ハニーポットを使用した攻撃の観測と考察

石川県 川北町立 川北中学校 2年 窪田 靖之

はじめに

現在、普及化を勧めているIPv6ではIPoE方式の通信が使われている。IPoE方式の通信ではルータやアダプターなどを必要とせず、エンドツーエンドで通信をする。これは、シンプルにインターネットへ接続できるというメリットがあるが、ルータにより守られないため多くの攻撃を受けると考えられる。

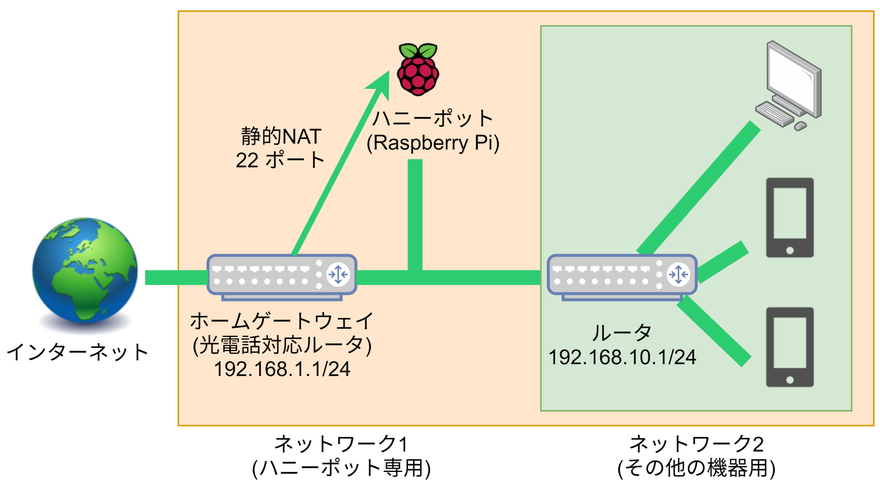
また、IPv4 over IPv6というIPv4でもIPoE方式の通信が使える仕組みもある。このような仕組みが広まれば、さらにIPoE方式の通信は増えるだろう。

一般的な家庭のインターネットの危険性を調べるために、自宅にハニーポットを設置し、実際に攻撃は来るのかを検証してみた。

調査方法

実験環境の説明

自宅のネットワークにRaspberry Piで構築したハニーポットを置くことにした。
ハニーポットを自宅内に置くというのは危険である。なぜなら、そのハニーポットが万が一乗っ取られて自宅内の他の機器に影響が出る可能性があるからである。 そこで下記のようなネットワーク構成にすることにした。 ハニーポットがあるネットワーク内にルータを2つ設置して、ネットワークを分けている。



今回はcowrieというSSHとTelnetのハニーポットを実装できるソフトウェアを使用し、SSHの機能のみ有効化した。ネットワーク1にあるホームゲートウェイからRaspberry Piへ22番ポートを転送するように設定した。7月28日16:00から8月3日17:00まで公開した。
データの解析にはGoogle データポータルを使用した。

```
{
  "eventid": "cowrie.login.success",
  "username": "root",
  "password": "admin",
  "message": "login attempt
[root/admin] succeeded",
  "sensor": "raspi-sub",
  "timestamp": "2019-08-
03T23:59:57.876701Z",
  "src_ip": "141.98.**.****",
  "session": "d2e1202cea5f"
}
```

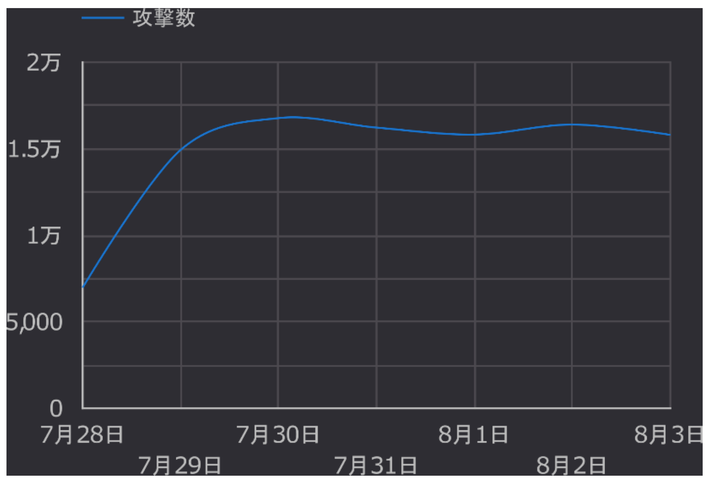
攻撃ログの一部
(IPアドレスを*で隠している)

