

ダークネット観測結果とアクティブスキャンを用いた 踏み台検出手法の提案

後藤 洋一

中村 康弘

防衛大学校 情報工学科
239-8686 神奈川県横須賀市走水 1-10-20
em52038@nda.ac.jp, yas@nda.ac.jp

あらまし ダークネットへ到達するパケットのほとんどはマルウェアの感染活動あるいは踏み台を経由した走査活動等に起因すると考えられる。これらの活動を分析してセキュリティ対策に役立てることを目的としたダークネット観測に関する様々な研究が行われているが、パッシブ観測のみでは当該攻撃が踏み台を経由したものであるか否かを判定することは困難であった。この研究では、TCP セッション開始時における送信元のパケット応答速度と送信元へのアクティブスキャンの応答速度を比較し、踏み台経由の攻撃を検出する手法を提案する。実ネットワーク上のダークネットにて実験を行った結果から提案手法を評価する。

A study of stepping stone detection using active scan and observation of Darknet

Yoichi Goto

Yasuhiro Nakamura

National Defense Academy and Department of Computer Science.
1-10-20, hashirimizu, yokosuka-shi, Kanagawa 239-8686, JAPAN
em52038@nda.ac.jp, yas@nda.ac.jp

Abstract Connection requests to Darknet are due to computer virus infection activities or network scanning via stepping stones. Various studies on Darknet monitoring have been carried out for that aims to effective security measure by analyzing these activities. But on the target side equipments of the attack or scan, it is difficult to determine the connection via stepping stones. In this study, a method will be proposed to detect the connection via a stepping stone, by compare a response time of TCP connection request and active scan to source address. Proposed method will be evaluated by the result of experiments on real Darknet.

1 はじめに

近年サイバー攻撃がますます増加しており、ネットワーク内の脅威が増大している [1]。こういったサイバー攻撃の発生状況を把握するために、NICTER [2, 3] や、警察庁が行っているセンサによる観測等がある [4]。サイバー攻撃の発生状況をモニタリングすることは、情報セキュリ

ティ対策を行う上で、非常に重要である。この NICTER や警察庁が行っている観測では、ダークネットと呼ばれる未使用 IP アドレス空間に到達するパケットを使用している。ダークネットに到達するパケットは基本的に不正であり、マルウェアの感染活動や踏み台を経由したものが多く考えられている。そこで本提案手法で

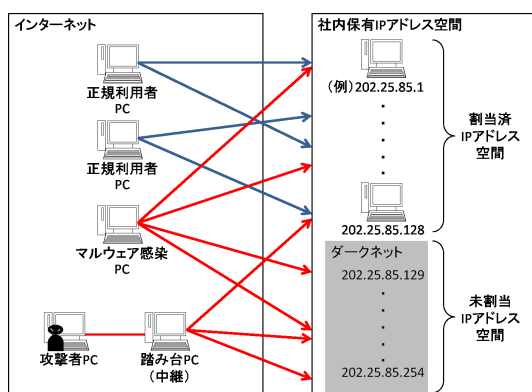


図 1: ダークネットと踏み台からの攻撃 [5]

はダークネットに通信する送信元アドレスのうち、踏み台と考えられるアドレスをアクティブスキャンを用いて検出する手法を提案する。

本論文の構成は、第 2 章でダークネット観測について、第 3 章で踏み台検知に関する研究、第 4 章で本論文の提案手法である踏み台の検出要領、第 5 章で実ネットワーク上のダークネットに着信のあった IP アドレスに対して本研究手法を適用した結果を述べ、第 6 章でまとめと今後の課題を述べる。

2 ダークネット観測

ダークネットとは機器が割り当てられていないが到達可能な IP アドレス空間である(図 1)。ダークネット上ではサービスの提供を行っていないため、ダークネット内のアドレスを宛先とする通信は発生しないはずであるが、実際には数多くのパケットが到達している。その発生原因は、アドレスの誤入力等の人為的な誤りの他、マルウェアの感染活動、DDoS 攻撃の影響によるバックスキャッタ、ホストスキャンなどの何らかの不正な目的に起因するものと考えられる。

ダークネットへ到達するパケットを観測することにより、ネットワークに対する脅威の兆候やサイバー攻撃の状況を大局的に把握することができるため、観測手法を確立することはセキュリティ対策を行うための有効な手段のひとつである。このため、近年、ダークネット観測に関する数多くの研究や実装が行われている。

