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

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

DDoS攻撃

DDoS攻撃（協調分散型DoS攻撃、分散型サービス拒否攻撃、Distributed Denial of Service attack）とは、踏み台と呼ばれる複数のコンピュータが、標的とされたサーバ等に対して攻撃を行うことである。

中国でのDDoS攻撃の変遷

初めての DDoS攻撃

米国ハッカーと 中国ハッカーの ２度目戦争

大規模なウェブ フィッシング攻 撃

SQL インジェク ション被害の拡大

最初のボットネッ トによる攻撃

Worm.WhBoy.h (パンダウイルス)

5.19 DNS collapse （DNS Attack）

Conficker ワーム の勃発

Grey Pigeon が猛威をふるう

100Gbps超えたDDoS攻撃 オンラインゲーム サイトに

?

2000 2002 2004 2005 2006 2007 2008 2009 2010 2011

中国ではDDoS攻撃が100Gbpsを超えた！

一発で100Gを超える攻撃

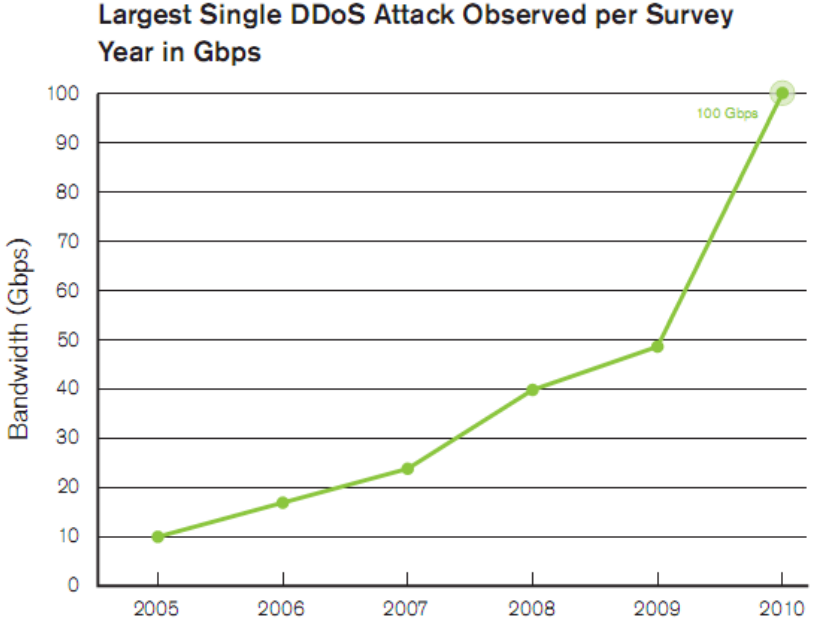


Figure 1
Source: Arbor Networks, Inc.

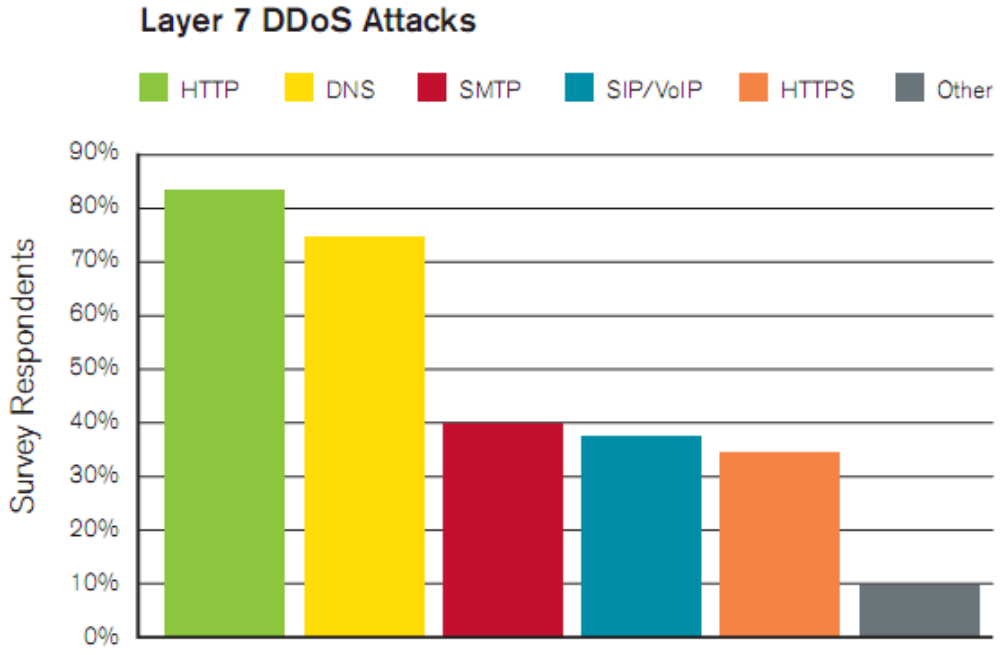


Figure 8
Source: Arbor Networks, Inc.

