情報保護學會論文誌
第20卷 第6號, 2010. 12

기업 사설 네트워크 우회 접속 분석 및 통제 대책 연구*

이 철 원,† 김 휘 강, 임 종 인‡
고려대학교 정보경영공학전문대학원

A Study on Analysis and Control of Circumvent Connection to the Private Network of Corporation*

Chul-won Lee,† Huy-kang Kim, Jong-in Lim‡
Graduate School of Information Management and Security, Korea University

요 약

기업의 사설 네트워크는 방화벽과 NAT(Network Address Translation)기술을 이용하여 외부 인터넷망으로부터 직접적인 접근이 불가능하다. 그러나 NetCat에서 이용되어지던 Reverse Connection 기술이 SSH Tunnel이나 HTTP Tunnel기술들로 확대됨에 따라 이제는 누구나 손쉽게 방화벽과 NAT로 보호되고 있는 기업의 사설 네트워크에 접근할 수 있게 되었다. 더욱이 이러한 기술은 원격제어서비스, HTTP Tunnel 서비스 등 상업적으로 확대되고 있는데 외부에서 원격으로 기업내 시스템에 접근하지 못하도록하는 기업 내부 규정이나 외부 지침에 위배되는 상황에서 기업내 보안 관리자나 일반 사용자들에게 혼란을 주고 있다. 더욱 심각한 것은 악성코드 또한 이러한 기술을 이용함으로써 기업 사설 네트워크에 침입할 수 있는 은닉 채널을 만들 수 있다는 것이다. 그런데 이러한 인지된 위험을 방화벽등 기존의 보안시스템에서 차단할 수 없다는 것에 문제의 심각성이 있다. 따라서 본 논문은 기업의 내부 네트워크에 대한 우회 접근의 기술적 방법들과 현황을 분석해 보고 위험을 제거하기 위한 통제 대책을 찾아 보고자 한다.

ABSTRACT

A company's private network protected by a firewall and NAT(Network Address Translation) is not accessible directly through an external internet. However, as Reverse Connection technology used by NetCat extends to the technologies such as SSH Tunnel or HTTP Tunnel, now anyone can easily access a private network of corporation protected by a firewall and NAT. Furthermore, while these kinds of technologies are commercially stretching out to various services such as a remote control and HTTP Tunnel, security managers in a company or general users are confused under the circumstances of inner or outer regulation which is not allowed to access to an internal system with a remote control. What is more serious is to make a covert channel invading a company's private network through a malicious code and all that technologies. By the way, what matters is that a given security system such as a firewall cannot shield from these perceived dangers. So, we analyze the indirect access of technological methods and the status quo about a company's internal network and find a solution to get rid of the related dangers.

Keywords: Covert Channel, Malicious Code, Remote Control, Reverse Connection, Private Network, Tunneling

I. 서 론

기업의 사설네트워크는 방화벽이나 IPS 등 많은 보안시스템으로 보호되고 있으며, 이러한 보안 인프라

접수일(2010년 9월 25일), 수정일(2010년 11월 21일), 게재확정일(2010년 11월 29일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT 연구센터 육성·지원사업"의 연구결과로 수행되었음 (NIPA-2010-C1090-1001-0004)
† 주저자, echulwon@gmail.com
‡ 교신저자, jilim@korea.ac.kr

구성은 2000년대 초반에 만들어진 Network Security Architecture[1]에 기반하고 있다. 이러한 아키텍처에서 기업의 사설 네트워크는 외부에서 접근이 불가능하다고 여겨져 왔었다. 그러나 최근 언론에서 보도 되고 있는 "원격 조정 가능한 DDoS 해킹프로그램"[2]이나 국가사이버 안전센터(NCSC)에서 발표한 "상용원격제어 프로그램을 이용한 해킹기법및 대처방안"[3]에서 나타난 위협들이 보안이 허술한 PC방이나 개인들에게만 국한되었다고 보기 어렵다. 2009년에 발생했던 7·7 사이버 대란에서 보듯이 기업내 많은 PC들이 좀비PC역할을 한 것으로 나타났기 때문이다. 이러한 상황은 기업의 사설 네트워크가 더 이상 안전한 네트워크가 아니라는 것을 말하고 있으며, 더욱 심각한 것은 해킹프로그램과 원격제어기술을 결합하면 기업내 PC나 시스템들을 외부에서 원격으로 제어 할 수 있다는 것이다.

기업의 사설네트워크에 대한 접근에 대한 논의과정에서 한 가지 중요한 사실은 외부에서 직접적으로 방화벽과 NAT(Network Address Translation)로 보호되고 있는 사설네트워크에 접근하는 것은 매우 어려운 방법이며, 최근의 기술들은 이러한 직접적인 접근 방법이 아니라 기업내부로부터 Outbound 접속 요청을 받아서 접근하는 우회접근방법을 사용하고 있다는 것이다. 또한 이러한 Outbound 접속 요청이 HTTP 프로토콜이나 SSH 프로토콜을 이용하여 Tunneling을 사용하기 때문에 우회접속을 탐지해내기 어려운 현실이다[4].

따라서, 본 논문에서는 기업의 사설네트워크 접근이 어떻게 이루어지고 있는지, 이러한 접근을 탐지하고 차단하기 위한 연구들이 어디까지 진행되고 있는지를 살펴보고, 기업에서 적용 가능한 통제 대책에 대해서 알아 보고자 한다.

II. 관련 연구

우회접속은 기업 내부로부터 악성코드나 기업내 비인가 어플리케이션이 HTTP 프로토콜을 이용하여 외부 시스템에 Tunnel을 만들어주는 방식이다. 따라서 우회접속이 가능하기 위해서는 Outbound 접속요청을 하는 악성코드를 포함한 기업내 비인가 어플리케이션과 HTTP 프로토콜에 대한 방화벽 허용이 필수적이다.

이러한 우회접속을 가능하게 하는 어플리케이션은 악성코드나 상용프로그램들을 포함하여 무수히 많다. 원격제어를 가능하게 하는 상용프로그램이나 상용서비스는 국내외를 포함하여 새로운 수익모델로 자리잡아가고 있다[5]. 상용서비스는 외부로 노출되어 있어서 보안 관리자가 주의를 기울인다면 충분히 차단할 수 있지만, 문제는 악성코드에 의한 우회접속 채널이다. 악성코드 중 Agent류의 악성코드는 해킹된 홈페이지를 통해서 기업내부로 다운로드 된 뒤 HTTP프로토콜을 이용하여 인터넷에서 추가적으로 악성코드를 다운로드받게 되고 다운로드된 악성코드들 중에는 우회접속이 가능한 해킹툴들도 있다. 이러한 Agent류의 악성코드의 기업내 감염현황을 살펴보면 '10년 7월 한 달간 인터넷 침해대응센터에 신고 된 1609의 악성코드 중 217개가 Agent류의 악성코드로 265개의 Onlie-GameHack류의 악성코드에 이어 2위를 차지하고 있다[6].

