인사이드 윈도우즈 포렌식

:디지털 해킹 분석 및 대응의 기술

Windows Forensic Analysis DVD Toolkit, 2nd edition

by Harlan Carvey

ISBN: 978-1-59749-422-9

Translated Edition ISBN:

Translated by Bjpublic

Printed in Korea.

책값은 뒤표지에 있습니다.

저자 서문

이 책의 목적은, 1판에서도 밝혔듯이, 필요성을 알리는 것이다. 많은 사고 대응자들과 컴퓨터 포렌식 조사자들이 알고 있는 문제는 포렌식 분석 도구 절차가 알려주는 정보가 어디에서 오며 어떻게 생성되고 파생되었는지, 실제로 이해하지도 않고 지나치게 신뢰한다는 것이다. '닌텐도 포렌식의 시대(Age of Nintendo Forensics)', 즉 수집된 이미지를 포렌식 분석 애플리케이션에 로딩하고 버튼을 누르는 것과 같은 시대는 끝났다. 분석자와 조사자로써 우리는 더 이상 그런 식의 사고 조사는 기대하지 않는다. 사이버 범죄는 점점 교묘해지고 조사자들은 어떤 흔적들이 시스템에서 이용가능한지, 또한 어떻게 그런 흔적들이 만들어지고 수정되는지를 이해하는 것이 필요하다. 이런 수준의 지식이 '흔적의 부재' 라는 것 자체가 '흔적' 이라는 것을 이해하게 한다. 게다가 안티 포렌식(anti-forensics)과 포렌식 분석을 더욱 어렵게 만드는 기술들에 대한 강연과 자료는 더욱 많아지고 있다. 그뿐만 아니라 안티 포렌식 기술을 토론하는 큰 컨퍼런스에서는 그것에 대항하는 포렌식 분석을 위한 대응자나 조사자의 교육 방법과 툴을 사용하기도 한다. 이 책은 좀더 자세하고 세분화된 수준의 이해에 대한 필요성을 알리고자 한다. 이 책의 목적은 동작중인 윈도우즈 시스템과 수집한 이미지의 분석을 위해 어떤 정보가 조사자에게 이용 가능한지를 설명하는 것뿐만 아니라 흥미 있는 추가적인 흔적들에 대한 위치를 찾아내고, 사고의 더욱 완전한 그림을 만들어 내기 위한 다양한 데이터 소스들을 연관시키는 방법에 대한 정보를 제공하는 것이다.

이 책을 쓰는 주된 이유는 나에게 많은 도움을 주려고 노력한 커뮤니티와 동료들에게 그 도움을 다시 되돌려 주기 위함이다. 12년이 넘는 기간 동안 정보 보안 분야에 있으면서(그전에는 군대에 있었고 물리학 및 통신 보안 분야에도 있었다) 많은 훌륭한 사람들을 만났고, 정말로 흥미로운 일들을 많이 이루어 냈다. 시간이 지나면서 사람들은 내게 매우 큰 도움이 될만한 것들을 공유해 주었고, 그 중의 몇몇은 다음 연구를 위한 발판을 제공했다. 그러한 연구의 몇 가지는 수많은 컨퍼런스의 강연을 통해 보급되었고, 컨퍼런스 참가자들의 질문을 통해 그 연구들에 박차를 가하는 데 도움을 주는 통찰력과 해답을 얻을 수 있었다. 토론에서 되풀이되는 정보의 교환과 교류는 그 분야를 진보시키면서 관심과 지식의 수준을 발전시켰다. 이 책은 그러한 내가 받은 도움을 되돌려 주고자 하는 나의 시도이며, 그렇게 해서 약간이나마

이 분야를 넓히고자 함이다.

이 책은 윈도우즈 시스템의 실시간 조사 및 사후 조사 중에 데이터를 수집하고 분석하는 기술적인 측면들을 알려주고 있다. 이 책에서 모든 것을 다루고 있는 것은 아니다. 여전히 몇몇 분야의 연구에서 상당히 미진한 부분이 많으며, 많은 정보들이 정리될 필요가 있다. 나의 바람은 이 책을 읽는 독자들이 좀 더 포괄적인 조사와 분석을 위해 윈도우즈 시스템에 존재하는 가능성과 기회들을 일깨울 수 있도록 도움을 주는 것이다.

독자 대상

이 책은 매우 한정된 기술적인 분야-윈도우즈 사고 대응과 포렌식 분석-에 초점을 맞추고 있으나 윈도우즈 시스템의 포렌식 분석을 수행하고 있는, 또는 수행 예정인 사람들을 위한 책이기도 하다. 이 책은 많은 사람들에게 매우 유용한 참고서가 될 것이다. 만약 독자들이 이 책을 읽으며 기술적으로 어렵다고 느끼는 부분이 있다면, 앞으로의 더 깊은 연구의 토대 및 출발점으로 삼고자 하는 자료로서 이 책이 사용되었으면 하는 것이 나의 바람이다. 나는 이 책의 1판을 쓸 때 더 이상 이와 관련된 책을 쓰지 않으려고 했었다. 내가 최초로 쓴 책은 2004년 7월에 Addison-Wesley에서 출간된 『윈도우즈 포렌식과 사고 복구(Windows Forensics and Incident Recovery)』이다. 나의 의도는 일반적인 관점에서 벗어나 나 자신뿐만 아니라 컴퓨터 포렌식 분석 분야에서 일하는 다른 사람들을 위한 자료를 제공하고자 하는 것이었다. 이번 2판 역시 같은 관점에서 쓰게 되었고, 특히 마이크로소프트에서 각각의 고유한 방식과 차이를 가지는 새로운 버전의 윈도우즈 운영체제를 꾸준히 개발하고 배포하기 때문이기도 하다.

