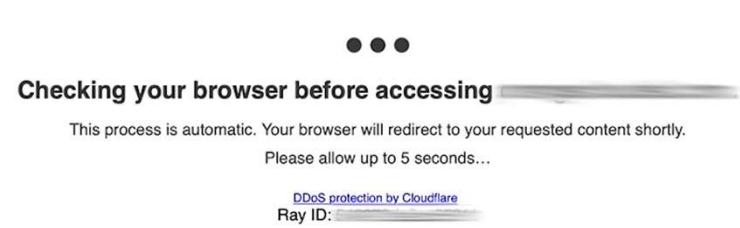


DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

ARSALAN SEFIDGAR

DoS / DDoS

حمله منع خدمت از سرویس (توزیع شده) (Distributed) Denial of Service



❖ سناریو های محتمل

❖ شبکه مخابرات (تلفن ثابت)

❖ سرویس آموزش آنلاین دانشگاه

انگیزه هکر

1. منافع متفاوت
2. رقابت
3. اخاذی
4. هکتوبیست ها
5. حواس پرتی

در سالی که گذشت

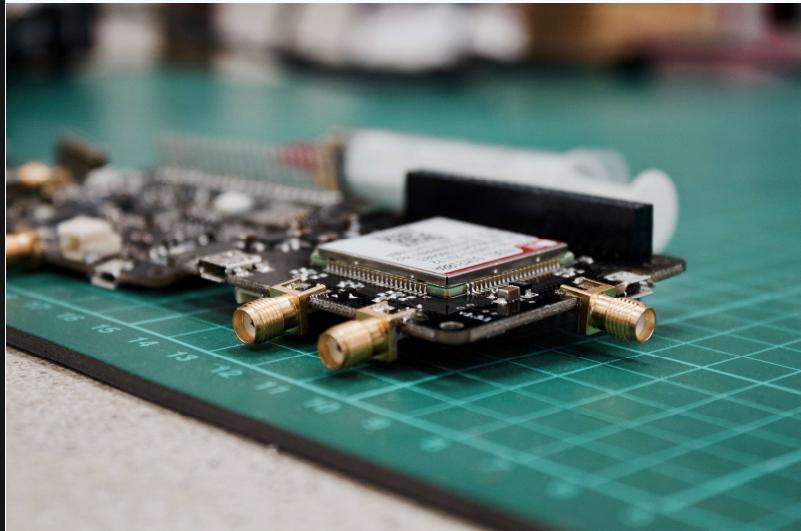
1. ابر آروان

2. شرکت زیرساخت کشور

3. اسنپ فود

4. و...

INTERNET OF THINGS



1. میلیون ها دستگاه: دوربین ها، روتراها
2. پسورد های از پیش تعیین شده در کارخانه
3. آپدیت نکردن / نقص های امنیتی قدیمی

INTERNET OF SHIT

 **Internet of Stay Home** @internetofshit · Apr 21

I don't know what's crazier here: that the website was hosted on the same server as their smart home platform or that we live in a dystopia where mask demand ddos'd an air conditioner



Demand for Sharp's face masks crashes website and smart home gadgets
Online store goes down, taking air conditioners with it
[theverge.com](https://www.theverge.com)