악성코드나 기업내 비인가 어플리케이션들에 대한 탐지 방법 연구는 최근까지 지속적으로 이어지고 있다. 이러한 연구는 네트워크 기반에서 동작하는 기술과 PC 기반에서 동작하는 기술로 나뉘어져 연구되어져 왔으며 최근에는 망분리기반에서 동작하는 기술로까지 발전하고 있다. PC기반에서 동작하는 기술 중 가상환경을 이용하여 악성코드를 탐지하는 기술[7]은 기존의 악성코드의 시그니처나 행동기반의 탐지기술들이 갖고 있는 사후 대응적인 문제점이 있으며, 네트워크 기반에서 ActiveX형태로 유입되는 악성코드에 대한 대책에 관한 연구[8]는 최근 악성코드들이 해킹된 웹사이트에 IFrame을 이용하여 숨겨진 뒤 사용자가 웹 접속시 실행파일형태로 유입[9]되고 있는 문제점에 대한 대책으로는 부족한 면이 있다. 또한, 망 분리를 통해서 악성코드를 격리시키는 연구[10]는 최근 가장 활발하게 진행되고 있는 연구 분야로 상품화도 많이 진행되고 있지만 인프라의 변경에 대한 리스크나 비용에 대한 부담이 문제가 되고 있다.

우회 접속에 대한 직접적인 연구를 살펴보면 국내보다는 해외에서 더욱 활발히 진행되고 있다. IDS의 구조적인 취약점을 이용하여 IDS의 자원을 고갈시킴으로써 IDS의 기능을 무력화시키거나 방화벽의 취약점을 이용하는 연구[11]가 국내에서 있었지만, 최근의 Tunneling을 이용한 우회기법에 대한 대책이나 논의는 아직까지 활발하지 않다. 반면에 해외에서는 HTTP Tunneling이나 SSH Tunneling 그리고 비인가 어플리케이션에 대한 탐지기술에 대한 연구가 활발한 편이다[12][13][14]. 기존의 Network anomaly 탐지 시스템들이 패킷의 헤더필드를 가지고 시그니처를 생성하는것에 비해 Payload 기반의 Application의 anomaly

탐지에 대한 연구[14]는 비정상 패턴을 찾아내는 또 다른 방식중의 하나를 제시하고 있으며, P2P트래픽을 탐지해내는 연구는 False Positives 모델과 False Negatives 모델 기반 하에 방화벽을 우회하는 P2P 트래픽에 대한 탐지율을 높이는데 중점을 두고 있다[13]. 그리고 보안 정책을 우회하는데 사용되어지는 HTTP Tunnel내에 숨겨진 blocked 프로토콜을 탐지해내기 위한 통계적 분류기법에 대한 연구는 행동기반하에 Tunnel을 찾아내고자 하는 것으로 IP level에서 수집된 패킷 사이즈, 패킷 순서, 패킷간의 inter-arrival time등의 정보를 이용하여 fingerprint를 만들어 Tunnel을 탐지하고자 한다[4]. 이렇듯 해외에서는 기업의 사설네트워크에 대한 우회기술들에 대한 대책이 활발하게 논의되어지고 있다. 그러나 이러한 논의들도 특정 비인가 어플리케이션에만 국한되거나 HTTP 프로토콜 등 특정 프로토콜에 대한 연구나 특정한 방식에 대한 연구로 한정되어 있어서 보안정책을 우회하는 알려지지 않은 비인가 어플리케이션들의 우회접속을 탐지하고 차단하기에는 한계가 있어 보인다.

III. 기업 사설 네트워크 우회 접속 분석 및 사례 연구

방화벽과 NAT(Network Address Tranlation)환경으로 보호되고 있는 기업의 사설네트워크를 외부에서 직접적으로 접근하는 것은 불가능하다. 왜냐하면 인터넷 구간의 공인 IP에서 사설네트워크의 사설 IP로는 라우팅이 불가능하기 때문이다. 또한 사설네트워크에서 인터넷에 접근하기 위해 사용하는 NAT IP를 알고 있다고 해도 사설 IP와 1대1로 매핑되는 공인 IP가 아니기 때문에 방화벽을 통과하지 못한다. 그러나 Reverse Connection이나 Tunneling, Proxy 등은 외부에서 기업 내부로의 접근을 가능하게 한다.

3.1 기업 사설 네트워크 취약성 분석

사설 네트워크는 RFC 1918과 RFC 4193에 따라 인터넷 주소 체계에서 사설 IP address를 사용하는 네트워크를 말한다. 사설 IP address의 목적은 IPv4의 address의 부족으로 인한 문제점을 해결하기 사용되었지만 Public 인터넷망을 통해서 라우팅 되지 않는 특성으로 인하여 기업의 내부 네트워크를 인터넷망으로부터 숨기는 기능을 하기도 한다.

이러한 사설 네트워크를 Public 인터넷망과 분리하기 위하여 방화벽이 사용되어진다. 또한 NAT(Network Address Translation)는 사설 IP를 Public IP 주소로 변환하여 사설 IP가 인터넷 망과 통신할 수 있게 할 뿐만 아니라 사설 IP를 외부로부터 숨길 수 있도록 한다. 방화벽은 사설 네트워크를 보호하는 기능을 수행함과 동시에 내부 사용자에게 인터넷 접속 서비스를 수행하게 된다. 이를 위해서 방화벽의 ACL(Access Control List) 정책은 Inbound에 대해서는 "All Deny" 정책을 적용하게 되지만 반면에 내부사용자의 인터넷 접속을 위해서 Outbound에 대해서는 "All Allow" 정책을 적용하게 된다.

방화벽은 Network Layer에 해당하는 보안시스템으로 IP와 포트기반으로 보안정책을 적용하게 된다. 방화벽은 패킷의 Payload나 데이터의 내용을 볼 수 없기 때문에 IP나 TCP 헤더 정보만을 인식하고 그에 따라 차단할지 허용할지를 결정한다. 따라서 알려진 블랙리스트 IP나 악성코드에 의해 사용되어지는 서비스 포트에 대한 통제 정책을 제외하고 Outbound 트래픽에 대해서는 차단 하지 못한다. 이러한 방화벽의 단점을 보완하기 위해서 Application Layer에 해당하는 보안시스템들인 IPS나 웹사이트 필터링 시스템 등이 도입되어 운영되어지고 있다. 이러한 시스템들은 패킷의 Payload나 데이터에서 특정한 시그니처를 탐지하고 차단하거나, 악성코드 유입이나 정보 유출 가능성이 있는 URL에 대한 차단 기능을 갖고 있다. 그러나 이러한 시스템들은 블랙리스트 기반하에 동작하는 시스템으로 알려지지 않은 위험에 대해서는 대응하지 못하는 단점이 있고 오탐의 가능성으로 인해 실제 완벽한 차단 기능을 이용하지 못하는 사례가 많다. 따라서 최근의 악성코드나 해킹툴 그리고 원격제어 상용서비스들은 이러한 사설 네트워크 보안인프라의 취약성을 이용하는 측면이 있다. 즉 사용자들의 인터넷 사용을 위해 오픈된 HTTP 프로토콜을 이용하고, Tunnel이나 Payload를 통한 은닉채널을 생성하는 등의 기법을 통해 기존의 보안시스템을 우회하여 Public 인터넷망으로부터 기업 사설 네트워크로의 접속을 가능하게 하고 있다.

