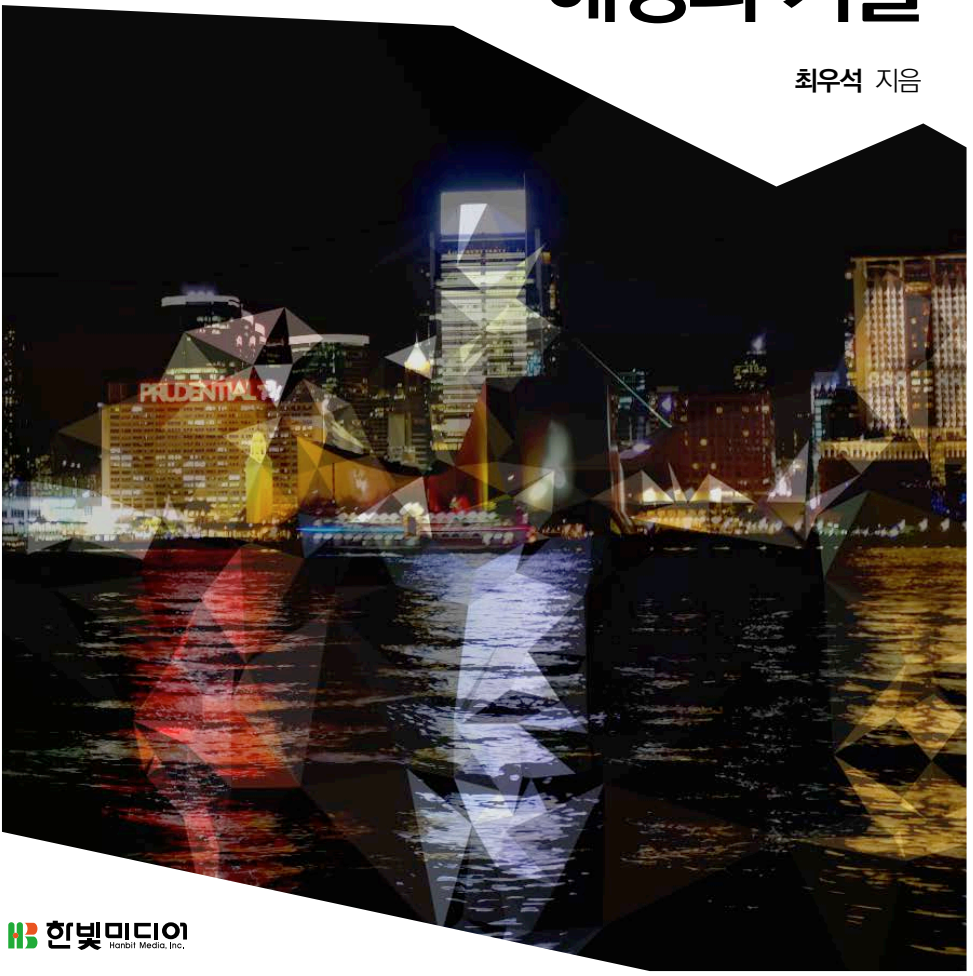
Hanbit RealTime 135

DBD 공격과 자바스크립트 난독화로 배우는 해킹의 기술

최우석 지음



한빛미디어 Hanbit Media, Inc.

DBD 공격과 자바스크립트 난독화로 배우는 해킹의 기술

최우석 지음

한빛미디어
Hanbit Media, Inc.

표지 사진 **김현용**

이 책의 표지는 김현용님이 보내 주신 풍경사진을 담았습니다.
리얼타임은 독자의 시선을 담은 풍경사진을 책 표지로 보여주고자 합니다.

사진 보내기 **ebookwriter@hanbit.co.kr**

DBD 공격과 자바스크립트 난독화로 배우는 해킹의 기술

초판발행 2016년 8월 5일

지은이 최우석 / **펴낸이** 김태헌
펴낸곳 한빛미디어(주) / **주소** 서울시 마포구 양화로7길 83 한빛미디어(주) IT출판부
전화 02-325-5544 / **팩스** 02-336-7124
등록 1999년 9월 30일 제10-1779호
ISBN 978-89-6848-827-6 95000 / **정가** 14,000원

총괄 전태호 / **책임편집** 김창수 / **기획·편집** 정지연
디자인 표지 강은영, 내지 여동일, 조판 최송실
마케팅 박상용, 송경석, 변지영 / **영업** 김형진, 김진불, 조유미

이 책에 대한 의견이나 오탈자 및 잘못된 내용에 대한 수정 정보는 한빛미디어(주)의 홈페이지나 아래 이메일로 알려주십시오.
한빛미디어 홈페이지 www.hanbit.co.kr / **이메일** ask@hanbit.co.kr

Published by HANBIT Media, Inc. Printed in Korea
Copyright © 2016 최우석 & HANBIT Media, Inc.
이 책의 저작권은 최우석과 한빛미디어(주)에 있습니다.
저작권법에 의해 보호를 받는 저작물이므로 무단 복제 및 무단 전재를 금합니다.

지금 하지 않으면 할 수 없는 일이 있습니다.
책으로 펴내고 싶은 아이디어나 원고를 메일(ebookwriter@hanbit.co.kr)로 보내주세요.
한빛미디어(주)는 여러분의 소중한 경험과 지식을 기다리고 있습니다.

