仮想計算機を利用したウイルスの捕獲解析システム

柴田 良子
千葉大学大学院自然科学研究科

今泉 貴史
千葉大学総合メディア基盤センター

インターネットの発展には、多くのユーザーが安心して利用できる環境が必要である。しかしネットワークを介した犯罪は増加しており、大きな社会問題となっている。特にネットワーク上でコンピュータウイルスが蔓延した場合、ネットワークを麻痺させ、業務に大きな支障をきたしてしまう。ネットワーク上からウイルスを完全に除去するためには、ウイルスの活動による影響を調査する必要がある。

そこで本稿では、ウイルスを詳細に解析するためのシステムを構築し、評価する。本システムは、ネットワーク上で活動するウイルスを捕獲し、安全な環境で解析するためのシステムである。本システムを利用することで、ネットワーク上に存在するウイルスの捕獲を行ったり、疑わしいファイルのウイルス検査及び解析を行うことができる。

Virus Analyzing and Capturing Environment built on Virtual Machines

SHIBATA Ryoko
Graduate School of Science and Technology,
Chiba University

IMAIZUMI Takashi
Institute of Media and Information Technology,
Chiba University

We need secure network environment for further evolution of the Internet. However, the crimes over the network are increasing and cause a big social problem. When a computer virus infects a lot of computers over a network, users on the network can not exchange messages, and it is difficult to continue the business. In this case, it is necessary to remove the virus from the network completely and to investigate the influence by activity of the virus.

In this paper, we construct a system for analyzing a virus in detail, and evaluate the system. This system helps us capture the virus which works on a network, and analyze it in a safe environment. Using this system, we can analyze the virus which exists on a network, and inspect and analyze suspect files.

1 はじめに

1.1 背景

近年、パソコンのセキュリティ対策は進歩し、ネットワークを守るためのセキュリティシステムも、堅牢なものとなっている。しかし、コンピュータウイルスやワームによる被害は年々拡大している。その理由として、複数の感染ルートを持つことなどによるウイルスの感染力の強さや、ゼロディ・アタックなどが挙げられる。

ゼロディ・アタックとは、ソフトウェアの脆弱性が公表されると同時に攻撃プログラムが出回ってしまうタイプの攻撃である。このような攻撃は、脆弱性に対する対策期間が短いほど、対策の徹底はむずかしい。ウイルスが先に出回ってしまうと、いかに最新のパッチ、最新のウイルス対策ソフト用パターンファイルを適用していても、そのウイルスには対抗できず、無防備になってしまう。

またセキュリティ対策が万全でないパソコンを外部から持ち込みネットワークに接続すると、ウイルスの蔓延によってネットワークが麻痺してしまう可能性がある。ネットワーク型セキュリティモデルの場合、ファイアウォールは外部から内部ネットワークへの攻撃に対しては有効であるが、内部で起こる攻撃には対処することができないからである。この具体的な例としてSlammerやBlasterなどが挙げられる。

1.2 研究の目的

このような背景を踏まえると、既知ウイルスの検出が主な目的であるウイルス対策ソフトだけでは、コンピュータやネットワークのセキュリティを確保することは不可能である。

そこで本研究では、「ネットワーク上で不正な動きをするプログラムを収集し、それを安全な環境で解析するシステム」を構築する。本システムの主な機能は以下の２つである。

1. ネットワーク上に存在するウイルスを収集し、システム内に捕獲する
2. 捕獲したウイルスを安全な環境で解析する

本システムを利用することで、ネットワーク上に存在するウイルスの解析を行ったり、疑わしいファイルのウイルス検査及び解析を行うことができる。

コンピュータやネットワークを攻撃する不正プログラムをその活動をもとに分類すると、ウイルスのほか、ワーム、トロイの木馬の3つに分かれる。現在、複合型ウイルスがウイルスの主流として猛威を振るっていることをふまえ、本論文では「他のプログラムに感染するプログラム」である狭義のウイルスだけではなく、ワームも含めてウイルスとして扱う。

