

# 블랙햇 USA 2023 & 데프콘 31

## 분석 보고서



---

\* 본 리포트는 보안뉴스 편집국 및 글로벌리서치팀과 인포마마켓비엔(주), 한국과학기술원(KAIST) 사이버보안연구센터(CSRC)에서 공동 제작했습니다.

\* 본 리포트는 저작권법에 의해 보호를 받는 저작물이므로 내용을 무단으로 복사, 전재 및 발췌하는 행위는 저작권법에 저촉되어 민형사상의 처벌을 받을 수 있습니다.

---

# 블랙햇 USA 2023 & 데프콘 31

## 분석 보고서

참관 목적 및 개요	1
------------	---

### Chapter 1. Blackhat USA 2023 Review

블랙햇 USA 2023 키노트	2
블랙햇 USA 2023 브리핑 패스	8
블랙햇 USA 2023 비즈니스홀	24
블랙햇 USA 2023 돋보기	32
글로벌 트렌드와 발 맞추기	34

### Chapter 2. Defcon 31 Review

DEF CON 31	36
DEF CON.run	42

## 1. 참관 목적 및 개요

### 가. 목적

- 전 세계 최신 정보보안 방어기술 및 해킹기술 동향 파악
- 해외 유명 교육 프로그램 참여를 통한 최신 기술 습득
- 기계학습/AI 보안, 사이버 보안, 능동 보안 등 보안기술에 관한 동향 파악 및 방향 참조
- 유명 전문가 및 현업 보안 담당자의 브리핑 참여를 통한 보안 이슈 및 현 세계 보안 상황 이해
- 세계 최대 해킹대회 관전을 통한 최신 및 다양한 해킹 기술 습득
- 다양한 국가의 해커 및 보안 전문가와의 교류 및 저변 확대
- 글로벌 사이버 보안 기술 트렌드 분석 및 센터 내 보유 기술 및 연구에 대한 홍보


### 나. 출장 개요

- 출장지 : 라스베이거스, 미국
- 출장기간 : 2023. 8. 6.~8. 15(7박 10일, 출국: 8월 5일, 입국: 8월 15일)
- 출장자 : 보안뉴스\_ 권준 편집국장(상무), 문가용 기자(국제팀장)  
카이스트 사이버보안연구센터\_ 조호묵 실장, 이정호/이경석  
선임 연구원, 유영락(이하 연구원), 임규민, 박상류

### □ 주요일정

구 분	주요 내용	비 고
8월 6일(일)	출국 및 라스베이거스 도착	인천→라스베이거스
8월 7일(월) ~8일(화)	Black Hat 트레이닝 세션 참가	Black Hat
8월 9일(수) ~10일(목)	Black Hat 브리핑 패스, 키노트 및 전시회 참관	
8월 11일(금)	DEF CON 31 등록 및 참관	DEF CON
8월 12일(토) ~13일(일)	DEF CON 31 행사 참여 및 DEF CON CTF 참관	
8월 13일(일)	라스베이거스 출국	인천→라스베이거스
8월 15일(화)	귀국 및 인천공항 도착	

## Chapter I. Blackhat USA 2023 Review




# Black Hat USA 2023

VENUE  
Mandalay Bay Convention Center

LOCATION  
3950 Las Vegas Blvd South Las Vegas, NV 89119

NAME  
anonymous

DATE  
Aug 05 - Aug 10



# Chapter 1. Black Hat USA 2023 Review

**KEYWORDS**

AI, LARGE LANGUAGE MODEL (LLM),

CYBER SECURITY THREAT, OSINT

HACKING, CYBER DEFENCE

## 1. 블랙햇 USA 2023 키노트

가. Guardians of the AI Era: Navigating the Cybersecurity Landscape of Tomorrow, 인공지능의 발전에 따른 사이버 보안의 변화와 미래

□ 일시: 2023년 8월 9일 수요일 9:00 AM ~ 10:00 AM

□ 연사: Maria Markstedter / Azeria Lab 창립자

□ 강연 내용

- 마리아 마르크스테터 Azeria Lab 창립자는 과거부터 최근까지의 인공지능 동향을 소개하며 최근까지의 인공지능은 단순히 정보검색 또는 시리와 같은 특정한 서비스를 제공하는 목적으로만 사용됐지만, ChatGPT와 같은 Large Language Model(LLM)의 등장은 많은 반향을 일으키고 LLM의 인해 인공지능을 보다 다양한 목적으로 폭넓게 사용할 수 있게 됐다고 설명함. 더 나아가 GPT의 단점인 단일데이터를 입력값으로 받아 결과를 도출하는 것에 벗어나 멀티모달의 등장으로 한 번에 다양한 형태의 입력값을 받아 결과를 도출할 수 있게 됐다고 언급함.
- 또한, 2023년 2월 Microsoft CEO의 말을 인용하며 인공지능의 경쟁은 앞으로 더욱 가속화될 것이라며, 나중에 고칠 수 있는 문제에 대해 걱정하는 것은 시기상조라고 말함. 또한, 많은 회사가 관련 기술을 개발하며 보안이 성능을 약화시킨다는 이유로 보안에 신경쓰기 보다는 시장 점유율에 집중하며 경쟁을 가속하고 있다고 설명함.
- 마리아 마르크스테터는 현재 인공지능의 상황을 사춘기 아이에 비유하며 현재 과도기를 지나고 있는 단계로, 생성형 모델과 거대모델이 발전할수록 문제점 또한 크게 제기되고 있다고 언급함. 또한, Google의 사례를 들며 Google은 몇 년 전부터 생성형 모델기술을 보유하고 있었지만, 생성형 모델이 가져올 문제점을 인식하여 해당 모델의 발표를 보류하고 있었다고 함. 또한, 인공지능 모델의 경쟁을 가속화시킨 Open AI의 수장 Sam Altman 또한 자회사 모델인 GPT의 위험성에 대해 꾸준히 목소리를 제기하고 있다고 소개함.
- 더 나아가, 마리아 마르크스테터는 인공지능의 다양한 위험성에 관한 토론이 현재진행형이며, 인공지능의 위험성 또한 다양한 분야에서의 정의로 아직 모호한 상태라고 언급하며 인공지능 개발자들은 기술적인 측면에서 위험성을 철저하게 평가하고 제기된 위험성에 대해 해결책을 제시하는 역할을 해야 한다고 강조함.
- 마리아 마르크스테터는 대표적인 인공지능 문제점을 소개하면서 현재 API 형태로 제공되고 있는 ChatGPT의 경우 현재까지 결과 도출과정을

알 수 없는 Black-box 형태로, 사용자가 질의하고 있는 질문 역시 Open AI의 데이터셋에 포함되어 정보 유출 가능성을 염려한 여러 회사는 ChatGPT의 사용을 금지하고 있다는 사례 또한 언급함. 더 나아가 사용자가 연산 과정을 모르는 Black-box 형태의 보안문제를 해결하기 위해 explainable AI와 같은 설명 가능한 모델이 절대적으로 필요하다고 함.

- 언급한 또 다른 문제로는 현재 개발되고 있는 멀티모달의 경우, 다양한 데이터를 수집하여 학습하나 숨겨진 멀웨어 정보를 실행하거나 하는 등 보다 위험에 노출되기 쉽고 이를 시스템 전체에 접근할 수 있는 인공지능 모델이 학습할 경우, 회사 전체의 막대한 피해를 불러올 수 있다고 소개하며 다양한 데이터를 수집하고 학습하는 모델이 단순히 보유하고 있는 데이터에 대해 보안을 적용할 것이 아니라 외부데이터로부터 인공지능을 어떻게 보호해야 할지 또한 고민해야 한다고 설명함.



〈 키노트 발표장 전경 〉

- 마리아 마르크스테터는 이러한 문제를 해결하기 위해 보안전문가의 수요는 폭증하고 있지만, 인공지능을 이해하고 기술을 가지고 있는 안전시스템을 구축할 전문가들이 절대적으로 부족하며, 앞으로 보안전문가들 또한 기존의 기술요구조건과는 다른 기술요구조건을 필요로 하게 될 것이라고 말함. 더 나아가 이러한 문제를 해결하기 위해 인공지능을 이용한 공격 경로를 예상하거나 연구하는데 더욱 효과적인 방법을 제시할 수 있을 것이라고 강조함.
- 현재 Google과 Microsoft의 AI Red Team을 소개하며 각 회사들이 적극적으로 인공지능 보안문제에 대응하고 있다고 언급함. 하지만 앞으로는 기존처럼 문제를 직면하고 문제를 해결해가며 성장해온 방식에서 벗어나 보안 분야를 재정립하고 해결해나가야 하며 이를 이루기 위해선 기존의

분리된 각각의 집단방식에서 벗어나 전문가 전체의 하나 된 집단지성이 필요하며 블랙햇과 데프콘이 그런 집단지성을 모으는데 마중물이 될 것이라며 강연을 마칩.

나. Phoenix Soaring: What We Can Learn from Ukraine's Cyber Defenders about Building a More Resilient Future, 우크라이나 사태를 통한 미래의 사이버 리질리언스 구축

□ 일시: 2023년 8월 9일 수요일 4:20 PM ~ 5:00 PM

□ 연사

- Jen Easterly / 미국 CISA 국장
- Victor Zhora / 우크라이나 특수 통신 및 정보보호국 부회장
- 진행자: Lily Hay Newman / WIRED 선임작가

□ 강연 내용

- 빅터 조라 우크라이나 특수통신 및 정보보호국 부회장과 젠 이스터리 미국 CISA 국장의 대담 형식으로 진행된 키노트에서 빅터 조라는 사이버상의 공격은 그동안도 계속 존재해 왔고 앞으로도 계속 있을 것이라고 서두를 꺼냄. 우크라이나에서 발생한 2014년 중앙선거관리위원회 공격, 2015년과 2016년 우크라이나 전력망 공격, 2017년 발견된 러시아의 2016년 미국 선거 사이버망 개입 정황과 같이 사이버 공격은 하나의 전쟁형태로 나타나고 있음. 또한, 현재까지도 러시아는 전투에 우위를 점하기 위해 다양한 사이버 공격을 감행하고 있다고 언급함.
- 또한, 우크라이나는 2014년부터 사이버 공격에 대비한 훈련을 지속적으로 진행했으며, 많은 정보를 수집·분석하며 사이버 공격에 대한 충분한 대비가 이루어졌다고 설명함. 이러한 대비는 사회적 생산기반을 보호하는 데 크게 이바지했고, 인공위성을 이용한 연결망 유지, 클라우드 시스템의 이용을 통해 전쟁을 비롯한 사회활동을 보장할 수 있었다고 설명함
- 빅터 조라는 사이버 공격 대비를 위해 우크라이나는 미국, 유럽 파트너들과 함께 역량을 기르고 더 나아가 민간기업과의 협업 또한 진행했고 다양한 협업과 정보공유 등을 통해 기존 사이버 공격을 판별하고 대응하는데 어려움을 극복할 수 있었다고 언급하며 미국 정부와 다양한 파트너들에게 감사를 표함.
- 젠 이스터리 미국 CISA 국장은 미국은 현재 Five Eyes 파트너들을 비롯하여 많은 국가와 파트너십을 지속해서 강화하고 특히 최근 몇 년간 보다 활발한 협력을 통해 보안위협을 명확하게 판단하고 다양한 훈련을 지

속하는 등 하나의 사이버보안대응 모델을 만들고 있다고 평가함. 또한, 미국은 Shields Up 캠페인을 통해 사이버상의 주요 시설 방어 및 사이버 보안에 대한 경계를 높이는 활동을 지속적으로 전개하고 있다고 설명함. 더 나아가 현재는 많은 양의 정보 및 노하우가 축적되어 이전 오바마, 트럼프 정부 때 보다 더욱 많은 정보를 공유하고 공표함으로써 앞으로 더 커지는 사이버위협에 공동으로 대응하는 노력을 기울이고 있다고 함.