2011년 겨울, 대구에서 친구들과의 술자리에서 한 친구가 꺼낸 "지방의 개발자로 남고 싶지 않아서 서울에 올라가 정보보안 분야 학원에 다니려고 해."라는 말에 공감해 서울로 함께 상경해 정보보안을 시작했다. 흔히 찾는 학원이 아닌 (주)한국정보보호교육센터를 선택해 40기로 이수했고, 같은 교육 센터 선배의 요청으로 2012년 (주)트라이큐브랩에 입사했다.

(주)트라이큐브랩 연구소에서 분석 업무를 시작으로 정보보안 실무를 시작했다. 첫 정보보안 실무가 드라이브-바이 다운로드 공격의 분석이었고, 추가로 연구한 것이 분석한 정보를 가공하기 위한 파이썬 오픈소스 도구의 기능과 아이디어 연구였다. 분석 정보와 연구한 오픈소스는 별도로 운영하는 분석 서버의 기능으로 추가됐다. 그 2년의 세월 동안 회사에서 밤새고, 자고, 주말, 휴가, 명절에도 공부하고 정리하며 사수를 괴롭혔다.

이렇게 주경야독하는 중에 잘했다고 생각하는 활동 두 가지가 있다. 바로 커뮤니티 활동과 블로그 활동이다. 교육센터에서 열심히 공부할 때 '선배와의 대화' 시간에 이야기를 나눈 한 분이 보안프로젝트 운영자 조정원 선배로, 이 선배를 통해 공유의 중요성을 알게 되어 커뮤니티에 참여하게 됐다. 블로그는 사회공헌을 목적으로 운영하기 시작했는데, 주경야독하는 과정에서 고통스러웠던 고민을 공개하면 누군가에게 도움이 되지 않을까 생각했다. 또한, 미래의 내가 똑같은 문제를 만났을 때 다시 참고할 수 있는 자료가 되리라 생각했고, 이 모든 것이 현재의 나에게 긍정적인 영향을 주고 있다.

커뮤니티와 인연으로 『칼리 리눅스와 백트랙을 활용한 모의해킹』[01] 『파이썬 오픈소스 도구를 활용한 악성코드 분석』[02]을 공동 집필했다. 필자의 필명과 아이디는 하카와티

01 조정원, 박병욱, 임종민, 이경철, 최우석 공저(2014). 에이콘출판사

02 조정원, 최우석, 이도경, 정지훈 공저(2015). 에이콘출판사

hakawati를 사용한다. 이는 서울에 상경해 고시촌에서 생활할 때 함께 올라온 대학 친구들과 같이 공부하기 위해 들렀던 카페 이름이기도 하고 아랍어로 '이야기꾼'이라는 뜻을 가지고 있어, 정보보안을 이야기하는 담소꾼이 되자는 의미로 사용하기 시작했다. 필자의 블로그(www.hakawati.co.kr)도 하카와티로 도메인을 등록해 사용하고 있다.

현재는 (주)한국정보보호교육센터의 부설연구소 F-NGS를 총괄하고 있다. 연구소 운영을 위한 프로세스를 만들고, GHOST 취약점 분석, 크립토락커CryptoLocker 분석, 해킹팀 정보유출 사건 분석 등 이슈와 관련된 분석을 진행했다. 새로운 교육과 컨설팅 방법론을 연구하기도 하며, 때론 강의와 모의해킹 컨설팅을 병행하기도 한다. 연구소를 총괄하면서 새로운 패러다임보다는 정보보안의 모든 정보를 담고 활용할 수 있는 데이터베이스를 만드는 것을 목표로 하고 있다.

개인적으로 관심 있는 분야는 침투 테스트다. 다양한 환경을 구축하고, 침투 테스트를 기술적 관점에서 접근하여 표준 기술 가이드라인을 만드는 것을 생각하고 있다. 거대한 프로젝트라서 완성된다면 침해사고 대응, 포렌식 등 다양한 방어 기법으로 확장 연구를 진행할 예정이다. 그 외 흥미가 있는 분야는 ICT 신기술로, 기계학습과 빅데이터, 이들을 이용한 데이터 분석과 가공 방식이다. 이 글을 작성할 때 이세돌 9단과 알파고의 바둑 경기로 가슴이 두근거렸다.

지은이 **최우석**

감사의 말

이 책을 집필하는 데 많은 분이 도움을 주셨다. 이분들이 없었으면 이 책을 출판하기가 매우 어려웠을 것이라 생각한다.

- 정보보안 삶의 기틀을 마련해주신 (주)한국정보보호교육센터 서광석 원장님
- 정보보안 삶의 정신적 지주이신 故 천성훈 소장님
- 정을 베푸시고 직원을 사랑하시는 (주)트라이큐브랩의 이석현 대표님과 어디에 있든 응원해주시는 안용태 부사장님
- 항상 기술 공유하고 토론하는 도반이자 평생의 사수 남석우 선배
- 집필에 도움을 주시고 새로운 정보와 아이디어를 제공해주시는 보안프로젝트 조정원 선배
- 함께 회사의 미래를 구상하고 현실화하기 위해 고민하시는 (주)시큐리티허브 대표 이경빈 선배
- 이 책을 쓰기 위해 함께 머리를 맞대고 고민해준 서준석 선배
- 다른 지역에서 생활하는 아들이자 동생을 걱정하고 챙겨주시는 아버지, 어머니, 누나 그리고 매형

지켜봐 주시고 응원해주시며 따끔한 충고도 서슴없이 해주시는 많은 분께 다시 한 번 감사드린다.