2 提案システムVACEの概要

提案するシステム VACE (Virus Analyzing and Capturing Environment) は、仮想計算機を用いて、仮想的なネットワーク環境を構築したウイルスの捕獲及び解析を行うためのシステムである。VACE を実現するために仮想計算機を用いる利点は2つある。第一に、1つの計算機で実際のネットワークと同様の環境を構築できる点である。よって移動性に優れたシステムを構築でき、様々な場所でシステムを利用することができる。第二に、ハードディスクに対する変更を無効化することが可能な点である。よって各仮想計算機の状態をウイルス感染前の状態に戻すことができるので、ウイルスに感染しない仮想的な実行環境を実現することができる。

VACE は、捕獲フェーズと解析フェーズの2つのフェーズをもつ。まず捕獲フェーズでウイルスを収集し、システム内に捕獲する。その後解析フェーズに切り換えて、安全な環境でウイルスを解析する。

2.1 VACEの構成

VACE は計算機の中に仮想的なネットワークを構築し、そこに4台の仮想計算機を設置する。

VACE の構成を図1に示す。

SG (System Gateway) 実ネットワークとシステム内ネットワークの境界に位置し、実ネットワーク上のウイルスを DM に転送する。さらに仮想ネットワーク内に存在するウイルスによる攻撃が実ネットワークに及ばないようにする。

DM (Decoy Machine) 実ネットワーク上からウイルスを捕獲したり、実行したりする。

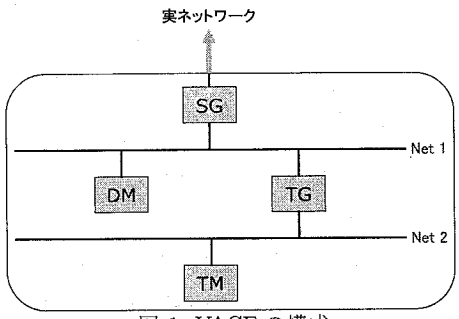

図 1: VACE の構成

TG (Transfer Gateway) DM で実行したウイルスによる攻撃を記録し、TM へ転送する。パケットを処理する際にパケットの情報を記録する。

TM (Target Machine) ウイルスが攻撃対象とするサービスを実現することにより、仮想インターネット機能を提供する。各サービスでは、通信内容を記録する。

2.2 捕獲フェーズ

VACE を実ネットワークと接続し、実ネットワーク上で活動するウイルスを収集し、システム内に捕獲する。ウイルスの捕獲方法には、ダイレクトモード、ブリッジモード、ステーションモードの3通りある。捕獲フェーズでは、SG、DM の2つの計算機が動作する。

ダイレクトモードは、ウイルスファイルまたは、疑わしいファイルを外部媒体から直接入手するモードである。主にメールの添付ファイルとして受信したファイルや、計算機内に存在している疑わしいファイルの検査を目的として捕獲する。

ブリッジモードは、システムがブリッジとして動作するモードである。VACE をゲートウェイとスイッチの間に接続して、実ネットワーク上に流れているパケットを調べる。まず SG で収集したパケットを調べ、パケット内に疑わしいキーワードやプログラムコードが含まれていないか検査する。検査によりウイルスの可能性があるパケットを発見した場合、SG はパケットを再構成して DM に転送する。

ステーションモードは、システムをスイッチに接続して動作するモードである。VACE をスイッチに接続し、通常は一般の端末のふりをして存在する。ステーションモードでは、主にネットワーク上の計算機に対して攻撃するウイルスの捕獲を目的とする。SG

が実ネットワーク上からの通信開始を検知すると、通信を行いながら動作を監視する。ウイルスの可能性がある通信があった場合、SGはファイアウォールのNAT機能を利用してDMにパケットを転送する。よって実際に実ネットワーク上の計算機と通信するのはDMである。SGでパケットフィルタリングを行うことにより、DMで捕獲したウイルスによる攻撃が外部に及ばないようにする。

