

DDoS攻撃10年の歴史を振り返る



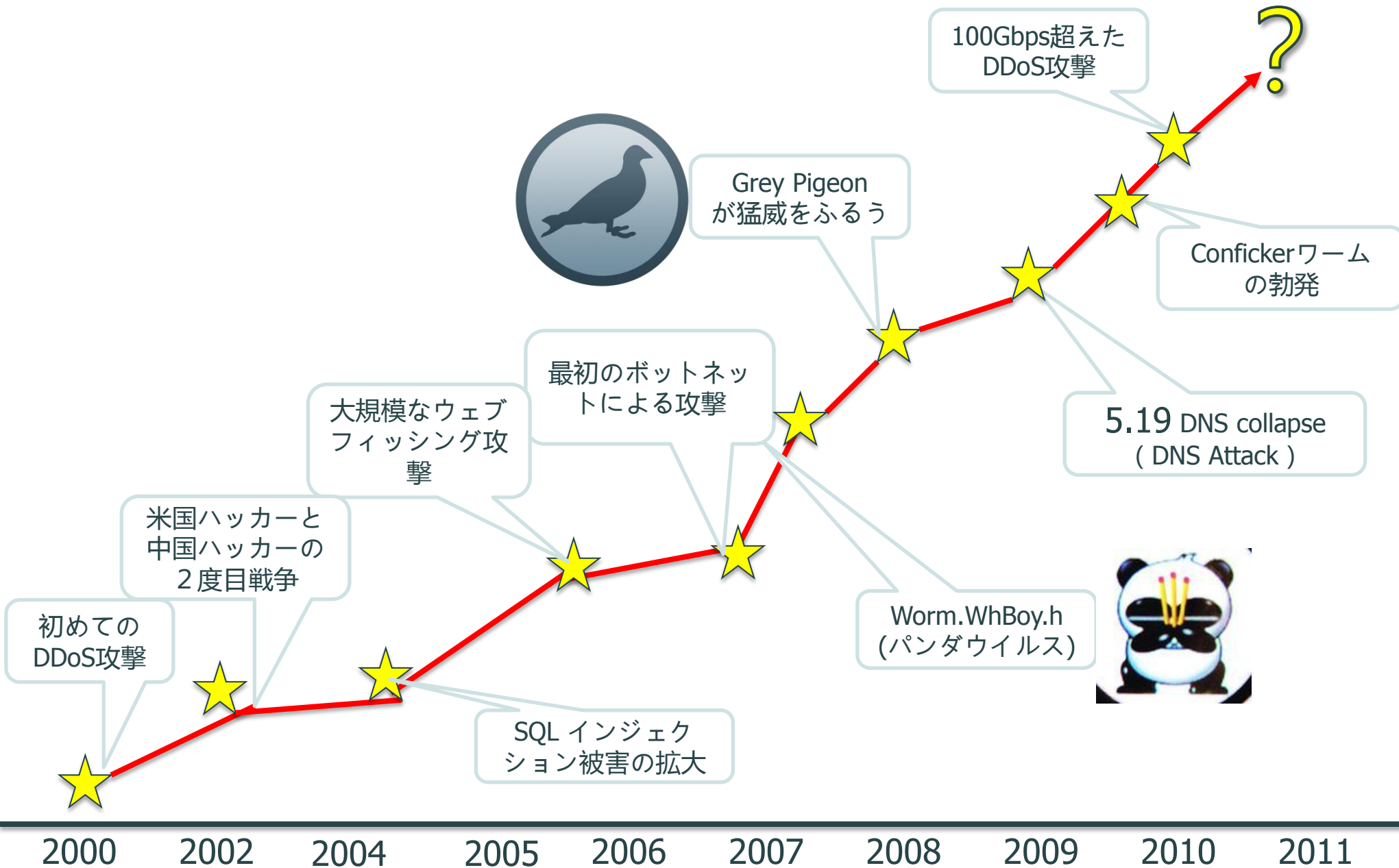
NSFOCUS 顧 茂林

gumaolin@nsfocus.co.jp

1 中国でのDDoS攻撃の変遷

2 よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス



一発で100Gを超える攻撃

