7ZC-08

ダークネットで観測された複数ポートに対するDDoS攻撃の分析

宮畑　歩†　　杉野　栄二†　　成田　匡輝†

岩手県立大学　ソフトウェア情報学部　ソフトウェア情報学科†

1. はじめに

近年，サイバー攻撃を行う攻撃者は，様々な手法を用いて攻撃を行っている．その中には，同一の攻撃先 IP アドレスの複数ポートを攻撃対象とした DDoS 攻撃（以下，マルチベクタ攻撃）も確認されている．

マルチベクタ攻撃に関する課題として，マルチベクタ攻撃の傾向や実態などの把握が十分とはいえない点が挙げられている[1]．そのため，マルチベクタ攻撃の傾向や実態を明らかにする必要がある．

本稿では，マルチベクタ攻撃の傾向を明らかにするため，ダークネットの観測データから複数の TCP ポートを攻撃対象としたマルチベクタ攻撃を抽出し，その結果をもとにマルチベクタ攻撃の分析を行った．

2. 先行研究

山村らは，ダークネットとハニーポットでの観測結果を用いることで，帯域幅消費型攻撃とサーバリソース消費型攻撃を併用した DDoS 攻撃の検知に成功した[1]．また，ダークネットの観測結果から複数の TCP ポートを対象にしたマルチベクタ攻撃も確認されたが，この攻撃の傾向についてはこの研究では明らかにされていなかった．

3. マルチベクタ攻撃の抽出手法

マルチベクタ攻撃の分析を行うため，山村らの提案手法を参考にし，ダークネットでの観測データからマルチベクタ攻撃を抽出するシステムを実装した．実装したシステムのフローチャートを図 1 に示し，以下に各処理の概要を述べる．

3.1　バックスキャッタの判定

ダークネットでは， DDoS 攻撃を受けているサーバからの応答であるバックスキャッタのほか，マルウェアによるスキャンパケットなども観測される．そのため，Liu らの研究[2]をもとに，TCP フラグに SYN-ACK， ACK， RST， RST-ACK のいずれかを含むパケットをバックスキャッタとして抽出することとした．

3.2　攻撃イベントの判定

抽出されたバックスキャッタを攻撃先 IP アドレスごとに分類する．その後，各観測パケットの受信時刻のインターバルが x 以内であるパケットを集めた観測パケット群をひとつの攻撃イベントと定義する．

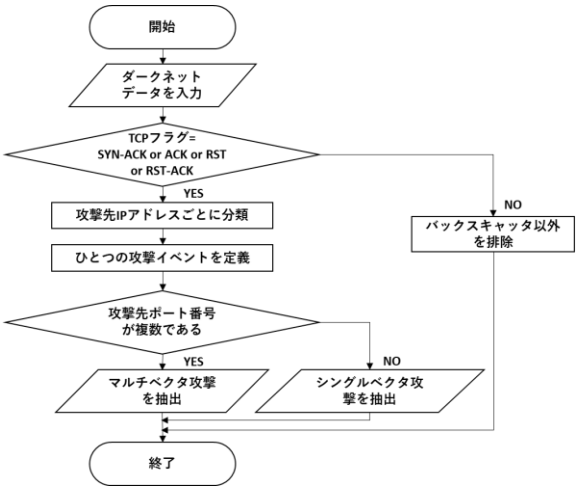

図 1　マルチベクタ攻撃の抽出手法

3.3　マルチベクタ攻撃の判定

攻撃先ポートが複数である攻撃イベントをマルチベクタ攻撃として判定し抽出する．

4. 評価実験

4.1　実験条件

実験に使用するデータセットの観測期間と各観測パケットの受信時刻のインターバルの設定値を表 1 に示す． 実験は， 合計 15 通りの組み合わせで行った．

表 1　実験条件

パラメータ名	設定値
観測期間	2012年1月1日～2012年6月30日 2017年1月1日～2017年6月30日 2022年1月1日～2022年6月30日
受信時刻のインターバル x	5分, 1時間, 6時間, 12時間, 24時間

4.2　実験結果

4.2.1　マルチベクタ攻撃の割合

ダークネットで観測された DDoS 攻撃のうち，マルチベクタ攻撃である割合を図 2 に示す．マルチベクタ攻撃の割合は，$x = 5$ 分の場合に約 23%，その他の場合では約 33%を占めた． また，$x = 5$ 分にした場合のマルチベクタ攻撃の割合は，2017 年から 2022 年にかけて約 13%上昇していた．

4.2.2　攻撃対象のポート数

ひとつの攻撃イベントで用いられた攻撃先ポートの種類数を図 3 に示す．観測されたマルチベ

Analysis of DDoS Attacks on Multiple Ports Observed in the Darknet
Ayumu Miyahata†, Eiji Sugino†, Masaki Narita†
† Iwate Prefectural University

