類も増加傾向にある [1]．こうした状況下において，マルウェアを解析し，適した対策を講じることがより重要とされる．マルウェア解析手法には，ファイル名や種別といった簡易的な情報を分析する表層解析，マルウェアを実行してその挙動を分析する動的解析，マルウェアのコードやアセンブリ言語を分析する静的解析がある．中でも，動的解析は多くのマルウェア解析者の解析プロセスにおいて，広く活用されている事が知られている [2]．

動的解析では，画面キャプチャを用いることで解析環境に表示されている画面（以降，解析画面）を取得できる．解析画面にはマルウェアの挙動に関する多用な情報が含まれていることから，様々な応用可能性が考えられる．例えば，起動されるアプリケーションや表示されるダイアログといったマルウェアの挙動に関する情報が含まれている．これらの情報を応用し，解析画面の情報を活用してランサムウェアの検出・識別を図る研究 [3] やスクリーンショッ

[1] 株式会社日立製作所 Hitachi, Ltd.
[a)] goki.hanawa.rc@hitachi.com

トを活用して Android マルウェアの検知精度を向上する研究 [4] が存在する．また，解析画面からはユーザの行動を引き起こすための攻撃者側の工夫点に関する情報も取得可能なため，攻撃者の手口の解明やユーザの教育への応用が期待される．

一方で，我々の知る限りでは，解析画面から取得可能な情報について体系的な調査は実施されておらず，解析画面の応用可能性が具体的に示されていない．調査によって解析画面から得られる情報を明らかにし，解析画面の応用可能性について整理することは，今後の動的解析システムの開発やユーザおよび解析者に対する教育の検討の一助になるものと考えられる．

そこで本研究では，解析画面から取得可能な情報の整理を目的として，解析画面の調査を実施した．また，ログから取得可能な情報との比較やユーザを欺くための工夫点についての分析を実施し，解析画面の応用可能性について整理した．

本稿における主要な貢献は以下の通りである．

- 93 ファミリを対象とした 213 件のレポートに含まれる 3,598 枚の解析画面の調査を実施し，解析画面から取得可能な情報を抽出・整理した．
- ログから取得可能な情報と比較することで，解析画面でのみ取得できた情報を明らかにし，解析の効率化や解析結果のカバレッジ向上に寄与する動的解析システムの機能拡張といった応用可能性を示した．
- 解析画面を分析し，攻撃を成功させるための攻撃者側の工夫を明らかにした．また，この結果を基に，エンドユーザの被害を抑制するための教育的対策を提言事項として示した．
- 解析画面から解析者の苦戦する様子が確認されたことに着目し，解析者のインシデント対応力向上に係る教育について提言事項を示した．

2. 研究背景

2.1 マルウェアの動的解析

マルウェアの動的解析では，解析環境内でマルウェアを動作させ，挙動を観測するため，安全かつ隔離された解析環境が必要とされる．解析環境は，解析者自身が用意する場合やインターネット経由でアクセス可能な解析環境であるオンラインサンドボックスを利用する場合がある [2]．オンラインサンドボックスの例としては，ANY.RUN [5] や Joe Sandbox [6]，Triage [7] などが挙げられる．これらでは，解析中に観測されたファイル操作やネットワーク通信，解析画面などの情報がレポートとしてまとめられており，一般に公開されている．

2.2 関連研究

関連研究として，解析画面をマルウェアの解析に応用した研究が挙げられる．Anderson らは，スパムメールを利用したインターネット詐欺のホスティングインフラストラクチャを解析するために解析画面を用いている [8]．スパムメールのリンク先の Web サイトが表示された解析画像を基に詐欺サイトの視覚的な類似性を算出し，詐欺サイトの識別や分類を効率化している．Chris らは，Exploit as a Service（EaaS）の傾向を調査するために解析画面を用いている [9]．具体的には，エクスプロイトキットからインストールされた偽のアンチウィルスソフト（偽 AV）が表示された解析画面を基に偽 AV の視覚的な類似性を算出し，エクスプロイトキットをクラスタリングしている．Dietrich らも，偽 AV やランサムウェア等の視覚的インターフェースを有するマルウェアについて，解析画面を基にクラスタリングして分類・分析している [10]．Kharaz らは，ランサムウェアの挙動を追跡した解析画面を基にデスクトップの視覚的な類似性を算出し，ランサムウェアの検知や識別に活用している [3]．また，Tan らは，ユーザインタフェース（UI）のスクリーンショットを活用することによって，Android マルウェアの検知精度向上を図っている [4]．

また，サイバー攻撃における視覚面での分析を行っている研究もある．Miramirkhani らは，テクニカルサポート詐欺において，偽のブルースクリーンを表示して危機感を煽ることやテクニカルサポートに電話するよう求めるアラートボックスを常に表示することにより，攻撃への誘導を行っていることを明らかにしている [11]．また，偽 AV を用いた攻撃においても，偽の感染アラートやユーザの危機感・心理的不安をあおる文言等によって，攻撃への誘導が行われていることが示されている [12], [13]．

