Flash Note 02, 24th February 2014

Large scale UDP attacks: the 2014 trend and how to face it

Recent news show the increase of large scale attacks[1] exploiting specific vulnerabilities of the Internet core protocols. In the latest cases, the Network Time Protocol (NTP), which allows synchronizing devices to the coordinated universal time (UTC), has been misused. Specifically, in December 2013, a vulnerability in this UDP protocol became mainstream and started to be exploited for large scale reflection attacks leading to a dramatic increase of the size of denial of services. Luckily, network providers can already put in place a series of known countermeasures to mitigate these threats, as ENISA underlined also for amplification attacks in April 2013[2].

The potential of using NTP in attacks is not new: NTP misuse and abuse have been around since the late nineties[3] , nevertheless the possibility to use the monlist vulnerability as an attack vector against specific targets was first publicly underlined in 2010 and early attempts to use this vulnerability can be traced back to 2011[4]. Unfortunately this specific vulnerability started to be exploited for highly recognizable objectives at the end of 2013, first on gaming sites and recently to target a content delivery network reaching enormous volumes per second. NTP allows synchronizing the time for any services between client and server and this attack exploits a functionality to retrieve a list of IP addresses that queried the server before the request. When addressing this specific request (monlist) using a spoofed victim IP address, the victim receives back the list of up to 600 IP addresses that queried the server before[5]. Due to the large size of incoming packets for a small request packet, the response can generate a denial of service as in the recent attack to a content delivery network where the attacker used 4,529 NTP servers running on 1,298 different networks generating approximately 400Gbps of traffic[6].

As Trusted Introducer reported on 13 January 2014, there are approximately 600,000 vulnerable hosts all over Europe[7]. Later in January Shodan published also a map of possible vulnerable servers around the world[8]. Fortunately, at the same time, official vulnerability advisories[9] [10] were released and various contributions for mitigations started to appear. It is clear that the trend of amplification and reflection attacks exploiting network core protocols is not going to stop: all UDP protocols that allow source IP spoofed attacks can be exploited for large scale DDoS or DRDoS[11]. This is not restricted to DNS and NTP but also CharGEN[12], SNMP[13], NetBIOS, QOTD and others services[14] that in some case are not even used anymore.

Recommendations

Reflected / spoofed attack have been around since 1997 but specific DNS and NTP (or other UDP protocols) amplification and reflections attacks have gained momentum only in the last few years. As for other attacks, first of all it is useful to

- disable unused services. If this is not possible, configure them with particular attention to the possible attack surface

Then, if possible, implement

- BCP38 ‘’Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing’’[15]
- BCP84 ‘’Ingress Filtering for Multihomed Networks’’ [16]

to filter traffic and block NTP and also all other source IP spoofed attacks[17].

Additionally, to prevent and mitigate NTP attacks use also the following resources:

- check if your machine is vulnerable on openntpproject.org[18]
- configure NTP client on Cisco IOS, Juniper JUNOS or iptables using Team Cymru Secure NTP Template[19]
- upgrade ntpd to at least 4.2.7 , if it is not possible check how to block/disable queries on ntp.org[20]

ENISA and the security and resilience of the Internet Infrastructure in Europe

ENISA will continue to investigate the area of Internet Infrastructure with the aim of providing all stakeholders in European Union Member States with recommendations on how to foster security and resilience. This year ENISA will follow up the 2013 report "Understanding the importance of the Internet Infrastructure in Europe" working with subject matter experts from the Internet operators' community, Cybersecurity agencies, NRAs and infrastructure security and resilience experts on vulnerabilities of the Internet infrastructure and related topics. For further information on the security and resilience of the Internet Infrastructure in Europe see also ENISA's website or send an email to resilience@enisa.europa.eu.

Flash Note produced by Rossella Mattioli, Security and Resilience of Communication Networks Officer, ENISA

ENISA's Flash Notes are issued by the Agency to draw the attention of the media and other interested parties to emerging issues in cyber security. The material contained in Flash Notes may be reproduced freely, provided the source is acknowledged.

References

[1] http://threatpost.com/high-volume-ddos-attacks-top-operational-threat-to-businesses-service-providers/103933

[2] http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability

[3] http://en.wikipedia.org/wiki/NTP_server_misuse_and_abuse

[4] https://labs.ripe.net/Members/mirjam/ntp-reflections

[5] http://www.us-cert.gov/ncas/alerts/TA14-013A

[6] http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

[7] https://www.trusted-introducer.org/news/TI-info-spreading.html

[8] http://shodanio.wordpress.com/2014/01/27/analyzing-ntp-usage-on-the-internet-with-shodan/

[9] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211

[10] https://www.cert-bund.de/advisoryshort/CB-K14-0020%20UPDATE%202

[11] http://blogs.cisco.com/security/a-smorgasbord-of-denial-of-service/

[12] http://www.iss.net/security_center/reference/vuln/Chargen_Denial_of_Service.htm

[13] https://www.cert.be/pro/docs/chargensnmp-ddos-attacks-rise

[14] https://www.us-cert.gov/ncas/alerts/TA14-017A

[15] http://tools.ietf.org/html/bcp38

[16] http://tools.ietf.org/html/rfc3704

[17] http://www.circl.lu/pub/tr-19/

[18] http://openntpproject.org/

[19] https://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

[20] http://support.ntp.org/bin/view/Main/SecurityNotice#DRDoS_Amplification_Attack_using