L-027

ダークネット観測を利用した踏み台検出手法の提案
A Study of Stepping-stone detection via Traffic Darknet Analysis

後藤 洋一 † 李 熙貞 † 中村 康弘 †
Yoichi Goto Hee Leong Lee Yasuhiro Nakamura

1. はじめに

一般に未使用のアドレス空間をダークネットと呼び，ダークネットへの通信は不正アクセスである可能性が高いと考えられる．このためダークネットへの通信を監視してその種類や傾向を把握することは不正アクセス対策を行う上で極めて重要である．一方，踏み台検出に関する従来研究では，主に踏み台からの攻撃の回避策が検討されてきた．これは攻撃やスキャンを受ける標的側において，攻撃元機器が踏み台であることを検出することは困難なためである．そこでこの研究ではダークネットへ到達するパケットの観測結果から OS フィンガープリントと TCP コネクション要求時の応答時間を計測し，通信特性を分析することにより踏み台の可能性のある通信を分類する手法を提案する．

2. 踏み台検出とダークネット観測

セキュリティホールの悪用などにより攻撃者の不正アクセスを中継する機器を踏み台と呼ぶ（図 1）．標的側で不正アクセスを検知した際は攻撃元アドレスが攻撃者アドレスと見なされ，攻撃元機器が踏み台かどうかを判定することは困難である．踏み台攻撃には，NAT 機能を利用した IP アドレス偽装，SSH などのトンネリング，リモートログインなどの方法があるが，いずれも送信元アドレスが攻撃者アドレスとは異なる．NAT の場合は IP アドレスのみが変化するが，ポート番号や TTL などを変換する機器も多く，踏み台検出を困難にしている．一方，ダークネットを観測する方法には，接続要求に応答をせずにパッシブに観測する方法とハニーポットなどを設置してアクティブに行う方法がある．

竹尾ら [1] は TCP の SYN パケットに着目し，監視下のネットワーク内の機器が踏み台となった場合，それをリアルタイムに検出する手法を提案している．笹生ら [2] はダークネットで検知したホストを通信パターンや OS フィンガープリント判定結果を基に分類し，トラフィックを解析することにより，大規模ワームの流行の検知を行っている．また後藤ら [3] は，攻撃者からの SYN パケットに対し，SYN+ACK パケットを送信する装置を用いて応答時間を計測し，これを基に通信頻度の自己相関を求めることで，IP アドレス毎の特徴を分類した．しかしながら，竹尾ら [1] の研究では踏み台となる機器の入出力パケットを監視可能なことを前提としており，標的側から攻撃元アドレスの機器が踏み台かどうかを判別することはできない．また，後藤ら [3] の研究では同一アドレスからの応答時間が大きく遅延する現象が確認されたが，その原因は明らかになっていない．そこでこの研究では，応答時間を用いた踏み台検出手法を提案するとともに踏み台経由の応答時間の遅延原因について検証実験を元に考察する．

†防衛大学校 理工学研究科情報数理専攻 〒 239-8686 神奈川県横須賀市走水 1-10-20 em52038@nda.ac.jp yas@nda.ac.jp

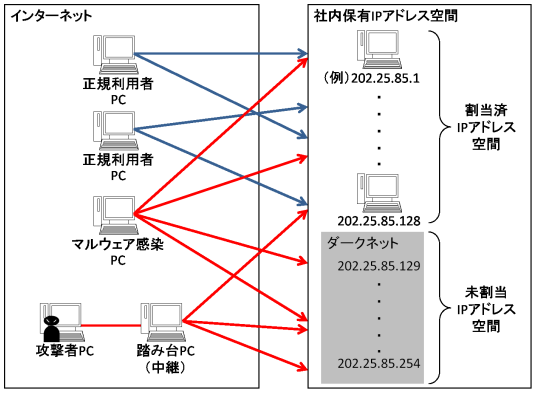

図 1: ダークネットと踏み台からの攻撃

3. 提案手法

3.1. 踏み台の判定根拠

マルウェア感染や脆弱性を利用したサイバー攻撃の多くは TCP 接続を試みるため，標的側で攻撃者からの TCP コネクション要求を観測することができる．ここでは，攻撃者からの SYN パケットに SYN+ACK パケットを返信した時刻と，それに対する ACK 応答パケットの受信時刻との差を応答時間と定義する．応答時間は距離や通信状態に応じて特定の値になると考えられるため，同一アドレスで応答時間が大きく変化した場合は，攻撃者側の環境変化を検出できたものと考えられる．さらに，攻撃側からのパケットの OS フィンガープリントを判定し，ひとつの IP アドレスから複数の OS が検出される場合を観測する．複数の OS が検出された場合には，踏み台となっている可能性が高いと推測できる．

3.2. 踏み台検出手順

まず，ダークネットへの到着パケットを観測できる位置で送受信パケットをキャプチャし，これを送信元 IP アドレスごと分割する．IP アドレスごとに文献 [3] の方法で応答時間を計測する．すなわち，攻撃者からの SYN パケット到着時刻 t_0，SYN+ACK パケット送信時刻 t_1，ACK パケット到着時刻 t_2 を観測し，着信時刻 t_0 と応答時間 $x_{t_0} = t_2 - t_1$ を記録する．

次に，取得したパケットデータから IP アドレス毎に p0f[4] を用いて OS 判別を行う．p0f の判別シグネチャは，IPversion, TTL, option length, mss, Window size, Window scale, option layout, quirks, payroad size の 9 種類である．特定の IP アドレスからの応答時間に大きな分散が発生している場合や 2 種類以上の OS が検出された場合は踏み台候補として