表 1: パッシブ型とアクティブ型の比較

項目	ブラックホール モニタリング	ハニーポット モニタリング
情報量	少ない	多い
安全性	高い	低い
運用コスト	低い	高い
アドレス範囲	広い	狭い

ダークネットの観測結果を公表している具体例には、NICTER や Network Telescope[6] がある。これらはブラックホールセンサを用いたブラックホールモニタリングであり、大規模なダークネットを対象とした実装である。一方、ダークネット内にハニーポットを設置してアクティブに観測するハニーポットモニタリング手法も検討されている。宇都宮ら [7] はダークネット内にハニーポットを設置することで、ダークネット観測への影響を調べた結果から、 $/24$ のネットワークにつき 1 台のハニーポットを設置することでライブネットに近い攻撃情報を取得できる可能性を示している。しかし、攻撃の詳細を取得できる代わりにハニーポット自身が攻撃者となる危険性があるため、運用のコストが増大する。ブラックホールモニタリングとハニーポットモニタリングの比較を表 1 に示す。

3 踏み台検知に関する既存研究

踏み台とはネットワークを経由して他所のコンピュータに不正アクセスを行うために中継として利用される機器のことを言う。攻撃者は中継機器のアクセス権を得るために、当該機器のセキュリティ上の脆弱性を利用する。攻撃者は踏み台を利用することにより、攻撃者自身のアドレスを隠蔽して不正アクセスを行うことができる。

踏み台が不正アクセスを中継する手法には、
 (1) NAT や NAPT[8] ,
 (2) トンネリング ,
 (3) リモート接続

などがある。(1) は一般に中継機器がルータとして機能する。(2) は SSL/TLS や VPN を用い

て中継機器が攻撃者のパケットをカプセル化して配送する。(3)は攻撃元から中継機器のアクセス権を得た上で中継機器を遠隔操作して不正アクセスを行う。いずれの手法においても中継機器がTCPセッションの発呼側となるため、標的である着呼側からは中継機器を攻撃者と見なしてしまう。このため、当該不正アクセスが踏み台を経由したものであるか否かを判別する手法の確立が望まれる。

文献[9]は、攻撃元から踏み台へのリモート接続と踏み台からの不正アクセスの両者を観測できる前提の下、これらの時間差を計測することで踏み台として動作している機器を特定する手法を提案している。したがって、ダークネット観測のように標的側でのみ観測を行う場合には踏み台判定ができない。

また、文献[5]は、ダークネットに到達するTCP接続要求に対し、セッション確立までを行い、その際のクライアント側の応答時間とOSフィンガープリントの判定結果が変化することを利用して踏み台を検出する手法を提案している。NATによる踏み台の場合は攻撃者のOSフィンガープリントを取得可能なため踏み台検出が可能であるが、トンネリングによる踏み台の場合は踏み台が発呼側となるため攻撃者側のOSフィンガープリントが取得できず、踏み台を検出することができなかった。

そこで本研究では、文献[5]の手法に加えて、アクティブスキャンを行い、それらの結果を比較することにより踏み台検出を行う。

4 提案手法

文献[5]ではクライアント側の応答時間とOSフィンガープリントが変化することを利用して踏み台検出を行っていた。したがって、これらに変化が無い場合は踏み台を検出できなかった。ここでは、パッシブ計測結果が得られたアドレスに対して同時にアクティブ計測を行い、これらの結果を比較することで踏み台検出を行う手法を提案する。

提案手法の全体の処理手順を図2に示す。以下、それぞれの処理について述べる。

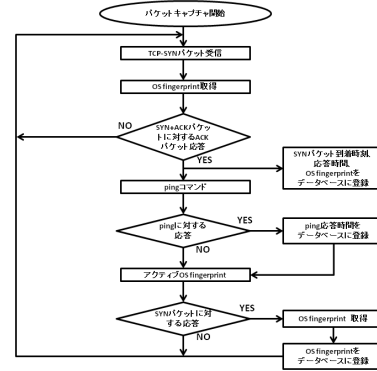


図 2: 提案手法の処理手順

4.1 パッシブ計測

文献[5]の手法を用いて、個々のクライアントアドレスごとに応答時間 T_t^p と OS 推定結果 F_t^p を取得する。ここで p はパッシブ計測を表し、 t は SYN パケットの着信時刻である。クライアント側の応答時間とは、TCPセッション確立時におけるサーバからの SYN+ACK パケットに対してクライアントから ACK パケットが返信されたとき、それらの時間差を言う。すなわち、ダークネットに到達した SYN パケットの到着時刻を t 、SYN+ACK パケットの送信時刻を t' 、返信された ACK パケットの到着時刻を t'' とすると、応答時間 T_t^p は、