マルウェア解析に係る関連研究は，いずれも解析画面の視覚的な類似性に注目したものであり，解析画面から取得可能な情報やその応用可能性について体系的には示されていない．また，視覚面の分析においても，テクニカルサポートや偽 AV には焦点が当たっているものの，マルウェア全般について体系的に整理されている研究は，我々の知る範囲では存在しない．マルウェア解析システムへの応用に係る検討，攻撃者の手口の整理や対策，およびエンドユーザの教育への活用のために，解析画面から取得可能な情報を整理する必要がある．

2.3 研究課題

以上の背景をふまえ，本研究では，3 つの研究課題（以降，RQ）を設定した．

RQ1. **解析画面からどのような情報が取得できるか**

RQ2. **解析画面とログの間で取得可能な情報にどのような差異があるか**

RQ3. **ユーザの行動を引き起こすためにどのような工夫をしているか**

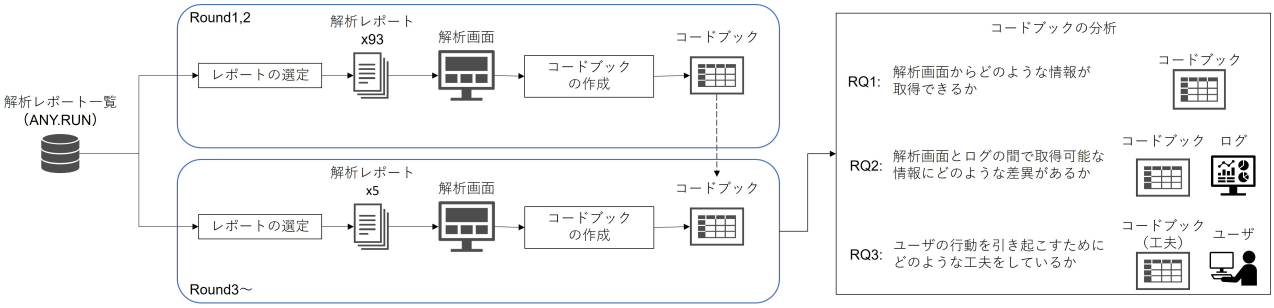

図 1　調査の全体像

表 1　調査対象とするファミリの一覧

adwind	agenttesla	amadey	arkei	asyncrat	azorult
blank grabber	cobalt strike	crimson rat	cryptbot	danabot	darkcloud
darkcomet	darkgate	darkside	dbatloader	dcrat	dharma
dridex	emotet	exela stealer	fabookie	fickerstealer	flawedammyy
formbook	gafgyt	gandcrab	gclaener	gh0strat	glupteba
gootkit	guloader	hancitor	hawkeye	hijackloader	icedid
kraken	laplas clipper	latrodectus	limerat	lockbit	loda
lokibot	losttrust	lu0bot	lumma	mars stealer	maze
medusa	metamorfo	mirai	nanocore	nemty	netwalker
netwire	njrat	orcusrat	parallax rat	phobos	phorpiex
pikabot	plugx	pony	predator the thief	privateloader	purelogs
qbot	quasarrat	raccoon	rasberry robin	redline	remcos
revenge	revil	rhadamanthys	risepro	ryuk	smokeloader
snake	socks5systemz	stealc	strat	systembc	trickbot
troldesh	ursnif	vidar	wannacry	warzone	wshrat
xeno rat	xworm	zloader			

3.　調査手法

3.1　調査方針

本研究では RQ を解明するため，オープンコーディング [14] による調査を実施した．オープンコーディングとは，質的データ分析の一手法であり，データを細かい単位に分割し，それぞれにラベル（コード）を付けることでデータ内の傾向を抽出する手法である．本研究では，オンラインサンドボックスの解析レポートに画像として含まれている解析画面を調査対象とし，オープンコーディングを実施した．オンラインサンドボックスには，動的解析のレポートに解析画面を含む ANY.RUN を選定した．また，ANY.RUN は解析中にインタラクティブに操作できる関係上，解析者の操作も解析画面に含まれる．今回の調査では，解析者の操作も調査対象ならびにオープンコーディングの対象に含むこととした．また，調査の網羅性を確保するために，種々のマルウェアファミリを調査対象とした．具体的には，2024 年 7 月 14 日の ANY.RUN 上のトレンドレポート [15] に記載された全 93 ファミリの解析画面を調査対象とした．今回調査対象とした 93 ファミリの一覧は，表 1 の通りである．

