ETRI

2014
Electronics and
Telecommunications
Trends

사이버공격 역추적기술 동향

Technical Trends of the Cyber Attack Traceback

김정태 (J.T. Kim) 네트워크보안연구실 선임연구원
한민호 (M.H. Han) 네트워크보안연구실 선임연구원
이종훈 (J.H. Lee) 네트워크보안연구실 선임연구원
김종현 (J.H. Kim) 네트워크보안연구실 선임연구원
김익균 (I.K. Kim) 네트워크보안연구실 실장

* This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

본 논문은 인터넷을 통해 급격히 확산되고 있는 해킹, 바이러스 및 DDoS (Distributed Denial-of-Service) 공격과 같은 사이버 보안 공격(Cyber Security Attack) 등이 발생하였을 경우 각 공격에 효과적으로 대비하기 위한 방향 및 그 방법을 제시하기 위해서 실제적인 공격 근원지 정보 역추적을 위하여 관련 추적 기술의 의미, 세부기술 분류, 관련 연구 및 동향 등을 통하여 기존 역추적기술의 제약사항을 극복하고 현재 또는 차세대 인터넷에서 적용가능한 역추적기술에 대한 요구사항 및 향후 전망을 기술하였다.

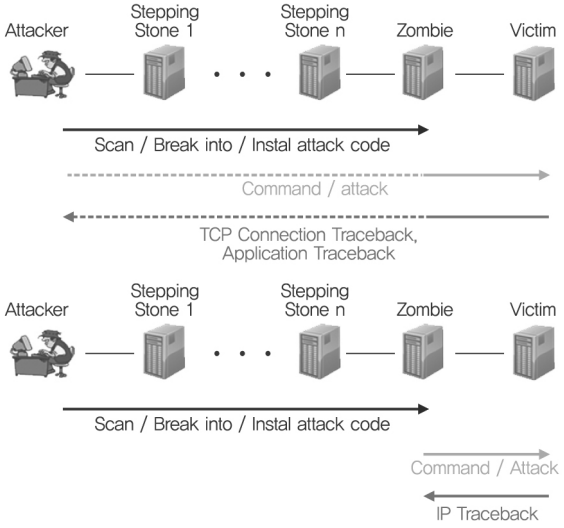
Ⅰ. 서론

사이버 표적공격(Target Attack) 역추적기술은 공격 시스템의 위치와 실제 해킹을 시도하는 해커의 위치가 서로 다르다 하더라도 실제 해커의 위치 즉, 공격의 근원지를 추적할 수 있는 기술을 의미한다. 현재 존재하는 역추적기술에는 모든 시스템에 설치한 역추적모듈을 이용하여 다수의 다른 시스템을 경유한 해커의 실제 위치를 찾아내는 호스트 기반의 연결 역추적방법(Host based TCP Connection Traceback), 네트워크 패킷을 감시할 수 있는 위치에 역추적모듈을 설치하여 다수의 다른 시스템을 경유한 해커의 실제 위치를 찾아내는 역추적방법(IP Packet based Traceback), IP(Internet Protocol)주소가 변경(IP Spoofing)된 패킷의 실제 송신지를 찾아내는 역추적방법 등이 제안되어 있으며, 모두 기본적으로 인터넷 공급자(ISP: Internet Service Provider) 오버헤드를 감수해야 하는 이론적인 단계이다. 또한 해커 유인용 Honeypot 위장 서버 및 해커 자동 추적 탐지 소프트웨어 등이 개발되어있으나 모두 가상망에서의 특정환경에서만 운용이 가능한 기술이다. 최근 인터넷의 거대화와 더불어 기본적으로 ISP 오버헤드 최소화라는 요구사항을 만족시켜줄 수 있는 역추적기술에 대한 연구가 집중되고 있다. 또한 방대한 분량의 실시간 네트워크 트래픽을 포함한 빅데이터(BigData) 및 사회 공학적인 공격에 타깃이 되는 다양한 소셜 어플리케이션(SNS: Social Network Service) 정보와 함께 사용자의 PC 메모리와 OS에 상주하는 프로세스 및 로그정보 분석을 통한 차세대 인터넷에서 적용가능한 역추적기술에 대한 연구가 활발히 진행 중이다.

Ⅱ. 역추적기술 및 분류

1. 역추적기술(Cyber Attack Traceback)

역추적기술은 우선 사이버공격의 유형을 파악함으로써 해당 공격에 따른 추적 대처방법으로 분류할 수 있다. (그림 1)과 같이 사이버공격의 대표적인 유형으로 공격자로부터 단방향 공격만 수행하는 DDoS(Distributed Denial-of-Service) Attack과 양방향으로 통신을 통한 정보 Hacking으로 구분할 수 있다.



(그림 1) Cyber Attack 유형별 역추적방법

먼저 DDoS와 같이 좀비 PC를 통한 특정 공격 수행코드 및 명령을 실행하는 공격인 경우는 IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술인 IP 패킷 역추적(IP Packet Traceback) 혹은 패킷 역추적(Packet Traceback) 추적방법이 사용된다. 또한 해킹을 통한 정보유출 및 추가공격을 위해 우회경로를 통하여 공격이 이루어지는 경우는 우회공격을 시도하는 경우의 해커의 실제 위치를 연결체인(Connection Chain)을 통해서 추적하는 기술인 TCP 연결 역추적(TCP Connection Trace-back or Connection Traceback) 방법이 사용된다[1][2]. TCP(Transmission Control Protocol)연결 역추적기술은 Connection Chain 또는 Trace Across Stepping-Stones[3]이라는 용어로도 사용된다.