$$T_t^p = t'' - t' \quad (1)$$

である。

4.2 アクティブ計測

次に、パッシブ計測結果が得られた個々のクライアントアドレスに対して、アクティブ計測による応答時間 T_t^a および OS 推定結果 F_t^a を求める。ここで a はアクティブ計測を表し、 t はパッシブ計測時のクライアントからの SYN パケットの着信時刻である。 T_t^a は ICMP ping により計測し、 F_t^a はアクティブ SYN に対する SYN+ACK 応答パケットにより判定する。

4.3 計測結果に基づく踏み台検出

パッシブ計測とアクティブ計測の両者の結果が得られたとき，以下の条件を満たす場合に踏み台であると判定する．

条件 (1) $F_t^p \neq F_t^a$

条件 (2) $T_t^p \gg T_t^a$

条件 (1) では，同一 IP アドレスに複数の OS が検出された場合に踏み台と判定する．すなわち，パッシブ計測結果のクライアントからの SYN パケットから推定される OS とアクティブ計測の SYN+ACK 応答から推定される OS が異なった場合，踏み台と判定する．条件 (2) では，アクティブに計測した応答時間よりも，サーバからの SYN+ACK に対しクライアントが ACK を応答する時間が大きいときに踏み台と判定する．

この際， T_t^p と T_t^a の各応答時間は経路上の輻輳状態などに依存したばらつきを含むため，比較が難しい．しかしながら，当該通信が踏み台を経由していた場合， T_t^p は攻撃者から踏み台までの遅延時間と踏み台から標的までの遅延時間の和になっていると考えられる．したがって，条件 (2) の比較は以下の手順で行う．

- (1) T_t^p が T_t^a の最大値よりも大きいアドレスを取得する．
- (2) 取得したアドレスについて，過去一定時間内の T_t^p の平均 $\bar{T}^p$ と T_t^a の最大値の平均 $\bar{T}^a$ を算出する．
- (3) $\bar{T}^p > \bar{T}^a$ のとき，踏み台と判定する．

5 提案手法の実装

提案手法を検証するために実装を行った．全体の構成を図 3 に示す．

システムはパッシブ計測を行う監視装置とアクティブ計測を行うアクティブスキャン装置から成る．監視装置はアドレスを割り当てないステルス型のネットワークインターフェースを用いて組織 LAN の境界ルータの通信を監視する．

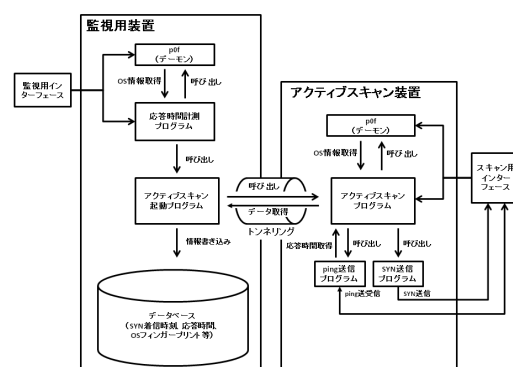


図 3: 実装システム構成図

アクティブスキャン装置内ではグローバルアドレスをもつインターフェースを経由してスキャンパケットの送受信を行う．監視装置とアクティブスキャン装置は複数のネットワークインターフェースがあれば 1 台の処理装置で兼ねることができるが，本実装においては 2 台構成としたため，SSH のトンネルを経由して相互通信させた．両装置の計測結果は監視装置側のデータベースに格納する．

監視装置内の処理プログラム

p0f p0f[10] をデーモンモードで動作させ，ACK 応答の OS フィンガープリントからクライアントの OS を推定する．

応答時間計測プログラム ダークネットに着信した SYN パケットに対し，TCP セッションの確立までを監視し， T_t^p を計測する．計測結果をデータベースに保存する．

