

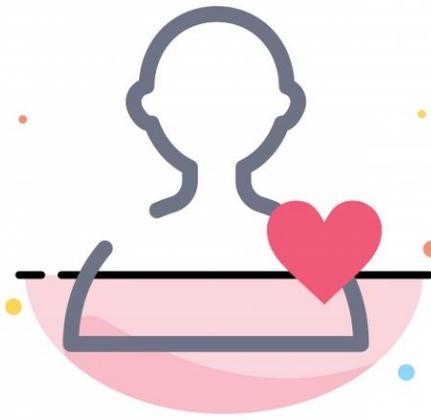
나도 될 수 있다! 화이트 해커

(2020. 08. 01 - 2020. 08. 31)



CONTENTS

학과소식



사이버보안공학과는 꿈과 미래를 정하고,
달려가는 학생들로 모여 있는 학과 입니다.

[한마디]

성공하기까지는 항상 실패를 거친다.

- 미키루니



사이버보안공학과
Cyber Security Engineering

사이버보안공학과 소식

건양대, 조인희 前 국군지휘통신사령관 초빙 강의



건양대학교 사이버보안공학과가 내달 1일부터 재학생을 대상으로 조인희 전 국군 지휘통신사령관 초빙 강의를 진행한다.

조 전 사령관은 국방 네트워크 작전·사이버전 방어 분야 전문가로, 제33대 국군지휘통신사령관을 역임했다. 전역 후 국방과학연구소 전문위원, 국방정보통신협회 수석부회장, 국방CIO 자문위원, 합동참모본부 정책발전위원 등을 지냈다.

건양대 사이버보안공학과는 군사 분야 사이버 인력 수요가 증가함에 따라, 사회수요 맞춤형 인재 양성을 실현하고 학과 체질 개선에 기여하고자 조 전 사령관을 초빙했다.

조 전 사령관은 2학기부터 사이버보안공학과 4학년 교과목 1개를 맡아 강의를 펼칠 예정이다.

사이버보안공학과 김동원 교수는 "대한민국을 방어할 국방 분야 사이버보안 전문가를 양성하는 데 있어 조 전 사령관의 역할을 기대한다"며 "이번 기회를 잘 살려 건양대 사이버보안공학과를 한 단계 더 성장시키는데 기여할 것"이라고 말했다.

사이버보안공학과 소식

사이버보안공학과 2020 대학생 금융보안캠프

참여자

- 서경원 남원정 금강민 이도희
이동규 이상아 정영석 유수연
진익상 김태현 조민기 이승호



김태현 학생이 2020 대학생 금융보안캠프에서 은상을 수상함.

수상소감

- 전국에 있는 대학교들 중 우리 건양대라는 학교의 이름을 올릴 수 있는 기회가 되어 큰 영광입니다. 앞으로 더 많은 배움을 통해 사회에 기여하는 사람이 되도록 열심히 하겠습니다.

사이버보안공학과 소식

여름방학 단기 현장실습

여름방학동안 사이버보안공학과 학생 7명이 공공기관, 산업체 등에서 현장실습을 잘 수행하고 마쳤습니다.

박천용, 박영우 두 학생은 국민연금관리공단에서 개인정보보호 실무 업무를 현장실습하였고, 이상아, 지성식, 손지혜, 복현아, 이보혜 학생은 민간보안전문기업에서 보안컨설팅 등의 실무를 산업체 현장 체계적인 실습을 완료하였습니다.

현장실습 지도교수인 정승욱, 이후기 두 교수님이 해당 기관을 방문하였을 때 학생들이 현장실습에 임하는 자세가 매우 우수하다는 각 기관 관계자의 호평을 받았습니다.

2020 2학기 장기 현장실습

사이버보안공학과 총 5명의 학생(최지현, 허연주, 박영우, 복현아, 이보혜)이 2학기 현장실습을 나가게 되었습니다. 해당 학생들은 15주간 정보보호 전문기업인 티앤디소프트, 앤오비즈, 엘엔제이테크에서 보안컨설팅, 보안엔지니어링 등 산업체의 실무 업무를 익힐 수 있는 좋은 기회가 될 것 같습니다.

