早稲田大学大学院 基幹理工学研究科

博 士 論 文 概 要

論 文 題 目

Taint-based Analysis Techniques against Evasive Malware
解析回避機能を持つマルウェアの解析手法：テイント伝播によるアプローチ

申 請 者

Yuhei	KAWAKOYA
川古谷	裕平

2018 年 12 月

インターネットにおける様々な問題の中でマルウェアは主要なツールとして利用されている。例えば、多数のマルウェア感染端末によって構成されるボットネットはサービス妨害攻撃やスパムメールの配信基盤としてブラックマーケットで取引されている。また近年では、Crypto Miningマルウェアが登場しマルウェア感染端末を利用して直接金銭を生み出している。これらボットネットやCrypto Mining マルウェアは犯罪組織の資金源として利用されており早急な対策が求められている。

これらマルウェアに対する効果的かつ直接的な対策を生み出す術としてマルウェア解析がある。セキュリティのエキスパート達は解析技術やツールを駆使してマルウェアを解析し、その挙動を明らかにする。さらにその目的や被害規模や組織・ネットワークに対するインパクトなどの情報も明らかにし適切な対処方法を生み出している。

マルウェアを解析する手法を大別すると、動的解析と静的解析の二つの手法がある。動的解析では、あらかじめ用意した隔離環境上でマルウェアを動作させ、その振る舞いを観測することでマルウェアの挙動を解析する。この観測する対象として、特定のプロセスから実行されるシステムサービスコールや Application Programming Interface (API)コールや実行命令がある。この中でも特にAPIは豊富なコンテキスト情報を保持しており、動的解析の観測対象として良く利用される。またAPIはドキュメントが豊富に整備されており、そのAPIを見ればマルウェアが行った挙動を容易に理解することができる。このため、APIを観測対象としたAPIモニタは学術界での研究のみならず産業界のセキュリティ製品にも頻繁に用いられている。

一方、静的解析はマルウェアの実行ファイルを実環境上で動作させずに解析する手法である。実際に動作させないので、マルウェアの悪性な挙動による環境の破壊や外部への攻撃等の被害を避けることができる。また静的解析は理論的にはマルウェアのすべてのコードを解析可能であり、マルウェアが持つ振る舞いをすべて抽出することができる。しかし、通常マルウェアは膨大な量の機械語で構成されており、これら機械語を解析対象とする静的解析は多くの時間を要する。また機械語はコンテキストに乏しく、その機械語やそれらの列から挙動を理解するのが難しい。そこで豊富なコンテキストを持つAPIをヒントに静的解析を行うことで、効率的に解析を進めることができる。このように動的解析と静的解析のどちらにおいてもAPIの情報は有用であり、マルウェア解析を効率的に行うには必要不可欠な情報源だといえる。

マルウェアの作者もこの“解析における API の有用性”を十分に理解しており、妨害する機能をマルウェアに埋め込み、解析を困難にしてくる。具体的には動的解析におけるAPIモニタの回避や静的解析におけるインポートAPIの隠蔽が

ある。動的解析を妨害する方法は、フック回避とターゲット回避の二つの方法に大別される。フック回避は、APIコール観測のために設置されたフックを回避してAPIを呼び出す方法である。例えばフックが置かれる可能性の高いAPIの先頭の数命令をあらかじめコピーしておき、そのコピーした命令経由でAPIを呼び出すStolen Codeといった手法がある。ターゲット回避は、マルウェアが特定の挙動をAPIモニタの観測対象から意図的に外すための方法である。例えば悪意のある挙動を行うコードの一部を正規のプロセスに注入し、そのプロセスの中で実行するCode Injectionといった手法がある。これらの解析妨害・回避手法が利用されると通常のAPIモニタではAPIの呼び出しが正確に取得できない。さらに大きな問題として、解析者がAPIの呼び出しを補足し逃していることに気がつきにくい。そのため、マルウェアが部分的にこれらの回避手法を利用すると、大事な部分の挙動を観測し逃がしている事態が発生する。

