보안 DNS의 데이터를 이용한 동적 감염 클라이언트 격리 기법

고귀한, 노동건
숭실대학교 IT 융합학과

kwihandream@naver.com, dnoh@ssu.ac.kr

Dynamic Infected Client Isolation Scheme Using the Data of Secured DNS

Ko Kwi Han, Noh Dong Kun
Dept. of IT Convergence, Soongsil Univ.

요 약

최근 다양한 DNS 공격이 생겨나고, DNS 공격 피해자가 많아지면서 DNS 보안이 중요해지고 있다. 이로 인해 오픈소스 DNS 진영 및 다양한 보안 기업에서 DNS 를 보안하는 독자적인 기술을 활발히 연구하고 있다. 그러나 보안 DNS 를 사용한다 할지라도, 이미 감염된 특정 사용자(단말)나 혹은 다수의 사용자들을 분별하여 그룹 및 개인에게 세밀한 보안 정책을 세우는 것은 매우 어렵다. 보안 DNS 는 도메인을 IP 로 매핑 시켜주는 단계에서 악성 URL 혹은 IP 의 접근 여부 정도만 블록하는 수준의 기능, 즉 서비스에 대한 접근제어 중심으로 설계되었기 때문이다. 결과적으로 감염된 클라이언트의 DNS 서비스 요청은 제한할 수 있으나, 최종적으로 감염 단말을 내부 격리시키거나, 해커의 외부 C&C 서버 통신을 직접적으로 차단하기 위한 외부 네트워크 차단 등의 조치를 취할 수는 없다. 이러한 격리 및 차단 기능은 대부분 방화벽 등의 네트워크 보안 솔루션에서 수행되는데, 따라서 본 논문에서는 보안 DNS 의 침해 지표 데이터를 네트워크 접근 제어 솔루션 및 차세대방화벽에게 Outbound Rest API 또는 Syslog Notification 형식으로 공유하여, 감염 클라이언트를 동적으로 격리, 차단시키고자 한다. 이를 통해 DNS Tunneling 등 DNS 공격이 막혔을 경우, 다음 우회 공격을 효과적으로 제한할 수 있게 되었으며, 같은 내부 네트워크 사용자의 중복 감염을 더 빠르게 예방할 수 있게 되었다.

Ⅰ. 서 론

인터넷을 사용을 위한 중요 서비스 중 하나는 DNS(Domain Name Service)일 것이다. DNS 가 생겨나면서 우리는 웹 브라우저를 통해 다양한 서비스를 접하게 되었으며, 어려운 IP 주소를 외울 필요가 없어졌다. 뿐만 아니라 DNS 를 통한 로드 분산을 통해 웹 서버의 부하를 줄여주는 역할도 똑똑히 수행하고 있으며, 최근에는 CDN(Content Delivery Network) 서비스와 같은 동영상, 이미지 등의 다양한 콘텐츠를 부하 분산하는 과정에서도 DNS 역할은 굉장히 중요시되고 있다.[1]

오픈소스 DNS 진영에서는 DNS 보안을 위해, 서비스 이상 유무를 수시로 확인하고, 데이터 동기화 검증을 진행하는 다양한 개발을 진행하고 있으며, 뿐만 아니라 다양한 DNS 프로토콜 공격(DNS 증폭 반사 공격, DNS 터널링 공격, DNS 캐시 포이즈닝 등)들로부터 서비스를 보호하기 위한 개발도 지속적으로 진행되고 있다. 또한, 많은 보안 기업에서도 최근 클라우드 환경으로의 전환 및 코로나로 인한 재택 근무 환경 마련, SaaS 형 Application 서비스를 이용하는 환경 등 다양한 환경 및 장소에서 인터넷으로 직접 연결하여 업무를 수행하는 과정 중 사용자를 보호 보안하기 위한 DNS 보안 솔루션을 제시하고 있다.

이러한 보안 DNS 솔루션의 가장 큰 장점은 개인의 PC 혹은 서버에 특별한 Agent 혹은 프로그램 설치 없이 보안 DNS IP 주소 입력 만으로 쉽게 사용자를 보호할 수 있다는 점이다. 또한 무선 환경에서 자주 사용하는 IP 발급 서비스인 DHCP(Dynamic Host Configuration Protocol)를 사용할 경우 IP 뿐만 아니라, DNS 주소를 일괄 적용시켜 줄 수 있으므로, 많은 기업의 직원 단말(노트북, 태블릿 PC)을 보호하기 위한 서비스 전환이 손쉽게 이뤄질 수도 있다. IoT 환경에서도 보안 DNS 가 효과적으로 적용될 수 있는데, IoT 기기는 소형 기기로써 대량으로 곳곳에 분포되어 있기 때문에 특정 프로그램을 설치해야하는 보안은 적용하기 매우 어렵기 때문이다. 따라서 DHCP 서버에 보안 DNS 주소를 입력해 놓으면 IoT 단말의 비정상인 이상 행동 감지를 빠르게 식별하고 차단할 수 있다.[2]