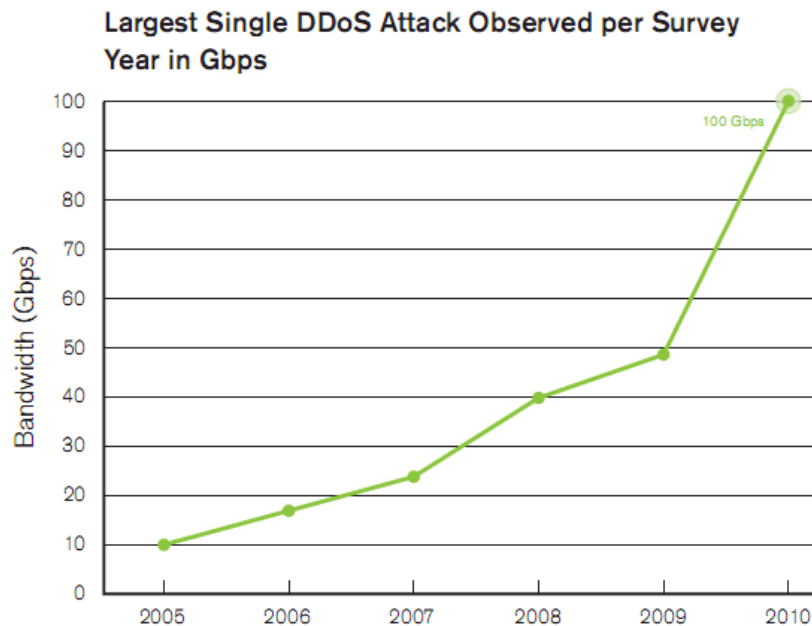


Figure 1
Source: Arbor Networks, Inc.

Layer 7 DDoS Attacks

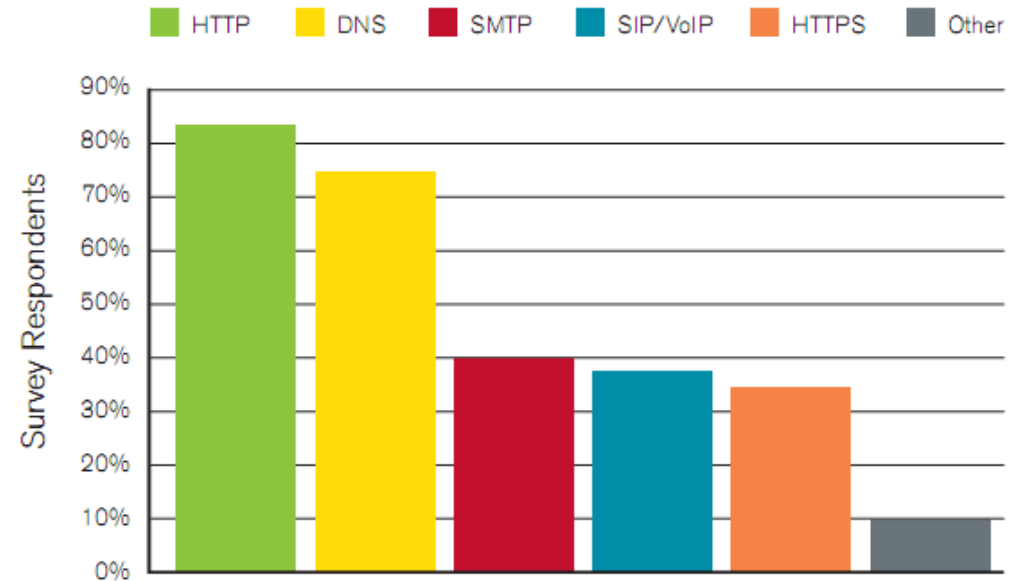


Figure 8
Source: Arbor Networks, Inc.

