「マルチメディア，分散，協調とモバイル
(DICOMO2019) シンポジウム」 令和元年7月

Fake Honeypotを利用した欺瞞的防御の提案

北沢 尭宏[1]　篠田 陽一[2]

概要：インターネット技術の発展に伴い、インターネットを利用できることを前提とした社会になった。その一方、ネットワークを介し、ネットワークに接続する端末を対象としたサイバー攻撃の技術も発達し、それによる被害は深刻な問題となっている。中でも、特定の攻撃対象に対し、その機関に最適化された戦略やツールを用いる標的型攻撃の中に位置付けられる高度で継続的なサイバー攻撃である APT 攻撃が問題視されている。これは、既存のセキュリティ製品では対応が難しいためである。この攻撃に有効な防御方法として、欺瞞的防御がある。攻撃コストを増加させることで攻撃者を撹乱し、攻撃者の目的を阻害することを本項の目的とする。本項では、攻撃者から観測した際に実端末に見えるような機構を持つハニーポットを用いて欺瞞的防御を行うのではなく、実端末をハニーポットのように見せることで欺瞞的防御を行う。

Proposal of Cyber Deception using Fake Honeypot

TAKAHIRO KITAZAWA[1]　YOICHI SHINODA[2]

1. 背景

インターネット技術の発展に伴い、インターネットを利用できることを前提とした社会になった。その一方、ネットワークを介し、ネットワークに接続する端末を対象としたサイバー攻撃の技術も発達し、それによる被害は深刻な問題となっている。中でも、特定の攻撃対象に対し、その機関に最適化された戦略やツールを用いる標的型攻撃の中に位置付けられる高度で継続的なサイバー攻撃 (Advanced Persistent Threat: 以降、APT 攻撃) が問題視されている。独立行政法人情報処理推進機構 (以降、IPA) によると、APT 攻撃は、「ソフトウェアの脆弱性を悪用し、複数の既存技術を組み合わせ、ソーシャルエンジニアリングにより特定の企業や個人を狙い、対応が難しく執拗なサイバー攻撃」と定義されている [1]。この攻撃では、複数の既存技術の組み合わせやソーシャルエンジニアリングの他に、未知の脆弱性 (以降、ゼロデイ攻撃) も利用されており、既存のセキュリティ製品を導入しても対策しきれない場合がある。これらのような、既存のセキュリティ製品では対策しきれない攻撃に対し、知的財産や個人情報、機密情報を守るための有効な防御技術として、欺瞞的防御 (Cyber Deception) がある。欺瞞的防御は、攻撃者が組織内部ネットワークに侵入することを前提としており、ハニーポット等の囮となるツールをネットワーク内部に設置することで攻撃者を撹乱し、防御を行う。欺瞞的防御を構成する技術として、ハニーポットと攻撃者に囮と悟られないようにするためのハニーポット隠蔽化と仮想環境隠蔽化技術、IDS(Intrusion Detection System) 等の侵入検知システムの 4 つがある。これら複数の技術を利用することで攻撃者を撹乱し、攻撃者の目的や戦略、使用しているツール群を分析している。しかし、高い技術を持つ攻撃者はハニーポットを検出する技術 (以降、Honeypot Detection) や仮想環境を検出する技術等を利用し、攻撃者の行動等を記録し分析されることを回避し、攻撃を行い続けるという問題がある。

本項では、上記の問題に対して、本物の端末をハニーポットであるかのように錯覚させる Fake Honeypot を利用し、欺瞞的防御を行うことを提案する。また、既存の欺瞞的防御とそれに関連する技術を分類する。

2. 各種既存技術と体系化

本章では、欺瞞的防御に関する基盤技術や既存研究、関連技術についてまとめ、分類することで体系化する。

[1] 北陸先端科学技術大学院大学先端科学技術研究科
Graduate School of Advanced Science and Technology,
[2] 北陸先端科学技術大学院大学情報社会基盤研究センター
Reserch Center for Advanced Computing Infrastructure,
Japan Advanced Institute of Science and Technology