2.3 解析フェーズ

VACEを実ネットワークから切断し、閉じたネットワーク環境の中でウイルスを解析する。解析フェーズでは、DM、TG、TMの3つの計算機が動作する。ウイルスの解析方法には、スタティックモード、ダイナミックモードの2通りある。

スタティックモードは、ウイルス、又は疑わしいファイルをプログラム解析ツールなどを用いて静的に解析する。ファイル内にウイルスの可能性があるプログラムコードが含まれていないか検査する。

ダイナミックモードは、ウイルス、又は疑わしいファイルをDMで実行し、ウイルスに感染した計算機の動作を解析する。実行したウイルスがネットワーク上の計算機に対して攻撃を行う場合、そのパケットはデフォルトゲートウェイであるTGに配送される。TGでは、その攻撃パケットのログを取り、パケットの宛先に関わらずすべてTMに転送する。パケットを受け取ったTMでは、ウイルスが攻撃対象とするサービスを実現することにより、仮想インターネット機能を提供する。各サービスでは、通信内容を記録する。

ダイナミックモードの動作を図2に示す。

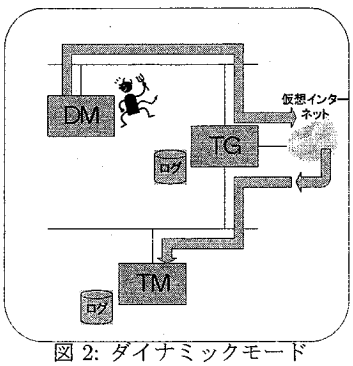

図2: ダイナミックモード

3 VACEの実現

VACEを実装するホストマシンは、ノート型の計算機で、CPUはPentium III 750MHz、メモリは496Mbyte、OSはWindowsXP Home Editionである。またネットワークインタフェースを2つもつ。ホストマシンでVMware Workstation4.5を使用して、仮想ネットワーク及び仮想計算機を実現する。DMにはウイルスに感染する可能性が高いOSとしてWindowsXPを、SG、TG及びTMには、ウイルスに感染する可能性が低いOSとしてFreeBSDを使用した。現在Windowsを感染の対象としたウイルスが多いため、DMでは今回WindowsXPを用いたが、必要に応じて、その他のOSを使用して実現することも可能である。

仮想計算機SGの実ネットワークとの接続には、VMwareのブリッジネットワークを利用する。ブリッジネットワーク接続により、仮想計算機は外部ネットワークに一般の計算機と同様に独立した計算機として存在し、独自のIPアドレスをもつ。よって仮想計算機はネットワーク上の実計算機にアクセス可能であり、またネットワーク上の実計算機から仮想計算機にもアクセス可能である。このとき、ホストマシン自体が実ネットワーク上に存在するウイルスの攻撃を受けないようにするために、ホストマシンにはIPアドレスを付けないでおく。

3.1 捕獲フェーズ

3.1.1 ブリッジモード

ブリッジモードのネットワーク構成を図3に示す。SGはVMwareのブリッジネットワークにより、ホストOSが接続している実ネットワーク上の計算機として存在する。

3つのネットワークインタフェースを持ち、2つのインタフェースはVMwareのブリッジネットワークを用いて実ネットワークと接続する。3つのインタフェースすべてをブリッジとして動作するように設定し、IPアドレスは付与しない。実ネットワーク上に流れているパケットをブリッジしながら中身を調べ、疑わしいパケットを発見したらログに保存する。

またDMのデフォルトゲートウェイのIPアドレスを192.168.11.1/24に設定する。よって捕獲フェーズの際はルータが、解析フェーズの際はTGがデフォルトゲートウェイとなる。