DNS攻撃はもっとも容易なDDoS
攻撃手口になってしまった！

1 中国でのDDoS攻撃の変遷

2 よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス

大流量型の攻撃：

攻撃トラフィックのソース：

- ・テスト用機器
- ・ハイパフォーマンスサーバーとソフト
- ・IDC



トラフィックの特徴：

- ・まったくランダムなSource IPまたはある決まった範囲でのランダムなIP
- ・スリーハンドシェイクができない
- ・1Gbpsから70Gbpsにまで及ぶトラフィック



防御方法：

- ・従来のリバースプロキシを使って偽装IPからのパケットをドロップする
- ・ただし大量のリバースプロキシトラフィックにより、アップリンク帯域が逼迫

実IPからの中規模の攻撃：

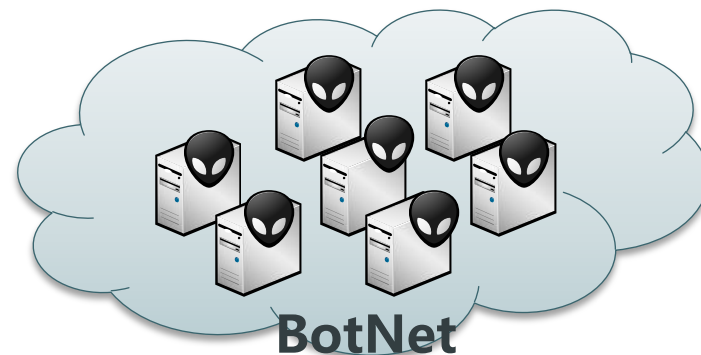
- ・ Botnet
- ・ Proxy Server

攻撃の特徴：

- ・ スリーハンドシェイクは完了する
- ・ 主にH T T Pのサービスをターゲットにする
- ・ 100M程度の攻撃トラフィック

防御方法：

- ・ SYN-Cookieのチェック
- ・ アプリケーション層のデータチェック
- ・ シグネチャを使ってパケットフィルタリングする



偽メッセージによる大規模な攻撃トラフィック：
異なる攻撃ターゲットごとに、攻撃がばれないように
攻撃のメッセージを偽装する。

例： ソースIPを偽装
TTL,Port,SNなどの偽装
コンテンツの偽装

防御の考え方：

UDPのサービスでは、どんな方法でもソースIPアドレスが偽装されて
いれば、スリーハンドシェイクができない

防御方法：

- リバースプロキシ
- SYN-Cookieのチェック
- 自動学習(Smart Technology)

No.	Time	Source	Destination	Protocol	Info
1272	9.595611	192.168.10.241	192.168.10.38	UDP	Source port: 1 Destination port: 80 [BAD UDP LENGTH 65008 > IP PAY
1372	9.878088	192.168.10.241	192.168.10.38	UDP	Source port: 1 Destination port: 80 [BAD UDP LENGTH 65008 > IP PAY
1416	9.879320	192.168.10.241	192.168.10.38	UDP	Source port: 1 Destination port: 80 [BAD UDP LENGTH 65008 > IP PAY
1460	9.880716	192.168.10.241	192.168.10.38	UDP	Source port: 1 Destination port: 80 [BAD UDP LENGTH 65008 > IP PAY
1504	9.900792	192.168.10.241	192.168.10.38	UDP	Source port: 1 Destination port: 80 [BAD UDP LENGTH 65008 > IP PAY

+ Frame 1272 (1402 bytes on wire, 1402 bytes captured)	
- Ethernet II, Src: Vmware_6f:88:c1 (00:0c:29:6f:88:c1), Dst: Wistron_3c:f4:39 (00:0a:e4:3c:f4:39)	
- Destination: Wistron_3c:f4:39 (00:0a:e4:3c:f4:39)	
Address: Wistron_3c:f4:39 (00:0a:e4:3c:f4:39)	
.... 0 = IG bit: Individual address (unicast)	
.... 0 = LG bit: Globally unique address (factory default)	
- Source: Vmware_6f:88:c1 (00:0c:29:6f:88:c1)	
Address: Vmware_6f:88:c1 (00:0c:29:6f:88:c1)	
.... 0 = IG bit: Individual address (unicast)	
.... 0 = LG bit: Globally unique address (factory default)	
Type: IP (0x0800)	
+ Internet Protocol, Src: 192.168.10.241 (192.168.10.241), Dst: 192.168.10.38 (192.168.10.38)	
- User Datagram Protocol, Src Port: 1 (1), Dst Port: 80 (80)	
Source port: 1 (1)	
Destination port: 80 (80)	
Length: 65008 (bogus, should be 1368)	
Checksum: 0x1d03 [correct]	
Data (65000 bytes)	

