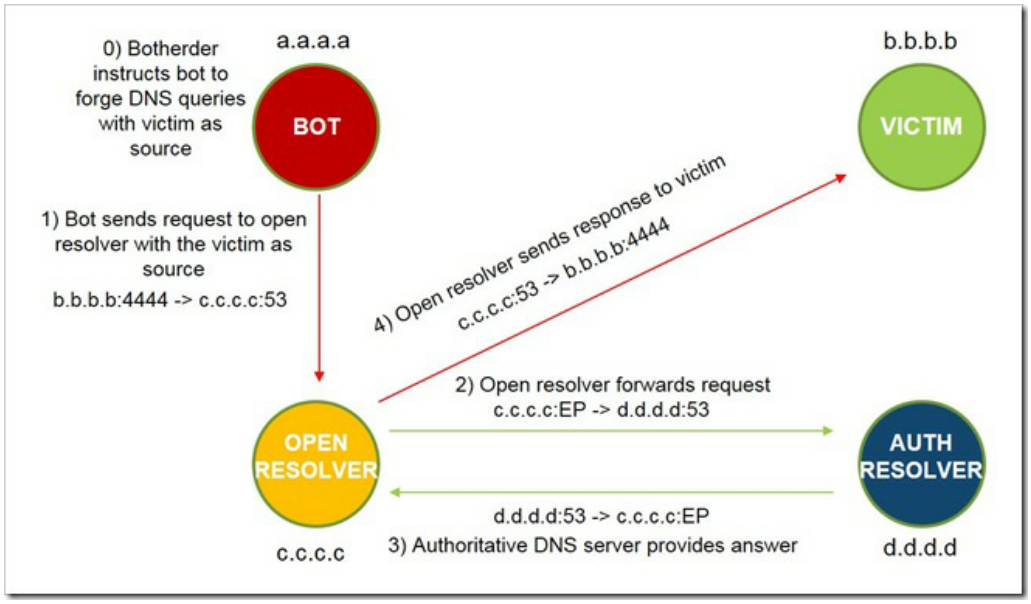
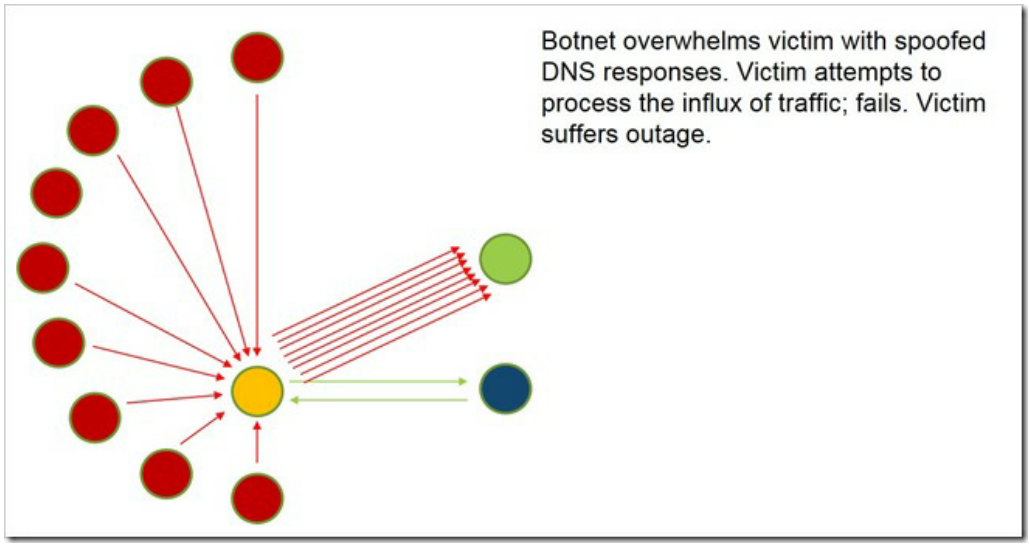
Abusing Open Resolvers

John Wagnon, 2017-15-02

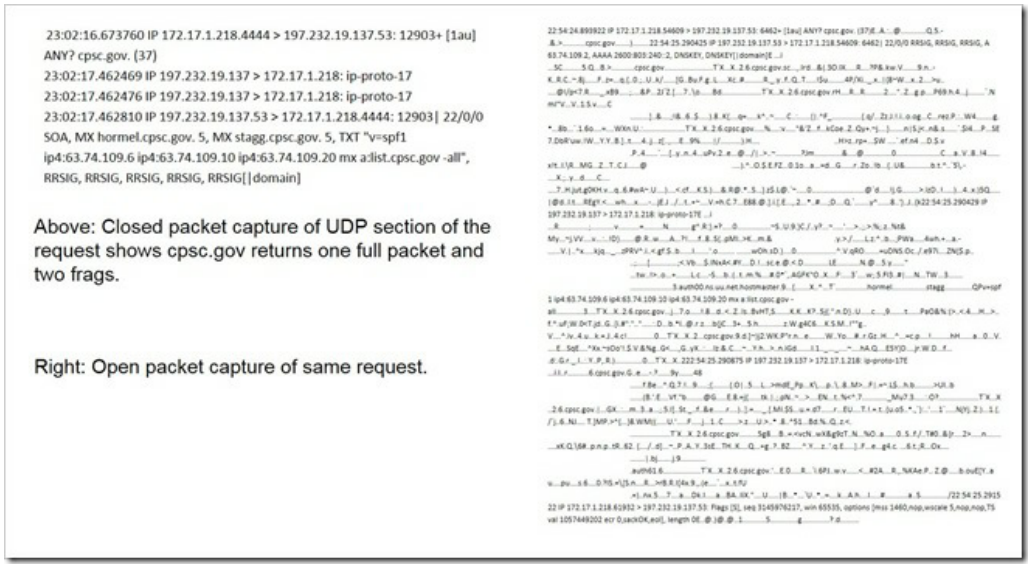
Open DNS resolvers can be used to recursively query authoritative name servers. In fact, a list of open resolvers can be found at http://openresolverproject.org/. Further, Network Time Protocol (NTP) servers with "monlist" enabled allow a host to query the last 600 connections who have connected to that server. Knowing this, an attacker (possibly using a bot) can send a DNS request using a source address that is spoofed as the IP address of the victim and the open resolver will send all the responses to the victim. See the figure below for a pictoral description of this:



While this is a serious problem, what's worse is that an attacker could use not only one bot to attack the victim but rather an entire army of bots (making up a "botnet") to each individually attack the victim using this same method. The figure below shows this scenario:



The following screen capture shows two requests to the same open DNS resolver. The left is capturing closed packets (not showing payload) while the right shows an expanded response. This shows the large amount of data that a single request can generate. An attacker can use this to overwhelm a victim.



F5 Security Operations Center (SOC) expert researcher Damien Rocha shows some very interesting details about many recent DNS attacks. These include:

- Many attackers use UDP port 4444
- DNS open resolvers and NTP servers with "monlist" enabled can be used together for amplification attacks
- NTP packets in 451B-600B range
- Attack durations ~30min, ~60min, ~90min: Indicates paid service

With all these research points, the SOC listed a series of recommended actions to defend against these attacks:

- Utilize Geolocation blocking
- Blacklist known open resolvers
- Alert on signatures (src port 53 & dst port 4444)

Related Resources:

iRule to protect against DNS amplification attacks

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com