이러한 두가지 방법, 즉 IP Traceback, TCP Connection Traceback의 경우 모든 네트워크 트래픽 packet과 통신 connection들을 모니터링해야 하는 오버헤드가 존

재하며 특히 tracing 기능을 제공하지 않는 네트워크장비(라우터) 혹은 ISP를 경유한 경우 더 이상의 추적이 불가능한 단점이 있다. 또한 연결체인을 통한 공격 시 경유지(Intermediate Host)들과 응용 레벨(Application Layer)에서 데이터를 주고 받으므로 네트워크계층에서의 추적을 불가능 하게 한다. 따라서 이를 극복하기 위한 Application based Traceback System, 즉 특정 Application 역추적(e.g., 악성코드, web/mail 및 기타 스크립트) 또는 플러그인 기반 역추적기법이 필요하다.

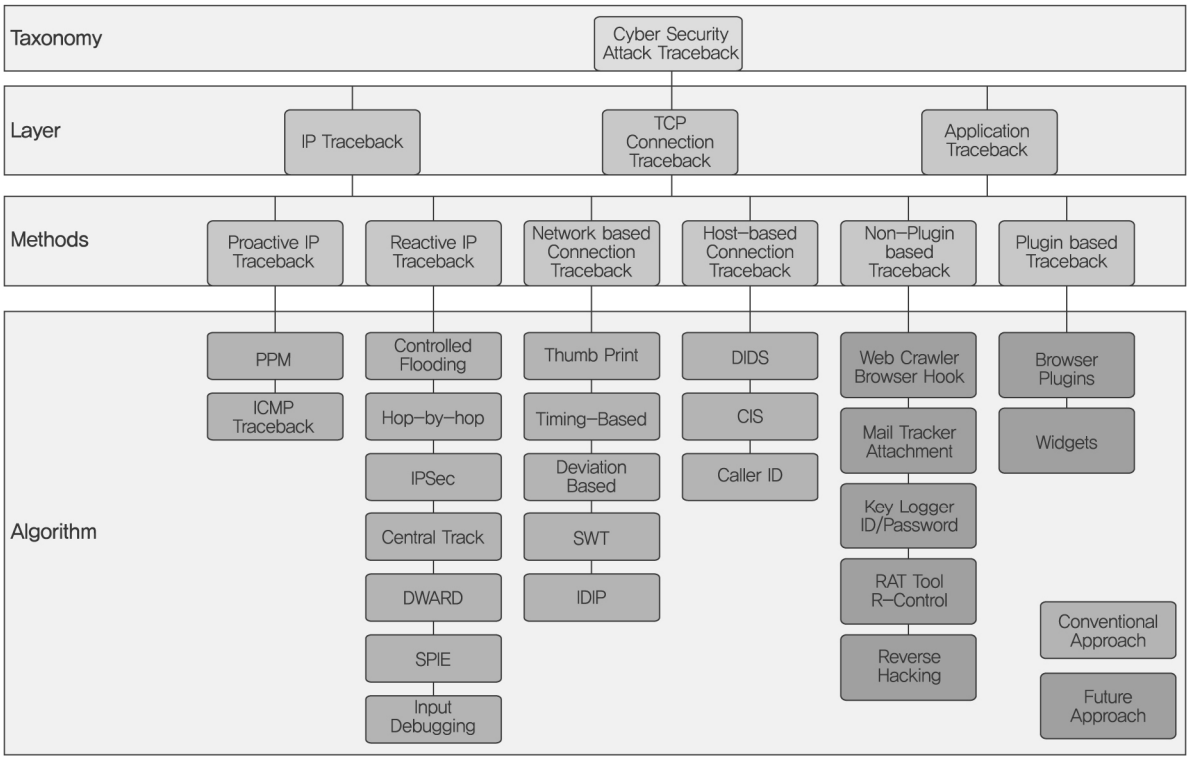
2. 역추적기술 분류(Classification of the Traceback)

기존의 역추적기술은 통신환경과 연결방법에 따라 다양한 알고리즘들이 연구되고 있으며, 연결 방법에 따라 TCP 연결 역추적과 IP 역추적기술로 크게 구분할 수 있다. 첫째로 IP 역추적기술은 비연결지향성 통신방식을 이용하기 때문에 공격을 당한 시스템에 남겨진 로그를 분석하여 그 흔적으로 공격자의 위치를 추적하는 기술로 IP Packet Header 및 Payload 분분의 추적 관련 정보의 삽입을 통한 Proactive 방식과 트래픽 감시 및 필터링을 통한 Reactive 방식으로 분류된다.

둘째로 TCP 연결 역추적은 TCP 통신방식의 특성을 이용하여 연결 지향성 통신방식에서 사용되는 역추적기술이며, 주로 통신을 위한 연결체인의 특성, 즉 네트워크 라우터 장비나 호스트 PC를 기반으로 한 방식으로 분류된다.

마지막으로 Application 역추적기술은 경유지를 포함 공격당한 PC의 OS 및 메모리에 상주하는 Process 및 로그분석을 위하며 단독으로 실행이 가능한 Stand-Alone 방식의 Non-Plugin 기반 추적과 웹 브라우저 및 OS 기능에 포함된 Plugin 기반의 추적방법으로 분류된다.

(그림 2)는 역추적기술의 분류를 해당 추적기술의 동



(그림 2) Cyber Attack 역추적기술 분류

작 layer 및 method에 따라 분류하였다. 특히 기존에 추적을 위한 알고리즘과 현재 지능화된 사이버공격, 메모리/OS/악성코드에 대응하기 위한 응용레벨의 추적방법을 제안하였다.