- 더 나아가 앞으로는 무력적인 공격과 사이버망을 이용한 중요시설 무력화와 같은 활동 가능한 사이버 공격을 막기 위해 적에 대응하고 필요한 사회기반 서비스의 온전한 제공을 위해 지속적으로 메시지를 낼 필요가 있으며 모든 사람들이 하나 되어 이러한 위협에 대응해야 한다고 강조함.
- 또한, 사이버 위협이 가중되고 국제적인 사이버 범죄 피해가 커질수록 기존 대응방식에서 벗어나 프로그램 설계단계에서의 강화와 더불어 더욱 높은 책임을 경영자들에게 요구하는 등의 보다 강도 높은 보안강화 방법이 필요하다고도 언급함.



#### 〈 키노트 강연 모습 〉

- 빅터 조와 젠 이스터리는 이러한 노력들은 단순히 사이버 리질리언스를 구축하는 것을 넘어 조직 리질리언스와 사회적 리질리언스를 구축하는데 도움이 된다고 언급하며, 사이버 리질리언스의 구축은 힘든 일이지만 정상시의 사회 구조를 유지하기 위해서는 많은 노력을 기울여야 한다고 강조함.
- 더 나아가 젠 이스터리는 지속적인 인력 훈련과 기술개발, 대응방식의 고도화를 통해 위협에 대응해야 하고 그럴 수 있을 것이라 평가하며 이를 통해 국제적 사이버망의 안전을 확보하고 위협으로부터 보호할 수 있을 것이라고 설명함.



다. Acting National Cyber Director Kemba Walden Discusses the National Cybersecurity Strategy and Workforce Efforts, 미국 국가 사이버보안 정책 및 사이버보안 인력, 교육 정책 설명

□ 일시: 2023년 8월 10일 목요일 9:00 AM ~ 10:00 AM

□ 연사

- Kemba Walden / 현 백악관 국가사이버국장
- 진행자: Jason Healey / 콜롬비아 대학교 국제학부 선임연구원

□ 강연 내용

- 캬바 월든 현 백악관 국가사이버국장과 제이슨 힐리 콜롬비아 대학교 국제학부 선임연구원과의 인터뷰 형식으로 진행된 키노트에서 캬바 월든 국장은 과거 사이버보안 정책과는 다르게 백악관 내의 국가사이버부서의 설립으로 더욱 다양한 분야의 사람들과 함께 사이버보안 정책을 강력하게 주도하고 있다고 설명함. 특히, 현재 백악관은 더욱 많은 사람이 안전하게 사이버 안에서 활동하고 방어 가능한 시스템을 구축하는 데에 주력하고 있다고 언급함.
- 또한, 캬바 월든 국장은 현 정부는 국가 안보정책의 하나로 사이버보안을 포함할 만큼 그 어느 정부보다 사이버보안에 대해 중요하게 생각하고 있고 단순히 사이버보안을 국가안보 목적으로만 생각하는 것이 아니라, 경제적인 성장의 기회와 기술 발전의 목적으로도 생각하고 정책을 수립하고 있다고 강조함. 더 나아가 바이든 정부의 사이버 보안정책은 기존의 사이버 보안정책과는 다르게 방어 가능해야 하고 자유의 가치를 지켜야 한다고 명시했다고 강조함.
- 캬바 월든 국장은 비록 사이버위협을 완전히 없애는 것은 불가능하지만, 사이버 보안 위협이 가해졌을 때 그것을 어떻게 극복할 것인지에 대한 목표 또한 필요하다고 설명함. 사이버보안 정책은 더욱 진보적으로 정책을 수립하여 위협을 뒤쫓아 가는 것이 아닌 위협에 앞서서 정책을 수립해야 한다고 주장함. 또한, 현재까지의 사이버 보안정책은 정당, 정치와 관련 없이 지속적이고 연속적으로 실행되고 있다고 소개함.
- 이렇게 다양한 분야에서 수립된 정책을 백악관 홈페이지에 타임라인과 함께 투명하게 공개하고, 각 커뮤니티의 의견 또한 현재 적극 모집하고 수용하고 있다고 전하며, 관련 전문가들 특히 블랙햇 참가자와 같은 사이버 보안 전문가들의 적극적인 참여를 독려함.
- 캬바 월든 국장은 또한 오픈소스의 발전 때문에 현재 95% 이상의 프로그램이 오픈소스를 사용하여 개발되는 중이고 오픈소스 보안에 대한 요구 또한 높아지고 있다고 지적함. 이러한 오픈소스의 보안 취약점에 대응

하기 위해 캄바 월든 국장은 기존 방식인 기술적으로 보안 위협을 제거하는 것에서 벗어나 프로그램 디자인 단계에서도 보안 요소를 고려해 설계돼야 한다고 주장함. 또한, 더욱 다양한 사람들이 안정성을 검증하는데 참여해야 한다고 강조함.

- 또한, 단순히 이러한 제안에서 그치는 것이 아니라, 더욱 많은 교육프로그램을 통해 보안전문가들을 양성할 필요가 있다고 언급함. 단순히 학습을 하는 것이 아니라 모든 사람이 사이버보안 위협으로부터 회복 가능한 상태가 되려면 어릴 때부터 사이버보안에 친숙해지는 교육이 필수적이라고 소개함.
- 캄바 월든 국장은 이러한 교육으로 프로그램과 모든 사람이 사이버 보안에 일조할 수 있는 환경을 조성하는 것이 필요하다고 언급함.



〈 연사 Kemba Walden과 진행자 Jason Healey의 키노트 강연 모습 〉

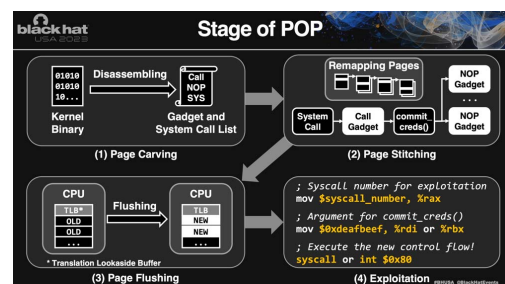
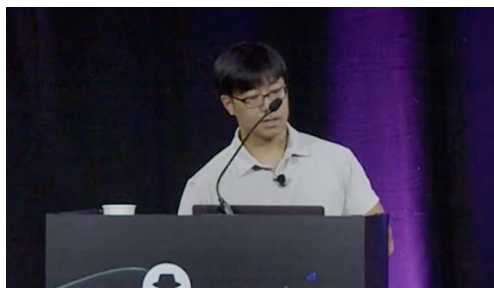
- 또한, 고나련 법률 위반 시 처벌하거나 규제하는 것이 아니라 많은 사람이 최소한의 사이버보안이 갖춰진 환경에서 자유롭게 이용할 수 있도록 하는 것이 중요하다고 강조함.

## 2. 블랙햇 USA 2023 브리핑 패스

가. Lost Control: Breaking Hardware-Assisted Kernel Control-Flow Integrity with Page-Oriented Programming

- 장소: South Seas AB, Level 3
- 연사: 한승훈(국가보안기술연구소 선임연구원)
- 강연 내용

현재 code reuse attack 방지에 state-of-the-art kernel CFI들의 취약점들과 새로운 page-level code reuse attack인 Page-Oriented Programming(POP)을 소개함. CFI는 의도하지 않은 실행을 방지할 수 있다고 알려졌으며, Microsoft Windows와 Linux에도 적용되어 있을 만큼 폭넓게 사용되고 있음. 특히, software-based CFI와 hardware-based CFI의 결합으로 각각의 약점을 상호보완하며 강력한 CFI 정책을 만들 수 있다고 설명함. 하지만 현재의 CFI들은 단지 indirect branches 보호에만 집중되어 있고 정작 direct branches 보호에 대해서는 전혀 없다고 설명하며 해당 문제점을 이용하여 공격하는 Page-Oriented Programming에 대해 강연해함. POP는 커널과 커널 메모리에 page table를 프로그램함으로써 커널과 커널 메모리를 읽고 쓸 수 있게 했고 더 나아가 POP은 새로운 control flow를 작성할 수 있는 취약점들을 소개하며 강력한 보안정책을 우회할 수 있다고 우려함. POP는 Page Carving, Page Stitching, Page Flushing 그리고 Exploitation의 총 4개의 단계로 구성되어 있으며, 각 단계의 설명 이후에는 실제 FineBT 커널을 POP을 통해 공격하는 실험을 데모 영상을 통해 시연하며, 실제 POP이 CFI의 보안정책을 우회하여 성공적으로 커널을 공격할 수 있다고 발표함.



### 〈 발표 장면 및 POP 전체 과정 설명 슬라이드 〉

마지막으로 한승훈 선임연구원은 POP과 같은 공격을 방지하는 방법으로 hyper visors를 통한 page table update와 Hypervisor-Managed Linear Address Translation과 같은 방법을 이용하는 것을 제안했지만, 위의 방법

또한 한계점은 명확하게 존재한다고 언급함.

#### 나. Devising and Detecting Phishing: Large Language Models(GPT3, GPT4) vs. Smaller Human Models(V-Triad, Generic Emails)

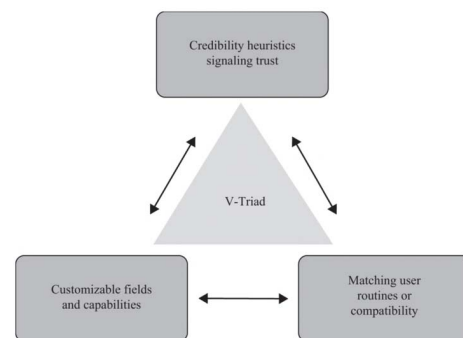
□ 장소: South Seas CD, Level 3

□ 연사

- Fredrik Heiding / 연구원, Harvard
- Bruce Schneier / 보안 전문가 / Adjunct Lecturer in Public Policy, Harvard
- Arun Vishwanath / 기술 전문가, 연구원, 강사, 작가, Avant Research Group
- Jeremy Bernstein / 박사 후 연구원, MIT

□ 강연 내용

현재 공개되어 있는 GPT3, GPT4와 같은 Large Language Model을 소개하며 이러한 모델들과 사용자가 제공하는 몇몇 정보를 바탕으로 피싱 이메일을 제작할 수 있다고 강연함. 해당 세션에서는 피싱 이메일의 공통점들을 학습한 모델인 V-Triad를 소개하며 해당 모델이 얼마나 효과적으로 피싱 이메일을 제작할 수 있는지 GPT3, GPT4 그리고, Generic Email과 비교하며 설명함. 또한, 단순히 각각의 모델로만 피싱 이메일을 제작하는 것이 아니라 GPT-4와 V-Triad를 결합해 가능성을 확인하는 시간을 가짐.



