사이버 감시/정찰 시스템 설계 및 제작 연구

염성규*, 윤호상**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail : dae02159@naver.com

A Study on the Design and Fabrication of Cyber Watchdog Systems

Seong-Kyu Yeom*, Hosang Yoon**, Dongkyoo Shin*, Dongll Shin*
*Dept. of Computer Engineering, Sejong University
**Agency for Defense Development

요 약

최근 ICT 기술이 발달함에 따라 전쟁의 양상이 물리적에서 사이버전으로 이동되고 있으며 이미 사이버 공간은 제 5 의 전장으로 불리운다. 또한 오랜 기간 동안 단계적으로 준비 과정을 거쳐 공격하는 APT 사례가 증가함에 따라 공격 징후를 사전에 탐지해 선제 대응하는 사이버 킬 체인이라는 방안이 각광받고 있다. 이러한 사이버 킬 체인 중 가장 기초가 되는 감시/정찰을 수행하기 위한 방안을 연구하면서 적의 영역에 침투했다는 가정하에서 정보를 수집하는 프로그램을 설계 및 제작해 보았다.

1. 서론

최근 ICT 기술이 발달함에 따라 물리적인 전쟁 양상에서 눈에 보이지 않는 사이버 전쟁으로 전장의 양상이 변화되고 있다[1]. 특히 모든 전력 요소들이 유기적인 연결을 통하여 통합 작전 체계를 구성하는 네트워크 중심전(NCW: Network-Centric-Warfare)으로 작전 수행이 변화하고 있다. 즉 파괴 중심에서 전쟁의 수행 체계를 마비시키는 전쟁으로 발전되고 있다[2].

오랜 기간 동안 단계적인 준비 과정을 거쳐 공격을 준비하고 감행하는 이른바 지능형지속가능위협(APT) 사례가 증가함에 따라, 공격 징후를 사전에 탐지해 선제 대응하는 사이버 킬 체인을 기반으로 한 방어 전력이 각광받고 있다[3].

사이버 킬 체인이란 적의 사이버 공격을 사전에 탐지해 공격이 이루어지기 전, 공격을 위한 일련의 진행 단계들 중에 하나를 제거하여 공격을 할 수 없도록 하는 방안이다[4].

이러한 사이버 킬 체인 전략에서 가장 중요한 것은 정보(Intelligence)이며 이를 유용한 자원으로 활용하기 위해서는 적의 네트워크, 호스트 등에 대한 정보를 수집하거나 아군의 네트워크에 대한 위협 징후를 사전에 판단하여. 아군에게 빠른 시간 내에 해당 정보를 제공하여야 한다[4].

또한 사이버 공간은 정보의 수집 및 분석이 제한되는 외부 영역과 아군의 정보 환경 영역인 내부 영역으로 크게 분류되는데[4] 본 논문에서는 사회공학 기법을 통해 먼저 적의 영역에 침투했다는 가정하에서 적을 감시 및 정찰하는 방안에 대해서 연구하며 적의 정보를 수집하는 시스템을 제안한다.

본 논문의 구성은 2 장에서는 실제 악성코드를 분석한 내용을 보고 수집할 항목을 정리한다. 그리고 3 장에서는 프로그램에 대한 설계를 하고 제 4 장에서 구현된 시스템을 설명 한 뒤에 5 장에서는 결론 및 향후 과제에 대해서 정리한다.

2. 관련연구

먼저 정보를 수집하기 위하여 수집할 항목을 정리할 필요가 있다. 수집할 항목은 악성코드를 분석한 보고서를 바탕으로 정리하였다. 아래 표 1 은 악성코드 별로 수집한 항목을 정리한 내용이다[5].

