윈도우 기반 악성코드 증거 수집 모듈 개선에 관한 연구

허건일* · 박찬욱* · 박원형* · 국광호*

요 약

최근 경제적 이득을 얻기 위한 목적으로 개인정보·신용정보·금융정보 등을 외부로 유출하는 악성코드가 증가하고 있으며 명의도용, 금융사기 등 2차 피해 또한 급증하고 있다. 그런데 정보 유출형 악성코드에 감염되었을 경우 이를 탐지하고 대응할 수 있는 악성코드 증거 수집 도구가 증거를 수집하지 못하기 때문에 보안담당자가 침해사고를 처리하는데 많은 어려움을 겪고 있다. 본 논문은 기존 윈도우 기반 악성코드 증거 수집 도구의 현황과 문제점을 분석하고 이를 개선할 수 있는 새로운 모듈을 제시한다.

A Study on the Improvement of the Malware Evidence Collection Module Based On Windows

Geon Il Heo* · Chan Uk Park* · Won Hyung Park* · Kwang Ho Kuk*

ABSTRACT

Recently a malware is increasing for leaking personal data, credit information, financial information, etc. The secondary damage is also rapidly increasing such as the illegal use of stolen name, financial fraud, etc. But when a system is infected by a malware of leaking information, the existing malware evidence collection tools do not provide evidences conveniently or sometimes cannot provide necessary evidences. So security officials have much difficulty in responding to malwares. This paper analyzes the current status and problems of the existing malware evidence collection tools and suggests new ways to improve those problems.

Key words : Forensics, Evidence Collection, Malware

접수일 : 2010년 8월 25일; 채택일 : 2010년 9월 25일

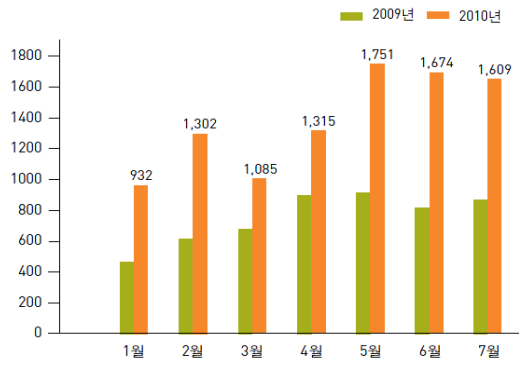
* 서울과학기술대학교 산업정보시스템공학과

1. 서 론

최근 금융거래, 교육, 쇼핑 등 생활 속 밀접한 서비스들이 웹을 통해 이용 가능해지면서 사용자들에게 많은 편리함을 제공해 주고 있다. 하지만 웹을 통한 정보유출사고 증가라는 역효과도 가져다주었다. 웹을 통해 다양한 정보와 서비스가 제공되면서 이를 노린 해커들의 공격도 확대된 것이다[1]. 그리고 웹은 현재 최고의 악성코드 배포 경로 수단으로 이용되고 있으며 이를 통해 정보 유출, 좀비PC 양산 등 많은 피해가 발생하고 있다[2].

2010년 7월 국내 백신업체와 한국인터넷진흥원(KISA)에 신고된 웜·바이러스 사고 신고 건수는 1,609건으로 전월(1,674건)에 비해 3.94% 소폭 감소했다. 하지만 대표적인 정보유출형 바이러스인 온라인게임의 계정을 탈취하는 것으로 알려진 ONLINE GAMEHACK의 신고 건수는 265건으로 전월(245건)에 비해 8.16% 증가했고 특히 INFOSTEALER, PCCLIENT 등 사용자의 입력을 가로채어 저장하는 정보유출형 악성코드 신고 건수는 전달에 비해 166.7%(33건→88건) 증가하였다[3].

(그림 1)은 월별 국내 웜·바이러스 신고 건수를 나타낸다.



