Poster: DRDoS Based on XXE

Jianjun Zhao[1], Siqi Yang[1,2], Di Wu[1,3], Qixu Liu[1,3]
1 (Institute of Information Engineering, Chinese Academy of Sciences)
2 (School of information and software engineering, University of Electronic Science and Technology of China)
3 (School of Cyber Security, University of Chinese Academy of Sciences)
zhaojianjun@iie.ac.cn

***Abstract*—Distributed Reflection Denial of Service(DRDoS) attacks have become one of the most significant web threats for a long time. Currently DRDoS Attacks are mainly based on transport layer protocol, such as UDP, while there is less based on application layer protocols. Therefore, we propose a type of DRDoS attack based on XML External Entity(XXE) vulnerability, which exhaust bandwidth resources of target server by using normal and not forged HTTP packets.**

Keywords—XXE; DRDoS; XML

I. INTRODUCTION

Distributed Denial of Service(DDoS) attacks have become an increasingly frequent disturbance of the global Internet. To achieve higher efficiency of attack with lower cost, DRDoS attack has become a trend. The advantage of DRDoS is that the attacker doesn't need a large botnet to perform an attack, they usually send payload to many intermediate servers called amplifiers or reflectors, which multiply the traffic flow many times and attack the target server.

There are two main implementations of DRDoS. One way is to modify the source IP address in the UDP packet, so that amplifiers or reflectors will send a large amount of response packets back to the forged IP address, such as Smurf attack[1] and super memcached DDoS[2]. The other way is to spoof the intermediate host to request a large file from target server, such as Joomla Googlemap plugin DRDoS[3].We found that XML parser could cause a same problem when loading an external entity.

XML is an markup language for transferring and storing data and is widely used for data interactions across platforms. But in recent years, the injection of XML external entity is more and more serious and widespread, which rises to fourth place of OWASP top 10. When XML allows references to external entity, the keyword "SYSTEM" causes the XML parser to read content from URL and allows it to be replaced in the XML document. The attacker customizes the value of the external entity, forcing the XML parser to access the contents of the attacker's specified resource. This is called XML external entity injection[4].

II. IMPLEMENTATION

For the reason that XML parser can load external file, we focus on exploring a novel DRDoS attack using XXE.

A. *Reference to external entity*

Some web servers use XML to transfer or store data, and also need to load external entities to support certain functions. We divide the specific operation of loading an external entity into 3 steps, as shown in a) of Figure 1. First, user send a normal HTTP request to a web server, the web server start process this request. Secondly, in order to process the request successfully, XML parser in the web server need to load external entities defined in a DTD file. The DTD file is prepared in advance on remote resource server, so it can be used by other web servers. The way of obtain a DTD file is send a HTTP request to download the DTD file from remote resource server. Thirdly, after the web server downloads the DTD file, the XML parser replace entities, processes data, and return a response to the user.

From the point of view of the web server, it downloads a DTD file, however, thinking from a different perspective, the remote resource server uploads the DTD file. If the file uploaded by the remote resource server is very large, the upstream traffic will be extraordinary large.

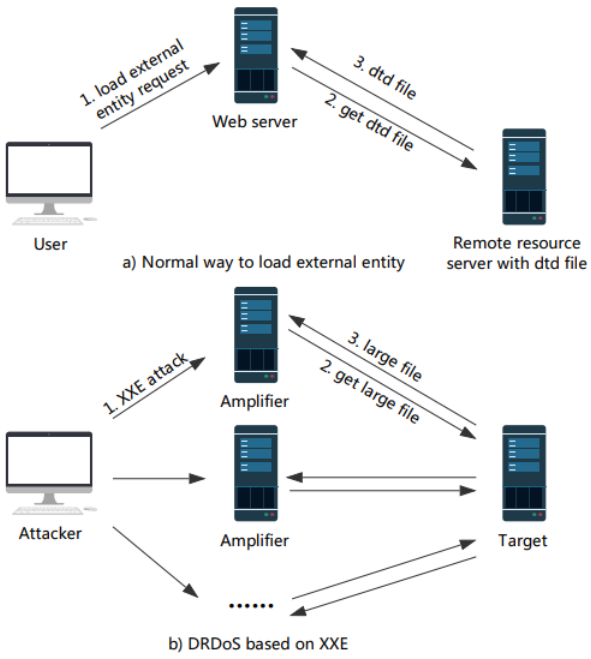

Figure 1. The process of DRDoS

B. *Replace external DTD files with other format files*

In a real network, an ordinary server usually does not have DTD file, but there are many other types of files in it. To verify whether a XML parser can load other format files, we replace the DTD file in remote resource server into other format files, such as TXT file, JPG file, ZIP file and DOC file etc.