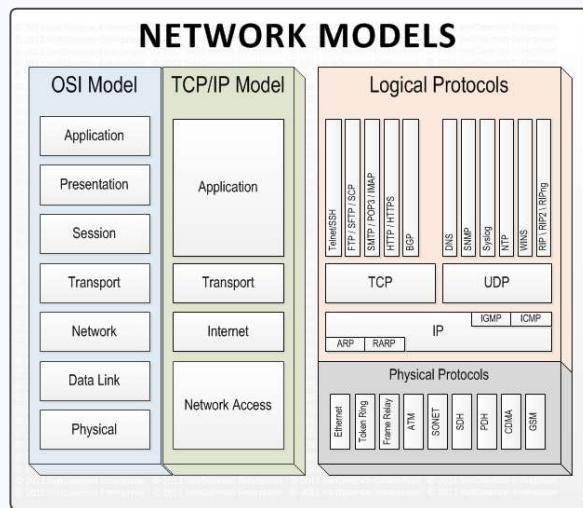
16 623 1.4K

تهدیدات دیگر

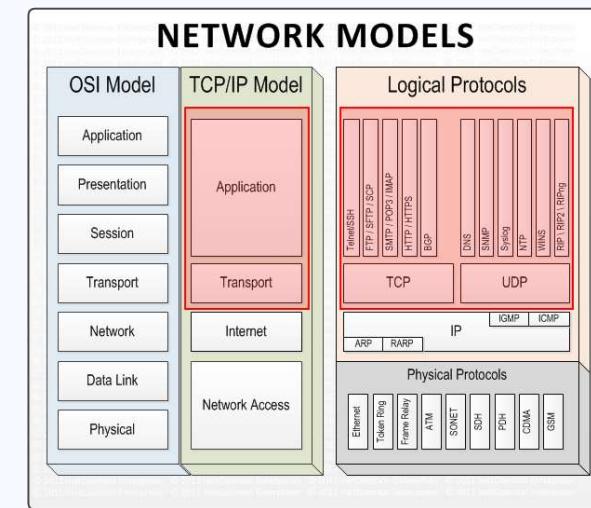
1. میلیون ها سایت مبتنی بر وردپرس با پروتوكل ping-back
2. میلیون ها کامپیوتر، لپ تاپ و سرور در معرض خطر
3. وب اپلیکیشن های در معرض خطر (گذرا)

TYPE OF ATTACKS

OSI STACK



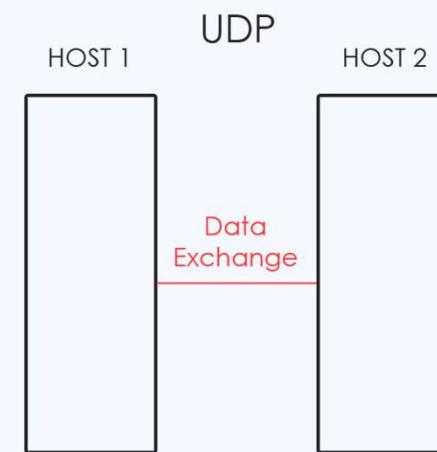
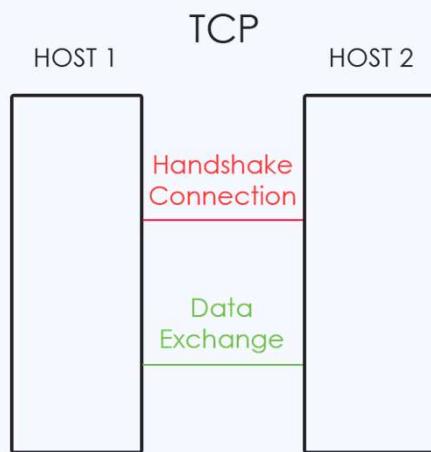
OSI STACK EXPOSURE