(그림 1) 월별 국내 웜·바이러스 신고 건수[3]

이와 같이 최근 발생한 침해사고 동향을 살펴보면 데이터를 삭제하거나 네트워크를 마비시키는 등의 행위를 하는 전통적인 악성코드는 감소하고 개인의 민감한 정보를 외부로 빼돌리는 정보유출형 악성코드가 상대적으로 증가하고 있음을 알 수 있다. 이러한 상황은 기존 윈도우 기반 악성코드 증거 수집 도구의 문제점을 드러나게 하였는데, 그것은 시스템이 정보유출형 악성코드에 감염되었을 경우 기존 도구가 이와 관련된 증거를 수집하지 못한다는 것이다. 즉 시스템이 정보유출형 악성코드에 감염되었을 경우 현존하는 증거 수집 도구로는 보안담당자가 감염여부를 인지하고 대응하는 것이 어렵다.

본 논문에서는 기존 윈도우 기반 악성코드 증거 수집 도구의 문제점을 분석하고, 최근에 발생하고 있는 정보유출형 악성코드의 감염여부를 탐지하고 대응할 수 있는 개선된 모듈을 제시한다.

2. 관련 연구

본 장에서는 기존 악성코드 증거 수집 도구의 개발 목적 및 구성 모듈에 대해서 알아본다.

2.1 美 공군 침해사고대응팀 "FRED"

FRED(First Responder's Evidence Disk)[4, 5]는 美 공군 내부에서 발생하는 침해사고에 좀 더 신속하고 효과적으로 대응하기 위해서 지난 2000년도 AFOSI(Air Force Office of Special Investigations)에 의해 개발된 윈도우 기반 악성코드 증거 수집 도구로서, 2002년 8월 8일 Digital Forensics Research Workshop을 통해 외부에 공개됐다.

FRED는 Commercial off-the-shelf(COTS) 기반의 여러 가지 시스템 분석 도구들이 저장된 플로피 디스크이다. FRED에 저장된 각각의 도구들은 스크립트로 작성되어 배치파일(FRED.bat)로 실행되고, 시스템 분석 결과는 audit.txt 형태로 플로피 디스크에 저장된다.

"FRED.bat" 파일에 포함된 시스템 분석 모듈들은 다음의 <표 1>과 같다.

〈표 1〉 "FRED.bat" 내의 시스템 분석 모듈[4, 5]

모듈	각 모듈이 제공하는 정보
date /t	분석 시작/종료 날짜
time /t	분석 시작/종료 시간
psinfo	OS이름, 버전, 패치수준 등 시스템 요약 정보
net accounts	계정 정책에 관한 정보
net file	원격에서 접근중인 파일 정보
net session	공유자원에 접속한 컴퓨터 정보
net share	시스템 공유 정보
net start	서비스 정보
net use	네트워크 드라이브 정보
net user	시스템에 존재하는 계정 정보
net view	네트워크 구성원 정보
arp -a	ARP Cache 정보
netstat -anr	네트워크 연결상태(라우트 테이블 정보 포함)
psloggedon	로컬/원격 로그온 정보
listdlls	프로세스들이 사용하는 DLL들의 정보
fport/p	포트 정보(번호 기준 오름차순 정렬)
pslist -x	프로세스 정보(메모리 및 쓰레드 정보 포함)
nbtstat -c	NBT에 연결된 세션 정보
dir /s /a : h /t : a c:\	숨김속성의 디렉터리 및 파일에 대한 정보(마지막 접근시간 기준 오름차순 정렬)
md5sum c:*.*	c드라이브의 모든 파일의 MD5값 획득

2.2 한국인터넷진흥원(KISA) "분석 스크립트"

KISA의 분석 스크립트[6]는 해킹피해기관이나 개인이 침해사고를 당하였을 경우 피해기관 혹은 피해자 스스로 신속하고 효율적으로 초동 대응이 가능하도록 하기 위해 개발된 윈도우 기반 악성코드 증거 수집 도구로서 2010년 KISA에서 발간한 "침해사고 분석 절차 안내서" 내에 분석 스크립트 전문이 수록되어 있다.