データの解析方法

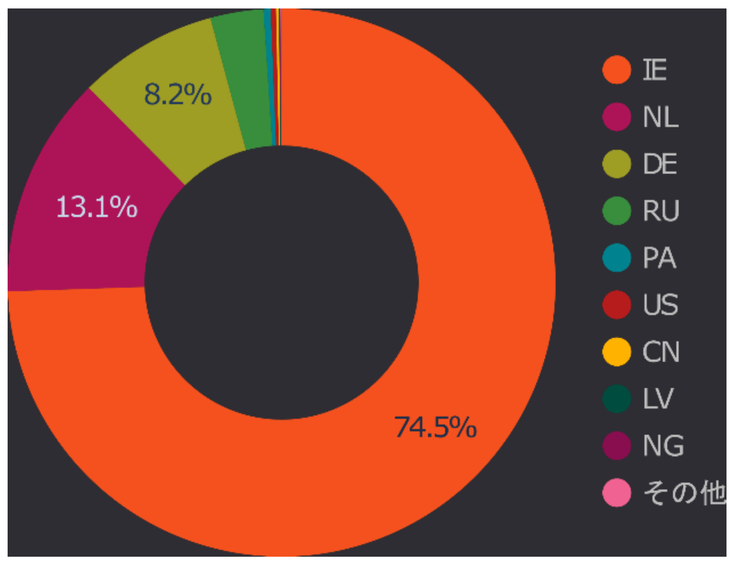
CowrieのログはJSONで出力されるが、Google データポータルへのファイルアップロードはCSVのみ対応している。JSONをCSVに変換することができるjqコマンドを使用して変換した。Cowrieのログには攻撃のログ以外の起動や終了のログもあるのでその部分は削除してから、 CSVに変換した。
また、国別のデータも作りたかったため、IPアドレスから国を調べることができるMaxMind社のGeoIP2というデータベースとPythonのライブラリを使用してすべてのIPアドレスを調べた。この処理には10分の時間がかかった。
Google データポータルへは攻撃のログと国のデータの2つをアップロードし、結合してインポートした。慣れておらず、操作が難しかったが、ドキュメントを読んで、ある程度ならグラフを出せるようになった。

結果

初の攻撃は公開してから30分後で、1週間の合計で102,961件の攻撃があった。初日は7,500件ほどだったが、2日目から急に増え、17,000件ほど攻撃が来ている。



MaxMind社のGeoIP2というデータベースを使い、攻撃者のIPアドレスを元に、国別でグラフを作ってみた。IE(アイルランド)からの攻撃が最も多く、その次にNL(オランダ)、DE(ドイツ)となっている。ちなみに日本からの攻撃はなかった。



日本に設置しているからといって、アジアからの攻撃が多いというわけではないようだ。インターネット上の攻撃には国など関係ないということがわかった。
攻撃者が実際にどのような操作をしているかも調べたかったが、ログインだけチャレンジして、ログアウトしていくようで、ログは残っていなかった。

考察

攻撃数は2日目から急に増え、以降は安定している。1日目から攻撃が多かったのは、以前、自宅サーバを公開していたためサーバを狙って攻撃を続けていたのだと考えられる。
また、自宅のIPアドレスを検索エンジンで調べてみると、Shodanというインターネットに繋がっている機器を表示する検索エンジンがあることを発見した。Shodanで、自宅のIPアドレスを調べるとSSHのポートが空いていることが表示されていた。このようなサイトを利用しているユーザーが攻撃をしたため、2日目から攻撃が増えたことが考えられる。
また、なぜアイルランドからの攻撃が多かったかということはわからなかった。

まとめ

ハニーポットは公開してから30分後に攻撃が来た。インターネットの世界には治安などはない。攻撃者は常にインターネットにつながっている機器を狙っていることがわかった。

自分は大丈夫だと、他人事に思っていてはいけない。

実際に一般的な家庭にも攻撃が来ていることから、身の回りに危険はあるということがわかった。ルータがいつも多くの攻撃から守ってくれていることを実感できた。

参考文献

IPoE接続とPPPoE接続との違い
https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_13.html 2020年3月2日閲覧
Installing Cowrie in seven steps.
https://cowrie.readthedocs.io/en/latest/INSTALL.html 2020年3月2日閲覧