5D-02

初期ペイロードに着目したネットワーク走査活動の分析

中村　康弘†
†防衛大学校情報工学科

1　はじめに

ダークネットへ到達するパケットは，走査活動，マルウェア感染活動，DoS 攻撃などを目的とした不正な通信の前兆と考えられ，これらを観測・分析・可視化する研究が数多く行われてきている．しかしながら，一般にダークネット観測はステルス型センサを用いており，コネクション要求パケットの送信元アドレスや宛先ポート番号の分析に留まり，接続以後に行われる通信を観測することはできない．実機と同様な応答を行い，攻撃の意図を分析するためにはハニーポットが用いられる．

この研究では，ダークネットに着信する TCP 接続要求に応答する観測システムを構築し，得られた初期ペイロードとともに走査活動を分析，可視化した結果について報告する．このため，ポートスキャン, SYN flood やその他の UDP パケットは対象とせず，TCP セッションを確立した後に何らかのペイロードを送付してくるタイプの攻撃のみを分析対象とする．すなわち，何らかの明確な意図を持つと推定される攻撃である．

2　関連研究

ダークネットに着信する走査活動の観測・分析・可視化については文献 [1] の nicter プロジェクトが代表的であり，いくつかの新しい可視化法も提案されている．文献 [2] では，さらに複数箇所にハニーポットを設置することで，観測点の違いによるマルウェアの差異などが指摘されている．また，文献 [3] では，HTTP ハニーポットへの攻撃状況の分析を行っている．

以上のように，これまでのダークネット観測は，そこに着信するパケット全体の傾向，発信元の国別あるいは AS 別の頻度，宛先のポートごとの頻度などを分析し，今現在の攻撃トレンドを判定することを目的としていた．また，ハニーポットを用いた観測は，特定のプロトコルに依存した通信手順やペイロードに含まれるマルウェアの解析など，具体的な攻撃手法を調査する場合に有益な情報が得られる．

この研究では，複数アドレスへの着信状況を可視化することで，走査活動をセンサから隠蔽しようとする挙動を見つけ出すことを目的として，観測結果の分析を行った．

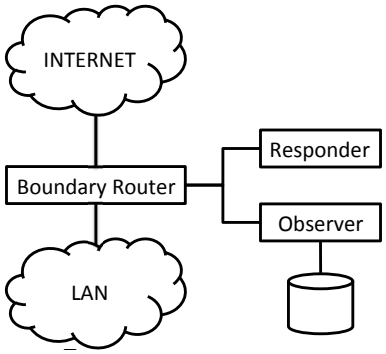
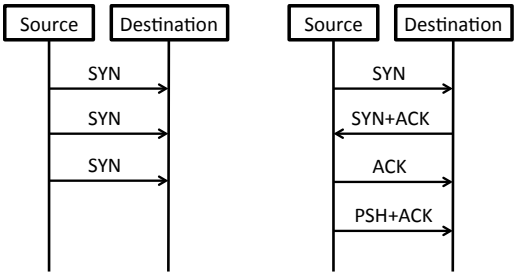


図 1: 応答・観測システム



(a) ステルスセンサ　(b) 擬似応答センサ

図 2: 擬似応答によるペイロードの取得

3　提案方式

3.1　観測システム

観測システムは図 1 のように，境界ルータのミラーポートにて擬似応答およびパケットキャプチャを行う．一般的なステルスセンサの場合は図 2(a) のように接続要求を着信するのみであるが，(b) のように SYN+ACK を応答することにより初期ペイロードが得られる．

3.2　可視化方法

得られたパケットキャプチャファイルから，ペイロードが得られたもののみを抽出し，パケットごとの到着日時 (time), IP アドレス (src,dst), ポート番号 (sport,dport), AS 番号, 国別コードを 1 日ごとにバイナリ形式の一時ファイルに保存する．これらの値を画面の縦横軸に配置して，1 パケットごとにプロットすることにより，値の範囲やパターンなどの特徴が視覚的に得られる．

An analysis of network scanning activity based on initial payloads
†Yasuhiro NAKAMURA
Computer Science, National Defense Academy

3.3 初期ペイロードによる分類

今回はペイロードのハッシュ値を特徴量に含めていないが，複数の異なるアドレスから同一のペイロードが送付される場合が多いことから，ペイロードを元に分類を行うことで，走査の意図の分析に役立つと考えられる．