분석 스크립트에 포함된 시스템 분석 모듈들은 다음의 <표 2>와 같다.

〈표 2〉 스크립트에 포함된 시스템 분석 모듈[4]

모듈	각 모듈이 제공하는 정보
date /t	분석 시작/종료 날짜
time /t	분석 시작/종료 시간
psinfo -h -s -d	OS이름, 버전, 패치수준 및 핫픽스, 소프트웨어, 디스크 정보
uptime	시스템 가동 시간
ipconfig /all	시스템 IP 정보
net session	원격에서 로컬로의 세션 정보
netstat -na	네트워크 연결정보
ntlast -f	원격접속 로그 정보
fport /i	포트 정보(PID 기준 오름차순 정렬)
promiscdetect	NIC가 promisc 모드로 동작중인지 확인
net start	서비스 정보
pslist -t	프로세스 정보(트리 구조)
listdlls	프로세스들이 사용하는 DLL들의 정보
handle	프로세스들이 참조하는 파일 리스트 출력
net share	시스템 공유 정보
net user	시스템에 존재하는 계정 정보
net group	시스템에 존재하는 도메인 그룹 정보
net localgroup	시스템에 존재하는 그룹 정보
net localgroup administrators	시스템에 존재하는 관리자 그룹 정보

10년 전에 개발된 FRED(2000년도에 개발)와 비교했을 때 크게 달라진 점이 없으며 KISA의 분석 스크립트 또한 피해시스템의 상황을 빠른 시간 내에 파악하기 위해 배치파일로 각각의 분석도구들을 실행하도록 설계되어 있다.

2.3 안철수연구소 "AhnReport"

안철수연구소의 AhnReport[7]는 개인이나 기업의 보안담당자가 시스템의 정보 및 안철수연구소 제품 정보, 악성코드 정보 등을 수집할 수 있도록 개발된 윈도우 기반 악성코드 증거 수집 도구이다.

AhnReport에서 분석하는 주요 항목들은 다음의 <표 3>과 같다.

〈표 3〉 AhnReport 주요 분석 항목[7]

분석 항목	설명
제품 정보	시스템에 설치된 안철수연구소 제품 정보 수집
사용자 정보	시스템에 설치된 안철수연구소 제품의 유효기간, 만료날짜 등의 정보 수집
파일 정보	dll, inf, sys 등 주요 파일 정보 수집
레지스트리 정보	주요 레지스트리 정보 수집
문서 파일	system.ini, hosts, win.ini 파일 정보 수집
프로세스와 모듈	Tree 구조로 정보 수집
실행중인 프로세스	실행중인 프로그램 정보 수집
로드된 모듈	로드된 모듈(DLL) 정보 수집
시작프로그램	시작프로그램 정보 수집
예약된 작업	예약된 작업 목록 수집
환경 변수	사용자 변수, 시스템 변수 정보 수집
네트워크 연결	현재 네트워크 연결 상태에 대한 정보 수집
서비스	현재 등록된 서비스 정보 수집
Uninstall 정보	시스템에 등록된 Uninstall 정보 수집
장치	시스템에 설치된 장치 정보 수집
프린터	시스템에 설치된 프린터 정보 수집
공유	공유된 자원 정보 수집
Internet Explorer	ActiveX, Active Desktop, Browser Extensions, Protocol Prefixes 등의 정보 수집
WinSock	DNS 정보 수집
Network	시스템에 설치된 네트워크 어댑터 상세 정보 수집

AhnReport는 앞서 소개했던 FRED, 분석 스크립트와 달리 GUI 기반으로 개발되었다. 직관적이고 편리하게 구성된 User Interface 환경은 보안담당자가 Command-line Interface(CLI) 기반의 도구보다 좀 더 쉽게 침해사고에 대응할 수 있도록 도와준다. 분석된 결과는 암호화 후 저장, 안철수연구소로 보낸다.