몇 권의 책을 공동 집필한 후 책 쓰는 것에 욕심이 생겨서 가장 오랫동안 연구하고 분석해 온 드라이브-바이 다운로드DBD, Drive-by Download를 집필하기 시작했다. 하지만 이 주제를 선정하고 집필하려니 여러 가지 고민이 생겼다.

드라이브-바이 다운로드 공격에 사용하는 필수적인 공격 기술에는 웹 해킹, 소프트웨어 취약점, 악성코드가 있는데, 이들은 각각 독립적인 주제로 책을 쓸 수 있을 만큼 많은 내용을 담고 있다. 자칫 특정 주제에 집중하게 되면 이 책에서 이야기하려는 주제와 거리가 멀어질 것 같았다. 그래서 편향되지 않게 드라이브-바이 다운로드 공격에 집중하고, 이 공격에서 만날 수 있는 자바스크립트 난독화와 해제 방법을 중심으로 책을 집필하기로 했다.

필자는 2012년부터 2014년까지 드라이브-바이 다운로드를 집중적으로 분석하고 연구해왔다. 처음 이 공격을 만났을 때는 자바스크립트 난독화 때문에 힘들었다. 자바스크립트 난독화를 분석한 후 추적하고 정리해야 회사가 원하는 드라이브-바이 다운로드 유포 구조도를 그릴 수 있고 대고객 서비스를 할 수 있었기 때문이다. 자바스크립트 난독화의 분석과 해제에 익숙해졌을 때 드라이브-바이 다운로드 공격 구조에 대한 호기심이 생겼고, 그 구조를 구성하는 범죄 그룹에 관심을 가지기 시작했다.

우리가 드라이브-바이 다운로드를 구현하는 공격자라면 어떤 일을 해야 할까? 먼저 사용자들이 자주 방문하는 웹 사이트를 해킹해 웹 서버에 침투하고, 소스 코드를 수정해 드라이브-바이 다운로드 구조를 만들 것이다. 이 구조에는 악성코드를 자동으로 다운로드하고 실행하도록 취약점을 사용하며, 유포하기 위한 악성코드가 백신 제품들에 탐지되는지 확인한 후 배포할 것이다. 또한, 구조 사이마다 트래픽 애널리틱스Traffic Analytics라는 기술로 웹 서비스에 방문하는 사용자의 정보를 수집해 좀 더 효율적인 악성코드 유포를 위한 통계를 낼 것이다.

하지만 이 많은 일을 혼자서 해낼 수 있을까 생각하면 선뜻 대답하기 어렵다. 결국 드

라이브-바이 다운로드는 한 사람이 모든 공격을 수행하는 것이 아니라 조직 구성이 필요하다는 생각을 하게 됐다. 이러한 생각들을 종합해서 정리한 이 책의 구성은 다음과 같다.

'1장 드라이브-바이 다운로드'에서는 드라이브-바이 다운로드의 개념을 이해하고, 이 공격이 대중화된 배경을 이해하기 위해 해킹 공격의 역사를 통해 온라인 지하 산업경제의 발생 배경을 살펴본다. 그리고 드라이브-바이 다운로드와 관련된 용어와 국내·외 드라이브-바이 다운로드 사례, 다양한 응용 공격을 살펴본다.

'2장 드라이브-바이 다운로드 공격 실습'에서는 드라이브-바이 다운로드 공격을 시나리오 기반으로 직접 구축하여 공격자들이 드라이브-바이 다운로드 공격을 하기 위해 행하는 동작들을 이해하고 이 동작 원리를 체험해본다.

'3장 자바스크립트와 자바스크립트 난독화'에서는 자바스크립트의 특징을 살펴보고, 드라이브-바이 다운로드에서 사용하는 다양한 자바스크립트 난독화를 소개한다.

'4장 자바스크립트 난독화 해제 방법 및 실습'에서는 다양한 자바스크립트 난독화들을 분석하고 필자가 제시하는 난독화 해제 방법들을 소개한다.

'5장 마무리'에서는 대응 방안과 드라이브-바이 다운로드와 관련된 추가 정보들 그리고 필자의 생각을 이야기하며 이 책을 마무리한다.

'6장 부록'에는 '2장 드라이브-바이 다운로드 공격 실습'에서 진행하는 가상머신 및 운영체제 설치 과정을 별도로 수록했다.

필자는 이 책의 모든 내용을 다 읽어야만 한다고 생각하지 않는다. '2장 드라이브-바이 다운로드 공격 실습'부터 살펴보고 '1장 드라이브-바이 다운로드'를 이해하는 것도 좋다. 따라서 가장 궁금한 부분만 골라 읽고 관심과 흥미가 생겼을 때 다른 부분을 읽어보는 것이 어떨까 싶다.

이 책의 대상 독자

드라이브-바이 다운로드 공격은 현업에 있는 분들이라면 자주 접할 것이다. 백신 회사라면 악성코드 유포의 근원지를 차단해 업무의 양을 줄이거나 고객의 PC를 안전하게 보호하는 과정에서 만날 수 있다. 사이트 관제에서는 고객사 사이트에서 악성코드가 유포되면 드라이브-바이 다운로드 구조에 맞게 대응을 수행하고, 침해사고 대응에서는 침해당한 웹 서버나 감염된 PC를 분석하는 과정에서 이 공격을 만나볼 수 있으며 공격당한 원인을 분석해 문제점을 개선할 수 있다. 그 외 흔하진 않지만, 일부 연구소에서 이 공격을 탐지하고 분석하고 통계 내어 공격 흐름을 파악하는 형태로 연구를 진행하고, 대학교에서는 산학 협력이나 논문을 쓰기 위한 목적으로 이 공격을 연구하기도 한다.