また静的解析を妨害する解析妨害として、インポートしているAPIの隠蔽がある。前述のように静的解析においてAPI情報は重要な情報源である。そのためマルウェアは自身が利用しているAPI情報を隠蔽する傾向にある。例えば、Portable Executable(PE)形式の実行ファイルはインポートしているAPIの一覧をPEヘッダの中に保持している。しかし、マルウェアはこれらの情報を削除してしまう。この状態で静的解析を行うと、逆アセンブラ等の静的解析ツールはAPIの情報を解決できず、APIの呼び出しがある命令やその周辺のコードの意味を認識できない事態が発生する。

このように攻撃者が様々な解析妨害手法を開発できる背景には、既存の解析手法が抱える設計上の一つの問題があると考える。既存の解析手法の多くは解析対象としているコードそのものではなく、そのコードの存在を示す情報を基に解析手法が設計されている。例えばマルウェアを動的解析で解析する際、そのマルウェアのコード自身ではなく、そのコードの実行インスタンスとしてのプロセスを一意に特定できるプロセス識別子の情報に基づいて解析対象か否かを判断している。別の例として特定のAPIの実行を監視したい場合、そのAPIのコード自体の実行ではなく、そのAPIが配置されていると考えられるメモリアドレスの実行に基づいてそのAPIの実行を判断している。これらの例のように本来捉えるべきものであるコードやコードの実行そのものではなく、そのコードの配置を意味する情報に基づいて既存の解析手法は設計されている。マルウェアは、この本来捉えるべきものとそれを指し示す情報のズレを悪用することで解析手法を欺いている。具体的にはStolen Codeは本来APIが配置されていると考えられるアドレスから別の場所にAPIのコードをコピーして、そのコピー先の場所で実行する。これによりAPIのコードを実行しているにも関わらず、APIの実行とは認識されないようにしている。

本研究ではこの問題に焦点を当て、テイント解析を利用して、従来のマルウェア解析技術を拡張する。テイント解析とはデータフローの解析技術の一つである。テイントタグと呼ばれる属性情報をプログラムの実行環境上の値に対して付与し、その値が環境上を移動する毎にこのテイントタグを伝播して追跡する手法である。このテイント解析を利用し、上記で述べた問題を解決する。

第 1 章では、本研究の背景と目標ならびに以降の章構成に沿って成果の概要を示す。

第 2 章では、マルウェアが利用する解析回避手法の全体像とこれらに対する既存研究を説明し、本研究との関連を説明する。

第 3 章では、上記で挙げた既存の動的解析と静的解析手法の問題点を立証するため、解析妨害の検証ツールを設計・実装・評価する。具体的には、Windows OS が管理するデータ領域上に、ロードした DLL の情報が残らないように、当該 DLL を実行可能にするプログラムローダを設計・実装する。これを用いてロードした DLL から API を呼び出すと、その API の実行や存在を観測することができない。評価では現場で広く使われている動的・静的解析ツールを利用し、これらに解析されることなく API を利用することができることを示す。

第 4 章では、動的解析における API モニタをテイント解析にて拡張する手法を提案する。この章では、通常はデータフロー解析に利用されるテイント解析をコードの実行を捉えるために利用する、コードテイント、を紹介する。またコードテイントを拡張として、各 API のコードに異なるテイントタグを用意し、実行されている命令に設定されているテイントタグと次に実行される命令に設定されているタグとの遷移パターンにより監視対象 API か否かを見分ける taint-based control transfer interception を提案する。これらの手法を実装して構築したシステムである API Chaser を利用してインターネットから収集した大量のマルウェアを解析し、提案手法とシステムの有効性を示す。

第 5 章では、静的解析における API の名前解決をテイントタグから行う手法である taint-based API name resolution を提案する。これはテイントタグに“メモリ上のバイト列がある特定の API のコードである”といった情報を載せ、動的解析時に伝播させる。動的解析終了後のメモリダンプ取得時にこの伝播したテイントタグの情報も一緒に取得し、その情報に基づいて API の名前解決を行う。これにより、API の名前解決を妨害する手法に影響を受けることなく API の名前解決が行えることを示す。

