

ハニーポットを設置したダークネットのアクセス特性

Access Characteristics of Darknet Including Honeypot

曾根 直人† 横田 凌一‡ 大久保 諒‡ 森井 昌克‡
Naoto Sone Ryouichi Yokota Ryo Okubo Masakatsu Morii

1. まえがき

今日では様々なシステムやデバイスがインターネットに接続され、ネットワークトラフィックは莫大なものとなっている。その中には正規の通信に加え、マルウェアや不正アクセスに由来する不正トラフィックも含まれる。不正トラフィックを阻止するためにファイアウォールやIPSが開発され利用されている。しかし正規のトラフィックと不正トラフィックが混在している場合、正確にそれらを分離することは困難である。そこで、原理的に正規トラフィックの発生しない未使用のIPアドレス空間(ダークネット)を利用し、ダークネットへ届くパケットを観測することでマルウェアなどの活動傾向を把握する研究が行われている。また、ハニーポットと呼ばれる罠サーバをネットワーク上に設置し、そこへ接続してくる通信を観測、分析する研究も行われている[1]。

ダークネットの観測は大規模な空間を簡単に観測することができるが、応答するサーバが存在していないため、不正トラフィックの詳細な解析には不向きである。一方、ハニーポットはより詳細な不正トラフィックの解析が可能であるが、一般に運用コストが高く、観測IPを増やすことが難しい。そこで我々はNAPT技術を応用し、複数のIPアドレスを1台のハニーポットで観測できるシステムを運用している[2][3]。そのシステムを用いてダークネットの一部に観測点と呼ぶハニーポットが応答するIPを設定し、ハニーポットが及ぼす影響について観測を行っている。本稿では、観測結果について述べると共にそれに対する考察を行う。

2. インターネットにおける不正トラフィックの観測

2.1 ダークネット

組織などに割当てられたグローバルIPアドレス空間のうち、未利用な空間をダークネットと呼び不正トラフィックの観測に利用されている。これはダークネットは未利用の空間のためサーバやクライアントは存在せず、その範囲内には応答を返す端末は存在しない。そのため、本来であればダークネットに届くパケットは存在しないはずである。しかし実際にはダークネット宛に送られてくるパケットが存在する。これらのパケットが発生する原因としては

- 誤設定による通信
- マルウェアその他によるスキャン
- ソースアドレスをダークネットに詐称されたパケットのバックscatter

が考えられる。実際にサーバや端末が利用しているネットワーク(ライブネット)では、正規な通信と上記の不正な通信が混在しており、正確な分類は困難であるがダークネットであれば正規な通信は存在しないため、不正な通信のみを観測することができる。この特性を利用し、大規模なダークネットを観測するシステムの開発が行われている。

2.2 ハニーポット

ハニーポットはネット上に設置された罠サーバであり、偽のサービスを稼働させ、不正な接続を待ち受けるシステムである。ハニーポットでは、通信や実行されるコマンドなどアプリケーション層におけるログを取得できるため、詳細な攻撃手法の分析が可能である。ハニーポットは実際のアプリケーションやOSを利用して応答する高対話型ハニーポットとエミュレーションによりアプリケーションやOSの応答を行う低対話型ハニーポットがある。高対話型は現実のシステムと同じ挙動を示すために見破られ難く、攻撃の様子を詳細に記録できる。しかし実際のシステムと同様にハニーポットで動かすアプリケーションに危険な脆弱性が存在していた場合、ハニーポットそのものへ侵入されるリスクがあり、慎重に運用する必要がある。低対話型ではアプリケーションの応答をエミュレーションにより行うため、実際とは異なる挙動を示す。したがって攻撃者にハニーポットということを見破られる可能性がある。但し、高対話型のようにシステムへ侵入される可能性は低く、運用のコストを抑えることができる。

2.3 複数IPでのハニーポット運用

ハニーポットは罠のサービスであるため、一般に公開されておらず、接続してくるのはポートスキャンやランダム接続してきた攻撃者に限られる。そのため、単独のIPで運用していたのでは攻撃を受けることは少なく、待機時間の占める割合が多い。複数のハニーポットを運用すればより多くの攻撃を受ける可能性が高くなるが、運用コストも増加する。そこでルーティングを工夫し、1台のハニーポットで複数のIPを観測するハニーポットファームが提案されている。一般的なハニーポットファームはGREによるトンネリングを利用し、ハニーポットへパケットを送り込むが、我々はより手軽な手法としてDNATを利用した手法も提案している。DNATを用いることで、より簡易に観測点を増やすことができる。

