4ZA-07

異なる手法のハニーポット運用による攻撃分析の基礎的研究

松永友寿 †　土田大貴 ††　沖野浩二 †††

† 富山大学大学院理工学教育部　†† 富山大学工学部　††† 富山大学総合情報基盤センター

1　はじめに

インターネットの普及に伴い増加の一途をたどるサイバー攻撃に対して，攻撃による侵入時の通信状況やマルウェアの動作など攻撃者の挙動について調査を行うことが重要である．調査する方法として，おとりサーバであるハニーポットを設置することで攻撃者の振る舞いを監視する方法がある．

ハニーポットはその対話レベルにより「低対話型」と「高対話型」の 2 種類に大別される．低対話型ハニーポットは，特定の OS やアプリケーションをエミュレートするため，比較的運用は簡単だが，得られる情報量は少ない．一方，高対話型ハニーポットは本物の OS やアプリケーションを利用するため，得られる情報量は多いが，運用が難しいという特徴がある．これらのハニーポットを用いることで，システムやネットワークへの侵入手法や侵入後の動作を分析することができる．

また，ハニーポットに蓄積される情報は，その観測環境に影響を受けることが知られている [1]．このため，手法の異なるハニーポットから得られたパケット情報を解析することで，攻撃者がどのような条件を元に攻撃を行っているかを把握することに利用できると考えられる．

そこで本研究では，手法の異なるハニーポットを新規に運用し，収集されたパケットの差に着目することで攻撃者を分類し，攻撃予知等に利用できるかを考察する．

2　実験

2.1　提案手法

本研究では対話レベルや OS が異なるハニーポットを運用する．データを取得するためのハニーポットについてまとめた表を表 1 に示す．

Lurker[2] と Dionaea[3] は低対話型に分類されるが，Lurker は SYN パケットに対して SYN+ACK のみを返す単純なハニーポットとなっているため，区別のため超低対話型としている．Ubuntu Server 18.04.3 LTS(以下，Ubuntu) と Windows Server 2019(以下，Windows) は高対話型に分類され，サーバとして運用していると見せかけるためのサービスをそれぞれ起動した．

以上，4 種類のハニーポットをデータ取得のために新設し，これらのハニーポットへの通信を PCAP として収集する．

表 1　設置ハニーポット

分類	OS	ソフトウェア
超低対話型	Unix 系	Lurker
低対話型	Unix 系	Dionaea
高対話型	Windows Server 2019	IIS + Default
	Ubuntu Server 18.04.3 LTS	Apache + Samba

2.2　開放ポート

各ハニーポットで開放するポートを表 2 に示す．Lurker は性質上，全ポートを開放している．残りのハニーポットについては HTTP(S) と SMB に対応したポートを開放している．また，高対話型ハニーポットの Ubuntu と Windows は OS を攻撃者に伝えるため，それぞれ遠隔操作を使用するための 22 ポート，3389 ポートを開放している．

表 2　開放ポート

ハニーポット	ポート番号
Lurker	全ポート
Dionaea	80，443，445
Ubuntu(高対話型)	22，80，443，445
Windows(高対話型)	80，443，445，3389

3　観測結果

本研究では異なる手法のハニーポット運用による攻撃分析の基礎的研究として日によるパケット数の変化，ポート別パケット数について着目し，観測を行った．また，比較しやすくするため，Ubuntu と Windows はそれぞれ 22 ポート，3389 ポートを除いてデータ解析をしている．実験に利用したデータは，2019 年 12 月の 2 週間に取得した．ハニーポットは，取得開始から 45 時間後以降に順次設置した．

3.1　時間によるパケット数の変化

総パケット数についての結果を図 1 に，SYN パケットについての結果を図 2 に示す．ハニーポットの運用を始めた 2 日目に総パケット数，SYN パケット数ともに多くなっていることが確認できる．特に，SYN パケット数での結果で顕著にあらわれている．

SYN パケット数の割合が高い Lurker に対して，Dionaea は総パケット数が多い結果となっている．また，Windows は突発的に総パケット数が多くなっているが SYN パケットをあまり送られていないため，同一 IP アドレスとの通信が多いと予想される．

Fundamental Study of Attack Analysis by Heneypots with different methods

†Tomotoshi MATSUNAGA, Graduate School of Science and Engineering for Education,University of Toyama

††Taiki TSUCHIDA, Faculty of Engineering,University of Toyama

†††Koji OKINO, Information Technololgy Center,University of Toyama

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.