After modifying XML document, what we only need to do is to send a very small request package, and no files will return to our host. The remote resource server just need to upload several format files.

It can be seen from Figure 2, this modified attack can indeed request the large JPG files successfully. In contrast to DTD file, the other format files can also be downloaded.

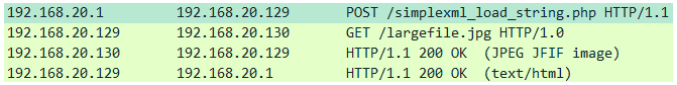

Figure 2. An attempt of loading an external JPG file

C. *Traffic analysis*

In our experiment of loading an external entity, the external entity DTD file requested by the web server was replaced with a JPG file. We count the traffic in the web server's log file and display the results in TABLE 1. The amplifier's traffic is almost the same as the target's traffic, and the upstream traffic is determined by the size of external file and number of files transferred. Therefore, as long as there are a large number of amplifiers, it is possible to launch a large-scale attack against the target.

TABLE I. TRAFFIC DEMO

	Upstream traffic	***Downstream traffic***
Attacker	406B	862B
Amplifier	1000B	134300B
Target	133894B	138B

D. *Possibility of DRDoS*

For XXE attack, attacker's remote VPS usually used to obtain some information or to provide some small DTD files. The upstream traffic is very small, so this will not cause any impact on the remote VPS. However, from the above experiment, we can speculate that, through XXE attacks, remote VPS can also upload large files of some common formats. Web servers with XXE vulnerabilities can increase the number of downloaded files at the same time by sending multiple requests, thereby consuming upstream traffic of remote VPS. Therefore, we speculate that the XXE vulnerability could lead to DRDoS.

This is the second way of implementation of DRDoS mentioned earlier in this poster, spoofing the intermediate host to request a large file from target server. With the XXE vulnerability, attackers can make the intermediary server requests arbitrary external files. In our DRDoS attack, the intermediate server is the amplifier, and the server hosting the external file is the target. As shown in b) in Figure 1, an attacker can use multiple hosts with XXE vulnerabilities as amplifiers and concurrently initiate file download requests to the target server so that the upstream traffic of the target server can rapidly increase. At this point, the attacker only needs to consume very few resources and can hide the attacker's real address.

III. COUNTERMEASURE

We also put forward some defense measures against this threat. Previous versions of libxml2.9.1 were able to parse external entities by default, but since libxml2.9.1 and later versions, load external entity is disabled by default, and some old PHP and Python functions have been disabled too. Therefore, upgrading the libxml system library can effectively prevent the server from being used as a DRDoS amplifier.

Compared with PHP and Python, the causes of XXE attacks in JAVA are more complicated. For JAXB, using the ISSUPPORTING_EXTERNAL_ENTITIES and IS_SUPPORTING_EXTERNAL_ENTITIES functions in the XMLStreamReader class may be subject to the XXE attack. In addition, if the SetExpandEntityReferences, setFeature, and setProperty in the parser configuration items are improperly set, they may also be subject to XXE attacks. So it is necessary to ensure that every function of XML parse is not allowed to load external entities.

IV. CONCLUSION

In our work, we discovery a novel application layer DRDoS which uses XXE vulnerabilities to attack servers in the network and the threat is universal. By using reflectors and amplifiers, real attackers can be hidden at the same time. For such attacks, we also talk about some defensive countermeasures.

ACKNOWLEDGEMENT

This work is supported by the National Key R&D Program of China (No. 2016YFB0801604, No. 2016QY08D1602), Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection.

REFERENCES

[1] Sanjeev Kumar, Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet, on Internet Monitoring and Protection, 2007.

[2] Steven J. Vaughan-Nichols, "Memcached DDoS: The biggest, baddest denial of service attacker yet", March 1, 2018. [Online]. Available: https://www.zdnet.com/article/memcached-ddos-the-biggest-baddest-denial-of-service-attacker-yet/

[3] Security Activity Bulletin, "Joomla! Google Maps Plugin Multiple Remote Security Vulnerabilities", January 8, 2014. [Online]. Available: https://tools.cisco.com/security/center/viewAlert.x?alertId=32348

[4] T Morgan, What You Didn't Know About XML External Entities Attacks, on Appsec Usa, 2013