나는 포렌식 분석자, 조사자, 그리고 사고 대응자들을 위한 자료를 제공하고자 이 책을 썼다. 이 책이 현재 포렌식 조사를 수행하는 사람들에게 유용한 자료를 제공하는 것뿐만 아니라 현재 사고 대응 활동을 해오며 '내가 무엇을 했어야 하나?' 라는 의문을 여전히 가지고 있는 시스템 관리자에게 통찰력을 제공할 수 있기를 바란다. 그와 더불어, 하드 드라이브를 완전히 지우고 손상되지 않은 미디어에서 운영체제를 재설치 하는 것이 문제의 적절한 해결책이라는 잘못된 생각을 근본적으로 바꿀 수 있기를 바란다. 시스템에서 패치를 업데이트하는 경우에도 환경설정 문제들을 처리하는 것이 아니라 대부분 또다시 시스템을 손상시키거나 재감염시킬 것이다.

이 책은 윈도우즈 시스템의 사고 대응 및 포렌식 분석을 수행하는데 관심이 있는 **모든 사람들**-회사나 정부 조사관들, 최근 몇 년 동안 급성장해온 교과과정의 학생들이나 교수님들, 법 집행 관리자들, 회사 컨설턴트(나와 같은)들과 같은-을 위한 책이다. 또한 이 책이 대학에서 컴퓨터 포렌식 프로그램을 개발하거나 관련 학과를 이수하고 있는 사람들에게도 유용한 참고서가 되기를 바란다.

이 책 전체에서 **조사자**(investigator), **초동 대응자**(first responder), **검사자**(examiner), **관리자**(administrator)라는 용어는 상호 호환적으로 사용된다. 사실상 많은 경우에 같은 사람이 여러 업무를 처

리할 수 있기 때문이다. 어떤 경우에는 조사자가 회사의 기반 시설에 들어가 데이터 수집을 수행하기 위해 도메인 내에 있는 관리자 수준의 계정을 얻는다는 점에서 관리자와 아주 비슷하게 일할 수도 있다. 또한 몇몇 경우에서는 관리자가 조사자나 초동 대응자를 손상된 시스템에 안내하기도 하고, 사용자 계정은 시스템에서 관리자 특권을 가질 수 있다. 따라서 위의 4가지 용어는 많은 경우에서 동의어이기 때문에 용어사용에 혼동하지 않아도 된다.

이 책을 읽으면서 여러분은 다음과 같은 점을 발견할 것이다. 첫 번째, 이 책에 사용되는 스크립트 언어는 펄(Perl)이다. 이러한 선택에 특별한 것은 아무것도 없다?펄은 코드를 수정해서 재컴파일 하지 않고 바로 실행할 수 있는 매우 단순하며 유용한 강력한 스크립트 언어다. 컴파일에 대해 말하자면, 나는 여러분이 펄에 익숙지 않거나 전혀 사용해본 적이 없다고 해도 전혀 걱정할 것이 없다는 것을 말하고 싶다. 단지 몇 가지를 제외하고는 책과 첨부된 CD에서 제공되는 펄 스크립트는 Perl2Exe를 사용하여 윈도우즈 단독 실행 파일로 '컴파일' 되어 있다. 즉, 여러분이 펄(이 책에서 사용되는 펄 버전은 ActiveState.com에서 무료로 얻을 수 있다)이나 그 밖에 다른 것을 설치하지 않고도 펄 스크립트를 실행할 수 있다는 것을 의미한다. 간단하게 필요한 위치나 CD에서 파일을 뽑아내어 실행하면 된다. 또 다른 유용한 특징은 펄 스크립트는 독립된 플랫폼에서 쓸 수 있다는 점이다. CD에 있는 많은 펄 스크립트는 바이너리 파일에서 데이터를 추출(또는 어느 정도 분석)하며, 가능한 플랫폼에 독립적으로 만들려고 노력했다. 이것이 의미하는 것은 펄 스크립트(그리고 첨부된 윈도우즈 실행파일)가 윈도우즈 플랫폼에서 실행되기도 하지만 리눅스 또는 맥 OS X에서도 실행될 수 있다는 것이다. CD에서 사용되는 대부분의 펄 스크립트(비록 전부는 아니지만)는 테스트되었고 성공적으로 리눅스의 펄 환경 내에서 실행된다. 이것은 검사자의 분석이 특정 플랫폼에 국한되지 않는 것을 의미하기도 한다. 몇몇 스크립트는 추가적인 모듈 설치를 요구하며 Perl의 ActiveState 배포의 일부인 펄 스크립트 매니저(Perl Package Manager, PPM) 애플리케이션을 통해 이루어지고 윈도우즈, 리눅스, 맥 OS X, 그리고 다른 종류의 많은 플랫폼을 지원한다. 펄을 사용하는 또 다른 매우 유용한 점은 자동화의 요구에 맞출 수 있다는 것이다. 나는 매번 반복해서 같은 종류의 일(데이터 추출, 바이너리 데이터를 사람이 읽을 수 있게 번역하는 작업 등)을 하고 있는 나 자신을 발견했고 대부분의 사람들처럼 나도 몇 가지 점에서 실수를 하고 있었다. 그러나 그러한 일들을 펄로 자동화하면 코드를 한번에 쓸 수 있고, 같은 일을 하면서 겪는 실수를 2번, 20번, 심지어 200번할 필요가 없을 것이다. 만약 여러분이 실제로 프로세스를 가지고 있다면 프로세스 자체를 교정하는 것은 쉬울 것이다. 그러나 정작 자신이 한 일이 무엇인지 모른다면, 자신이 한 일을 바로잡는 것은 대단히 어렵다.