3. ダークネット観測環境

ダークネット観測環境は純粋なダークネットに届くパケットの情報を保存するシステム及びハニーポット、ハ

† 鳴門教育大学大学院学校教育研究科

‡ 神戸大学大学院工学研究科

ニーポットへパケットを転送するルータから構成される。
(図1)

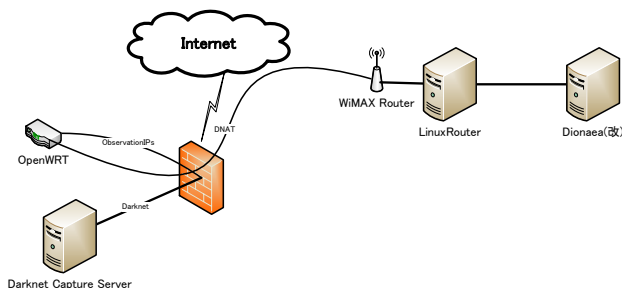


図1 ダークネット観測環境

3.1 ダークネット

ダークネットとしてクラス B ネットワークの一部(/18)を利用した。インターネットからルーティングされてきたパケットはファイアウォールで組織の LAN へのルーティングされる。ここでダークネット向けのトラフィックは観測用のサーバへ送られる。サーバではダークネット宛のパケットをキャプチャし、パケットのヘッダ情報をデータベースに蓄積している。

3.2 ハニーポット

ダークネットは届いたパケットに対して応答するホストが存在しないため、アプリケーション層などの詳細な情報は入手できない。そこでハニーポットを利用し、それらの情報を得られるようにした。具体的には/18のダークネットの一部に観測点を設置し、そのアドレスではハニーポットが応答するようにした。観測点はダークネット内に32個設置した。観測点として設定したIPアドレスはルータにより、DNATを実施するOpenWRTルータへルーティングされる。OpenWRTルータ[4]では観測点IPへ送られてきたパケットのデスティネーションアドレスをハニーポットのIPへ書き換え(DNAT)を行う。

ハニーポットシステムとしてはDionaea(改)[6]を利用した。これはオリジナルのDionaea[5]ではMySQLをエミュレーションが十分に実装できておらず、多くのMySQLコマンドに対する応答が”Lean SQL!”に固定されており実際のMySQLサーバーとは異なる応答を行ってしまうため

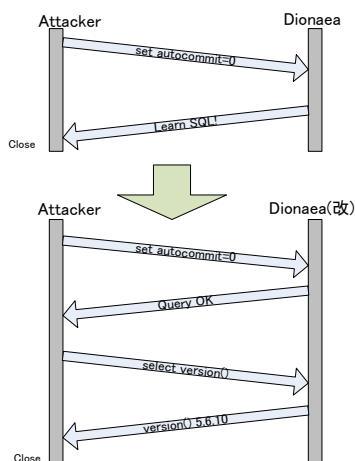


図2 Dionaeaの改良

ある。Dionaea(改)はMySQLの応答バリエーションを増やし、実際のMySQLの応答に近づけるよう修正を行なった。この改良により、従来型では”Learn SQL!”を応答直後に切断されていたが改良型ではversionを確認するためのコマンドが送信されてくるなど通信に変化が見られた(図2)。Dionaeaで観測されたいくつかのMySQLコマンドに対して表1に示すような応答を行うよう改良を施した。

表1 DionaeaにおけるMySQLコマンドの改良

攻撃者の入力	従来型の応答	改良型の応答
set autocommit=0	Learn SQL!	Query OK
drop function cmdshell	Learn SQL!	ERROR 1305 (42000: FUNCTION(UDF) cmdshell does not exist
drop function my_udfdoor	Learn SQL!	ERROR 1305 (42000: FUNCTION(UDF) my_udfdoor does not exist
drop function do_system	Learn SQL!	ERROR 1305 (42000: FUNCTION(UDF) do_system does not exist
use mysql	Learn SQL!	Database changed

4. 観測結果

2013年4月10日から4月25日の観測データからハニーポットによる応答の影響が見られたと考えられる観測結果についてまとめる。

観測環境の接続ログからTCP445番ポートに注目し、ソースアドレス毎に受信した個数を計数した。(図3)

