L-016

ダークネットに対するネットワークスキャナの判別手法の比較
Comparative Analysis of Network Scanner Detection Techniques for Darknet

鹿内 嵩天† 角田 裕‡
Takuma Shikanai Hiroshi Tsunoda

1. はじめに

ダークネットは，通常のネットワークから到達可能かつ未使用な IP アドレス空間であり，いかなる要求や応答も送信しない．そのため，ダークネットでは，不特定多数に向けて送られる不審な通信のみが観測されるという特徴がある．そこで，インターネット空間のトラフィックの傾向把握や不特定多数を標的としたサイバー攻撃の分析を目的としてダークネットトラフィックの分析が行われている．近年，セキュリティに関連した組織が行う調査目的スキャンが増加傾向にあり[1]，これらが分析上のノイズになることが指摘されている [2][3]．調査目的スキャナのトラフィックは，ダークネットトラフィック中の半数以上を占めるという報告もあり[1]，ダークネット分析における障害を取り除くためそのスキャナの実態を明らかにする必要がある．スキャナを判定する指標は複数提案されているが，それらの比較は行われていない．本研究では，2 つの指標を比較し，指標ごとの特徴を明らかにするとともに，既存指標で特定できていないスキャナの存在を調査する．具体的には，2 つの既存の判定指標をダークネットトラフィックに適用し，結果を可視化し比較することで各スキャナの挙動を分析した．そして，スキャナと挙動が類似するが各指標で見落としてしまう事例について調査した．

2. 既存の調査目的スキャナ判定指標の概要

本研究では中川らによって提案されたネットワーク単位でスキャナを判定する判定指標（以下，ネットワーク指標）[4]と情報通信研究機構がダークネット分析に使用しているホスト単位でスキャナを判定する判定指標（以下，ホスト指標）[1]を用いる．図 1 にそれぞれのスキャナ判定条件の概要を示す．

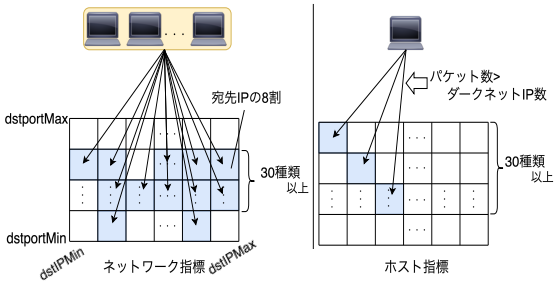

図 1 各調査目的スキャナの判定指標の概要

ネットワーク指標では，あるネットワークが 1 日に送信したパケットが以下の両方の条件を満たす場合にそのネットワークをスキャナと判定する．

条件 1 特定のポートに対してダークネットのアドレスレンジの 8 割以上にパケットを送信
条件 2 **条件 1** を満たすポートが 30 種類以上

ホスト指標では，ある 1 日について各送信元ホストが以下の両方の条件を満たす場合にそのホストをスキャナと判定する．

条件 1 ダークネットのアドレス数以上のパケットを送信
条件 2 30 種類以上のポートにパケットを送信

3. 各指標の適用方法とその結果

3.1 観測環境と適用方法

本研究室で運用している数百程度の IP アドレスを有する小規模なダークネットで 2024 年 1 月 1 日に観測されたパケット群に対して，各指標を適用した．

ネットワーク指標についてはクラス B のネットワーク単位で，ホスト指標ではホスト単位でスキャナを判定した．ただし，ネットワーク指標との比較のため，ホスト指標で 1 台でもスキャナと判定されたホストが属するクラス B のネットワークをスキャナと判定する．

次に，スキャナと判定されたネットワークがダークネットのどの IP アドレスのどのポートにパケットを送信しているのかを挙動と定義し，ネットワーク毎にそれを可視化した．その図から特徴や類似性を目視で確認し，各指標でスキャナと判定されたネットワークについての挙動を分析した．また，スキャナと判定されなかったネットワークについても同様の可視化を行い，判定漏れの可能性を検証した．