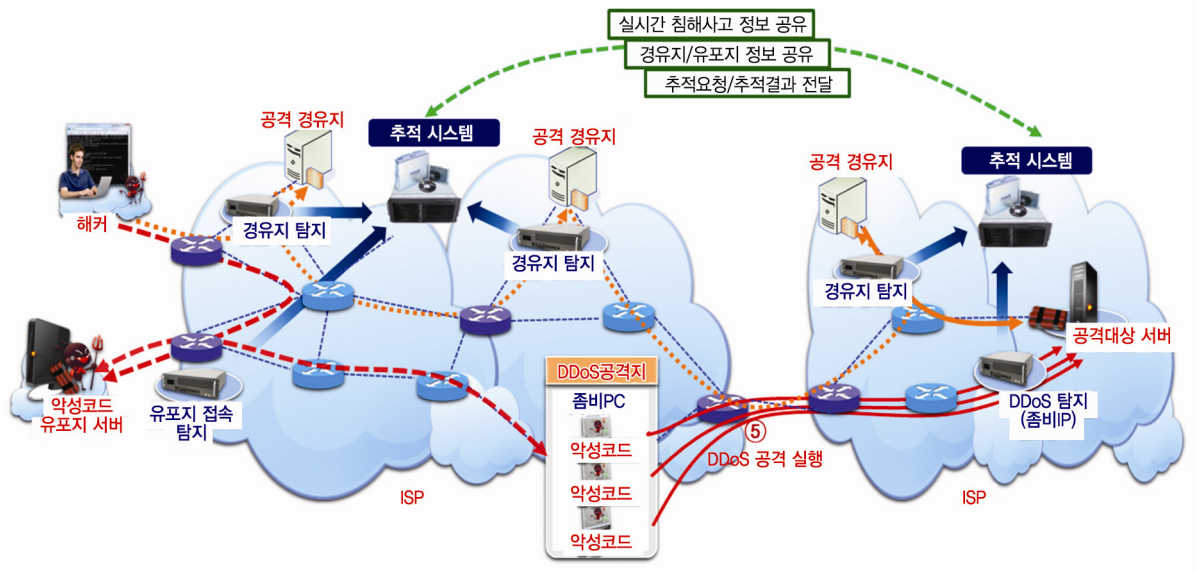
현재 사회 공학적 지능형 사이버공격(APT: Advanced Persistent Threats)의 경우 특정 웹 article 및 e-mail을 이용한 표적공격을 위해서 시스템 또는 어플리케이션의 취약점을 통한 악성코드 첨부 및 악의적인 웹 리다이렉트(redirects) 과정 등을 거쳐 개인 및 회사의 식별정보나 기밀 데이터를 탈취해 가는 만큼 application 레벨에서의 역추적기술에 대한 요구가 급증하고 있는 추세이다.

Ⅲ. 역추적 기술 동향

현재 역추적기술은 Ⅱ장의 역추적기술 및 분류에서 살펴본 바와 같이 사이버공격의 형태에 따라 크게 비연결 지향성 통신 방식인 IP 역추적기술과 TCP 통신 방식의 특성을 이용한 연결 지향성 통신 방식으로 구분된다. 즉, IP 역추적기술은 공격을 당한 시스템에 남겨진 로그를 분석하여 그 흔적으로 공격자의 위치를 추적하는 반면, TCP 연결 역추적기술은 연결체인의 특성을 이용한 기술 위주로 개발 및 관련 제품이 국내외에서 진행 및 생산되고 있다.

먼저 역추적기술의 동향에 앞서 사이버공격(DDoS) 관련 용어들을 (그림 3) DDoS 공격시나리오와 관련하여 설명한다. 먼저 해커는 악의적인 목적으로 해킹을 하는 사람이라는 뜻으로, 컴퓨터 전반, 특히 정보보안에 능통한 전문가를 칭한다. 해커가 생성한 악성코드(malware)는 바이러스를 포함한 다양한 악성 소프트웨어의 일종으로 해커가 웹을 통해서 악성코드 유포지 서버를 통해서 배포한다. 해커는 자신의 IP 주소를 은닉하기 위하여 IP 자체의 보안 취약성을 악용하여 자신의 IP 주소를 숨긴 IP Spoofing 공격을 통해서 경유지를 거쳐 공격대상 서버 혹은 PC를 선택한다.

이러한 다양한 공격 경유지로 사용되는 ISP 네트워크는 여러 대의 라우터, 게이트웨이 스위치 등으로 연결되어 있으며 기존의 추적시스템은 이러한 ISP 네트워크 상 또는 엣지(Edge)에서 관련 데이터 패킷 및 통신채널(connection) 위주로 공격을 탐지하기 위해 동작한다.

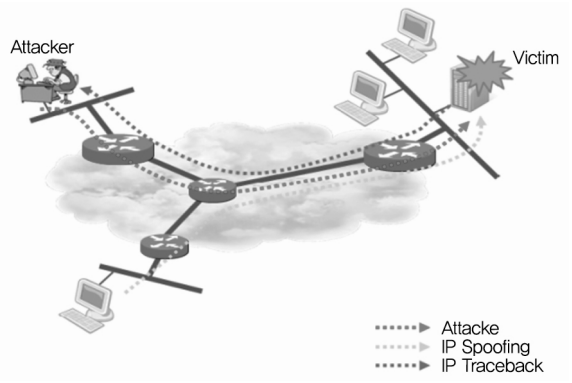


(그림 3) DDoS 공격시나리오

현재 국내에서는 네트워크 기반 악성코드 추적을 위하여 제한적으로 연구가 진행되고 있으며 상용제품으로 출시가 이루어지지 못하고 있는 추세이다. 사이버공격의 추적기술에는 방대한 양의 데이터수집을 위한 기술을 필요로 하고, 다수의 노드들에 기술이 적용되어야 하는 기술적, 환경적 제약이 존재한다. 따라서 네트워크 기반의 추적기술은 현재 제한적으로 연구/개발되고 있으나, 빅데이터 분석과 같은 대용량, 이종데이터 분석을 위한 인프라 제공 시 향후 해당분야의 연구가 활성화 될 것으로 전망된다. 일례로 한국전자통신연구원의 지능형 사이버공격 감시 및 추적시스템(AMTRAC) 기술은 네트워크 트래픽 데이터를 이용하여 공격상황을 탐지하고 공격자의 위치를 고정밀 지도를 통해 시각화하는 기술로 경유지 및 유포지 추적의 한계를 가지고 있다.

