급변하는 위협에 대응하기 위한 DNSBL을 이용한 IPS

왕정석° 권희웅 곽후근 정규식
숭실대학교 정보통신 전자공학부
{wang°, hukwon, gobarian, kchung}@q.ssu.ac.kr

The IPS using DNSBL to Protect Rapidly Changing Threats

Jeongseok Wang° Huiung Kwon Hukeun Kwak Kyusik Chung
School of Electronics Engineering, Soongsil University

요 약

최근 개인 정보 취득에 대해 가장 널리 사용되는 방법 중 하나는 특정 사이트의 모조를 통해 사용자를 혼란 시켜 개인 아이디, 계좌 정보 등을 입력하도록 하여 개인 정보를 취득하거나, 일반적으로 많이 사용되는 신뢰된 인터넷 상의 공간(Portal BBS, 카페, 블로그 등)에 특정한 스파이웨어 등을 숨겨놓아 사용자 컴퓨터에 설치되도록 유도 한 후 개인 정보를 취득하는 등의 지능적이고 기존의 방법으로는 차단하기 어려운 방식을 사용하고 있다. 최근 더욱 그 기세를 넓히고 있는 다양하고, 빠르게 변화하는 위협들로부터 사용자 정보 및 네트워크를 안전하게 보호하기 위한 다양하고 적극적인 방법이 필요하다. 이를 위해 보안 장비와 계층적 RBL DNS를 이용한 근본적인 위협원 접근 차단 방법을 통해 급변하는 위협으로부터 사용자의 정보와 네트워크를 안전하게 보호할 수 있는 방법을 제안한다.

1. 서 론

인터넷의 사용이 개인적, 업무적인 영역을 통해 급격히 증가하고, 그에 대한 의존도가 높아가고 있으며, 이로 인해 인터넷을 통한 위협과 정보 보호의 중요성 역시 함께 증대되고 있다. 그로 인해 인터넷을 통한 다양한 위협으로부터 사용자 및 네트워크의 자원과 정보를 보호하기 위한 방법 역시 꾸준히 발전하고 있다. 하지만 현재까지 사용되고 있는 많은 방법들은 현존하거나 잠재적인 위협들로부터 네트워크 및 사용자 정보를 보호하기 위한 측면의 보호는 있지만, 최근 위협원으로 떠오르는 피싱(Phishing)등의 급격히 변하는 다양한 종류의 위협을 막기에는 부족한 측면이 존재한다[1].

최근 개인 정보 취득에 대해 가장 널리 사용되는 방법은 특정 사이트의 모조를 통해 사용자를 혼란 시켜 개인 아이디, 계좌 정보 등을 입력하도록 하여 개인 정보를 취득하거나, 일반적으로 많이 사용되는 신뢰된 인터넷 상의 공간(Portal BBS, 카페, 블로그 등)에 특정한 스파이웨어 등을 숨겨놓아 사용자 컴퓨터에 설치되도록 유도 한 후 개인 정보를 취득하는 등의 지능적이고 기존의 방법으로는 차단하기 어려운 방식을 사용하고 있다[2].

이에 보안 장비와 도메인 네임 서비스의 연계를 이용하여 급격히 변하는 위협으로부터 사용자의 개인 정보 및 네트워크를 보호하기 위한 구조를 제안한다.

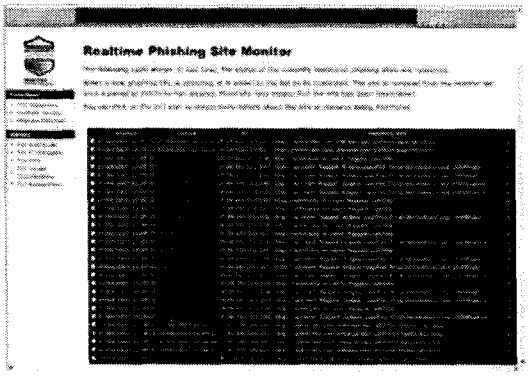
2. 관련 연구

2.1. Phishing Monitor[3]

현 시점에도 인터넷을 통한 사용자 정보 유출의 시도는 계속 진행되고 있으며, 이는 특정 장소의 특정 서버를 이용하는 방식이 아닌, 해커가 또 다른 희생자를 이용하는 방식으로 이루어 지고 있다. 즉 보안이 취약한 특정 웹서버 등을 해킹하는 방식으로 자신의 위치를 전혀 추적당하지 않으면서 희생자의 서버를 이용하여 또 다른 희생자가 나타나서 개인 정보를 유출해 주도록 노리고 있는 것이다.