3.2　調査手順

調査手順を図 1 に示す．以降の各項では，調査の各手順（レポートの選定，コードブック（コードの一覧表）の作成，および分析）について詳述する．

3.2.1　レポートの選定

今回活用した ANY.RUN には，マルウェアだけでなく URL を起点とした解析レポートも含まれている．本研究はマルウェアを対象としているため，検索条件として「Runtype: File」と指定し，URL を除外してマルウェアの解析レポートのみを抽出した．また，ANY.RUN には解析画面が 1 枚しか掲載されていないレポートや解析途中で公開されているレポートが複数存在した．これらのレポートは RQ の解明に適さないと判断し，本研究では調査対象から除外した．具体的には，解析画像が 2 枚以上含まれるレポートを調査対象とすると共に，ANY.RUN によってその挙動が悪性と判定されているもの（Verdict: Malicious）を調査対象とした．また，前述の通り 93 ファミリを調査するため，ファミリ名を Tag に指定して検索を行った．ただし，一つのレポートに複数のファミリに関するラベルが付与されている場合が散見された．このため，レポートの重複を抑制するために，検索期間をランダムに設定し，その中での最新のレポートを調査対象とした．重複が見られた場合は人手で除外し，次点のレポートを選定した．

以上の方針を反映した検索条件は以下の通りである．

検索条件

- Runtype: File
- Verdict: Malicious
- Tag: 調査対象内のファミリ名
- Date To: 2021/07/01 から 2024/06/31 の期間内でランダムに選択された日程

3.2.2　コードブックの作成

本研究では，3.2.1 節のレポート選定に基づいて解析画面を決定し（調査対象の決定），著者らが独立して解析画面の取得可能な各情報にラベル（コード）を付けそれらのコードを分類し（コーディング），著者間で当該ラベルの妥当性に関して議論する（レビュー）一連のラウンドを繰り返す．当該ラウンドを繰り返す中で，理論的飽和 [14] の概念に従い，新たなコードが発見されなくなった場合，取得したコードが飽和し取得可能な情報を網羅的に集められたとみなし，その時点のコードで最終的なコードブックを作成する．以降では，ラウンド全体の流れについて説明し，次

にラウンド中のコーディング，レビューに関する注意事項を補足する．

ラウンドは，Round1,2 と Round3 以降で大別される．Round1,2 では，初期段階であるため，それぞれ 93 ファミリの各ファミリから 1 件ずつ合計 93 件のレポートを選定しコーディングを実施した．Round3 以降では，93 ファミリの中からランダムに 5 つのファミリを選択し，合計 5 件のレポートを対象とした．なお，分割しラウンドを複数回実施する理由は，ユーザブルセキュリティ分野の質的研究を分析した研究 [16] において，反復的な著者間の議論（レビュー）の重要性について言及されていたためである．

コーディングの段階では，主著者と第二著者の 2 名で独立して解析画面を確認し，その中の取得可能な情報にラベル付けを実施した．なお，主著者はマルウェア解析に関する研究およびコーディングの経験がなかったが，第二著者は 5 年間のマルウェア解析に関する研究への従事および 5 回のコーディングの経験を有した．また，コーディングの際に，事前に以下のコーディングの方針・留意事項を定め，著者間でコーディングの観点が一致するよう努めた．レビューの段階では，それぞれの著者がコーディングし，作成した仮のコードブックを持ち寄り，内容について議論を重ね，共通認識を取った暫定版のコードブックを作成した．著者らは当該コードブックを参考に，次のラウンドでのコーディングを実施した．

コーディングの方針と留意事項

- 時系列順に解析画面を 1 枚ずつ確認する．
- 直前の解析画面との差分に着目してコードを記載する．
- 何が変化したか，どう変化したかの 2 段階に分けてコードを記載する．
- 特徴的な見た目や文言についてコードを記載する．
- 事前にログや通信先などの情報は確認しない．
- 画像間の動作は想像せず，画像から取得できる情報のみを記載する．

3.2.3 コードブックの分析

作成した最終的なコードブックを分析し，RQ に対する回答を得る．RQ1 に関しては，コードブックのコードとその分類を分析することで，解析画面から取得可能な情報の傾向を明らかにする．RQ2 に関しては，コードと ANY.RUN のレポート内に掲載されるファイル情報，プロセスや通信先などのログの情報を比較することで，解析画面とログから取得可能な情報の差異を明示する．RQ3 に関しては，ユーザの行動に関与するコードに着目し，その傾向を分析することで攻撃者が講じる工夫点を示す．

4. 調査結果

4.1 RQ1. 解析画面からどのような情報が取得できるか

表 2 に作成したコードブックの一部を示す．最終的なコードブックは，新たなコードが発見されなくなった Round7 のコーディング終了時点のものである．コードブックでは，アプリケーションやシステムの動作に関わる情報を “画面の変化”，攻撃者による工夫点と推察される情報を “工夫” として大別し，抽出されたコードを階層的に分類している．例えば，Winrar アプリケーションの起動が解析画面で確認された場合，大カテゴリ “画面の変化”，中カテゴリ “アプリケーション”，カテゴリ “Winrar” のコード “起動” とした．なお，表 2 では，スペースの都合上，各カテゴリの代表的なコードのみ記載する．

大カテゴリ: 画面の変化.