〈 발표장 전경 및 V-Triad 설명 슬라이드 〉

각각 이메일의 평가는 200명의 불특정 인원을 대상으로 평가를 진행, 각각의 이메일이 피싱 이메일로써 얼마나 효과가 있는지 판단했고, 그 결과 GPT-4와 V-Triad로 제작된 각각의 이메일이 비슷한 효과가 있는 것으로 나타남. 더 나아가 평가단에게 GPT-4와 V-Triad를 결합하여 제작한 피싱 이메일에 대한 평가도 진행하여 단순히 LLM을 이용하여 제작하는 것보다

목적에 특화되어 제작한 결과물과 LLM을 결합했을 때 효과가 더 좋은 것으로 나타났다고 소개함.

다. BTD: Unleashing the Power of Decompilation for x86 Deep NeuralNetwork Executables

□ 장소: South Pacific F, Level 0

□ 연사

- Zhibo Liu / 박사과정 학생, Hong Kong University of Science and Technology
- Yuanyuan Yuan / 박사과정 학생, Hong Kong University of Science and Technology
- Xiaofei Xie / 부교수, Singapore Management University Tianxiang Li / 보안 연구원, CSI AI Red Team
- Wenqiang Li / 보안 연구원, CSI AI Red Team
- Shuai Wang / 부교수, Hong Kong University of Science and Technology

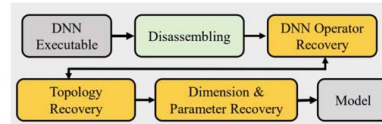
□ 강연 내용

현재 많은 딥러닝 모델들이 exe 형태로 배포되어 보다 저사양에서도 실행할 수 있게 됐다고 언급하며 배포되고 있는 exe 형태의 딥러닝 모델을 디컴파일 할 수 있는 기술 BTD(Bin to DNN)에 대해 강연함.

BTD는 Operator recovery, topology recovery, dimension & parameter recovery의 단계를 가지고 있으며, Operator recovery는 exe에서 디어셈블한 binary를 바탕으로 LSTM을 학습시켜 복구를 진행했다고 밝혔다. 이후 topology recovery는 메모리 주소를 참고하여 원래의 순서대로 복구를 진행했고, Dimension과 Parameter 복구는 Symbolic execution을 이용해 DNN의 차원 수와 로컬 파라미터를 성공적으로 복구할 수 있었다고 언급함. BTD는 Deep Neural Network의 exe 형태를 입력으로 받아 모델의 사양과 네트워크 구성, 사용된 Neural Network 차원과 사용된 parameter를 성공적으로 복원했다고 밝힘. 또한, BTD로 디컴파일된 exe 형태의 DNN을 다른 컴파일러를 통해 exe 형태로 변환했을 때 성공적으로 작동할 수 있다는 것 또한 확인할 수 있었음. 또한 BTD의 성능을 확인하기 위해 다양한 오픈 소스 모델의 exe를 바탕으로 parameter 복원과 차원 복원을 확인했고, 2개의 Case를 제외하고 모두 성공적으로 복원하는 결과를 확인할 수 있었다고 발표함.

## Workflow

- BTD consists of 3 steps: **operator recovery**, **topology recovery**, **dimension & parameter recovery**.



- BTD is able to recover **full model** specification (including **operators**, **topologies**, **dimensions**, and **parameters**) from DNN executable.

### 〈 BTD 전체 과정 설명 프리젠테이션 〉

라. IR-on-MAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing

□ 장소: Jasmine AE, Level 3

□ 연사

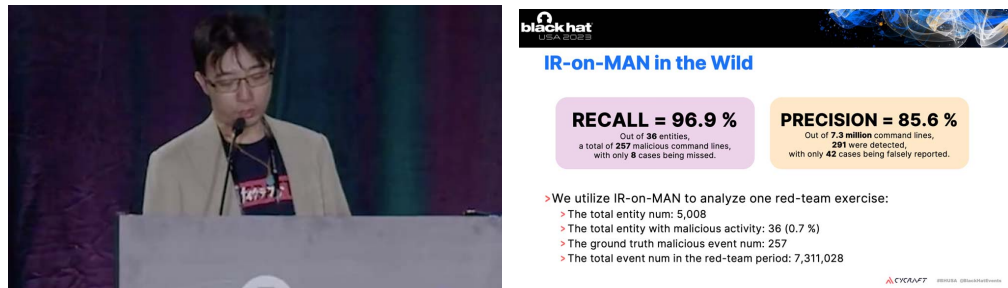
- Sian-Yao Huang / 데이터 사이언티스트, CyCraft Technology
- Cheng-Lin Yang / 선임 데이터 사이언티스트, CyCraft Technology
- Chung-Kuan Chen / 보안 연구원장, CyCraft Technology

□ 강연 내용

Large scale Language Model(LLM)과 Association Mining을 결합하여 Command line 명령을 조사할 수 있는 IR-on-Man에 대해 강연함. 우선 SECCON에서 공개된 CmdGPT를 비롯하여 traditional heuristic approach에 대해 설명하며 그동안 위험 요소를 탐지하는 방법들은 command line 상의 약간의 변화만 발생해도 토큰화하지 못한다는 문제점을 가지고 있고 이러한 문제점은 최종적으로 악의성이 있는 명령을 전부 탐지하지 못한다는 문제점에 대해 언급함. 따라서 IR-on-MAN은 그동안 여러 command line을 비교하며 자주 반복되는 토큰을 중심으로 중요한 토큰을 찾던 방식에서 벗어나 LLM embedding 모델을 이용하여 command line에게서의 중요한 토큰을 찾는 방법을 제안함. 이러한 방법은 더욱 정확하게 command line 명령을 인식할 수 있다는 장점이 있다고 언급함. 보다 정확한 command line 명령 인식을 위해 약 4,000개의 보안 command line 명령을 토큰화하여 미세조정 학습을 진행했다고 소개하며 이런 학습을 통해 더욱 중요한 토큰을 정확하게 표현할 수 있었다고 설명함. 또한, 각 토큰



큰끼리의 영향력을 점수화하고 자주 등장하는 토큰에는 가중치를 부여함으로써 보다 정확하게 명령어 내의 중요한 토큰을 추출할 수 있었다고 소개함. 이러한 방법으로 학습된 IR-on-MAN은 96.9% Recall과 85.6%의 정확성을 보였고, 기존에 방식에서 제기되었던 문제점들을 보다 효과적으로 해결할 수 있었다고 설명하함. 또한, 직접 사용하여 볼 수 있는 사이트를 소개하며 발표 세션을 마무리함.



#### 〈 발표 장면 및 IR-on-MAN 성능 설명 슬라이드 〉

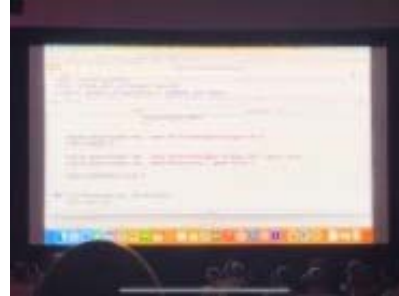
#### 마. Smashing the State Machine: The True Potential of Web Race Conditions

- 장소: Oceanside A, Level 2
- 연사: James Kettle / 연구소장, PortSwigger
- 강연 내용

Web race conditions(웹상에서 동작 타이밍에 따라 예기치 않게 다른 동작에 영향을 끼치는 결함)을 이용한 취약점을 토대로 서버 측에 단일 요청 공격(Single-packet attack)을 수행하는 내용에 대해 설명함. 웹 서버 측과의 요청이 여러 단계임을 확인하고 요청 동기화를 통해 race condition을 만드는 기술을 개발함. 첫 번째 구현에서 사용자 ID에 대한 키를 식별했고, 두 번째 구현에서 공격자가 동시에 두 개의 서로 다른 이메일에 대한 재설정을 트리거하여 모두 동일한 세션의 토큰과 사용자 ID 속성을 변경할 수 있었음. 실제 구버전의 Github를 대상으로 다른 사용자의 이메일을 마음대로 변경하는 모습을 시연함. 전체적으로 Race conditions를 이용한 취약점에 대한 문제점 제기, 해당 공격을 이용하여 공개된 취약점 소개, 실제 계정 탈취 데모 시연, 향후 연구 문제 및 해결방안을 제시함.

행사장 분위기와 다르게 발표자는 긴장하고 경직된 상태로 발표를 진행함. 하지만 실제 해킹 데모 영상을 보면서 사람들은 환호하며 소리를 쳤고 적극적으로 호응하는 분위기가 일반적인 학회와는 많이 다르게 느껴졌음. 발

표 앞뒤에 배경음악은 TV 토크쇼를 진행하는 느낌으로 중요한 발표를 하는 것 같은 인상을 받았음.



〈 발표장 전경 및 해킹 시연 화면 〉

바. Weaponizing Plain Text: ANSI Escape Sequences as a Forensic Nightmare

- 장소: Oceanside A, Level 2
- 연사: STOK . / 해커, 크리에이터, Truesec
- 강연 내용

로그(Log) 파일을 이용한 악성 콘텐츠 삽입 공격을 통해 애플리케이션에 손상을 입히는 기술에 대해 발표함. ANSI Escape Sequence를 사용하여 로그 파일을 변조함으로써 애플리케이션의 파손 및 무기화하는 방법을 제시함. 그리고 악의적인 Escape Sequence를 전달하지 않는 대응책을 제시하여 안전한 로그 파일 운영방법을 제안함. 최종적으로 블랙박스 테스트를 시연하며 공격이 성공하는 것을 보여줌. 발표자는 해커로서 굉장히 자유분방한 사람으로 280장에 달하는 프레젠테이션을 막힘없이 소화함. 덕분에 발표장 분위기는 긴 발표시간에도 흥미롭게 즐길 수 있었으며 공격이 성공했을 때 모두가 환호함.