1. IP Packet 기반 역추적기술(IP Traceback)

IP Traceback은 1990년도 후반 DDoS 공격이 다수의 발생한 이래 관련 연구가 진행되고 있으며 (그림 4)와 같이 공격자로부터 단방향 공격만 수행하는 DDoS Attack과 같이 좀비 PC를 통한 특정 공격 수행코드 및 명령을 실행하는 공격인 경우는 IP주소가 변경된 패킷(IP Spoofing)의 실제 송신지를 추적하는 기술인 IP 패킷 역추적(IP Packet Traceback) 혹은 패킷 역추적(Packet Traceback) 추적방법이 사용된다.



(그림 4) IP Traceback 개념도

IP 역추적기술은 비연결지향성 통신방식을 이용하기 때문에 공격을 당한 시스템에 남겨진 로그를 분석하여 그 흔적으로 공격자의 위치를 추적하는 기술로 IP Packet Header 및 Payload 분분의 추적 관련 정보의 삽입을 통한 전향적(Proactive)방식과 트래픽 감시 및 필터링을 통한 대응적(Reactive)방식으로 분류된다.

가. 전향적 IP 역추적(Proactive IP Traceback)

전향적(Proactive)방식은 네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로정보를 생성하여 패킷에 삽입하거나 목적지로 전달하여 주기적으로 관리하면서 만일 해킹 공격이 발생하면 이미 생성, 수집된 정보를 이용하여 해킹 공격 근원지를 판별하는 기술이다.

구체적으로 분류하는 패킷에 대한 확률적 마킹(PPM: Probability Packet Marking), 즉 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더에서 변형가능한 필드에 대해서 라우터에 해당하는 주소정보를 마킹하여 다음 라우터로 전달하는 기법과 전통적인 ICMP(Internet Control Message Protocol)메시지를 변형한 iTrace(ICMP Traceback), 즉 확률적 패킷마킹 기법과는 달리 특정 확률로 패킷을 샘플링하여 전 단계 라우터의 정보와 다음 단계 라우터 정보, 패킷의 Payload 정보 등을 포함한 ICMP 역추적(iTrace) 메시지를 생성하여 이를 목적지로 전송하는 기법으로 나눌 수 있다[4].

나. 대응적 IP 역추적(Reactive IP Traceback)

대응적(Reactive) 역추적기술은 해킹공격이 발생하였을 경우 피해 시스템에서 해킹 트래픽 연결에 대한 공격경로를 홉 단계로 추적해 가는 방식이다.

구체적인 기법으로는 첫째로 네트워크 관리자의 지원을 요구하지 않는 링크 검사 역추적으로 많은 양의 트래

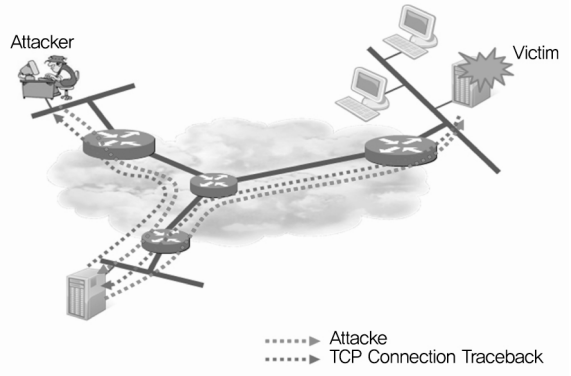
픽을 통해 링크를 폭주시켜서 공격자의 패킷이 어떠한 경로로 관찰되는지를 검사하는 Controlled Flooding 기법이 존재한다.

둘째로 ISP에서 DoS 공격 발생시 Victim PC로부터 가장 인접한 라우터의 진단, 디버깅 및 로깅 기능을 이용하여 Input Link와 Upstream 라우터를 Hop-by-Hop으로 진단하여 ISP상의 Entry Point를 거쳐 네트워크 분석을 통해 공격자의 위치를 추적하는 Hop-by-Hop Tracing 기법[5]이 있다.

셋째로 해킹 공격 발생 시 네트워크상의 라우터와 피해 시스템 간에 IPsec(Internet Protocol Security) 연결이 구성되어 공격자에 의한 공격패킷이 해당 라우터를 통해 전송될 경우 IPsec 터널을 통해 공격자의 경로정보를 피해 시스템에 전달하는 IPsec 기반 역추적기법과 네트워크 안에 TR(Tracking Router)을 도입하여 네트워크를 통하여 지나가는 모든 트래픽에 대한 감시터널을 설정하여 공격자를 추적하는 오버레이 네트워크 기반의 Central Talk 기법이 있다.

넷째로 DDoS 공격을 자동적으로 탐지하고 네트워크상의 DDoS 관련 트래픽플로우의 근원을 차단하기 위한 DWARD(DDoS Network Attack Recognition and Defense) 기법[6]이 있다.

다섯째로 Hash based IP Traceback이라고도 불리며, 전체 네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리하여 침입을 추적하는 SPIE (Source Path Isolation Engine) 기법이 있으며, 마지막으로 input debug 필터를 설치하고 있는 라우터 관리자와 피해 시스템 간의 공격패킷에 대해 상호협력하여 이 공통적인 특성을 갖는 패킷들을 라우터 출력링크에서 분별해내고 이들의 입력 링크를 찾아내 원래의 사이트를 검출하는 Input Debugging 기법 등으로 나눌 수 있다.



