ЗАЩИТА NTP-СЕРВЕРОВ ОТ DDOS-АТАК

Чан Тхюи Зунг , Ха Туан Кханг
Научный руководитель: Ботыгин И.А., к.т.н., доцент
(г. Томск, Томский политехнический университет)

PROTECTION FROM SERVER NTP-DDOS-ATTACKS

Tran Thuy Dung, Ha Tuan Khang
(s.Tomsk, Tomsk Polytechnik University)

The realization of DDoS-attacks using the protocol NTP. The amplification of traffic NTP-server when you issue monlist. The recommendations for the protection of NTP-server from DDoS-attacks.

Атаки с распределенным отказом в обслуживании – это реальная и растущая угроза, с которой сталкиваются компании во всем мире. Цель подобной атаки заключается в создании потока флуд-заявок, вызывающих затруднения у авторизованных пользователей получить предоставляемые ресурсы или информационные сервисы. Как правило, атака «отказ в обслуживании» реализуются большим количеством программных агентов, которые злоумышленник ранее разместил на подчиненных ему хостах (зомби- компьютерах).

В последнее время очень популярны DDoS-атаки с усилением трафика. Но если раньше для усиления трафика подобные атаки проводились с задействованием DNS-серверов, то сейчас для многократного усиления трафика используются серверы синхронизации точного времени. Это – так называемая атака с использованием протокола NTP (Network Time Protocol), предназначенного для синхронизации внутренних часов в компьютерах [1,2]. Специалистами угроза усиления UDP-трафика через серверы сетевого времени NTP оценивается как новая угроза для сети. Именно подобными потоками ложных запросов были атакованы и, фактически, выведены из строя игровые серверы EA, Blizzard's Battle.net и League of Legends.

Необходимо отметить, что протокол NTP непрерывно совершенствуется и находит широкое применение для реализации серверов точного времени. В NTP используется многоуровневая система источников времени (рис. 1).

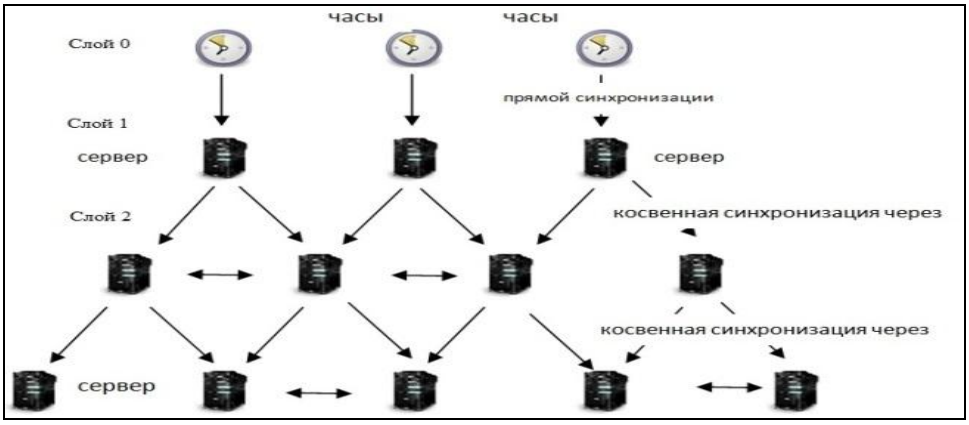

Рис. 1. Иерархическая система источников времени в NTP

Слой 0 синхронизирован с высокоточными часами. Например, с Единой Государственной шкалой времени Российской Федерации или с атомным эталоном

времени. Слой 1 прямо синхронизируется с одной из машин слоя 0. Все последующие слои осуществляют косвенную синхронизацию через серверы предыдущего слоя.

Для обеспечения надежности и устойчивости работы в NTP для передачи пакетов данных используется протокол UDP. Именно отправка UDP-пакетов с зомби-компьютеров с подставным обратным адресом на атакуемый сервер и используется для промежуточного усиления трафика. Незащищенному публичному NTP-серверу отправляется запрос с адресом атакуемого сервера в качестве отправителя. Запрос содержит команду monlist, результатом которой является отправка списка шестисот последних IP-адресов, с которых были обращения к NTP-серверу. Таким образом, на атакуемый сервер направляются сотни мегабайтов ненужного ему трафика. А поскольку трафик этот состоит из легитимных данных, поступающих с легитимных же серверов, блокировка подобных атак оказывается крайне затруднительной.

На рис. 2. представлен фрагмент применения команды monlist через демон ntpd для одного из NTP-серверов. Отметим, что команда monlist выполняется без всяких ограничений на ее использование.

```
root@bt:~# ntpdc -c monlist 221.240.6.134
***Warning changing to older implementation
remote address          port local address      count m ver code avgint  lstint
===============================================================================
visor.vpn-pool.zzzing. 49977 221.240.6.134          2 7 2    0      0        0
s630170.xgsspn.imtp.ta 37775 221.240.6.134          1 3 3    0      0        0
i58-89-115-36.s41.a022   123 221.240.6.134          7 3 4    0      0       19
s2012045.xgsspn.imtp.t 55379 221.240.6.134          1 3 3    0      0        0
122x219x133x245.ap122. 54368 221.240.6.134          1 3 4    0      0        0
om126204003072.3.openm 47736 221.240.6.134          2 3 3    0      0        3
softbank219172074021.b 60185 221.240.6.134        603 3 4    0      0     1521
s670096.xgsspn.imtp.ta 35162 221.240.6.134          3 3 3    0      0        0
s664142.xgsspn.imtp.ta 45714 221.240.6.134          1 3 3    0      0        0
s691137.xgsspn.imtp.ta 42142 221.240.6.134          1 3 3    0      0        0
```

Рис. 2. Фрагмент запроса с использованием команды monlist.

Выполнение утилиты ntpdc -c monlist NTP_IP_Address вместе с программой анализа трафика компьютерных сетей Wireshark показало, что возможно усиления объема трафика в 1000 раз.

Для защиты NTP-сервера от ложных запросов можно настроить брандмауэр так, чтобы заблокировать все запросы monlist от IP-адресов вне сети. Такого же эффекта можно добиться и модификацией утилиты ntpd (отключить поддержку команды monlist).

ЛИТЕРАТУРА

1. Network Time Protocol // In Wikipedia, The Free Encyclopedia. 2014. URL: http://en.wikipedia.org/w/index.php?title=Network_Time_Protocol&oldid=601605831 (дата обращения: 10.04.2014).

2. NTP: The Network Time Protocol // Network Time Foundation. 2014. URL: http://www.ntp.org/index.html (дата обращения: 10.04.2014).