악성코드	수집 항목
3.20 사이버 테러	사용자 이름, 서비스명, 사용중인 모듈, 현재 시간, 운영체제 정보, 레지스트리 정보
6.25 사이버 테러	파일 시그니처, 컴퓨터 시간, 서비스 레지스트리,특정 확장자 파일, 사용자 계정 정보
한글 문서 취약점	시스템 정보, 디스크드라이브목록, 드라이브 유형 정보, 컴퓨터

	이름, 사용자 이름, 컴퓨터 시간, 시스템 버전, 운영체제 플랫폼, 운영체제 버전, 윈도우 서비스 팩 정보, 키로거
Kimsukey APT	시스템 정보, 사용자 정보, 키로깅 정보, 방화벽 정보
IceForg APT	호스트 이름, 프록시, 사용자 이름, 시스템 디렉토리 위치. OS 언어, 시스템 버전
라이브리	BITS 서비스 상태, 백신의 설치 경로,mac 주소 운영체제 정보, 익스플로러 정보

<표 1> 악성코드 별 수집하는 항목

위의 정리한 항목을 바탕으로 적의 컴퓨터에서 수집할 항목을 정리하였다. 아래 표 2 는 제안한 시스템에서 수집할 항목을 정리하여 놓은 목록이다.

분류	수집 항목
system	Host 이름 OS 이름 OS 버전 OS 구성 OS 빌드 등록된 소유자 설치 날짜 시스템 부팅 시간 실행 중인 프로세스 정보 BIOS 버전 시스템 디렉토리 시스템 언어 입력 언어 시스템 시간 메모리 정보 페이지 파일 위치 소속 도메인 핫 픽스 내역 연결 장치 정보 그래픽카드 정보 드라이브 목록 별 파일 시스템 사용중인 DLL 환경 변수
network	랜카드 이름 랜카드 제조업체 맥 주소 DNS 캐시 정보 할당된 IP 라우팅 테이블 목록 프로세스 별 사용 중인 포트 서브넷마스크 게이트웨이 주소 DHCP 사용 여부 NetBIOS 사용여부 어뎁터 종류 네트워크 드라이버 Winsock 정보 공인 IP
기타	각종 로그파일 네트워크 망 구성 정보 네트워크 방화벽 유무

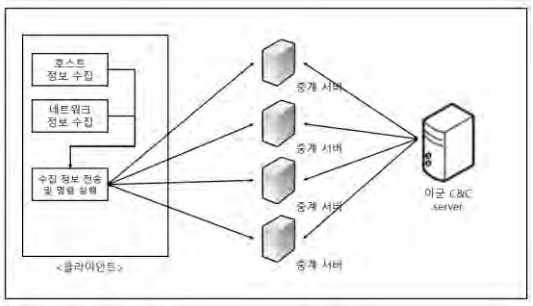
<표 2> 제안 시스템에서 수집할 항목

3. 시스템 설계

전체적인 시스템은 적의 정보를 수집하는 클라이언트와 수집된 정보를 저장하고 보여주는 서버로 구성되어 있다.

클라이언트의 구성요소는 하드웨어 정보, 사용 중인 프로세스, 환경 변수 등 적의 호스트 정보를 수집하는 모듈, 침투한 적의 네트워크의 환경을 수집하고 전체 네트워크에 대한 구조를 분석 하는 모듈, 읽어들인 정보를 암호화 하여 서버로 전달 할 수 있는 모듈로 크게 3 개로 분리된다.

서버의 구성요소는 수집된 정보를 데이터베이스 서버에 저장하고 명령을 내리는 C&C 서버와 적의 수집된 정보와 아군의 명령을 전달하는 등 C&C 서버와 클라이언트를 이어주는 중계 서버 들로 구성된다. 전체 프로세스는 아래 그림 1 과 같다.