(그림 5) TCP Connection Traceback 개념도

2. TCP 연결 기반 역추적기술(TCP Traceback)

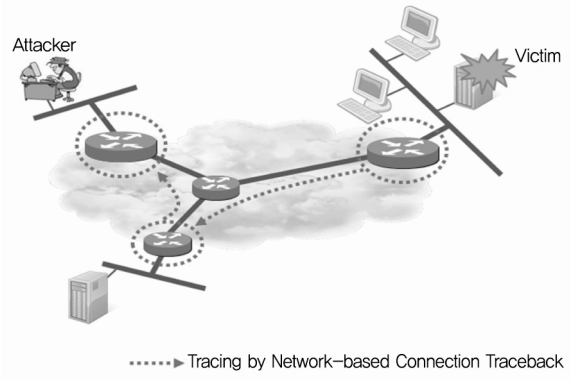
(그림 5)와 같이 양방향 해킹을 통한 정보유출 및 추가 공격을 위해 우회경로를 통하여 공격이 이루어지는 경우는 우회공격을 시도하는 경우의 해커의 실제 위치를 연결체인(Connection Chain)을 통해서 추적하는 기술인 TCP 연결 역추적(TCP Connection Tracebackor Connection Traceback) 방법이 사용된다.

TCP 연결 역추적기술은 TCP 통신방식의 특성을 이용하여 연결 지향성 통신방식에서 사용되는 역추적기술이며, 주로 통신을 위한 연결체인의 특성, 즉 ISP 상에 존재하는 네트워크 라우터 장비(Network-based Connection)나 호스트 PC(Host-based Connection)를 기반으로 한 추적 방식으로 분류된다. 추가적으로 네트워크 커넥션의 추적방법에 따라 Active or Passive 방식[7]으로 나누어진다.

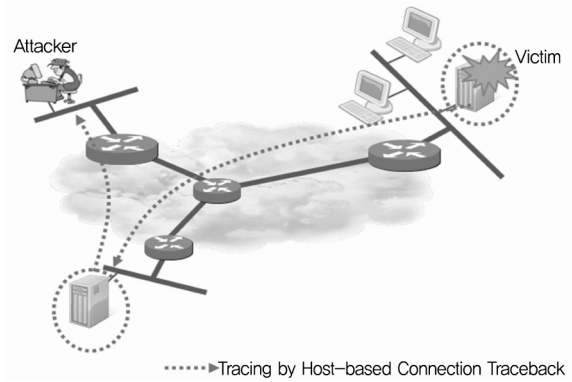
가. Network-based Connection Traceback (Router 기반 추적)

(그림 6)과 같이 네트워크 기반 연결 추적기술은 공격자를 Chain of Connections(예, connections established with telnet, rlogin, or ssh)들을 통해서 추적하는 방식이다.

먼저 네트워크 라우터 장비(Network-based Connection)를 기반으로 하며 네트워크 트래픽 정보를 이용



(그림 6) TCP Connection Traceback-Network Based 개념도



(그림 7) TCP Connection Traceback-Host Based 개념도

하여 다양한 Connections들을 상호분석 및 정리하는 상관관계 분석을 통해 공격자를 추적하는 Thumb Printing[8] 기법, 실시간 통신 Connection 정보 및 내용이 아니라 양방향 트래픽의 특별한 타이밍 특성 분석을 시도한 Timing-based[9] 기법, 2개의 TCP 연결들로부터 생성되는 sequence number들로부터 최소 편차를 사용하는 Deviation-based[10] 역추적, Active Networking[11] 개념과 Watermarking[12] 기법을 이용하여 connection을 추적하는 SWT(Sleepy Watermark Tracing) 및 침입 탐지시스템(IDS)과 필터링 라우터 방화벽 및 호스트 기반 모듈의 상호 작용으로 침입경로를 추적하여 근원지를 차단하는 IDIP(Intrusion Detection and Isolation Protocol)[13] 기술로 분류된다.

나. Host-based Connection Traceback(Host Server 기반 추적)

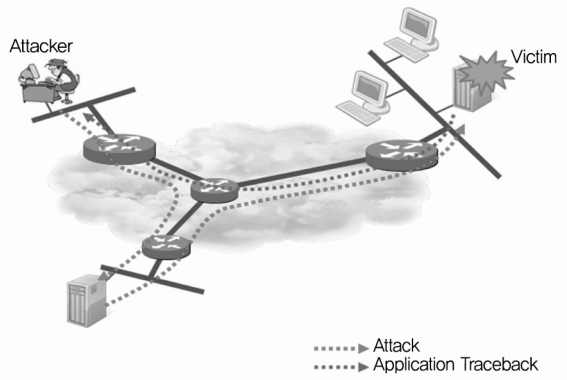
(그림 7)과 같이 호스트 PC(Host-based Connection)를 기반으로 한 추적기술로는 먼저 분산 환경에 적합화된 분산 침입 탐지시스템(DIDS: Distributed Intrusion Detection System) 도메인 내에서 사용자의 Login 및 Connection 경로를 추적하는 DIDS[7], 분산 IDS에서 문제가 되는 중앙집중 관리의 문제를 해결하여 분산 환경에서 각각의 호스트가 사용자의 접속경로(Login Chain) 분석을 시도한 CIS(Caller Identification System)[7]이 있다.

또한 미공군에 의해서 사용된 방법으로 호스트 기반의 active한 방식으로 공격자가 여러 경유지(sequence of stepping-stones)를 거쳐 호스트 PC에 접근 시 비슷한 공격에 대한 정보가 있다는 가정 하에 역해킹을 통해서 공격자가 거친 경유지를 역추적하는 Caller ID(Caller Identification System)[8]로 분류된다.