	이름	학년	실습회사명
1	최지현	4학년	티앤디소프트
2	허연주	4학년	티앤디소프트
3	박영우	4학년	앤오비즈
4	복현아	4학년	앤오비즈
5	이보혜	4학년	엘엔제이테크



사이버보안공학과 소식

여름방학 단기 현장실습

여름방학 단기 현장실습을 수료 학생 명단

- 1) 국민연금공단 : 박천용, 박영우
- 공공기관의 개인정보보호 실무 업무 현장실습
- 2) 티앤디소프트 : 지성식, 이상아
- 보안컨설팅 실무 업무 현장실습
- 3) 손지혜, 복현아, 이보혜



사이버보안공학과 소식

PRIME 창의융합대학 Online 입시설명회

PRIME 창의융합대학

새내기 여러분 환영합니다 ———

2020 건양대학교 PRIME 창의융합대학 Online 입시설명회

<https://www.facebook.com/watch/?v=313820949731834&extid=GqdTtLwKSiurUQW4>

위 링크에 사이버보안공학과에 대한
많은 내용이 있으니 영상을 참고해주세요!



사이버보안공학과 소식

사이버보안공학과 입시 전형

			모집인원	전형방법
수시	학생부교과	일반학생부전형	25	<ul style="list-style-type: none"> 학생부 교과 100%, 학년별 4개(국어, 영어, 수학, 사회/과학 교과별 1개 과목) 과목 총 12개 과목 반영 $\sum(\text{과목별등급} \times \text{과목별이수단위}) + \sum(\text{과목별 이수 단위})$ 수능최저학력 없음 지역인재전형 대상: (충청권: 대전, 충남, 충북, 세종지역) 소재 고등학교 입학부 터 졸업(예정)한 자
		지역인재전형	5	
	학생부종합	건양사람인 전형	10	<ul style="list-style-type: none"> 1단계[학생부종합(교과/비교과) 100%] 3배수 2단계 [1단계 60% + 면접 40%] 면접: 인성 30%, 발전가능성 40%, 전공적합성 30% 수능최저학력기준 없음
	정원의 전형	농어촌전형	2	<ul style="list-style-type: none"> 농어촌 소재지 중학교 입학 시부터 고등학교 졸업시 까지 교육과정을 이수하고 본인 및 부모가 농어촌 지역에 거주하는 자 농어촌 소재지 학교에서 초, 중, 고 전 교육과정을 이수하고 농어촌 지역에 거주한 자 검정고시출신자 및 특수목적고 출신자 제외
특성화고교졸업자		2	<ul style="list-style-type: none"> 특성화고등학교 졸업(예정)자 특성화고와 같은 교육과정을 운영하는 학과가 있는 종합고 포함 지원모집단위에 해당되는 특성화고교 동일계열 기준 학과의 교육과정을 이수한자 또는 지원 모집단위에 해당되는 특성화고등학교 전문교과를 30단위 이상 이수한자 	
정시			0	수시 미달시

2020학년도 입시 결과

	모집인원	지원인원	지원율
학생부교과전형	25	120	4.8
지역인재전형 (교과)	5	23	4.6
농어촌학생전형	2	4	2
건양사람인	10	25	2.5