© 2019 Information Processing Society of Japan

2.1 Honeypot

ハニーポットは、サイバー攻撃手法の流行や攻撃者の目的、使用されるツール群や戦略を分析するためのセキュリティツールである。ハニーポットで得られた情報をもとにサイバー攻撃を行う攻撃者を分析することで、マルウェアや攻撃ツールに対する早期対応が可能になっている。

ハニーポットには本物のシステムの再現度や対話数、設置する環境等によって呼称が変わる。本項では、低対話型ハニーポットと高対話型ハニーポット、仮想環境型ハニーポットを取り上げる。

低対話型ハニーポットは、OS を使用せずにアプリケーションとして実装することが多く、サポートするアプリケーションやプロトコルに制限をかけているという特徴がある。サポートする要素は、ハニーポットの管理者が観測したい内容に最適化している。そのため、特定のサービスに対する攻撃の分析ができるうえ、行動に制限をかけるため運用・管理が比較的簡単である。一方で、攻撃者の多種多様な行動の観測・分析には適さず、制限の多さからハニーポットであると容易に判断される。

高対話型ハニーポットは、一部行動に制限がかかった OS を使用し、通常の端末とほぼ同等の動作をサポートしている。そのため、低対話型ハニーポットに比べて攻撃者やマルウェアの多種多様な行動や動作の観測が可能になっている。主に、攻撃手法の全容を明らかにする際に用いられることが多い。一方で、適切に攻撃者の行動制限をかけていない場合には、ハニーポットが攻撃者に不正利用され、マルウェアの拡散や侵入端末を踏み台とした更なる不正アクセスにも繋がるため、管理・運用する際には最新の注意を払わなければいけない。

仮想環境型ハニーポットは、実際の端末上にハニーポットを設置するのではなく仮想環境上にハニーポットを設置している。そのため、スナップショット機能による行動記録や新規設置等の管理が非常に容易であるという特徴がある。

これらのハニーポットを利用し、ネットワークのセキュリティ性を向上させることもできる。これは、欺瞞的防御と呼ばれ、守りたい端末の囮として設置することで防御を行うことが可能である。

2.2 欺瞞的防御

欺瞞的防御は、攻撃者を騙す仕組みを用いて防御を行う手法である。これは、既存のセキュリティ製品とは異なり、APT 攻撃やゼロデイ攻撃に有効な防御方式とされている。主に、ネットワーク内に守りたい端末の囮として脆弱性を保持したハニーポットを設置することで、攻撃者を誘引し攻撃コストを増加させることを目的としている。欺瞞的防御を成立させる基盤技術には、ハニーポットとハニーポットの隠蔽化技術、仮想環境の隠蔽化技術が不可欠である。そのほかにも、IDS 等の侵入検出技術とログ情報を収集するシステムを取り入れることで、防御技術としての側面とハニーポット本来の攻撃者分析ツールとしての側面の 2 つを持つことができる。

以下に、欺瞞的防御の関連技術を紹介する。

2.2.1 組織ネットワークにおける内部攻撃に対する模擬的欺瞞方式

角丸ら [2][3] は、APT 攻撃の各段階に対して防御を行う縦深防御に注目していた。その中で角丸らが欺瞞機構を提案していた段階は、攻撃者がネットワーク内部の端末に感染し、次の攻撃対象を探す”索敵段階”である。シナリオとしては、不審なメールを発端とした標的型攻撃を受け、攻撃者は他端末への侵攻拡大を行う。その際、ブロードキャストで送信される NetBIOS Name query に対して、到達性のない IP を持つメッセージを大量に返答する。これにより、攻撃者が本当の端末を把握するまでに時間的なコストを消費させることができる。