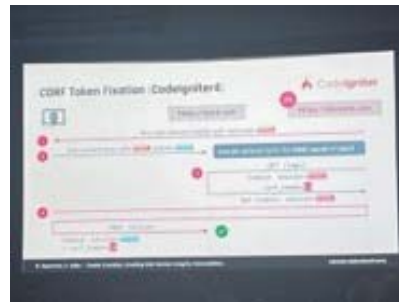
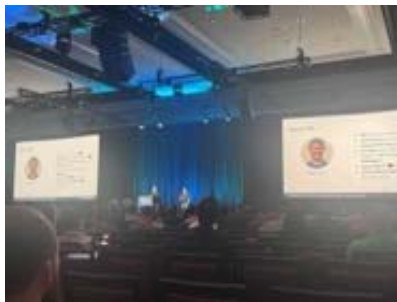
〈 발표장 전경 및 공격 코드 삽입 프레젠테이션 〉



사. Cookie Crumbles: Unveiling Web Session Integrity Vulnerabilities

- 장소: Woxslander FG, Level 0
- 연사
  - Marco Squarcina / 선임 과학자, TU Wien
  - Pedro Adão / 부교수, Instituto Superior Técnico, Universidade de Lisboa
- 강연 내용

세션 고정, CORF(Cross-Origin Request Forgery)를 활용한 쿠키 던지기 기술에 대해 발표함. 브라우저, 웹 개발 프레임워크 등에 영향을 미치는 쿠키 표준과 12개의 CVE, 30개의 취약점 관련 업데이트에 기여한 연구결과를 발표함. 주로 실제 취약점과 관련하여 악용한 소스코드에 대해 설명했으며 CSRF 보호 매커니즘을 우회하는 CORF 토큰 고정 공격에 대하여 제시함. 발표자는 2명으로 대담 형식의 발표를 진행했는데, 국내에선 접하기 힘든 형식의 발표 형태라 새로웠음. 실제 공격행위를 보여주는 데모를 시연하지 않았지만 소스코드에 대한 상세한 설명이 있는 깊이 있는 연구발표라고 평가할 수 있음.



〈 발표장 전경 및 공격 코드 설명 화면 〉

아. Oven Repair (The Hardware Hacking Way)

- 장소: Oceanside A, Level 2
- 연사: Colin O'Flynn / CTO, NewAE Technology Inc.
- 강연 내용

오븐에 설치되어 있는 하드웨어와 임베디드 소프트웨어에 공격을 가해 부트로더와 함께 동작하는 도구를 구축해 실제 삼성 오븐의 패널에 실시간 온도가 출력되게끔 패치하고 데모 영상을 시연함. 전자 기판에 약간의 전기적 공격을 통하여 부트로더를 불러올 수 있었고, 리버스 엔지니어링을 통하여 펌웨어를 수정함. 온도 로직을 추가해 항상 실제 내부 온도가 출력

되게 만들고 고장난 오븐을 고치며 실제 사용에 문제가 없는 것을 보여줌. 최근에 IoT 기기 펌웨어의 취약점은 네트워크 기반 공격으로 많이 알려진 것에 반해, 기판에 대한 물리적 공격과 함께 리버스 엔지니어링을 통한 펌웨어 수정은 흥미로운 공격 방식이었음.



〈 발표장 전경 및 해킹 성공에 따른 온도 조절 화면 〉

#### 자. Reflections on Trust in the Software Supply Chain

- 장소: Woxslander FG, Level 0
- 연사: Jeremy Long / 수석 엔지니어, ServiceNow
- 강연 내용

최신 소프트웨어의 70~90%가 무료/오픈 소프트웨어로 추정되며 CI/CD 인프라 및 빌드 관리 소프트웨어, CI/CD 관련 타사 서비스도 모두 공급망 소프트웨어의 일부인 상황에서 공급망을 대상으로 하는 위협이 증가하고 있는 상황임. 이에 직접 만들지 않은 코드는 신뢰할 수 없으며 공급망 소프트웨어의 보안을 강화하기 위해서는 소프트웨어 코드 및 구성 요소의 출처, 소프트웨어 재료 명세서(SBOM), 소프트웨어 구성 분석(SCA)를 살펴봐야 한다고 강연자는 강조함. 이와 관련 손상된 런타임 종속성 사용을 이용한 악의적인 종속성 위협 데모를 시연함. 빌드 중에 실행되는 모든 코드는 빌드 출력에 영향을 줄 수 있기에 OWASP Dependency-check를 사용하여 Maven 및 Gradle 빌드용 플러그인을 스캔하고 오픈소스 개발자의 지원을 받아 위협을 줄여야 한다고 발표함.



〈 발표장 전경 〉

#### 차. Becoming a Dark knight Adversary Emulation Demonstration for ATT&CK Evaluations

□ 장소: Islander FG, Level 0

□ 연사

- Cat Self / 엔지니어, MITRE
- Kate Esprit / 수석 사이버 위협 인텔리전스 분석가, MITRE

□ 강연 내용

MITRE ATT&CK은 공격자들의 최신 공격 기술 정보가 담긴 저장소로서 실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적 행위 (Adversary Behaviors)에 대해서 공격방법(Tactics)과 기술(Techniques)의 관점으로 분석하여 다양한 공격그룹의 공격기법들에 대한 정보를 분류해 목록화해 놓은 표준적인 데이터임. MITRE ATT&CK Evaluations는 ATT&CK 지식 기반의 언어와 구조를 통해 각 벤더가 위협 탐지에 접근하는 방법을 보여주는데, 각 평가의 결과는 철저하게 문서화되고 공개적으로 게시됨으로써 사용자가 투명한 평가 프로세스와 공개적으로 사용 가능한 결과를 통해 알려진 적의 행동을 더 잘 이해하고 방어하도록 도와줄 수 있음. 이번 강연에서는 블라인드 이글(Blind Eagle)로 알려진 APT를 사용하여 적 에뮬레이션 시연을 위해 사이버 위협 인텔리전스 팀(CTI)와 Red 개발 기능을 병합하는 방법을 시연함. ATT&CK Evaluations를 사용하면 에뮬레이션 개발 프로세스에 투명성을 제공하고 CTI와 Red 개발 협업을 위한 솔루션을 제공하며 에뮬레이션 계획을 세우는데 도움을 준다고 설명함. 강연자는 블라인드 이글을 사용하는 시나리오는 곧 공개할 예정이라고 밝힘.



〈 발표장 전경 및 프레젠테이션 화면 〉

#### 카. Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater

□ 장소: South Pacific F, Level 0

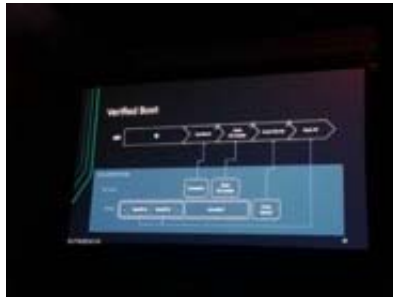
□ 연사

- Christian Werling / 박사과정 학생, TU Berlin
- Niclas Kühnapfel / 박사과정 학생, TU Berlin
- Hans Niklas Jacob / 박사과정 학생, TU Berlin
- Oleg Drokin / 보안 연구원

□ 강연 내용

전기자동차 시장을 이끄는 테슬라(Tesla)는 내부의 패널을 이용한 엔터테인먼트 기능부터 완전 자율 주행 기능에 이르기까지 다양한 기능을 접목한 최첨단의 기기임. 이러한 기능들은 임베디드 자동차 컴퓨터로 작동됨. 그렇기에 이 시스템을 해킹한다면 해커는 자동차의 모든 기능을 자유자재로 작동 및 조절할 수 있음. Technische Universität Berlin의 Security in Telecommunications(SecT) Lab의 박사과정 학생들은 Tesla에서 사용되는 최신 AMD 기반 인포테인먼트 시스템(MCU-Z)을 공격해 탈옥을 시연함. 첫째로 차량 내부 서비스 네트워크에서 차량을 인증하고 권한을 부여하는데 사용되는 차량 고유의 하드웨어 바인딩 RSA 키를 추출함. 둘째로 AMD 보안 프로세서(ASP)를 해킹하기 위해 다양한 방법을 시도했고, 전압을 주입하여 오류를 발생시키는 글리치 공격으로 ASP의 초기 부팅 코드 무력화에 성공함. 그 후, 리버스 엔지니어링을 이용하여 Linux 루트 셸을 획득할 수 있었음. 루트 권한을 획득하여 재부팅과 업데이트 후에도 Linux OS를 임의로 변경할 수 있었고, 이를 통해 암호화된 NVMe 스토리지의 암호를 해독하고, 사용자의 개인정보와 같은 개인 사용자 데이터에 접근할 수 있었음. 강연자는 탈옥하여 권한을 획득한 Tesla MCU-Z 시스템을 이

용하여 공조 장치를 임의로 구동시키는 영상을 선보였음. 특히, AMD 보안 프로세서를 해킹하기 위해 레이저, 전자파, 전압 주입 등을 이용하여 해킹하는 방법은 꽤 흥미로웠음.



< 해킹 과정 절차 슬라이드 및 해킹 시연 화면 >

타. Defender-Pretender: When Windows Defender Updates Become a Security Risk

□ 장소: Mandalay Bay H, Level 2

□ 연사

● Tomer Bar / 보안 연구 부사장, SafeBreach

● Omer Attias / 보안 연구원, SafeBreach

□ 강연 내용

엔드포인트 위협탐지 및 대응(EDR)은 컴퓨터 및 서버 등 단말에서 발생하는 악성 행위를 감지하고 이를 분석하여 대응하는 강력한 대응 방법임. 특히, 시그니처 업데이트 프로세스는 이 대응 방법의 핵심 구성 요소인데, 이 과정이 무력화되면 보안 장치는 무용지물이 됨. 10년 전 처음 발견된 Flame 멀웨어 공격은 악성 인증서를 바탕으로 MITM을 구현, Microsoft 업데이트를 사칭해 합법적인 코드로 위장함으로써 멀웨어를 전파했음.

이렇듯 서명 업데이트 파일은 Microsoft에 의해 서명되고 관리되기에 절대적으로 신뢰함. 이에 SafeBreach 연구팀은 인증서를 소지하지 않고 권한이 없는 사용자가 동일한 업데이트가 가능한지 연구함. 이러한 방법으로 Windows Defender 프로세스를 무력화시키는 것을 목표로 함. 연구진은 mpengine.dll 파일을 변조하는 방법을 시도했으나 실패함. 연구진은 MpSigStub.exe 파일 내에 VDM 파일 버전을 변조해 멀웨어들을 심어 시도함. 하지만 시그니처를 합법한 시그니처로 위장하는 방법에서 다시 벽에 봉착함. 이 시그니처 정보들을 리버스 엔지니어링으로 분석 추측했고, 결국 zlib을 이용한 압축 시, 데이터 크기인 점을 찾아내어 Microsoft 업데이트

트에 성공할 수 있었다고 함. 결국 Windows Defender 프로세스는 무력화되었고, 이에 따라 Windows의 시스템 파일이 삭제되는 시연을 보여줌.