그러나 보안 DNS 를 사용한다 할지라도, 이미 감염된 특정 사용자(단말)나 혹은 다수의 사용자들을 분별하여 그룹 및 개인에게 세밀한 보안 정책을 세우는 것은 매우 어렵다. DNS 는 UDP 프로토콜을 사용하여 단순 쿼리 요청/응답 형태로 서비스를 제공하도록 되어있다. 따라서 대부분의 보안 DNS 솔루션들에서는 도메인을 IP 로 매핑 시켜주는 단계에서 악성 URL/IP 접근을 블록하는 수준의 서비스에 대한 접근 제어 수준에서 구현되어 있고, 결과적으로 감염된 클라이언트의 DNS 서비스 요청은 제한할 수 있으나, 최종적으로 감염 단말을 내부 격리시키거나, 해커의 외부 C&C 서버 통신을 직접적으로 차단하기 위한 외부 네트워크 차단 등의 조치를 취할 수는 없다.[3]

따라서 본 논문에서는 보안 DNS 의 침해 지표 데이터를 대표적인 보안 제품군인 네트워크 접근 제어 솔루션(NAC) 및 차세대방화벽(NGF)에게 Outbound Rest API 또는 Syslog Notification 형식으로 공유하여, 감염

클라이언트를 동적으로 격리시킴으로써, 앞서 언급한 보안 DNS 의 문제점을 개선하고 보안 인프라의 통합 수준을 높일 수 있는 방안을 제시하고자 한다.

Ⅱ. 문제점 분석

2.1 전형적인 멀웨어/APT 감염 과정

인터넷 사용이 가능한 환경에서 전형적인 멀웨어/APT 감염 과정은 다음과 같다. PC 사용자가 악성 사이트에 접속할 경우 웹 사이트가 초기 드로퍼를 전달하고, 설치된 드로퍼는 CnC 서버로 연결을 시도한다. CnC 서버에 통신이 성공하면 악성 페이로드가 다운로드, 실행되며 클라이언트는 랜섬웨어, 봇넷 등 다양한 해커의 공격에 조종당하게 된다.

이 과정에서 위험 웹서버 및 CnC 서버 자체로의 접근은 대부분의 방화벽에서 위험 IP 차단 기능으로 제공하기 때문에 쉽게 막을 수가 있다. 그러나 위험 웹사이트 또는 CnC 서버로 접근하기 전 단계에서도, 즉 DNS 로 웹서버나 CnC 서버의 IP 를 알아내는 과정에서도 2.2 장에서 설명할 DNS Tunneling 과 같은 공격이 발생할 수 있다.

2.2 DNS Tunneling 을 통한 정보 유출

DNS 프로토콜을 사용하여 임의 데이터를 송수신하는 기술을 DNS Tunneling 이라고 한다. 실제로 최근 많은 보안 사고 사례에서, 해커가 DNS Tunneling 을 통해 악성코드 배포, 원격 CnC 통신, 중요 정보 유출 등 다양한 공격 용도로 사용된다고 전해진다. 이는 대부분의 기업에서 DNS 보안에 대한 관심이 낮기 때문이다. 이러한 부분을 이용해 해커들도 네트워크 공격 위주가 아닌 DNS 프로토콜(TCP/UDP53) 위주 공격으로 전환하게 되었다.[4] Local DNS 는 언제든지 외부로 나가서 상위 DNS 서버들을 거쳐, 필요할 경우 타겟 네트워크의 DNS 서버까지 도달하는 Recursive Query 를 수행한다. 따라서, Local DNS 서버 및 상위 DNS 서버들이 신뢰할 만한, 즉 Trusted DNS 서버라 할지라도, 타겟 네트워크까지의 모든 DNS 서버의 신뢰성은 담보할 수 없다. 그럼에도 불구하고, 방화벽은 Trusted Local DNS 가 보낸 Request 이므로 외부로 이를 전달하게 된다. 이를 이용하여, 공격자는 감염된 PC 의 개인 정보 및 데이터를 암호화하여 DNS 요청 패킷에 임베디드 한 후 위협 도메인의 IP 를 찾게 되고, 최종적으로 위협 도메인의 DNS 서버에 도착하게 된다. 공격자는, 삽입된 데이터를 조합하여 원하는 목적을 달성하게 된다.

이처럼 DNS 터널링 공격은 DNS 서버를 대상으로 실행되기 때문에 위협 도메인들에 대한 정보를 항상 최신으로 유지하고, DNS 패킷들을 상시 모니터링하여 위협 도메인에 대한 DNS Request 등의 문제가 발견됐을 경우 즉각적으로 차단하는 것이 중요하다. 이러한 기능을 제공하는 DNS 를 보안 DNS 라고 하는데, 현재 많은 연구자들의 관심 대상이 되고 있다.