表 2　攻撃に使用されるポートの組み合わせ 上位 5 件（2022 年）

	受信時刻のインターバル x				
	5分	1時間	6時間	12時間	24時間
1	80, 443 (0.39%)	80, 443 (1.02%)	80, 443 (2.41%)	80, 443 (2.87%)	80, 443 (3.15%)
2	9916, 9918 (0.27%)	9916, 9918 (0.56%)	9916, 9918 (1.20%)	9916, 9918 (1.51%)	9916, 9918 (1.71%)
3	22, 80 (0.11%)	22, 80 (0.32%)	22, 80 (0.84%)	22, 80 (1.01%)	22, 80 (1.10%)
4	22, 443 (0.06%)	22, 443 (0.14%)	22, 443 (0.31%)	22, 443 (0.40%)	22, 443 (0.45%)
5	9917, 9918 (0.06%)	22, 53 (0.13%)	22, 53 (0.25%)	9917, 9918 (0.30%)	9917, 9918 (0.32%)

クタ攻撃のうち，約 45%が 2 種類のポートを攻撃対象としていた．また，6 種類以上のポートを対象とした攻撃も観測された．

4.2.3　攻撃先ポートの組み合わせ

2022 年に観測された観測頻度上位の攻撃先ポートの組み合わせを表 2 に示す．攻撃先ポートの組み合わせとしては，特に 22 番(ssh)，80 番(http)，443 番(https)を併用した攻撃が多く観測された．

表 2 の x を 24 時間に設定した場合の結果について，攻撃件数の推移を図 4 に示す．80 番と 443 番を併用した攻撃が恒常的に多い一方で，9916～9918 番(用途不明)を併用した攻撃は同年 4 月に急増していた．

5. 考察

4.2.1 節より，$x = 5$ 分の時のマルチベクタ攻撃の割合が増加していたことから，近年，5 分以内の短い期間で行われるマルチベクタ攻撃が増加傾向にある可能性がある．また，xの値を 5 分から 1 時間に変化させた際に，マルチベクタ攻撃の割合が大きく変化していたことから，1 時間以内に行われているマルチベクタ攻撃も多い可能性があると考えられる．

4.2.3 節より，ある観測月のみで急増している攻撃先ポートの組み合わせが確認されたことから，攻撃者はマルチベクタ攻撃においても脆弱性や効率などに考慮し，特定の攻撃先ポートを意図的に組み合わせて攻撃していると考えられる．

6. おわりに

本稿では，マルチベクタ攻撃の傾向を明らかにするため，ダークネットデータからマルチベクタ攻撃を抽出し，その結果をもとにマルチベクタ攻撃の分析を行った．その結果，マルチベクタ攻撃をダークネットで観測することに成功し，特にダークネットで観測された DDoS 攻撃のうち約 25%がマルチベクタ攻撃である可能性が高いことが判明した．

今後の課題として，攻撃者がマルチベクタ攻撃を行う目的を明確にする必要がある．特に，数百，数万種類のポートを対象としたマルチベクタ攻撃も観測されたため，攻撃先ポートの種類数によって攻撃の目的が異なる可能性があると推測される．

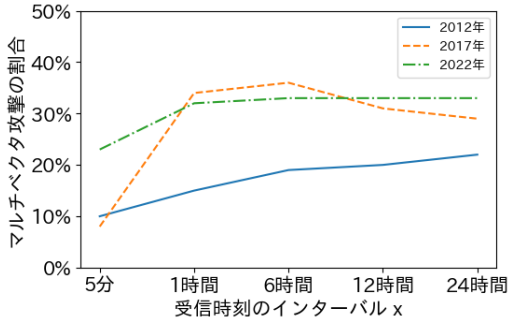

図 2　マルチベクタ攻撃の割合

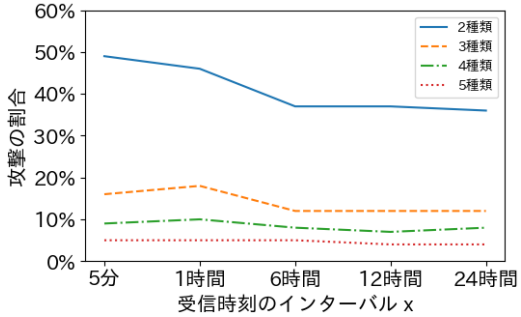

図 3　攻撃先ポートの種類数（2022 年）

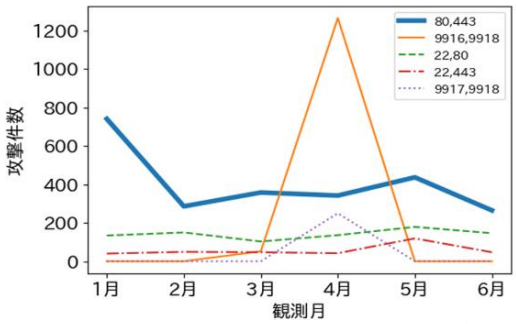

図 4　攻撃先ポートの組み合わせの推移
（2022 年，$x = 24$時間）

謝辞

本研究では，情報通信研究機構が提供しているダークネットデータを使用しました．貴重なデータセットを提供していただいた情報通信研究機構の関係各位に深く感謝します．

参考文献

1) 山村翔，神谷和憲，倉上弘：Darknet 及びハニーポットの比較分析に基づくマルチベクタ型 DDoS 攻撃の検知方法の検討，コンピュータセキュリティシンポジウム 2018，pp. 718-725(2018)．

2) Jun Liu and Kensuke Fukuda: An Evaluation of Darknet Traffic Taxonomy, *Journal of Information Processing*, Vol. 26, pp. 148-157(2018)．