仮想ネットワークの動的構成による侵入活動観測システムの提案

ファン スォン ホアン[1]　中村 康弘[2]

概要：近年，特定の個人や組織を狙ったサイバー攻撃は手口が巧妙化しており，様々なの手段を組み合わせて多様化している．攻撃する際にはマルウェアが組織のネットワークへ不正侵入した後，水平展開という組織内部ネットワークに感染を拡散させていくが，完璧な防御対策を実現することは困難であるため，被害を最小限に抑えるためにはマルウェアに侵入されても素早く検知し，侵入後の挙動を収集しておくことが重要である．従来では組織内ネットワークを模擬するシステムで侵害活動を観測するが，構成したネットワーク環境は固定であり，全ての水平展開手法を観測できるとは限らない．そこで，外部ネットワークの攻撃者からの接続要求を観測した結果に基づいてネットワーク構成を動的に変更する目的として，本研究では Docker を用いて侵入させるホストを仮想プライベートネットワーク環境内で実現することで，侵入してきた攻撃者の侵入後の挙動を観測するシステムを提案・評価する．

キーワード：Docker, 侵入挙動, 動的構築, 仮想ネットワーク, コンテナ

Dynamically Configuring Virtual Network to Observe Intrusion Activity

Hoang Xuan Pham[1]　Yasuhiro Nakamura[2]

Abstract: In recent years, cyberattacks targeting specific individuals and organizations have become more sophisticated and diversified by combining various means. When attacking, malware spreads to the organization's network and then spreads the infection to the organization's internal network called lateral movement, but it is difficult to realize perfect defense measures, so the damage is minimized. To suppress it, it is important to quickly detect malware intrusion and collect post-intrusion behavior. Although in the past, infringing activities are observed by a system that simulates an in-house network, the configured network environment is fixed, and not all lateral movement methods can be observed. Therefore, to dynamically change the network configuration based on the observation result of the connection request from the attacker of the external network, in this research, by using Docker, a host to be intruded is realized in the virtual private network environment. Propose and evaluate a system to observe the post-invasion behavior of an attacker who has intruded.

Keywords: Docker, Intrusion behavior, Dynamic construction, Virtual network, Container

1. はじめに

近年，インタネットを介したサイバー攻撃が活発になっており，重要なファイルの流出，個人情報漏洩，フィッシングといった大きな脅威をもたらすマルウェアに対して早期に検知し，対策を行うには，ネットワークを観測し，その脅威を把握することがますます重要になってきている．マルウェアが組織のネットワークへ不正侵入した後に，水平展開という組織内部ネットワークに感染を拡散させていくことが行われる [1]．システムへの侵入を防ぐことが最も

[1] 防衛大学校理工学研究科
Graduate School of Science and Engineering, National Defense Academy
[2] 防衛大学校情報工学科
Computer Science, National Defense Academy

重要なセキュリティ対策であるが，もし侵入された場合には，侵入後の攻撃者の挙動がいかなるものであるのかについて、情報を収集しておくことが重要である．一方，攻撃者に気付かれないように侵入後の挙動を観測するために，実ネットワークと類似した仮想ネットワーク環境を用いる研究があるが，構成したネットワーク環境は固定であり，全ての水平展開手法を観測できるとは限らない．

そこで，本研究では外部ネットワークの攻撃者からの接続要求を観測した結果に基づいてネットワーク構成を動的に変更する目的として，Docker を用いた仮想ネットワーク環境を構築し，侵入してきた攻撃者の侵入後の挙動を観測するシステムについて提案する．

2. 侵入挙動観測の既存研究

攻撃者の侵入挙動を観測するためのいくつかの既存手法が提案されている．Andronikos ら [2] は，攻撃者の行動を監視及び調査するために Docker コンテナ上で複数のハニーポットセンサーを配置し，それらを用いて侵入してきた攻撃者からの行動を収集する．収集した全てのキャップデータを ELK Stack により保存，分析，そして単一のダッシュボードで攻撃者の分析したデータを表示する手法を提案している．しかしながら，構成したシステムではそれぞれのハニーポットが独立であるため，相互に侵入不可になり，不正侵入後の活動が得られない．

