環境選択型マルウェアの挙動解析による自動対策システムの研究

2017 年 1 月 23 日

「博士学位請求論文」審査報告書

審査委員（主査）　総合数理学部　専任教授

氏名　　菊池　浩明　　㊞

（副査）　総合数理学部　専任教授

氏名　　二宮　広和　　㊞

（副査）　総合数理学部　専任講師

氏名　　池田　幸太　　㊞

（副査）　理工学部　専任教授

氏名　　齋藤　孝道　　㊞

（副査）　立命館大学情報理工学部　教授

氏名　　毛利　公一　　㊞

1　論文提出者　　氏名　　仲小路　博史

2　論文題名

（邦文題）環境選択型マルウェアの挙動解析による自動対策システムの研究

（欧文訳）　A Study on Automated Defense System with Behavior Analysis Against Environment-Sensitive Malware

3　論文の構成

本論文の構成は以下の通りである.

1 章　研究背景と目的
2 章　マルウェア挙動解明
3 章　マルウェア通信制御
4 章　プロキシアクセス型マルウェア解析
5 章　サンドボックス最適化
6 章　不正サイト挙動解明
7 章　挙動に基づく自動対策
8 章　結論

４　論文の概要

コンピュータウイルス等のマルウェアが高度化し，マルウェアの侵入，感染を完全に防御することは困難な状況になってきている．対策技術を予測して，狙った環境でのみしか動作しない環境選択型マルウェアを開発して，解析回避を図る攻撃者が現れ，大きな課題となっている．攻撃者の脅威情報を共有して，特定のアドレスからのアクセスを遮断する対策技術もあるが，脅威情報が共有されることを見越した攻撃者により，意図的に検索エンジンなどの正規サイトにアクセスするマルウェアが導入されて，それらの対策技術が有効に活かせなくなってきている．

このように高度化なマルウェアを用いた標的型攻撃に対して，本論文では，業務への影響を考慮した自動対策システム「自律進化型防御システム（AED：Autonomous Evolution of Defense)」を提案している．提案システムは，(1) 挙動の解析が困難になってきている環境選択型マルウェアの増加という問題に対して，環境選択型マルウェアを自動解析し，攻撃者による遠隔操作や情報搾取を防止するために有用となる“マルウェアの接続先（不審サイト)”を効果的に抽出する，(2) 抽出された不審サイト情報に含まれている誤った情報によって，利用者の業務への影響に影響させないように接続先を自動的に学習する，という二つの目標を挙げている．

1 章では，研究の背景と目的を述べている． まず，(1)の目標に対して，環境選択型マルウェアの挙動を解明可能な動的解析の実現と，動的解析で一般的に利用されているインターネット隔離環境では現れない機能の把握する課題を設定した．(2)の目標には，マルウェアによる不正なアクセスの遮断と，誤った情報による対策であったとしても業務上必要なアクセスは許可することを設定した．これらの技術の位置づけと，各章の関係を説明している．

2 章では，環境選択型マルウェアへの対策に有用な情報“マルウェアの接続先（不審サイト)”を得るために，多種環境でマルウェアを解析する多種環境マルウェア動的解析システム（M3AS）を提案している．マルウェアが感染しやすい環境（解析エンジンや OS，アプリケーション）を，公開されている脆弱性の数を基準として選定することで，感染（観測）しやすいサンドボックスを構成する方法を示している．本システムを用いてマルウェア 633 種を解析し，マルウェア対策に有用なマルウェアの接続先 6,542URL を取得する実験結果を報告している．

３章では，インターネットと隔離された環境では動作しないマルウェアの機能の把握するため，閉塞環境で解析していた前記 M3AS を拡張し，第二のマルウェアのダウンロード通信のみ限定的にインターネットに接続させて解析精度を向上させる手法を提案している．評価により 644 種のマルウェアから 58 の第二のマルウェアの取得に成功し，さらに解析中に外部への攻撃がなかったことを確認することで，外部への攻撃を行うことなく，組織に侵入したマルウェアの特性を解明できることを明らかにしている．

4 章では，多層防御における出口対策として導入が推奨されている認証付プロキシをも突破するマルウェア（プロキシアクセス型マルウェア）が増加している懸念から，M3AS を拡張してプロキシアクセス型マルウェアのプロキシ対応能力を判定するプロキシ認証突破判定システムを提案している．本システムを用いて，2014 年 10 月に取得したマルウェア 629 種を解析し，そのうち 84 種がプロキシ利用するプロキシアクセス型マルウェアで，8 種がプロキシ認証をも