“画面の変化” としては，3 つの中カテゴリが抽出された．

中カテゴリ “アプリケーション” として，解析中にマルウェアが起動したアプリケーションが抽出された．具体的には，マルウェアの起点となるマクロが実行される Office ソフトの起動，PowerShell や Command Prompt を介したコード実行等が確認できた．なお，前述の通り，ANY.RUN はその性質上解析者の操作を含む．このため，解析者の作業に起因するもの，例えば手動でのブラウザの起動や手動でのフォルダ操作等も含まれることに留意されたい．

中カテゴリ “Windows システム” としては，主に Windows が備える各種機能に関連する画面の変化を抽出した．中でも，コード数が最も多いカテゴリは “ダイアログ” であり，種々のアプリケーションに起因するダイアログが確認された．ダイアログについては，後段で別途詳述する．

大カテゴリ: 工夫. “工夫” には，攻撃者が攻撃を成功させるために具備したと推察されるものに係る画面変化を中心に分類した．

“工夫” において多くのコード数が確認されたカテゴリは，Word や Excel であった．Word や Excel で開いたファイルには，“Enable Editor” と記載されたボタンのクリックを促す多様な文言や図が散見された．これらは，ファイル保護機能をバイパスしてマクロを実行させるための工夫と推察される．

“工夫” のコードは，テキストに関する工夫（65.72%）と，グラフィカルな工夫（34.28%）に大別できた．テキストに関する工夫では，ランサムウェアの脅迫文中でユーザに支払いを促すための文言や “click” や “download” のようなユーザにマルウェアの実行を誘発するような文言が確認できた．グラフィカルな工夫では，著名なサービスを偽装する目的と推察される Windows や Intel のマークや，恐怖感をあおる目的と推察される錠や神の画像が確認できた．テキストとグラフィカルな工夫の割合は偏っておらず，攻撃者は多様な工夫を講じているといえる．

カテゴリ: ダイアログ.

ダイアログとして最も多く見られたものの一つに，ファイルの実行エラーに関するものが挙げられる．具体的には，“Dll not found” や “[ファイル名] has stopped working” のようなダイアログであり，これらは検体の実行に必要な環

表 2 コードブックの一部

大カテゴリ	中カテゴリ	カテゴリ	コード数	代表的なコード（レポート数）
画面の変化	アプリケーション	Winrar	12	起動 (71)，解凍パスワード入力 (37)，ファイル解凍 (17)，ダイアログ (8)，Rename(2)
		Explorer	31	起動 (42)，Libraries(27)，C ドライブ (20)，Admin(13)，Downloads(6)，ダイアログ (4)
		Word	6	起動 (23)，ダイアログ (8)，マクロ起動 (2)，ファイル保存 (1)，新規ファイル作成 (1)
		Excel	3	起動 (6)，ダイアログ (2)，マクロ起動 (1)
		OneNote	1	起動 (1)
		Notepad	3	起動 (20)，ファイル保存 (1)，新規ファイル作成 (1)
		Outlook	4	起動 (5)，ダイアログ (1)，送信者の情報確認 (1)，保存 (1)
		Adobe Acrobat Reader	2	起動 (4)，ダイアログ (1)
		Microsoft Edge	10	起動 (7)，ファイルダウンロード (2)，特定の URL へのアクセス (2)，403 forbidden(1)，検索 (1)
		Google Chrome	11	起動 (16)，検索 (7)，404 not found (5)，Gmail アカウントのログイン (1)，CAPCHA 認証 (1)
		Firefox	5	起動 (4)，検索 (2)，CAPCHA 認証 (1)，特定の URL へのアクセス (1)，ファイルダウンロード (1)
		Internet Explorer	8	起動 (5)，検索 (5)，特定の URL へのアクセス (3)，Can't be displayed(2)，Cannot found(2)
		Visual Basic	2	起動 (1)，コードの確認 (1)
		PowerShell	2	起動 (8)，ファイルの実行 (3)
		Command Prompt	2	起動 (7)，コマンドの実行 (2)
		Windows Photo Viewer	1	起動 (8)，ダイアログ (2)
		PoweShell ISE	1	起動 (1)
		Windows Script Host	1	起動 (1)
		Skype	1	起動 (2)
		Broom Cleaner	1	起動 (6)
		Paint	1	起動 (1)
		Windows Media Player	1	起動 (2)
		VLC Media Player	1	起動 (1)
		未知のアプリケーション	5	起動 (13)，インストール (6)，セットアップ (5)，ファイル保存 (1)，ファイル作成 (1)
	Windows システム	ダイアログ	64	ファイル名 has stopped working(41)，User Access Control(8)，Can't open(8)
		Task Manager	7	Processes(14)，Performance(7)，Services(5)，プロセス終了 (3)，Applications(1)，Users(1)
		Property	17	General(4)，Digitalsignatures(2)，Security(2)，Compatibility(1)，Previous version(1)
		Control Panel	2	Screeen resolution(1)，Personalization(1)
		Setting	2	Optional features(1)，Region and language(1)
	その他	Desktop	7	ファイル作成 (20)，ファイルアイコン変更 (19)，背景変更 (8)，ファイル削除 (4)，ファルダ作成 (2)
		電源	2	再起動 (5)，シャットダウン (2)
		Screenshot	1	スクリーンショット取得 (1)
工夫	アプリケーション	Winrar	1	文字化け (1)
		Word	19	単語の羅列 (9)，クリック推奨 (8)，"protected"(4)，錠マーク (2)，英語以外の言語 (1)
		Excel	12	クリック推奨 (5)，ぼかし (3)，錠マーク (2)，"protected"(2)，英語以外の言語 (2)
		Notepad	5	文字化け (1)，英語以外の言語 (1)，ソースコード (1)，ソフトウェアの説明 (1)
		Adobe Acrobat Reader	8	"protected"(1)，"click"(1)，"download"(1)，pdf アイコン (1)，黒背景 (1)，パスワード (1)
		Outlook	4	英語以外の言語 (1)，"urgent"(1)，アクセスキー (1)，リンク (1)
		Microsoft Edge	5	英語以外の言語 (1)，Word マーク (1)，クラウドビューへ誘導 (1)，双頭の鷲マーク (1)
		Google Chrome	2	URL 記載 (2)，"contact"(1)
		Internet Explorer	1	"Anonymous Proxy detected, click here"(2)
		Command Prompt	1	難読化 (1)
		Windows Photo Viewer	3	ファイル名表示 (6)，連絡先 (1)，英語以外の言語 (1)
		未知のアプリケーション	1	独自の UI(6)，UI なし（黒背景）(5)
	Windows システム	ダイアログ	5	英語以外の言語 (3)，意味のない文字列 (1)，文字化け (1)，赤× (1)，空欄 (1)
	Ransomware	デスクトップ背景画像	8	黒背景 (8)，ノイズ (4)，赤字 (4)，緑字 (3)，赤背景 (2)，青背景 (1)，縦線模様 (1)，黄字 (1)
		ファイルアイコン	2	白アイコン (14)，独自アイコン (2)
		マーク	4	錠 (4)，カウントダウンタイマー (3)，Bitcoin(2)，神 (1)
		文言	6	"encrypted"(20)，連絡先 (6)，"contact"(6)，"attention"(4)，口座番号 (2)，英語以外の言語 (1)
		内容	10	一部無料で復号 (12)，時間制限 (7)，暗号アルゴリズム (4)，拡張子の説明 (4)，復号の実績 (2)
		その他	2	独自アプリケーションの起動 (4)，ファイル名の変更 (2)
	その他	検体名	6	業務関係ファイル名 (23)，英語以外の言語 (5)，既存のサービス名 (4)，不正ツール名 (4)