(그림 1) 전체 시스템 구상도

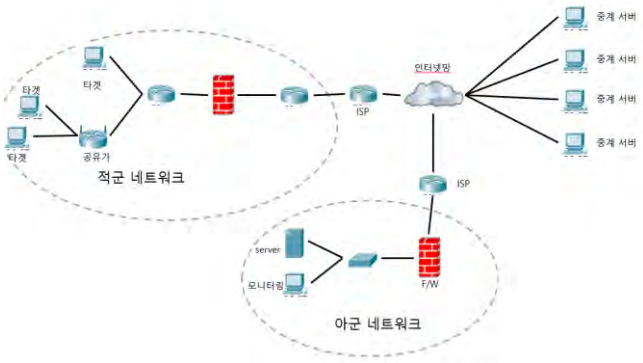
클라이언트의 구성요소 중 호스트의 정보를 수집하는 모듈은 주기적으로 하드웨어 정보, OS 설정 환경 ip 정보 등을 수집한다. 이전에 수집된 내용이 있을 시 최신 내용으로 덮어쓴다. 중계 서버와 통신이 가능할 시에 수집된 내용을 전송하고 흔적을 지운다. 만약 중계 서버와 통신이 불가하다고 판단될 시에 전송을 하지 않고 연결이 될 때까지 기다렸다가 전송을 한다. 네트워크 정보를 수집하는 모듈은 중계 서버와 통신이 가능할 시에는 내부에서부터 인터넷 망까지의 패킷의 라우팅 정보를 추적한다. 인터넷 망으로 나가기 전까지의 이동되는 라우터의 ip 정보를 모아 연결되어 있는 모든 호스트 들의 ip 와 열려 있는 포트 번호를 수집하여 네트워크의 구조를 파악하고 중계 서버에 전달을 한다. 수집을 할 시에는 중간에 방화벽을 거칠 수 있도록 패킷을 조각 내어서 보낸다. 또한 침입탐지시스템에 기록이 남는 것을 최소화 하기 위하여 3-way Handshaking 이 이루어 지기 전에 연결을

끊는다. 수집된 정보 전송 및 명령 실행 모듈은 수집된 내용을 암호화 하여 여러 개의 중계 서버 중 한 군데에 랜덤으로 전송을 한다. 또한 전달 받은 명령을 실행하여 응답을 돌려준다.

서버의 구성요소 중 중계 서버는 아군의 C&C 서버와 적의 시스템에 들어 있는 클라이언트를 연결해 주는 역할을 하며 중계 서버를 여러 개를 둔 이유는 특정 ip 로 많은 접속을 하면 적의 네트워크 관리자가 의심을 할 수 있기 때문에 의심을 최소화하기 위함이다. 아군의 C&C 서버는 수집된 정보를 웹 페이지를 통해서 볼 수 있으며 클라이언트로 명령을 내리고 응답을 받을 수 있도록 하였다.

4. 시스템 구현 및 실험

본 장에서는 3 장에서 제안한 시스템 설계를 통하여 구현을 하고 가상의 네트워크 망을 구성하여 실험을 하였다. 실험 네트워크의 구성은 아래 그림 2 와 같다



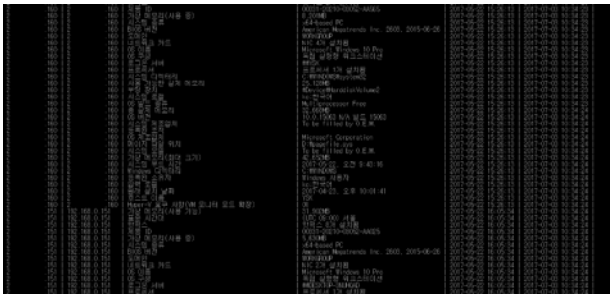
(그림 2) 테스트 환경 네트워크 구성도

적군의 네트워크 내의 방화벽은 포트 http, https out bound 만 허용되어 있다는 가정을 하였고 중계 서버는 외부에 봇넷으로 구성을 하였다.

타겟의 호스트가 중계 서버를 거쳐 아군의 server 로 연결이 확인이 되면 자신의 ip 정보를 전송한다. 아래 그림 3 은 수집된 ip 리스트이다. 수집된 정보가 있을 시에 빨간색으로 표시를 해준다. 수집된 ip 를 클릭 할 시에 수집된 호스트 정보 목록과 명령어를 전송 할 수 있는 페이지로 이동한다.