두 번째, 여러분은 이 책에서 사용되는 포렌식 분석 애플리케이션이 Technology Pathways의 ProDiscover Incident Response Edition이라는 것을 알 수 있을 것이다. 크리스 브라운(Chris Brown)의 관용덕분에 나는 버전 3(이 책이 쓰여질 때에는 버전 5가 가능했다)부터 ProDiscover로 작업을 해왔고 인터페이스가 사용하기 매우 직관적이고 쉽다는 것을 알게 되었다. 윈도우즈 시스템에서 획득한 이미지를 조사하고자 할 때 ProDiscover는 훌륭한 도구(비록 유일한 것은 아니지만)이며 많은 유용하고 강

력한 특성을 지닌다. 크리스와 알렉스 어거스틴(Alex Augustin)은 의문사항들과 업데이트를 매우 빠르게 처리해주었고, 내가 컨퍼런스에서 테드 어거스틴(Ted Augustin, 이 세 명은 모두 Technology Pathways에서 근무한다)을 만나 그와 얘기할 수 있는 기회를 가진 것은 매우 훌륭한 자산이다. ProDiscover 그 자체로도 훌륭한 분석 플랫폼일 뿐만 아니라 Incident Response Edition은 휘발성 데이터를 수집하기 위해 쉽고 유용한 수단을 제공하면서 실시간 대응 분야에 큰 발전을 만들고 있다. 또한, 내 견해로써 크리스가 펄을 ProDiscover의 스트립트 언어로서 선택한 것은 최고의 결정이며, 이는 조사자가 펄 'ProScripts'을 통해 이미지에서 함수들(예: 조사, 데이터 추출, 어느 정도의 데이터 분석 등)을 수행할 수 있게 한다. 첨부된 CD는 내가 직접 만들어 조사할 때 자주 사용하는 몇몇의 ProScripts를 포함하고 있다(비록 ProScripts가 펄 스크립트이긴 하지만 ProScripts는 ProDiscover에서 쓰이는 스크립트여야만 하기 때문에 Perl2Exe로 '컴파일' 되지 않았다).

이 책의 여러 곳에서 언급된 또 다른 유용하고 강력한 유틸리티는 F-Response이다. 2008년에 매튜 섀넌(Matthew Shannon)은 노력 끝에 실시간 시스템에서의 사고 대응과 데이터 획득에 있어서 새로운 시대를 인도했다. F-Response는 세 가지 유형이 있으며, 가장 강력한 유형은 Enterprise Edition(EE)이다. F-Response EE는 한 명의 관리자 또는 컨설턴트에게 읽기 전용 모드로 데이터 센터, 도시, 또는 심지어 대륙 간의 시스템에 접속할 수 있는 기능을 제공한다. 또한 매튜는 지금 이 문장을 쓰는 것보다도 더 쉽게 F-Response EE을 수행하게 하는 강력한 관리 콘솔을 제공한다. 한번 수행하게 되면 F-Response EE는 읽기 전용(쓰기 작업은 버퍼링되고 쓰여진다)의 완벽한 도구 불가지론(不可知論)적인 방식으로 원격 시스템의 하드 드라이브뿐 아니라 물리 메모리(또는 램)의 접근을 제공한다. 이것은 여러분이 하드 드라이브의 이미지를 얻고 물리 메모리에 접근하는 등의 작업을 하기 위해 현재 가능한 자원에 접근하려 할 때 어떠한 도구든 사용할 수 있다는 것을 의미한다. 여러분은 단지 하나의 상업적인 애플리케이션 사용에 국한되지 않고 그 어떤 것도 사용이 가능하다.

이 책의 구성

이 책은 다음의 9개 장으로 구성된다.

1장. 실시간 대응: 데이터 수집

이 장은 실시간 시스템에서 휘발성 데이터를 수집하는 기본적인 주제에 대하여 설명한다. 몇 가지 요인들(사이버 범죄의 복잡성 증가, 저장 용량 증가 등) 때문에 실시간 대응은 많은 관심을 갖게 되었고, 대응자들도 날이 갈수록 실시간 대응의 필요성을 인식하고 있다. 이러한 관심의 증가는 나와 같은 컨설턴트에 제한되지 않는다-법 집행에 있어서도 조사를 뒷받침하기 위한 실시간 시스템에서의 휘발성 정보 수집에 대한 필요성이 보이기 시작한다. 이 장은 휘발성 정보를 수집하기 위한 도구들과 방법들을 나열하

며, 포렌식 서버 프로젝트의 가장 최근의 형태를 소개한다.

2장. 실시간 대응: 데이터 분석

데이터 수집과 데이터 분석을 별개의 주제로 보기 때문에 분리를 했다. 대부분 경우, 여러분이 특정 시점의 시스템 동작에 대한 스냅샷을 얻길 원하듯이, 수집하려는 데이터는 변하지 않는다. 그러나 데이터를 어떻게 해석하는지는 그 사건에서 중요할 수 있다. 또한 현장에 접근하여 초동 사건 보고가 단지 시스템에서 실제로 발생한 일의 징후뿐이었거나 실제 문제와 아무런 관계가 없다는 것을 발견하는 것은 드문 일도 아니다. 실시간 대응을 하는 동안 여러분이 수집한 데이터를 어떻게 분석하고 무엇을 찾아야 하는지는 사기 사건인지, 침입 사건인지, 또는 악성코드 감염 등에 따른 것인지, 각각의 상황에 따라 달라질 수 있다. 이 장은 시스템 동작에 대한 근접한 상황을 전개하고 근본적인 원인의 분석과 증명을 좀더 쉽고 이해할 수 있도록 하기 위한, 실시간 대응을 하는 동안 수집된 데이터를 연관시키고 분석하기 위한 구조에 대해 설명한다.

