1ZD-01

マイクロ VM を活用した動的活動観測システムの検討

鈴木克拓　　寺田真敏
東京電機大学

1. はじめに

アクティブサイバーディフェンスの考え方のもと，攻撃者の活動を観測する Cyber Deception が注目されており，著者らは，動的活動観測システム[1]を通して，攻撃者の活動を観測する活動を進めている．

本研究は，アプリケーション単位に仮想マシンを作成し隔離実行する手法であるマイクロ VM を活用することで，攻撃者の活動を観測する動的活動観測システムの利用の範囲拡大を目的としている．本稿では，マイクロ VM を活用した動的活動観測システムの構想と共に，試行的に構築した動的活動観測システムの概要について報告する．さらに，構築した動的活動観測システムを利用し，攻撃者と観測者視点からマイクロ VM を活用した動的活動観測システムを検証する．

2. 関連研究

2.1 動的活動観測

Cyber Deception とは，ネットワーク内におとりサーバやハニーポット等を設置し，攻撃者を誘導してその手口の情報を収集したり，攻撃活動を遅らせたりすることを意味する．Cyber Deception 構築については，国立研究開発法人情報通信研究機構(NIST)が 2017 年にサイバー攻撃誘引基盤 STARDUST を発表しており[2]，基盤としての有効性や改善点なども検討されている[3]．攻撃者の活動観測を通したサイバー攻撃活動分析については，2014 年から動的活動観測 BOS(Behavior Observable System)とその研究用データセットとして報告されており，この中で 2017 年から観測基盤としての STARDUST 利用について言及している[4]．

2.2 解決したい課題

著者らは，STARDUST を大学ネットワークと一体化し，サイバーセキュリティ対策教育プログラムの一環として動的活動観測を実施している[1]．一方，多くの動的活動観測を実施するためには，多くの観測基盤が必要となる．本研究では，Cyber Deception による動的活動観測を普及するために，マイクロ VM を活用することで，この課題解決に取り組むこととした．

3. マイクロ VM を活用した動的活動観測

本章では，マイクロ VM を活用した動的活動観測システムについて述べる．

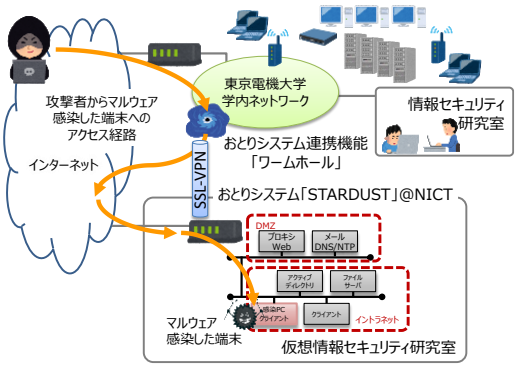

図 1　大学ネットワークへのおとりシステムの組み込み

3.1 マイクロ VM＋仮想ハニーネット経由方式

BOS で採用している動的活動観測環境は，システムそのものが組織内ネットワークを模擬しており，感染 PC は，システムの一部として実装されている(図 1)．この場合，新たなマルウェア検体を感染 PC で実行するたびに，システム全体を観測初期状態にリセットする必要がある．マイクロ VM を活用した動的活動観測は，感染 PC と組織内ネットワークとを分離することで，おとりシステム内の組織内ネットワーク部の効率的な共用化を図るアプローチである(図 2)．

具体的には，マイクロ VM は，PC 内部でアプリケーション単位に仮想マシンを作成し隔離実行する手法で，図 2 のマイクロ VM そのものが感染 PC という位置付けになる．さらに，インターネット接続にあたり，おとりシステム内の組織内ネットワーク部(以下，仮想ハニーネット)を経由することで，感染 PC と仮想ハニーネットとの独立性を確保しつつ，仮想ハニーネットの共用を実現する．

3.2 試行的な動的活動観測システムの構築

本節では，3.1 節のアプローチの実現性を確認するために構築した環境について述べる．

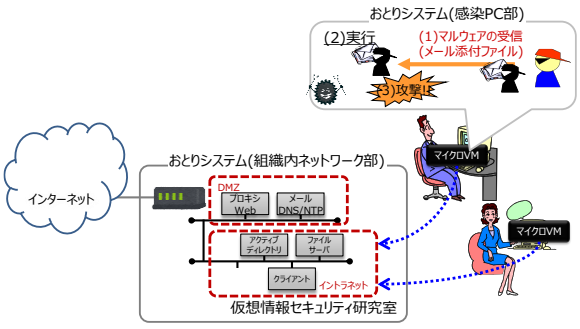

図 2　マイクロ VM＋仮想ハニーネット経由方式

Feasibility Study on Behavior Observable System using microVM
KATSUHIRO SUZUKI and MASATO TERADA, Tokyo Denki University

3.2.1 システム要件

試行的な動的活動観測システムの構築にあたり，設定した要件を示す．

要件 1　マイクロ VM から端末のホスト OS へ攻撃はできない．

要件 2　マイクロ VM とインターネットの間に設置する仮想ハニーネットからは，インターネットにのみアクセスできる．

要件 3　マイクロ VM からは，仮想ハニーネットとインターネットにのみアクセスできる．

3.2.2 システム構成

構築した動的活動観測システムの構成を図 3 に示す．

(1) マイクロ VM セグメント

おとりシステムの感染 PC 部に相当するマイクロ VM を動作させる端末を接続するセグメントである．なお，マイクロ VM については，HP sure click pro[5]を使用し構築した．

