“The- Cat- is- Out- of- The- Bag” DNS Bug

by Ravi Balupari

본문서는 최근 이슈가 되고 있는 Dan Kaminsky의 DNS 취약점에 대한 Ravi Balupari의 글을 번역한 것이다.

Hacking Group “OVERTIME”

force <forceteam01@gmail.com>2008.08.13

“The- Cat- is- Out- of- The- Bag” DNS Bug

역자 주 : 제목 The- Cat- is- Out- of- The- Bag 은 고양이를 가방에서 풀어놓다 라는 뜻으로 비밀을 풀어놓다 와 같은 뜻으로 해석됨

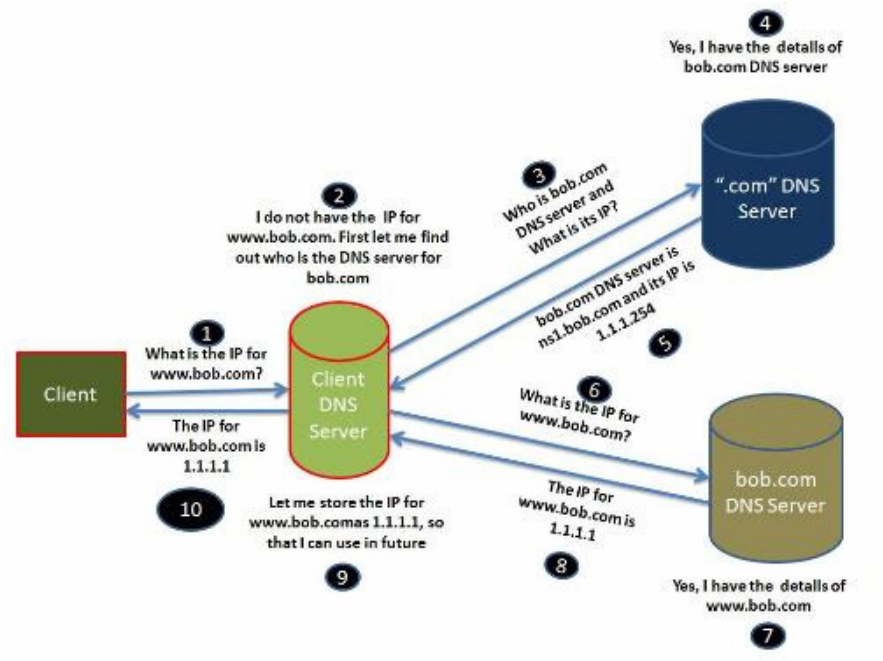
최근 Dan Kaminsky에 의해 발견된 DNS 보안 이슈에 관한 내용이 자주 다루어지고 있다. Dan에 의해 야기된 관련 산업 전체의 효과는 여러 밴더가 관련 패치를 발표했다는 것이다. 아직 Dan에 의해서 관련 이슈의 기술적인 상세 내용이 발표되지 않았지만 우연히 Matasno 보안 블로그에 이와 관련된 많은 정보들이 누설된 것으로 보인다.
아직 블로그에 누설된 정보가 Dan이 블랙햇에서 발표할 내용과 동일한 내용인지 아직 확실하지 않다.

