14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)

14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)

* **Sending DNS resolution request from source computer (your.machine.52444) to DNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com).**
* **Reply comes back from the DNS server with IP address of the destination URL (203.0.113.22).**

14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0

14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0

* **Send a connection request (Flags [s]) from source computer to destination.**
* **.HTTP means port 80 commonly**
* **Received connection request (Flags [S.]).**

14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

* **HTTP: GET / HTTP/1.1 means requesting data from yummyrecipesforme.com this could be the download request for the malicious file**

14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

…<a lot of traffic on the port 80>...

14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0

14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0

14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1

14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0

…<a lot of traffic on the port 80>...

* **Sudden change happends, routed from source computer to DNS server again**
* **New IP address and its URL (greatrecipesforme.com)**