(2) 仮想ハニーネットセグメント

おとりシステムの組織内ネットワーク部を再現するセグメントで，組織内サーバ群として Web サーバを配置した．

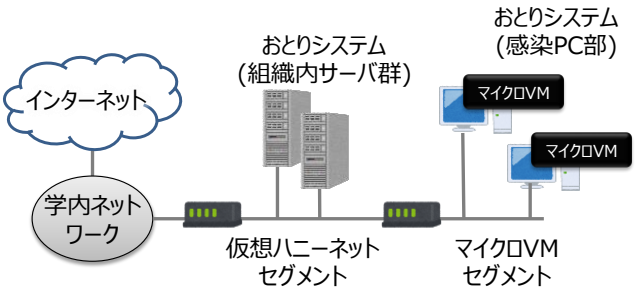

図 3　動的活動観測システム

3.3 システムの動作確認

システムの動作確認においては想定した要件を満たしていることを確認した．本章では，動作確認結果を元に，攻撃者と観測者視点から動的活動観測システムの構築ならびに運用上の留意点について述べる．

3.3.1 攻撃者視点

攻撃者視点では，動的活動観測システムを構成するマイクロ VM と仮想ハニーネットがどのような環境に見えるのかを中心にまとめておく．

(1) マイクロ VM

構築に使用したマイクロ VM が作成するアプリケーション単位の仮想マシンは，Windows PC そのものを模擬し，さらに端末のホスト OS に付与されているホスト名を使用するなど，攻撃者に特殊な環境であると悟られない工夫がされている．その一方，セキュリティ確保のために，疑似的なフォルダ構成やコンテンツを使用しており，特殊な環境であると悟られてしまう可能性は残っている．

(2) 仮想ハニーネット

構築に使用したマイクロ VM では，セキュリティ確保のためにポートを Web 系アクセスに制限をしている．このため，攻撃者による仮想ハニーネットへの攻撃については，Web サーバを想定した組織内サーバ群の配置が必要となり，感染 PC から仮想ハニーネットへの誘導方法についても工夫が必要となる．

3.3.2 観測者視点

観測者視点では，感染 PC 部にマイクロ VM を利用すること，感染 PC と仮想ハニーネットとに分離することの効果について述べる．

(1) マイクロ VM の利用について

アプリケーション単位に仮想マシン化することによって，アプリケーションを起点としたプロセス操作グラフを作成できるため，感染 PC における攻撃者の初動活動を把握しやすくなる(図 4).

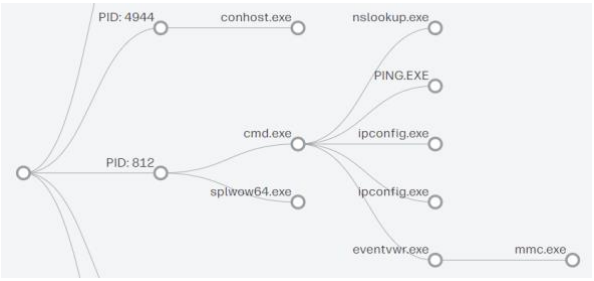

図 4　攻撃者によるマイクロ VM 上でのプロセス操作例

(2) 感染 PC と仮想ハニーネットとの分離の効果について

組織内ネットワークを模擬したおとりシステムの場合，システム内への検体移動を伴う投入などの操作が必要であった．マイクロ VM を活用し，分離することで，手元の端末で検体実行が可能となり，検体実行までを操作時間を短縮できる効果がある．

4. おわりに

本稿ではマイクロ VM を活用した動的活動観測システムの構想と共に，試行的に構築したシステムの動作確認を通して実現性を検証した．試行的に構築した環境は，制約があるものの，Web 系アクセスを主体としたサイバー攻撃を対象とした動的活動観測が可能であることを確認した．今後は課題の整理を通して，検討したシステムを実環境で稼働できるよう整備を進めるとともに，マイクロ VM を活用した動的活動観測システムを用いた観測を進めていく予定である．

謝辞

本研究を進めるにあたり有益な助言と協力をコいただいた株式会社日本 HP ならびに関係各位に深く感謝致します．

参考文献

[1] 松井紘大ほか：学内 CSIRT と連携した学生自主運用型マルウェア対策教育プログラムの提案，情報処理学会論文誌，Vol.63, No.12, p.1716-1725 (2022).

[2] 津田侑ほか：サイバー攻撃誘引基盤 STARDUST，コンピュータセキュリティシンポジウム 2017 (2017).

[3] 水口喬詔ほか：サイバー攻撃誘因基盤「STARDUST」の検証，コンピュータセキュリティシンポジウム 2019 (2019).

[4] 寺田真敏ほか：サイバーセキュリティ対策のための研究用データセット「動的活動観測 2014～2017」，情報処理学会論文誌，Vol.60, No.12, pp.2211-2222 (2019).

[5] HP Wolf セキュリティ - HP sure click pro, https://jp.ext.hp.com/business-solution/endpoint_security/, 2023 年 12 月 29 日参照