Dark IP と Snort によるネットワーク上の攻撃の検知法
New detection method of Internet attacks by Dark IP

田中 祐樹　後藤 滋樹
早稲田大学大学大学院 基幹理工学研究科 情報理工学専攻

インターネットの普及が進み、ほとんどの家庭がインターネットに接続するようになった。便利な社会が実現されたことになるが、その一方でブロードバンドの普及が不正アクセスの脅威を増幅している。インターネットが社会において重要な役割を果たすようになるにつれて、不正アクセスが社会に与える影響も大きくなっている。不正アクセスから情報を守るためには、セキュリティ技術の向上が必須である。本研究は Snort を Dark IP に適用する技法を提案して、セキュリティ技術の向上をはかる。この提案を実装して実証実験を行う。

1 Dark IP

Dark IP は「割り当てられていない IP アドレス」を利用してネットワークを観測する技術である。実際には図 1 のようにファイアーウォールまたはルータを用いて、incoming (入ってくる) パケットを受け付けて、outgoing (外に向かう) パケットは遮断するように設定する。このようにすると、Dark IP の外側から見れば、この IP アドレスが使用されていないように見える。実際には入ってくるパケットを記録して分析することで、インターネットにおける攻撃状況やワームの影響などを観測できる [1]。

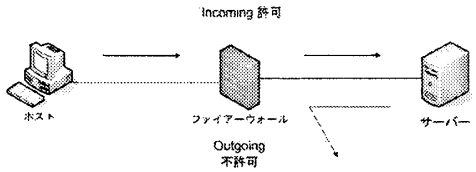

図 1: Dark IP

2 Snort

Snort は代表的な侵入検知システムである [2]。Snort は種々の OS 上で動作する。また、多くのプリプロセッサ、アウトプットプラグインが用意されていて、不正アクセスに対して柔軟な対応が可能である。Snort の利用者のコミュニティが形成されていて、情報の共有がはかられている。

3 本論文の提案

3.1 提案の概要

Dark IP を対象として Snort による観測を行う。Dark IP のアドレスに流入するパケットは、通常では利用されていない筈の宛先を持っている。つまり正常ではないと思われるパケットである。そのようなパケットが実際に正常であるか否かを判定するために、その送信元 IP アドレスが、通常のサービスの送信元、あるいは宛先 IP アドレスとなっているかどうかを調べる。

この結果として、Dark IP に流入するトラフィックの中で正常でないパケットを区別することができる。そのようなパケットに、Snort のルール文を適用して、その効果を調べる。

3.2 実証実験

本実験では、実際に Dark IP を実装したサーバと通常のサービスを行うサーバを用意して、両者が送受信したパケットを tcpdump を使って 1 週間記録する。この記録を分析して、Dark IP に記録された正常でないパケットの送信元 IP アドレスを取得する。その取得した IP アドレスに Snort のルール文を適用して、通常の Snort を適用した場合と比較検討する。

3.3 実験の結果

1 週間の間に Dark IP で受信したパケットの送信元の IP アドレスの数、Dark IP に Snort のルール文を適用した時にアラートを発生する IP アドレスの数 (併用)、Snort のルール文をデフォルトの状態で動かした時にアラートを発生する IP アドレスの数を、それぞれ表 1 に示す。

表 1: Dark IP

date	1/15	1/16	1/17	1/18	1/19	1/20	1/21
Dark IP	86	64	32	152	71	60	53
併用	13	9	11	18	11	14	18
Snort	5	10	3	9	6	15	6

Dark IP が受信したパケットの例を図 2 に示す。これは 1 月 15 日のデータである。同じ 1 月 15 日に通常のサービスのサーバに送られたパケットの例をを図 3 に示す。

Time	Destination	Protocol
2007-01-15 13:24:16.555109	.140	TCP
2007-01-15 13:24:16.555169	.138	TCP
2007-01-15 13:24:16.557516	.128	TCP
2007-01-15 13:24:16.557893	.130	TCP
2007-01-15 13:24:16.557910	.134	TCP
2007-01-15 13:24:16.559167	.132	TCP
2007-01-15 13:24:16.559191	.136	TCP
2007-01-15 13:24:16.574891	.135	TCP
2007-01-15 13:24:16.574907	.129	TCP
2007-01-15 13:24:16.576073	.131	TCP
2007-01-15 13:24:16.594118	.144	TCP
2007-01-15 13:24:16.594135	.152	TCP
2007-01-15 13:24:16.594339	.146	TCP
2007-01-15 13:24:16.594355	.156	TCP
2007-01-15 13:24:16.594366	.154	TCP
2007-01-15 13:24:16.594378	.142	TCP
2007-01-15 13:24:16.595376	.158	TCP
2007-01-15 13:24:16.595394	.150	TCP
2007-01-15 13:24:16.595404	.148	TCP
2007-01-15 13:24:16.614699	.141	TCP
2007-01-15 13:24:16.627367	.133	TCP
2007-01-15 13:24:16.627384	.137	TCP
2007-01-15 13:24:16.627395	.139	TCP