3.2 各指標の適用結果

3.2.1 各指標でスキャナと判定されたネットワーク

観測された 13421 個のクラス B のネットワークのうち，各指標でスキャナと判定されたネットワーク数を図 2 に示す．

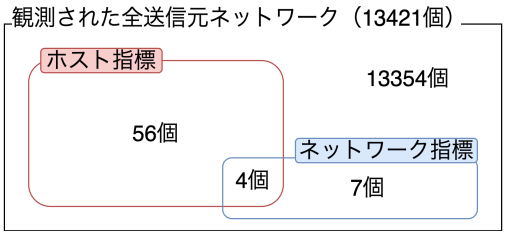

図 2 各指標での判定結果

ネットワーク指標とホスト指標のいずれか一方のみでスキャナと判定されたネットワークの挙動例をそれぞれ図 3, 4 に示す．両図において，横軸は当該ネットワークから送信されたパケットの宛先 IP アドレス，縦軸は宛先ポートを示している．なお，紙面の都合上，本稿ではポート番号についてはウェルノウンポートの範囲のみを表示している．

† 東北工業大学大学院工学研究科 Graduate School of Engineering, Tohoku Institute of Technology
‡ 東北工業大学工学部情報通信工学科 Department of Information and Communication Engineering, Tohoku Institute of Technology

図 3 より，ネットワーク指標のみでスキャナと判定されたネットワークは，連続する IP アドレスに対してパケットを送信していることがわかる．一方で，図 4 からわかるように，ホスト指標のみでスキャナと判定されたネットワークは宛先とする IP アドレスが連続していない．

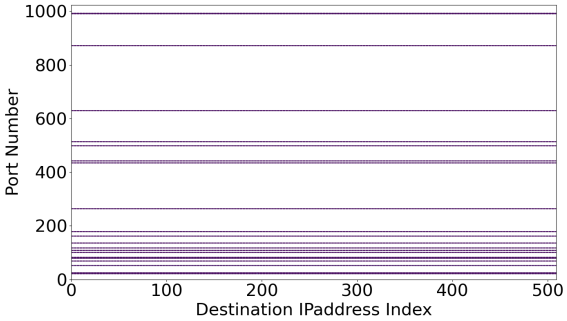

図 3 ネットワーク指標で判定された挙動例

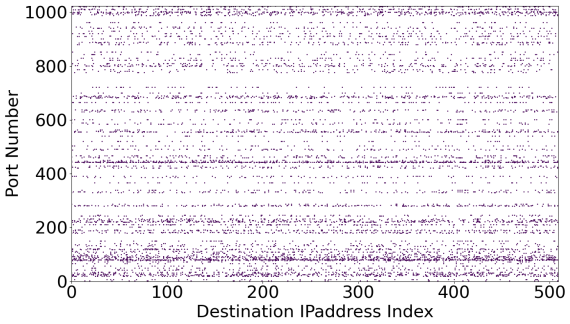

図 4 ホスト指標で判定された挙動例

図 3 のネットワークは 105 個のホストがパケットを送信していた，そのうち 99 個のホストはダークネットの IP アドレス数以上のパケットを送信していたが，その宛先ポートが 1, 2 種類しかなかったため，ホスト指標ではどのホストもスキャナとは判定されなかった．ネットワーク指標では，複数のホストでスキャン対象のポートを分担しているスキャナや，各ホストの送信パケット数は少数だがネットワーク全体では活発にスキャンを行うスキャナを特定した．ネットワーク指標でスキャナと判定されたネットワークは同様の挙動が多く確認された．

図 4 のネットワークからはダークネットの IP アドレス範囲の 8 割に満たない範囲にしかアクセスがなかったため，ネットワーク指標ではスキャナと判定されなかった．ホスト指標でスキャナと判定されたネットワークの多くが同様の挙動をしていた．