2.2.2 行動制限型ハニーポットにおける内部攻撃に対する欺瞞的防御方式

小泉ら [4] は、行動制限型の中対話ハニーポットを用いて攻撃者の行動を観測するために、ハニーポットであると気づかれにくいハニーポットを作成した。小泉らが提案したハニーポットはコマンドラッパーと名付けれれ、攻撃者が侵入する際は OS 上で動作する特殊 OS のダミープロンプトに接続されるように構成されている。これにより、実際の端末を危険に晒すことなく攻撃者の観測が可能になっている。

2.2.3 セキュリティ無効化攻撃を利用したマルウェアの検知と活動抑制手法の提案

松本ら [5] は、セキュリティプロセスを検知し、無効化するマルウェア対抗する方法を提案している。偽のセキュリティプロセスを動作させ、これを強制停止したプロセスを検知することでマルウェアの存在を検知している。

2.2.4 仮想環境の隠蔽化

ハニーポットが設置される環境として、実端末の利用や UML(User Mode Linux)、仮想環境が考えられる。仮想化技術の向上により、VMware 社 [6] の製品等を利用した仮想環境型ハニーポットが利用されている。これにより、多くのコストをかけずに複数のハニーポットを設置できるようになったが、攻撃者は仮想環境を検出するための技術を開発・公開している。

VMware 製品では、通常の端末と同様にネットワークに接続するための NIC(Network Interface Card) が存在する。そのため、VMware 社に割り当てられた OUI(Organizationally Unique Identifier) を含む MAC アドレスが割り振られてるため、これをもとにした検出が可能になっている。

Kostya Kortvhinsky は、攻撃者が侵入した環境が

© 2019 Information Processing Society of Japan

VMware 環境であることを隠すために、MAC アドレスやビデオカード名等を偽装するためのパッチを作成・公開していた。しかし、現在は公開されていない。

2.3 Honeypot Detection

ハニーポットの管理者は、攻撃者やマルウェアの行動を監視するために、ハニーポットや仮想環境等の疑わしい環境であることを隠す技術を導入する。Honeypot Detection は、疑わしい環境を検出する技術であり、攻撃者は攻撃を行う前に Honeypot Detection を用いることが知られている。これを用いることで、攻撃者は目的や行動、使用するツール等の情報を観測者に与えることなく攻撃ができる。

本項では、攻撃者が利用する Honeypot Detection に対抗する手段を探るべく、Honeypot Detection を以下の 4 種に分類した。

- ハニーポットの特性にもとづいた手法
- ハニーポットの種類にもとづいた手法
- ログ収集機能を想定した手法
- 仮想環境特有の情報をもとにした手法

また、攻撃対象となる端末外から疑わしい環境を検出するリモート検出と、攻撃対象となる端末への侵入後の操作で疑わしい環境を検出するローカル検出の 2 種にも分類した。

本節では、欺瞞的防御を妨げる Honeypot Detection に関して説明し、その体系化を行う。

以下が、Honeypot Detection 各種の具体例とその詳細である。

2.3.1 ハニーポットの特性にもとづいた手法

ハニーポットが攻撃者を誘引するために保持する脆弱性や十分なセキュリティ製品を導入しないことを逆手にとり、攻撃者はこれを利用してハニーポットの検出を行なっている。極端な例ではあるが、LAND 攻撃を挙げる。LAND 攻撃は、送信元アドレスの IP アドレスとポート番号を、攻撃対象の IP アドレスとポート番号に偽装したパケットを送信することでメッセージ送受信のループを引き起こし、正常に動作できなくする攻撃である。攻撃対象となった端末が十分に対策をしていれば、処理の実行には至らず不具合を起こさない。一方で、攻撃者を誘引するために十分な対策をしていない端末であれば不具合が発生する。その際、十分なサイバー攻撃対策をしている場合に、不具合が発生しないことがわかっていれば、それはハニーポットである可能性が高くなる。このように、ハニーポットの特性を利用することで検出できる。