アクティブスキャン起動プログラム データベースのトランザクションを監視し，アクティブスキャンプログラムを起動させる．

アクティブスキャン装置内の処理プログラム

p0f デーモンモードで動作させ，アクティブスキャンの応答を監視してクライアントの OS を推定する．

アクティブスキャンプログラム 監視装置からの起動指示を待ち受け，指定の IP アドレスに

表 2: 計測情報

パッシブ計測	アクティブ計測
SYN パケット到達時刻 t	ping の T_t^a の平均値
送信元 IP アドレス src	ping の T_t^a の最小値
送信先 IP アドレス dst	ping の T_t^a の最大値
応答時間 T_t^p	ping の T_t^a の分散
OS 判定結果 F_t^p	SYN による T_t^a
	OS 判定結果 F_t^a

表 3: ダークネットへの着信状況と実験結果

	個数
ダークネット内のアドレス数	962
応答のあったコネクション要求数	333
同上ユニークソースアドレス数	257
条件 (1) による踏み台検出数	8
条件 (2) による踏み台検出数	31
踏み台検出総数 (重複除く)	37

対して ping スキャンおよび SYN スキャンを行い, p0f による OS 判定結果を取得して監視装置側に返送する.

ping 送信プログラム ping パケット送信を複数回行い, 応答時間を求める.

SYN 送信プログラム SYN パケットを複数同時に送信する.

パッシブ計測およびアクティブ計測により取得する情報を表 2 に, データベースに記録された計測情報の例を図 4 に示す. 表示データの各列はそれぞれ, t , src, dst, T_t^p , ping 応答時間の最小値, 平均値, 最大値, 分散値, F_t^p , F_t^a を表しており, 時間の単位は μs である.

6 実験結果

実ネットワーク上のダークネットを用いて本提案手法を検証した. 実験は 2014 年 8 月 19 日 18 時 00 分から 20 日 18 時 00 分の 24 時間で行った. この間のダークネットへの着信状況を表 3 に示す.

条件 (1) により, F_t^p と F_t^a が異なったアドレスは 8 個検出され, 同一アドレスで Windows

系と Linux 系の両者の OS が検出されたアドレスは 3 個存在した.

次に, 条件 (2) により $T_t^p \gg T_t^a$ となったアドレスは 33 個あり, このうち $\bar{T}^p > \bar{T}^a$ となったアドレスは 31 個であった.

条件 (1) により踏み台と検出されたアドレスと条件 (2) により踏み台と検出され, かつアドレスの重複を除いたアドレス数は 37 個であった.

以上の実験結果により, 条件 (1) に基づいて 8 個のアドレスが踏み台と判定することができたが, 踏み台と攻撃者の OS が同じ場合にはこの条件のみでは踏み台を検出することができない.

これに対し, 条件 (2) による検出では 31 個のアドレスが踏み台と判定された. すなわち, OS が同一のために条件 (1) では判定できない場合においても, 応答時間の差異から踏み台を検出できる可能性を示唆しているものとする.

7 まとめと今後の課題

本論文では, TCP コネクション要求時の応答時間と OS フィンガープリントに着目し, ダークネットに通信してきたアドレスに対してアクティブスキャンを行い, 踏み台を判別する手法を提案した. 本提案方式では, TCP コネクション要求を行ったアドレスに対して即時に応答時間と OS フィンガープリントを確認するため, クライアントアドレスが DHCP による動的なものであっても, アドレスが変更される前に判定を行うことができる. 実ネットワーク上のダークネットを用いて提案手法を検証した結果, ダークネットには踏み台を経由していると思われる通信が多く発生していることが分かった.

なお, アクティブ計測における応答時間は, その値のばらつきが大きいため, 特定の条件下で判定精度が低下する可能性がある. 判定の安定性および精度向上のためには, 複数回の計測結果を元に判定する必要があると考える.

今後は, 実ネットワーク上に踏み台を設置して実験を行い, 提案手法の有効性を評価する必要がある.