이 책의 독자는 이처럼 사이버 공격 동향에 관심이 있는 모든 사람이 될 수 있다. 특히 APT(Advanced Persistent Threat) 공격의 공격자들이 가장 애용하는 방법인 스피어 피싱(Spear Phishing), 트로이목마화 소프트웨어(Trojanization Software), 워터링 홀 공격(Watering Hole Attack)에 관심이 있다면 말이다(여기서 워터링 홀 공격이 바로 드라이브-바이 다운로드 공격이다). 사이버 공격을 연구하고 방어하는 데 이 책이 도움이 되었으면 한다.

이 책의 예제 코드는 다음 링크에서 다운로드할 수 있다.

- http://www.hanbit.co.kr/exam/2827/

차례

chapter 1

드라이브-바이 다운로드

드라이브-바이 다운로드DBD, Drive-By Download 공격은 하나의 공격 기술만을 사용해 사용자에게 피해를 주는 공격 기술이 아니다. 그래서 필자는 이 주제로 특강을 할 때 '공격 프로세스'로 표현한다. 이러한 공격 형태는 한순간에 생겨난 것이 아니므로 '1.1 드라이브-바이 다운로드란'에서 간단하게 드라이브-바이 다운로드의 사전적 의미를 살펴보고 '1.2 정보통신 산업과 사이버 공격'에서 이 공격과 관련된 역사적 배경을 해석해 이 공격이 발생하게 된 이유를 설명한다.

드라이브-바이 다운로드 공격은 한 사람이 모든 공격을 수행하고 성공한 공격 결과를 유지하고 관리하기는 힘들다. 그래서 '1.3 온라인 지하산업경제 활성화'에서는 이 공격을 진행하는 사람들(조직)에 대한 이야기를 한다. 또한, 이 공격을 진행하는 과정과 악성코드 감염 이후에 파생되는 다른 공격들, 수익을 위해 활동하는 범죄 행위에 대해 언급한다.

다양한 산업과 학계에서 드라이브-바이 다운로드에 대한 서로 다른 구성요소의 표현을 쓰고 있어서 '1.4 드라이브-바이 다운로드 용어 정리'에서는 필자 나름대로 용어를 정리했다. '1.5 드라이브-바이 다운로드 국내 동향'에서는 실제 유포된 사례와 특정 기간 동안의 유포 기록을 추적해 드라이브-바이 다운로드의 위험성에 관해 이야기한다. 마지막으로 '1.6 드라이브-바이 다운로드 유포 기술'에서는 기본 공격에서 응용된 형태를 설명하고 각각의 형태에 맞는 시나리오를 다루어 이해하기 쉽도록 구성했다.

1.1 드라이브-바이 다운로드란

드라이브-바이 다운로드란 무엇인가? 어떤 사람은 '악성코드를 드라이브Drive로by 다운로드하는 행위'라고 해석하기도 하고, 어떤 사람은 단순히 '악성코드를 감염시키는 하나의 방법'으로 이해하기도 한다. 드라이브-바이 다운로드의 사전적 정의를 찾으려면 'Drive-By'라는 숙어의 의미를 이해해야 한다.

'Drive-By'는 '~쪽으로 자동차를 운전하다'라는 의미다. 외국 범죄 영화에서 자동차를 타고 주행하며 총격전을 벌이는 장면을 자주 볼 수 있는데, 이러한 행위를 '드라이브-바이 슛팅Drive-By Shooting'이라 부른다. 또는 일상생활에서 자주 사용할 수 있는 표현으로 '(차를 타고) 교회를 지나간다'는 의미의 'drive-by church'가 있다. 그러면 여기서 이해하고자 하는 '드라이브-바이 다운로드'는 '(컴퓨터에) 지나가듯 다운로드 행위가 발생한다'고 해석할 수 있다.

드라이브-바이 다운로드 용어의 시초는 2002년 스테파니 올슨Stefanie Olsen 기자가 쓴 기사[01]에서 살펴볼 수 있다. 당시 온라인 광고 업체는 사용자가 아무런 의심 없이 동의 버튼을 누르는 버릇을 악용해 광고 콘텐츠를 설치하도록 유도했고, 이를 '드라이브-바이 인스톨Drive-By Install' 또는 '한 번 클릭하는 선택적 설치One-Click Opt-Install'라고 표현했다. 그리고 일부 광고 업체는 사이트 방문과 동시에 사용자의 컴퓨터에 광고 콘텐츠를 다운로드하고 설치하도록 구성했고, 이 과정에 아무런 메시지를 표시하지 않는 형태로 진화했다. 스테파니 올슨 기자는 이 모든 과정을 '드라이브-바이 다운로드drive-by download'로 표현했다. 기사의 끝부분에서는 일부 성인 사이트가 방문자를 자동으로 다른 곳으로 보내어 악성코드에 감염되도록 공격했음을 언급한다. 현재는 드라이브-바이 다운로드를 '스크립트 등을 매개로 웹 사이트 방문 시 사용자의 인식(동의) 없이 자동으로 악성코드를 다운로드하고 실행하는 현상'으로 정의한다.