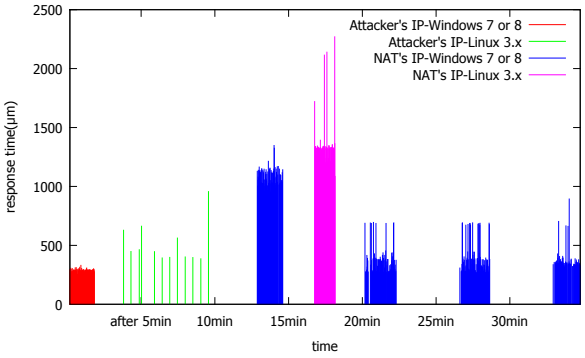

図 2: 実験 1 遅延時間検証実験結果

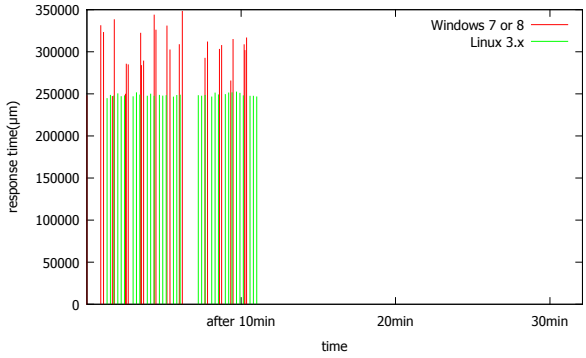

図 3: 実験 2 ダークネット観測結果の例

グラフ化して確認する．

4. 実験結果

提案手法の有効性を確認するため，踏み台による応答時間遅延の検証実験（実験 1）と実ネットワーク上のダークネット観測結果の分析実験（実験 2）の二つの実験を行った．実験 1 では，LAN 内で踏み台を介した通信と直接接続の通信のそれぞれをキャプチャし，応答時間と OS フィンガープリント判定結果を確認して踏み台検出手法の有効性を検証した．実験 2 では，実ネットワークのダークネットに到達した通信のキャプチャデータを使用し，IP アドレスごとの踏み台判定を行ってその傾向を分析した．

4.1. 実験 1 踏み台検出手法の検証

攻撃者側に Windows7 及び Ubuntu10 を用意し，標的 PC へ以下の通信を行って通信状態をキャプチャした．

(1) 攻撃者側から標的 PC へ直接 SSH 接続を行う．
(2) NAT による踏み台を介して SSH 接続を行う．
(3) トンネリングによる踏み台を介して SSH 接続を行う．
(4) 踏み台機器から直接 SSH 接続を行う．

得られた応答時間と OS フィンガープリント判定結果を図 2 に示す．横軸は経過時間，縦軸は応答時間，OS の種類を色で表す．NAT を介して接続した場合の応答時間は，Windows7 及び Ubuntu10 の両者とも，直接接続した場合に比べて概ね 800 μ s の遅延が発生している．OS フィンガープリント判定結果では，NAT による踏み台の IP アドレスから Windows と Linux の 2 つの OS が検知されている．この結果から NAT では踏み台と攻撃者の OS が同一であった場合には応答時間の遅延が発生し，OS が異なる場合には複数の OS が検知されるため，踏み台と判別することができる．SSH トンネリングの踏み台では応答時間に大きな変化は無く，OS フィンガープリントも踏み台機器の OS を検知しているため判別はできなかった．

4.2. 実験 2 実ネットワークでの検証

次に，実ネットワークのダークネットに到達したパケットのキャプチャデータを用いて検証を行った．この実験では 2014 年 6 月 15 日 00 時 00 分から 23 時 59 分までの 1 日分のパケットキャプチャデータを使用した．1,730 個の未使用アドレスからなるダークネットへの着信と応答をキャプチャした結果，総パケット数は 7,844,879 個，接続のあったユニークな送信元 IP アドレス数は 58,115 個，このうち 268 個の IP アドレスで複数の OS が検知された．検出結果の一例を図 3 に示す．この例では応答時間が安定せず，遅延が発生しており，OS の判定結果も変化している．

得られた実験結果から，

(1) 応答時間に遅延が発生し，複数の OS を検出，
(2) 応答時間に遅延は無いが，複数の OS を検出，
(3) 応答時間に遅延が発生しているが OS は 1 種類のみ，

の 3 通りの場合，そのアドレスの機器は踏み台であると考えられる．ただし，(3) の場合は応答時間の遅延判定に一定のしきい値を設ける必要があるが，今回の実験では目視により判別した．また，DHCP により IP アドレスが他の OS の機器に再利用される場合も考えられるため，別途検討する必要がある．

5. まとめと今後の課題

標的側の監視結果から NAT 機能を使用した踏み台を検知することができ，ダークネットで観測された応答時間の遅延の原因の 1 つを明らかにすることができた．今後は SSH トンネリングを使用した踏み台の検出が課題となる．また，応答時間の変化により踏み台を判別するためには適切なしきい値判定が必要になる．さらに，DHCP により IP アドレスの再利用についても考慮する必要がある．

参考文献

[1] 竹尾 大輔, 伊藤 将志, 鈴木 秀和, 岡崎 直宣, 渡邊 晃, ” コネクションベース方式による踏み台攻撃検出手法の提案”, 情報処理学会論文誌, Vol.48, No.2 pp.644–655 (2007).

[2] 笹生 憲, 森 達也, 後藤 滋樹, ” 通信源ホストの分類を利用したダークネット通信解析”, コンピュータセキュリティシンポジウム論文集, No.4 pp.729–736 (2013).

[3] 後藤 洋一, トラン コン マン, 中村 康弘, ” ダークネット観測結果に基づく攻撃元アドレスの傾向分析手法の提案”, 暗号と情報セキュリティシンポジウム, 2C2-1 (2014).

[4] Michal Zalewski,”p0f v3 (version 3.07b)”, http://lcamtuf.coredump.cx/p0f3/.