Botnet

大量なゾンビPCから構成され、通信可能で、リモートコントロールできるネットワーク

特徴:

- コントロールが可能
- 悪意を持って拡散
- 同じ動きをする悪意のある行動が一つのボットマスターからたくさんのゾンビPCに拡散

脅威:

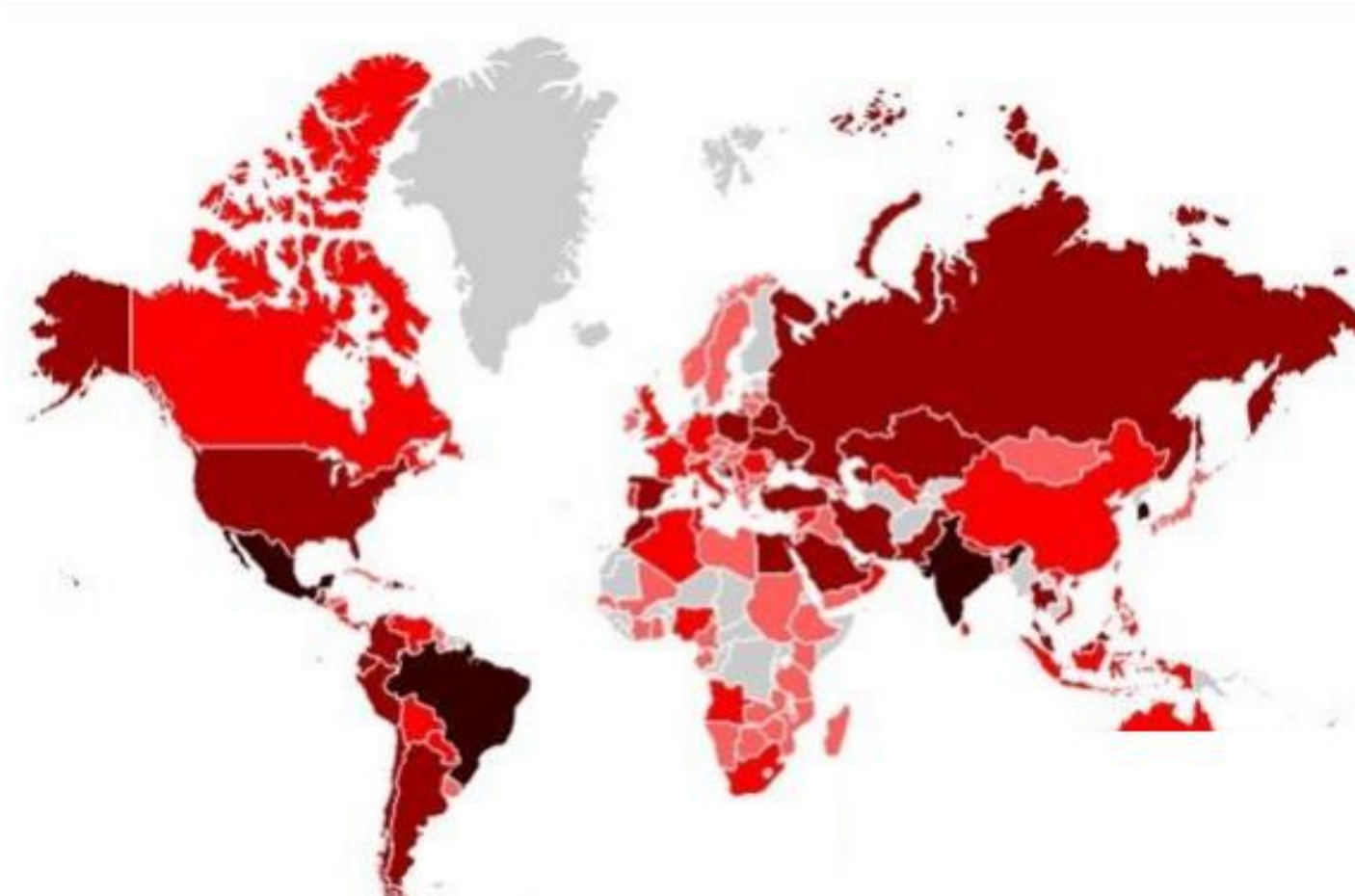