第 6 章では、本研究の内容をまとめ、1 章で指摘した問題を解決できることを示す。またテイント解析をコードの実行を捉えるために利用するといったアイデアとその応用により、従来技術では成しえなかった解析回避機能を持ったマルウェアを正確に解析可能にしたことを主張し、本研究をまとめる。

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　川古谷　裕平　印

（2019 年 2 月 3 日 現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
○論文	Yuhei Kawakoya, Eitaro Shioji, Makoto Iwamura, Jun Miyoshi, “API Chaser: Taint-Assisted Sandbox for Evasive Malware Analysis”, Journal of Information Processing (JIP)(in printing).
○論文	Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, “Taint-assisted IAT Reconstruction against Position Obfuscation” (Recommended Paper), Journal of Information Processing (JIP), vol.26, pp.813-824, December 2018 (Recommended Paper, JIP Specially Selected Paper).
○論文	Yuhei Kawakoya, Eitaro Shioji, Yuto Otsuki, Makoto Iwamura, Jun Miyoshi, ″Stealth Loader: Trace-free Program Loading for Analysis Evasion″, Journal of Information Processing (JIP), vol.26, pp.673-686, September 2018.
○論文	Yuhei Kawakoya, Makoto Iwamura, Takeo Hariu, “Tracing Malicious Code with Taint Propagation”, Journal of Information Processing Society of Japan (IPSJ), vol.54 no.8, pp.2079-2089, August 2013 (in Japanese) (Recommended Paper, IPSJ Specially Selected Paper, IPSJ Yamashita SIG Research Award).
国際会議	Yuhei Kawakoya, Eitaro Shioji, Yuto Otsuki, Makoto Iwamura, Takeshi Yada, “Stealth Loader: Trace-free Program Loading for API Obfuscation”, Proceedings of 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), pp.217-237, September 2017.
国際会議	Yuhei Kawakoya, Makoto Iwamura, Eitaro Shioji, Takeo Hariu, “API Chaser: Anti-analysis Resistant Malware Analyzer”, Proceedings of 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), vol.8145, pp.123-143, October 2013.
国際会議	Yuhei Kawakoya, Makoto Iwamura, Mitsutaka Itoh, “Memory behavior-based automatic malware unpacking in stealth debugging environment”, Proceedings of 5th IEEE International Conference on Malicious and Unwanted Software (MALWARE), October 2010.
国際会議	Yuhei Kawakoya, Yoichi Muraoka, “Proposal and Implementation of Router-Based Traceback Technique”, Proceedings of the International Conference on Security and Management (SAM), June 2004.