3. 기존 윈도우 증거 수집 도구의 문제점

본 장에서는 피해 시스템이 정보유출형 악성코드에 감염되었을 때 기존 증거 수집 도구를 사용하여 증거를 수집할 경우 어떠한 문제가 발생하는지 알아본다.

3.1 네트워크 연결 정보와 프로세스 정보간의 단편화

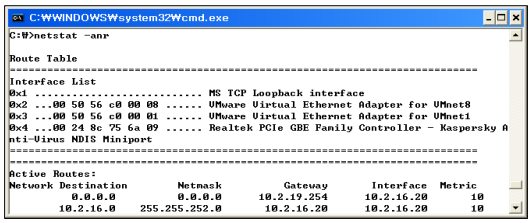
피해 시스템이 정보유출형 악성코드에 감염되었을 경우 이것을 탐지하고 대응하기 위해서는 네트워크 연결 정보와 각각의 연결을 생성하는 데 관여한 프로세스의 정보를 수집해야 한다. 그리고 결과물 중 의심스러운 네트워크 연결이 인지되었을 경우 해당 네트워크 연결 정보 및 관련 프로세스의 정보를 신속히 분석해야 한다.

〈표 4〉 기존 증거 수집 도구 모듈 비교[4-7]

획득정보 / 분석도구	네트워크 연결 정보	프로세스 정보
美 공군 "FRED"	netstat -anr	pslist -x listdlls
KISA "분석 스크립트"	netstat -na	pslist -t listdlls
안철수연구소 "AhnReport"	"네트워크 연결" 항목	"프로세스와 모듈" 항목

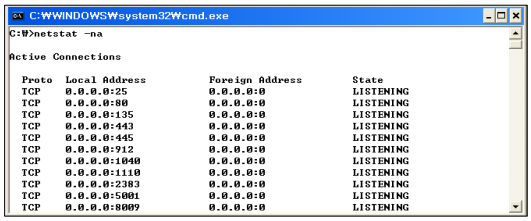
<표 4>는 기존 증거 수집 도구에서 네트워크 연결 정보와 프로세스 정보 수집 시 사용하는 각각의 모듈에 대하여 정리한 표이다.

FRED의 netstat -anr 명령문을 실행하면 다음의 (그림 2)에서 볼 수 있듯이 라우트 테이블 및 경로 정보만 출력된다. 이 정보만으로는 네트워크 연결 정보와 프로세스 정보와의 연관성 분석을 할 수 없는 문제가 발생한다.



(그림 2) netstat -anr 실행 결과

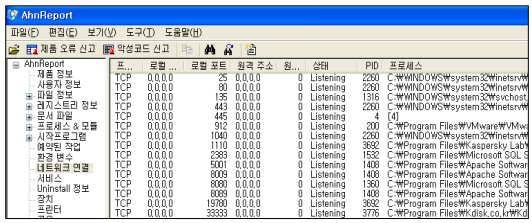
분석 스크립트의 netstat -na 명령문은 아래의 (그림 3)과 같이 네트워크 연결 정보를 보여준다. 하지만 네트워크 연결 정보만 출력되고 각 연결을 생성하는데 관련된 프로세스 정보는 얻을 수 없어 이것 역시 연관성 분석을 위해서는 어려움이 있다.



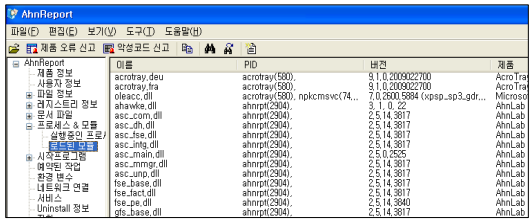
(그림 3) netstat -na 실행 결과

AhnReport의 경우 "네트워크 연결"을 실행하면 아래의 (그림 4)와 같이 네트워크 연결 정보와 각각의 연결을 생성하는 데 관여한 프로세스의 PID, 경로를 보여줘 연관성 분석이 가능하다.