사이버보안공학과 소식

건양대학교 전형일정

전형 일정

구 분		기 간(일 시)	비 고
원서접수	인터넷	2020.9.23(수)~28(월) 19:00까지	·인터넷접수(진학사)
	현장접수[하루만 운영]	2020.9.28(월) 09:00~18:00까지	·대전메디컬캠퍼스 죽헌정보관 L층 입학처
서류제출	등기우편 발송	2020.9.23(수)~10.8(목) 18:00까지	·세부사항 27p 참조 필수
1단계 합격자 발표	군사학전형 1단계 합격자 발표	2020.10.8(목) 16:00	·입학홈페이지 합격자 조회 (https://ipsi.konyang.ac.kr) ※ 개별 통보 없음
	·특기자전형 면접대상자 발표 ·창업특기자전형 면접대상자 발표 ·지역인재전형[교과] : 의학과 면접대상자 발표	2020.10.30(금) 16:00	
	학생부종합전형 면접대상자 발표	2020.11.11(수) 16:00	
	의학과 면접대상자 발표 일반학생[최저], 지역인재[최저], 농어촌	2020.12.24(목) 16:00	
면접고사	·특기자전형 ·창업특기자전형 ·지역인재전형[교과] : 의학과	2020.11.7(토)	·대전 메디컬캠퍼스 ·논산 창의융합캠퍼스 ※ 면접은 대상자에 따라 오전, 오후 분할 시행 ※ 면접시간은 추후 입학홈페이지를 통해 공지 예정
	학생부종합전형	2020.11.21(토)	
	의학과 일반학생[최저], 지역인재[최저], 농어촌	2020.12.25(금)	
군사학전형 2차 평가	인성검사, 신체검사, 체력검정, 면접	2020.10.26(월)~28(수)	·논산 창의융합캠퍼스
전공실기 고사	재활퍼스널트레이닝학과 전공실기고사	2020.10.28(수)	·논산 창의융합캠퍼스 ※ 일반학생전형[실기]만 해당
최종 합격자 발표	수능최저학력기준 미적용 모집단위	2020.11.25(수) 16:00	·입학홈페이지 합격자 조회 (https://ipsi.konyang.ac.kr) ※ 개별 통보 없음
	수능최저학력기준 적용 모집단위 [의학과(지역[교과] 제외), 군사학과]	2020.12.27(일) 16:00	
최초합격자 등록 기간		2020.12.28(월)~30(수) 16:00까지	·예치금 납부
총원합격 통보 및 등록 기간		2020.12.31(목)~2021.1.5(화) 16:00까지 ※ 총원통보마감은 1.4(월) 21시까지, 1.5(화)는 등록만 가능	·총원합격 통보는 지원 학과 에서 유선으로 통보
최종 등록금 납부		2021.2.8(월)~2.10(수)	·농협 및 하나은행 전국지점



사이버보안 주요 이슈 (ISSUE)

» 다시 한 번 북한 찍은 미국, 이번엔 암호화폐 계정 노린다

[보안뉴스 문가용 기자] 미국 정부가 280개의 불법 암호화폐 계정들을 압수하려는 목표를 가지고 있다고 발표했다. 이 계정들은 북한의 정부 지원 해커들이 운영하는 것으로 알려져 있으며, 공격자들은 이를 통해 수천 만 달러에 해당하는 암호화폐를 부당하게 가져간다고 한다. 이 돈은 중국인으로 주로 구성된 세탁자 및 자금 운반책들이 처리한다.

미국 사법부는 지난 주 북한을 대상으로 한 민사몰수 항소를 제기했다. 특히 작년에 발생한 두 가지 암호화폐 거래소 탈취 사건을 바탕으로 이러한 내용의 항소장이 마련되었는데, 이 두 사건 모두 북한 해커들의 소행이라고 사법부는 주장하고 있으며, 중국인들도 돈 세탁에 연루되어 있다고 한다. 해커들이 가져간 돈은 2억 5천만 달러로 추정된다.

사법부의 법무부 보좌관 대행인 브라이언 래빗(Brian Rabbitt)은 "이 고소장을 통해 북한의 사이버 공격자들과 중국의 암호화폐 세탁 전문 집단 사이의 커넥션을 확실히 공개했다"고 설명했다.

이번에 공개된 두 가지 사건은 작년 7월과 9월에 일어난 것으로, 7월 사건에서 해커들은 27만 달러가 넘는 돈에 해당하는 암호화폐와 토큰을 훔쳐냈다. 여기에는 프로톤 토큰(Proton Token), 플레이게임(PlayGame) 토큰, IHT 리얼 이스테이트 프로토콜(IHT Real Estate Protocol) 토큰 등이 포함되어 있었다. 이 토큰과 가상 화폐들은 여러 교환소를 통해 세탁되었다.

9월 사건의 경우, 북한과 관련이 있는 해커들이 이름을 밝히지 않은 회사의 암호화폐 지갑에 접근하는 데 성공한 것부터 시작됐다고 한다. 뿐만 아니라 해당 기업의 자산이 마련되어 있던 플랫폼과, 그 회사의 파트너들의 자산이 저장되어 있던 플랫폼에까지 접근할 수 있었다. 해커들은 250만 달러의 돈을 훔쳐갔고, 약 100개 계정으로 나누어 송금되는 세탁 과정을 거쳤다.

