SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ハニーポットで観測される絨毯爆撃型 DRDoS 攻撃の分析
Analyzing Carpet Bombing DRDoS Attacks Observed by Honeypot

毛　清昕*　　牧田　大佑†　　吉岡　克成†　　松本　勉†
Mao Qingxin　Daisuke Makita　Katsunari Yoshioka　Tsutomu Matsumoto

キーワード DRDoS 攻撃，絨毯爆撃型

あらまし

DRDoS (Distributed Reflection Denial of Service)攻撃は近年大きな脅威となっており，これを観測するためにリフレクタの視点で攻撃を観測する囮システムである DRDoS ハニーポットが提案されている[1,2]．近年，単一の IP アドレスではなく広いアドレスレンジに対して攻撃を行う絨毯爆撃型の DRDoS が報告されている．我々が運用する DRDoS ハニーポットでは，宛先 IP アドレスごとに攻撃イベントを定義しており，絨毯爆撃型 DRDoS 攻撃は多数の攻撃イベントとして検知されるため，実質的な攻撃件数の把握が困難になっている．そこで，本研究では，DRDoS ハニーポットにより同時刻に観測される攻撃のうち，宛先アドレスが一定範囲に含まれる攻撃イベントを集約し，同一の攻撃イベントと捉えることで，攻撃の実態を把握することを試みた．分析の結果，従来の攻撃イベントの定義では急激に攻撃件数が増加している期間において上記の集約アルゴリズムにより，件数が大幅に削減されることを確認した．これらの期間では，特定のアドレス帯に対して行われた絨毯爆撃型 DRDoS 攻撃が多数のイベントとして過剰にカウントされていたと推測できる．

同一アドレス帯への攻撃の集約方法

2018年3月から3年分の観測結果について，同時刻(60秒以上の間隔を空けず)に観測される同一アドレス帯(/24)への攻撃イベントを集約した結果を図1に示す．同時刻に同じ/24 ネットワークに対して行われた攻撃イベントを集約した結果，攻撃イベント数が急激した時期のいくつかで，急激な増加がみられなくなった．これらの時期には同一ネットワーク内の異なる IP アドレスに対して絨毯爆撃型 DRDoS 攻撃が行われており，多数のイベントとして過剰にカウントしていたと思われる．

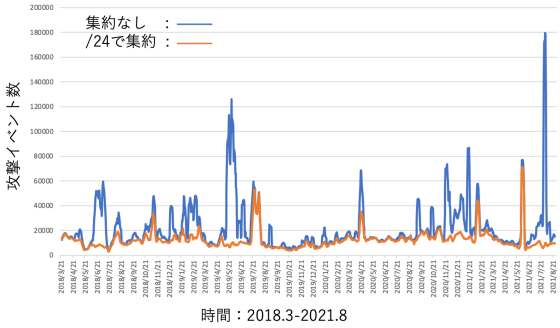

図 1．同一アドレス帯への攻撃イベントの集約効果

参考文献

[1] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow，“AmpPot: Monitoring and Defending Amplification DDoS Attacks，” Proc. Research in Attacks, Intrusions, and Defenses (RAID15), Lecture Notes in Computer Science, Vol. 9404, pp.
[2] 牧田大佑，西添友美，吉岡克成，松本勉，井上大介，中尾康二，“早期インシデント対応を目的とした DRDoS 攻撃アラートシステム，” 情報処理学会論文誌，Vol.57, No.9, pp. 1974-1985, 2016.

* 横浜国立大学大学院環境情報学府　吉岡研究室，240-8501 神奈川県横浜市保土ヶ谷区常盤台　79-7, Yoshioka Lab, Graduate School of Environment and Information Sciences, Yokohama National University , 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501
† 横浜国立大学大学院環境情報研究院/先端科学高等研究院，240-8501 神奈川県横浜市保土ヶ谷区常盤台　79-7，Graduate School of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501