境・ツールの不備を示唆している．本ダイアログの内容を活用することにより，解析環境由来で実行に失敗した検体の環境更新・再解析に必要な情報を機械的に導出できる可能性がある．実際に，本ダイアログの確認後，一部の解析者はブラウザを通して実行に必要だと思われるファイルの追加ダウンロードを試みていた．

また，"[ファイル名] has stopped working" のような，実行中の検体の途中終了あるいは完了を示唆するダイアログも散見された．同じ情報を活用することにより，検体の主たる動作箇所を推定し，全体のうち注力して分析すべき部分を推量できる可能性がある．或いは，検体の動作状況を見極め，検体の動作終了に併せて解析を終了することで，解析に利用する計算機やログを格納するストレージ等のリソースを最適化できる可能性がある．実際に，本ダイアログの確認後，一部の解析者は Task Manager を開き，プロセスの起動状況を通して検体の動作状態を確認していた．

また，マルウェア独自のダイアログとして，ユーザを欺瞞するための偽装メッセージや不安を煽るエラーメッセージが確認できた．これらのメッセージは，攻撃者にとって有利な操作をユーザに促すためと考えられる．これらはマルウェア特有のものであるため，マルウェアの検知や分類に活用できる可能性がある．

カテゴリ: 未知のアプリケーション.

マルウェア特有のアプリケーションやアプリケーション名で検索しヒットしなかったものについては，カテゴリ "未知のアプリケーション" とした．中でも，図 2 に示したような独自の UI を持つアプリケーションは，特徴，動作，および機能を解析画面から推察できた．

例えば（a）は，上段の「Arkei Stealer」からそのファミリ名が，また「Crack」というテキストから具備する機能が推察できる．また（b）は，イタリア語のメニュー項目が確認できることから，攻撃者はイタリア語を可読し，データ管理やファイル操作，設定変更などの操作を行うと推察される．このように，UI を有するマルウェアについては，

(a) (b)

図 2 未知のアプリケーションの UI 例

解析画面の情報が各種機能の推定や検知・分類に活用できる可能性がある．

まとめ．コードの分析を通して，マルウェアの実行に起因する画面の変化を抽出し，カテゴリに分類した．また，マルウェア解析の高度化や効率化に寄与し得る解析画面の情報について検討し，整理した．

4.2 RQ2. 解析画面とログの間で取得可能な情報にどのような差異があるか

本節では，コーディングの結果を基に，従前のログベースの分析に加えて解析画面から得られる情報がどのように解析へ活用出来るか検討する．

まず，解析画面のみでは全ての情報を取得することはできないため，解析画面だけでなくログベースの分析との組み合わせが必要であると考えられる．例えば，バックグラウンドで実行されるプロセスや各種処理は画面には情報として出現しないため，取得できない．ただし，これらの情報は，ANY.RUN を含む動的解析システムに典型的に含まれる各種ログ，具体的にはプロセスログや通信ログ等から取得できる．