3.2 사설 네트워크 우회 기술 분석

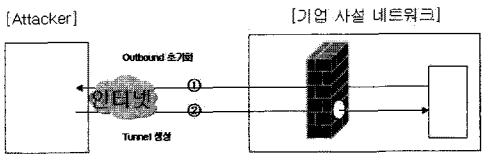
기업의 사설 네트워크를 인터넷과 분리하는 중요한 보안시스템은 방화벽이다. 또한 기업 사설 네트워크를 우회하는 핵심적인 기술도 방화벽을 우회하는 기술이다. 이러한 방화벽을 우회할 수 있는 기반 기술들로 내

부 시스템이 외부시스템으로 하여금 내부 네트워크로 연결할 수 있도록 허용하는 Reverse Connection, 기업 내부 PC와 외부 PC간의 Tunnel을 생성하여 네트워크 보안시스템들이 패킷 내용을 알 수 없게 하는 방법[4], 중간 경유지 서버를 이용하여 최종 목적지 서버로의 접근을 숨기는 Proxy Server 기술, 출발지와 목적지 시스템간의 통신구간을 암호화 하여 은닉채널을 생성하는 방법 등이 있으며, 이러한 방법들은 개별적으로 사용되거나 조합되어 사용되어지고 있다. 따라서 이러한 우회방법들에 사용되어지는 기술들에 대해서 알아보고자 한다.

3.2.1 Reverse Connection 분석

기업의 사설네트워크를 외부에서 접속 할 수 있게 하는 기본 기술중에 하나가 Reverse Connection기술이다. 방화벽과 NAT로 분리된 사설네트워크로의 직접적인 접근이 어렵기 때문에 사설네트워크에서 외부로 우회 채널을 생성시켜 주는 기술이 Reverse Connection이다.

Reverse Connection기술과 관련되어 가장 대표적인 것은 1996년에 발표된 NetCat이라는 네트워크 프로그램이다[15]. NetCat은 TCP/IP protocol suite을 사용하는 TCP와 UDP통신상의 데이터를 읽고 쓸 수 있는 프로그램으로 Shell의 Input과 Output을 리다이렉션하는 Shell Shoveling[16]기법으로 방화벽으로 인해 접근이 불가능한 사설 네트워크에 있는 시스템의 Shell을 획득 할 수 있는 기능을 제공한다. Reverse Connection 기술은 Reverse Telnet이나 Shell Shoveling으로도 불리는데 표준화된 용어는 아니다. 단지 개념적으로는 리모트 시스템의 Shell 명령어의 결과를 리다이렉션을 통하여 획득 한다는 것이다. 이러한 것을 가능하게 하는 프로그램으로 NetCat뿐만 아니라 SSH프로그램을 이용할 수도 있다. SSH프로그램을 사용하면 통신상의 암호화가 가능하다는 장점이 있다. Reverse Connection기술에 중요한 점 한 가지는 공격자가 리모트 시스템의 IP를 알고 있을 필요가 없다는 것이다. 리모트 시스템이 먼저 공격자의 시스템에 접속 시도를 하기 때문이다. 이것은 최근 변화된 해킹흐름과도 연관이 있다. 과거에는 기업내 중요 시스템에 직접 접근하려고 했었지만, 지금은 굳이 보안 체계가 잘 되어 있는 시스템을 타킷으로 삼기 보다는 동일 네트워크에 있는 PC들을 우회해서 접근하는 것이 더 일반화된 방법이 되었다.



[그림 1] Reverse Connection 과정

Reverse Connection을 위해서는 중요한 사전 환경이 필요하다. 첫째, NetCat이나 SSH프로그램등 Reverse Connection을 위한 프로그램이 있어야 한다. 둘째, 방화벽에서 Outbound에 사용되는 해당 포트가 오픈 되어 있어야 한다. 대개 인터넷 사용의 접점에 있는 방화벽 정책은 모든 Inbound에 대해서는 차단되어 있지만 인터넷을 사용하기 위해 필요한 HTTP나 HTTPS에서 사용하는 80이나 443포트는 오픈되어 있기 때문에, Outbound포트로 80이나 443을 이용하면 된다. 셋째, 최초로 Outbound 통신을 초기화 할 수 있는 스크립트나 어플리케이션이 필요하다. 이러한 스크립트나 어플리케이션을 사용자 모르게 기업 내부망에 있는 PC에서 구동시키는 것이 관건이 되는데, 사회공학적 방법으로 이메일의 첨부파일을 이용하거나 SQL Injection과 같은 웹 해킹을 이용하여 웹 사이트에 IFrame과 악성코드 배포 IP를 삽입하고 PC의 보안취약점이 있는 사용자가 해당 웹 사이트를 방문하였을 경우에 초기화 프로그램이 다운로드되어 실행되도록 하는 방법이 사용된다.

[그림 1]은 Reverse Connection과정을 간략화 한 것으로써 기업의 사설 네트워크에 있는 시스템이 NetCat이나 SSH프로그램 등을 이용하여 Outbound 접속을 초기화 한 후에 기업 사설 네트워크로 우회 채널이 생성되는 것을 설명하고 있다. 기업 사설 네트워크로 접속하려는 Attacker는 반드시 그림의 1번 과정을 통해서 기업내부로부터의 우회 접속 요청을 받아야 한다. 이를 위해서 기업내부 사용자들에게 문서파일로 위장한 악성코드가 첨부된 이메일을 발송한다든지 기업내부 사용자들이 신뢰할만한 언론사 홈페이지에 악성코드 배포사이트를 삽입하는 등의 방법을 사용한다. Attacker가 우회 접속을 위해서 배포한 프로그램이 기업내 사용자 PC에 설치되면 해당 악성코드 프로그램은 직원들의 인터넷 사용을 위해 방화벽에서 오픈된 포트를 통해 Attacker에게 우회 접속 채널을 생성시킨다. 그리고 나서 그림의 2번 과정을 통해서 Attacker는 기업내부PC에 설치된 악성코드에 명령어를 전송한다.

3.2.2 Tunneling

우회 접속 기술에서 Tunneling은 Attacker가 Reverse Connection에서 우회채널을 생성하기 위해서 사용하는 명령어나 우회 채널 생성 후 기업 내부 시스템으로 전송하는 명령어의 내용이 기업내부의 보안시스템들에 의해서 탐지 또는 차단되지 않도록 하기 위하여 사용되어진다.

Tunneling은 TCP/IP 네트워크에서 하나의 네트워크 프로토콜이 다른 Payload protocol을 캡슐화하여 전송하는 것을 의미한다. Tunnel을 사용하여 호환되지 않은 네트워크간의 통신이나 비신뢰구간에서의 안전한 통신채널을 만들 수 있다. 이러한 Tunneling에는 SSH, L2TP(Layer 2 Tunneling Protocol), HTTP 프로토콜을 이용하는 방법들이 있다.

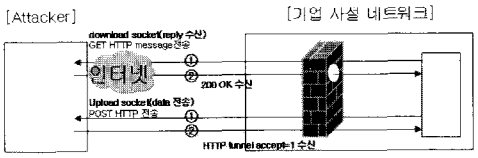
SSH는 두 개의 네트웍 디바이스사이에서 안전한 채널을 사용하여 데이터를 교환하는 네트웍 프로토콜로 OSI 7 Layer의 Application Layer 프로토콜이다. SSH는 사용자 인증을 위해 공개키 암호화를 사용하는데 Tunneling, TCP port 포워딩, 파일전송 등의 기능이 있다. L2TP는 가상사설네트워크(Virtual Private Network)를 지원하기 위한 터널링 프로토콜로 그자체로는 암호화나 기밀성을 제공하지는 않으며 터널내에서 Privacy를 제공하기 위해 별도의 암호화 프로토콜(IPsec)에 의존한다.