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

よく見られるDDoS攻撃

1. 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

   ・IDC

2. 実IPからの中規模の攻撃：

   ・Botnet

   ・Proxy Server

3. 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

5. Botnet

大量のゾンビ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:

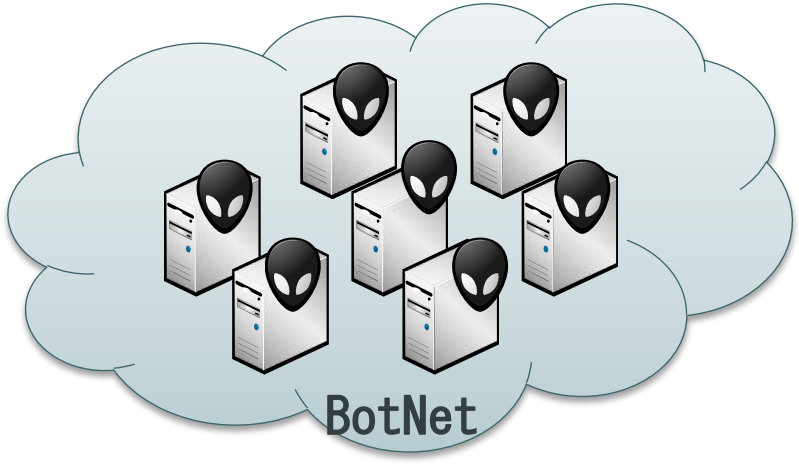
- コントロールが可能
- 悪意を持って拡散
- 同じ動きをする悪意のある行動が一つのボットマスター
  からたくさんのゾンビPCに拡散

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

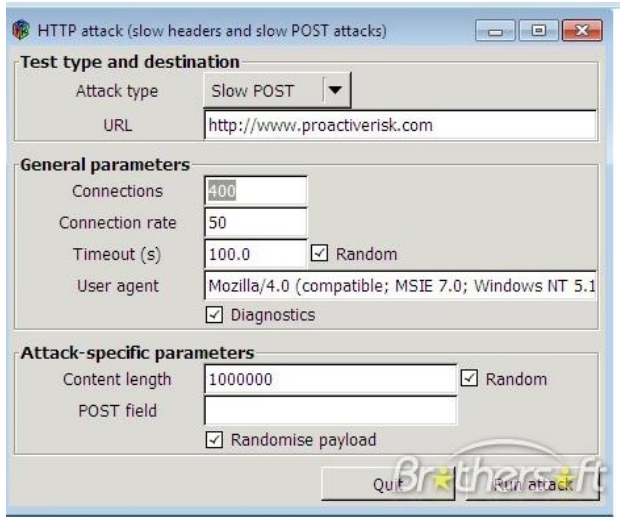
Mariposa Botnet infected 14,000,000 computers in 31901 cities of 190 countries all over the world.