최근의 이러한 경향은 자신이 운영하는 웹서버 등을 이용하거나, 피싱을 위해 해킹한 사이트를 계속 유지하는 것이 해커 자신에게도 굉장히 위험한 행동이 될 수 있기 때문이다. 따라서 최근의 피싱 사이트는 극도로 짧은 시간 동안만 존재하다가 사라지는 현상을 반복하고 있다[4].

이 경우 해커는 실제 피싱에 사용되는 서버로의 원활한 접속 관리를 위해 도메인 네임을 이용하고 있다. 도메인 네임 서버에 자신이 피싱에 사용하는 도메인 네임을 등록 시킨 후 도메인 네임의 호스트 아이피를 해킹한 서버의 아이피로 변경하는 과정을 통해 접속이 항상 원활히 될 수 있도록 하는 것이다.



[그림 1] 실시간 피싱 사이트 모니터

[그림 1]은 InternetDepence.net의 실시간 피싱 사이트 모니터링 결과를 나타낸다.

이와 같은 피싱 모니터링 정보를 이용하여 실시간으로 계속 발생되는 해킹과 그 결과로 이용되는 피싱 사이트의 도메인 네임, URI 등의 정보를 확인할 수 있다.

2.2. Using RBL in Anti-Spam

최근 가장 RBL을 많이 사용하는 영역이 바로 Anti-Spam 부분일 것이다. Anti-Spam에서 사용되는 RBL 데이터는 주로 최근 스팸 메일을 보내는 것으로 판명되는 아이피 주소, Relay 기능의 잘못된 설정으로 스팸 Relay 서버로 악용될 수 있는 메일 서버, 그리고 정상적으로 메일서버가 사용되기 어려운 ISP의 일반 가입자망 주소 등이 사용된다[5].

이를 이용하여 메일이 도착할 경우 송신자의 아이피 주소를 이용하여 이상 없는 송신지에서 발송되거나 경유된 메일인지를 확인하여 수신 여부를 결정한다[6].

최근 대다수의 Anti-Spam 솔루션과 메일 서버가 스팸 관리에 도움을 받을 수 있도록 RBL 기능을 지원하고 있다.

2.3. DNSBL (Domain Name Service Black-hole List)[7]

이미 Anti-Spam 영역에서 RBL을 이용한 송신자 검출이 잘 활용되고 있다. 이는 목적지(수진자)의 입장에서 송신지의 주소 정보를 RBL의 주요 정보로 이용하여 검출하는 것으로 일반적인 인터넷 이용 환경, 특히 웹과 같은 환경에는 적용이 어려운 것이 현실이다.

하지만 인터넷을 이용하는 사용자 네트워크 측면에서는 송신지의 주소보다 해당 사용자가 접속하게 될 목적지가 더욱 중요하고, 정보 유출의 가능성 역시 목적지를 통해 이뤄진다고 봤을 때, Anti-Spam 에서의 접근법과는 다른 방식이 필요하다.

이것이 목적지의 주소를 이용한 RBL의 필요성이며, 이를 이용해 목적지 주소의 유효성 여부를 기록하는 것을 DNSBL이라 한다[8].

3. 계층적 DNSBL을 이용한 보안장비 구성

IPS와 같은 보안 장비에 DNSBL의 계층적 구조를 이용하면, 피싱 사이트 등에 대한 사용자의 접속을 미연에 방지하여 사용자의 정보 및 접근을 보호할 수 있다. 앞에서 살펴 봤듯이 피싱 사이트는 그 떳떳하지 못한 특성 때문에 보안이 취약한 개인 및 조직의 웹 서버를 해킹하여 자신이 원하는 화면을 보여 줄 수 있도록 꾸민 후 해당 페이지에 대해 사용자가 접속하도록 하여 원하는 사용자의 정보를 입력 받는다. 따라서 이와 같은 피싱 사이트에 접속할 수 없도록 하면 사용자가 해커에게 속아 정보가 유출되는 것을 막을 수 있다.

하지만 이 경우 대단히 많은 유해 도메인 정보를 각 IPS가 가지고 있어야 하고, 모든 IPS가 급격히 변하는 피싱 사이트들에 대한 내용을 검색해야 하므로 상당한 오버헤드가 발생할 수 있다. 이를 해결하기 위해 일반적인 도메인 네임 서버의 동작처럼 계층 구조의 상위 도메인 네임 서버(이하 RBL 도메인 네임 서버)를 두어 해당 RBL 도메인 네임 서버가 피싱 사이트에 대한 정보를 갱신하고, 하위로부터 온 도메인 네임 정보에 대한 응답을 담당한다.