L2TP는 OSI 7Layer 모델에서 Data Link Layer 프로토콜처럼 동작하지만 사실은 Session Layer Protocol이다. HTTP(Hypertext Transfer Protocol)은 분산환경 및 공동작업 환경의 하이퍼 미디어 정보시스템들을 위한 네트워크 프로토콜로 World Wide Web을 위한 데이터 통신의 기반이며 요청과 응답(request, response)동작에 기반하여 서비스를 제공한다.

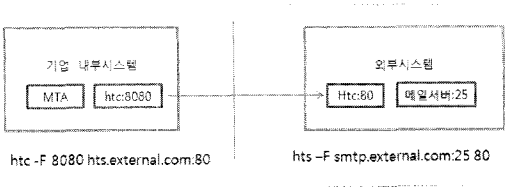
HTTP 메소드중 CONNET, GET, POST메소드를 이용하여 터널링을 구현한 것이 HTTP Tunneling이며 최근에 가장 많이 사용되는 방식으로 다음에서 구체적으로 알아보고자 한다.

3.2.2.1 HTTP Tunnel를 이용한 우회 기법 분석

HTTP Tunnel은 다른 프로토콜에 의해서 생성된 패킷들을 캡슐화하기 위해서 Application level의 Payload를 사용한다. 또한 기업내의 PC에 Tunnel entry point와 외부에 Tunnel exit point가 구성되어져야 한다[13]. 이러한 Tunnel은 HTTP 프로토콜의 CONNECT, GET, POST 메소드를 사용하여 생성된다. HTTP CONNECT 메소드는 Http Proxy접속을 위해 RFC 2817[17]에 정의된 방법인데, CONNECT 메소드는 GET이나 POST메소드가 일반적인 인터넷 트래픽과 구분이 어려운 것과 달리 쉽게 구분이 가능해서 차단이 될 가능성이 있다. 따라서 GET이나 POST 메소드를 이용한 방법이 더 많이 사용된다. 이러한 HTTP Tunnel의 잇점은 인터넷을 사용하는 트래픽과 구분이 힘들기 때문에 보안시스템을 우회하는데 더욱 안전 하다는 것이다. 특히 Payload를 암호화해서 보내게 되면 더욱 구분이 어렵게 한다.



[그림 2] HTTP Tunnel 생성과정



[그림 3] GNU httptunnel 접속 과정

[그림 2]는 GET과 POST 메소드를 이용한 HTTP Tunnel 생성과정을 보여주는데, HTTP Tunnel은 크게 download socket과 upload socket이라는 두가지 채널을 생성한다. download socket에서는 GET 메소드를 이용하여 Attacker의 명령어를 수신하게 되고, upload socket에서는 POST 메소드를 이용하여 명령어의 수행 결과를 Attacker에게 전송하는 역할을 하게 된다.

[그림 3]은 오픈 소스 기반의 HTTP Tunnel 프로그램인 GNU httptunnel의 예를 설명한 것으로 이러한 예를 통해서 HTTP tunnel 과정에 대해서 쉽게 이해할 수 있다. httptunnel패키지는 hts와 htc데몬으로 구성되어 있는데, 기업내부시스템에는 htc 데몬이 주어진 포트로 서비스 요청을 기다리고 기업 외부 시스템에 hts 데몬이 동작한다. 연결이 이루어지면 htc는 hts를 향해서 두 개의 HTTP 세션(GET, POST)을 오픈

한다. hts는 HTTP로 접속이 들어오면 데몬이 수행되면서 정의한 포트로 포워딩하게 된다. 그리고 htc는 서비스 요청을 받아주는 특정포트로 접속요청이 들어오면 hts의 HTTP요청으로 리다이렉션하게 된다.

3.2.3 Proxy Server

Proxy Server 는 우회 접속에서 출발지 IP의 요청을 받아 목적지 IP로 전달하는 중개 기능을 수행할 수 있는데 많은 상용 원격 프로그램들이 이 기술을 사용하여 기업 내부 시스템으로의 접속을 가능하게 하고 있다.

Proxy Server는 클라이언트로부터의 요청에 대해서 중개자로써 동작하는 컴퓨터 시스템이나 응용프로그램을 말하는 것으로, 사용자의 PC에 설치될 수도 있고 사용자와 인터넷상의 목적지 서버들 사이의 다양한 접점에 위치 할 수도 있다. Proxy 서버는 보안적인 측면에서 보면 컨텐츠 필터링, web surfing시 Client IP 숨기기, data 도청 등의 목적으로 사용될 수 있다. Proxy 방식으로는 Socks와 HTTP 방식이 있다.

Socks는 Proxy 서버를 통해 클라이언트와 서버간의 네트워크 패킷을 라우팅 하는데 이용되어지는 인터넷 프로토콜로 OSI 모델의 Layer 5 Session Layer에서 동작한다. Socks 프로토콜이 Session Layer에서 동작하는것과 달리 Http Proxy는 HTTP CONNECT 메소드를 이용하여 Application Layer에서 동작한다. SOCKS Proxy는 UDP 트래픽을 포워드할 수 있으나 HTTP Proxy는 그럴 수 없으며, SOCKS는 Proxy 소프트웨어에게 연결요청을 하기 위하여 Handshake 프로토콜을 사용하지만 HTTP Proxy는 클라이언트가 보내는 HTTP 헤더를 분석하게 되기 때문에 HTTP 트래픽에서만 사용될 수 있다.

최근에는 Socks Proxy가 프로토콜적 특징이나 시그니처를 활용하여 보안시스템을 통해 차단될 수 있기 때문에사용자들이 인터넷 사용시 나타나는 일반적인 HTTP 패턴과 구별하기 어려운 HTTP Proxy 가 많이 사용되어 지고 있다.

3.3 사례 연구

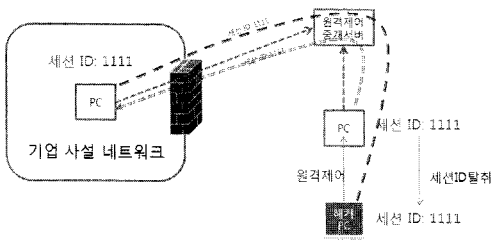
3.3.1 우회 접속 서비스의 상업화

우회 접속 방식을 이용한 상업화된 서비스로 대표적인 것이 원격 제어 서비스이다. 재택근무나 장애지원 서비스를 위해 국내뿐만 아니라 국외에서 만들어진 서비스 및 프로그램을 많이 볼 수 있다. 이러한 원격제어 프로그램이나 서비스는 사용자 편의를 위해서 중계시스템을 제공하고 있으며 이러한 중계시스템을 통해 다른 사람의 도움없이 세션 ID나 패스워드를 가지고 혼자서 내부 PC로 접속할 수 있게 된다. 특히 이러한 시스템은 방화벽을 우회하기 위하여 HTTP 서비스 포트인 80이나 443을 이용한다. 이러한 원격제어 프로그램을 이용하게 되면 기업외부에서 기업내 PC나 서버로 접속이 가능하기 때문에 내부직원에 대한 사고의 위험성이 매우 높다고 할 수 있다. 단 이러한 프로그램을 이용해 기업 내부로의 원격 접속이 가능하기 위해서는 기업 내부 PC가 원격서비스를 제공하는 중개서버와 세션이 맺어져 있어야 한다. 즉 내부 PC의 Outbound 초기화 없이 외부에서 직적접으로 내부로 접근하는 것은 불가능하다.