3장. 윈도우즈 메모리 분석

윈도우즈 메모리 분석은 2005년 여름에 관련 모임에서 정식으로 소개된 이후 실직적으로 시작된 연구 영역이며, 2008년에 들어 비약적으로 커졌다. 과거에는 실시간 시스템에서 수집된 물리 메모리(RAM)의 내용이 있다면 그 내용들에서 문자열(비밀번호일 가능성이 있는), IP, 그리고 전자우편 주소 등이 탐색되어 보관되었다. 불행하게도 이런 방법으로 발견된 정보에서는 거의 사건의 정황을 찾을 수 없다. 고맙게도 DFRWS 2005 메모리 챌린지(Challenge)를 통해 RAM 덤프(dump)를 획득하는 방법들이 연구되었고, RAM 덤프 내부의 데이터는 식별되어 더 작은 수준으로 추출될 수 있었으며, 심지어 덤프 파일에서 실행 이미지를 추출하는 것도 가능하다. 이 장에서는 메모리 수집과 분석을 수행하고 메모리 덤프에서 어떤 데이터(레지스트리 하이브, 암호화된 비밀번호 등)가 수집될 수 있는지를 알려주는데 사용 가능한 도구들을 소개할 것이다.

4장. 레지스트리 분석

윈도우즈 레지스트리는 시스템 상태와 관련하여 실제의 다양한 정보를 관리한다. 그리고 많은 경우, 레지스트리가 관리하는 정보는 어떤 식으로든 그것과 관련된 타임 스탬프를 가지고 있기 때문에 그 자체가 로그 파일처럼 다루어 질 수 있다. 그러나 데이터가 저장되는 특정한 방식 때문에 아스키(ASCII) 또는 유니코드(Unicode) 문자열의 조사는 가장 중요하고 유용한 정보의 단편을 드러내지 않는다. 이 장은 획득한 이미지 내의 2진 데이터 및 할당되지 않은 공간에서 레지스트리 흔적들을 인식할 수 있도록 그 구조에 대하여 설명한다. 그리고 나서 조사에 있어서 여러 흔적들의 유용성과 가치에 대한 설명뿐만 아니라 획득한 이미지로부터 그런 정보들을 추출하는 몇 가지 도구들에 대한 소개를 통해 다양한 흔적들에 대해 장황하게 논의할 것이다. 이 장에서 논의되는 다른 중요한 요소들은 하이브(hive) 파일에서 정보들

을 추출하고 연관시켜주는 RegRipper와 같은 도구의 사용과 하이브 파일에서 할당되지 않은 공간으로부터 삭제된 레지스트리 키를 복원하는 방법에 대한 윈도우즈(예를 들면, XP 대 비스타)의 다양한 버전마다의 고유한 차이점을 포함한다는 것이다.

5장. 파일 분석

윈도우즈 시스템은 많은 검사자들이 모르는 다수의 로그(log) 파일들을 관리하며, 그 로그 파일들은 대게 기록되는 항목들에 대한 타임스탬프(time-stamp) 정보를 가진다. 그에 더하여, 윈도우즈 시스템에는 타임 스템프 정보를 사건의 타임라인 분석에 통합될 수 있는 파일 그 자체에 보존하는 파일들이 있다. 이 타임스탬프들의 대부분은 애플리케이션에 의해 관리되며 즉각적으로 확인되지는 않는다. 이 장에서는 다양한 파일들, 파일 형식들, 그리고 파일 메타데이터(metadata)에 대해서 상세하게 논의할 것이고, 논의된 많은 정보를 추출하기 위한 도구들을 설명할 것이다. 2판(이 책)의 5장에서는 운영체제에 의해서 '보호된' 파일이 수정되거나 감염된 것을 확인하기 위한 애플리케이션인 WFPCheck(이 애플리케이션은 첨부된 CD로는 제공되지 않으니 주의하자)의 설명과 더불어 1판에서 다루었던 주제들을 확장하여 다룰 것이다.

6장. 실행 파일 분석

실행 파일은 파일 분석에 있어서 특별한 경우로 나타난다. 대부분의 경우, 실행 파일은 다양한 윈도우즈 버전에서 실행되어야 하기 때문에 이미 알려진 문서화된 구조를 따른다. 그러나 악성코드 제작자들은 그들의 악성코드를 더욱 분석하기 어렵게(불가능하지는 않더라도) 만들기 위한 목적으로 구조를 난독화하는 방법을 사용한다. 이들 파일 포맷(format)을 이해하고 어떻게 생겼는지 볼 수 있는 것은 윈도우즈 시스템 상에서 어느 파일이 합법적인지, 의심스러운 파일이 어떤 영향을 가지는지 확인하게 해주며, 검사자는 그들의 조사를 더 진행해 나아갈 수 있다. 이 장에 나와있는 기술과 정보를 사용하여 검사자는 악성코드의 특정 부분 속성에서 어떤 흔적을 확인할 수 있는지는 물론이고 어떤 파일이 합법적인지 결정할 수 있다.

7장. 루트킷과 루트킷 탐지

이 장은 신비한 베일에 쌓인 특별한 형태의 악성코드를 파헤치고 관리자, 초동 대응자, 그리고 포렌식 분석자(이들은 모두 같은 사람이라는 것을 기억하라)에게 루트킷을 인식하고 밝혀내는데 필요한 정보를 제공하고자 루트킷에 대해 설명한다. 루트킷은 사이버 범죄에서뿐만 아니라 '합법적인' 상업용 애플리케이션에서도 급격하게 사용되고 있다. 루트킷과 루트킷 탐지 기술을 이해하는 것은 윈도우즈 시스템에서 작업하는 사람에게 대단히 중요하다. 그래서 이 장은 조사자에게 필요한 많은 정보에 대하여 자세히 설명한다. 대부분의 경우, 대응자들은 비정상적인 행동의 원인을 신속하게 파악하는 것이 불가능하다. 그래서 철저하고 엄격한 조사를 통해 접근하는 대신 그냥 '루트킷'일 것이라고 추측한다. 나의 바람은

루트킷과 '루트킷 역설'에 대한 정보를 설명함으로써 대응자와 조사자가 그들의 사고에 루트킷이 있는지 또는 루트킷과 유사한 기능을 가진 그 어떤 것이 관련되어 있는지 정확하게 판단하기 위해 필요한 도구들을 보유하는 것이다.