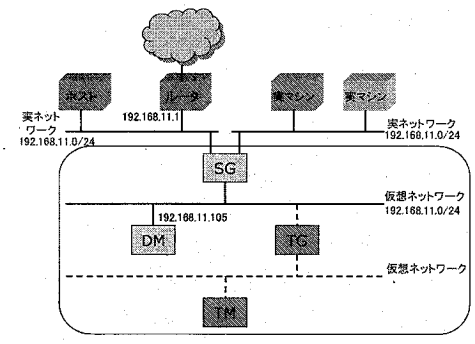

図 3: ブリッジモードのネットワーク構成

3.1.2 ステーションモード

ステーションモードのネットワーク構成を図 4 に示す。SG は VMware のブリッジネットワークにより、ホスト OS が接続している実ネットワーク上の計算機として存在する。

2 つのネットワークインタフェースを持ち、1 つのインタフェースは VMware のブリッジネットワークを用いて実ネットワークと接続する。2 つのインタフェースにはそれぞれ IP アドレスを設定し、実ネットワークを外部ネットワークとして NAT を行う。パケットの転送には NAT のオプション redirect_address を使用する。これは公式な IP アドレスへのパケットの流れを、ローカルネットワーク内のマシンにリダイレクトするオプションである。以下のように設定することで、SG の実ネットワーク側のインタフェースに対する接続をすべて DM に転送する。

redirect_address 192.168.11.4 192.168.200.5

また DM のデフォルトゲートウェイの IP アドレスを 192.168.200.2/24 に設定する。よって捕獲フェーズの際は SG が、解析フェーズの際は TG がデフォルトゲートウェイとなる。

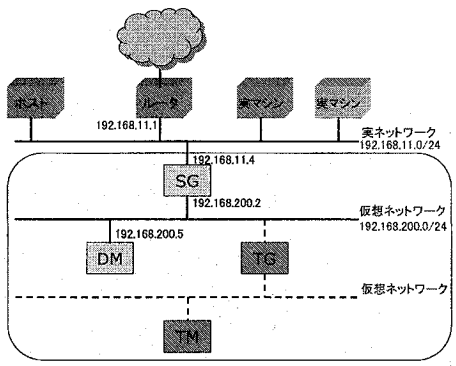

図 4: ステーションモードのネットワーク構成

3.2 解析フェーズ

3.2.1 スタティックモード

現在のところ、既存のウイルス対策ソフトを用いてファイルの解析を行っている。

3.2.2 ダイナミックモード

ダイナミックモードのネットワーク構成を図 5 に示す。DM で実行したウイルスによって送信されたパケットは、デフォルトゲートウェイである TG に転送される。TG では受け取ったパケットを、宛先に関わらずすべて TM に転送する。TG 及び TM の実現についての詳細は以下のようになる。

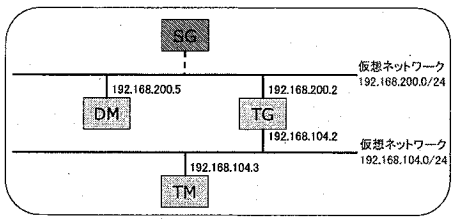

図 5: ダイナミックモードのネットワーク構成

TG では DM から送信された任意の宛先へのパケットを TM へ転送し、その内容をログとして記録する。この機能を実現するために、パケットフィルタと NAT の機能を使用した。

パケットフィルタで受け取ったパケットは、DIVERT ソケットを通じて NAT 機構に送られる。NAT 機構では target_address というオプションを使用する。target_address は、既存のリンクとは関連付けられていない入力パケットが到着したとき、指定されたアドレスにパケットを転送するオプションである。このオプションで TM の IP アドレス (192.168.104.3) を指定することで、パケットの宛先にかかわらず TM にパケットを転送することができる。オプションを適用後、処理はパケットフィルタへ戻り、該当パケットは TM へ転送される。

TM からのパケットも同様にして、DIVERT ソケットを通じて NAT 機構に送られる。NAT 機構で DM が送信したパケットに対する応答パケットであることを認識すると、処理はパケットフィルタへ戻り、該当パケットは DM へ転送される。

TM ではウイルスが攻撃対象とするサービスを実現することにより、任意の宛先へのパケットを受信し

て仮想インターネット機能を提供する。実現するサービスは、SMTP、HTTP、TELNET、FTP、DNSである。それぞれのサービスでは後で解析することが可能なように、通信内容を記録する。