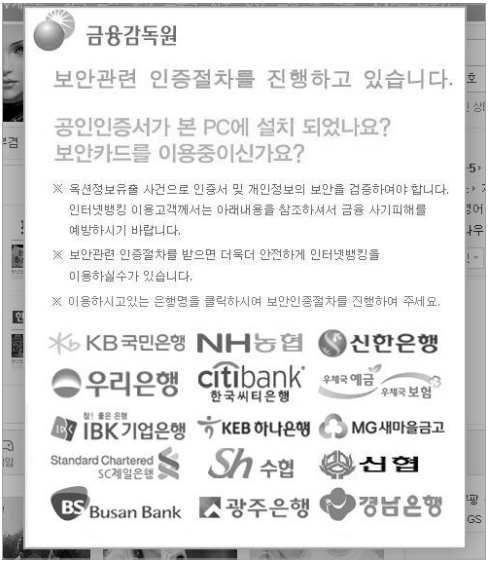
---

01 출처: www.cnet.com/news/web-surfers-brace-for-pop-up-downloads

다음 철수의 상황을 이해해보자. 여기서 철수는 별다른 행위 없이 웹 서핑만 했다.

철수는 옷을 살 때 인터넷 쇼핑몰을 자주 이용한다. 오늘도 늘 그랬듯이 검색 사이트에서 검색해 자주 방문하는 인터넷 쇼핑몰에 방문했다. 그동안 눈여겨봤던 옷을 결제하고, 다른 쇼핑몰을 이용하기 위해 다시 검색 사이트에 접속하니 조금 전에 보지 못했던 알림창이 나타났다.

그림 1-1 파밍 공격



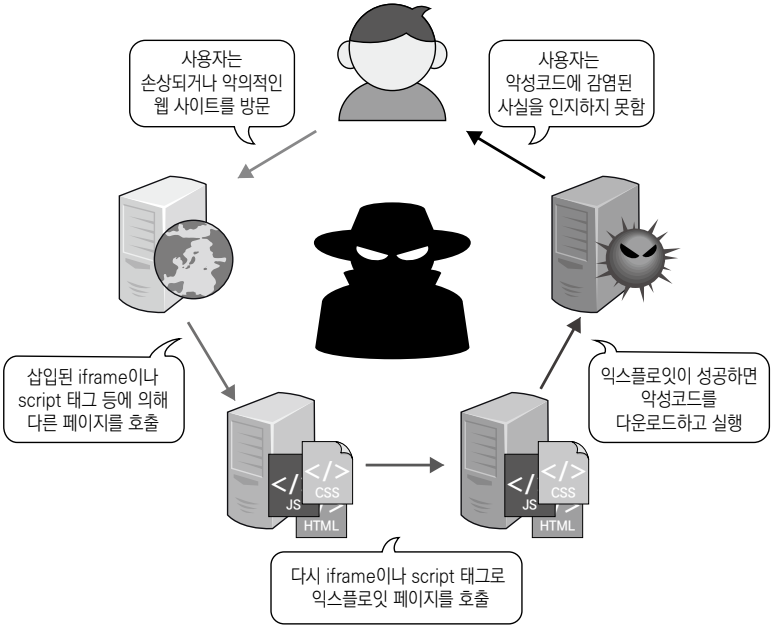
이야기를 정리해보면 철수는 처음 검색 사이트를 이용했을 때 [그림 1-1]의 알림창을 보지 못했다. 하지만 쇼핑몰 사이트에 접속해 쇼핑한 후 다시 검색 사이트에 방문하니 알림창이 나타났다. 이 상황은 철수의 컴퓨터가 악성코드에 감염됐음을 의미하고, 감염되는 과정은 철수가 알아차리지 못했다. 그럼 어떤 사이트에서 악성코드에 감염됐을까? 검색 사이트일 수도 있고, 쇼핑몰일 수도 있다. 여기서는 철수가 사이트에 접속한 것 외에 별다른 행위를 하지 않았지만, 드라이브-바이 다운로드 공격으로 파밍Pharming 형태의 악성코드에 감염된 것이 주안점이다.

NOTE **파밍이란?**

악성코드 또는 다른 공격에 의해 DNS가 변경되어 피싱 사이트로 유도하는 공격 방식을 '파밍Pharming'이라 한다. 흔히 윈도우 시스템에서는 'C:\Windows\System32\drivers\etc'에 존재하는 Hosts 파일 또는 새롭게 생성한 Hosts.ics 파일을 변조해 공격자가 구성한 피싱 사이트로 유도한다. 최근에는 레지스트리를 변조해 로컬 프락시를 설정하고, 악성코드 자체가 로컬 DNS가 되는 방식도 있다. 이 경우 악성코드의 메모리에 설정된 주소(흔히 은행 사이트들)에 접속하면 공격자가 구성한 피싱 사이트로 유도하는 형태를 가지고 있다. 또한, 공유기의 취약점을 이용해 공유기에서 설정 가능한 DNS를 피싱 사이트로 유도하게 구성하기도 한다. 사용자를 피싱 사이트로 유도하는 대부분의 국내 파밍 공격은 사용자의 금융 정보를 훔치는 것이 목적이다.

여기서 드라이브-바이 다운로드의 대표적인 특징을 알 수 있다. 웹 서핑만 해도 사용자는 악성코드에 감염되고 감염된 사실을 인지하기 어려우며, 보통 여러 사이트를 방문하므로 어떤 사이트가 원인이 되어 악성코드에 감염됐는지 알아내기 힘들다. 드라이브-바이 다운로드 공격의 핵심적인 흐름을 한번 살펴보자.