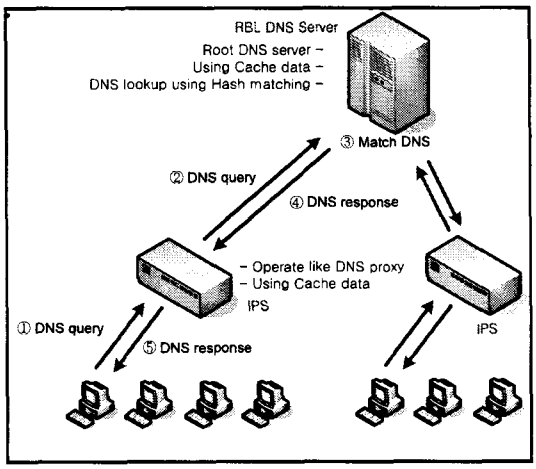
해커가 사용하고 있는 도메인 네임에 대해 Black-hole List에 등록하고, 이에 대한 요청 쿼리에 대해 응답을 해주지 않음으로써 사용자의 접속을 막을 수 있다.

도메인 네임 서버를 기준으로 볼 때 일반적으로 로컬 네트워크는 두 가지의 형태로 구분을 둘 수 있는데, 이는 내부에 자체 도메인 네임 서버를 운영하고 있는 경우와 외부의 공개된 도메인 네임 서버를 이용하는 경우이다.

먼저 작은 네트워크의 경우 일반적으로 내부에 도메인 네임 서버가 없이 외부의 공개된 도메인 네임 서버를 이용하게 되는데, IPS는 외부로 향하는 도메인 네임 정보 요청 쿼리를 가로채어 이에 대한 응답을 대신 할 수 있다.

[그림 2]는 내부에 네임서버가 없는 네트워크 환경에서의 동작을 보여준다.

이 그림에서처럼 사용자로부터의 도메인 정보 요청을 가로챈 IPS는 이 요청을 RBL 도메인 네임 서버로 보내고, RBL 도메인 네임 서버로부터의 응답을 사용자에게 전달하는 과정을 통해 투명하게 동작한다. 사용자가 요청한 도메인이 위협원으로 판명되어 black-hole list에 등록되어 있는 상태라면 해당하는 사용자에게 원래 도메인이 향하도록 되어있는 아이피 주소의 응답을 주지 않음으로써 사용자가 근본적으로 피싱 사이트에 접근할 수 없게 된다.

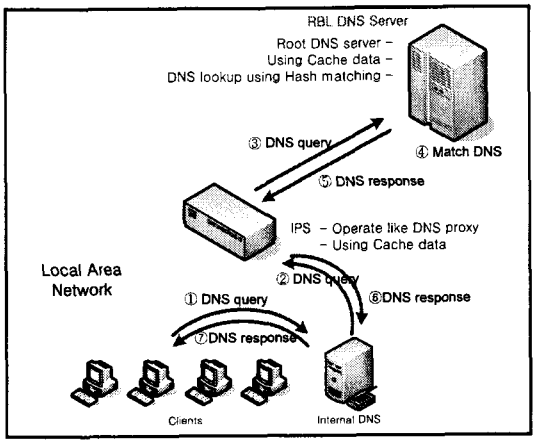


[그림 2] 도메인 네임서버가 없는 네트워크 환경

두 번째 네트워크 환경은 내부에 도메인 네임 서버를 운영하고 있는 경우의 네트워크 구성이다. 일반적으로 중소 규모 이상의 기업, 학교 등의 네트워크 구성으로 일반 사용자의 도메인 네임 정보 요청은 내부 도메인 네임 서버를 통해 이루어 지게 된다. 따라서 사용자의 도메인 네임 정보 요청은 직접적으로 IPS를 통과하지 않게 된다.

하지만 이 경우에도 내부 도메인 네임 서버는 자신이 직접적으로 관리하는 도메인에 대한 정보만을 가지고 있으며, 사용자가 자신이 관리하지 않는 도메인 정보를 요청할 때에는 그 자신도 상위의 도메인 네임 서버로 요청을 보내 해당하는 도메인 정보를 얻어오게 된다. 이 경우 내부 도메인 네임 서버에서 외부로 전달되는 요청을 첫 번째 경우와 같은 방법으로 가로채어 RBL 도메인 네임 서버로 요청을 보내 처리할 수 있다.