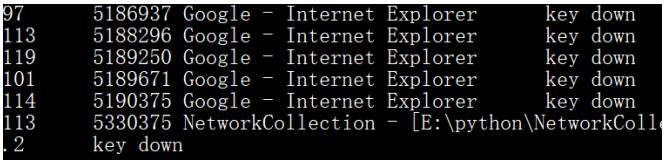
(그림 3) 수집된 ip 목록

수집된 데이터는 추후 활용을 위하여 데이터 베이스에 속성별로 나누어서 저장을 한다. 아래 그림 4 는 수집된 내용을 속성별로 나누어 놓은 그림이다.

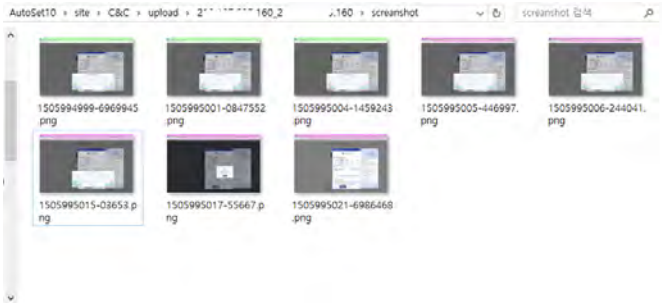


(그림 4) 세부 항목으로 분리 된 시스템 데이터

또한 적의 컴퓨터에서 입력한 키를 로그 파일로 남겼다가 주기적으로 서버로 전송하는 기능과 동시에 마우스 클릭이나 엔터 키 등의 이벤트가 발생할 시에 적의 컴퓨터화면을 캡쳐를 하여 서버로 보내는 기능을 구현하여 실시간으로 적이 무엇을 하는지의 감시가 가능한 것을 확인하였다.



(그림 5) 키로깅을 한 결과



(그림 6) 적 화면 모니터링

위의 그림 5 는 적의 컴퓨터의 키보드를 후킹을 하여. Key down 이벤트가 발생할 때마다 아스키코드값, 타임스탬프, 프로그램제목, 발생이벤트를 기록하였고 그림 6 은 마우스를 후킹을 하여 click 이벤트가 발생 시 주 모니터를 캡쳐를 하여 서버로 전송한 결과이다.

5. 결론 및 향후 과제

본 논문에서는 사이버전에서 적의 컴퓨터에 이미 침투하였다는 가정하에 정보를 얻기 위한 시스템을 설계 및 구현해 보았다. 방화벽에서 포트 80 과 443 out-bound 만 허용했음에도 많은 정보를 얻어 올 수 있었다. 특히 적의 컴퓨터 화면을 캡쳐를 해오는 부분은 적이 무엇을 하는지 실시간으로 파악할 수 있어 영향이 크다고 생각된다.

적의 공간에서 정보를 수집하기 때문에 발각될 위험이 크다. 앞으로 발각될 위험을 줄이기 위한 연구와 기계 학습을 통해 정보를 스스로 판단하는 등 지

능형으로 바꾸기 위한 연구를 진행하면서 발전시킬 예정이다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] 조현숙, “사이버 냉전시대 : 현황와 미래 과제”, KOFST Issue Paper 2011-3 호 2011.8 월

[2] Won-suk, Ou Myungsin, Chae Daesung, Yeum “Influence Factors of Effectively Executing NCW by User's Point of View”, 한국 인터넷 정보학회 11 권 2 호

[3] MoonGoo Lee, Chunsock Bae, “A Study for the Principle Cases of Advanced Persistent Threat Attacks”, 2013 년도 대한전자공학회 추계종합학술대회, 2013.11, 939-942

[4] Younghwan Kim, Soojin Lee, “Cyber Kill Chain Strategy for Offensive and Integrated Cyber Operations”, 보안공학연구논문지 Journal of Security Engineering Vol.13, No.5 (2016), pp.325-340

[5] 고재남 외 12 명, “악성코드 분석, 한국 인터넷진흥원 보고서 KISA-WP-2014-0038