그림 1-2 드라이브-바이 다운로드 공격 흐름



먼저 공격자는 사용자가 방문하는 웹 사이트를 해킹한다. 공격자가 웹 사이트를 직접 구축해 운영할 수 있지만, 사용자가 방문하지 않는다면 공격에 의미가 없다. 많은 사용자가 방문해야 공격의 효율성을 높일 수 있기 때문에 사용자들이 자주 방문하는 웹 사이트를 해킹한다. 그래서 공격자는 사용자들이 자주 방문하는 사이트를 미리 조사하고 잘 이해한다. 예를 들면, 입학 시기에는 대학 사이트, 휴가 시기에는 여행사 사이트나 펜션 사이트가 해킹당해 드라이브-바이 다운로드로 악성코드를 유포한다.

공격자가 웹 사이트를 해킹하면 소스 코드에 '`iframe`, `script`, `meta`, `embed`'와 같은 리디렉션 코드Redirection Code를 삽입한다. 이 코드를 사용하면 사용자가 웹 서비스를 이용할 때 브라우저 내부에서는 다른 서버의 다른 파일을 호출할 수 있기 때문이다.

공격자가 삽입한 리디렉션 코드는 다른 자바스크립트 파일이나 HTML 페이지를 호출하고, 호출된 페이지에 의해 다시 한 번 다른 페이지를 요청할 수도 있으며 바로 악성코드를 유포하는 페이지를 불러올 수 있다. 호출한 페이지는 악성코드를 유포하는 페이지가 될 수 있고 악성코드를 유포하는 페이지로 전달하는 징검다리 역할을 하는 페이지일 수 있다. 경유 페이지에 방문하게 되면 충분한 징검다리를 건너 최종으로 악성코드를 유포하는 페이지에 도착하는 것이 일반적이다.

악성코드를 유포하는 페이지는 하나의 소프트웨어 취약점을 쓰기도 하고 여러 개의 소프트웨어 취약점을 사용하기도 한다. 취약점은 악성코드를 다운로드하고 실행하도록 구성되는데, 이 과정에서 당연히 다운로드하는 악성코드 주소가 포함된다. 이때 사용하는 취약점 정보와 함께 악성코드의 주소가 노출되기 때문에 이 페이지의 소스 코드를 보호하기 위해 높은 난이도의 자바스크립트 난독화를 사용한다. 고난이도의 난독화는 대부분 익스플로잇 도구Exploit Kit로 분류되는 공격 도구에 의존해 제작된다.

악성코드를 저장한 웹 서버는 공격자들이 침해한 곳이거나 직접 구축한 형태로 운영하고, 악성코드를 저장하는 곳은 공격자가 쉽게 조작할 수 있는 곳을 선택한다. 그 이유는 이미 드라이브-바이 다운로드 구조도가 완성됐다면 악성코드를 저장한 웹 서버에 똑같은 파일 이름을 가진 다른 형태의 악성코드를 덮어써서 실시간으로 다른 악성코드를 유포할 수 있기 때문이다.

과거에는 기업 서버를 직접 공격했지만, 드라이브-바이 다운로드 공격은 철저하게 사용자를 대상으로 진행하는 공격이다. 필자는 여기서 의문이 들었다. 왜 산업 기반의 서버를 공격하다가 사용자 기반으로 공격을 전환하게 됐을까? 이 의문을 해결하기 위해 공격의 흐름이 바뀌게 된 배경을 살펴보자.

1.2 정보통신 산업과 사이버 공격

드라이브-바이 다운로드 공격은 다양한 공격 기술을 하나의 공격 형태로 묶어 사용하기 때문에 매우 복잡한 공격 형태를 가지고 있다. 그러므로 이렇게 만들어지게 된 다양한 시대적 배경과 변화되는 공격의 흐름을 이해할 필요가 있다.

현재 온라인에는 헤아릴 수도 없는 많은 산업이 활발하게 운영되고 있다. 다르게 말하면 금전적 가치가 있는 많은 부분이 아니 어쩌면 거의 대부분이 컴퓨터 속 가상세계에 녹아있다. 집안 장롱 속에 현금이나 패물을 보관하던 시절에는 빈집털이도 도둑이 많았다. 금전적 가치가 있는 무언가가 어딘가에 존재할 때 범죄가 발생하는데, 이러한 이치에 따라 가상세계에 녹아있는 금전적 가치를 훔치기 위해 사이버 범죄 즉, 해킹이 발생했다.

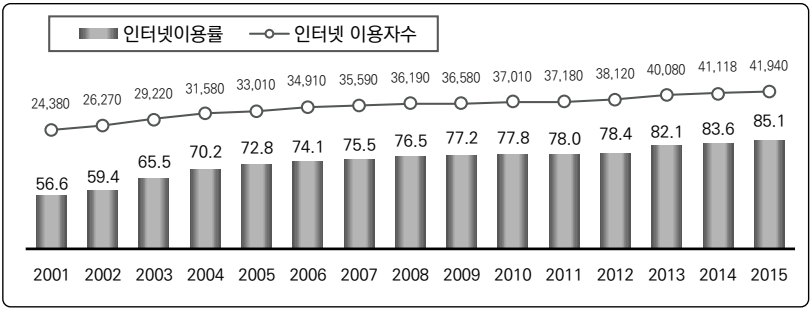
사이버 공격은 오래전부터 진행되어 왔다. 다양한 기술의 역사와 공격의 역사를 종합해 타임라인을 구성해보면 다음과 같이 핵심적인 흐름을 찾을 수 있다.