解析手順

動的解析の手順は以下の通りである。

1. ウイルス実行の前に以下の準備を行っておく。
   - メールソフトのアドレス帳にダミーのメールアドレスを登録する
   - メールアドレスを含む内容のファイルを複数用意し、計算機内に置く
2. ダイレクトモードを使用してDMでウイルスを実行する。
3. ウイルスの発病には日付などの条件を要するものもあるので、仮想計算機の時刻を段階的に進める。
4. TG、またはTMのログへ書き込みが発生した時点で、ウイルスプログラムであると判断する。
5. ログを解析し、攻撃内容を調べる。
6. すべての仮想計算機を終了し、DMを感染前の状態に戻す。

4 評価

4.1 動作の確認

W32/Klez.H@mmとW32.Welchia.Wormを用いて、実際にシステムの動作を検証した。

W32/Klez.H@mm ウイルスは計算機内で収集した数十件のメールアドレスに対し、自分自身を添付したメールを送信した。またメールの送信元アドレスは、計算機内に存在するメールアドレスで偽造をしていた。さらに受信者のSMTPサーバへ直接接続を行っており、独自のSMTPエンジンを使うことがわかった。妨害活動としては、ウイルス対策ソフトのリアルタイム監視や、タスクマネージャを強制終了するなどの行為を行っていた。

W32.Welchia.Worm ウイルスを実行したところICMPエコー要求パケットを送信した。ウイルス実行計算機のアドレスをa.b.c.dとすると、送信先アドレスは、a.b.0.0から1ずつ値を増やしながら、連続してパケットを送信する。そのエコー要求に対し、TMが偽の応答をすると、応答したアドレスのTCP135番ポートに対してさらにパケットを送信した。

4.2 考察

4.2.1 VACEの動作

今回用いたウイルスは実際には既知のものであるが、VACEを構築する際にウイルスの特徴を考慮したわけではなく、本システムにおいては未知ウイルスとして扱うことが可能である。よってVACEは、未知ウイルスに対しても有効なシステムである。

また既知ウイルスをシステム上で実行し、新たな活動を発見した場合は、その行為をウイルスの活動の一つとして登録できる。さらに、実際にウイルスに感染してしまった計算機上に存在するウイルスプログラムを本システム上で実行することで、そのウイルスプログラムが計算機やネットワーク上に与えた影響を探索できる。ウイルスを計算機やネットワークから除去する際に、この情報を利用できる。

しかし問題点も見つかっている。ウイルスがSMTP、HTTP、TELNET、FTP、DNS以外のサービスを使って攻撃を行った場合には、パケットの送信先や送信元、使用したプロトコルの情報は得られるが、攻撃内容を詳しく探索できない点である。現在は、ネットワークを介して感染するウイルスは、SMTPやHTTPのサービスを使うものが多いが、今後他のサービスを利用したものも出現することが予測される。よって今回実装した以外のサービスも実装する必要があると考える。

4.2.2 ウイルス対策ソフトとの比較

ウイルス対策ソフトは、主に既知ウイルスに含まれるプログラムコードをデータベース化し、そのデータベースと計算機内に存在するファイルのパターンマッチングをリアルタイムで行うことにより、ウイルスの検出を行っている。

これに対しVACEは、リアルタイムではないが、ネットワーク上で活動するウイルスを様々な手法で捕獲し、それを解析するシステムである。ウイルスを安全なネットワーク環境で実行することができるので、ウイルスの計算機内での動作や、ネットワーク上に与える影響を詳細に解析することができる。

4.2.3 VMwareへの依存

本システムはVMware Workstaion上で動作するシステムである。現在のところVMwareを動作させているホストマシンへは、ウイルス感染の恐れはない。しかし将来ホストマシン上のOSを攻撃するウイルスが登場した場合、ホストマシン自体が感染してしまうという問題がある。しかし、実際の計算機やVMware以外のエミュレータを利用して本システムを構築することで、問題を解決できると考える。