- DDoS攻撃
- Spam
- Phishingと成りすまし
- 情報搾取

Botの分類:

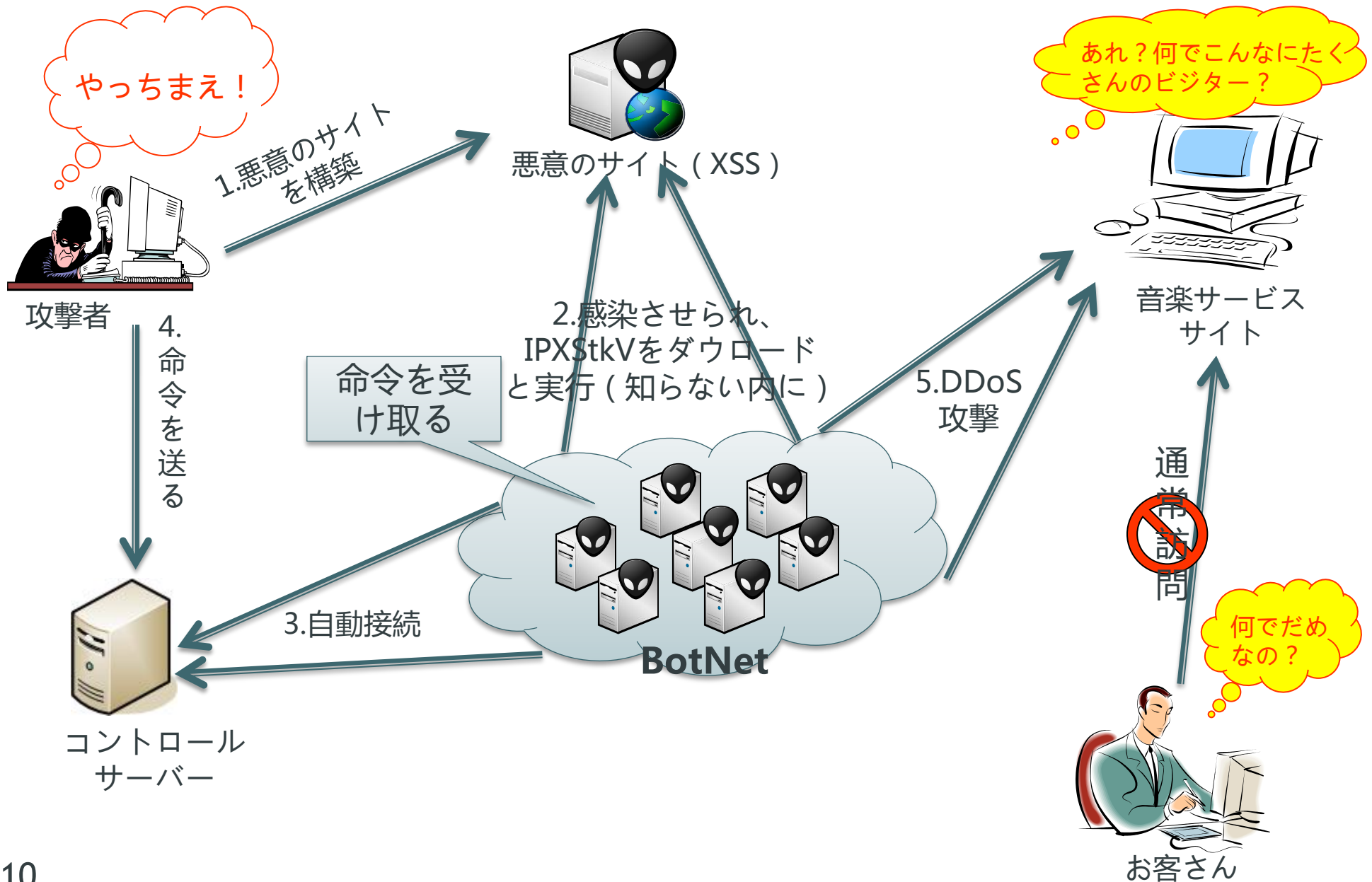
- IRC Bots
- P2P Bots
- HTTP Bots
- DNS Bots