1.2.1 2000년 이전

1994년에는 인터넷을 이용한 상용 서비스가 등장했고, 1996년도에는 바람의 나라, 리니지와 같은 게임 산업이 발전하면서 많은 사용자가 인터넷으로 몰리기 시작해 지금의 인터넷 환경으로 발전한 시발점이 됐다. 물론 1998년 ADSL 기반의 초고속 인터넷 서비스, 스타크래프트와 같은 e-스포츠 대중화로 인해 등장한 PC방도 인터넷 이용자 수 증가와 인터넷 환경의 발전에 빠질 수 없는 요소다.

인터넷 이용자 수가 더욱 증가하게 된 시기는 1999년이다. 인터넷 뱅킹이 1999년에 시작되면서 온라인 금융거래가 가능해졌고, 같은 해 인터넷 포털 서비스들이 대거 등장해 많은 사용자가 인터넷을 통해 정보를 공유하고 찾기 시작했다. 또한, 싸이월드, 블로그와 같은 SNS의 등장으로 인터넷 이용자가 폭발적으로 증가했다.

그림 1-3 인터넷 이용률 및 이용자 수 변화 추이[02]



(단위: %, 천 명)

이용자가 증가함에 따라 이용자 수가 곧 수익을 창출할 수 있는 지표가 되자 기업들은 온라인에 사업 환경을 구축하기 시작했다. 그래서 공격자들은 이러한 기업을 대상으로 공격을 진행했다. 이때의 공격 방식은 APT 공격이라고 하기에는 다소 부족한 표적 공격Target Attack으로, 회사 내부에 침입해 쓸만한 정보를 절도하는 수

02 출처: 2015년 인터넷이용실태조사, 한국인터넷진흥원, http://isis.kisa.or.kr/board/?pageId=060100&bbsId=7&itemId=813&pageIndex=1(단축 URL http://goo.gl/koQm7j)

준의 해킹과 웹 페이지를 변조해 해킹 기술력을 자랑하거나 정치적 의도를 표현하기 위해 웹 사이트를 변조하는 변조 공격Modification Attack인 핵티비즘Hacktivism 형태가 주류를 이루었다.

당시는 방어 솔루션의 필요성을 인지해 활발하게 제작되던 상황이 아니어서 서버가 침투당하는 것을 막기 위해 가장 먼저 한 행동은 철저한 권한 관리였다. 관리자가 주요 시스템에 접근했을 때 일반 사용자 권한을 우선으로 부여하고, 필요에 따라 관리자 권한을 가지는 것이다. 공격자는 외부에서 접속하다 보니 당연히 사용자 권한을 부여받기 때문에 공격이 제한적일 수밖에 없다. 그래서 이 시기의 취약점을 이용한 공격은 침투한 시스템에 사용된 소프트웨어의 사용자 권한을 일반 사용자에서 관리자로 올리는 권한 상승Privilege Escalation 공격이 주류를 이루었다.

다음은 한국인터넷진흥원에서 공개한 「KISA-2000 정보시스템 해킹 바이러스 현황 및 대응」[03] 보고서의 내용으로, 언급되는 취약점들이 권한 상승을 위해 사용됐음을 알 수 있다. 그 외에는 서비스 거부 공격DoS, Denial of Service이 대부분이다.

> **KISA-2000 정보시스템 해킹 바이러스 현황 및 대응(일부 발췌)**
>
> (생략)
>
> NXT 레코드에 대한 적절한 validate를 하지 못하는 버그를 가지고 있다. 이러한 NXT 레코드 확인 작업수행 중의 버그를 이용해 외부에서 buffer를 overflow시켜 임의의 code를 수행함으로써 named를 수행하고 있는 권한에 해당하는 권한의 셸을 획득할 수 있게 된다.
>
> (생략)

03 출처: KISA-2000 정보시스템 해킹 · 바이러스 현황 및 대응, 한국인터넷진흥원, http://www.kisa.or.kr/public/library/report_View.jsp?regno=003336&searchType=&searchKeyword=&pageIndex=38(단축 URL http://goo.gl/5stUKG)

1.2.2 2000년 초

잦은 공격과 침투로 기업은 정보보안의 필요성을 인식하기 시작했다. 하지만 여전히 시스템은 안전하지 않았고, 공격자는 새로운 공격 방식들을 테스트하기 시작했다. 이 시기에 공격 동향이 변모한 가장 큰 이유는 취약점의 새로운 활용과 웜 악성코드다.

2001년 발생한 코드레드 웜CodeRed Worm은 마이크로소프트의 IIS 웹 서버에서 발생한 버퍼 오버플로우Buffer Overflow 취약점을 이용해 시스템에 파괴형 악성코드를 감염시켰다. 약 36만 대의 서버가 감염됐으며 잠복기간을 거쳐 서비스를 파괴시켰다. 미국방부 펜타곤Pentagon도 이 공격을 당한 것으로 알려졌다.

코드레드 웜은 스스로 전파하는 웜이라는 악성코드와 취약점이 융합되어 사이버 테러가 가능하다는 것을 전 세계에 알린 것으로 이후 악성코드와 취약점을 융합해 사용하는 형태의 악성코드가 다양하게 발견됐다. 월드 트레이드 센터와 다시 한 번 펜타곤을 혼란에 빠트린 님다 웜Nimda Worm과 2003년 1월 25일 국내에서 발생해 '1.25 대란'으로 잘 알려진 슬래머 웜Slammer Worm 등을 예로 들 수 있다.