하지만 프로세스가 실행되면서 로드된 DLL 정보를 확인하기 위해서는 (그림 5)와 같이 "로드된 모듈"을 실행한 후 PID를 기준으로 다시 분석해야 하는 문제가 있다.



(그림 4) AhnReport "네트워크 연결" 실행 결과



(그림 5) AhnReport "로드된 모듈" 실행 결과

美 공군의 FRED와 한국인터넷진흥원의 분석 스크립트의 경우 연관성 분석이 불가능하다. 그리고 안철수연구소의 AhnReport의 경우 연관성 분석이 가능하지만 관련 프로세스 실행 시 로드되는 DLL 정보를 얻기 위한 과정은 분석의 효율이 매우 떨어진다. 수작업을 수반한 여러 절차를 거치는 것보다는 가능하다면 자동화된 단일 모듈만을 사용하여 필요한 데이터를 종합적으로 수집·분석하는 것이 효율적이다.

3.2 도메인 주소 정보 수집 모듈 부재

피해 시스템이 정보유출형 악성코드에 감염되어 외부의 특정 도메인으로 접근을 시도했을 경우 기존 증거 수집 도구 내의 모듈만을 사용하여 정보유출형 악성코드의 동작흐름을 파악하는 것은 불가능 하다.

netstat 명령어를 통해 수상한 IP 주소를 식별하였다 하더라도 해당 IP 주소에 매핑되는 도메인 주소를 확인하기 위한 추가적인 분석이 요구된다.

이는 방화벽이 IP 주소와 Port를 기준으로 접근제어를 하기 때문으로, 보안담당자가 아웃바운드 정책 변경을 통해 수상한 IP 주소로의 접근을 차단했다 하더라도 해커가 해당 IP 주소를 변경한 후 피해 시스템이 변경된 IP 주소로 접근하게 하면 위의 조치는 의미가 없다.

따라서 의심스러운 IP 주소를 발견하면 이에 매핑되는 도메인 주소를 추가적으로 확인해야 하고, 해당 도메인 주소에 매핑되는 IP 주소를 지속적으로 관제하여 IP 주소가 변경될 때마다 방화벽의 아웃바운드 정책을 지속적으로 관리해야 한다.

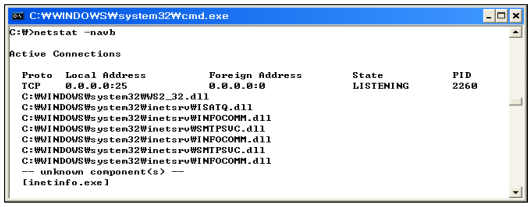
4. 윈도우 증거 수집 모듈 개선 방안

본 장에서는 기존 증거 수집 도구의 문제점을 개선한 새로운 모듈을 제안한다.

4.1 네트워크 연결 정보와 프로세스 정보의 통합

기존 악성코드 증거 수집 도구에서는 네트워크 연결 정보와 각각의 연결을 생성하는 데 관여한 프로세스의 정보를 얻지 못하거나 얻는다 하더라도 추가적인 연관성 분석이 요구되었다.

악성코드 탐지를 위해 네트워크 연결 정보와 프로세스 정보의 보다 간단하고 신속한 연관성 분석을 위해 netstat -navb라는 모듈을 제안한다.



(그림 6) netstat -navb 실행 결과

이는 기존의 netstat -na 또는 netstat -anr 모듈을 개선한 것으로서 여기서 -v, -b 옵션은 MS Windows XP Service Pack 2부터 추가된 것이다[8]. -b 옵션은 각각의 연결에 관련된 프로세스 명을 표시하고, 잘 알려진 프로세스에 한해서 해당 프로세스가 로드한 DLL 파일의 목록을 표시한다. -v 옵션은 -b 옵션과 같이 사용되는 옵션으로 잘 알려진 프로세스만이 아닌 모든 프로세스에 대하여 각각의 프로세스가 로드한 DLL 파일의 목록을 표시한다[9].