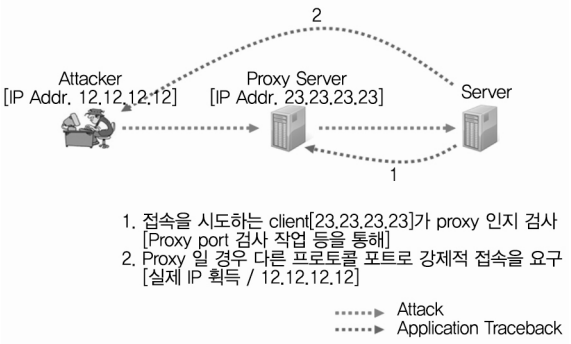
3. Application 기반 역추적기술(Application Traceback)

IP 역추적및 TCP 연결 기반 역추적과 함께 최근 분산 DDoS 및 APT 공격과 같은 고난도 사이버침입에 대한 역추적기술로 application 기반 역추적기술을 통한 대안들이 제시되고 있다. Gartner Forecast가 최근 발표한 'Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats' 자료에 따르면 2013년 한 해 동안 모든 DDoS 공격의 25%가 Application 기반으로 발생할 것으로 추정되고 있다.

즉 Application 기반 공격들은 네트워크 기반의 기존의 방어 시스템을 무력화 하여 주로 공격 대상 응용에 대한 명령어를 전송하여 원격지 호스트의 CPU 및 메모리뿐만 아니라 다른 응용에 대한 치명적인 피해를 입힐 수 있는 보다 정교화된 공격으로 진화되고 있다. 또한 이러한 DDoS 및 APT 공격은 사전에 오랜 기간 동안 치



(그림 8) Application Traceback 개념도



(그림 9) Application Traceback-Inspector 개념도

밀하게 준비되고 사회 공학적 해킹(social engineering hacking)과 같은 방식을 이용하므로 각 사용자의 PC 즉 End-Point에서 Secure Web Browser 및 Hardware와 같은 방어 및 추적시스템 구축이 요구된다.

또한 각 Application 별로 통신절차에 따른 Signing Device와 같이 사용자 응용 Navigation Layer에서 정상적인 패턴과 비교하여 비정상행위에 대한 모니터링이 요구된다. 이러한 사전징후 포착 및 추적에 대한 Application 레벨에서의 시발점을 기준으로 내외부 관련 개체들의 관계를 하위 Network Layer에서 분석하여 위협적인 공격 및 관련 활동에 대한 사전 또는 즉시적 탐지를 통한 추적기술이 요구된다.

(그림 8)은 Application Traceback에 대한 개념도로 공격자가 경유지를 통해서 지능화된 잠복공격을 시도하더라도 피해 호스트 PC에서 방어 및 추적 시스템을 통해서 Application 소켓 통신 기반으로 실시간 근원지 역추적기술을 보여준다. 즉 경유지(Steeping-Stone) 에 상관없이 각 호스트에서 CPU 및 메모리에 존재하는 프로세스 및 로그 정보를 즉시 탐지하여 공격 근원지에 대한 통신 채널을 역추적하는 방식이다.

또한 (그림 9)는 공격자가 익명으로 서버접속을 위해서 Proxy Server(중계서버)를 통해서 Hidden IP로 접속하는 경우 관련 접속 식별코드(사용자가 사이트에 처음 접속 시, 기록되는 고유의 IP를 랜덤코드와 결합하여 클라이언트 PC에 저장되는 코드)를 기반으로 Proxy Port 검사 작업 등을 통해서 다른 프로토콜 포트로 강제적 접속을 요구하여 실제 IP를 획득(inspector)하는 방법을 보여준다[14].

특히 최근 APT 관련하여 익명의 인터넷 사용을 제공하는 토르(Tor) 네트워크(자유 소프트웨어 양파 라우팅)[15]를 기반으로 가상회로와 데이터 암호화 등의 트래픽 분석 공격을 피해 숨겨진 공격행위를 할 수 있는 방식을 Proxy로 사용함으로써 이에 대한 사전대응이 요구된다.

Ⅳ. 역추적기술 요구사항 및 전망

최근 지능형 사이버공격에 대한 대비책으로 현재 이슈화 되고 있는 APT 공격을 포함하여 Application Traceback을 위한 제안 방법은 (그림 2) 역추적기술 분류에서와 같이 실시간 해킹공격을 탐지 및 추적하기 위한 Stand-Alone 타입 Non-Plugin 기반의 역추적방식과 웹 브라우저나 OS 등에 부가적으로 동작하는 Plugin 기반의 역추적방식을 제안한다.

1. Non-Plugin 기반 역추적(Application Traceback)

먼저 Non-Plugin 기반 역추적방식은 사용자 시스템에서 독립적으로 동작하는 애플리케이션으로 Browser

Hooking(후킹: 운영 체제나 응용 소프트웨어 등의 각종 컴퓨터 프로그램에서 소프트웨어 구성 요소에 발생하는 함수 호출, 메시지, 이벤트 등을 중간에서 바꾸거나 가로채는 명령, 방법, 기술이나 행위)을 통한 정보유출 방지를 위한 Web Crawler 방식과 이메일 첨부 파일을 통한 악성코드 유포 방지를 위한 Mail Tracker 방식이 대표적인 지능형 공격의 시작점에서 공격자 역추적이 가능하다.

Web Brower 및 Email에 내포된 악성코드를 사전에 탐지함과 동시에 호스트 PC에 피해가 발생하게 되면 실시간 사용자 PC의 프로세스 및 메모리에 상주하는 악성코드를 분석하여 배포지를 역추적할 수 있다.

또한 악성코드 배포를 통한 해킹 및 정보유출을 탐지/추적하기 위하여 주로 PC 관리자의 ID/Password를 탈취하기 위한 Key Logger 및 원격 접속을 통한 호스트 PC 제어를 위한 다양한 RAT Tool(Remote Administration / Access Tool)에 대한 실시간 탐지를 통한 추적 방식이 요구된다.