Mariposa Botnet infected 14,000,000 computers in 31901 cities of 190 countries all over the world.



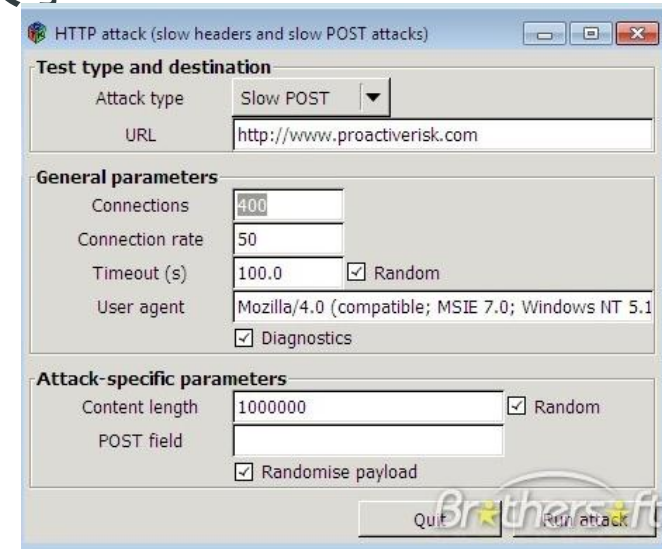
