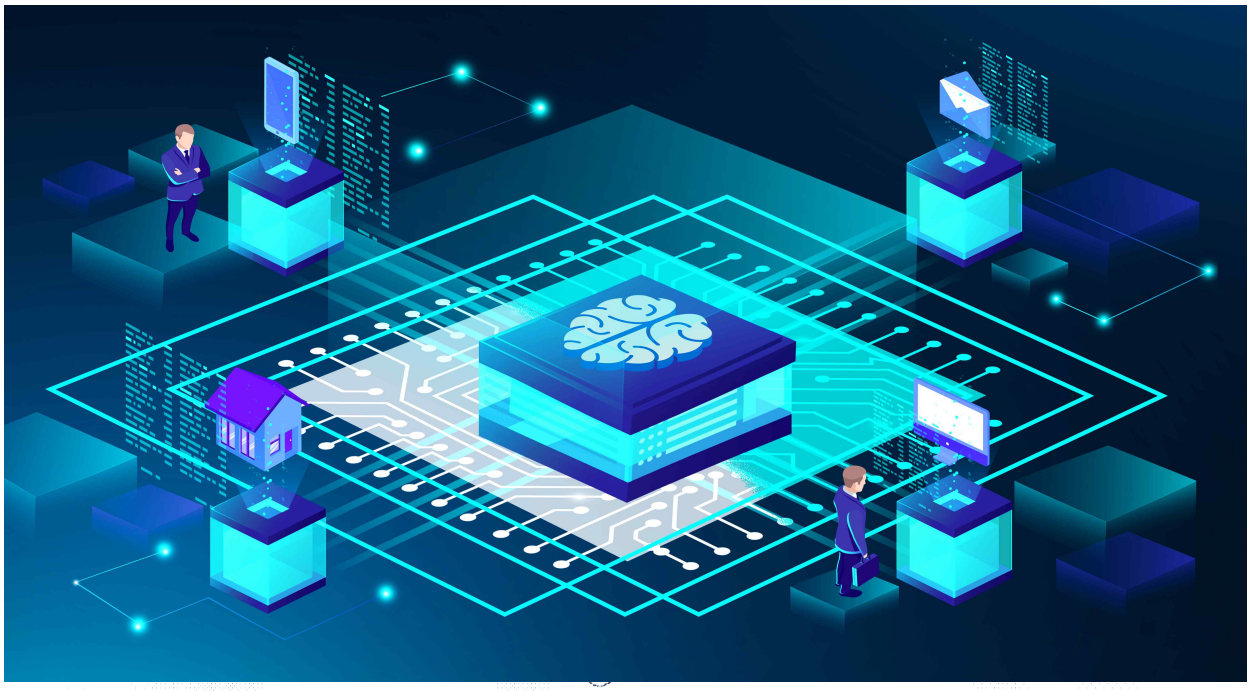
나도 될 수 있다!
화이트 해커

(2020. 06. 01 - 2020. 06. 30)



2020 사이버보안공학과 보안매거진 제 4호

사이버보안공학과
Cyber Security Engineering

건양대학교
KONYANG UNIVERSITY

CONTENTS

학과소식



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

[한마디]

우리 모두 살면서 몇 번의 실패를 겪는다. 이것이
바로 우리를 성공할 수 있도록 준비시킨다.
-랜디 K.멀홀랜드

사이버보안공학과 소식

건양대 사이버보안공학과-국민연금공단, 산학협력 업무협약 체결



굿모닝충청 백승협 기자] 건양대학교와 국민연금공단은 지난 9일 오후 건양대 논산캠퍼스에서 산학협력을 통한 기관간 개인정보보호 동반성장을 위한 업무협약을 체결했다.

이번 협약체결을 통해 건양대 사이버보안공학과는 국민연금공단 임직원들에게 개인정보보호 인식제고를 위한 교육프로그램을 지원하고 개인정보보호 관련 자문 및 지원을 하게 된다.

국민연금공단은 건양대 사이버보안공학과의 우수인력 양성을 위한 학생 현장실습을 지원하기로 했으며 향후 공단과 건양대 간 사업추진 및 협력관계를 이어나가기로 했다.

이날 건양대 논산창의융합캠퍼스 명곡정보관에서 진행된 협약식에는 건양대 이원묵 총장, PRIME창의융합대학 양계탁 학장, 차건상 정보통신원장, 사이버보안공학과 김동원□정승욱□이후기 교수와 국민연금공단 박정배 이사장(직무대행), 천득출 고객지원실장, 권혁일 개인정보보호부장 등이 참석했다.

출처 : 굿모닝충청(http://www.goodmorningcc.com)

사이버보안공학과 소식

여름학기 현장 실습

2020학년도 여름학기 현장실습 신청현황

No	대학	학부(과)	성명	확정 여부	신청학점	실습기간	실습기관
1	PRIME창의융합대학	사이버보안공학과	복O아	0	8학점	06/29~08/21	에프원시큐리티
2	PRIME창의융합대학	사이버보안공학과	손O혜	0	4학점	07/06~07/31	에스지에이비엘씨
3	PRIME창의융합대학	사이버보안공학과	이O혜	0	8학점	06/29~08/21	에프원시큐리티
4	PRIME창의융합대학	사이버보안공학과	이O아	0	4학점	06/29~07/24	T&D SOFT
5	PRIME창의융합대학	사이버보안공학과	박O용	0	4학점	07/13~08.09	국민연금공단
6	PRIME창의융합대학	사이버보안공학과	박O우	0	4학점	07/13~08.09	국민연금공단
7	PRIME창의융합대학	사이버보안공학과	지O식	0	4학점	07/20~08.14	T&D SOFT

▶ 4학년 학우분들이 여름학기에 에프원시큐리티, 에스지에이비엘씨,T&D SOFT, 최근 업무 협약을 맺은 국민연금공단에 현장실습을 나가게 되었습니다.