이러한 원격제어 사례를 살펴보면, 일부 사용자의 경우 회사 PC를 외부의 원격제어 서비스 서버에 로그인 하여 세션을 유지하게 한 후 퇴근을 한다. 회사내 PC에 접속해야 할 상황이 발생하면 집에서 외부의 원격제어 중개 서버에 회사 PC가 접속한 동일한 세션 ID와 패스워드를 가지고 접속한 후 자신의 회사 PC에 접속하여 장애를 처리하거나 업무를 수행하게 된다. 이러한 처리 방법은 상황에 따라서 심각한 위협이 될 수 있다. 기업 외부에 있는 PC들은 기업내부에 있는 PC들에 비해 보안상태가 나쁜 경우가 많다. 가정에서 사용하고 있는 PC들 중에는 사용상 편의를 위해 패스워드 설정 없이 사용하거나 기업에서 강제로 이루어지는 윈도우 보안 패치도 가정의 PC에는 적용되지 않는 경우가 많다. 이러한 PC에는 원격제어 기능이 있는 악성코드나 해킹툴 등이 설치되어 있을 가능성이 높다. 특히 PC방의 PC등은 이러한 위험이 더 높다고 볼 수 있다.

이러한 상황에서 만약 외부의 원격제어용 PC가 악성코드에 감염되어있다면 기업내부에 있는 PC에 접속하기 위해서 외부의 중개서버에 로그인하게 될 때 세션 ID와 패스워드가 유출될 가능성이 높다. 유출된 ID와 패스워드는 기업내 PC와 중개서버와의 세션이 유지되고 있는 동안에는 누구나 기업내 PC에 접근할 수 있는 수단이 된다. 결국 해커에 의해 세션 ID와 패스워드가 유출된다면 기업 내부 시스템은 심각한 위험에 빠지게 된다.

[그림 4]는 원격제어용 세션 ID와 패스워드가 유출될 수 있는 경우와 그로인해 기업 내부 시스템이 위험



〔그림 4〕 내부 사용자의 원격 제어 위험

에 빠질 수 있는 사례를 보여주고 있다.

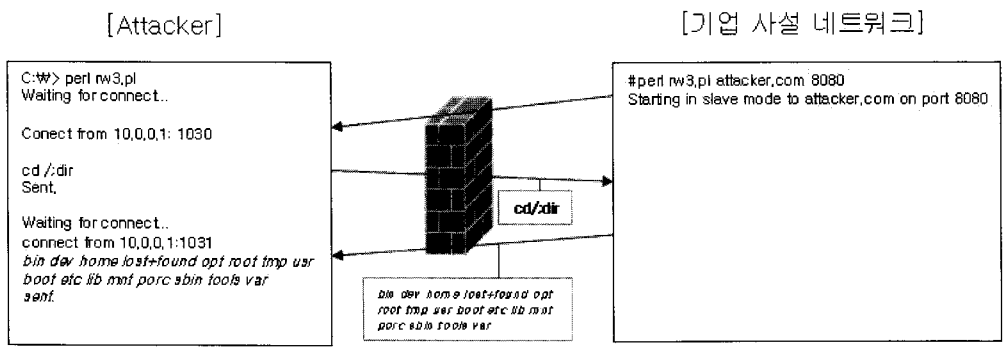
3.3.2 악성코드 및 해킹툴의 우회접속 기술 사용

악성코드가 HTTP Tunnel를 이용하여 기업 내부 네트워에 접근할 수 있는 사례로 Reverse WWW Tunnel Backdoor Malware를 예로 들 수 있다. 이 툴은 HTTP protocol를 통해서 두 시스템의 통신이 이루어지는데 1998년에 최초로 만들어진 스크립트 형태의 툴로, 방화벽을 우회하는 기술이 가능한가를 시험해 보기 위해서 만들어졌다. 이 스크립트는 일반적인 웹 트래픽처럼 보이게 하기 위하여 GET 메소드를 사용한다. 이 스크립트는 자신을 은폐하기 위해서 프로세스 이름을 유닉스에서는 "vi" 윈도우에서는 "Explorer" 또는 "Taskmgr"로 변형한다.

〔그림 5〕는 악성코드의 동작을 설명한 것으로 Attacker는 사회공학적 방법이나 홈페이지 해킹 등을 통해서 우회접속이 가능한 악성코드(rw3.pl)를 기업내 사용자 PC에 설치한다. 인터넷 공간에 있는 Attacker는 동일한 악성코드인 rw3.pl을 자신의 시스템에서 실행시킨다. 악성코드 프로그램명은 동일하지만 기업내 PC에 설치된 악성코드는 Attacker에게 우회 채널을 생성시켜주고 Attacker로부터 명령어를 수신하는 역할을 하게 된다. 반면에 Attacker가 실행시킨 악성코드는 기업내 PC와 우회 채널을 생성 한 후에 명령어를 전달하고 그 결과를 수신하게 된다. 그림에서 기업내 PC가 최초로 Attacker에 접속 요청을 한 후 Attacker는 두 개의 명령어(cd /, dir)를 전송하였고 기업내 PC는 그 결과(bin dev home lost+found opt root tmp usr boot etc lib mnt porc sbin tools var)를 Attacker에게 전송하였다.

IV. 기업 사설 네트워크 우회 접속 차단 방안

지금까지 분석결과를 보면 기업 사설 네트워크의 우회 접속은 크게 2단계로 나누어서 볼 수 있다. 첫 번째 단계는 우회 접속에 사용되는 악성코드나 상용프로그램이 기업내 PC로 유입되는 단계이다. 두 번째 단계는 유입된 악성코드나 상용프로그램이 외부의 Attacker 등에게 우회접속 연결 요청을 시도하는 단계이다. 따라서 기업사설 네트워크 우회 접속 차단 방안에 대해서 크게 두 가지로 나누어서 살펴볼 것이다. 첫 번째 단계에 대한 대책으로는 "ID 인증 기반의 웹사이트 접근통제"를 통해서 기업 내부로 유입되는 우회접속 악성코드나 상용프로그램들을 통제하고, 두 번째 단계에 대한 대책으로는 이미 유입된 우회 접속 악성코드나 상용프로그램들이 외부의 Attacker와 우회채널을 생성하는 것을 차단하기위한 "화이트리스트 기반



〔그림 5〕 Reverse WWW Tunnel Backdoor Malware 동작 예

의 어플리케이션 통제" 방안을 제시한다. 마지막으로 새로운 정책을 기업에서 적용하기 위해서는 기술적인 대책들에 앞서서 보안정책이나 교육적인 문제가 선행되어야하기 때문에 이러한 부분에 대한 대책도 제시할 것이다.