< 발표장 전경 및 업데이트 성공 화면 >

카. Small Leaks, Billions Of Dollars: Practical Cryptographic Exploits That Undermine Leading Crypto Wallets

□ 장소: Jasmine AE, Level 3

□ 연사

- Nikolaos Makriyannis / 선임 암호화 연구원, Fireblocks
- Oren Yomtov / 선임 블록체인 연구원, Fireblocks
- Arik Galansky / 기술 부사장, Fireblocks

□ 강연 내용

파이어블록스 연구팀은 코인베이스, 바이낸스, 젠고, 비트고 및 파이어블록스 등 대형 가상화폐 거래소에서 사용하고 전 세계 수억 명의 사용자의 지갑을 보호하는 다자간 연산(MPC) 알고리즘에 대해 설명함. 이 MPC 알고리즘은 수천억 달러 규모의 암호화폐 지갑을 보호하는 일반적인 방법임. 연구팀은 간단한 MPC 프로토콜 구현과 기능을 소개하고 이 MPC 보안이 어려운 점을 설명함. 또한, 수백 개 이하의 서명이 필요한 실제 키 유출 공격을 시연하며 서명 공격을 통해 익스플로잇의 문제점 및 보완 필요성을 보여줌. 또한 256개, 16개, 하나의 서명이 필요한 다른 프로토콜에 대한 다양한 공격 양상을 보여주며 경각심을 불러일으킴.



〈 발표장 전경 〉

파. A Manufacturer's Post-Shipment Approach to Fend-Off IoT Malware in Home Appliances

□ 장소: Islander HI, Level 0

□ 연사

- Yuki Osawa / 수석 엔지니어, CISSP, Panasonic Holdings Corporation
- Satoru Higuchi / 선임 엔지니어, CISSP, Panasonic Holdings Corporation
- Satoshi Ito / 스텝 엔지니어, Panasonic Holdings Corporation
- Manabu Nakano / 총괄 관리자, Panasonic Holdings Corporation
- Takayuki Uchiyama / 매니저, Panasonic Holdings Corporation

□ 강연 내용

이번 강연은 파나소닉 IoT 위협 인텔리전스 플랫폼 연구 개발팀의 연구 현황을 소개함. 파나소닉 사는 실제 IoT 제품을 물리적 허니팟 시스템으로 사용하는 IoT 위협 인텔리전스 플랫폼을 5년 이상 운영중에 있음. 특히, 전체 제품 수명 주기 동안 보안 활동을 지속적으로 업데이트하는 것을 목표로 'ASTIRA'라는 에코시스템을 구축했고, 심층적인 위험성 평가를 위해 물리적 허니팟을 통한 데이터 피드를 활용하고 있음. IoT에 특화된 자체 보호 모듈인 'THREIM'을 개발했는데, ARM, MIPS, 인텔 CPU 아키텍처가 적용된 IoT 제품에서 악성코드 샘플을 실행해 THREIM을 평가함. ASTIRA 허니팟에서 수집한 5,000개의 샘플 중 선별한 1,800개의 악성코드 샘플에 대해 ARM 기반 제품에서 86.1%의 악성코드 탐지율을 확인했다고 연구진은 홍보함.





〈 발표장 전경 및 프레젠테이션 화면 〉

하. Civil Cyber Defense: Use Your Resources to Defend Non-Profits as They Combat Human Trafficking and Subvert Authoritarian Regimes

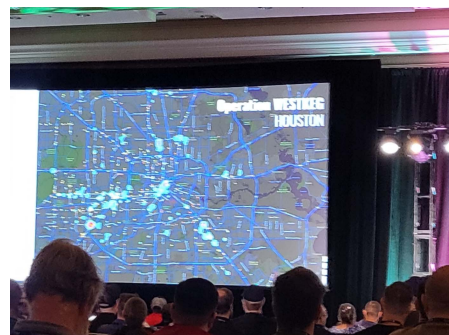
□ 장소: Jasmine AE, Level 3

□ 연사

- Tiffany Rad / 강사, U.C. Berkeley
- Austin Shamlin / 설립자, Traverse Project

□ 강연 내용

인터넷 보안 문제 이외에도 인신매매, 비영리 단체 보호 등의 사회적 문제에 대해 설명하고, OSINT, 오픈소스 도구 등을 활용하여 인신매매의 문제점을 어떻게 해결했는지 등의 방안을 논의함. 실제 인신매매의 경우 여성의 납치가 대다수였으며, 20대 미만의 어린아이가 가장 취약 계층이라는 설명을 덧붙였다. 이러한 납치의 경우 최근 SNS 활동 반경을 통해 실종자가 가장 최근에 활동했던 지역을 중심으로 포괄적인 수사 과정을 설명하고, 현재 활동하고 있는 비영리 단체의 가입 독려 및 적극적인 홍보로 강연을 마무리함.



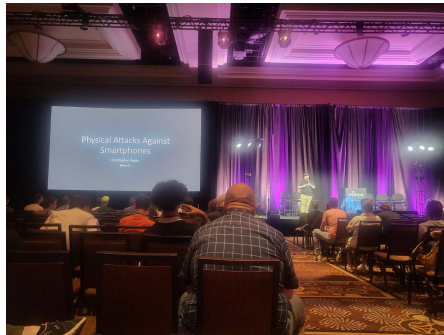
〈 발표장 전경 및 OSINT를 활용한 인신매매 추적 시연 화면 〉

가. Physical Attacks Against Smartphones



- 장소: South Seas AB, Level 3
- 연사: Christopher Wade / 보안 연구원
- 강연 내용

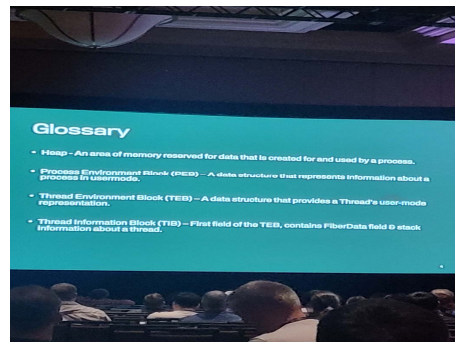
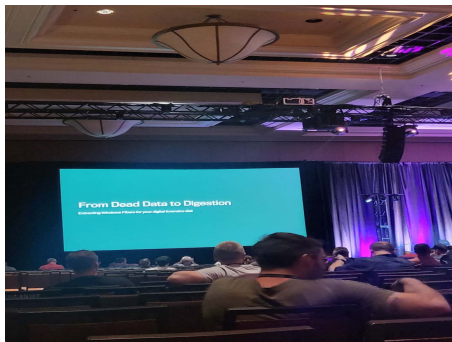
현재 안드로이드 스마트폰이 내재하고 있는 보안 취약성(루트 권한 상승, 부트 로더)에 대한 취약성을 설명함. 먼저 Bootloader에 액세스 권한 없이 루트로 권한 상승을 하거나 복구 단계에서 Android를 순회할 수 있는 취약점을 설명함. 두 번째로 Secondary Bootloader의 취약점에 대하여 소개함. USB 메모리 스택 취약점을 사용하여 스마트폰의 장치적 기능을 손상시키는 문제점을 시연을 통해 설명했음.



〈 강사진 소개 및 발표장 전경 〉

## 나. From Dead Data to Digestion: Extracting Windows Fibers for Your Digital Forensics Diet

- 장소: South Seas AB, Level 3
- 연사: Daniel Jary / 보안 연구원
- 강연 내용



〈 강사진 소개 및 주요 용어 설명 슬라이드 〉

Windows 도구 중 Fibers에 대한 설명 및 활용 방법에 대해 설명하고, 프

로세스 메모리에서 세분화된 감지 원격 분석을 생성하는 방법에 대한 소개  
함. 이후 강연자가 직접 작성한 소스코드에 대한 설명 및 포렌식을 어떻게  
효율적으로 분석할 수 있는지에 대해 강연함.

보안 뉴스

### 3. 블랙햇 USA 2023 비즈니스 홀

#### □ 개요

엄청난 인파가 몰려든 Business Hall 행사장에서는 화려한 부스, 시끄러운 음악 소리와 함께 다양한 행사가 진행됨. 국내 기업 스파로우(Sparrow)를 비롯하여 CrowdStrike, Darktrace, KnowBe4 등 전 세계 유명 보안업체 429개가 black hat 스폰서로 행사에 참여했고, 미국 사이버보안 및 인프라 보안국을 비롯하여 HP, AT&T, Github 등 다양한 기관 및 기업에서 행사장을 채웠음. 각 기업별 부스 이외에도 Arsenal, 미팅룸, Start-up City 등 특별 부스 공간에서도 발표와 미팅이 진행됨. 홀 중앙에 위치한 각 기업별 부스에서는 자체 보안 제품 홍보와 더불어 개별 프레젠테이션이나 미팅, 이벤트가 진행됐고, 각종 상품과 기념품으로 사람들의 이목을 집중시키고자 함.



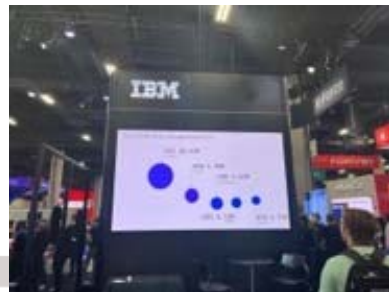
〈 Business Hall 전경 및 발표 세션 스케줄 〉

#### □ 유명 회사 및 기관, 한국 기업 활동

메인 스폰서 기업과 유명 보안 업체는 가장 커다란 부스를 운영하며 눈길을 끌었으며 많은 수의 사람들이 몰려들었음. Akamai에서는 개별적으로 보안 관련 프레젠테이션을 진행하며 참여자들과 소통하는 시간을 가졌고, 특별 이벤트로 옛 비디오 게임을 체험할 수 있게 준비하여 사람들의 이목을 집중시킴. Darktrace에서는 F1 차를 전시하며 가장 큰 부스를 운영하고 있었고 제품에 대한 시연, 미팅을 진행함. IBM에서는 소속 화이트해커인 Cris Thomas의 책 사인회와 여러 프레젠테이션을 진행하며 자사 제품 홍보에 나섰으며, Microsoft에서도 개별 발표와 더불어 제품 데모 시연을 진행하며 사람들의 관심을 모음.

글로벌 통신 업체인 AT&T에서도 Cybersecurity가 참여하며 네트워크 관련 제품, SaaS 솔루션 등 다양한 제품을 홍보했고, VMware에서도 최근 인수한 Carbon black을 토대로 엔드포인트 보호 및 대응(EDR) 솔루션을 내세우며

행사장에 자리함. 특이하게도 기업이 아닌 미국 CISA(Cybersecurity and Infrastructure Security Agency)에서도 부스를 운영하며 행사에 참여했고, 국내에서는 유일하게 Sparrow에서 보안 테스트 솔루션을 홍보하기 위해 대표를 비롯한 직원들이 자리하고 있었음.