Source: Panda Security 2010 March



ページリフレッシュによる攻撃



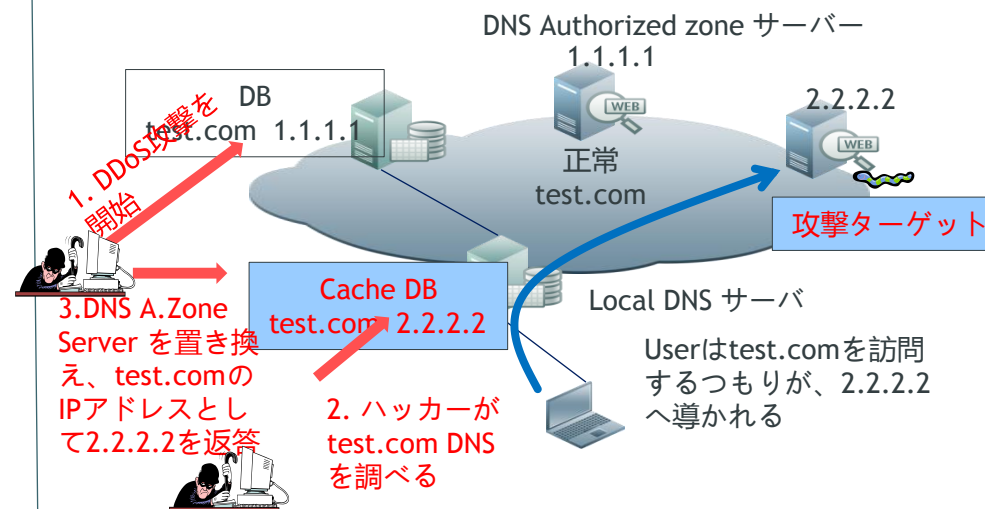
静的な攻撃

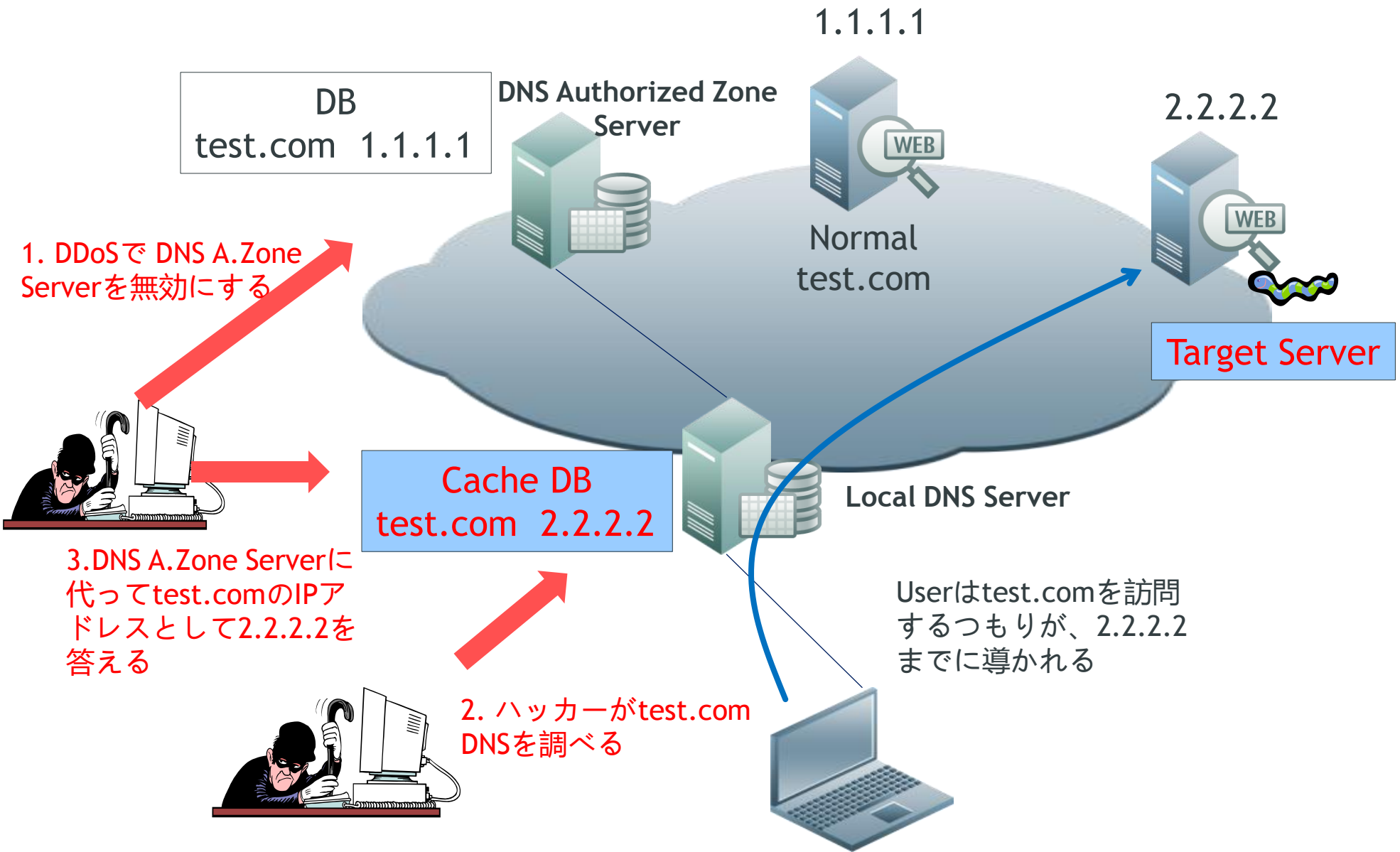