8장. 모두 함께 결합하기

이 책의 1판 이후로 많은 조사자들이 하나의 장에서 정보를 얻어 그것을 적용한 다음에는 무엇을 해야 하는지 모른다는 것을 알게 되었다. 나는 법인 컨설턴트뿐만 아니라 사법 집행관들로부터 이러한 현상에 대하여 알게 되었다. 이 장의 목표는 여러분이 '트로이 목마 방어'를 반증하는 사법 집행관이나 법인 분석가이든지, 또는 시스템이 손상되었는지 결정하는 컨설턴트이든지 간에 여러분이 조사하는 서로 다른 영역-파일 시스템, 특정 파일, 이벤트 로그, 그리고 레지스트리-으로부터의 정보들이 좀 더 완전한 그림을 만들기 위해 어떻게 서로 관련되고 함께 결합될 수 있는지 설명하는 것이다. 이 장을 사례 연구나 '실전 이야기'의 시리즈로 읽음으로써, 이러한 예제들을 통해 조사(단지 획득한 이미지에서만이 아니라) 내의 다양한 장소로부터 어떻게 데이터가 다른 데이터와 보강되어 사용되고 철저한 조사가 이루어지는지 설명할 수 있기를 바란다.

9장. 예산 안에서 분석 수행하기

때로는 분석에 있어서 단순히 모든 특성을 가진 상용 포렌식 애플리케이션들을 사용하는 것은 적합하지 않다. 그것들은 일부 필요한 기능들이 부족하거나 또는 여러분이 필요한 기능을 사용하기에 너무 복잡할 수도 있다. 무료로도(또는 저렴하게) 충분한 기능을 사용할 수 있는 도구들이 있다면 추가적인 상용 애플리케이션을 위해 많은 자금을 낭비하는 것만이 해결책은 아닐 것이다. 이번 장의 목표는 포렌식 분석 이 절차에 관한 것이지 도구에 관한 것이 아니라는 걸 설명하는 것이다. 기억해라. 닌텐도 포렌식의 시대는 끝났다! 데이터를 어디서 찾아야 하고, 그 데이터를 어떻게 추출하고 해석하는지 이해하는 것은 검사자가 업무를 위한 적절한 도구를 선택할 수 있도록 해준다. 많은 무료(freeware) 도구들이 상용 도구가 제공하지 못하는 기능을 제공할 수 있으며, 상용 도구들은 그러한 무료 도구들로부터 얻어낸 조사 결과의 검증을 제공할 수 있다.

CD

이 책에 첨부된 CD에는 많은 유용한 정보와 도구가 들어있다. 제공된 모든 도구들은 각 도구들을 설명하는 장을 기준으로 적절한 디렉터리에 저장되어 있다. 또한 이 책 2판에서는 다른 도구들로 교체되었지만 1판에서 제공된 모든 도구들이 여전히 CD에 포함되어 있다. 예를 들어, 1판의 4장에 있는 모든 스크립트들은 RegRipper 프레임워크에 의해 교체되었음에도 불구하고 여전히 CD에서 제공받을 수 있다.

거기에다가 이 책의 어떤 장에서도 특별히 설명되지는 않았지만 다른 사람들이 유용하게 쓸 것이라 생각하여 내가 개발한 몇몇 도구들을 포함한 보너스 디렉터리도 있다. 또한 이 디렉터리에는 특정 주제에 대한 분석을 담고 있는 PDF 문서들이 있는 'WFX articles' 라는 이름의 하위 디렉터리가 있다. 각각의 문서들은 분석에 대한 한가지 관점씩을 자세히 설명하고 있다. 예들 들어, 어떤 문서는 분석자가 이미지 내의 서로 다른 위치에서 호스트 시스템의 미디어 액세스 컨트롤(media access control, MAC) 주소에 대한 정보를 얻는 것에 대하여 설명하고, 다른 문서는 각 ACMru 서브키의 목적에 대하여 상세히 설명한다. 내가 이 문서를 쓴 목적은 특정 주제의 분석에 대한 교육의 배포에 의미가 있다. PDF마다 각각의 주제를 제공하여 사용자들은 책을 읽는 동안 이 문서들을 프린트하고 읽을 수 있으며(주석도 달아가며), 또한 임의의 디렉터리에 복사하여 필요할 때마다 문서들을 검색할 수 있다.

CD에 있는 모든 도구들은 펄 스크립트로 작성되어 있다. 그러나 펄 스크립트의 거의 대부분은 윈도우즈 시스템에서 쉽게 사용하도록 '컴파일' 되어 있다. 펄 스크립트 자체는 대부분 플랫폼 독립적이며, 윈도우즈, 리눅스, 그리고 맥 OS X(몇 개는 제외하고)에서 실행되고, 펄이 설치 되어있지 않아도 좀더 쉽게 실행 될 수 있도록 윈도우즈 실행파일을 제공한다. 몇몇 디렉터리들은 Technology Pathways에서 만든 ProDiscover 포렌식 분석 프로그램(현재 버전 5.0)에서 전용으로 사용하는 펄 스크립트인 ProScript들을 가지고 있다. 이 펄 스크립트들은 '컴파일' 되어있지 않고 ProDiscover를 통해 실행된다.

