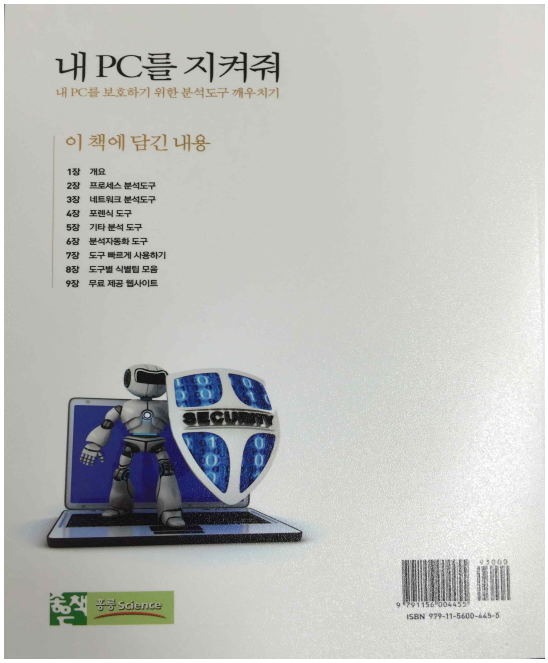

소 개

본 도서는 18종의 악성코드 분석 도구를 기술하고 있다. 도구들은 크게 프로세스 분석 도구, 네트워크 분석 도구, 포렌식 도구 및 기타 도구, 자동화 도구로 나누었다.
각 도구를 기술하기 위한 세부 목차는 크게 악성코드 식별 도구 소개, 악성코드 식별을 위한 도구 기능 설명, 도구 실습 내용을 기술하고 있다. 악성코드 식별 도구 소개는 도구의 정의, 특징, 주요기능 소개, 다운로드 받을 수 있는 URL 주소, 메인화면 메뉴, 주요 기능 등을 기술하였다. 주요 기능의 경우 악성코드 식별 기능 혹은 관련된 기능을 위주로 기술하였으며 식별에 도움이 되는 "***식별팁***"을 넣었다. 또한 도구를 빠르게 사용할 수 있도록 "***도구 빠르게 사용하기***"와 "***식별팁 모음***"을 기술하여 책을 전부 읽지 않고도 편리하게 사용 가능하도록 구성하였다.

또한 분석 도구를 무료로 제공하는 사이트 정보와 무료로 악성코드 정보를 제공하는 웹사이트를 기술하여 추가적인 정보를 참고할 수 있도록 기술하였다.

목 차

미리보기

클릭

서 평

원동호(현 성균관대학교 행단석좌교수, 제7대 정보보호학회 회장, 국가정보화추진위원회 자문위원)

기존의 악성코드 분석에 대한 책들은 전문가 위주의 어려운 내용인데 반해 이 책은 분석 도구 화면을 캡쳐하고 그 실행 순서와 기능을 설명하여 누구나 쉽게 따라할 수 있도록 기술하였다. 특히, 이 책의 "제7장 도구 빠르게 사용하기", "제8장 악성코드 식별팁 모음"은 쉽고 빠르게 악성코드를 식별할 수 있도록 내용을 기술하여 초보자도 쉽게 악성코드를 식별 및 분석할 수 있을 것으로 보인다.

또한 이 책에서 다루고 있는 분석도구들은 대부분 무료로 사용할 수 있어서 국가공공기관 전산 및 보안 담당자뿐만 아니라 보안에 관심이 있는 중/고/대학생들도 이 책을 참고하여 공부하면 악성코드 분석 도구들을 잘 다룰 수 있을 것으로 생각한다.

임종인(현 고려대학교 정보보호대학원 교수, 제15대 정보보호학회 회장, 전 대통령비서실 안보특별보좌관)

우리 사회는 '제4차 산업혁명'을 맞이하고 있다. 제4차 산업혁명의 핵심은 초연결 사회 기술로 우리를 구성하는 모든 디바이스들이 IT 기술과 결합하여 자동으로 통신을 하고 가치를 창출하는 것이다. 이러한 사회 변화에서 가장 주의해야 할 역기능은 바로 보안 위협이다. IT 기술들은 다양한 취약점을 가지고 있으며, 이를 노리는 보안 위협들은 점차 증가하고 있다. 다양한 기업과 기관들은 지능형타깃지속공격의 피해를 받고 있으며, 최근에는 랜섬웨어의 확산 등에 따라 개인 사용자들 역시 피해를 입고 있다.

보안 위협에 대응하기 위한 정보보호 기술 역시 함께 발전해왔다. 본 도서는 PC 보안을 위한 대표적인 18종의 분석 도구들을 총망라하여 이를 활용할 수 있는 방법을 제공하고 있다. 이 분석도구들은 모두 실제 보안 환경에서 널리 활용되는 도구들로, 쉽게 접할 수 있는 도구들이다. 이러한 분석 도구들을 적절히 잘 활용한다면 단기간 내에 보안에 대한 전문지식과 실전 역량을 배양할 수 있을 것이다. 본 도서는 이 분석도구들을 처음 접하는 사람들도 누구나 쉽게 활용할 수 있도록 활용법과 팁을 자세히 설명하고 있다. 본 도서는 보안에 대한 공부를 시작하는 학생들과 해당 분야의 실무를 처음 접하는 보안 담당자들에게는 최고의 길라잡이가 될 것이라 생각한다.

김광호(현 국가보안기술연구소장, 현 한국정보보호학회 고문)

최근 북한을 비롯한 적대적 해커집단으로 부터의 사이버 위협이 끊임없이 발생하고 있는 현실입니다. 그러나 정부 및 공공기관 담당자의 경우, 각종 해킹사고에 대한 체계적이고 적절한 대응 교육 및 훈련 부족으로 내 PC가 위험에 노출되어 있는지 조차 판단하기 어려운 상황입니다. 이러한 시점에서 초보자도 쉽게 이해할 수 있는 가장 기본적인 교재가 출간된 것을 매우 기쁘게 생각합니다. “내 PC를 지켜줘”가 우리나라의 사이버 공간을 안전하게 지킬 수 있는 시금석이 되기를 기대합니다.

책 정보

출판사 : 홍릉과학출판사
발행일(출간일) 2016년 06월 26일
저자 : 양진석, 엄정호, 김인중, 정태명
ISBN-13(ISBN-10) : 9791156004455 (1156004454)
페이지수 : 172쪽(풀컬러)
크기 : 188*256mm

관련 링크

- 단체구매(10권 이상 구매시) : 정가의 80%, 구매처 : 홍릉과학출판사(02-999-2274~5)
- 개인구매 : 서점 및 아래 링크 참조하세요.

1. 교보문고
http://www.kyobobook.co.kr/product/detailViewKor.laf?mallGb=KOR&ejkGb=KOR&linkClass=330303&barcode=9791156004455

2. 인터파크 도서
http://book.interpark.com/product/BookDisplay.do?_method=Detail&sc.shopNo=0000400000&dispNo=&sc.prdNo=255575366&sc.saNo=002001023001

3. 예스24
http://www.yes24.com/24/goods/29214493

4. 반디앤루니스
http://www.bandinlunis.com/front/product/detailProduct.do?prodId=3970615

* 본 도서 정보는 사이버보안에 관심이 있는 분들의 교육 및 훈련에 대한 이해 증진을 위해 제공하는 정보이며, 사이버안전훈련센터에서 제공하는 교재가 아님을 알려드립니다.