DRDoS攻撃を観測するハニーポット

牧田 大佑　情報通信研究機構

〔受賞論文〕
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
牧田大佑（横浜国立大学／情報通信研究機構），西添友美（横浜国立大学），吉岡克成（横浜国立大学），松本　勉（横浜国立大学），井上大介（情報通信研究機構），中尾康二（情報通信研究機構）
情報処理学会論文誌　Vol.57, No.9, pp.1974-1985（2016）

このたび，本会の論文賞という栄誉ある賞をいただくことになり大変光栄に思う．論文の執筆にあたり貴重なご意見をくださった関係者および査読者の皆様に感謝している．さて，標記の論文はDRDoS攻撃と呼ばれるDDoS攻撃のアラートシステムを提案した論文である．しかし，その本質はDRDoS攻撃を観測する仕組みにあると思うので，本稿ではその話題を示す．

DDoS（Distributed Denial-of-Service）攻撃とはインターネット上で提供されるWeb等のサービスの妨害を目的としたサイバー攻撃である．最近はニュース等でも取り上げられるので，ご存知の方も多いと思う．標記の論文で扱うDRDoS（Distributed Reflection Denial-of-Service）攻撃はDDoS攻撃の実行手法の1つで，不適切な設定で動作するDNSやNTP等のサーバを経由して大量の攻撃通信を送りつける攻撃である．我々は，DRDoS攻撃を観測する仕組みとして，不適切な設定で動作するフリをした囮システム（ハニーポット）を提案しており，2012年10月からこれを運用している．

だが，実をいうと運用開始当初，このハニーポットはDRDoS攻撃の観測を目的としたものではなかった．当時，インターネット上の複数のDNSサーバを使用するマルウェアを調べていて，一般のISP回線でDNSサーバを運用したらどのような通信が見えるのかを調査するためにハニーポットの運用を開始した．すると，運用開始直後はほとんど通信が観測されなかったが，2カ月ほど経ってから突然大量のパケットが観測されるようになった．そのときはその大量のパケットが何を示しているのか分からなかったが，調べていくうちにDNSサーバを悪用するDRDoS攻撃であるという結論に辿り着いた．そこで，観測の目的を切り替え，攻撃に加担しないように通信制御機構等を追加し，このDNSサーバをDRDoS攻撃のハニーポットにすることを決めた．その後，ハニーポットの改良を進める過程でドイツのSaarland大学の研究者らも同様のハニーポットを構築していることを知り，彼らとともにAmpPot（標記の論文ではDRDoSハニーポットと記載）という名前で，このハニーポットを情報セキュリティ系の国際会議RAID'15で発表した．

標記の論文のアラートシステムは，このAmpPotの技術を応用し，主に総務省プロジェクト“PRACTICE”において研究開発したものである．そして，国内のあるISPと連携し，アラートの精度を検証した．標記の論文はこれらの内容をまとめたものである．本稿で述べてきたように，本研究は「これをやりたい！」という意志のもとに進めてきたというよりは，偶然の発見やさまざまなきっかけから成長してきたものである．このようなきっかけを与えてくださった皆様に改めて感謝するとともに，今後も初心を忘れることなくサイバーセキュリティに関する研究に邁進していきたい．

（2017年5月17日受付）

牧田 大佑（正会員）　makita-daisuke-jk@ynu.jp
2017年3月横浜国立大学大学院環境情報学府博士課程後期修了，博士（工学）．2014年より国立研究開発法人情報通信研究機構に研究員として勤務．