게다가 몇 개의 디렉터리에는 독자들이 도구들을 쉽게 다룰 수 있도록 샘플 파일들을 추가하였다. 도구나 유틸리티를 단지 소유하고 그 사용법에 대해 알고 있는 것과 정보를 얻기 위해서 실제로 도구를 사용하는 것은 매우 다른 것이다. 즉시 시험해볼 수 있는 무엇인가를 이미 가지고 있다는 것은 그런 파일들을 구할 때까지 기다릴 필요가 없이 독자들이 비행기와 같은 어떤 장소에서도 노트북을 이용해 툴들을 작동해 볼 수 있다는 것을 의미한다.

– 할랜 카비(Harlan Carvey)

감사의 글

먼저 내 인생에 많은 축복을 내려준 하나님께 감사를 드리고 싶고 이에 대해 이루 헤아릴 수 없을 만큼 고맙게 생각한다. 예수님을 내 마음과 삶에 받아들인 이후로 그의 놀라운 은혜를 끊임없이 받고 있다.

나의 네 번째 책이 되는 이 책, 2판을 집필하는 동안 지속적인 인내와 이해로 나를 지원해준(마치 초판에서는 충분하지 않았던 것 같다!), 내 삶의 빛이자 진정한 사랑인 테리(Terri)와 아름다운 딸 카일리(Kylie)에게 감사하고 싶다. 내 마음속의 문구들을 '종이'에 옮기기 위해서 허공을 바라보며 고민하는 모습에 가족 모두가 궁금했을 것이라는 걸 알지만, 나같이 일밖에 모르는 사람과 살고 있는 이 멋진 두 여인에게 마음을 전하기가 쉽지 않다.

이 책 제 2판을 위해서 기술 편집자를 맡는데 동의해 주었고 훌륭한 작업이 되도록 앞장서서 노력해준 오간 케이시(Eoghan Casey)에게 무한히 감사한다. 책을 작성하거나 분석을 수행하는데 있어서 한가지 위험한 점은 종종 핵심에서 벗어나거나 엉뚱한 곳에서 헤매게 된다는 것이다. 그러나 오간은 내가 이 책에 전념할 수 있게 해주었으며, 적어도 그런 일들이 나에게는 일어나지 않았다. 다만 유감스러운 것은 시간이 부족해서 오간의 제안들을 충분하게 이행하지 못했던 것이다. 하지만 이런 제안들을 다음 작업에는 포함시킬 것이다.

또한 이러한 성과에 기여해 준 다른 많은 사람들에게 감사하고 싶다. 브렛 셰이버즈(Brett Shavers)와 그의 아들에게 특별히 감사하는데, RegRipper 및 관련 도구들에 대한 소개 사이트인 RegRipper.net(그리고 이 사이트에 대한 로고를 제작)을 관리해 주었다. 맷 셰넌(Matt Shannon)을 만난 이후로 F-Response 제작에 대한 독창성은 물론이고 삶에 대한 전망과 그의 사업 방식 및 그가 나에게 제공한 통찰력과 조언은 나에게 영감을 주었다. 애런 월터즈(Aaron Walters)는 나를 끊임없이 놀라게 하는 정말 영리한 사람 중에 한 명이다. 맷처럼 그 역시 닮고 싶은 한 사람이며 똑똑하고 열정적이다. 그들이 원하는걸 함께 하기에 충분한 시간은 없었지만 그들이 하고 싶은 것은 놀라운 것이었다. 애런과 함께 일하는 브렌던 돌란-개빗('Moyix' , Brendan Dolan-Gavitt)도 2008년에 만났던 정말 영리한 사람중의 한 명이다.

첫 번째 책을 집필한 이후로 제니퍼 콜드(Jennifer Kolde)에게 감사하지 않고는 다른 글을 작성할 수

없었다. 그녀는 인내심을 가지고 『윈도우즈 포렌식과 사고 복구(Windows Forensics and Incident Recovery)』의 괴로운 교정 과정을 통해서 나에게 많은 것을 가르쳐 주었다. 나는 제니퍼가 검토할 수 있도록 8페이지 분량의 원고를 보냈었으며, 제니퍼가 많은 것을 교정한 이후에 그것을 수정하게 되었을 때에 '내가 정말 이것을 작성했었나? 장난하는 거지!' 라고 스스로 생각했던 것이 생각난다.

SANS 협회를 통해 커뮤니티에 기여한 모든 것은 물론이고 내가 수행했던 것들, 우승자가 된 것에 대해서 롭 리(Rob Lee)에게 아주 많이 감사하고 있다. 2008년 봄에 '이렇다면 좋지 않겠어……' 라고 ripXP(이 책의 4장에서 논의됨)에 대한 아이디어를 떠오르게 해준 것이 바로 롭이다.

매기 그레이스 홀브룩(Maggi Grace Holbrook), 그녀가 나를 위해 해준 모든 일에 감사한다-단지 듣기만 하는 것이 아니라 실제로 내 도구들을 사용해 보았고 나의 부족한 노력들을 인정해주기 위해 많은 시간을 내주었다. 초기에 우리가 만나고 얼마 지나지 않아 매기 그레이스는 친절하게도 나에게 감사 편지를 작성해 주었다. 이런 커뮤니티에서 누군가가 '감사합니다' 라고 말하는 것은 흔한 일이 아니다. 또한 매기 그레이스는 기꺼이 권한 밖의 일들을 해주었으며, 그것에 대해서도 한없이 고맙게 생각한다.