また，津田ら [3] は，標的型攻撃の攻撃者を実ネットワークに類似した仮想ネットワーク環境を自動構築し，その環境に誘い込み，長期にわたって手動攻撃の挙動を観測している．しかし，このシステムはクライアントセグメント上の Windows ホストではマルウェアを実行するため侵入口の Linux ホストを対象としたマルウェアの挙動について検討されてない．

そして，田辺ら [4] は，Linux 上で動作するマルウェアをプライベートネットワークとパブリックネットワーク内で安全に解析可能な動的手法を提案している．しかし，実際にはマルウェア検体が行なった通信挙動のみ観測可能であるが，解析環境の内部挙動が観測されていない．

そこで，本研究では Linux マシンを感染ホストとして，外部の攻撃者に侵入させ，さらに内部ネットワークでは攻撃者からの接続要求に応じて自動的に内部ネットワーク構成を行い，攻撃者の侵入後の挙動を観測する目的とする．

3. 提案手法

サイバー攻撃では，組織内のネットワーク，コンピュータに不正侵入後にマルウェアを他のコンピュータに感染拡大させるにはブロードキャストで送信して同じネットワーク上のすべてのマシンを検索することが多い．そこで，本研究ではこれを着目して，**図 1** の通りに提案手法を示す．

- 内部の仮想マシン同士の通信用路カール VLAN を構築する．
- 外部の攻撃者に侵入させるような中間マシンを作成し，上記の VLAN に接続する．
- 攻撃者が中間マシンを介して，内部のネットワーク上のすべてのマシンを検索する（ブロードキャスト アドレスへ通信を行う）．その際，中間マシン上のブロードキャストプログラムにより内部のネットワーク上の存在しないマシンの IP アドレスを応答する．
- 攻撃者が応答結果により同じネットワークの他のマシンへ侵入するため，攻撃者からの接続要求 IP アドレスに応じて内部ネットワークのマシンを素早く作成し，さらに侵入させる．
- 内部ネットワーク内の全ての仮想マシン上で発生した通信挙動と内部挙動を観測する．

4. 侵入挙動観測の実装

提案システムの実装について説明する．本システムでは VMware を用いて，2 台のマシン（Linux と Windows) 上に実装した．以下，各構成要素を説明する．

- Vmware を用いて内部の通信用 VLAN を作成する．2 台のマシン（Linux と Windows) をこの VLAN に接続を行う．
- Linux マシンでは，Docker ツールを用いて脆弱性のある中間マシン（コンテナ）を構築し，上記の作成した VLAN に接続する．
- Linux マシンでは，攻撃者から中間マシンを介して VLAN 上に発生する通信をキャプチャーし，攻撃者に対する通信できる振りをするマシンの IP アドレスを自動的に応答するようブロードキャストプログラムを設定する．
- 次に攻撃者からの接続 IP アドレスを要求する瞬間にその IP アドレスに応じてホストマシン上に設定したプログラムを介して Docker のコンテナとして内部のネットワーク内に接続するマシン（コンテナ）を作成・起動し，そして不正に侵入させる．
- Linux マシン側と Windows 側内のすべての仮想マシンから発生する通信挙動と内部挙動を記録する．

上記の手順を実装した上で仮想内部ネットワーク環境（VLAN）を構築することができた．さらに，中間マシンにログインしてきた攻撃者が入力したコマンド（内部挙動）及び通信データを記録されていた．

5. まとめと今後の課題

Docker を用いて仮想ネットワーク環境を動的に構築し，侵入後の攻撃者の挙動を観測する手法を提案した．初期侵入されたマシン（中間マシン）の内部挙動と通信挙動を確認できた．この結果により，侵入してきた外部ネットワークの攻撃者に対して内部ネットワークを動的に構築して内