他方で，解析画面に有意性がある情報も幾つか確認できた．例えば，ダイアログに含まれる情報は，先述の通り解析の高度化・効率化に寄与する可能性がある．具体的には，未知のアプリケーションのダイアログからは，当該アプリケーションの機能や攻撃者が利用すると思われる言語を推測できる事が確認できた．また，UAC に代表されるユーザに向けたダイアログでは，ユーザへの操作要求やその一つとしての権限昇格要求の可能性などが把握できる．これらの情報は，ダイアログボックスを表示するを WindowAPI の引数等からも取得できるため，解析画面のみから取得できるものではない．ただし，解析画面では視覚的な情報として即応的に取得・確認が可能なことから，大量のログから上述の情報を抽出する事に対しての優位性があると推察される．

加えて，先述の通り，検体の動作失敗や動作完了に係る情報も解析画面から取得可能である．これらの情報を活用して動作失敗の理由や動作完了の時間を推定することで，ログのうち注力して確認するべき情報や検証するべき箇所を抽出し，ログのみを用いる場合よりも効率的に解析を遂行できる可能性がある．

また，各種 Office アプリケーション等に含まれる画像やランサムウェア等の画面に影響を及ぼす検体のデスクトップ背景画像，および未知のものを含む各種アプリケーションの UI に関する情報である．後述の通り，Office アプリケーション等に含まれる画像にはユーザの行動を誘導するような情報も含まれている場合があり，攻撃者の TTPs を把握するうえで重要な情報の一つであると言える．他の画像についても，同じく後述の通り攻撃者の手口や検体ごとの特徴が見られたことから，TTPs の把握に加えて検体の分類・分析に活用できる可能性があると言える．特に，図 2 で部分的に示した通り，既存研究で焦点を当てられている偽 AV やランサムウェアに限らず，視覚的な特徴を有するマルウェアは存在するため，マルウェア全般の検知・分類に UI をはじめとした画像情報が寄与できる可能性がある．上述の情報は，いずれもログからは取得することが難しいものである．

まとめ．コーディングの結果を基に，従前のログベースの分析に加えて解析画面から得られる情報がどのように解析へ活用出来るか検討した．具体的には，解析画面のダイアログの情報を用いることで，ログのみを用いる場合よりも効率的に解析出来る可能性を示した．また，画像情報をはじめとした解析画面のみで取得できる情報が存在すること，および同情報を活用することによって解析の高度化・効率化の可能性があることを示した．

4.3 RQ3. ユーザの行動を引き起こすためにどのような工夫をしているか

コードブックの “工夫” に基づいて，ユーザの行動を引き起こすために攻撃者が講じる工夫について分析した．

クリックを誘導する工夫．クリックを誘導する工夫例を図 3 に示す．図 3 における（a）・（b）は Word から，（c）・（d）は Excel から確認された工夫である．（a）では，公式の Microsoft Office のロゴや錠のアイコンを使用することで，ユーザの警戒心を低減させ，指示に従わせやすくする効果があると推察される．（b）では，人間による操作を確認するメッセージにより，ユーザに即座の行動を促していると推察される．（c）では，警告バーの右側に「Enable Content」というボタンがあり，その横に赤い矢印が描かれていることで，視覚的にクリックを促進し，ユーザが次に行うべき操作を明確に示している．また，ビジネス関連のファイル名にすることで，重要なファイルと誤認させ，ユーザに迅速な対応を求める心理的圧力をかける効果があると推察される．（d）では，英語とスペイン語の両方を使用することで，広範なユーザ層にアプローチしていることが確認できる．