突破するマルウェアであることを報告している．

５章では，M3AS で用いるサンドボックスの最適配置の問題取り組んでいる．サンドボックス数と解析精度にはトレードオフの関係があり，サンドボックスの拡充（精度向上）がコスト高騰に直結する．そこで，サンドボックスの個数と顕現（マルウェアがいずれかのサンドボックスで動作）の成否の関係を検証し，少ないサンドボックスでより多くのマルウェアを顕現可能なサンドボックス選定方式を提案している．本方式を適用してサンドボックスの数を 76 個から 27 個に減らした場合でも，すべてのマルウェアを顕現させられることを評価し，サンドボックス数を約 65%削減している．

6 章では，M3AS を拡張して不正サイトを解析するシステムを提案している．解析対象サイトへのアクセスに用いるブラウザ等の環境にバリエーションを持たせたサンドボックスを新たに構築し,不正サイトへアクセスするブラウザによって応答を変化させる巧妙な不正サイト(クローキング）の解析に対応した不正サイト挙動解明システムの開発について述べている．代表的なブラウザ 4 種をインストールしたサンドボックスを用いて，実際に不正サイトの疑いのある 2,439 サイトを解析し，ブラウザによって挙動を変化させる不正サイトの存在を報告している．

7 章では，M3AS により得たマルウェアの接続先（不審 URL）を用いて，マルウェアによる不正なアクセスの遮断を実現する自動対策システムを提案している．不審 URL へ端末がアクセスする際に，人間と機械とを判別可能な CAPTCHA 認証を端末に対して与えることで，マルウェアによる機械的なアクセスのみ遮断する自律進化型防御システム（AED）である. M3AS 等から得た 52,653 種類のユニークな不審 URL リストと AED を用いて評価した結果，2,064 種類のマルウェアの 99%以上の遮断に成功したことを報告している．実証実験に参加した被験者に対して実施したアンケート結果では,誤った情報に基づく本提案手法による自動対策に「不便を感じた」と回答した被験者は 0 であった．

8 章では，以上の課題を解決するための手法提案，実装，実験評価をまとめ，本研究を結論付けている．環境選択型マルウェアを自動解析して対策に有効な情報を抽出することで目的(1)を達成し，この情報に「業務へ悪影響を与える情報」が含まれていたとしても業務への影響を最低限に抑えて迅速，自動的に対策する目的(2)の二つを満たしている．

５　論文の特質

本論文で提案されている動的解析システム（M3AS）は，多種環境でマルウェアを解析する多種環境マルウェアに対する初めての試みである．多種多様な環境を並列に解析するために，異なる OS やソフトウェアをインストールした 70 台以上の仮想マシンを構築して，マルウェアに含まれる不正アクセス先情報などの動的解析を並列実行するシステムは独創的であり，明確な新規性と潜在的な応用を多く含んでいる．実際に，3 章から 6 章で提案される方式の多くは，この大規模な仮想環境を用いて行われており，第二アクセス先の抽出や，サンドボックスの最適配置問題など，多くの新たな研究課題に繋がっている．

研究の新規性に加えて，実環境での実証実験を幅広く行っていることも大きな特徴である．7 章では，誤りを含む不正アクセス先情報に対して機械人間認証 CAPTCHA を導入して，誤りを自動的に削減する機構を提案しているが，それを 30 名以上の被験者を用いて一週間程度の

実証実験を繰り返し，50 万件以上のウェブアクセスに対する提案システムの検出精度を評価している．これらの実験結果は，同様のシステムを導入する際の効果を予測する有益な情報を提供している．開発だけに終わらず，アンケートを含む利用者評価情報は貴重であり，組織における情報セキュリティマネージメントに大きく寄与するものである．

６　論文の評価

マルウェアの高度化とその対策は，多くの組織を悩ませる社会的に重要な課題である．多くの先行研究がなされているが，対策技術の裏をかき，標的に応じて攻撃の手段を変化させるマルウェアに対処するには大きな困難性がある．この課題に対して，多様な環境を模擬したサンドボックスを複数構築し，マルウェア動的解析を並列実行するアプローチには高い新規性があり，そこから多くの派生する問題についても幅広く，研究開発を重ねている．技術的な難易度に加えて，提案システムの実証実験に基づいてマルウェアの検出精度や業務への影響評価を定量的に行っており，利用者アンケートを含む評価結果には十分な有用性がある．

学位論文には，100 件を超える参考文献が挙げられており，本分野の最新の関連研究に対しても十分な調査が行われている．学位論文は 8 章に渡り，研究成果を論理的に構成して，適切に研究をまとめている．研究成果は，情報処理学会や国際会議を含む学会にて発表されており，本分野の複数の専門家による公平な査読が行われており，十分な信頼性を持っていることを裏付けている．

従って，以上の点から，本論文は，情報セキュリティの為の応用研究として独創的かつ有益性の高いものであると評価する．

７　論文の判定

本学位請求論文は，先端数理科学研究科において必要な研究指導を受けたうえ提出されたものであり，本学学位規程の手続きに従い，審査委員全員による所定の審査及び最終試験に合格したので，博士（数理科学）の学位を授与するに値するものと判定する．

以　上