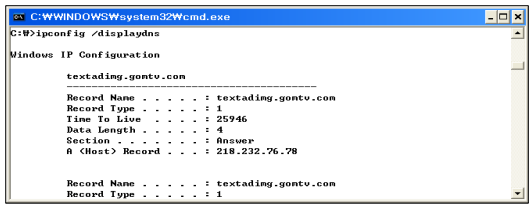
위 (그림 6)에서 볼 수 있듯이 단 하나의 명령문만으로 네트워크 연결정보와 그와 연관된 프로세스 정보를 수집함으로써 정보유출형 악성코드에 감염되었을 경우 좀 더 효과적으로 대응할 수 있다.

4.2 도메인 주소 정보 수집 모듈

4.2.1 DNS Resolver Cache 정보 수집

제 3.2절에서 보안담당자가 의심스러운 IP 주소를 발견했을 경우 IP 주소 변경에 지속적으로 대응하기 위해서 최초 발견한 IP 주소에 매핑되는 도메인 주소를 확인해야 한다.

이를 분석하기 위해서는 ipconfig/displaydns라는 모듈을 제안한다.



(그림 7) ipconfig/displaydns 실행 결과

ipconfig/displaydns 명령문은 위의 (그림 7)과 같이 DNS Resolver Cache의 내용을 보여주는데, 이를 통해 시스템이 접근한 외부 호스트의 IP 주소와 도메인 주소를 함께 알 수 있다. DNS Resolver Cache에는 사용자가 웹브라우저를 통해 정상적으로 접근을 시도한곳 뿐만이 아니라 악성코드의 동작으로 인해 비정상적인 방법으로 접근을 시도한

곳의 정보도 기록되기 때문에 DNS Resolver Cache 정보는 양질의 증거로 활용될 수 있다.

DNS Resolver는 DNS 서버 또는 DNS 클라이언트에서 DNS 이름에 대한 질의를 수행하는 객체로서, DNS 서버로 하여금 같은 질의를 반복적으로 수행하지 않도록 하기 위하여 최초 질의 결과를 DNS Resolver Cache 영역에 저장한다[10]. 하지만 DNS Resolver Cache 영역에 저장된 데이터는 휘발성 데이터이기 때문에 시스템이 다시 시작되거나 네트워크 연결이 끊어질 경우 데이터가 사라지는 문제점이 있다. 따라서 DNS Resolver Cache 정보가 훼손되었을 경우 시스템이 접근한 도메인 주소 정보를 획득할 수 있는 다른 방법이 필요하다.

4.2.2 index.dat 정보 수집

index.dat 파일은 사용자가 방문한 모든 웹 사이트에 대한 쿠키, 히스토리, 인터넷임시파일 정보 등이 기록된다[11, 12]. 또한 사용자의 인터넷 사용 패턴이나 접속 기록 등을 확인할 수 있으며 증거수집 모듈과 함께 연관성 분석을 통해 의미 있는 정보를 도출 할 수 있다.

윈도우 운영체제별 index.dat 파일 위치는 <표 5>과 같다.

그리고 앞서 설명한 DNS Resolver Cache의 단점인 휘발성 데이터를 보완해 줄 수 있다. index.dat 파일은 접속기록을 반영구 보존할 수 있으며 PC에서 인터넷접속기록을 저장하는 블랙박스이기 때문에 시스템을 다시 시작하더라도 보존이 가능하다. 그래서 휘발성 도메인을 탐지하지 못하더라도 index.dat 파일을 분석하면 정보유출형 악성코드에 감염된 도메인 위치를 찾을 수 있다.