4.1 ID인증 기반의 웹사이트 접근 통제

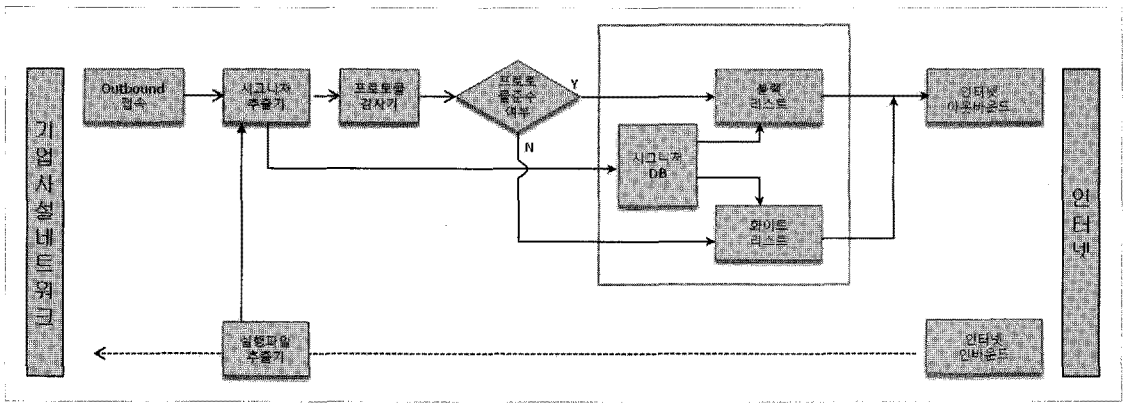
웹 필터링 시스템은 기업에서 음란, 주식, 도박, 게임과 같은 유해한 사이트 차단이나 웹하드나 웹메일 등의 내부 정보 유출 경로가 되는 인터넷 사이트의 URI를 통제하기 위한 시스템으로 운영되고 있다. 이러한 웹 필터링 시스템의 문제는 크게 두 가지로 나누어 볼 수 있는데, 첫째는 정상적인 사이트로 분류된 웹사이트가 해킹되어 악성코드가 유입될 경우에 대한 대책이 없다는 것이다. 앞에서 살펴본 바와 같이 언론사와 같은 인터넷 사이트가 최근 유행하고 있는 SQL Injection을 이용한 해킹 기법 등으로 해킹되어 악성코드 배포 사이트를 포함한 IFrame이 삽입되어도 관리자나 사용자는 인지하기 어렵기 때문에 악성코드 배포 사이트로 많이 이용되어 지고 있다. 둘째는 웹 필터링 시스템이 블랙리스트 기반의 사후 조사에 의해서 유지되는 시스템이고 사람에 의해서 리스트가 관리되어지고 있어서 알려지지 않은 악성 웹사이트에 대해서 선제적인 조치가 어렵다는 것이다.

따라서 현재와 같은 목적지 사이트 ACL 기반 웹 필터링 시스템은 출발지(사용자) 인증 기반으로 변경되어야 한다. 인터넷에 접속할 때 목적지 사이트가 허용된 사이트인지 아닌지를 검증하는 것이 아니라 인터넷에 접속하려는 출발지나 사용자의 접속이 정상적인 접속인지 ID 인증을 통해서 접속을 허용한다. 그리고 이러한 접속 현황은 로깅을 통해서 사용자의 불법적인 인터넷 사용을 모니터링 해서 자발적인 통제를 하도록 유도한다. 현재의 웹 필터링 시스템은 일괄적인 URL 통제 기반을 갖고 있어서 모든 사용자는 동일한 URL 통제 정책을 따르게 된다. 그러나 사용자 개별적으로 URL 통제 정책을 수행하고 블랙리스트 기반이 아니라 화이트리스트 기반으로 바뀌어야 한다.

이러한 방식을 구체화하면, 인터넷을 사용하고자 하는 사용자가 인터넷 브라우저에 URL를 입력하면 웹 필터링 시스템은 사용자 인증 페이지로 리다이렉션 한다. 사용자는 기업내 인증기반을 이용하여 ID로 인증을 수행하면 웹 필터링 시스템은 인터넷에 접속하려는 사용자가 올바른 접속을 시도하는지 검증을 한 후 접속하려는 해당 URL로 접속을 허락 한다. 이러한 개별 인증방식의 URL 접속 방식을 사용하게 되면 악성코드가 사이트에 접속하려고 할 경우에 인증이 실패하기 때문에IFrame으로 숨겨진 악성코드 배포 URL에 대한 접근을 차단할 수 있을 뿐만 아니라, 알려지지 않은 유해 사이트나 Agent류 악성코드가 또 다른 악성코드를 다운로드 하기 위해 접속하는 웹 사이트도 모두 차단되게 된다. 또한 사용자가 반드시 접속해야 하는 모든 웹 사이트에 대한 접속 판단을 사용자에게 맡기는 대신 로깅을 통해 사후 감사를 수행함으로써 사용자에게 자유와 책임을 동시에 부여할 수 있다.

4.2 화이트 리스트 기반의 어플리케이션 통제

외부에서 기업의 방화벽 등 보안시스템을 우회하여 기업 내부로의 접속이 성공하려면 반드시 기업 내부 시스템에서 외부 시스템에 은닉 채널 생성을 위한 Outbound 접속 요청 시도가 있어야 한다. 접속 요청



〔그림 6〕 화이트 리스트 기반의 비정상 어플리케이션 차단 모델

시도를 받은 외부 시스템과 은닉 채널이 형성된 후 외부에서 기업내부 시스템으로 접속 할 수 있다. 결국, Outbound 접속 요청 시도가 없을 경우에는 우회 접속은 이루어 지지 않는다. 지금까지 연구들은 이러한 은닉 채널을 탐지하려는 연구들이었고 알려지지 않은 은닉채널에 대해서는 한계가 있었다. 따라서 은닉채널을 탐지하는 방식 보다는 우회 접속을 차단하기 위해서 Outbound 접속을 시도하는 알려진 정상적인 어플리케이션만을 허용하고 알려지지 않은 비정상 어플리케이션을 네트워크에서 차단하면 될 것이다. HTTP 프로토콜의 User-Agent 등을 분석하여 사용자가 인터넷 브라우저를 통해서 접속하는 정상적인 접속이나 HTTP 프로토콜을 준수하면서 악성코드가 아닌 어플리케이션에 대해서만 인터넷 Outbound 접속 요청 시도를 허용하고 그 외 알려지지 않은 어플리케이션에 대한 Outbound 접속 요청 시도를 차단함으로써 기업 사설 네트워크 우회 접속을 통제 할 수 있다. 이러한 방법을 적용하는데 있어서 중요한 점은 정상 어플리케이션과 비정상 어플리케이션을 구별해 내는 것으로 시그니처 기반과 프로토콜 기반의 방법을 병행하여 효율성을 높일 수 있다.

알려지지 않은 어플리케이션의 프로토콜적 특징과 시그니처을 찾아내기는 지금까지의 연구결과를 보더라도 어려운 일이지만 기업내에서 사용되고 있는 알려진 어플리케이션에 대해서는 프로토콜적 특징과 시그니처를 찾아내는 것은 상대적으로 쉽다. 따라서 Outbound 접속을 시도하는 알려진 어플리케이션의 특징을 추출하여 어플리케이션 시그니처 DB를 만들고 이것을 바탕으로 허용리스트를 만들어서 허용리스트에 있는 어플리케이션에 대해서만 Outbound 접속을 허용하는 화이트리스트 정책을 수립하여 적용할 수 있다.

이와 같은 접근 방법의 필요성은 네트워크 기반에서 Anomaly detection[14]의 정확성 한계와 악성코드에 대한 시그니처 기반의 보안 시스템들의 사후대응적인 탐지 및 제한적인 조건에서의 대응으로는 알려지지 않은 우회접속 위협에 대한 근본적인 해결책이 될 수 없기 때문이다. 또한, 이러한 방법이 적용 가능한 이유 중에 하나는 기업내의 PC의 사용 목적이 업무와 관련 있어야 한다는 기업내 법규 준수 항목에 기반하여 업무적으로 사용하는 어플리케이션들에 대해 일정기간의 모니터링 기간을 거치면 제한적인 어플리케이션 사용 목록을 만들 수 있기 때문이다.