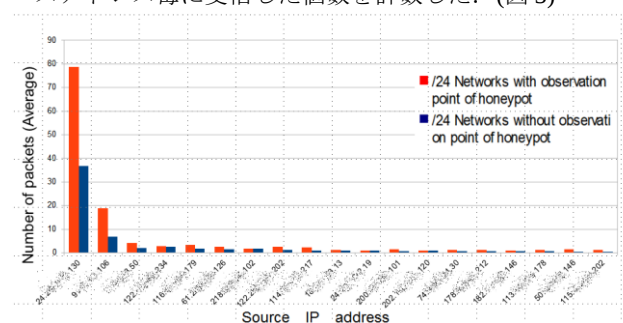


図3 TCP445へ送られたパケット

図3では観測点を含む/24ネットワークでの受信数および観測点を含まない/24ネットワークでの受信数を平均した値を示している。この図からいくつかの発信者は観測点を含む/24ネットワークでの受信数が増えていることがわかる。

最も多くのパケットを受信した発信者(24.242.*)の接続に注目し、時系列をX軸、到達IPアドレスをY軸とし図4に示す。

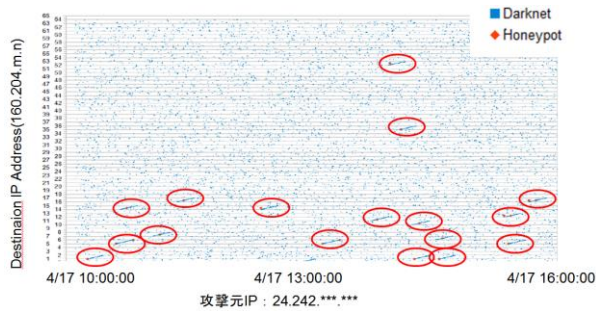


図4 24.242.*.*から TCP445 へ送られたパケット

図4において○で囲った部分は観測点を含む/24のサブネットに対してはそのサブネットの範囲を全てスキャンしていることがわかる。あるサブネットへのスキャンを拡大したものを図5に示す。

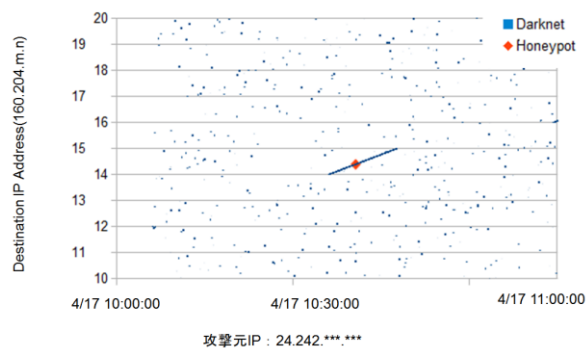


図5 サブネットへのスキャン

図3で2番目に多くのパケットを受信している発信者についてもダークネット上で得られた観測データを図6に示す。この発信者も観測点を含む/24ネットワークに対してポートスキャンを実施していることがわかる。

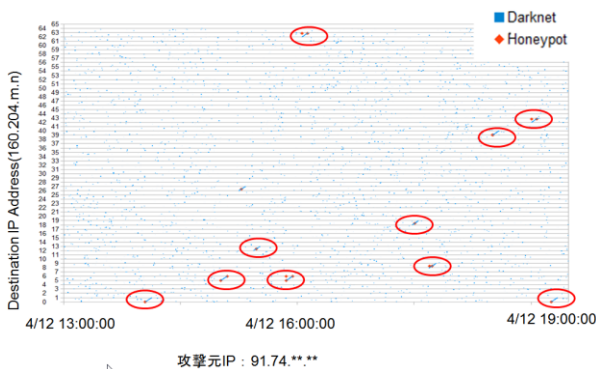


図6 91.74.*.*から TCP445 へ送られたパケット

次にMySQLへの接続に関して述べる。MySQLのエミュレーションはDionaeaの改良により従来型と比べて実機に近い応答を行う。そこでMySQLのバージョンの違いによる攻撃の変化を観測するため、select version()によるバージョン確認が実行された際に異なるバージョンで応答する実験を行なった。

実験には表2に示す2つのバージョンを返すことで、バージョンの違いによる影響を観測した。

表2 MySQLのバージョン

バージョン	
5.6.10	最新版であり、脆弱性の報告がまだない。
5.1.54	MySQLのパーミッションチェックに起因するバッファオーバーフローの脆弱性などが報告されている。

MySQLの実験期間は5.6.10を2013年4月17日から4月24日、5.1.54を2013年5月2日から5月9日に実施した。バージョン5.6.10を応答した際の発信者116.254.*.*からのMySQLへの接続を図7に示す。