動的な攻撃



DNSを利用する攻撃

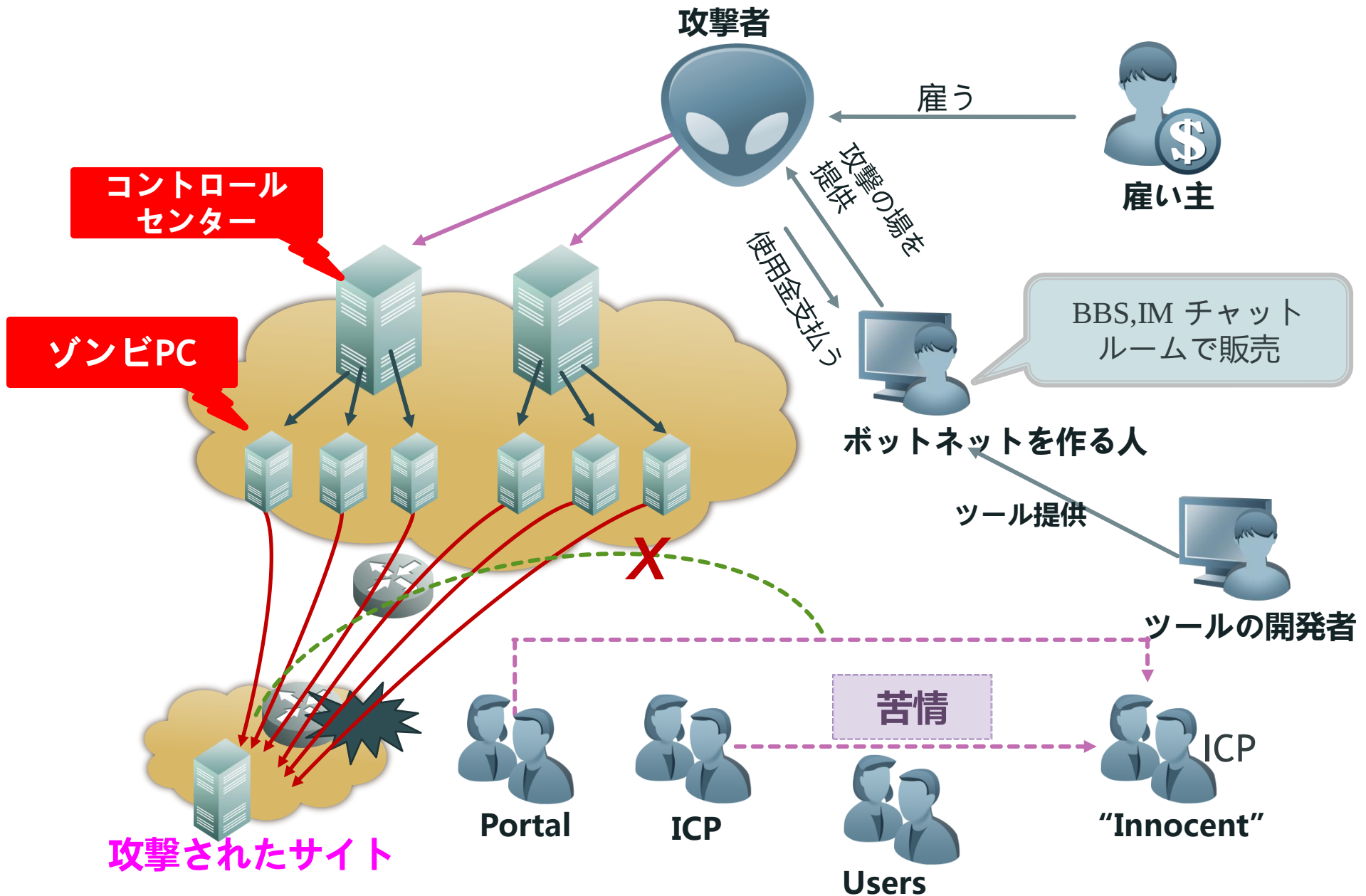




1 中国でのDDoS攻撃の変遷

2 よく使われているDDoS攻撃の手口

3 DDoS 攻撃のアングラビジネス





ご清聴どうもありがとうございました