취약점을 이용한 가성성 파괴뿐만 아니라 다른 악성코드를 감염시킬 수 있음을 시사하는 내용은 「2002 정보시스템 해킹 바이러스 현황 및 대응」[04] 보고서에서 확인할 수 있으며, 이때부터 소프트웨어 취약점이 악성코드가 빨리 확산되는 근본 원인임을 이야기하기 시작했다.

---

04 출처: 2002 정보시스템 해킹 · 바이러스 현황 및 대응, 한국인터넷진흥원, http://www.kisa.or.kr/public/library/report_View.jsp?regno=006805&searchType=&searchKeyword=&pageIndex=38(단축 URL http://goo.gl/zmuAoS)

한빛 리얼타임

한빛 리얼타임은 IT 개발자를 위한 전자책입니다.

요즘 IT 업계에는 하루가 멀다 하고 수많은 기술이 나타나고 사라져 갑니다. 인터넷을 아무리 뒤져도 조금이나마 정리된 정보를 찾기도 쉽지 않습니다. 또한, 잘 정리되어 책으로 나오기까지는 오랜 시간이 걸립니다. 어떻게 하면 조금이라도 더 유용한 정보를 빠르게 얻을 수 있을까요? 어떻게 하면 남보다 조금 더 빨리 경험하고 습득한 지식을 공유하고 발전시켜 나갈 수 있을까요? 세상에는 수많은 종이책이 있습니다. 그리고 그 종이책을 그대로 옮긴 전자책도 많습니다. 전자책에는 전자책에 적합한 콘텐츠와 전자책의 특성을 살린 형식이 있다고 생각합니다.

한빛이 지금 생각하고 추구하는, 개발자를 위한 리얼타임 전자책은 이렇습니다.

1 eBook First – 빠르게 변화하는 IT 기술에 대해 핵심적인 정보를 신속하게 제공합니다

500페이지 가까운 분량의 잘 정리된 도서(종이책)가 아니라, 핵심적인 내용을 빠르게 전달하기 위해 조금은 거칠지만 100페이지 내외의 전자책 전용으로 개발한 서비스입니다. 독자에게는 새로운 정보를 빨리 얻을 기회가 되고, 자신이 먼저 경험한 지식과 정보를 책으로 펴내고 싶지만 너무 바빠서 엄두를 못 내는 선배, 전문가, 고수 분에게는 좀 더 쉽게 집필할 수 있는 기회가 될 수 있으리라 생각합니다. 또한, 새로운 정보와 지식을 빠르게 전달하기 위해 O'Reilly의 전자책 번역 서비스도 하고 있습니다.

2 무료로 업데이트되는 전자책 전용 서비스입니다

종이책으로는 기술의 변화 속도를 따라잡기가 쉽지 않습니다. 책이 일정 분량 이상으로 집필되고 정리되어 나오는 동안 기술은 이미 변해 있습니다. 전자책으로 출간된 이후에도 버전 업을 통해 중요한 기술적 변화가 있거나 저자(역자)와 독자가 소통하면서 보완하여 발전된 노하우가 정리되면 구매하신 분께 무료로 업데이트해 드립니다.

3 독자의 편의를 위해 DRM-Free로 제공합니다

구매한 전자책을 다양한 IT 기기에서 자유롭게 활용할 수 있도록 DRM-Free PDF 포맷으로 제공합니다. 이는 독자 여러분과 한빛이 생각하고 추구하는 전자책을 만들어 나가기 위해 독자 여러분이 언제 어디서 어떤 기기를 사용하더라도 편리하게 전자책을 볼 수 있도록 하기 위함입니다.

4 전자책 환경을 고려한 최적의 형태와 디자인에 담고자 노력했습니다

종이책을 그대로 옮겨 놓아 가독성이 떨어지고 읽기 어려운 전자책이 아니라, 전자책의 환경에 가능한 한 최적화하여 쾌적한 경험을 드리고자 합니다. 링크 등의 기능을 적극적으로 이용할 수 있음은 물론이고 글자 크기나 행간, 여백 등을 전자책에 가장 최적화된 형태로 새롭게 디자인하였습니다.

앞으로도 독자 여러분의 충고에 귀 기울이며 지속해서 발전시켜 나가겠습니다.

지금 보시는 전자책에 소유 권한을 표시한 문구가 없거나 타인의 소유권한을 표시한 문구가 있다면 위법하게 사용하고 있을 가능성이 큽니다. 이 경우 저작권법에 따라 불이익을 받으실 수 있습니다.

다양한 기기에 사용할 수 있습니다. 또한, 한빛미디어 사이트에서 구매하신 후에는 횟수와 관계없이 내려받으실 수 있습니다.

한빛미디어 전자책은 인쇄, 검색, 복사하여 붙이기가 가능합니다.

전자책은 오탈자 교정이나 내용의 수정·보완이 이뤄지면 업데이트 관련 공지를 이메일로 알려 드리며, 구매하신 전자책의 수정본은 무료로 내려받으실 수 있습니다.

이런 특별한 권한은 한빛미디어 사이트에서 구매하신 독자에게만 제공되며, 다른 사람에게 양도나 이전은 허락되지 않습니다.