〈 Akamai, Darktrace, IBM, Microsoft 부스 전경 〉



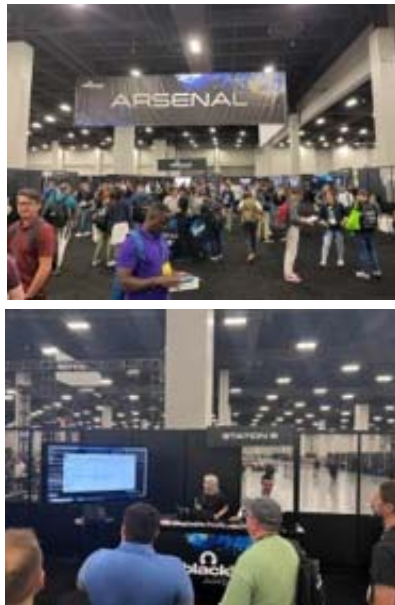
〈 AT&T, VMware, CISA, Sparrow 부스 전경 〉

제품군 기준으로 살펴보면 엔드포인트 보안, 네트워크 보안, 위협 탐지 및 대

응 등 기업 및 일반 사용자를 위한 제품을 많이 홍보했으며, 발표 세션에선 최근 보안 트렌드에 맞춰 AI, XDR에 관한 발표가 주를 이룸.

□ Arsenal 및 특별 구역

한편, 비즈니스 홀 안에서는 기업에서 진행하는 개별 부스 이외에도 직접 개발한 오픈소스 도구의 데모를 발표하는 Arsenal이 진행됨. AI 기반 피싱 도메인 탐색 도구, 데이터 포렌식 도구, IoT 스캐너, 모바일 해킹 툴, OSINT 정보 수집 도구, 악성코드 공격 및 방어 기술에 관한 다양한 발표가 진행됨. 총 8개의 Station에서 동시에 발표가 진행되며 직접 데모 시연을 하는 것을 보며 사람들이 환호하기도 함. 이외에도 Networking Lounge, Start-up City, Career Zone, Meeting Room 구역에서도 구인/구직을 위한 미팅이나 기술 관련 대화를 나누는 것을 확인할 수 있었음.



〈 Arsenal 발표 전경 및 세션 〉

□ 국내 보안 컨퍼런스 및 전시회와의 차이점

미국뿐만 아니라 글로벌 기업들의 참여로 인하여 화려한 부스에서 다양한 이벤트가 경쟁적으로 열리고 있었음. 시끄러운 음악과 함께 사이버 보안을 주제로 랩 배틀을 하는가 하면 게임기, 신발 등 고가의 경품을 건 이벤트와 음식, 음료를 제공하며 사람들을 끌어들이려 함. 국내 전시회에서는 각종 기념품으로 행사 참여 혹은 부스 관람을 유도하지만 보다 차분하고 조용한 환경에서 행사장을 관람할 수 있는 점에서 큰 차이점이 있었음. 또 다른 특징으로 국



내에서는 기업 부스를 방문할 경우, 이메일과 같은 개인정보를 직접 입력해야 하지만 Black hat에서는 뱃지에 있는 QR코드를 활용하여 비교적 쉽게 개인정보를 수집함. 라스베이거스라는 도시의 특색에 따라 Black hat 행사 시간 이외에 별도 장소에서 칵테일, 위스키, 클럽 등 각종 파티를 각 기업에서 자체적으로 주관했고 이 행사를 통하여 기업 내 운영진과 실무자와의 미팅을 주선함.

# 보안 뉴스

※ 별첨. 참여 기업 및 활동 내역

기업명	활동 내역
Akamai Technologies	<ul style="list-style-type: none"> <li>-연구 프레젠테이션 제공</li> <li>-보안 인텔리전스 그룹과의 대화(연구관련 질문, 위협 인텔리전스 분석 등)</li> <li>-비디오 게임(old game)을 통한 홍보</li> </ul>
Armis	<ul style="list-style-type: none"> <li>-라이브 해킹 프로그램 운영</li> <li>-CEO, CTO 등 운영진과의 미팅</li> <li>-음식 제공</li> </ul>
Axonius	<ul style="list-style-type: none"> <li>-수석 보안 이사, Dan Trauner 발표 "Dogfooding Axonius: Unmanaged Applications Patching"</li> <li>-사이버 보안 자산 관리 플랫폼 제품 홍보</li> </ul>
BlackBerry	<ul style="list-style-type: none"> <li>-Cylance AI 홍보(Malware 방지 Endpoint 제품)</li> <li>-CylanceENDPOINT, CylanceGUARD, CylanceEDGE, CylanceINTELLIGENCE 등 제품 데모 시연</li> <li>-후드티 제공</li> </ul>
Cisco	<ul style="list-style-type: none"> <li>-"실무자 이점: XDR이 현재 올바른 접근 방식인 이유", Nick Biasini(아웃리치 책임자), AJ Shipley(위협 및 탐지, 대응 부사장) 발표</li> <li>-보안 솔루션 데모, Talos 연구원과의 대화 진행</li> <li>-자물쇠 해제 대회</li> </ul>
Claroty	<ul style="list-style-type: none"> <li>-주요 인프라 보호를 위한 솔루션 홍보</li> <li>-커스텀 물병 제공</li> </ul>
CrowdStrike	<ul style="list-style-type: none"> <li>-생성형 인공지능 기반 사이버보안 분석 AI Charlotte AI 홍보</li> <li>-CTO 세션 발표, "Smarter. Better. Faster. Stronger: How Generative AI Will be a Force Multiplier for Security Analysts."</li> <li>-아침식사 제공</li> </ul>
Cyders	<ul style="list-style-type: none"> <li>-강연 세션 운영, "In an AI-Centric World, Forewarned is Good but Forearmed is Better"</li> <li>-칵테일 파티 주관, 경영진 참석</li> </ul>
Darktrace	<ul style="list-style-type: none"> <li>-발표 세션 운영: SOC 강화, 위협관리, 공격 표면 관리, 이메일 및 클라우드 보안, 기술 통합</li> <li>-Darktrace HEAL 데모 시연: 사이버 공격 발생 시 복구</li> <li>-Darktrace Leader 및 전문가 미팅</li> <li>-칵테일 리셉션 주관</li> </ul>
Dazz	<ul style="list-style-type: none"> <li>-발표 세션 운영 "Dazz Remediation Cloud: The backbone of CNAPP" "Automate remediation with AI, LLM, and ChatGPT" "3</li> </ul>

	<p>biggest mistakes in securing SDLCs for cloud environments"</p> <p>-경품 추첨 진행</p>
DNSFilter	<p>-DNSFilter 제품 홍보 및 시연</p> <p>-차세대 실시간 도메인 위협 분류 및 차단 솔루션 홍보</p> <p>-Indycar 레이싱 전시</p>
ExtraHop Networks	<p>-발표 세션 운영</p> <p>-마술 이벤트를 통한 블랙박스 기술 홍보</p> <p>-상자 잠금 해제 이벤트를 통한 기념품 제공</p>
Fortra	<p>-포트폴리오 전체 데모 진행: 데이터 보호, 관리 서비스, 인프라 보호, 보안 인식 교육, 파일 전송, 피싱 보호 등</p> <p>-발표 세션 진행</p> <p>-물병 제공</p>
IBM	<p>-Space Rogue 책 사인회 진행(작가: Cris Thomas)</p>
Invicti	<p>-AppSec with Zero Noise 제품에 대해 전문가와 상담</p> <p>-웹 어플리케이션 보안 제품 데모</p> <p>-"실제 환경에서의 API 취약성 테스트", 화이트 페이퍼 제공</p> <p>-발표 세션 진행 및 기념품 제공</p>
KnowBe4	<p>-발표 세션 진행: 최고 연구 및 전략 책임자 발표</p> <p>-부스 내 전문가 미팅 진행</p> <p>-기념품 모자 제공</p>
Lacework	<p>-클라우드 기반 데이터 보호 플랫폼 홍보</p> <p>-자선활동을 위한 프로모션 진행</p>
Microsoft	<p>-Threat Intelligence Interactive Experience 홍보</p> <p>-제품 데모: Microsoft Security Copilot, Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for IoT, Azure Network Security, Microsoft Defender Threat Intelligence</p> <p>Microsoft Entra</p> <p>-발표 세션 진행(Red Canary, Quorum Cyber, Ontinue, PwC, Synack, Vectra AI 함께 진행)</p>
NEXT DLP	<p>-내부자 위협 및 데이터 보호 솔루션 Reveal 홍보</p> <p>-발표 세션 운영 및 경품 제공</p>
Noname Security	<p>-발표 세션 운영(30분 단위)</p> <p>-API 보안 전문가가 진행하는 커스터마이징 데모 제공</p> <p>-저녁식사 및 파티 제공</p>
Pentera	<p>-First Cyber Rap Battle을 이용한 홍보</p> <p>-엔드포인트 탐지 및 대응 솔루션 홍보</p>



Qualys	<ul style="list-style-type: none"> <li>-자사 제품 및 솔루션 홍보, 데모 시연</li> <li>-전문가와의 1:1 미팅 진행</li> <li>-발표 세션 진행 및 경품 제공</li> </ul>
SentinelOne	<ul style="list-style-type: none"> <li>-"HypeGPT: What LLMs Really Can and Can't Do for Security" 발표 진행</li> <li>-엔드포인트 제품, 클라우드 보호 제품 홍보 프레젠테이션 및 데모 시연</li> <li>-티셔츠 및 파티 제공</li> </ul>
Sophos	<ul style="list-style-type: none"> <li>-MDR 및 위협 인텔리전스 제품 발표</li> <li>-공격자가 AI를 활용하여 공격을 수행하는 새로운 방법 발표</li> </ul>
Splunk	<ul style="list-style-type: none"> <li>-데모 시연 및 프레젠테이션 발표</li> <li>-"Bluenomicon: The Network Defender's Compendium", 사이버 보안 리더십 전략, 사고 조사 및 대응 지침, 사이버 보안 일화를 제공하는 에세이 책 발표 및 제공</li> </ul>
Synack	<ul style="list-style-type: none"> <li>-취약점 탐색 방법 관련 데모 시연</li> <li>-음식 및 기념품, 추첨 행사 제공</li> <li>-위스키 시음 이벤트 및 경영진과의 1:1 미팅 제공</li> </ul>
Sysdig	<ul style="list-style-type: none"> <li>-허니팟 해킹 시연</li> <li>-취약한 허니팟 탐색 베팅 게임 이벤트 진행</li> <li>-공연 및 기념품 제공</li> </ul>
Syxsense	<ul style="list-style-type: none"> <li>-"Cortex Co-Pilot" 제품 홍보 및 데모 진행</li> <li>-발표 세션 운영</li> </ul>
Tenable	<ul style="list-style-type: none"> <li>-Tenable Nessus를 위한 해커톤 개최</li> <li>-SANS, 보안 인식에 대한 2023년 보고서 발표</li> </ul>
ThreatLocker	<ul style="list-style-type: none"> <li>-Threat Talk; 다양한 공격 및 방지에 대한 프레젠테이션</li> <li>-제로 트러스트 기반 엔드포인트 제품 데모 진행, 새로운 UI 및 확장 솔루션 홍보</li> <li>-경품 추첨 및 기념품 제공</li> </ul>
Trellix	<ul style="list-style-type: none"> <li>-랜섬웨어 위협 탐지 및 대응 솔루션, 개방형 XDR 플랫폼 홍보</li> <li>-발표 및 데모 세션 운영</li> </ul>
Trend Micro	<ul style="list-style-type: none"> <li>-Red Team 역할을 수행할 수 있는 사이버 보안 챌린지 개최</li> <li>-클라우드 기반 보안 플랫폼 홍보 및 데모 시연</li> </ul>
TXOne Networks	<ul style="list-style-type: none"> <li>-OT 중심 보안 솔루션 홍보 및 데모 시연</li> <li>-엔드포인트 탐지 관련 발표 세션 운영</li> </ul>
Uptycs	<ul style="list-style-type: none"> <li>-인프라 보안 관련 제품 홍보</li> <li>-전문가와의 대화 진행</li> </ul>