역자 주: 블랙햇에 발표된 내용을 정말 간단히 살펴봤을 때 동일 내용으로 보이며 익스플로잇을 보면 같은 방식으로 공격하는 것을 확인할 수 있다

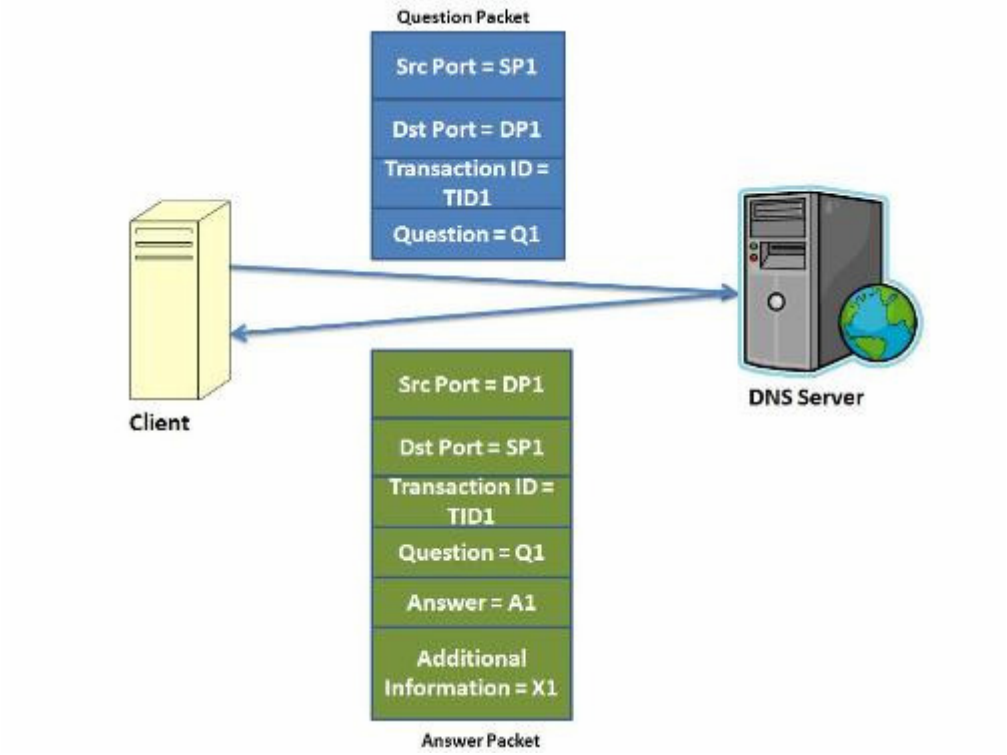
그러나 블로그에 설명된 시나리오에 따르면 인터넷에서 매우 심각한 위협임이 틀림없다, 그 후 여러 블로그와 문서에서 관련 내용이 토론되었고 결론적으로 해당 취약점에 대한 위협은 DNS 프로토콜의 두 가지 사항에서 나타난다는 것을 알게 되었다.

1. 예측 가능한 소스 포트 와 트랜잭션 ID

   DNS는 원래 질문을 보내고 답변을 받을 때 UDP 패킷을 사용한다. 아래 있는 그림은 클라이언트가 www.bob.com IP 주소를 찾고자 할 때의 상황을 간단하게 묘사한 그림이다