4.2.4 関連研究

未知ウイルス検知システム[1][2]は、仮想マシンとその閉じたネットワーク内でウイルスを実行し、その行動パターンを観測することによって未知ウイルスの検知を行うシステムである。

このシステムでも、動作確認としてKlezウイルスを用いた実験を行っている。しかしウイルスを実行した仮想計算機と同じネットワーク上に、SMTPサーバ実装計算機を設置していたため、受信者のSMTPサーバに直接接続して電子メールを送信しようとする、Klezウイルスのウイルスメールを取得することができなかった。

しかし本研究では、Klezウイルスを用いた実験で電子メールの送信行為を検出し、送信したメールの情報を収集できた。検出成功の理由として、DNSサーバを実装したこと、ファイアウォールを構築したことがあげられる。DNSサーバを実装したことで、メール転送の際にウイルスプログラムが指定したSMTPサーバを解析することが可能である。またTMでNATの機能を利用したことにより、DMから送信されたパケットをすべてTMへ転送することができる。よってウイルスがネットワーク上に送信したパケットをすべて解析することが可能である。

VM Nebula[3][4]は、仮想PCとVLANを利用した不正アクセス等に関する再現・模擬実験環境である。この再現実験環境は、仮想PCを実行する複数台のサーバとそれらをつなぐマルチレイヤスイッチ、実験環境のイメージを格納・配布するためのライブラリサーバから成っている。複数の計算機とVMware GSX serverを利用しているため、約100台の仮想PCを同時実行することができる。

しかし、外部のネットワークとは接続されていない閉じた環境であるため、ウイルスの検体は手動でVM Nebula環境内に持ち込む必要がある。また環境自体は複数の計算機で構成されているため、実験環境を簡単に移動することができない。

これに対してVACEは、実ネットワークからのウイルス捕獲を行っており、ネットワークで活動しているウイルスをリアルタイムで収集し、解析することができる。よって捕獲及び解析対象をウイルスやワームに限定することなく、不正アクセスなどにも応用できる。またVACEは一つの計算機で構成できることから、移動性に優れている。よって様々なネットワークに存在するウイルスを捕獲し、解析することができる。

5 おわりに

本稿では、ウイルスを詳細に解析するためのシステムの構築について述べ、評価を行った。本システムを利用することにより、ネットワーク上で活動するウイルスを捕獲し、安全な環境で解析することができる。

現在、解析フェーズについては実装済みであり、実在するウイルスを用いて実験を行った[5]。捕獲フェーズについては、ブリッジモードとステーションモードをある程度実現しており、実ネットワークと接続して動作の確認を行っている。

今後の課題として、疑わしいパケットの転送機構の構築、ログの自動解析などが挙げられる。さらに対象をウイルスやワームに限定せず、不正アクセスを含めて捕獲及び解析できるシステムの実現方法について検討する。

参考文献

[1] 三宅 崇之, 白石 義明, 森井 昌克. 仮想サーバを使った未知ウイルス検知システムの提案. 情報処理学会研究報告, CSEC, vol 18, pp.45-52, 2002.

[2] 神薗 雅紀, 白石 義明, 森井 昌克. 仮想ネットワークを使った未知ウイルス検知システム. 情報処理学会研究報告, CSEC, vol 22, pp.113-120, 2003

[3] 三輪 信介, 滝澤 修, 大野 浩之. 仮想PCによるインターネットセキュリティ実験環境『VM Nebula』の設計と構築. 電子情報通信学会, 暗号と情報セキュリティシンポジウム(SCIS), 2003.

[4] 三輪 信介, 大野 浩之. 再現実験環境『VM Nebula』を用いたウィルス・ワームの解析. インターネットカンファレンス論文集, pp.67-75, 2003.

[5] 柴田 良子, 今泉貴史. 仮想計算機を利用したウイルスの影響探索システム. 日本ソフトウェア科学会第20回大会, 2003.