〈표 5〉 윈도우 OS별 index.dat 파일 위치[11]

윈도우OS	위 치
윈도우 2000 · 윈도우 XP	Documents and Settings\user\Cookies\index.dat
	Documents and Settings\uesrname\ Local Settings\Temporary Internet Files\index.dat
	Documents and Settings\username\Local Settings\History\History.IE5\index.dat
윈도우 VISTA	Users\<Username>AppData\Roadming \Microsoft\Windows\Cookies\low\index .dat
	Users\<Username>AppData\Local\Mic rosoft\Windows\Temporary Internet Files\Content.IE5\index.dat
	Users\<Username>AppData\Local\Mic rosoft\Windows\History\Content.IE5\in dex.dat
	Users\<Username>AppData\Roadming \Microsoft\Windows\Cookies\index.dat

5. 결 론

본 논문에서는 최근 증가하고 있는 정보유출형 악성코드에 대응하기 위하여 기존 윈도우 기반 악성코드 증거 수집 도구의 일부 모듈을 수정하고 새로운 모듈을 추가하였다.

기존 증거 수집 도구는 네트워크를 마비시키는 등의 행위를 하는 전통적인 악성코드의 동작흐름을 파악하는데 필요한 모듈을 중심으로 구성되어 있었다. 그래서 피해시스템이 정보유출형 악성코드에 감염됐을 경우 악성코드 작동흐름은 물론 감염사실조차 파악하기 어려웠다. 하지만 본 논문에서 제시한 개선된 모듈을 사용할 경우 정보유출형 악성코드의 감염여부 및 연관성분석에 대해 빠르고 쉽게 파악이 가능하다.

그러나 본 논문에서 제안한 개선된 모듈의 효과를 검증하기 위해서는 자동 스크립트를 개발하고 정확한 실험이 추가적으로 필요하다. 특히, netstat -navb 명령어는 윈도우 XP 이하 커널의 운영체제에서 실행할 경우 다른 모듈보다 상대적으로 많은

시간을 필요로 하기 때문에 향후 이에 대한 추가적인 연구가 필요하다.

참 고 문 헌

[1] 장영준, 차민석, 정진성, 조시행, “악성 코드 동향과 그 미래 전망”, 한국정보보호학회, 2008.

[2] ASEC Report, 안철수연구소, 2010.

[3] 인터넷 침해사고 동향 및 분석 월보, KISA 인터넷 침해대응센터, 2010.

[4] Special Agent Jesse Kornblum, “Preservation of Fragile Digital Evidence by First Responders”, Air Force Office of Special Investigations, 2002.

[5] Special Agent Jesse Kornblum, “Simple but Sound Tools for First Responders”, Air Force Office of Special Investigations, 2002.

[6] 침해사고 분석 절차 안내서, KISA 해킹대응팀, 2010.

[7] 임채영, “AhnReport 분석”, 안철수연구소 ASEC, 2009.

[8] Greg Shultz, “Windows XP SP2 adds a new parameter for Netstat”, TechRepublic, 2005.

[9] http://en.wikipedia.org/wiki/Netstat.

[10] http://en.wikipedia.org/wiki/Domain_Name_System.

[11] http://www.forensic-proof.com/20, index.dat 분석.

[12] 김용호, 디지털증거확보를 위한 파일 삭제 탐지 모델, 경기대학교 박사논문, 2008.

허 건 일

2004년 서울과학기술대학교 산업정보시스템공학과 입학

현재 서울과학기술대학교 산업정보시스템공학과 네트워크보안 Lab 연구원

박 찬 욱

2004년 서울과학기술대학교 산업정보시스템공학과 입학

현재 서울과학기술대학교 산업정보시스템공학과 네트워크보안 Lab 연구원

박 원 형

2009년 경기대학교 정보보호학과 이학박사(정보보호전공)

2010년 서울과학기술대학교 산업정보시스템공학과 겸임교수

국 광 호

1979년 서울대학교 공과대학 (공학사)

1981년 서울대학교 대학원 (공학석사)

1984년 청주대학교 산업공학과 전임강사

1989년 Georgia Institute of Technology, U.S.A (공학박사)

1993년 한국전자통신연구원 선임연구원

현재 서울과학기술대학교 산업정보시스템공학과 교수