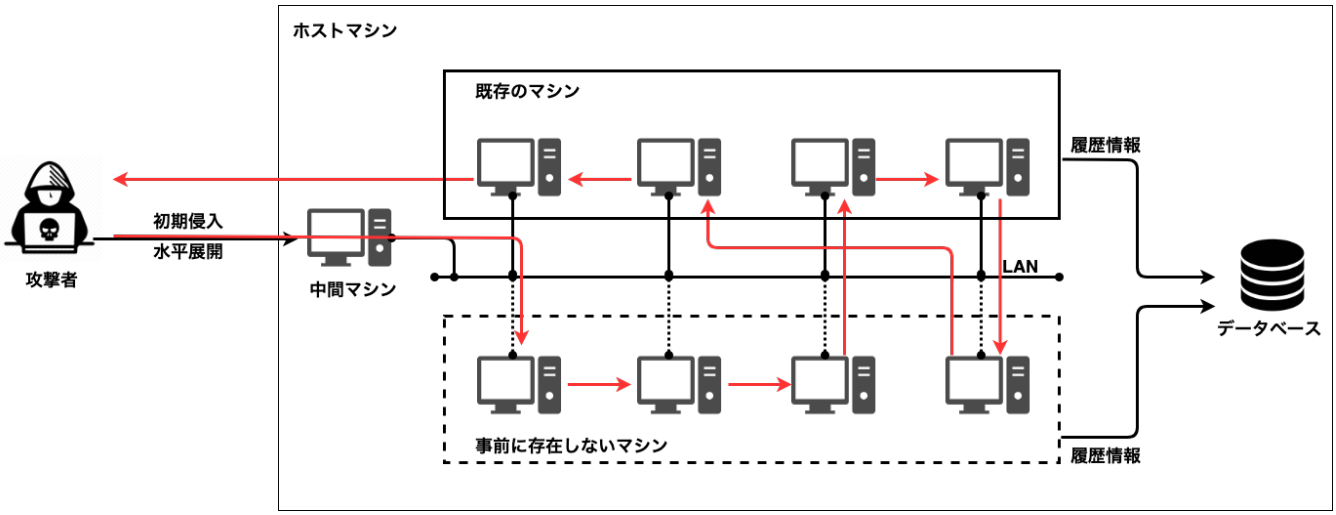

図 1　提案手法の概要図

Fig. 1　Overview of the proposed method

部ネットワーク内の侵入挙動を観測することが可能と考えられる．今後，攻撃者がブロードキャストアドレスを送信することに対する自動的に応答するようプログラムを設定することで攻撃者からの接続要求マシンの IP アドレスを合わせて Docker のコンテナで内部のネットワーク内のマシン（コンテナ）を動的に作成・起動し、内部にアクセスさせる．また、構築したシステムによる侵入後の攻撃者の挙動を観測するとともに，その無限侵入の問題に対しての対策も検討したい．

参考文献

[1] NEC 技報，Vol.70 (2017 年)，AI (人工知能) を活用した未知のサイバー攻撃対策，https://jpn.nec.com/techrep/journal/g17/n02/pdf/170215.pdf，(2017/02/15).

[2] Andronikos Kyriakou, Nicolas Sklavos, “Container-Based Honeypot Deployment for the Analysis of Malicious Activity”, Global Information Infrastructure and Networking Symposium (GIIS’18), 2018.

[3] 津田 侑, 遠峰 隆史, 金谷 延幸, 牧田 大佑, 丑丸 逸人, 神宮 真人, 高野 祐輝, 安田 真悟, 三浦 良介, 太田 悟史, 宮地 利幸, 神薗 雅紀, 衛藤 将史, 井上 大介, 中尾 康二, “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.

[4] 田辺 瑠偉, 筒見 拓也, 小出 駿, 牧田 大佑, 吉岡 克成, 松本 勉, “Linux 上で動作するマルウェアを安全に観測可能なマルウェア動的解析手法の提案”, コンピュータセキュリティシンポジウム, 2014.