지난 9월 미국 정부는 북한의 공격 단체인 라자루스에 대한 제재를 선포했다. 이에 따라 라자루스와 관련이 있는 모든 형태의 자산들은 미국 영토 내에서 동결 및 차단되었다. 뿐만 아니라 라자루스와 관련이 있는 하위 단체인 블루노로프(Bluenoroff)와 안다리엘(Andariel)도 제재 대상에 포함되었다. 이 세 단체 전부 북한의 정찰총국 소속인 것으로 보인다.

라자루스는 최근 암호화폐 거래소 및 지갑을 노리는 공격을 다시 시작했다. 특히 최근에는 링크드인 플랫폼의 비밀 메시지를 통해 '당신을 영입하고 싶다'거나 '좋은 직책이 있어 제안한다'는 식으로 블록체인 산업 종사자들에게 접근하고 있다는 경고가 얼마 전 나온 바 있다. 소셜 엔지니어링 공격으로 금전적 이득을 취하려 호시탐탐 기회를 노리고 있는 것이다. 이번 사법부의 움직임은 미국 정부의 '북한 관련 사이버 공격 행위 근절시키기'의 일환으로 이뤄진 일이다. 미국 법무부 차관인 존 데머스(John Demers)는 언론 발표를 통해 "북한의 공격을 전부 다 막기는 힘들고, 북한 역시 스스로 그만두지 않을 것이지만, 이런 미국 사법부의 움직임에 부담감을 하나도 느끼지 않을 수는 없다"고 오늘 사법부의 발표 동기를 설명했다.

"사법부는 이번 몰수 소송을 통해 강력한 메시지를 북한에 전달하고자 합니다. 북한만이 아니라 미국의 자산과 기업, 시민들에게 피해를 입히는 그 모든 시도와 전략들을 근절시키기 위해 미국은 최선을 다할 것입니다. 그러므로 미국을 대상으로 사이버 범죄를 저지를 때는 반드시 기억하십시오. 우리가 늘 뒤에 있다는 것을요."

사이버보안 주요 이슈 (ISSUE)

» 인스타그램 고객 지원 센터 위장한 공격자들 주의보

[보안뉴스 문가용 기자] 터키어를 구사하는 사이버 범죄자들이 인스타그램 사용자들에게 메시지를 보내고 있다. 마치 인스타그램 고객 지원 센터에서 보낸 것처럼 꾸며진 이 메시지는 인스타그램 로그인 정보를 노린다고 한다.

보안 전문가들에 의하면 공격자들이 노리는 건 유명인, 스타트업 오너 등 팔로워 규모가 뒷받침 되는 사용자들이다. 이 중 1만 6천 명의 팔로워를 보유한 경찰이 공격에 포함되면서 수사가 시작됐다고 한다.

기존 인스타그램 겨냥 공격이 이메일로 인스타 링크를 보내는 방식으로 진행되었다면 이 공격은 인스타그램 플랫폼에서 이뤄진다는 특징을 가지고 있다. 공격자들은 고객 지원 센터(Instagram Help Center)로 스스로를 위장하고 "당신의 계정이 저작권 위반 소송 대상이 되었다"는 알림 메시지를 보낸다. 그러면서 "곧 삭제될 것"이라고 경고한다.

공격자들은 항소를 위해서는 자신들이 전송한 링크를 누르라고 하는데, 이 링크가 바로 피싱 링크다. 보안 업체 트렌드 마이크로(Trend Micro)에 의하면 "이 링크를 누르면 사용자 이름을 입력해야 하는 페이지로 접속된다"고 설명한다. 입력한 후 '다음' 버튼을 누르면 화면이 바뀌는데, 여기에서 피해자는 이름, 비밀번호, 이메일 주소, 이메일 비밀번호를 입력하라고 안내받는다.

이렇게 크리덴셜을 가져가는 데 성공한 공격자들은, 이 정보를 가지고 로그인을 하고, 계정에 연결된 핸드폰 번호가 있다면 이 연결성을 해제시킨다. 그 다음 계정에 연결된 이메일을 바꾼다. 이 단계에서 공격자들은 이미 이메일 계정 크리덴셜도 가지고 있는 상태이기 때문에 이메일도 침해할 수 있게 된다.

인스타그램은 공격자들이 자주 노리는 플랫폼이다. 인스타그램 계정을 훔치기 위한 피싱 캠페인은 꾸준히 이어져 오고 있다. 작년에는 사용자의 계정을 '확인'하라는 이메일이 인스타그램 사용자들 사이에서 퍼지기도 했었다. 사용자가 '확인' 버튼을 누르는 순간 피싱 페이지로 연결되고, 여기서 사용자들은 각종 크리덴셜을 빼앗겼다.