これらの結果より，ネットワーク指標では，特定の宛先 IP アドレス範囲に対してのみスキャンを行うネットワークを見落としてしまうといえる．例えば，特定のダークネットをあるスキャナが複数日にわたってスキャンした場合，1 日にスキャンする IP アドレス範囲が限定されるため見落とされる．また，ホスト指標では，ネットワーク単位では活動量が多いがホスト単位では活動量が少ないスキャナや，同ネットワーク内のホストで宛先ポートを分担してスキャンを行うスキャナを見落としてしまう．

これより現状でのスキャナの判定指標では大規模で挙動が明確なスキャナは発見できるのに対し，活動量が限定的な一部のスキャナを発見できない可能性が考えられる．

3.2.2 スキャナと判定されなかったネットワーク

スキャナと判定されなかったネットワークについても挙動を可視化し，スキャナと判定されたネットワークとされなかったネットワークで類似している挙動を発見するために比較を行なった． スキャナの目的として，インターネット空間の情報収集が考えられるため，送信パケット数が少数のネットワークはスキャナである可能性が低い．そのため，本稿ではスキャナと判定されなかったネットワークのうち，1 日の送信パケット数が 500 個以上である 35 個のネットワークについて調査した．そのうちスキャナと挙動が類似しているネットワーク例を図 5 に示す．

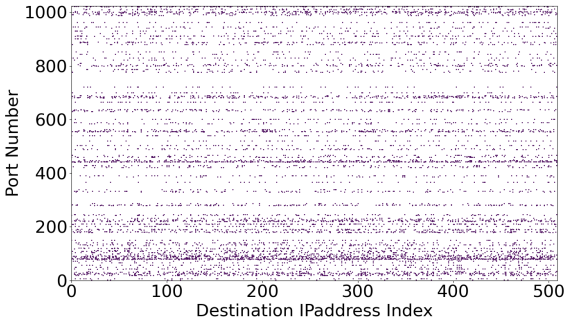

図 5 スキャナと判定されなかった例

このネットワークからは 505 台のホストがダークネットに向けてパケットを送信しており，そのうち 504 台のホストが対象ダークネットの IP アドレス数の 7 割以上の数のパケットを送信していた．また，このネットワークにおいて最多のパケットを送信したホストはパケット数がホスト指標の条件をわずかに下回っているだけであり，事実上はスキャナとみなすことができる．その他にも， 送信パケット数は少ないが，同様の挙動のネットワークもいくつか存在した．その他のネットワークの多くが多数の IP アドレスの少数の特定のポートにパケットを送信していた．これらは調査目的スキャンとは違い特定のポートを意図的に狙ったネットワークであると考えられる．

4. おわりに

本稿では，2 つのスキャナ判定指標をダークネットトラフィックに適用し，それぞれの挙動を可視化した．そのうち，各指標でスキャナと判定されたネットワークの特徴を比較し，各指標で発見できるスキャナと発見できないスキャナの挙動について考察した．また，スキャナと判定されなかったネットワークの中でスキャナと判定されたネットワークと挙動が類似しているネットワークについても考察を行った．今後は，まだ特定できていないスキャナを発見するため，各ネットワークのパケット到着間隔やパケット送信順序などのパラメータについても分析する．

参考文献

[1] 国立研究開発法人情報通信研究機構，“NICTER 観測レポート 2023 ”，https://csl.nict.go.jp/nicter-report.html (accessed Jun. 10, 2024)
[2] 笠間ら，“Can’t Stop The Scan: インターネットスキャンのオプトアウト実態調査”，信学技報, ICSS2022-76, pp. 169-174, 2023.
[3] C. Han, et al., “Dark-TRACER: Early Detection Framework for Malware Activity Based on Anomalous Spatiotemporal Patterns”, IEEE Access, vol. 10, pp 13038-13058, 2022.
[4] 中川ら, ”ダークネットトラフィックの分析に基づく継続的な広域ネットワークスキャンの調査”, CSS2019, pp. 1422 – 1428, 2019.