2.3.2 ハニーポットの種類にもとづいた手法

中-低対話型ハニーポットで見られる行動制限型のハニーポットは、攻撃者が行動可能な範囲や利用可能なコマンドにかける制限が強い。そのため、攻撃者は実際の端末であれば利用可能であるが、ハニーポットであれば利用不可な範囲を見つけることでハニーポットを検出できる。また、通信プロトコルを利用することでリモートで検出できる。ハニーポットを実際の端末のように動作させるためには、ネットワーク外部または内部の端末と通信する必要がある。その場合、TCP と UDP、HTTP 等の最低限の機能さえ対応していればいいが、通常あまり利用しないメッセージが届いた際には通常とは異なる動作が発生する。このように、通常発生しない応答を観測することで、ハニーポットの検出が可能になる。また、攻撃対象の各ポートで待機するサービスの情報を確認する方法として、THC-Amap[7] がある。これを用いることで、制限のかかったハニーポットの検出や、不自然なアプリケーションの動作を確認することができる。ハニーポットの検出以外にも、攻撃対象が持つアプリケーション名も確認できるため、攻撃対象の選出にも利用される。

2.3.3 ログ収集機能を想定した手法

確実にハニーポットを検出する方法ではないが、パッシブネットワークスニッフィングによって疑わしい環境を検出することができる。パッシブネットワークスニッフィングの例として、ICMP を利用する方法がある。同一ネットワーク内の端末に対して ICMP ECHO request を送信し、RTT(Round Trip Time) を計測する。その際に、ハニーポット等の疑わし環境があれば、他の端末と比べて RTT が大きな端末を確認することができる。これは、ログ収集機能が動作している可能性があることを示す。ログ収集機能が動作している場合、メッセージの受信から返答までにログ記録が行われ、余分な時間が経過する。Honeypot Detection ではこれを利用し、疑わしい環境を検出している。しかし、同一ネットワーク上にあったとしても実距離が離れている場合や ICMP ECHO query を受信した端末がビジー状態である場合にも遅延が発生することがあるため、確実な検出法ではない。また、クライアントサーバ型のログ収集を行う Sebek ハニーポット [8] のような環境の場合は、ログ収集される行動を大量に行うこでサーバへのメッセージ送信を発生させ、輻輳を引き起こすことで検出する方法もある。

2.3.4 仮想環境特有の情報をもとにした手法

ハニーポットは簡単に管理・運用ができる仮想環境を利用する場合が多い。そのため、攻撃者は侵入した端末が仮想環境上に存在しているのかを確認することで、疑わしい環境を検出することができる。実際に、仮想環境を検出・回避する技術を施された Agobot のようなマルウェアも存在する。VMware の場合、ホスト OS と VMware 上にインストールされたゲスト OS が通信を行うために使用する VMware Hypervisor Port(0x5658) と呼ばれるポートが予約されている。このポートと VMware 社が設定しているマジックナンバー、操作コマンドを使用することで、VMware 環境を検出することができる。他にも、BIOS DMI 情報や

© 2019 Information Processing Society of Japan

CPUID ハイパーバイザーの存在ビットの確認など、仮想環境特有の情報を用いた様々な検出方法がある [9]。マルウェアや攻撃者は、これらの仮想環境特有の情報の存在を確認することで仮想環境を検出している。また、仮想環境ベンダに割り当てられた MAC アドレスやドライバ情報を読み取ることで検出する方法もある。

上記の検出方法の他にも、Honeypot Hunter 等の商用ハニーポット検出ツールを利用する場合も考えられる。

2.4 Fake Honeypot

上記の Honeypot Detection の発展により、ハニーポットを利用した情報収集や欺瞞的防御が難しくなる。これに対抗して、ハニーポットの研究者は Honeypot Detection に検出されない技術の開発に注力する。そのため、攻撃者と研究者の間でいたちごっこが続いている。本研究では、ハニーポットに対し欺瞞機構を加えることで攻撃者を騙す欺瞞的防御とは異なる技術として Fake Honeypot に注目した。Fake Honeypot は、実際の端末に対して欺瞞機構を加えることにより、攻撃者やマルウェアにハニーポットと誤認識させる。これにより、守りたい端末を攻撃者の攻撃対象から外すことを目的とした技術である。