2014/08/19 18:28:55.370063	202.xxx.xxx.153	202.xxx.xxx.8	48845	48829	49702	52556	860	41683	"Windows XP"	"Windows 7 or 8"
2014/08/19 18:30:31.703530	68.xxx.xxx.188	202.xxx.xxx.90	128893	126986	129062	151668	4269	127288	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 18:35:29.952816	68.xxx.xxx.188	202.xxx.xxx.90	130892	127003	129288	141445	2665	128752	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 19:10:14.529742	68.xxx.xxx.188	202.xxx.xxx.191	132782	126978	128473	144022	2569	128702	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 19:21:05.749697	196.xxx.xxx.137	202.xxx.xxx.97	838269	615178	626948	643433	9467	631154	"Linux 3.1-3.10"	"Linux 3.x"
2014/08/19 19:24:02.442438	202.xxx.xxx.153	202.xxx.xxx.10	47796	48873	49645	52241	635	51207	"Windows XP"	"Windows 7 or 8"
2014/08/19 20:37:36.878735	196.xxx.xxx.137	202.xxx.xxx.66	452010	444841	471734	513249	15690	549620	"Linux 3.1-3.10"	"Linux 3.x"
2014/08/19 22:03:22.677312	68.xxx.xxx.188	202.xxx.xxx.131	129844	126989	129166	143999	3313	136522	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 22:03:44.561479	68.xxx.xxx.188	202.xxx.xxx.245	129662	127005	129044	145116	2828	128511	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 22:10:36.861572	68.xxx.xxx.188	202.xxx.xxx.245	129013	126987	128751	141067	3069	137388	"Windows XP"	"Windows XP [fuzzy]"
2014/08/19 23:11:21.311523	112.xxx.xxx.99	202.xxx.xxx.44	49840	46141	50596	56724	3039	50280	"Windows XP"	"Windows XP [fuzzy]"
2014/08/20 00:42:42.474862	68.xxx.xxx.188	202.xxx.xxx.43	130953	127007	129425	151997	5174	127283	"Windows XP"	"Windows XP [fuzzy]"
2014/08/20 02:21:41.783363	211.xxx.xxx.231	202.xxx.xxx.222	80019	76156	76302	76706	392	76280	"Linux 3.1-3.10"	"Linux 3.x"
2014/08/20 03:04:06.158682	68.xxx.xxx.188	202.xxx.xxx.130	127493	126999	130116	145518	4422	127514	"Windows XP"	"Windows XP [fuzzy]"
2014/08/20 04:40:10.832518	119.xxx.xxx.123	202.xxx.xxx.125	72271	0	0	0	0	76887	"Windows XP"	"Windows 7 or 8 [fuzzy]"

図 4: 計測情報の例

参考文献

- [1] 総務省, 情報通信白書, 第 1 部 第 3 章 第 2 節 第 1 項, 高度化・複雑化するサイバー攻撃, <http://www.soumu.go.jp/menu/seisaku/hakusyo/index.html>
- [2] 中里純二, 島村隼平, 衛藤将史, 井上大介, 中尾康二, nictar によるネットワーク観測および分析レポート～ネットワークインシデントの前兆～, 信学技報, Vol.113, No.95, ICSS2013-14, pp.79–84 (2013)
- [3] 中尾康二, 松本文子, 井上大介, 馬場俊輔, 鈴木和也, 衛藤将史, 吉岡克成, 力武健次, 堀良彰, インシデント分析センタ nictar の可視化技術, 信学技報, ISEC2006-51 (2006).
- [4] 警察庁情報通信局情報技術解析課サイバーテロ対策技術室長, インターネット定点観測の結果と攻撃の技術的手法, http://www.npa.go.jp/cyberpolice/material/pdf/20130709_teiten.pdf
- [5] 後藤洋一, 李熙貞, 中村康弘, ダークネット観測を利用した踏み台検出手法の提案, FIT2014, L-027 (2014)
- [6] CAIDA (Center for Applied Internet Data Analysis), The UCSD Network Telescope, <http://www.caida.org/projects/network.telescope/>.
- [7] 宇都宮理人, 土田耕平, 曽根直人, 森井昌克, ダークネット観測に対してハニーポットが与える影響, 暗号と情報セキュリティシンポジウム SCIS2013, 4C2-1 (2013)
- [8] G. Tsirtsis, P. Srisuresh, Network Address Translation – Protocol Translation (NAT-PT), RFC 2766 (2000)
- [9] 竹尾大輔, 伊藤将志, 鈴木秀和, 岡崎直宣, 渡邊晃, コネクションベース方式による踏み台攻撃検出手法の提案, 情報処理学会論文誌, Vol.48, No.2, pp.644–655 (2007)
- [10] Michal Zalewski, p0f v3(version 3.07b), <http://lcamtuf.coredump.cx/p0f3/>.