마지막으로 역해킹(reverse hacking, hacking back, counte rhacking, active defense) 정당방위 이론을 원용해 해킹공격에 대응해 공격자 및 공격사이트에 대한 정보수집, 공격저지/중단시키는 조치, 원격접속(RAT)의 무력화, 유출된 정보가 스스로 파괴되도록 하는 조치 등의 방법으로 최근 미국 내에서 미국기업이나 공공기관의 중국 해킹에 대한 불만이 높아지면서 정당방위 이론을 역해킹에 도입해 역해킹을 정당화하려는 시도가 보이고 있다. 즉 호스트 기반 TCP Connection 역추적 기술 중 하나인 Caller ID 기술과 같이 호스트 기반의 Active 한 방식으로 공격자가 여러 경유지(Sequence of Stepping-Stones)를 거쳐 호스트 PC에 접근 시 비슷한 공격에 대한 정보가 있다는 가정 하에 역해킹을 통해서 공격자가 거친 경유지를 역으로 추적하는 Application 기반 역추적방식에 대한 요구사항이 증대되고 있는 추세이다.

2. Plugin 기반 역추적(Application Traceback)

Stand-Alone 타입의 Non-Plugin 기반 역추적방식과 함께 실시간 해킹공격을 탐지 및 추적하기 위한 방법으로 웹 브라우저나 OS 등에 부가적으로 동작하는 Plugin 기반의 역추적방식이 요구된다.

현재의 윈도우 OS 상에서 인터넷 익스플로러 웹 브라우저 위에서만 동작하는 싱글 플랫폼, 싱글 웹 브라우저 기반의 플러그인 방식인 ActiveX의 개념을 이용하여 멀티 플랫폼을 위한 전용 애플리케이션 Plugin을 개별 호스트에 설치함으로써 무결성(Integrity)을 제공할 수 있다. 일례로, 미국 에너지 부(DOE: Department of Energy, United States)와 버클리 랩(University of California)은 일부 플래시 및 자바(JRE: Java Runtime Environment) 환경에서 바이러스의 피해를 막기 위해 Qualys tool[16]이란 웹 브라우저용 Plugin 보안 프로젝트[17]를 수행 중에 있다.

또한 웹 브라우저를 통하여 해당 웹사이트 접속 시 사용자 인증을 위한 1회용 패스워드(OTP:One-Time Password)를 제공하기 위하여 개별 호스트에 인증 Plugin을 설치함으로써 세션 컨트롤을 통해 임의의 악성코드 다운로드나 타 사이트로의 접속 유도 등의 위험을 피할 수 있다. 현재 온라인 게임 업체인 한게임에는 U-OTP(유-오티피)란 서비스, 즉 로그인 시 기본적으로 입력하는 아이디와 비밀번호 이외에 휴대폰으로 생성한 일회용 인증번호를 입력해야 로그인이 되는 보안 서비스가 존재한다. 또한 금융권의 경우 계좌 이체 시 사전에 등록된 휴대폰 번호로 일회용 인증번호를 추가로 사용하여 공인인증서 이외에 추가적인 보안을 제공하고 있다.

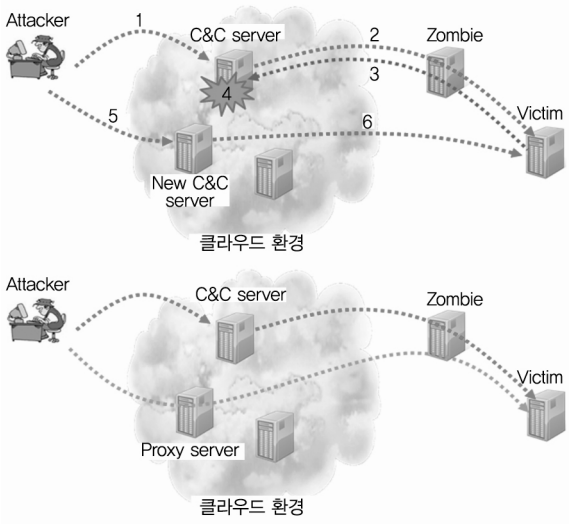
이러한 Plugin 기반의 역추적방식은 해당 사이트나 세션별로 별도의 Plugin을 설치해야 하는 번거로움이 존재하지만 백그라운드에서 사용자 행위에 대한 실시간 보안 추적 및 검사 기능과 함께 업데이트 기능도 제공하므로 Non-Plugin 기반 역추적방식에 비해 light-weight한 기능을 제공한다.

V. 결론

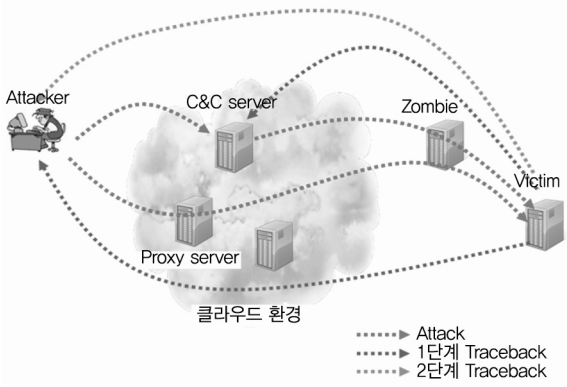
APT 공격은 표적공격이 발전한 것으로 특정 대상이 목적이 아니라 좀 더 구체적으로 특정 데이터 유출 및 특정 피해를 목적으로 하기 때문에 DDoS/DoS 공격이라기보다는 해킹 공격에 유사하다고 볼 수 있다.

이러한 해킹 공격에 대해 과거에는 C&C(Control and Command) 서버의 IP 주소를 차단하면 문제가 해결되었으나, 지금은 정확한 위치를 추적하기 힘든 아마존 웹 서비스(AWS: Amazon Web Service) 혹은 구글앱스 등의 클라우드 환경에 Proxy Server 혹은 C&C 서버를 설치하고, 이를 통해 Zombie PC를 제어하는 방식으로 진화하고 있다.