図 2: 1/15 に Dark IP に送られたパケット

Time	Protocol
2007-01-15 13:26:29.293945	TCP
2007-01-15 13:26:29.295248	TCP
2007-01-15 13:26:32.293349	TCP
2007-01-15 13:26:32.998466	TCP
2007-01-15 17:21:48.664313	TCP
2007-01-15 17:21:48.665778	TCP
2007-01-15 17:21:49.342553	TCP
2007-01-15 17:21:49.366663	SSH
2007-01-15 17:21:50.042547	TCP
2007-01-15 17:21:50.042571	SSH
2007-01-15 17:21:50.042884	TCP
2007-01-15 17:21:50.046374	SSHV2
2007-01-15 17:21:52.042690	SSHV2
2007-01-15 17:21:52.042766	TCP
2007-01-15 17:21:52.078801	SSHV2
2007-01-15 17:21:52.761485	SSHV2
2007-01-15 17:21:52.761553	TCP
2007-01-15 17:21:53.430111	SSHV2
2007-01-15 17:21:53.430161	TCP
2007-01-15 17:21:53.451352	SSHV2
2007-01-15 17:21:54.131017	SSHV2
2007-01-15 17:21:54.170489	TCP
2007-01-15 17:21:54.837703	SSHV2

図 3: 1/15 に通常のサービスのサーバに送られたパケット

Snort をデフォルトで動かしたときに検知した最初の alert は下記のようなものであった。

```
[**] [116:54:1] (snort-decoder):
Tcp Options found with bad lengths [**]
01/20-16:23:13.282908 ipaddress →
service-ipaddress:portnumber
```

Dark IP が受信したトラフィックの例として、1 月 20 日のデータを図 4 に示す。また、Dark IP の正常ではないパケットに Snort を適用するときに対象となるトラフィックの例を図 5 に示す。

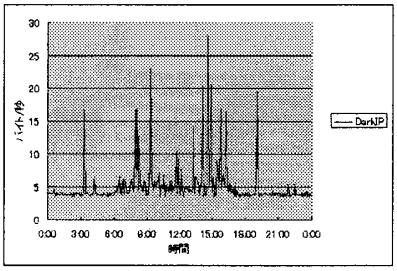

図 4: 1/20 Dark IP の受信トラフィック

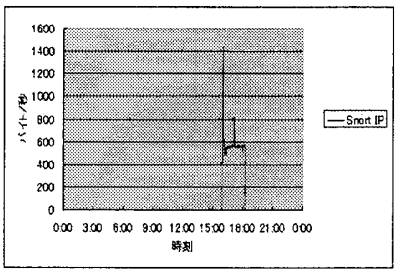

図 5: 1/20 Dark IP に Snort を適用した時

3.4 考察

Dark IP が受信する IP アドレスの数は日によって変動している。そのパケットの内容を見ると、確かに攻撃と考えられるものが Dark IP では検出されている。その中には Snort で検出できなかったものが幾つか含まれている。上に掲げた図 2 と図 3 は、そのような例である。なお Dark IP に流入するパケットが、すべて攻撃というわけではない。1 日当たり 10 ～ 20 個のパケットは通常のサービスの場合と送信元や宛先 IP アドレスが一致している。

Dark IP と通常サービスの IP のトラフィックを比較すると攻撃の特徴が分かる。DarkIP には元来はトラフィックがほとんど流れないはずであるが、攻撃を行う前の事前の下調べに相当するポートスキャンやスキャニングなどにより、一定時間にトラフィックが急増する。例えば、1 月 20 日の 15 時 45 分から 16 時 15 分をピークに Dark IP のトラフィックが増加している (図 4)。

Snort に Dark IP を適用する時の対象となるトラフィックが図 5 に示してある。図 5 でもピークが顕著に出ている。Snort をデフォルトの状態で稼働した場合に検知された最初のアラートは、上に述べたように 16 時 23 分である。図 5 に示した Snort に Dark IP を適用した場合の IP トラフィックを見ると、Snort に Dark IP を適用した場合にはピークの最大値が 16 時にある。つまり、Dark IP に Snort を適用すると、より早い段階で検知できることがわかる。

4 まとめ

本研究は Dark IP を使用してより効率的に攻撃を検知する方法について提案した。具体的には、Dark IP で取得した正常でないパケットの送信元に Snort のルール文を適用するという方式である。この方法を用いて実証実験を行ったところ、正常でないパケットを効果的に絞り込むことができることが確認できた。この新しい方法を用いると、Snort をデフォルトのルール文で動かした場合のアラートに比べて、攻撃をより多く、しかも早く検知することができた。

5 今後の課題

以下の点は今後の課題である。

- DarkIP から取得した IP を Snort にリアルタイムに反映することが望まれる。今回はリアルタイムの実装までは至らなかった。
- 今回は DarkIP として設定する IP アドレスを固定していたが、アドレスを何種類か設けて実験してみる価値がある。
- 今回の観測は 1 週間の期間であった。DarkIP の観測を長期間 (6ヶ月間ないし 1 年間程度) 継続してみることは意義がある。
- 今回は通常のサービスの種類が限られていた、サービスの種類を増やすことにより、正常なパケットを判別する精度が向上する。
- より多くのデータに適用して、Snort の閾値を最適に調整したい。

参考文献

[1] Team Cymru Darknet Project http://cymru.com

[2] Snort.org http://www.snort.org

[3] 田中祐樹「Dark IP によるネットワーク上の攻撃の検知法」早稲田大学理工学部 卒業論文 2007 年 2 月.