트렌드 마이크로에 의하면 이번 공격은 꽤나 높은 성공률을 거뒀다고 한다. "이번 피해자들 중에 유명인이 많다는 것이 추가 범죄의 변수가 될 수 있습니다. 일부 피해자들은 구글에 검색이 될 정도로 유명합니다. 검색된 정보와 인스타그램 정보를 합쳤을 때 각종 협박을 하는 게 가능합니다. 심지어 인스타그램 비밀번호를 다른 서비스에도 똑같이 사용한다면, 피해는 더 커질 수 있습니다."

트렌드 마이크로는 인스타그램 사용자들에게 "정상적으로 보이는 사이트라고 하더라도 계정 정보를 입력하라고 요구한다면 일단 의심하고 보라"고 권장한다

사이버보안 주요 이슈 (ISSUE)

» 전 세계 9천여 대 서버·PC '폼북' 악성코드에 당했다! 한국 311대 감염

[보안뉴스 권 준 기자] 전 세계 9천여 대의 서버 또는 개인 PC가 악성코드의 일종인 폼북(FormBook) 봇넷에 감염된 것으로 추정된다.

다크웹 위협정보 탐지 전문업체 에스투더블유랩(S2WLAB)은 다크웹에서 폼북의 운영·관리용으로 추정되는 사이트를 탐지해 현재 분석 중에 있다고 밝혔다. 이는 최신 봇넷이 전 세계를 대상으로 다크웹에서 체계적으로 관리되는 정황을 탐지한 첫 사례에 해당된다.

폼북은 이메일 첨부파일 등 다양한 형태로 감염되며, PC에 설치되면 해당 PC의 계정 정보, 데이터 통신 내용 등을 지속적으로 명령제어(C&C) 서버로 전송된다. 폼북은 다크웹에서 판매되고 있는 악성코드의 일종으로 여러 버전이 있으나, 현재 발견된 버전은 최신 변종 형태로 추정된다.

에스투더블유랩은 9천여 개 PC의 IP 주소 중에서 국내로 특정되는 IP에 대해서 우선적으로 파악해 한국인터넷진흥원 등 관련기관에 전달했으며, 폼북에 감염된 서버나 PC를 보유한 기업 및 기관은 21일 모두 대응조치가 완료된 것으로 알려졌다.

현재 폼북 악성코드의 최대 확산 국가는 중국(1,976대), 터키(647대), 미국(566대), 인도(480대) 순으로, 한국의 경우 311대로 확산대수 기준 7위에 해당되는 것으로 분석됐다. 최초 감염지는 유럽으로, 감염 PC 대수는 실시간으로 증감하고 있으며 올해 6~7월을 기점으로 폭발적인 증가세를 보이고 있는 것으로 드러났다.

감염 IP 분석 결과에 따르면 C&C 서버와 통신이 매우 짧게 이뤄진 경우도 있지만, 장시간 동일한 C&C 서버와 통신이 진행된 경우도 있어 지속적인 정보 탈취 가능성 등 추가 피해가 우려된다.

에스투더블유랩의 서상덕 대표는 "다크웹발 위협이 마약, 음란물 등 민생 범죄를 넘어서 악성코드 거래나 공격과 같은 보안 위협으로 더 활성화될 것으로 우려된다"며, "익명 네트워크의 악용을 막는 데는 국제 공조가 필요하며 이러한 활동에 우리도 최선을 다할 것"이라고 말했다.

또한, 광경주 인텔리전스 팀장은 "폼북에 대한 추가적인 분석 내용을 계속 공유하고, 앞으로도 이러한 공격 시도들이 파악되는 즉시 국내 기업과 기관을 보호하기 위해 지속적으로 노력하겠다"고 밝혔다.



건양대학교
사이버보안공학과
Department of Cyber Security Engineering

- ✓ 행정실 : 041-730-5579
- ✓ Reporter : dlalsdud4755@naver.com
kkco8@naver.com
- ✓ Café : <http://cafe.naver.com/kysecurity>
- ✓ Facebook : <https://www.facebook.com/kycybersec>