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
招待講演	Yuhei Kawakoya, “Analysis Evasion. Introduction of Self-Made Packer”, IPA SecurityCamp 2018, August 2018 (in Japanese).
招待講演	Yuhei Kawakoya, “Unpacking Introduction”, anti Malware engineering WorkShop 2011 (MWS2011), October 2011 (in Japanese).
招待講演	Yuhei Kawakoya, “The Secrets of the Development of Stealth Debugger”, RSA Conference Japan 2010, September 2010 (in Japanese).
講演	Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, Tatsuya Mori, “IOC Conversion with Symbolic Execution”, Proceedings of the Computer Security Symposium 2018 (CSS2018), vol.2018, no.2, pp.762-769, October 2018 (in Japanese).
講演	Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, “Taint-assisted Forensics for IAT Reconstruction”, Proceedings of the Computer Security Symposium 2017 (CSS2017), vol.2017, no.2, October 2017 (in Japanese) (CSS Excellent Paper Award).
講演	Yuhei Kawakoya, Eitaro Shioji, Makoto Iwamura, Takeo Hariu, “Identifying the Contents of Malware Communication Using Data Dependency Between API Calls”, Proceedings of the Computer Security Symposium 2013 (CSS2013), vol.2013, no.4, pp.745-752, October 2013 (in Japanese)
講演	Yuhei Kawakoya, Eitaro Shioji, Makoto Iwamura, Takeo Hariu, “Tracing malicious code with Taint Propagation”, Proceedings of the Computer Security Symposium 2012 (CSS2012), vol.2012, no.3, pp.1-8, October 2012 (in Japanese) (MWS Best Paper Award)
講演	Yuhei Kawakoya, Makoto Iwamura, Takeo Hariu, “Identifying the Code to be Analyzed with Taint Tags”, IEICE Technical Report, vol.112, no.128, pp.77-82, July 2012 (in Japanese).
講演	Yuhei Kawakoya, Makoto Iwamura, Takeo Hariu, “Dynamic Packer Identification Based on Instruction Trace”, Proceedings of the Computer Security Symposium 2011 (CSS2011), vol.2018, no.3, pp.18-23, October 2011 (in Japanese).
講演	Yuhei Kawakoya, Makoto Iwamura, Mitsutaka Itoh, “Dense Ship: Virtual Machine Monitor Specialized for Server-Type Honeypot”, IEICE Technical Report, vol.111, no.81, pp.63-68, June 2011 (in Japanese).
講演	Yuhei Kawakoya, Makoto Iwamura, Mitsutaka Itoh, “Automatic OEP Finding Method for Malware Unpacking”, IEICE Technical Report, vol.110, no.79, pp.13-18, June 2010 (in Japanese).

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
著書	川古谷他５名（監訳），“サイバーセキュリティプログラミング ―Python で学ぶハッカーの思考”,オライリー・ジャパン，2015 年 10 月
著書	川古谷他７名（翻訳），“実践 Metasploit――ペネトレーションテストによる脆弱性評価”，オライリー・ジャパン，2012 年５月
著書	川古谷他４名，“アナライジング・マルウェア――フリーツールを使った感染事案対処 オライリー・ジャパン，2010 年 12 月
その他(論文)	Mitsuaki Akiyama, Kazufumi Aoki, Yuhei Kawakoya, Makoto Iwamura,　Mitsutaka Itoh, “Design and Implementation of High Interaction Client Honeypot for Drive-by-download Attacks”, IEICE Transactions on Communication, vol.E93-B no.5 pp.1131-1139, May 2010
その他(論文)	Kazufumi Aoki, Yuhei Kawakoya, Mitsuaki Akiyama, Makoto Iwamura, Mitsutaka Itoh, “Investigation and Understanding Active/Passive Attacks”, Journal of Information Processing Society of Japan (IPSJ) vol.50, no.9, pp.2147-2162, September 2009 (in Japanese).
その他(国際会議)	Yuto Otsuki, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, Kazuhiko Ohkubo, “Building stack traces from memory dump of Windows x64”, Proceedings of the Digital Forensic Research Workshop EU 2018 (DFRWS EU) vol.24, pp.S101-S110, March 2017
その他(国際会議)	Eitaro Shioji, Yuhei Kawakoya, Makoto Iwamura, Takeo Hariu, “Code Shredding: Byte-Granular Randomization of Program Layout for Detecting Code-Reuse Attacks”, Proceedings of 28th Annual Computer Security Applications Conference (ACSAC), pp. 309-318, December 2012.
その他(国際会議)	Mitsuaki Akiyama, Yuhei Kawakoya, Takeo Hariu, “Scalable and Performance-Efficient Client Honeypot on High Interaction System”, Proceedings of 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet (SAINT), pp.40-50, July 2012.
その他(講演)	Eitaro Shioji, Yuhei Kawakoya, Makoto Iwamura, Takeo Hariu, “Detecting Invalid Control Flow with Pseudo-Dispersion of Program Code”, IEICE Technical Report, vol.112, no.128, pp. 103-108, July 2012 (in Japanese)(ICSS Research Award). その他　国際会議共著１件、講演 15 件(主著４件、共著 11 件)、特許 25 件、総説４件