本節では、Fake Honeypot に関する研究をまとめる。

2.4.1 Fake Honeypot: A Defensive Tactic for Cyberspace

Neil ら [10] は、ハニーポットで利用するアプリケーション名のファイルやディレクトリを持つことで、侵入した攻撃者を牽制できると仮定している。事前研究では、段階的に不自然な内容を持つファイルを被験者に見せ、疑いを持つかどうかを検証している。結果として、不自然な内容は被験者に疑いを持たせることができると結論づけている。実際の研究では、攻撃者が侵入している環境に対する新態度を示す数学モデルを提案していた。また、ハニーポット特有のアプリケーション名をのファイルやディレクトリを持つ端末をネットワーク上に配置し、実証実験を行っていた。

2.4.2 欺瞞を用いた能動的サイバー攻撃防御手法の提案と実装

山田 [11] は、攻撃者が攻撃対象を調査する際に使用するポートスキャンに対して Fake Honeypot を利用している。ポートスキャンをトリガーとして、実際のシステムとは異なる情報を応答する仕組みである。これにより、攻撃者は撹乱され、攻撃にかかるコストが増える。

3. 考察

本章では、2 章で紹介した既存の欺瞞的防御とそれに関連する技術を分類し、欺瞞的防御の整理と Fake Honeypot の位置付けを明確化する。

表 1 Honeypot Detection の分類

目的	アプローチ	動的	静的
攻撃者の誘引・観測	ハニーポット	Honeypot Honeynet Sebek Honeypot	仮想環境のスナップショット
端末の希薄化	偽情報の保持・拡散	組織ネットワークにおける内部攻撃に対する模擬的欺瞞方式	HoneyAccount HoneyFile
疑わしい環境の隠蔽化	仮想環境の隠蔽		(Patch for VMware)
	ハニーポットの隠蔽	行動制限型ハニーポットの改良方法の提案・実装・運用	
侵入検知	侵入検知		HoneyFile HoneyAccount セキュリティ無効化攻撃を利用したマルウェアの検知と活動抑制手法の提案

表 2 Honeypot Detection の分類

目的	アプローチ	動的	静的
疑わしい環境の検出	ハニーポットの特性をもとにした検出	悪意のあるメッセージ受信可否 Honeypot Hunter	
	ハニーポットの種類をもとにした検出	行動制限による検出 対応する通信プロトコルメッセージによる検出	THPAmapによるポート状態の確認
	高負荷なシステムの検出	Sebekハニーポットの検出	Requestメッセージをブロードキャストすることで発生するRTTによる検出
	仮想環境の検出	VMware Hypervisor I/Oポートによる検出	仮想環境特有の値による検出 稼働中のプロセスとプロセスIDによる検出

欺瞞的防御

本節では、既存の欺瞞的防御を目的と手法、動的か静的かで分類を行う。欺瞞的防御はハニーポットと環境隠蔽技術、侵入検知技術の 3 つで構成される。The Honeynet Project?等で提供される HoneyAccount や HoneyFile は、本研究では侵入検知に分類した。これは、攻撃者の行動監視に用いられるハニーポットとは異なり、アカウント情報を盗み出した攻撃者を撹乱し、不正アクセスの抑制や不正アクセスが行われていることを検出していたからである。角丸らの研究は、これら 3 つの技術に該当せず、守りたい端末の存在を希薄化していることから、本項では”端末の希薄化”に位置付けた。