ランサムウェアの脅迫文の工夫．ランサムウェアの脅迫文の工夫例を図 4 に示す．これらの工夫には，フィッシング

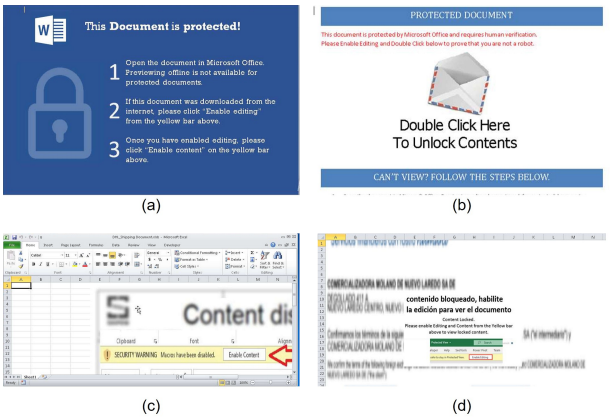

図 3　クリックを誘導する工夫例

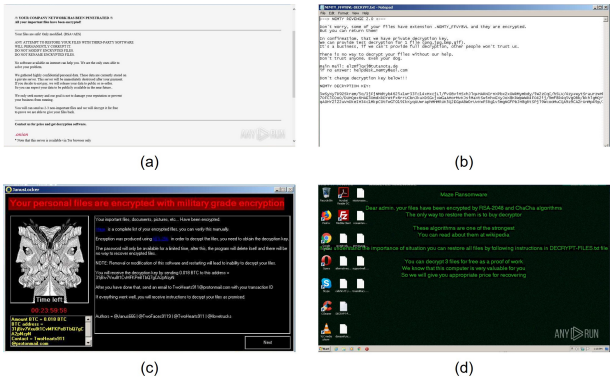

図 4　ランサムウェアにおける脅迫文の工夫例

メールにおける工夫 [17] と同様に，ユーザの行動や意思決定に与える影響を示したチャルディーニの心理的原則 [18] との関連性が見られる．チャルディーニの心理的原則は，心理学者であるチャルディーニが提唱した原則であり，返報性，一貫性，社会的証明，好意，権威，希少性で構成される．図 4 における（a）・（b）・（d）では，一部のファイルを無料で復号できる旨が記載されており，ユーザに恩を感じさせ，支払いへの返報行動を促すためと推察される．これは，返報性の原則に当てはまる．また，復号の証拠を提供することで，他のユーザも支払いによって復号できたと認識させ，行動の正当性を被害者に感じさせる効果があると推察される．これは，社会的証明の原則に当てはまる．（d）の「RSA-2048 and ChaCha algorithms」のような暗号アルゴリズムや （b） の「NEMTY」のようなファミリ名は，強力な技術力を示すためと推察される．これは，権威の原則に当てはまる．さらに，（c）のカウントダウンタイマーは，「限られた時間内に支払いを行わないとデータが永久に失われる」といった心理的圧力をかける効果があると推察される．これは，希少性の原則に当てはまる．

言語の工夫．検体のファイル名や，Word・Excel のテキスト内に英語以外の言語が確認された．英語以外の言語を用いる理由としてユーザの誤認を誘発するためだと考えられる．例えば，ターゲットの地域や文化に合わせた言語を使用することで，ユーザが正規のファイルと誤認しやすくし，攻撃成功率を高める意図が伺える．また，ユーザがその言語に精通していない場合，マルウェアの意図や機能を正確に把握するのが難しくなり，攻撃者にとって有利に働くと考えられる．

まとめ．攻撃者はテキストに関する工夫とグラフィカルな工夫を組み合わせていることが確認できた．テキストやアイコン，マークを用いて，ユーザの心理を利用し，ユーザに即座の行動を促すような工夫が散見された．また，多言語を使用することで，ユーザが正確な攻撃の手口を認識しづらくする工夫も見られた．これらの工夫は，ユーザを欺くために有効といえる．

5.　議論

5.1　研究機会に関する提言事項

本研究で確認されたダイアログは 64 種類であり，その多様さからユーザが十分に確認しない懸念が残る．検体実行の失敗に関するダイアログも含まれるため一概には言えないが，実際のユーザの業務・利用環境においても多様なダイアログが提示される可能性がある．その場合，ダイアログの種別を個々に確認することがユーザの負担となり，ユーザはダイアログを確認しない習慣が定着する可能性がある．これは，UAC といった重要なセキュリティのダイアログに直面したユーザが十分に確認せず判断を下し，マルウェアに権限を与えるといった望ましくない行動につながる恐れがある．そのため，ダイアログに関する追加の実態調査を含む研究分野の発展が望ましい．

また，ダイアログに関する分析により，解析の効率化と動的解析のカバレッジ向上に役立つことが示唆された．4.2 節で述べた通り，UAC や未知のアプリケーションのダイアログに対する適切な反応がないと解析が進行しない場合，解析終了，サンドボックス機能による自動クリックによる解析の進行，解析者の手動クリックによる解析の進行のいずれかの対応がなされる．サンドボックスの機能では，UAC のようなダイアログに自動対応しているが未知のアプリケーションにより表示されるダイアログには対応していない場合が多い．一方で，解析者が手動で操作する場合，検体実行中において常に動作を確認する必要があり，解析者の負担が大きい．そのため，ダイアログの分析結果を踏まえたサンドボックス操作の拡張は，解析の効率化と解析結果のカバレッジ向上に貢献すると考えられる．

5.2　解析者の教育に関する提言事項

本研究で確認されたマルウェアの実行・解析に苦戦する事例を解析者に周知させることで，教育・インシデント対応力の向上に繋がると考えられる．実際に，検体の実行失敗や停止に関わるダイアログが提示される事例やデバッカのダウンロードを試みる事例，bin ファイルや RYK ファイ

ルの実行方法を検索する事例が解析画面から確認された．こうした事例は解析者に共通すると考えられるため，解析手順やトラブルの対処方法を共有することで，インシデント対応力の向上に繋がることが期待される．また，本研究で確認された個人情報の漏洩につながる恐れがある事例についても周知させる必要がある．具体的には，解析者がGmail に接続するために Google アカウントにログインする事例であり，ログインパスワードの入力の様子や Gmail アドレスが解析画面から確認された．Google アカウントが解析用の場合でも，認証情報の漏洩はアカウントの乗っ取りや悪用が懸念される．また，認証情報を窃取する機能を有するマルウェアも存在することからも，認証情報の入力に関するリスクを解析者に教育する必要がある．