제시 콘블럼(Jesse Kornblum)의 해시 도구인 FRED부터 그가 집필한 많은 문서들까지 컴퓨터 포렌식 분석 분야에 대한 그의 많은 기여에 대해서 감사하고 싶다. 코리 알싸이드(Cory Altheide)에게도 감사하고 싶다. 그는 아주 오래 전에 USB 이동식 저장 장치를 사용할 경우 윈도우즈 시스템에 남겨지는 흔적들을 추적하기 위한 아이디어로 인해서 가까워졌다. 안드리아스 슈스터(Andreas Schuster)가 일찍이 윈도우즈 메모리 분석 분야에 기여 했던 것을 알고 있으며, 그 분야에 대한 지금과 앞으로의 많은 기여에 대해서도 감사하고 싶다. 이 분야에 여러 방면으로 기여해준 forensickb.com 블로그의 관리자인 랜스 뮬러(Lance Mueller), 콜로라도 레이크우드 경찰청의 돈 루이스(Don Lewis), 몬테나주 범죄 수사부 컴퓨터 범죄 담당요원 지미 웩(Jimmy Weg), HBGary 사의 CTO인 리치 커밍스(Rich Cummings)를 포함한 여러 사람들에게 그들의 도구를 볼 수 있도록 허락해준 것에 대해 이 책을 빌어 감사하고 싶다.

저자 소개

할랜 카비(Harlan Carvey, CISSP)는 북부 버지니아/메트로 DC 외각에 기반을 둔 컴퓨터 포렌식 및 사고 대응 컨설턴트이며, 호평을 받았던 『Windows Forensics and Incident Recovery』의 저자이기도 하다. 최근에는 긴급 사고 대응과 컴퓨터 포렌식 분석 서비스를 미국 전역의 고객에게 제공하고 있다. 특히 그의 전문 분야는 윈도우 2000과 이후 버전의 플랫폼에서 사고 대응, 레지스트리 및 메모리 분석, 그리고 사후 컴퓨터 포렌식 분석에 초점을 맞추고 있다. 상근 보안 기술자 그리고 취약점 평가 및 침입 테스트 수행 컨설턴트로서의 경력을 가지고 있으며, 이 밖에도 사고 대응 및 컴퓨터 포렌식 서비스를 통해 연방 정부 기관도 지원하고 있다.

기술 편집자

오간 케이시(Eoghan Casey)는 cmdLabs의 공동 설립자로 『Digital Evidence and Computer Crime』의 저자이자 『Malware Forensics』의 공동 저자이며, 10년 넘게 사건 처리 및 디지털 포렌식 업무의 발전을 위해 헌신하고 있다. 그는 범 국제적인 네트워크 침입을 포함한 광범위한 조사에서 조직의 보안 침해를 다루며 디지털 증거를 분석하도록 도와주고 있다. 민-형사 사건들에서 증거 입증 및 전문가 의견서를 제출하며, 컴퓨터 포렌식 및 사이버 범죄 사건에 대한 법적 증거물을 작성하기도 한다.

오간은 전자우편과 파일 서버, 모바일 장치, 백업 테이프, 데이터베이스 시스템과 네트워크 로그를 포함한 수많은 포렌식 검사와 수집, 그리고 취약점 평가를 수행했고, 침입 탐지 시스템, 방화벽 및 공개키 기반구조를 배포하고 유지 보수했으며, 다양한 조직을 위한 교육 프로그램 및 절차, 정책을 개발했다. 또한 그는 존스 홉킨스 대학교 정보 보안 연구소에서 대학원생들을 가르치고 연구를 수행하고 있으며, 『Handbook of Digital Forensics and Investigation』의 편집자이자 Elsevier 출판사의 『International Journal of Digital Investigation』의 주 편집자이기도 하다.

기술 리뷰어

트로이 라슨(Troy Larson)은 마이크로소프트 네트워크 보안팀의 선임 포렌식 기술자로 마이크로소프트 기술에 대한 포렌식 업무를 수행하며 새로운 기술들을 분석하는 것을 즐긴다. 윈도우와 오피스에서 수반되는 포렌식 문제에 대한 강연자로 자주 활동하며, 최근에는 비스타와 오피스 2007에 대한 포렌식 기술의 개발에 중점을 두고 있다. 트로이는 마이크로소프트 포렌식 팀에 합류하기 전에 Ernst&Young의 국제 포렌식 업무 및 Attenex 사에서 근무했다. 워싱턴 주 법조계의 회원이며, 버클리의 캘리포니아 대학에서 학사 및 법률 학위를 받았다.

롭 리(Rob Lee)는 정보 보안 및 포렌식 컨설턴트로 포춘 500대 기업과 미국 정부에 서비스를 제공하고 있으며 사고 대응 및 침입 탐지, 취약점 발견 등 컴퓨터 포렌식 분야에 13년이 넘는 경력을 가지고 있다. 미 공군 사관학교를 졸업했으며 정보 운영에 초점을 맞춘 첫 미군 작전 부대인 609 정보전 소대의 창단 일원으로 복무했다. 이후에 공군 특수 수사대의 일원이 되어 컴퓨터 범죄 수사 및 컴퓨터 포렌식을 수행했다. 현재의 컨설턴트 업무를 수행하기 전에는 다양한 정부 기관의 계약 업무를 수행하면서 취약점 발견팀을 위한 기술 책임자, 사이버 포렌식 부서를 위한 계약 책임자, 그리고 보안 소프트웨어 개발팀의 수장을 역임했다. 또한 SANS 연구소의 포렌식 교육 과정의 의장 및 연구원으로서 개인적으로 9년간 8000명 이상의 포렌식 및 사고 대응 전문가들을 양성했다. 또한 베스트셀러인 『Know Your Enemy, 2nd Edition』의 공동 저자이기도 하다. SANS 연구소에서 보안 컨설턴트로 근무하면서도 워싱턴 DC의 조지타운 대학교에서 MBA를 마쳤다.