[그림 3]은 내부에 도메인 네임 서버가 있는 네트워크 환경에서의 동작을 보여준다.



[그림 3] 도메인 네임서버가 있는 네트워크 환경

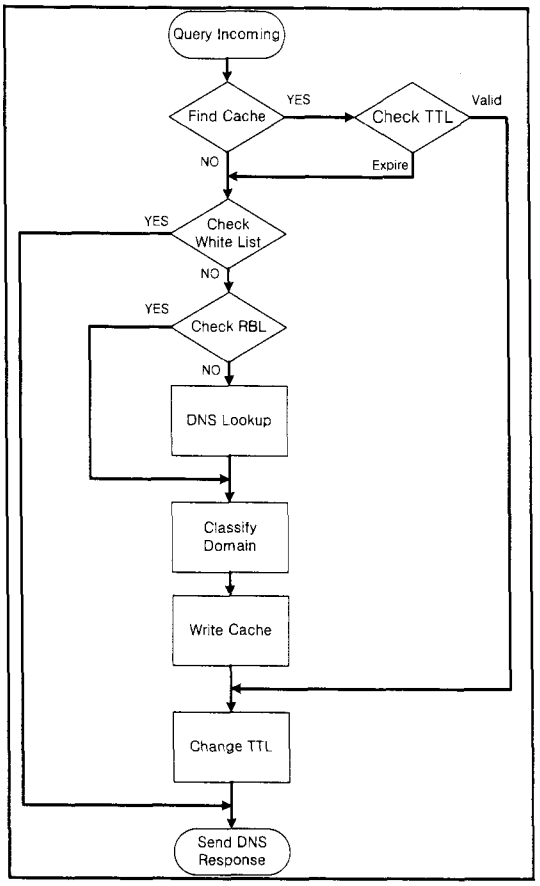
[그림 2]와 [그림 3]에서 나타나듯이 각 IPS 및 RBL 도메인 네임 서버는 1차적으로 자신이 전달한 응답에 대해 캐싱을 하고, 요청이 캐싱된 데이터 중에 없는 경우 RBL에 있는 도메인인지 검사한 후, 이상이 없는 도메인에 대해서만 정상적인 도메인 정보 응답을 보낸다. 각 IPS에서 자주 접속하는 도메인에 대해 일차적으로 캐싱을 하고, RBL 도메인 네임 서버 역시 캐싱 방법을 통해 주요 도메인에 대한 응답이 늦어지는 것을 방지할 수 있다.

[그림 4]는 RBL 도메인 네임 서버 내부의 동작을 나타낸다.

이 그림에서 살펴 볼 수 있듯이 일반적인 도메인 네임 서버가 수행하는 여러 동작의 앞부분에 오탐을 방지하기 위한 White list 확인 및 RBL 데이터 확인 과정을 통해 원하는 응답을 할 수 있게 된다.

앞서 살펴 봤듯이 주요 위협원인 피싱 사이트는 수시로 그 위치와 이름을 변경하며 사용자의 정보를 노리므로, 이를 대처하기 위해서 주기적으로 RBL을 갱신하는 작업이 필요하다. 이러한 주기적 갱신 작업을 통해 리스트를 항상 새롭게 유지할 수 있게 된다.

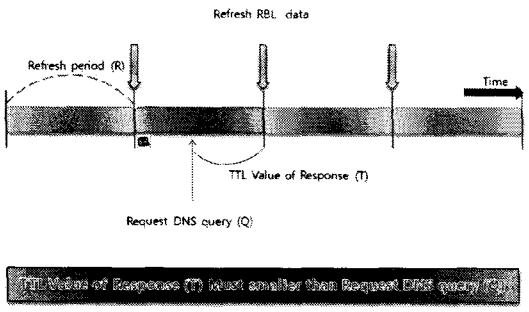
이 갱신 주기는 사용자의 도메인 정보 요청 응답에 매우 중요한 데이터로 작용한다. 모든 도메인 요청 정보에는 TTL(Time To Live)값이 존재하고, 이는 도메인 정보가 너무 오래되어 잘못 사용되거나, 너무 짧은 요청 주기로 인해 도메인 네임 서버가 받을 수 있는 부하를 줄여주는 중요한 역할을 한다.



[그림 4] RBL 도메인 네임 서버 내부 동작 순서도

RBL 도메인 네임 서버는 이 TTL 값을 적절하게 수정하여 항상 각 IPS 및 사용자가 RBL 갱신 주기와 일치되어 새로운 정보를 얻을 수 있도록 한다.