Source: Panda Security 2010 March

Http Get Flood 攻撃

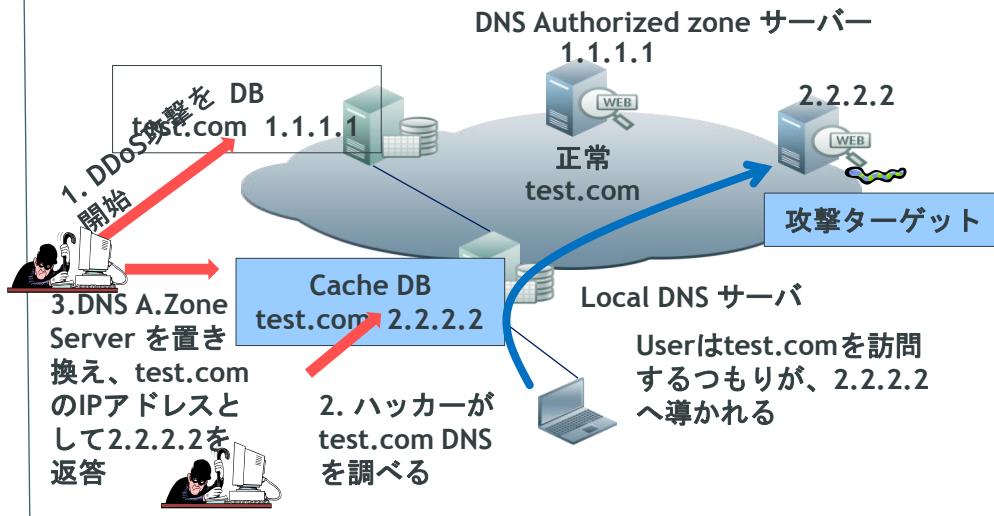
ページリフレッシュによる攻撃

静的な攻撃

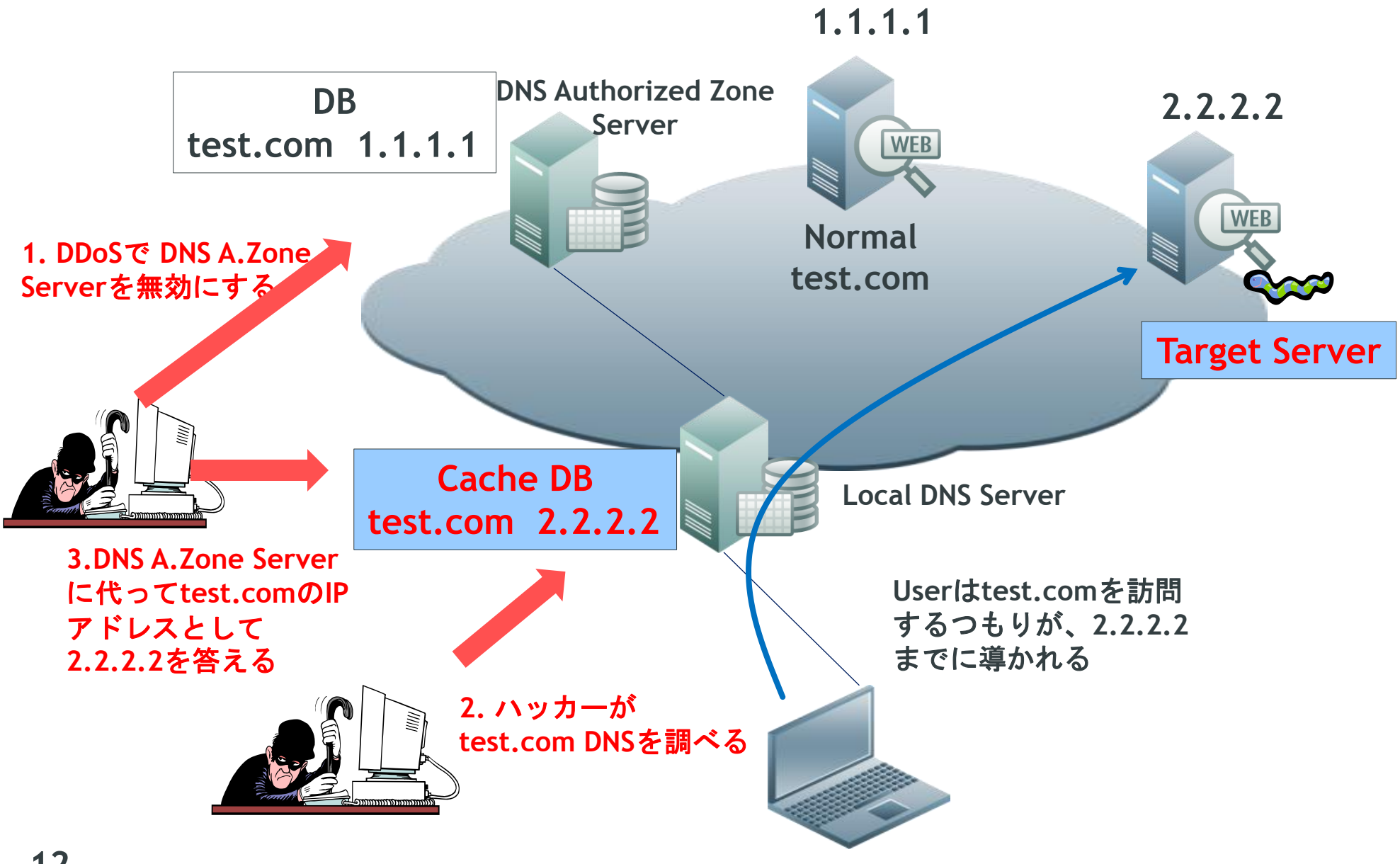


動的な攻撃

DNSを利用する攻撃