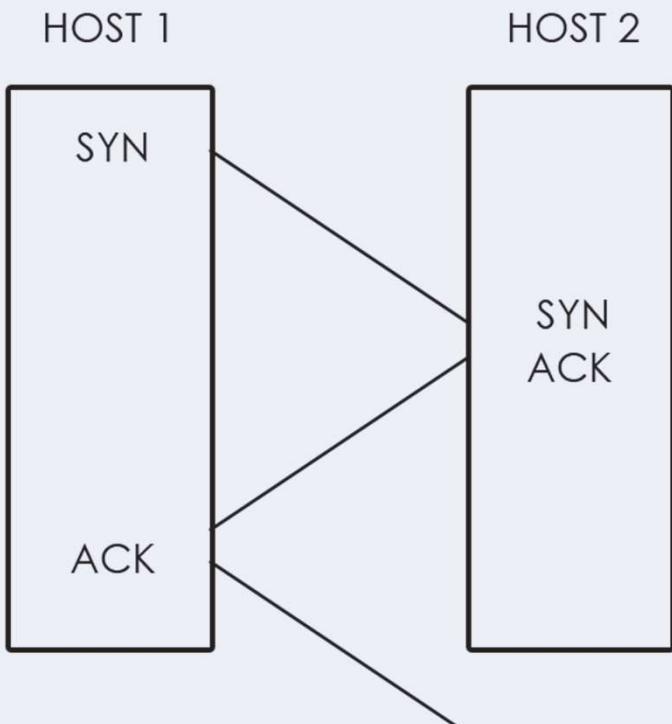
TCP VS UDP

SPOOF ZONE

AUTHENTIC HOSTS



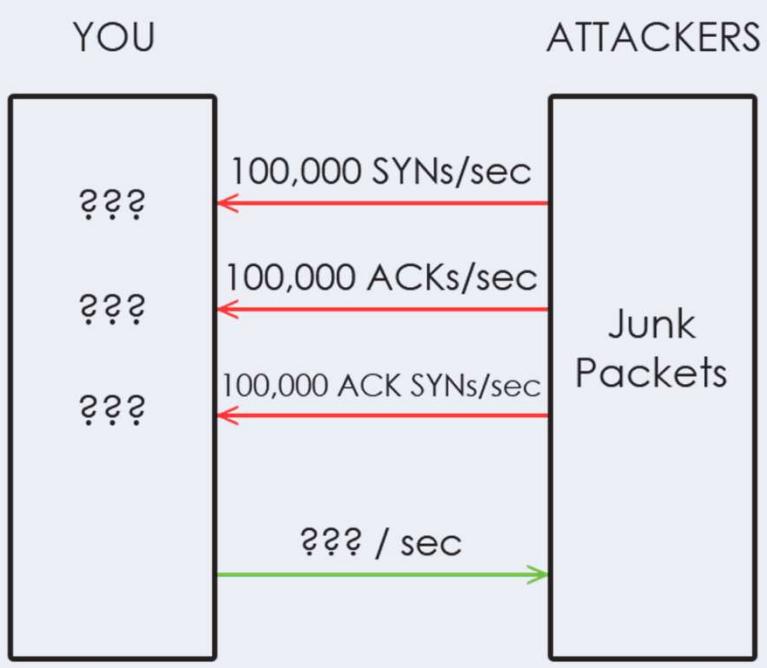
TCP: Attack Transport



TCP Handshake Lifecycle

- ❖ Each handshake packet has **its own source IP**
- ❖ Source IP **blindly trusted** by both end-points

TCP Handshake Lifecycle Floods



Real hosts

Fake hosts aka “spoofed”

- ❖ CPU
- ❖ MEMORY

YOU

ATTACKERS:
Real Hosts

100,000 GET/sec

100,000 POST/sec

HTTP
Floods

200,000
HTML Docs / sec

TCP: Attack Application (HTTP)

Hundreds of Infected machines

- ❖ CPU
- ❖ MEMORY
- ❖ Bandwidth

Beyond:

*Default ulimit is 1024 connection sockets

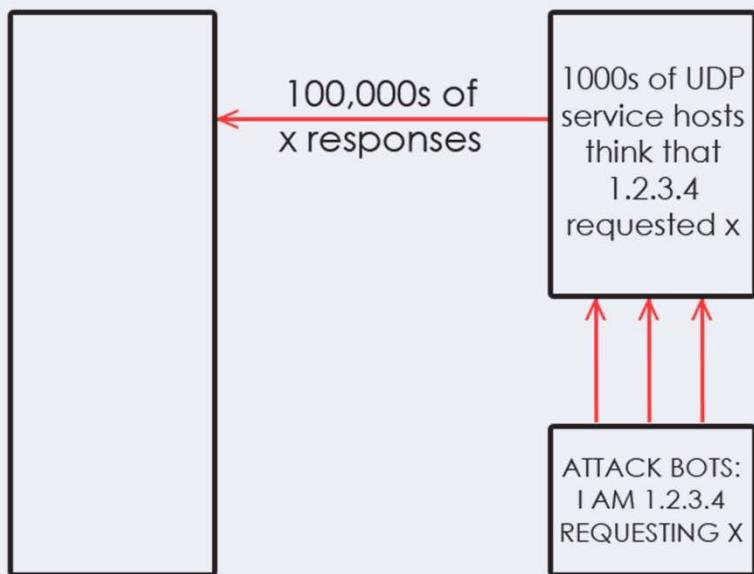
Slowloris: open connection, and keep it opened

