Mirai Bot:

Thunder TPSで最新のDDoS攻撃を防御

目次

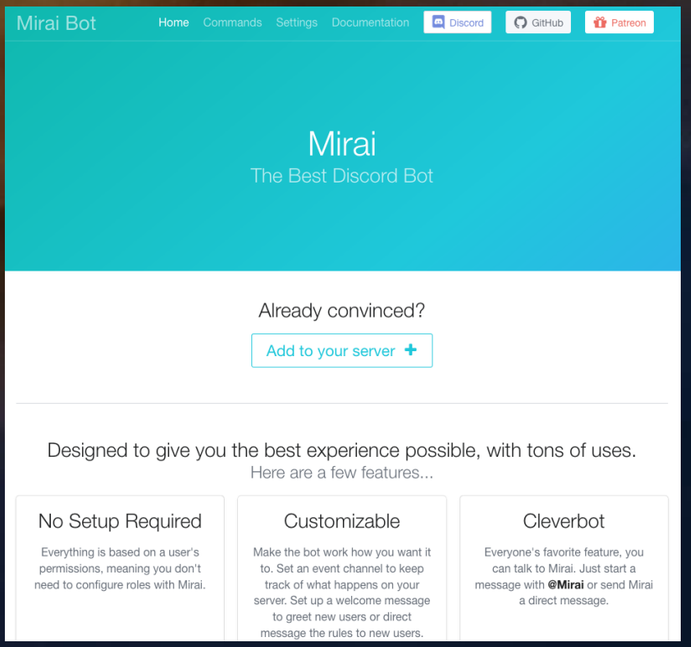
Mirai Bot (ミライ ボット)とは

Miraiの攻撃手法

Thunder TPSによるDDoS対策

Mirai Bot (ミライ ボット)とは

- 2016年秋に登場したDoS攻撃を仕掛けるマルウェア
- マルウェアを仕掛ける標的はWebカメラやIoTデバイス
- 感染されたデバイスは50万台以上
- 攻撃者は感染したデバイスを操作し、標的のサーバ/サービスに対して600Gbps以上の攻撃が可能
- Miraiのソースコードが公開されそれをもとに亜種のマルウェアが相次いで出現
- 実際に被害を受けたユーザー:AWS/Twitter/CNN/Google等



Mirai Bot webサイト

Miraiの攻撃手法

- 8種のDDoS攻撃

```
#define ATK_VEC_UDP             0       /* Straight up UDP flood */
#define ATK_VEC_VSE             1       /* Valve Source Engine query flood */
#define ATK_VEC_DNS             2       /* DNS water torture */
#define ATK_VEC_SYN             3       /* SYN flood with options */
#define ATK_VEC_ACK             4       /* ACK flood */
#define ATK_VEC_STOMP           5       /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP           6       /* GRE IP flood */
#define ATK_VEC_GREETH          7       /* GRE Ethernet flood */
//#define ATK_VEC_PROXY         8       /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN       9       /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP            10      /* HTTP layer 7 flood */
```

Miraiのソースコード

L3～L7に渡るマルチレイヤーの攻撃・手法

Miraiを根本から止めるのは困難

Miraiは

- セキュリティ対策が十分でないIoTデバイスを狙う
  （管理アカウントがデフォルト状態のLinux系のデバイス）
- 既に50万台以上が感染*

* http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet

全てのIoTデバイスに対策が取られることを期待するのは現実的ではない

今後もIoTによるDDoS攻撃は増大することが予測される

root	xc3511	root	(none)
root	vizxv	admin	password
root	admin	root	root
admin	admin	root	12345
root	888888	user	user
root	xmhdipc	admin	(none)
root	default	root	pass
root	juantech	admin	admin1234
root	123456	:	
root	54321	:	
support	support		

60個以上の初期の管理アカウントを使用し感染を試みている

サーバ/サービス側のDDoS対策が急務

Thunder TPSによるDDoS対策

A10 THUNDER TPSで、Miraiによる全てのDDoSを
“L3～L7に渡るマルチレイヤー”でMitigationします

Miraiによる攻撃種別	Thunder TPSによる対策
0 /* Straight up UDP flood */	○ UDPレベルのMitigation
1 /* Valve Source Engine query flood */	○ UDPレベルのMitigation
2 /* DNS water torture */	○ DNSレベルのMitigation
3 /* SYN flood with options */	○ ハードウェア/ソフトウェアによるMitigation
4 /* ACK flood */	○ TCPレベルのMitigation
5 /* ACK flood to bypass mitigation devices */	○ TCPレベルのMitigation
6 /* GRE IP flood */	○ GREレベルのMitigation
7 /* GRE Ethernet flood */	○ GREレベルのMitigation
8 /* Proxy knockback connection */	(Mirai未実装)
9 /* Plain UDP flood optimized for speed */	○ UDPレベルMitigation
10/* HTTP layer 7 flood */	○ HTTPレベルのMitigation


Thank you
A10ネットワークス株式会社
Mailto: jinfo@a10networks.com
03-5777-1995