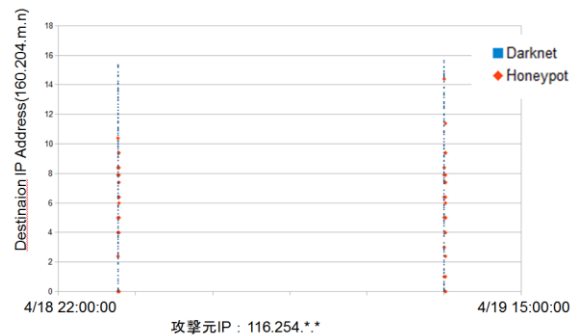


図7 発信者116.254.*.*からMySQL 5.6.10への接続

MySQLバージョン5.6.10はまだ脆弱性が発見されていない。発信者116.254.*.*からはダークネットヘランダムスキャンを続けているように見受けられる。

MySQLのバージョンとして5.1.54を応答するように設定した際、図7と同じ発信者116.254.*.*の接続を図8に示す。

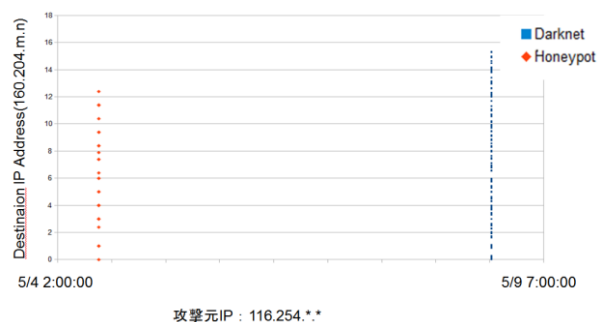


図8 発信者116.254.*.*からMySQL 5.1.54への接続

図8からまず最初に観測点のみに接続が行われていることが読み取れる。その後ダークネットに対してMySQLへのスキャンが観測されているが、観測点を除外したアドレスのみに接続を試している。これは他のアドレスに脆弱性が報告済みのMySQLが存在していないかスキャンしているのではないかと予測している。

このようにMySQLへの接続は、ハニーポットに接続後得られたバージョンの違いにより、その後のアクセス傾向が変化することが伺える。

5. まとめ

/18のダークネット内部に32個の観測点を設け、観測点のアドレスはハニーポットが応答するようにした環境を利用して、接続傾向を観測した。その結果、ハニーポットにより応答があった場合、応答アドレスを含む/24をシークエンシャルにスキャンする例を確認した。また、低対話型ハニーポット *Dionaea* を改良し、MySQLの応答精度を向上させた。これはハニーポットによるMySQLに接続後、コマンドの応答を確認しハニーポットを見破ろうとしているためである。また発信者はバージョンを確認するコマンドを利用し、接続しているMySQLのバージョンを確認する場合がある。この場合も応答するバージョンにより、その後の接続傾向が変化する事例を確認した。これは、脆弱性を含むバージョンを検索しているのではないと思われる。

MySQLのバージョン確認後のスキャンなど、アプリケーション層の情報を利用し、その後の検索活動を変化させる場合がある。このような事例は単なるダークネット観測では十分に活動を把握できない。また疎な間隔で設置したハニーポットでも不十分である。ダークネットの内部にいくつかの観測点を設置することで、このような事例を観測することができた。今後はより長期的な観測やそこから得られたデータの分析を行い、ハニーポットの設置がダークネット観測に与える影響についての分析および考察を行っていきたい。

参考文献

- [1] 中里 純二, 島村 隼平, 衛藤 将史, 井上 大介, 中尾 康二: "nicter によるネットワーク観測および分析レポート 長期ネットワーク観測に基づく攻撃の変遷に関する分析", 信学技報, ICSS2010-65, pp.53-58, Mar 2011.
- [2] 曾根直人, 正力達也, 鳥居明久, 村尾岳人, 森井昌克: "可視化によるダークネットの不正パケット解析- ハニーポットとの併用による相関分析", 信学技報, ICSS2011-46, pp.43-48, Mar. 2012.
- [3] 宇都宮理人, 土田耕平, 曾根直人, 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", SCIS2013
- [4] OpenWRT - Wireless Freedom, "<https://openwrt.org/>"
- [5] dionaea - catches bugs, "<http://dionaea.carnivore.it/>"
- [6] 横田凌一, 大久保諒, 曾根直人, 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 (その2)", 信学技報, LOIS2013-4, pp.97-100, May. 2013.