5.3 ユーザの教育に関する提言事項

RQ3 の結果，攻撃者によるユーザ欺瞞の工夫が解析画面から確認された．巧妙なユーザ欺瞞への対策として，ユーザへの周知・注意喚起による教育・セキュリティ意識向上が必要である．本研究で明らかにした攻撃者の工夫を具体例としてユーザに提示して教育することで，セキュリティに関する理解を深めると共に，ユーザが実際に直面した際，提示した例を想起し，被害の未然防止に繋がることが期待される．特に，クリックを誘導する工夫として，図 3 の (c) のような視覚的に次に行うべき操作を示した誘導は word と Excel に共通して確認されたため，例示による教育の効果が高いと考える．また，ランサムウェアの脅迫文に関しても，同様に教育が必要であると考える．ユーザが脅迫文に直面した際に，チャルディーニの原則に従った誘導で支払いに誘導される可能性がある．チャルディーニの原則に関してユーザに周知し，巧妙な手口で支払いに誘導されることをユーザに教育するとともに，今後の研究では文献 [17] で議論されているようにチャルディーニの原則に関するどのような工夫に対してより脆弱であるか調査することで，ユーザごとに適した教育の検討が期待される．

5.4 制約

3.1 節で述べた通り，我々は ANY.RUN で挙げられている 93 ファミリに焦点を当てて調査を実施した．このため，文献 [19] 等の既存の調査研究と同様に完全性を主張するものではない．その代わりに，厳密なオープンコーディングにより，解析画面と同画面から得られる情報のマッピングの質を保証することに重点を置いた．また，理論的飽和の概念 [14] に従い，新たなコードが発見されるまで調査対象数を増やしコーディングを反復することで，より多くの情報が抽出できるように努めた．

6. おわりに

本研究では，解析画面から取得可能な情報を整理するとともに，解析画面の応用可能性を示した．本研究の成果は，今後の動的解析に関わるシステム開発や解析者およびユーザに対する教育の一助になると考えられる．

謝辞 本研究は日立グループ内のサイバー攻撃解析に関わる佐藤隆行氏や専門家各位に有益な助言とご協力を頂きました．深く感謝致します．

参考文献

[1] AV-TEST: Malware Statistics & Trends Report, available from `https://www.av-test.org/en/statistics/malware/` (2024-07-20 accessed).
[2] Wong, M., Y., et al.: An inside look into the practice of malware analysis, CCS '21, pp. 3053–3069 (2021).
[3] Amin, K., et al.: UNVEIL: A large-scale, automated approach to detecting ransomware. USENIX Security '25, pp. 757–772 (2016).
[4] Tan, S., et al.: A Novel Android Malware Detection Method Based on Visible User Interface, TrustCom '21, pp. 659–666 (2021).
[5] ANYRUN: ANYRUN, available from `https://any.run/` (2024-07-20 accessed).
[6] Joe security LLC: JoeSandbox cloud basic, available from `https://www.joesandbox.com/` (2024-07-20 accessed).
[7] Recorded Future: Triage, available from `https://tria.ge/` (2024-07-20 accessed).
[8] Anderson, D., S., et al.: Spamscatter: Characterizing Internet Scam Hosting Infrastructure. USENIX Security '16, pp. 135–148 (2007).
[9] Chris, G., et al.: Manufacturing compromise: the emergence of exploit-as-a-service. CCS '12, pp. 821–832 (2012).
[10] Dietrich, C., J., et al.: Exploiting Visual Appearance to Cluster and Detect Rogue Software, SAC '13, pp. 1776–1783 (2013).
[11] Miramirkhani, N., et al.: Dial One for Scam: A Large-Scale Analysis of Technical Support Scams, NDSS '17, pp. 1–15 (2017).
[12] Stone-Gross, B., et al.; The Underground Economy of Fake Antivirus Software, Economics of Information Security and Privacy III, pp. 55-78 (2013).
[13] Koide, T., et al. It never rains but it pours: Analyzing and detecting fake removal information advertisement sites, DIMVA '20, pp. 171–191 (2020).
[14] Glaser, B., et al.: The Discovery of Grounded Theory: Strategies for Qualitative Research. (1967).
[15] ANYRUN: Malware Trends Tracker, available from `https://any.run/malware-trends/` (2024-07-20 accessed).
[16] Ortloff, A., et al.: Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. CHI '23, pp.1–21 (2023).
[17] Heijden, A., et al.: Cognitive Triaging of Phishing Attacks. USENIX Security '19, pp. 1309–1326 (2019).
[18] Cialdini, R.: Influence: The Psychology of Persuasion. (1984).
[19] Wong, M., Y., et al.: Comparing Malware Evasion Theory with Practice: Results from Interviews with Expert Analysts, SOUPS '24, pp. 61–80 (2024).