TLS Exhaustion

HashDoS: kill CPU with a few requests

UDP: NO TRANSPORT TO ATTACK

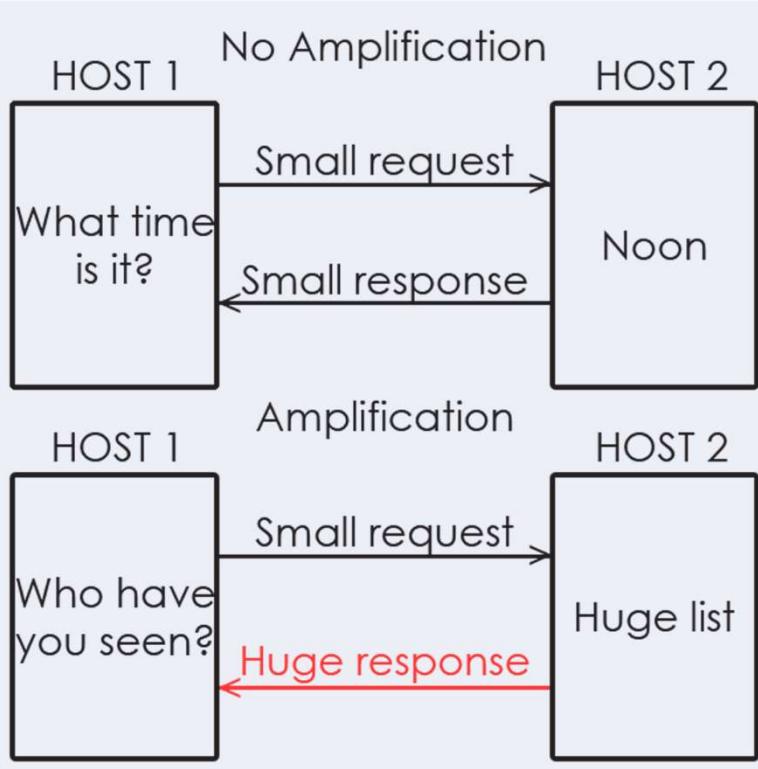
YOU: 1.2.3.4



UDP Reflection

*Bandwidth

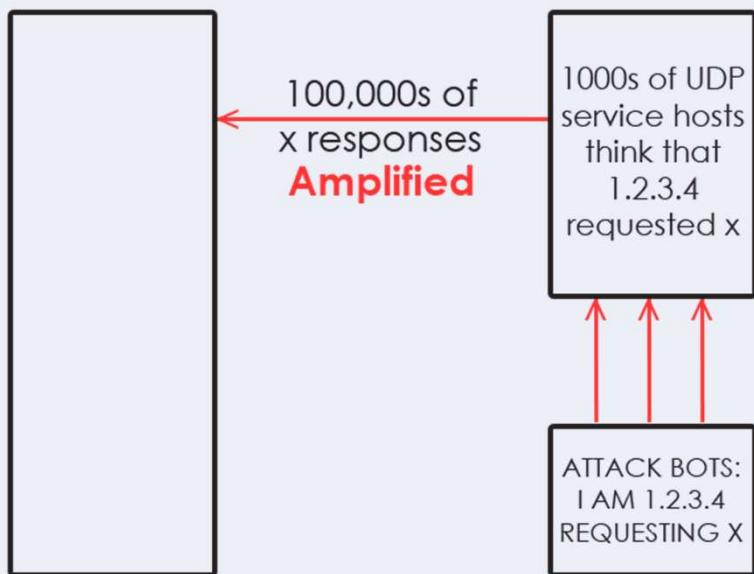
UDP: NO TRANSPORT TO ATTACK



UDP Amplification

UDP: NO TRANSPORT TO ATTACK

YOU: 1.2.3.4

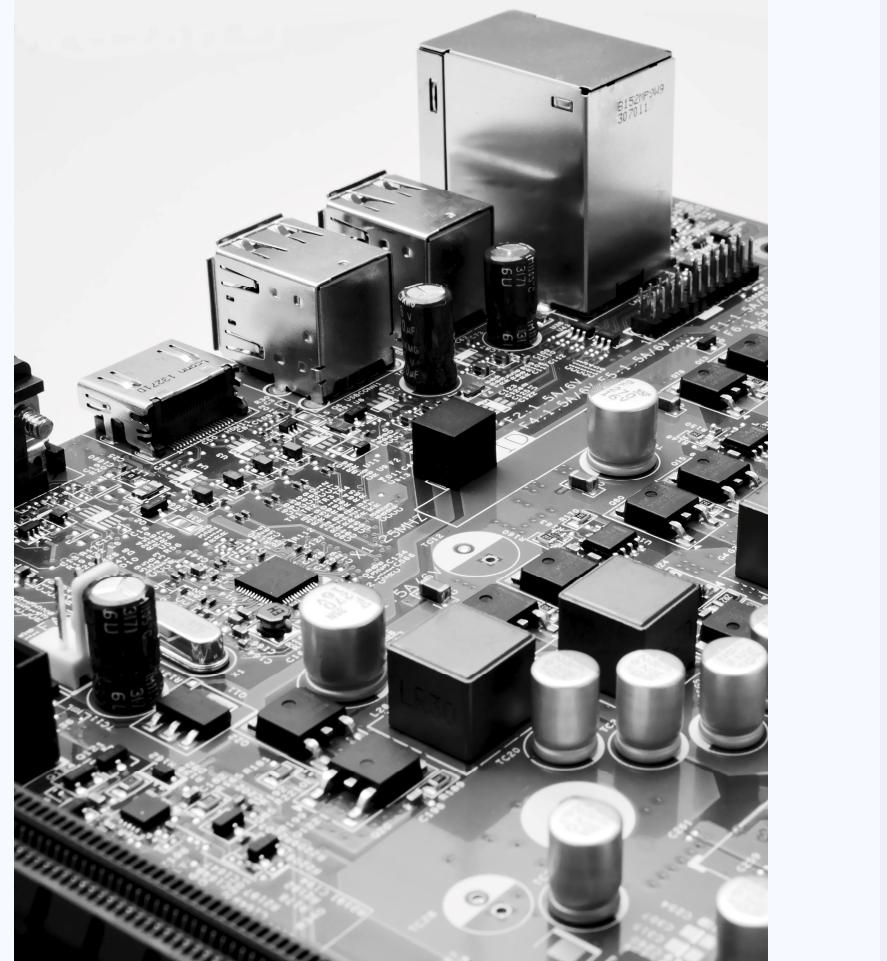


UDP Reflection + Amplification

*Bandwidth

FIX IOT

- ❖ MUD: Manufacturer Usage Descriptions
 - ❖ Manufacturer Usage Descriptions (MUD) is meant to defend against. MUD works by providing a formal language and mechanism for manufacturers to specify which systems a device is designed to connect with. The converse, therefore, is that the network can prevent the device from both being attacked and attacking others. The key to all of this are manufacturer and their willingness to describe these devices.



REDUCE REFLECTION & AMPLIFICATION

- ❖ Close-Down Open DNS Resolvers
- ❖ Use a Secure NTP Template
 - ❖ Network Time Protocol