Honeypot Detection

本節では、既存の Honeypot Detection を疑わしい環境の検出に用いる 4 つの要素とリモートまたはローカル検出の 2 種類の観点で分類する。ハニーポットの特性をもとにした検出は、攻撃者を誘引するために持つ脆弱性や仕組みを利用している。そのため、悪意のあるメッセージの受信可否と Honeypot Hunter を分類した。ハニーポットの検出や仮想環境の検出に感汁技術は、本項で取り上げた技術以外にも多数存在する。これらは、仮想環境特有の情報やハニーポットで頻繁に使用されるサービスの稼動状態、要求に対する応答のタイムラグ等から判断されている。そのため、これらに対する欺瞞方法を検討する必要がある。

Fake Honeypot

本節では、既存の Fake Honeypot の分類を行う。既存研究では、欺瞞的防御と明示していた山田の研究を Fake Honeypot に分類した。これは、実際に動作する端末に向けて送信される要求に対し、情報を偽装して応答を行っているため、欺瞞的防御には分類しなかった。松本らの研究

© 2019 Information Processing Society of Japan

表 3　Honeypot Detection の分類

目的	アプローチ	動的	静的
攻撃者の撹乱	メッセージ送出	欺瞞を用いた能動的サイバー攻撃防御手法の提案と実装	
	偽情報の保持		Fake Honeypot:A Defensive Tactic for Cyberspace セキュリティ無効化攻撃を利用したマルウェア検知と活動抑止手法の提案

は、本物の端末で動作する偽のセキュリティプロセスを保持していることから、Fake Honeypot に分類した。また、偽のプロセスを無効化するマルウェアを検出することが可能であるため、欺瞞的防御の侵入検知にも分類している。

4. 提案手法

前章で行った分類の結果、本項では、攻撃者がハニーポットを検出・回避するために Honeypot Detection を使用することに注目した。攻撃者の行動を逆手に取り、実際の端末を Honeypot Detection に検出させることで攻撃の対象から外すことができると仮定し、その手法を提案する。

本章では、2.4 で分類した Honeypot Detection の各種に対し、Honeypot Detection に意図的に検出されるための機構を提案する。

4.1 ログ監視等の高負荷なアプリケーションをもとにした手法と種類に応じた手法に対する欺瞞

ハニーポットの検出要素として RTT を参考に判断している場合、何かしらの要求メッセージを受信した際に意図的に間隔をあけてから返答することで対応が可能である。しかし、意図的に RTT を長くすることで、悪意のない機器との通信に支障をきたす可能性がある。また、悪意のあるメッセージを利用する検出法に関しては、パケットをキャプチャし、実際には破棄するが偽のレスポンスを返すことで対応が可能である。この際、メッセージ作成の処理に時間を要しするが、ここで発生する RTT の増加によって疑わしい環境であると示すことができる。レスポンスが間違っている場合であっても、正確な返答ではないことから中-低対話型ハニーポットである可能性を示すことができる。

端末がメッセージを受信した際、RTT を増加または偽の応答を返答するために、ICMP や IP、TCP などの通信プロトコルの返答までに、意図的に間隔をあける機構が必要である。これら通信プロトコルの返答はカーネルが返答を行なっている。そのため、実装を行う際にはカーネルレベルで実装する必要がある。

図 1 には、RTT の遅延と間違った応答を返すプログラムの動作フローを示した。ネットワークからのメッセージを受信した際、メッセージのペイロード部と悪意のあるメッセージとの間でパターンマッチを行う。パターンマッチにより悪意があると判定した場合は、メッセージを破棄し、意味のないメッセージを返す。悪意がないと判断された場合は、プロトコルに則ってメッセージを作成、応答する。