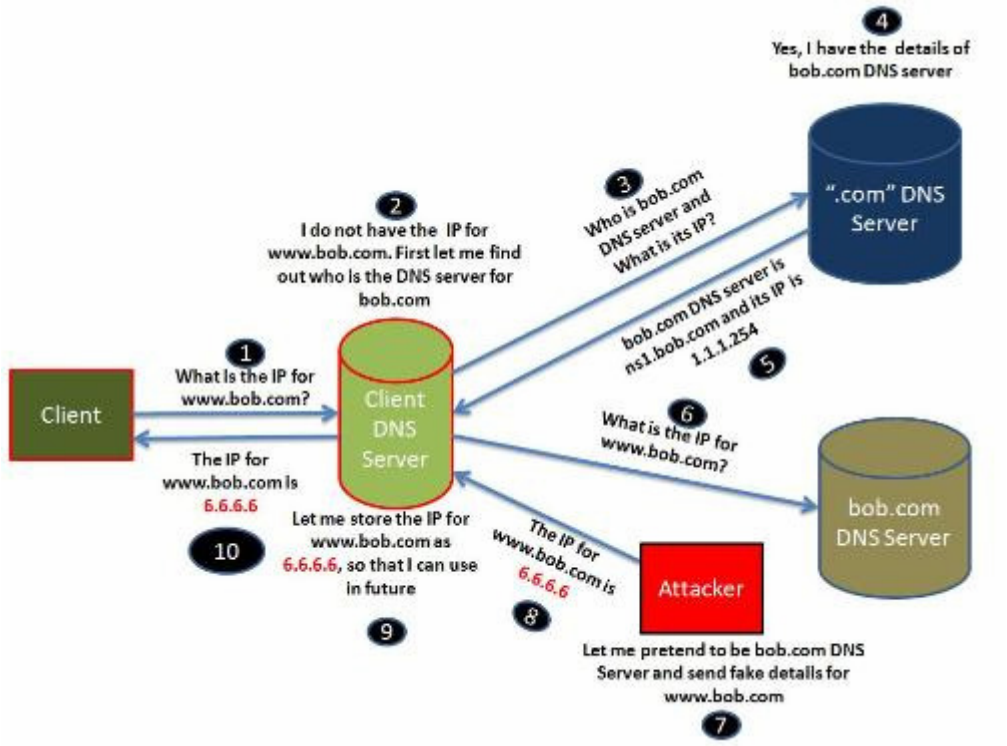


또한 DNS 질의(요청) 와 답변(응답) UDP 패킷은 아래 그림과 같은 간단한 구조를 가진다.

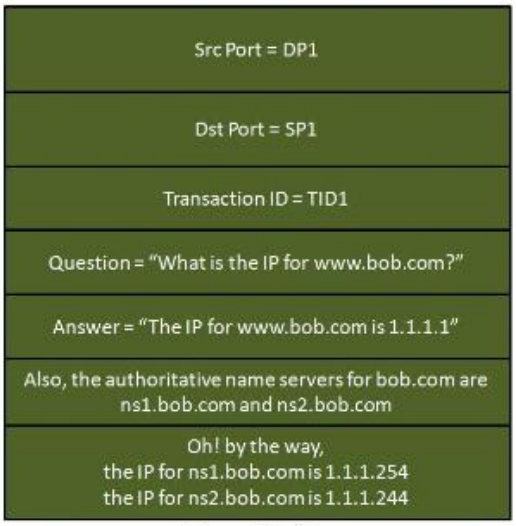


클라이언트는 질문에 대한 답변으로 패킷이 DNS 서버로부터 오는 한은 해당 패킷을 받을

것이다. 여기서 답변 패킷의 소스 와 목적지 포트는 질문 패킷의 목적지 와 소스 포트와 동일하며 또한 가장 중요한 Transaction ID 와 Question은 질문 패킷과 동일해야 한다.
공격자는 정상적인 DNS 서버를 사칭하는 동안 이와 같은 응답 패킷을 속일 수 있다. 그리고 또한 소스 포트(SP1) 와 transaction ID(TID1)를 추정할 수 있다. (목적지 포트는 일반적으로 53번이다).
공격자는 또한 정상적인 DNS Server로부터 오는 실제 응답 패킷이 클라이언트에 도달하기 전에 변조된 응답 패킷이 도착하도록 확실히 할 필요가 있다. 아래 그림은 매우 간단한 공격 시나리오를 나타낸다.



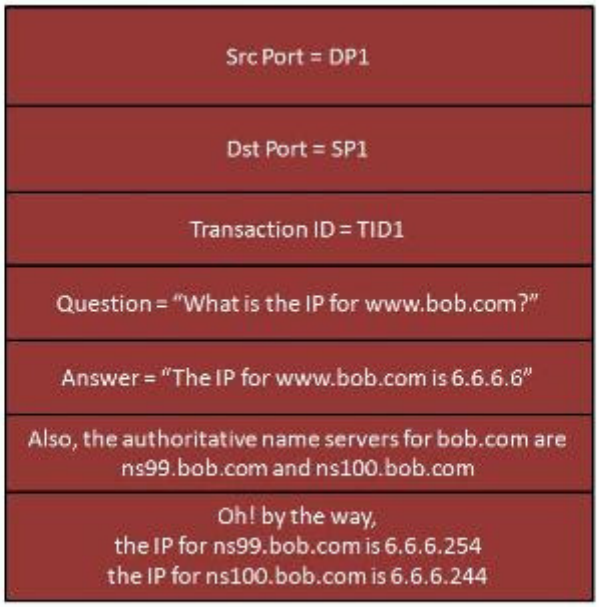
2. 추가 리소스 레코드(Additional Resource Records)
DNS 서버가 질문에 응답할 때 향 후 진행과정을 효율적으로 하기 위한 추가적인 정보를 답변에 포함해야 한다. 클라이언트 DNS 서버에서 bob.com DNS 서버로 “www.bob.com의 IP 주소는 무엇인가?”와 같은 질문의 응답 패킷은 아래 그림과 같은 형태를 보인다.