DNSポイズニング攻撃

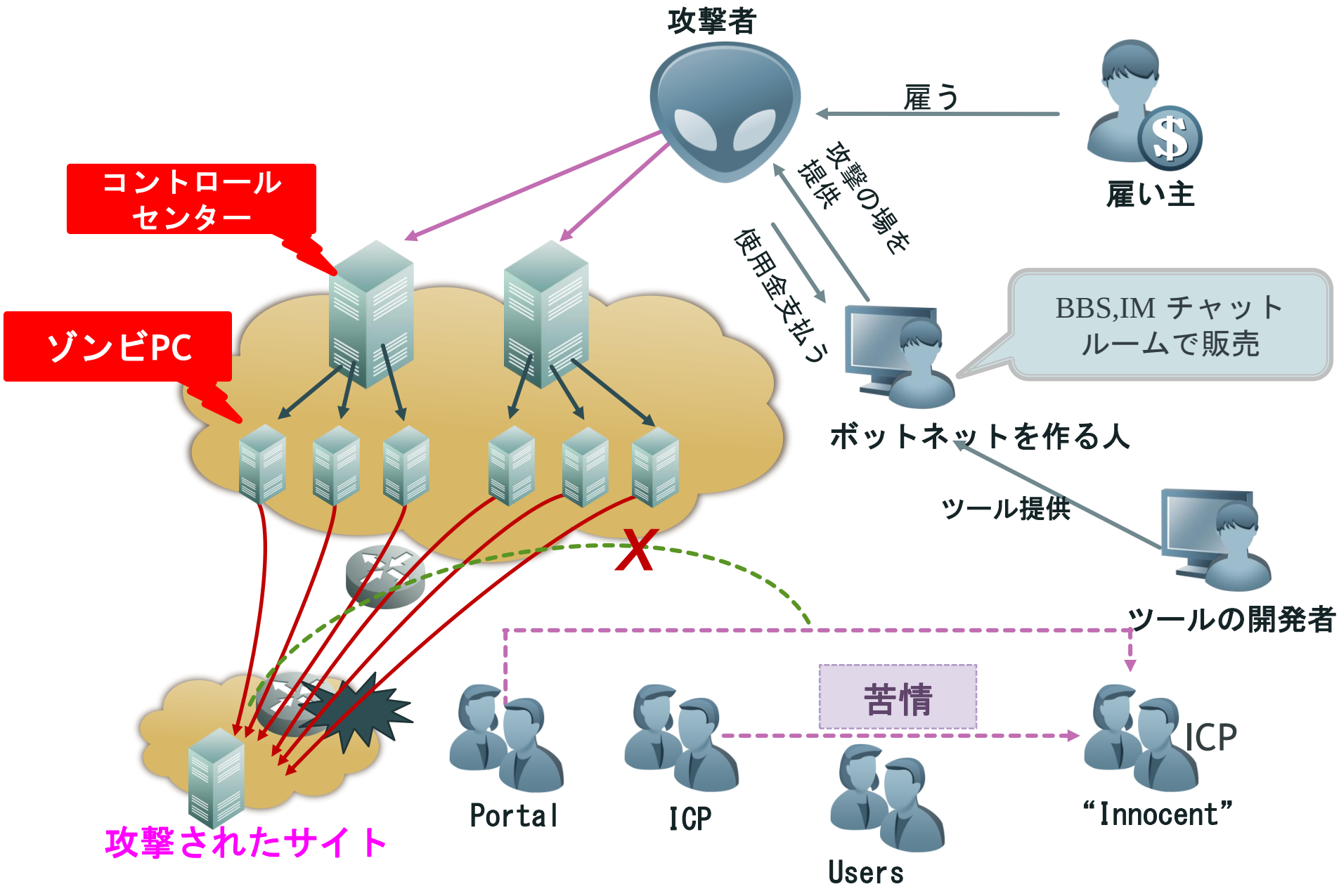


1 中国でのDDoS攻撃の変遷

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

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