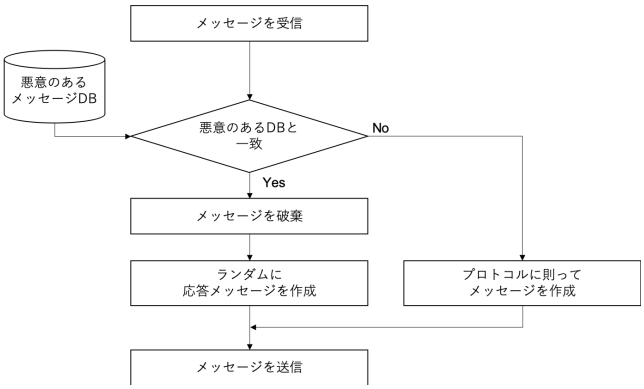

図 1　提案するカーネルモジュールの動作フロー

これにより、RTT の増加と意味のない応答を観測した攻撃者に対して、疑念を抱かせることができる。

4.2 Honeypot の特性と種類に応じた手法に対する欺瞞

攻撃者が対象の端末への侵入に成功し、端末を操作する際、通常とは異なる応答や利用不可能な入力の存在を知ることでハニーポットと判断し攻撃を止めると予想する。本項では、実際の端末を低対話型ハニーポットのようにふるまわせるために、入力に対して定期的に誤った返答を行う。

この機能の実装における課題は、正規のユーザが使用する際の可用性である。この欺瞞機構を導入した中で高い可用性を求める場合、不正アクセスの検出が必須となるが、不正アクセスを検知した場合の最善行動は端末をネットワークから隔離することであるため、欺瞞することが最善ではない。そのため、攻撃者が端末に侵入した後に不正確な結果を観測した際、どのような行動をとるのかの把握するために検証実験を行う。

4.3 仮想環境特有の情報をもとにした手法に関する欺瞞

本研究では、WMware 環境を想定する。VMware 環境で仮想環境特有の情報を確認する方法として、マジックナンバーと VMware Hypervisor I/O Prot を用いて VMware の存在を検出する方法がある (図 2)。VMware 製品では、ゲスト OS とホスト OS 上の VMware が通信を行う際、VMware に指定された I/O ポートを通じて通信している。その際は、マジックナンバーとコマンドを含むアセンブリデータで通信している。本項ではこれに注目し、攻撃対象から外すことを目的として、VMware に指定された I/O ポート宛に作成される VMware バージョン確認メッセージをカーネル上で検出し、正規の応答に似せた偽のバージョンデータを作成、送出するカーネルモジュールを作成することを提案する。その概念を図 3 に示す。