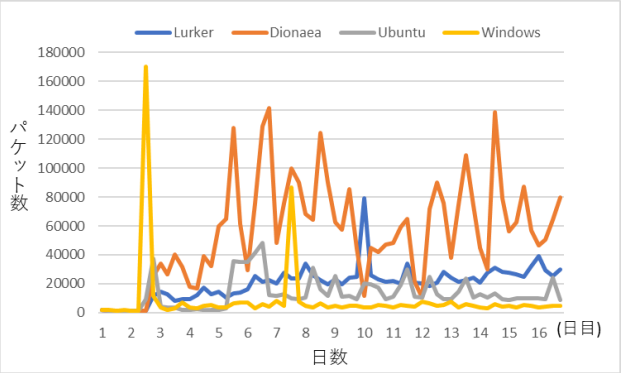

図 1　総パケット数の変化

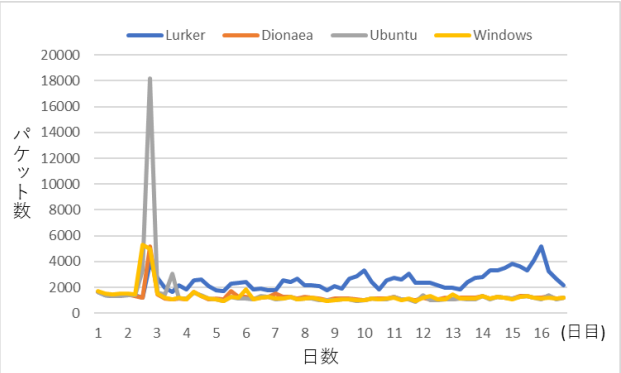

図 2　SYN パケット数の変化

3.2　ポート別パケット数

次に，各ハニーポットに対するアクセスポート上位 5 つについての結果を表 3 に示す．超低対話型ハニーポットの Lurker と他のハニーポットで上位ポートの順位に違いが出ていることが確認できる．また，445 ポートについて比較すると，Dionaea のパケット数が最も多くなっている．本実験での Windows は，脆弱性の多い SMBv1 を有効化していない．そのため，SMBv1 が有効であると見せかけている Dionaea のパケット数が多くなったと推測される．高対話型ハニーポットの Ubuntu と Windows ではウェルノウンポートでの大きな差はないが，いずれも開放していないポートへのパケット数が多くなっている．

4　考察

超低対話型ハニーポットである Lurker は SYN パケットに対して SYN+ACK を返し，全てのポートを開放しているため，SYN パケット数や送信先ポートにおいて他のハニーポットとの差が出ている．しかし，他のハニーポットで上位に来ている 445 ポートや遠隔操作を目的としているポートを狙っているため，全てのポートに対して無差別にパケットを送っているわけではなく，意図してポートを選んでいると考えられる．

22 ポート，3389 ポートを除いて解析することでポート条件がほぼ同じになっている Dionaea，Ubuntu，Windows は SYN パケット数の変化に対して，総パケット数の増加のタイミングが異なる．以上より，攻撃者は狙いやすいポートを選んでおり，SYN パケットに対するハニーポットの応答や有効バージョンによって手法を変えている可能性がある．

表 3　上位アクセスポート (パケット数)

Lurker		Dionaea	
ポート番号	パケット数	ポート番号	パケット数
22	114,441	445	1,805,941
1433	69,151	80	13,747
445	47,520	23	3,925
23	39,387	443	3,104
3389	16,459	1433	2,646
Ubuntu		Windows	
ポート番号	パケット数	ポート番号	パケット数
445	25,999	445	30,640
80	17,438	80	16,749
54770	11,516	51088	10,925
59586	11,469	51087	10,796
23	4,349	443	5,731

5　今後の課題

本実験は 2 週間と短期間でのデータ解析となったため，今後は長期的な観測による差異を調査することが課題である．また，Lurker の上位アクセスポートのみに遠隔操作を目的としたポートが多いことや 445 ポートへのパケット数が多い原因を探るため，SYN+ACK に対する攻撃者の反応を調べていく．さらに，日にちや時間帯によるパケット数の変化と国との関連性を調査するため，IP アドレスに着目して分類を行っていく．

6　おわりに

対話レベルや OS が異なる複数のハニーポットを新たに設置して得られたデータを項目ごとに分析した．観測結果から，対話レベルによって総パケット数や送信先ポートに差が出ることが確認できた．また，バージョンの有効化の有無でそのポートに対するパケット数に差異が出ることが分かった．短期間の調査では，対話レベルや OS に差をつけることで攻撃者は攻撃対象の環境により送信先ポートや送信回数を変えている可能性がある．

今後の課題としては，長期的な観測による差異を調査することや，IP アドレスを分類することで国と攻撃先ハニーポットとの関連性について調査することなどが挙げられる．

参考文献

[1] 青木一史，川古谷裕平，秋山満昭，岩村誠，針生剛男，伊藤光恭他，”能動的攻撃と受動的攻撃に関する調査及び考察，”情報処理学会論文誌，vol.50，no.9，pp.2147-2162，2009.
[2] Lurker，https://github.com/m-mizutani/lurker
[3] Dionaea，http://dionaea.carnivore.it

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.