랜스 뮬러(Lance Mueller, CISSP, GCIH, GREM, EnCE, CFCE, CCE)는 BitSec Forensics 사의 공동 소유주이고 전세계적으로 컴퓨터 포렌식 수사를 수행하며, 추가적으로 지역, 주, 연방 경관에게 컴퓨터 포렌식을 가르친다. 15년간의 법 집행 경력 동안에 컴퓨터 포렌식 검사를 수행하는 컴퓨터 포렌식 태스크포스(task force)에 임명되어 복잡한 침해 조사도 수행했었다. 남미와 동남아시아 및 아프리카의 외교안보부, 미 국무부의 수석 컨설턴트로서 국제 사법 기관 및 정부 기관이 사이버 테러리즘 및 사이버 범죄에 관련된 사고를 조사하고, 예방하고, 탐지하는 데 필요한 기술들을 습득할 수 있도록 선임 컨설턴트로서 지속적인 기여를 해왔다.

역자 서문

아직도 많은 사람들에게 디지털 포렌식은 생소한 분야일 것이다. 하지만 일상에서 흔하게 접하고 있는 분야이기도 하다. 예를 들어, 공용 컴퓨터에서 설치되거나 삭제된 프로그램을 찾으려고 하거나, 사용하던 프로그램에서 발생한 오류의 원인을 확인하거나, 각종 로그 파일을 열어서 동작 상태를 점검하는 각각의 과정들이 바로 디지털 포렌식에서 사용되는 기본적인 분석 절차의 일부분이다. 이러한 과정을 한번이라도 경험했던 독자라면 이미 이 책을 읽기 위한 모든 준비는 마친 것이다.

저자의 경험에서 나오는 많은 사례들과 절차 그리고 기법들은 기존에 미쳐 몰랐던 윈도우즈 자원의 활용 방법과 체계적인 분석 및 대응 기술들을 알려줄 것이다. 이는 실무를 수행하고 있는 보안 전문가에게도 해당되는 내용들이다. 저자인 할랜 카비가 말하고 있는 것처럼 모든 상황에 통용될 수 있는 하나의 해결책은 존재하지 않는다. 하지만 최선의 방법을 찾을 수 있는 훌륭한 사례들은 이 책 안에 존재하고 있다.

마지막으로, 도움을 주신 모든 분들에게 감사의 인사를 전하고자 합니다. 함께 작업 해주신 정명주 과장님, 많은 도움을 준 유학파 이동성 과장님, 매일같이 고생하는 생산도구개발 팀원들과 이기현 팀장님, 내가 만난 가장 스마트한 개발자인 권용식 과장님, 그리고 보안과 개발에 대한 열정을 깨워준 안철수연구소 핵쉴드 팀원들과 이호웅 팀장님, 책의 완성도를 높이기 위해서 고생하신 김범준 실장님 모두에게 감사의 마음을 전합니다.

번역을 진행하면서 많이 소홀했던 경천과 이현에게 사랑한다는 말로 다시 한번 미안함 마음을 대신하려고 합니다. 감사합니다.

– 정상민

'쉽지 않아……' 이 책을 번역하는 동안 가장 많이 내뱉은 말이다. 예상은 했지만 읽는 것과 번역을 한다는 것에는 생각보다 많은 차이가 있었다. 특히 용어 선정에 있어 가급적이면 한글로 표현을 하고자 했는데, 오히려 어색하게 느껴질까 걱정이 된다.

이 책은 윈도우즈 포렌식 분석에 관심이 있거나 포렌식 분석을 시작하려는 분들이 반드시 읽어야 하는 필독서인 책이다. 역자가 악성코드 분석을 하면서 실무에서 사용하던 방법과 툴들을 이 책에서 아주 상세히 소개하고 있으며, 포렌식 방식으로 어떻게 접근해야 하는지를 자세히 보여주고 있다. 이미 리버싱이나 해킹에 대한 충분한 지식이 있는 분들에게는 특별히 기술적인 부분에 있어서는 새로운 것이 없으리라 생각된다. 하지만 포렌식 분석 및 접근에 대한 다양한 기술을 습득하고 정리하는 차원에서 한번쯤은 읽어봐도 많은 도움이 될 것이라 믿어 의심치 않는다. 이 책을 읽고 포렌식 분석에 대한 이해를 바탕으로 깊이 있는 리버싱을 학습한다면 훌륭한 보안 전문가가 될 수 있을 것이다.

번역을 제안하여 많은 고생을 한 정상민 과장, 초벌 감수를 해준 이동성 과장과 생산도구개발팀 팀원들에게 고맙다는 말을 전하고 싶다. 항상 곁에서 지켜봐 주시고 응원해 주시는 부모님과 처가 부모님께 지면을 통해서나마 감사의 마음을 전한다. 얼마 전에 태어나 무럭무럭 잘 자라고 있는 우리 아들 승호야! 항상 건강하게 꽃미남으로 자라렴. 끝으로, 언제나 남편을 믿고 사랑해주는 엄공주 혜민이에게 이 말을 전하고 싶다. '사랑한다.'

– 정명주

역자 소개

정상민 CISA(http://blog.naver.com/iwillhackyou)

금융 시스템 및 다양한 보안 제품들을 개발하였으며, 핵쉴드의 핵심 개발자로 많은 기술 특허들을 출원하였다. 안철수연구소 선임연구원을 거쳐 현재 NHN에 근무하고 있으며, 기술혁신센터에서 다른 개발자들을 위한 통합 개발환경을 프로그래밍하고 있다. 저서로는 『애플리케이션 해킹』이 있다.

정명주

부푼 꿈을 안고 실리콘 밸리에서 데이터 웨어하우징 제품을 개발하였으나 쓰디쓴 고배를 마시고 안철수연구소에 입사하게 된다. V3 개발 및 분석팀에서 악성코드 분석에 매진하다가 현재는 NHN에서 기획자, 개발자들이 사용하는 토탈 솔루션 개발에 몰두하고 있다.

차례

제2장 실시간 대응: 데이터 분석 61

제3장 윈도우즈 메모리 분석 85

제4장 레지스트리 분석 147

제5장 파일 분석 241