기업내 사용되는 어플리케이션의 정보는 네트워크 기반에서 조사되어질 수도 있겠지만 보조적인 수단으로 PC내 설치 되어 있는 자산관리 프로그램 등을 통해서도 얻어질 수 있다. 이러한 사전 정보를 가지고 기업내 정상 어플리케이션의 시그니처를 수집할 수 있다.

[그림 6]은 알려진 어플리케이션에 대한 시그니처를 기반으로 수립된 화이트 리스트 정책기반 통제 시스템 모델이다. 이 모델은 지금까지 비정상 어플리케이션에 대한 탐지 및 차단에 중점을 두고 시도되어졌던 많은 연구들이 보이고 있는 한계점을 보완할 수 있다. 네트워크에서 알려지지 않은 비정상 어플리케이션을 탐지하는 것은 항상 False negatives나 False positives 문제에 부딪히게 된다. 하지만 기업내에서 인터넷 Outbound 접속을 시도하는 정상적인 어플리케이션이 한정되어 있다면 비정상 어플리케이션을 찾아내기 위한 블랙리스트 기반 정책보다는 정상적인 어플리케이션에 대한 시그니처 관리를 통한 화이트 리스트 기반 정책이 더 효율적일 것이다.

인터넷 Outbound 접속이 필요한 어플리케이션은 관리자에 의해 화이트 리스트에 등록되어져야 하고 등록되지 않은 Outbound 접속은 모두 차단되어진다. 성능적인 문제나 정책 적용 과정에서 가용성 확보를 위해 프로토콜 준수 여부를 검사하는 기능이 추가되어져 있다. 그러나 최근의 악성 코드들 중에는 프로토콜 스펙을 지키는 유형이 나타나고 있기 때문에 상황에 따라서 모든 패킷이 화이트리스트 정책을 통과하도록 할 수 있다. 또한 인터넷을 통해 유입되는 어플리케이션에 대한 시그니처 확보를 위해서 인터넷 인바운드 중 실행파일에 대해서 별도 저장하여 시그니처를 추출할 수 있다.

4.2.1 Outbound 초기화 어플리케이션에 대한 분류 및 식별

네트워크 기반에서 어플리케이션을 구분해내는 방법으로는 사전지식(Priori Knowledge)에 기반한 패킷 헤더 필드, Payload 내용, 네트워크 트래픽의 통계적 특성, 통신 패턴 등의 방법들과 실시간 시그니처 추출 방법 등을 활용할 수 있다[13]. 예를 들어 P2P 어플리케이션중 BitTorrent는 HTTP 프로토콜을 이용하여 방화벽을 우회하는데 'get request'의 URI 파트에 'info_hash', 'peer_id', 'ip', 'port', 'uploaded', 'downloaded', 'left' 그리고 'event' 같은 파라미터들을 포함하고 있으며 이것들이 BitTorrent어플리케이션의 시그니처가 될 수 있다[13]. 또한, 인터넷 인바운드를 통해서 저장된 파일의 Magic Number나 컨텐츠 기반의 파일 타입 분석기법[18]을 활용한 시그니처 생성도

활용할 수 있을 것이다. 실시간 생성된 시그니처는 False Negatives나 False Positives의 가능성이 있기 때문에 허용리스트에 바로 등록하기 보다는 인터넷 인바운드를 통해 저장된 파일에서 생성되는 시그니처와 비교 작업으로 시그니처의 정확성을 높인 후 허용리스트에 등록할 수 있다. 또한 운영초기에는 일정기간 시뮬레이션 모드로 어플리케이션의 시그니처 수집과 정합성을 높이는 작업이 선행되어야 한다.

4.3 우회 접속 차단을 위해 필요한 보안 정책 및 교육

기업에서 우회 접속이 가능한 이유는 앞에서도 살펴본 바와 같이 알려진 악성코드에 대한 패턴기반 차단이나 알려진 유해사이트의 URI차단 등 Outbound 정책이 블랙리스트 기반의 정책이기 때문이다. 방화벽의 HTTP 서비스를 위한 오픈된 정책과 IPS나 웹필터링 시스템의 블랙리스트 정책은 Outbound 접속을 통한 보안 위협에 완전한 대책이 될 수 없음을 알 수 있었다. 블랙리스트 기반으로는 일부 알려진 패턴에 대해서만 대응이 가능하고 알려지지 않은 우회 접속에 대한 선제적인 통제 대책이 되지 못하기 때문이다. 따라서 우회접속을 차단하기 위해서는 현재의 블랙리스트 기반의 보안 정책은 화이트리스트 기반의 보안정책으로 변경 강화되어야 한다.

또한, Outbound 접속에 대한 구체적인 정책이 수립되어 있지 않은 것도 하나의 이유가 된다. 사용자들은 인터넷을 사용하면서 기술적으로 통제 되지 않은 방법들에 대해서는 원칙적으로 허용된 정책으로 판단하게 된다. 어떤 방법이 금지되고 허용되는지 구체적인 가이드라인이 사용자에게 제공 되어져야 한다. 이러한 구체적인 정책 수립을 위해서 기업에서 Outbound 접속과 관련된 위험 분석과 그에 대한 보안 대책의 매핑 작업이 선행되어야 한다. 예를 들면 원격제어 서비스 관련하여 공공기관, 금융회사 그리고 교육기관 등의 웹 서비스의 장애처리를 위한 원격제어 중 사용자 동의를 거쳐야만 가능한 원격제어 등은 허용하되 세션 ID만을 통해서 접속 가능한 원격제어 등은 금지하는 등의 구체적인 가이드라인이 필요하다. 사용자 허용에 의한 원격제어에 대해서도 원격 제어 시 사용자가 알아야하는 사항이나 원격 제어 서비스를 제공하는 기관에 대한 안정성 검증을 위한 세부적인 안전대책이 마련되어야 한다. 따라서 지나치게 PC에 대한 강력한 제어기능이 있는 안정성이 검증되지 않은 기관으로 부터의 원격제어 서비스를 제한하는 정책이 필요하다.

"화이트 리스트 기반의 어플리케이션 통제" 모델은 기업내 사용자들의 인터넷 사용에 불편함을 가져다줄지 모른다. 새로운 어플리케이션 설치 후 해당 어플리케이션이 동작하지 않을 수 있기 때문이다. 그러나 기업의 사설네트워크를 보호하기 위해서는 사용자 편리성을 우선하기보다는 기업의 정보자산 보호를 우선하는 방향으로 보안정책이 변화해야 한다. 이를 위해서 지금까지의 블랙리스트기반의 보안정책보다는 제안하는 모델과 같은 화이트 리스트 기반의 보안정책을 적극적으로 도입할 단계에 도달했다고 볼 수 있다. 기업의 보안정책이 강화되게 되면 사용자들은 일반적으로 자신들에 대한 통제로 여기고 반감을 표시하기 마련이다. 하지만 통제는 기업의 네트워크와 자산을 보호하기 위한 것임을 교육을 통해서 적극적으로 홍보할 필요가 있다. 기업의 정보관리 실태 분석에 따르면 기업들의 정보보호교육에 대한 효과 측정 및 분석절차를 누락하여 정보보호교육이 형식적이거나 일회성의 교육에 그치는 경우가 많은 것 같다[19]. 현재 기업 사설네트워크의 보안 위협상황에 대한 교육 및 화이트리스트 기반의 보안정책 시행 후 나타난 기업내 악성코드 감염현황 및 보안사고 현황에 대한 분석 결과를 적극적으로 교육하고 홍보한다면 사용자의 불만을 없애나가는 방법이 될 것이다.