2.3 도출된 문제점

네트워크의 방화벽이 매우 잘 갖추어져 있다 하더라도, DNS Tunneling 을 수행하는 감염된 기기가, 어떤 유입 경로(예를 들어 외부 PC 의 반입, 모바일 기기의 이동 등)들을 통해 네트워크 내에 존재할 수 있다. 이 경우, 감염 기기들은 DNS Tunneling 공격을 수행하고자, 위험 도메인 주소를 IP 로 변환하기위해 그에 대한 DNS Reqeust 보낸다. 이 Reqeust 는 내부 Trusted DNS 를 통해, (방화벽을 통과하여) 외부 상위 Trusted DNS 들을 거쳐, 다시 위험 도메인의 DNS 서버까지 보내지게 되므로, 결과적으로 DNS Tunneling 공격이 성공하게 된다. 방화벽은 당연히 내외부 Trusted DNS 서버들을 신뢰하기 때문에, 방화벽 수준에서 이 공격을 차단할 수 없게 된다. 따라서, DNS Tunneling 공격을 차단하기 위해 보안 DNS 서버가 등장하게 된다.

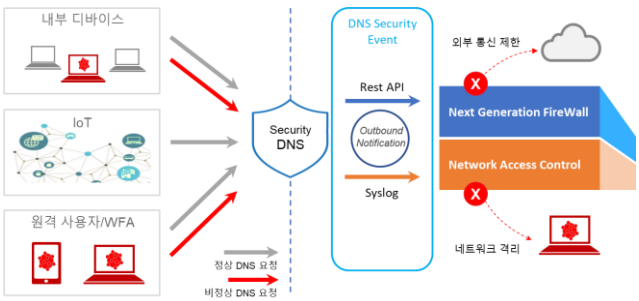
보안 DNS 서버는 DNS 서비스 단계에서 최신 멀웨어 및 C&C 위협 도메인을 식별 후 해당 DNS Reqeust 를 차단한다. 그러나, 보안 DNS 의 역할은 여기까지이고, 감염된 PC 에 대한 추가적인 조치를 취하지는 않는다. DNS 서버의 입장에서는 위협 도메인에 대한 접근만으로 감염이 되었는지 확인할 수 없기 때문이다. 감염된 PC 인지 확인하기 위에 해당 기기를 격리하고 차단하는 것은 방화벽 등의 보안 솔루션의 역할이다. 만약, 보안 솔루션에서 이러한 확인 및 격리 조치를 취하지 않는다면, 공격자는 감염된 PC 를 통해 (보안 DNS 를 통해 막힌) DNS Tunneling 공격이 아닌 다른 우회 공격을 할 수 있을 뿐 아니라, 같은 내부 네트워크 사용자의 중복 감염도 유발하게 된다. 따라서 DNS Tunneling 공격을 막고, 잠재적인 감염 PC 의 격리를 위하여, 보안 DNS 와 (방화벽 등의) 보안 솔루션의 협력적 동작이 필요하다. 이를 위해, 본 연구에서는 보안 DNS 정보를 방화벽 등의 네트워크 보안 솔루션과 공유하여, 보안 솔루션으로 하여금 DNS Tunneling 공격을 수행한 감염 PC 를 동적으로 격리시키는 기법을 제안하려 한다.

Ⅲ. 제안 기법

3.1 보안 DNS 위협 침해 데이터 공유 구조

보안 DNS 에서 유지 관리하는 위협 침해 지표는 대표적으로 랜섬웨어, 멀웨어, 악성 C&C 서버, 위협 피싱 메일 도메인, IoT/OT 공격지 정보 등이 있으며, 지능형 데이터 유출을 위한 악성 DGA(Domain Generation Algorithm) 목록 및 DNS 터널링 공격 위협 침해 데이터를 포함하며, 이러한 데이터를 통해 비정상 DNS 요청을 차단한다.[5]

보안 DNS 에서 차단된 사용자의 정보를 기업 보안 대표 제품군인 네트워크 접근 제어 솔루션(Network Access Control, NAC)와 차세대 방화벽(Next Generation FireWall, NGF)솔루션에게 Outbound Rest API 또는 Syslog Notification 형식으로 공유함으로써, 감염된 사용자의 외부 통신을 제한하고, 네트워크를 격리시킬 수 있다.[6]



<그림 1. DNS Security Event 공유로 인한 사용자 제한>

3.2 Rest API 를 이용한 NGF 와 보안 DNS 의 정보 공유 구현

본 연구에서는 REST API 를 이용하여 3.1 장에서 설명한 위협 침해 데이터를 차세대 방화벽에서 공유하여 위험 기기의 동적 격리를 구현하고 테스트 하였다.
테스트 결과 차세대 방화벽에서 악성 도메인을 질의한 Client IP 가 Rest API 를 통해 동적으로 Deny Group 에 등록되는 과정을 확인하였다. 많은 보안 기업이 자신들의 솔루션을 Rest API 로 원하는 일부 기능을 구현할 수 있도록 제공하고 있기 때문에 이를 이용한 구현이 용이하다.