4 実験結果

可視化の一例として，横軸を日時 (time)，縦軸を宛先 IP アドレス (dst) として表示した際の画面の一部を図 3 に示す．縦方向の線は極めて短時間に多くのアドレスを走査しているもの，横方向の線は長時間に渡って特定の宛先を走査しているもの，斜めの線は一定の走査間隔で多くのアドレスを走査しているものを表しており，それぞれ送信元アドレスは単一のアドレスである場合が多い．また，右半分で短い線分が分散したもの，および部分的に一定密度でドットが分散しているものは特定のアドレスに固執せずに分散的に行われている走査活動を表している．

一定時間内の走査回数が多い走査活動では，その時間内の走査頻度を求めることで容易に検知可能であるが，長時間に渡って一定の時間間隔で行われる走査活動は頻度の変化が顕著でなく，検出が難しい．しかしながら，図 3 のように可視化することで，その連続性などの特徴が顕著となる．

その他の顕著な例を図 4 に示す．いずれも画面の一部である．(a),(b) は横軸は時刻，縦軸は宛先 IP アドレスである．(a) は，図 3 の右側のタイプの密度が濃くなったものと考えられる．(b) は，一定時間ごとに階段型にアドレスを変更して走査している．(c),(d) は横軸は時刻，縦軸は宛先ポート番号（上が下位ポート）である．(c) の縦線はある時刻に多くのポートがほぼ同時に走査されたもの，横線は長時間に渡って特定のポートへアクセスされ続けている状況を示している．(d) は下位ポートから順に上位まで時間間隔を置いて走査が行われ，それが連続して生起している．

5 まとめ

走査パケットの特徴量を可視化することで，頻度の変化だけでは検出できない独特な走査パターンを発見することができた．このようなパターンが現れるのは，走査プログラムのアルゴリズムに依存すると考えられるため，今後，走査ツールを推定できるかも知れない．また，ペイロードのハッシュ値の同一性を根拠に類別することにより，複数アドレスの結託走査の状況も可視化できる可能性がある．

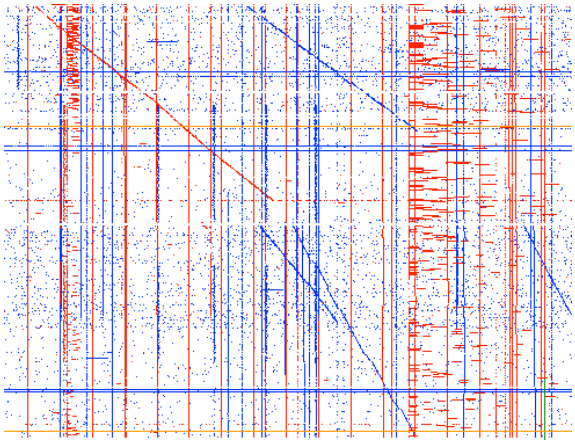
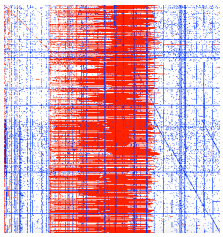
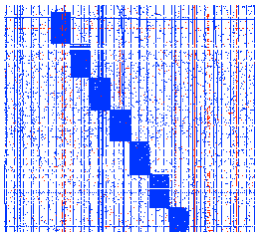


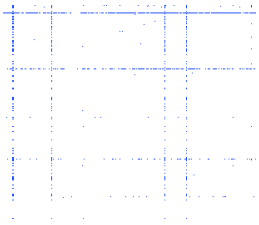
図 3: 可視化の一例



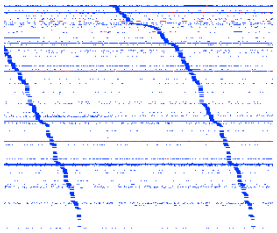
(a) dst:ランダム型



(b) dst:階段型



(c) dport:縦横線



(d) dport:なだれ型

図 4: 走査パターンの検知例

参考文献

[1] 中尾康二, 松本文子, 井上大介, 馬場俊輔, 鈴木和也, 衛藤将史, 吉岡克成, 力武健次, 堀良彰, “インシデント分析センタ nicter の可視化技術”, 信学技報 ISEC Vol.106, No.176, pp.83-89, 2006.

[2] 曽根直人, 正力達也, 鳥居明久, 村尾岳人, 森井昌克, “可視化によるダークネットの不正パケット解析 : ハニーポットとの併用による相関分析”, 信学技報 ICSS Vol.111, No.495, pp.43-48, 2012.

[3] 池部実, 宮崎桐果, 吉田和幸, “ハニーポットによる大分大学におけるダークネット宛通信の分析”, 情報処理学会 CSEC Vol.69, No.17, pp.1-8, 2015.