V. 결론 및 향후 과제

기업의 사설네트워크에 대한 위협은 갈수록 심화되고 있다. 내부 사용자의 편리함 추구나 악의적인 목적으로 외부에 기업의 중요 시스템이 노출될 수 있고, 악성코드는 현재의 기업보안인프라의 구조적 문제점을 이용하여 내부 시스템에 대한 권한을 획득할 수 있는 위협이 있다. 이러한 위협을 제거하기 위한 많은 대책들이 있지만, 이러한 대책들이 알려진 특정한 위협에는 효과가 있을지 모르지만 알려지지 않은 위협들에 대해서는 적절한 대책이 되지 못하고 있다. 따라서,이제는 기업 사설네트워크를 보호하기 위한 새로운 보안 모델을 적용할 필요가 있다고 본다.

본 논문에서 제안한 새로운 보안 모델은 화이트 리스트 기반의 정책들이다. 기존의 보안 시스템들에서 채택한 화이트리스트 기반의 보안 모델이 Inbound에 대한 화이트리스트 정책이었다면 본 논문에서 제안한 모델은 Outbound에 대한 화이트 리스트 정책으로 지금까지 기업에서 시도되지 못한 방식이다. 과거처럼 외부로부터 직접적인 공격이 아닌 내부 시스템으로부

터의 우회 채널이 생성되는 최근의 사례들을 볼 때 기업의 사설네트워크가 이제 안전하다고 볼 수 없기 때문에 Outbound 정책에 대해서도 화이트 리스트 기반의 정책이 필요한 시점이 되었다.

기업 사설네트워크 우회 접속 관련하여 국외에는 비인가 어플리케이션에 대한 탐지나 우회 접속 트래픽에 대한 탐지등 다양한 연구들이 진행되고 있는 것을 알 수 있었다. 그러나 국내에는 아직 이 분야에서 논의나 연구가 미진한 상태인 것 같다. 특히 어플리케이션 시그니처 탐지에 대한 연구는 우회 접속 차단모델에 있어서 중요한 부분으로 앞으로 더 많이 연구되어져야 할 것이다.

참고문헌

[1] Marc S. Sokol, "Security Architecture and Incident Management for E-Business", pp. 9-14 , May. 2000.

[2] 경기경찰청 사이버 수사대, "원격조정 가능한 디도스 해킹프로그램", 2010년 9월(웹검색일), http://www.cbs.co.kr/nocut/Show.asp?IDX=1509157, 2006년 6월.

[3] 국가 사이버 안전센터, "상용 원격제어프로그램을 이용한 해킹기법 및 대처방안", pp. 2-6 , Apr. 2005.

[4] Manuel Crotti, Maurizio Dusi, Francesco Gringoli, and Luca Salgarelli, "Detecting HTTP Tunnels with Statistical Mechanisms", 2007 IEEE International Conference on Communications, pp. 6162-6168 , Jun. 2007.

[5] 전자신문, "토종 SW벤처 알서포트, 日 PC 원격제어시장 점령", Sep. 2010년 9월(웹검색일), http://www.etnews.co.kr/news/detail.html?id=200911190122, 2009년 11월.

[6] 인터넷 침해대응센터, "2010년 07월 인터넷침해사고 동향 및 분석 월보", pp. 5-6 , 2010년 7월.

[7] 서정택, "가상환경을 이용한 악성코드 탐지기술," 정보보호학회지 17(5), pp. 74-82, 2007년 10월.

[8] 박성용, 문종섭, "보안 인증을 통한 ActiveX Control 보안 관리 모델에 관한 연구," 정보보호학회 논문지 19(6), pp. 113-119, 2009년 12월.

[9] 성재모, 노봉남, 안승호, "최근 주요 해킹 피해 동향과 대응 방안," 정보보호학회지 16(1), pp. 80-84, 2006년 2월.

[10] 이은배,김기영, "망 분리기반의 정보보호에 대한 고찰," 정보보호학회지 20(1), pp 39-46, 2010년 2월.

[11] 손태식, 김진원, 박일곤, 문종섭, 박현미, 김상철, "보안솔루션에 대한 우회 공격 기법 연구," 정보보호학회 종합학술발표회 논문집 12(1), pp. 139-143, Jan. 2002.

[12] Yu Wang, Yang Xiang, and Shun-Zheng Yu, "Automatic Application Signature Construction from Unknown Traffic," 24th IEEE International conference on Advanced Information Networking and Applications, pp. 20-23, Apr. 2010.

[13] Zhenbin Guo and Zhengding Qiu, "Identification Peer-to-Peer Traffic for High Speed Networks Using Packet Sampling and Application Signatures," Signal Processing, 2008. ICSP 2008. 9th International Conference on, pp. 2013-2019, Oct. 2008.

[14] Like Zhang and Gregory B. White, "Analysis of Payload Based Application Level Network Anomaly Detection," Proceedings of the 40th Hawaii International Conference on System Sciences-2007, pp. 1-10, Jul. 2007.

[15] Jan Kanclirz, NetCat Power Tools, Syngress, Feb. 2008.

[16] Wikipedia, "Shell Shoveling," 2010년 9월(웹검색일), http://en.wikipedia.org/wiki/Shell_shoveling

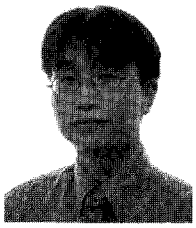
[17] Network Working Group, "Upgrading to TLS Within HTTP/1.1," 2010년 9월(웹검색일), http://www.apps.ietf.org/rfc/rfc2817.html

[18] Mason McDaniel and M.Hossain Heydari, "Content Based File Type Detection Algorithms," Proceedings of the 36th Hawaii International Cnference on System Sciences, vol. 9 pp. 332, Jan. 2003.

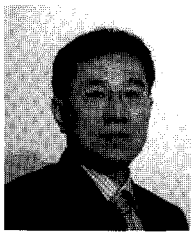
[19] 김지숙, 이수연, 임종인, "민간기업과 공공기관의 정보보호 관리체계 차이 비교," 정보보호학회 논문지 20(2), pp. 117-129, Apr. 2010.

〈著者紹介〉

이 철 원 (Chul-won Lee) 정회원
2000년 2월: 전북대학교 정보통신공학과 졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
현재 국민은행 재직 중
〈관심분야〉 정보보호정책, 기업 보안, 네트워크 보안



김 휘 강 (Huy-kang Kim) 정회원
1998년 2월: KAIST 산업경영학과 졸업
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직



임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보경영공학전문대학원 원장 및 정보보호기술연구원 원장,
금융보안연구원 보안전문기술위원회 위원장,
검찰청 디지털수사자문위원회 위원장,
행정안전부 정책자문위원회 위원,
경찰청 정보통신위원회 자문위원 등
〈관심 분야〉 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등