5. まとめ

本項では、欺瞞的防御とそれに関係する既存技術を分類し、Fake Honeypot を利用した欺瞞的防御の提案を行

© 2019 Information Processing Society of Japan

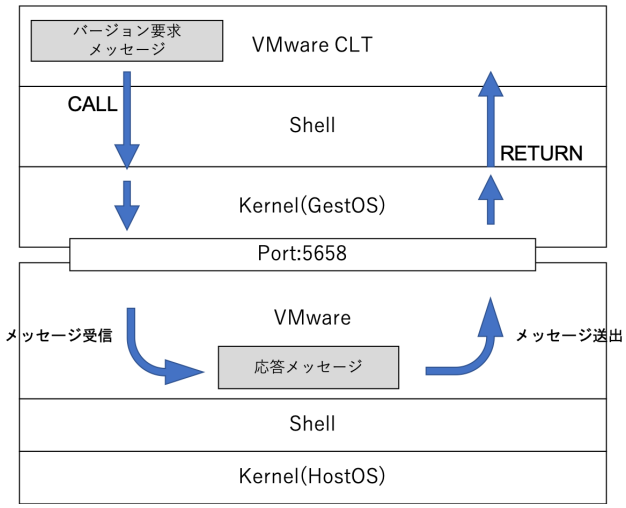

図 2 VMware 検出プログラムの動作フロー

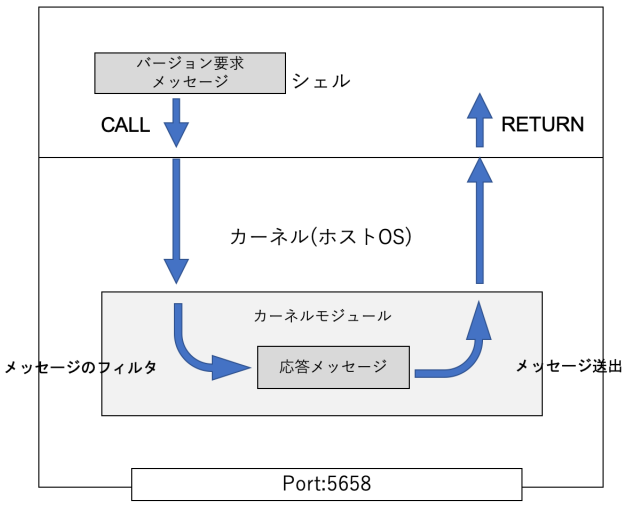

図 3 提案する VMware 検出プログラムを騙すカーネルモジュールの動作フロー

なった。欺瞞的防御を分類することで、既存研究の欺瞞と Honeypot Detection の目的や位置付けを明確化した。また、Honeypot Detection が行う動作を整理することで、Fake Honeypot を利用した欺瞞的防御の方向性をまとめることができた。

欺瞞的防御を行う上で、仮想環境やハニーポットを隠蔽化する技術に加え、欺瞞的防御に対抗する Honeypot Detection のような技術が存在していた。また、Honeypot Detection を騙すための方向性として、守りたい端末自体をハニーポットのように見せる Fake Honeypot も存在し、それぞれの技術が関係し合っていた。また、分類と提案の結果から、欺瞞的防御は攻撃対象となった組織が将来の対策として利用することに適しているのではないかと考える。

参考文献

[1] 独立行政法人情報処理推進機構: IPA テクニカルウォッチ 新しいタイプの攻撃に関するレポート, https://www.ipa.go.jp/about/technicalwatch/20101217.html. (2019 年 5 月 13 日閲覧).

[2] 貴洋角丸，成佳　島，正文渡部，克成吉岡: 標的型攻撃対策に向けた欺瞞機構を用いた防御アーキテクチャ (情報通信システムセキュリティ)，電子情報通信学会技術研究報告 = IEICE technical report : 信学技報， Vol. 114, No. 117, pp. 69–74（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110009945908/⟩ (2014).

[3] 貴洋角丸，成佳　島，克成吉岡: 組織ネットワークにおける内部攻撃に対する模擬的欺瞞方式，コンピュータセキュリティシンポジウム 2014 論文集，Vol. 2014, No. 2, pp. 735–742 (2014).

[4] 直人谷本，毅　八木，剛男針生，光恭伊藤: 複数のドメインに配置されたハニーポットを用いた Web サイトへの攻撃の実態調査，電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ : IEICE technical report， Vol. 109, No. 476, pp. 25–28（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110007999842/⟩ (2010).

[5] 隆宏松木, 悠　新井, 真敏寺田, 範久土居: セキュリティ無効化攻撃を利用したマルウェアの検知と活動抑止手法の提案, 情報処理学会論文誌, Vol. 50, No. 9, pp. 2127–2136（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110007970499/⟩ (2009).

[6] VMware: VMware, https://www.vmware.com/jp.html. (2019 年 5 月 13 日閲覧).

[7] THC-Amap: THC-Amap, https://sectools.org/tool/amap/. (2019 年 5 月 13 日閲覧).

[8] Sebek: Honeypot Project, http://old.honeynet.org/tools/sebek/. (2019 年 5 月 13 日閲覧).

[9] VMware: Mechanisms to determine if software is running in a VMware virtual machine (1009458), https://kb.vmware.com/s/article/1009458. (2019 年 5 月 13 日閲覧).

[10] Rowe, Duong and Custy: Fake Honeypots: A Defensive Tactic for Cyberspace, *2006 IEEE Information Assurance Workshop*, pp. 223–230 (online), DOI: 10.1109/IAW.2006.1652099 (2006).

[11] 山田　大: 欺瞞を用いた能動的サイバー攻撃防御手法の提案と実装 (2016).

© 2019 Information Processing Society of Japan