(그림 10)은 현재 그리고 향후의 공격경로 및 클라우드환경에 설치된 C&C 서버 혹은 Proxy Server가 탐지 및 차단되었을때 재설치하는 예를 나타내는 그림이다. 보안관리자가 해킹공격을 탐지하여 클라우드 환경에 설치된 C&C 서버 혹은 Proxy Server를 차단하여도 쉽게 서버를 재구축할 수 있다는 점도 문제가 되고 있다. 따라서 이제는 해킹을 시도하는 C&C 서버의 IP 차단이 아니라 클라우드환경에 존재하는 C&C 서버 추적 및 Proxy Server를 경유하는 공격에 대한 Attacker를 추적



(그림 10) 현재 및 향후 공격 환경 및 시나리오



(그림 11) 향후 요구되는 추적기술의 단계적 시나리오

하는 기술, 그리고 더 나아가 클라우드환경에 존재하는 C&C 서버를 경유한 공격에 대해 Attacker 를 추적하는 기술이 요구된다.

특히 APT 공격에 대해 (그림 11)은 향후 요구되는 추적기술의 단계적 시나리오를 보여주는 그림이다. 기존 TCP Connection Traceback 기술은 앞서 말한 추적 기능을 제공하지 않는 네트워크 장비 및 ISP를 경유할 경우 더 이상의 추적이 불가능한 단점이 있으므로, 향후 Application Traceback 기술의 보완을 통해 네트워크의 도움없이 직접 C&C 서버 및 공격자를 찾는 추적기술이 요구될 것이다.

용어해설

APT (Advanced Persitsent Threat) 사이버공격의 일종으로특정 단체나 대상을 공격하기 위하여 인터넷 기반으로 다양한 보안 취약점을 이용하여 장기간에 사회공학적 기법을 통한 개인정보나 기업 기밀정보를 탈취하는 행위

C&C (Control and Command) 해커가 악성프로그램을 전송하여 원격에서 명령을 내려 악성행위를 수행하는 매개체 PC

DDoS (Distributed Denial-of-Service) 여러 대의 공격자를 분산적으로 배치해 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

RAT (Remote Access Tool) 원격접속 및 제어툴로 보안이 취약한 상대방 컴퓨터를 해킹을 통해서 원격지에서 해당 PC의 관리자 권한을 취득하여 제어할 수 있는 공격 기법

SPIE (Source Path Isolation Engine) 대응적 IP 기반 역추적기술 중 하나로 전체 네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리하여 침입을 추적하는 기법

약어 정리

APT	Advanced Persistent Threats
AWS	Amazon Web Service
C&C	Control and Command
CIS	Caller Identification System
DDOS	Distributed Denial-of-Service
DIDS	Distributed Intrusion Detection System
DOE	Department of Energy, United States
DWARD	DDoS Network Attack Recognition and Defense
ICMP	Internet Control Message Protocol
IDIP	Intrusion Detection and Isolation Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
JRE	Java Runtime Environment
OTP	One-Time Password
PPM	Probability Packet Marking
RAT	Remote Access Tool
SNS	Social Network Service
SPIE	Source Path Isolation Engine
SWT	Sleepy Watermark Tracing
TCP	Transmission Control Protocol
TR	Tracking Router

참고문헌

[1] 이재광, "역추적기술 동향," 전자정보센터, 2005. 1.

[2] 한국기술거래소, "네트워크 침입자 역추적기술 동향," 전자정보센터, 2004. 10.

[3] P. Ning, "Network Security lecture Note,"Department of Computer Science, North Carolina State University, 2003.

[4] 한국전자통신연구원 부설연구소, "사이버공격 근원지 역추적기술," Monthly 사이버 시큐리티, 국가사이버안전센터

[5] A. A. Aly, "Tracking and Tracing Spoofed IP Packets to Their Sources," College of Information Technology, U.A.E. University.

[6] J. Mirkovic, "D-WARD: DDoS Network Attack Recognition and Defense (DARPA contract N66001-01-1-8937)," Ph.D. Dissertation, Computer Science Department at UCLA.

[7] P. Ning, "A Little Background On Trace Back," Network Security Lecture Note, Department of Computer Science, North Carolina State University 2003.

[8] S. Staniford-Chen and L. T. Heberlein. "Holding Intruders Accountable on the Internet," *Proc. IEEE Symposium Security Privacy,* May 1995.

[9] Y. Zhang and V. Paxson. "Detecting Stepping Stones," *Proc. 9th USENIX Security Symposium,* 2000.

[10] K. Yoda and H. Etoh. "Finding a Connection Chain for Tracing Intruders," *Proc. 6th European Symposium on Research Comput. Security(LNCS 1985),* Toulouse, France, Oct. 2000.

[11] R. H. Campbell et al., "Dynamic Interoperable Security Architecture for Active Networks," *Proc. IEEE OPENARCH 2000,* Mar. 2000.

[12] N. Johnson, Z. Duric, and S. Jajodia. "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures," Kluwer Academic Publishers, Feb. 2001.

[13] J. Rowe, "Intrusion Detection and Isolation Protocol: Automated Response to attacks," Second International Workshop on the Recent Advances in Intrusion Detection, 1999.

[14] 유동훈, "출원특허: 10-2005-0020368웹 접속자 위치 추적 시스템 및 그 추적 방법," ㈜ 아니넷캅, 2005.

[15] Anonymity Online, "Tor Network" https://www.torproject.org/

[16] Qualys Browser Check, "Browser Check FAQ", Qualys Inc. https://browsercheck.qualys.com/

[17] Web Browser Plugin Security, U.S. Department of Energy National Laboratory Operated by the University of California https://commons.lbl.gov/display/cpp/Web+ Browser+ Plugin+ Security