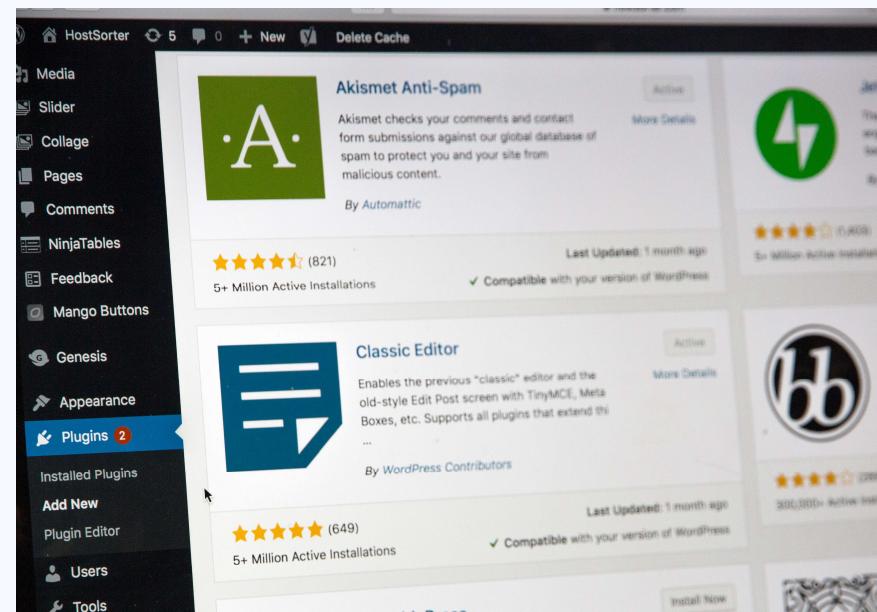
FIX SPOOFING

- ❖ Stop spoofing
 - ❖ RFC 2267: Ratified in 1998, Now BCP38
 - ❖ RFC 3704: Ratified in 2004, Now BCP84

```
 90 //fires the appear event when appropriate
 91 var check = function() {
 92   //is the element hidden?
 93   if (!t.is(':visible')) {
 94     //it became hidden
 95     t.appeared = false;
 96   }
 97
 98   //is the element inside the visible window?
 99   var a = w.scrollLeft();
100  var b = w.scrollTop();
101  var o = t.offset();
102  var x = o.left;
103  var y = o.top;
104
105  var ax = settings.accX;
106  var ay = settings.accY;
107  var th = t.height();
108  var wh = w.height();
109  var tw = t.width();
110  var ww = w.width();
111
112  if (y + th + ay >= b &&
113      y <= b + wh + ay &&
114      x + tw + ax >= a &&
115      x <= a + ww + ax) {
116
117    //trigger the custom event
118    if (!t.appeared) t.trigger('appear', settings.data);
119
120  } else {
121
122    //it scrolled out of view
123    t.appeared = false;
124  }
125
126  //create a modified fn with some additional logic
127  var modifiedFn = function() {
128
129    //mark the element as visible
130    t.appeared = true;
131
132    //is this supposed to happen only once?
133    if (settings.one) {
134
135      //remove the check
136      w.unbind('scroll', check);
137      var i = $.inArray(check, $._fn.appear.checks);
138      if (i >= 0) $._fn.appear.checks.splice(i, 1);
139
140    }
141
142    //trigger the original fn
143    fn.apply(this, arguments);
144  }
145
146  //bind the modified fn to the element
147  if (settings.one) t.one('appear', settings.data, modifiedFn);
148
149  //bind the original fn to the element
150  w.bind('scroll', check);
151}
```

FIX WORDPRESS

- ❖ WordPress ping-back verification protocol
 - ❖ Exposed and Exploited since 2014
 - ❖ The World's easiest Botnet
 - ❖ Millions of WordPress sites



ATTACK SURFACE: REDUCE

- I. Before
 - I. UDP services: NTP, DNS, RTP
 - II. TCP services: HTTP, SSH, FTP, SIP
- II. After
 - I. NMAP
 - II. TCP services: HTTP(S)

ATTACK SURFACE: DIVERSIFY

- I. Use Dedicated Host Names or even Domains
 - I. API: api.yoursite.com, yoursiteapi.com
 - II. Content / Marketing: www.yoursite.com
 - III. Commerce: shop.yoursite.com
 - IV. SaaS: app.yoursite.com

DNS: PERFORMANCE & AVAILABILITY

- I. pingdom.com or statuscake.com to monitor
- II. Keep Tabs on DNS Performance & Availability

WEB APPLICATION PERFORMANCE

- I. Tune NGINX for High-Throughput Levels
- II. Configure gzip / deflate compression carefully
- III. Reduce number of DB queries per request
- IV. RDBMS backed by SSDs
- V. PHP: Ensure OpCache Properly Configured

WEB APPLICATION SCALABILITY

- I. Redis Data Caches
- II. Web Servers: NGINX
- III. Content Caching Servers: Varnish
- IV. CDN for Static Resources

MONITOR: PERFORMANCE & AVAILABILITY

- I. Profile Application, Fix Bottlenecks with newrelic.com or appdynamics.com
- II. zabbix.org
- III. Conduct Load-Tests: loader.io

CONTACT ME



LINKEDIN
ARSALANSE



TWITTER
@ARSALANSE



EMAIL
ASEFIDGAR@BIRJAND.AC.IR



PHONE
0914-773-4436

LINKS

1. [Github](#)
2. [Arvancloud](#)
3. [RFC 2267](#)
4. [BCP38](#)