[그림 5]는 RBL 정보 갱신 주기와 응답 TTL 간의 상관관계를 나타낸다.



[그림 5] RBL 정보 갱신 주기와 TTL 값

위의 그림에서 볼 수 있듯이 도메인 정보 요청(Q)의 시점을 기준으로 다음 RBL 정보 갱신 때까지 남은 시간이 해당 도메인 정보의 TTL로 대체되어 사용자에게 전송된다.

이러한 과정을 통해 사용자는 최초 요청 시간과 상관없이 다음 RBL 정보 갱신 시점 이후에 재접속을 원할 경우, 다시 RBL 도메인 서버로 요청을 보내게 되어 항상 새롭게 적용된 데이터에 의한 응답을 받을 수 있게 된다.

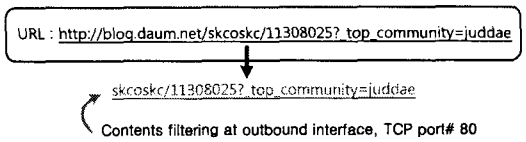
4. URI 필터링

앞서 우리는 일반적으로 위협원이 되는 도메인에 대해 해당 도메인에 대한 응답을 차단함으로써 근본적으로 접근을 막아 문제를 해결하였다. 하지만 이러한 경우 이외에도 많은 피싱 및 스파이웨어는 안전하다고 생각되거나, 일반적인 방법으로 검출이 어려운 경로를 이용해 자신의 활동 영역을 넓힌다.

일반적인 포털 사이트의 게시판, 카페나 블로그 등의 커뮤니티를 이용한 경우 등이 그 대표적인 예인데, 이 경우 도메인 네임 등으로는 차단할 수 없는 상황이 존재한다[9].

이런 경우의 접속을 차단하려면 도메인 중심이 아닌 위협원이 되는 특정 페이지에 대한 차단이 필요하다.

[그림 6]은 위협원이 되는 특정 페이지의 URI를 컨텐츠 필터링 기법을 이용하여 차단하도록 하는 방법에 대해 설명한다.



[그림 6] URI 필터링 정책 설정

위의 그림에서 볼 수 있듯이 도메인 주소 부분을 제외한 URI를 이용하여 해당 페이지로 접속하는 요청을 차단할 수 있다.

5. 결론

해킹이 더 이상 컴퓨터 및 정보 기술의 능숙함을 뽐내는 수단이 아닌, 악의적 정보 수집과 자원 파괴를 위해 사용된 이래 수없이 많은 개인과 집단이 피해를 입었고, 현재도 사용자를 속이려는, 그리고 속지 않으려는 정보의

전쟁은 계속되고 있다.

이에 우리는 최근 더욱 그 기세를 넓히고 있는 다양하고, 빠르게 변화하는 위협들로부터 사용자 정보 및 네트워크를 안전하게 보호하기 위한 다양한 방법에 대해 살펴 보았다.

앞서 살펴본 바와 같이 기존에 적용되던 단편적인 대응 방법으로는 개인 정보의 유출로부터 더 이상 사용자를 보호하기 어려운 것이 현실이다. 이를 위해 본 논문에서 제안한 복합적이고 적극적인 방법을 사용하면 사용자의 정보를 보다 안전하게 보호할 수 있으리라 기대한다.

6. 참고 문헌

[1] Suspicious e-Mails and Identity Theft. Internal Revenue Service. Retrieved on Jul 5, 2006.

[2] Malicious Website / Malicious Code: MySpace XSS QuickTime Worm. Websense Security Labs. Retrieved on Dec 5, 2006.

[3] http://www.internetdefence.net

[4] Stuart Schechter, Rachna Dhamija, Andy Ozment, Ian Fischer (May, 2007). The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. IEEE Symposium on Security and Privacy, May 2007. Retrieved on February 5, 2007.

[5] http://www.kisa.or.kr

[6] Anirudh Ramachandran, Nick Feamster, Understanding the NetworkLevel Behavior of Spammers, SIGCOMM'06, September 1116, 2006, Pisa, Italy.

[7] Cole, William K (2007-01-16). Blacklists, Blocklists, DNSBL's, and survival:. Retrieved on 2007-01-26.

[8] Anirudh Ramachandran, Nick Feamster and David Dagon, Revealing Botnet Membership Using DNSBL Counter-Intelligence

[9] Hampton, Catherine A. (2005). The URIBL Blocklist Family. Blocklists Supported by the SpamBouncer. SpamBouncer. Retrieved on 2007-01-26.