Answer Packet

그래서 클라이언트 DNS 서버가 bob.com 도메인의 mail.bob.com과 같은 또 다른 IP를 알고 싶을 때는 1.1.1.254 또는 1.1.1.244 DNS 서버에 직접 질문을 보낸다.

위의 두 가지 이슈의 결합은 좀 더 흥미로운 상황을 만든다. 만일 공격자가 소스 포트 와 transaction ID(위의 첫째 항목에서 다룬)를 예측하고 또한 DNS 서버를 자신의 악의적 DNS 서버를 가리키도록(위의 두 번째 항목에서 다룬) 추가적인 정보를 조작해서 응답 패킷에 삽입한다면 공격자는 bob.com 도메인에 대한 트래픽을 통제할 수 있게 된다.
아래 그림은 이와 같은 조작된 응답 패킷에 대한 그림이다.



Evil Answer Packet

이론적으로 모든 것이 간단한 것처럼 보이지만 공격이 성공하기 위해서는 소스 포트와 transaction ID를 추측하는 두 가지 중요 과정에 달려 있다. 실제로 공격자가 정상 DNS 서버의 응답을 피해자가 받기 전에 DNS 요청의 소스 포트와 transaction ID를 추측하기 위해서는 무차별적인 시도가 요구된다. 몇몇 DNS들은 transaction ID가 완벽하게 랜덤 한 형태로 생성되지 않는 것들도 있다. 이와 같은 DNS들은 또한 짧은 시간에 오는 순차적인 질문을 해결하기 위해서 같은 목적지 DNS 서버에 접속할 때에는 같은 소스 포트를 사용하는 경우도 있다. 이와 같은 패턴은 피해자의 네임 서버에 특정 도메인들을 찾는 행위들을 통해서 공격자가 해당 DNS 서버가 이와 같은 취약점을 가지고 있는지 확인할 수 있다. 또한 이 패턴을 찾는 방법은 생일공격(birthday attack)과 같은 또 다른 방법들과 결합해서 좀 더 쉽게 적은 시도만으로 소스 포트와 transaction ID를 추측할 수 있다.

이 DNS 위협이 좀 더 심각한 상황에 있을 수 있는 또 다른 이유는 피해 네임 서버가 NAT 장비 안쪽에 위치해 있을 경우 내부에서는 랜덤 소스 포트를 생성하지만 외부로 나갈 때 포트 변환이 순차적인 순서로 변환될 수 있다.(또는 다른 고정된 패턴의 소스 포트로) 이와 같은 현상은 공격자의 수고를 한층 덜어줄 수 있다.

우리는 공격이 성공했을 때의 잠재적인 효과가 DNS Server cache가 오염되었을 때 보다 훨씬 더 크다는 것을 유념해야 한다. 만일 당신의 DNS 서버가 취약한지 점검하고 싶다면 Dan의 DNS CHECKER(http://www.doxpara.com/)를 이용하여 점검하거나 또는 Sans

Dairy(http://isc.sans.org/diary.html?storyid=4765)에서 제공하는 여러 방법을 이용하면 된다.

McAfee Network Security Platform(IntruShield 이전)을 소요한 McAfee 고객은 다음 공격 시그니쳐 id 0 x 40303200이 sigset4.1.30.4 와 sigset3.1.67.3에 발표되었다.