VMware Carbon Black	<ul style="list-style-type: none"> <li>-엔드포인트 제품인 Carbon Black 홍보</li> <li>-발표 세션 진행</li> </ul>
Wiz	<ul style="list-style-type: none"> <li>-사이버 보안 미래 주제 발표 진행</li> <li>-Azure Active Directory 해킹 발표</li> <li>-전문가 미팅 및 파티, 기념품 제공</li> </ul>
ZeroFox	<ul style="list-style-type: none"> <li>-물리적 보안 인텔리전스 제품 홍보 및 발표</li> <li>-다크웹 보안 및 위협 인텔리전스 홍보</li> <li>-ZeroFox Dark Web Intelligence 제품 홍보</li> </ul>

보안 뉴스

#### 4. 블랙햇 USA 2023 돋보기

세계 최대 사이버 보안 콘퍼런스(학회) 'Black Hat USA 2023'이 8월 7일부터 10일까지 미국 라스베이거스 만달레이 호텔에서 성대하게 진행됨. 첫날 학회 등록 대기 줄이 호텔 입구까지 늘어선 모습은 이 행사가 사이버 보안 분야에서 어떤 의미를 갖는지 보여주는 대표적인 모습이었음. 행사에 모인 다양한 인증 및 연령의 참석자들은 등록 후 자신이 관심 있는 세션에 참여하기 위해 발 빠르게 움직였음. 참가자들은 발급받은 배지를 목에 패용한 후, 이동했는데 자신의 소속 및 직업이 적혀 있는 배지를 통해 아마존 및 마이크로소프트와 같은 유수의 글로벌 대기업 및 각 국가의 정보기관 및 군인 등을 통해 이번 행사의 위상을 짐작할 수 있었음.

##### □ 여전히 뜨거운 감자 'Large Language Model(LLM)'

AI의 발전과 더불어 ChatGPT와 같은 LLM의 등장은 Computer Science 분야에 시대의 전환점을 맞이하게 하였고, 이 기술은 많은 반향을 일으키며 LLM의 인해 인공지능을 보다 다양한 목적으로 폭넓게 사용할 수 있게 됨. 따라서 사이버 보안에서 인공지능이 차지하는 비중은 더욱 중요해졌고, 위험성 역시 강조되고 있음. 트레이닝 세션에서도 ML 혹은 LLM을 이용한 해킹 기술 교육이 가장 뜨거운 인기를 차지하였으며, 행사의 첫 번째 키노트인 Azeria Lab의 창립자 Maria Markstedter는 Guardians of the AI Era: Navigating the Cybersecurity Landscape of Tomorrow(인공지능의 발전에 따른 사이버보안의 변화와 미래) 주제로 인공지능 분야의 동향과 미래의 시장성, 인공지능의 발전과 함께 제기되는 인공지능의 모호성에 따른 위험성을 지적함. 브리핑 패스에서도 인공지능과 관련된 세션들이 다수를 차지하며 인공지능의 인기를 다시금 느낄 수 있었음.

##### □ '우크라이나-러시아' 전쟁을 통한 사이버 보안의 국가적 중요성

장내에서 심심치 않게 CIA와 같은 국가 정보기관 보안 담당자와 군인들을 마주칠 수 있었음. 아직 진행 중인 '우크라이나-러시아' 전쟁에서 양 국가는 다양한 방법으로 사이버전을 전쟁 발발 전부터 시도했고 현재에도 정보 탈취 및 전력 약화를 위해 전투 병력과 함께 복합적으로 진행되고 있음이 여러 기사를 통해 알려진 바 있음. 이번 행사에서는 빅터 조라 우크라이나 특수통신 및 정보보호국 부회장과 젠 이스터리 미국 CISA 국장과의 대담을 진행하며 미국이 우크라이나 내에서 사이버 인프라 구축과 인력양성에 힘을 쏟고 있으며 사이버공격 및 대비 훈련을 통해 러시아를 상대로 공격

및 방어를 펼치고 있음을 알렸음. 또한, 다양한 세션들에서 IoT 기기 및 하드웨어 해킹 및 보안기술을 군사 기술과 접목해 소개함. 현 국제정세 속에서 사이버 보안 기술이 갖는 위상과 중요성을 되새길 수 있는 자리였음.

한낮 기온 40도의 육박하는 찜찜 끓는 사막 위의 도시인 라스베이거스에서 열린 블랙햇 USA 2023은 전 세계에서 모인 참석자들이 다양한 주제로 나흘간 사이버 보안 및 해킹 기술의 현주소와 미래 동향에 대해 정보에 대해 교류를 나눴고, 현재 우리의 기술 수준 및 방향을 다른 참가자들을 통해 확인할 수 있는 좋은 기회가 됐음.



보안뉴스

## 5. 글로벌 트렌드와 발 맞추기

이번 블랙햇에서 주로 다루었던 주제는 단연 인공지능과 리질리언스 구축이었음. 특히, 블랙햇 기간 중 진행된 3개의 키노트 세션 모두 인공지능과 리질리언스 구축에 대해 이야기하며 현재 인공지능의 발전으로 인한 IT 업계에 대변화에 관련 전문가들이 적극적으로 새로운 질서를 구축하기를 희망함.

- 켄바 월든(Kemba Walden) 현 백악관 국가사이버국장은 블랙햇 키노트세션 마지막 연사로 등장하여 인공지능의 발전으로 더욱 활발해진 오픈소스의 보안 연구의 필요성에 대해 강조하면서 어려서부터의 보안 교육 등을 통해 많은 사람이 보안에 대해 친숙해지고 더 나아가 보안전문가로 거듭나갈 수 있도록 해야 한다고 언급하며 향후의 보안 생태계는 현재의 정책과 교육에 달려있다고 강조함. 또한, 1일차 오후에 진행된 키노트 또한 우크라이나 사태를 통하여 더욱 강력한 리질리언스를 구축해야 한다고 강조함.
- 더 나아가 미국 고등연구계획국(DARPA)은 AIXCC(AI Cyber Challenge) 대회 개최를 발표하는 등 앞으로 더욱 인공지능에 관한 보안 연구를 독려하고 있어 경쟁 또한 더욱 치열해질 것으로 예상됨.
- 앞으로 국내뿐만 아니라 전 세계 보안업계는 현재 제기되고 있는 인공지능의 다양한 보안 문제점을 해결하기 위한 연구에 집중하게 될 것이며, 또한 인공지능을 이용한 보안솔루션 연구에도 집중하게 될 것으로 보임.
- 또한, 인공지능의 보안 문제점뿐만 아니라, 인공지능을 이용한 공격 또한 현재 다양하게 개발되고 있는 만큼, 앞으로는 이를 보다 효과적으로 방어해낼 지가 보안업계의 주요 화두가 될 것으로 보임
- 리질리언스 구축의 경우, 앞으로 더욱 다양한 연구기관, 기업들이 리질리언스 구축에 참여하게 될 것으로 예상되며, 우리나라 보안업계도 리질리언스 구축에 있어 적지 않은 영향을 받을 것으로 전망됨. 따라서 더욱 적극적인 참여로 새롭게 정의되는 보안 생태계에서 우리나라가 한 축을 맡을 수 있도록 다양한 연구 및 협력이 필요하다는 판단임.

## Chapter II. Defcon 31 Review





**THEME: THE FUTURE WILL PREVAIL**

**ONE BADGE FULL ACCESS**

**PRICE: \$460**

보안뉴스

# Chapter 2.

# DEF CON 31

# Review

**KEYWORDS**

HACKING, VILLAGE, DEMO LABS

MAPLE MALLARD MAGISTRATES,

CTF(CAPTURE THE FLAG)

## 1. DEF CON 31

### 가. 개요

데프콘은 1993년 제프 모스가 Platinum Net 회원인 친구의 송별회에 각 분야의 해커들을 초대한 파티에서 시작되었으며 해킹 기술을 깊이 있게 공유하고 토론할 수 있도록 구성된 매년 라스베이거스에서 열리는 세계 최대 규모의 컨퍼런스 및 해킹 대회임. 이 대회는 사이버 보안 및 해킹에 중점을 두고 전 세계에서 수천 명의 해커, 사이버 보안 전문가 및 정부기관 종사자들이 모임.

올해 데프콘은 Caesars Forum 메인 행사장을 비롯해 Flamingo, Harrah's, LINQ 호텔에서 분산 개최됨.

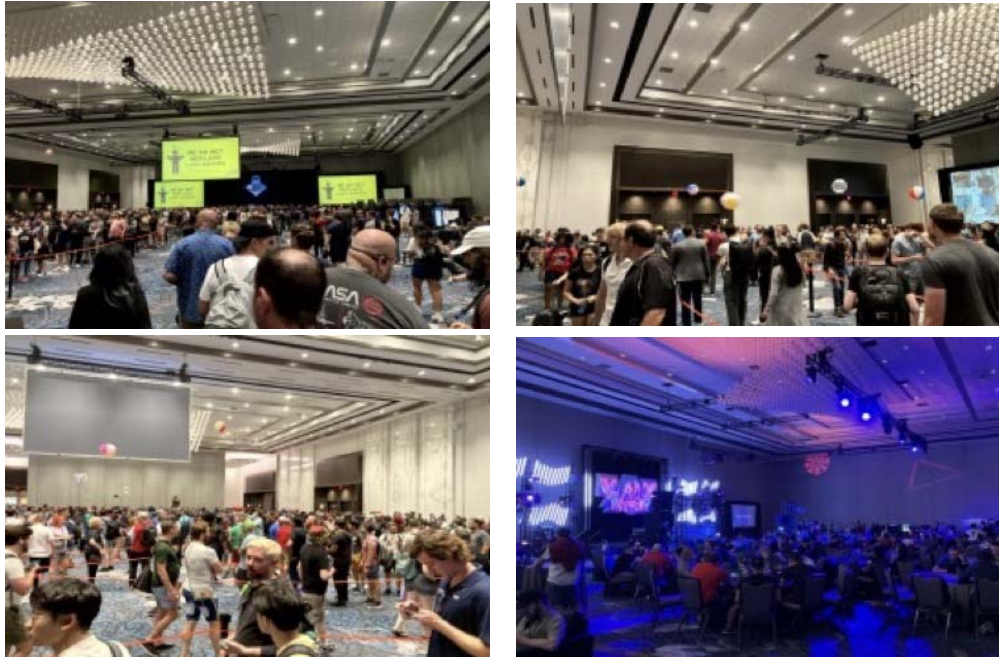


〈 데프콘 행사장 내·외부 전경 〉

전체 32개 빌리지와 43개에 달하는 콘테스트 및 이벤트, 파티, 미팅, 워크숍, 데모랩, CTF 해킹대회 등 많은 참여 행사와 볼거리가 자유로운 분위기 속에서 열렸음.