3.3 Syslog 를 이용한 NAC 솔루션과 보안 DNS 의 정보 공유 구현

API 를 지원하지 않는 환경이라면, Syslog 를 이용하는 것도 좋은 방안이다. Syslog 는 많은 시스템에서 범용적으로 사용하는 표준 메시지 로깅 기술이다. NAC 솔루션에서는 DNS Event Syslog 를 전달받아 감염된 사용자를 Tagging 하여 필터 하는 방식을 사용한다. 필터 된 사용자에게는 정책이 부여 되는데, 네트워크를 온전히 단절시키는 것도 가능하지만, 특정 서비스(DNS, Http, Https 등)만을 제한하는 것도 가능하다.

<그림 2. NAC 에 격리된 감염 Client IP>

그림 2 와 같이, 국내 네트워크 접근 제어 솔루션에서도 위와 동일하게 테스트 결과, 전달받은 Syslog 를 통해 해당 사용자를 자동으로 네트워크 격리함을 확인할 수 있었다.

3.4 DNS 위협 감염 사용자의 동적 격리 및 해제 기능

앞서 설명한 바와 같이 Rest API 나 Syslog 를 이용하여 보안 DNS 정보를 공유한 결과 감염된 Client 의 내부 격리 및 외부 네트워크 통신이 실시간으로 제한됨을 확인할 수 있었다. 또한 NGF 와 NAC 솔루션의 그룹 및 태그 관리 기능을 통해 격리된 사용자들(그룹)을 일괄 정책 해제하여, 쉽게 격리를 해제할 수도 있게 하였다.

Ⅳ. 결론

본 논문에서 보안 DNS 의 위협 침해 지표 데이터를 네트워크 접근 제어 솔루션 및 차세대 방화벽 제품에 Rest API 나 Syslog 로 공유함으로써, 감염된 사용자를 동적으로 제한시키는 감염 클라이언트 격리 기법을 제안하였다. 해당 과정을 통해 DNS 위협 지표를 보안 DNS 뿐 아니라 다른 보안 인프라에 적용함으로써 통합 보안 인프라의 가능성을 제시하였다. 제안 기법을 통해 보안 DNS 에서 개별 사용자 혹은 그룹의 DNS 서비스를 제한하는 것뿐 만 아니라, 감염된 PC 를 내부 격리시키고, 외부의 네트워크를 중단할 수 있게 하였다. 이를 통해 DNS Tunneling 등 DNS 공격이 막혔을 경우, 다음 우회 공격을 효과적으로 제한할 수 있게 되었으며, 같은 내부 네트워크 사용자의 중복 감염을 더 빠르게 예방할 수 있게 되었다. 뿐만 아니라 IoT 나 센서 같은 넓게 분포되어 있는 소형 기기에 대한 위협으로부터 가시성을 높여 줄 수 있게 되었으며, 보안 운영 담당자가 각 솔루션에 정책을 수동으로 적용시키는 수고도 줄게 되었다.

참 고 문 헌

[1] N. H. Go, “Response to SSL communication abuse cases by DNS service providers,” in *Proceedings of the Korean Society of Computer Information Conference*, pp. 107-108, Korea, January 2022.

[2] D. H. Kang and J. D. Lim, “Network Security Protocol Performance Analysis in IoT Environment,” *Journal of the Korea Institute of Information Security & Cryptology*, vol. 32, no. 5, pp. 955-963, Oct. 2022.

[3] G. Zhao, K. Xu, L. Xu and B. Wu, “Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis,” *IEEE Access*, vol. 3, pp. 1132-1142, Jul. 2015.

[4] Sanjay, B. Rajendran, and P. Shetty D, “DNS Amplification & DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches,” in *2020 International Conference on Inventive Computation Technologies (ICICT)*, pp. 230-236, Coimbatore, India, February 2020.

[5] Y. Iuchi, Y. Jin, H. Ichise, K. Iida and Y. Takai, "Detection and Blocking of DGA-based Bot Infected Computers by Monitoring NXDOMAIN Responses," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 82-87, New York, USA, August 2020.

[6] S. M. Hur and Ki. H. Kim, “Sharing Method of Cyber Threat Information Using DNS Protocol,” in *Proceedings of the Korean Information Science Society Conference*, pp. 781-783, Korea, December 2016.