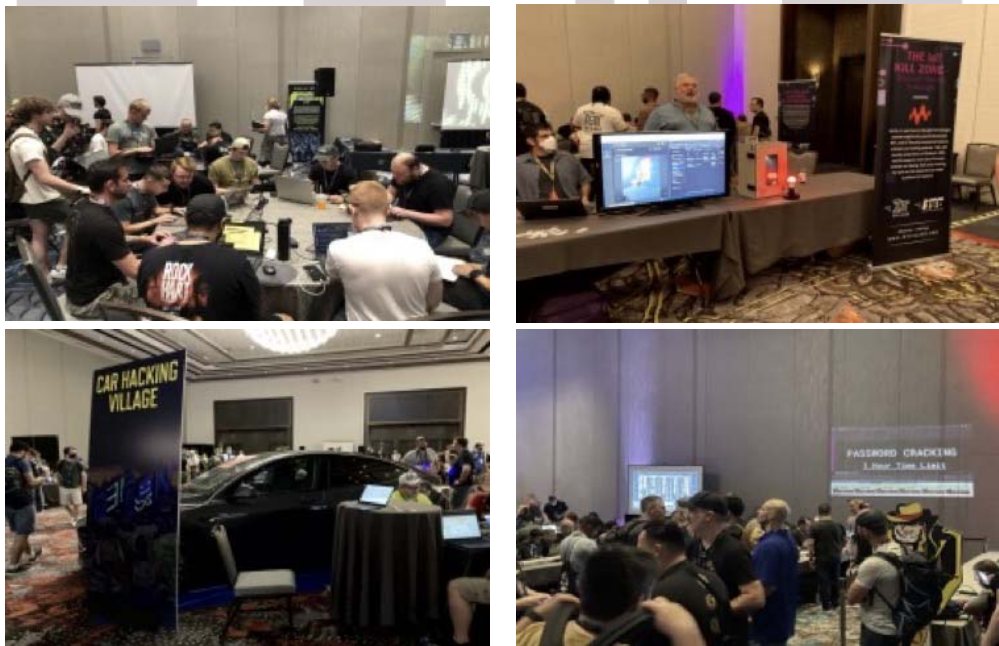
이러한 자유로운 분위기는 등록을 위해 길게 줄을 서서 기다리는 곳곳에서 풍선을 하늘 높이 튕겨가며 긴 시간을 대기하던 참가자들은 물론 밝은 표정으로 담소를 나누는 ChillOut 룸에서도 쉽게 찾아볼 수 있었음.





〈 데프콘 등록장 전경 〉

나. Village



〈 데프콘 빌리지 부스 전경 〉

Village는 항공, 우주 보안 부문의 AeroSpace Village, ChatGPT, StableDiffusion, 멀웨어 탐지기, ML 방화벽 및 기타 AI 기반의 보안 분야 AI Village, 소프트웨어 취약점을 악용하고 소프트웨어를 보호하는



AppSec Village, 실제 차량을 해킹할 수 있는 개방적이고 협력적인 공간인 Car Hacking Village, 생명공학, 의료, 제약 등의 실습 위주의 학습랩을 제공하는 BioHacking Village, POS 단말기, ATM, 디지털 지갑 등의 결제 기술 관련 Payment Village, 통신 보안 관련 Telecom Village 등 32개의 분야로 구별되어 행사장 곳곳에 흩어져 진행됨. Car Hacking의 경우 1위 상품으로 Gforce ZM Bike를 주는 등 각 Village 내에서 열리는 콘테스트도 상금이 결코 작지 않았음.



#### 〈 부모와 아이가 함께 프로그램 참여 〉

또한, 아이들이 참여할 수 있는 다양한 프로그램 및 공간들이 존재했는데, 아버지와 아이가 같이 참여해 아버지가 아이에게 가르쳐주는 모습도 쉽게 찾아볼 수 있었음.

#### 다. 데모랩

데모랩은 데프콘 커뮤니티 회원들이 개인 오픈소스 기술 프로젝트를 공유하는 공간으로 Andorid 바이트코드를 한번에 하나씩 실행할 수 있는 환경을 구축하여 대량의 문자열 난독화 기술이 적용된 멀웨어를 쉽게 처리하는 KATALINA, 오픈소스 클라우드 보안 자동화 프레임워크인 Dracon, 2023년 Metasploit에 새롭게 추가된 Active Directory 공격 워크플로우 및 진공청소기 로봇의 다양한 모델에 대해 쉽게 루팅하는 데모 등 36개의 다양한 소프트웨어 및 하드웨어 관련 데모가 Unity, Council, Caucus, Committee, Society, Accord Boardroom에서 시연됨.

#### 라. 키노트

포드 자동차를 랜섬웨어로 만드는 방법, IDTECH 제품에 대해 NFC를 통한 결제 단말기 및 ATM의 비접촉식 오버플로 코드 실행, 의료 데이터 해킹 등 사람들의 흥미를 끌 수 있는 다양한 세션들도 마련됨.



〈 키노트 현장 전경 및 제품 시연 〉

마. DEF CON CTF

DEF CON에서 가장 주목받는 행사는 바로 DEF CON CTF이다. 올해는 5월에 DEF CON CTF 예선전이 치러졌으며 총 1,828개 팀이 참여하여 535개 팀만이 점수를 획득함. Blue Water팀이 3,753점을 획득하여 예선전 1위를 차지함.

Place	Team Name	Score
1	Blue Water	3753
2	The Parliament of Ducks	3499
3	Orgakraut	3466
4	SuperDiceCode	3398
5	TWN48	3236
6	StrawHat	3204
7	Norsecode'23	3090
8	mhackeroni	2920
9	P1G_BuT_S4D	2745
10	Shellphish	2500
11	undef1ned	2481
12	HypeBoy	2417

〈 DEF CON CTF 예선전 순위 〉

8월 11일부터 13일까지 DEF CON 31에서는 예선의 상위 11개 팀과 작년 우승팀(Maple Mallard Magistrates)이 결승에 진출하여 DEF CON CTF 본선을 치렀음. 행사장에는 결승에 진출한 12개 팀들이 3일간의 공격-방어 활동을 통해 점수를 획득하며 3일 연속 해킹 끝에 Maple Mallard Magistrates 팀이 압도적인 점수 차를 보이며 작년의 타이틀을 성공적으로 방어함. Maple Mallard Magistrates(MMM)은 한국의 The Duck(티오리) 팀 15명과 미국 Carnegie Mellon 대학의 사이버보안 동아리 PPP팀 15명, 그리고 캐나다 British Columbia 대학 사이버보안 동아리팀 Maple Bacon 15명이 모인 연합팀임. 또한, 한국의 이종호 멘토가 이끌고 BoB 수료생이 주축이 된 14명으로 구성된 HypeBoy팀은 4위를 차지함. SuperDiceCode 팀은 BoB 출신 수료생들과 미국 팀의 연합으로 구성되어 있으며 8위를 차지했음.

Place	Team Name	Atk	Def	KotH	Live	Total
1	Maple Mallard Magistrates	6436	329	1699	1337	9801
2	Blue Water	4879	208	1741	600	7428
3	TWN48	5128	370	758	500	6756
4	HypeBoy	3545	163	1086	1000	5794
5	StrawHat	3788	115	662	900	5465
6	Norsecode	4411	108	196	700	5415
7	P1G_BuT_S4D	3358	75	1360	600	5393
8	SuperDiceCode	3992	143	680	500	5315
9	Orgakraut	3839	165	249	500	4753
10	mhackeroni	3382	236	144	800	4562
11	Shellphish	3077	110	393	700	4280
12	Under1ned	3129	153	370	500	4152

〈 DEF CON CTF 결승 순위 〉

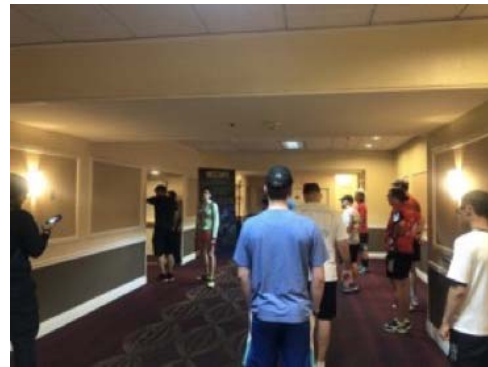


〈 데프콘 CTF 행사 전경 〉

보안뉴스

## 2. DEF CON.run

DEF CON은 전 세계의 해커, 해킹에 관심이 있는 일반인 및 사이버 보안 관계자 등 다양한 성격의 참가자로 구성되어 있음. 해킹이라는 하나의 주제로 연결되어 있기에 외부 활동과는 다소 동떨어져 있을 것으로 생각되지만, 데프콘은 러닝 이벤트를 열어 참가자들이 라스베이거스를 함께 달리며 서로 사교 모임을 할 수 있도록 하고 있음. 이전 데프콘까지 이 행사는 게릴라 이벤트로 진행됐으나 이번 데프콘 31부터 정식 행사로 발전함. 데프콘 행사 기간인 4일간 진행되며 참가를 원하는 인원은 등록을 통하여 이벤트에 참여할 수 있었음. 오전 6시에 Harrahs 호텔의 모이는 장소에서 만나 원하는 코스의 그룹에 가입하게 됨. 달리기 전, 간단히 코스 소개와 에너지 젤, 그룹 간 인사가 진행되는데, 오전 6시에도 라스베이거스의 외부 기온은 30도이기에 바로 러닝을 시작함. 약 50~60명이 참여하여 각각의 그룹으로 나뉘었음.



〈 DEF CON.run 정보 및 행사장 전경 〉





〈 DEF CON.run 행사 〉

러닝 기록은 Strava 앱을 통해 공유하고 서로의 소셜 네트워킹을 통해 나누게 됨. 러닝 동안 참가자들은 간단한 인사와 '어디서 왔는지?', '데프콘 참여 목적', 직업 등 여느 달리기 모임과 같은 이야기를 나누며 러닝이 진행됨. 함께 달린 참가자 중 오스트리아에서 온 학생, 미국 내에서 참여한 보안 연구원, 비행 시뮬레이터로 빌리지에 참여한 업체 직원, 캘리포니아 공과대학 강사 등 다양한 인원이 모여 코스를 달렸음. 목표까지 러닝을 완료한 후, 그룹 참가자들은 사진을 찍고 모였던 장소로 돌아가 결과를 관계자에게 확인함. 사흘째에 처음 참여했지만 서로 반겨주어 어색하지 않게 어울릴 수 있었고, 모니터 앞에 앉아만 있을 것 같은 참가자들이 땀을 흘리는 행사에 참여하는 것이 꽤 신선하다고 생각됐음.