연무고 진로체험

▶ 일시 : 2020.8.4

· 사이버보안공학과 재학생들이 연무고등학교에서 진로체험이 예정되어 있습니다.

· 미래 신입생들의 흥미와 관심유발을 위해 실습 체험을 준비하고 있습니다.

사이버보안공학과 소식

동영상 공모전

사이버보안공학과에서 6월 30일까지 진행되었던 동영상 공모전이 연장되었습니다. 현재 서류 제출이 마감된 상태이며, 동영상 제출 후 심사가 이루어질 예정입니다. 재학생 여러분의 많은 관심 부탁드립니다!

- 7월 5일 : 1차 서류 제출 (제목 및 대략적 내용(동영상 아웃라인))
- 7월 19일 : 2차 동영상 제출 (완성본)
- 7월 24일 : 심사 결과 발표 (게재 가능/ 불가능 여부)
- 8월 30일 : youtube, facebook 등 좋아요 수 집계를 통한 결과 선정
- 9월 7일 : 최종 결과 발표

- 시상 장소 : 건양대학교
- 시상내역

대상 : 학장상 50만원 상당의 상품 및 50만원의 상금 (총 상금액 100만원)
최우수상 : 학과장상 30만원 상당의 상품 (총 상금액 50만원)
우수상 : 입시책임교수상 20만원 상당의 상품 (총 상금액 20만원)
※사이버보안공학과 학술제에서 공모전 시상식이 진행됩니다.

사이버보안 주요 이슈(ISSUE)

» "긴급생할비 지원사업이 집수되었습니다"긴급생활비 지원 사칭 스미싱 발견



안랩(대표 강석균)이 최근 정부/지자체의 긴급재난 지원금 지원 사업을 사칭해 사용자 개인정보 탈취를 노리는 스미싱 유포 사례를 발견해 사용자의 주의를 당부했다.

먼저 공격자는 "긴급생할비('긴급생활비'의 오타) 지원사업이 집수('접수'의 오타)되었습니다 다시한번 확인 부탁드립니다. http://******.***" 등 긴급 재난 지원금 관련 내용을 사칭해 문자메시지를 발송했다.

사용자가 무심코 스미싱 문자메시지 내 URL을 실행하면 휴대폰 본인인증을 위장한 피싱 사이트가 나타난다. 만약 사용자가 속아 해당 피싱 페이지에 개인정보 입력 후 '인증번호 요청' 버튼을 누르면 입력한 개인정보(이름, 성별, 생년월일, 휴대폰 번호 등)가 즉시 공격자에게 모두 전송된다. 해당 피싱 사이트는 실제 휴대폰 본인인증 화면과 매우 유사하고, 정상 인증 과정과 유사한 기능을 수행하기 때문에 사용자가 피싱 사이트임을 인지하기 어렵다. 탈취된 개인정보는 보이스피싱이나 금융정보 탈취 시도 등 공격자의 목적에 따라 다양하게 악용될 수 있어 더욱 주의해야 한다.

이와 같은 피해를 줄이기 위해서는 ◇출처가 불분명한 정보성 문자메시지 내 URL/첨부파일 실행금지 ◇인터넷 상에서 개인정보 입력시 접속한 웹페이지 이상 여부 꼼꼼히 확인 ◇스마트폰에 V3 모바일 시큐리티 등 모바일 백신설치 및 관련 기능 활성화 등 필수 보안 수칙을 실행해야 한다.

안랩 ASEC대응팀 박태환 팀장은 "최근 몇 개월 동안 재난 지원금을 사칭한 스미싱이 지속적으로 발견되고 있다"며 "사회적 이슈를 활용한 스미싱 공격은 앞으로도 발생할 것이므로 문자메시지 내 출처 불분명 URL은 가급적 접속을 자제하는 것이 좋다"고 말했다.

출처 : 데일리시큐(https://www.dailysecu.com)

사이버보안 주요 이슈 (ISSUE)

» 코그니잔트마저...대형 IT 기업도 피해갈 수 없었던 랜섬웨어 공격

IT 기업 코그니잔트(Cognizant)가 고객들에게 "메이즈(Maze) 랜섬웨어에 감염됐다"는 사실을 알리고 있다. 코그니잔트 측의 설명에 따르면 공격이 발생한 건 2020년 4월의 일이고, 이 사건으로 인해 개인 식별 정보와 금융 정보가 도난당했다고 한다. 지난 4월 20일, 누군가 네트워크에 불법적으로 침투하는 데 성공했으며, 이를 통해 내부 시스템의 데이터가 암호화 되는 일이 발생했다. 메이즈 랜섬웨어 때문에 벌어진 일이었다.

코그니잔트는 이 랜섬웨어 사건에 대한 내부 수사를 진행했고, 데이터가 도난당한 시점이 4월 9일에서 11일 사이인 것으로 보고 있다. "도난당한 개인정보 대부분은 코니잔트의 법인 신용카드와 관련이 있는 것들입니다. 현재 코그니잔트의 법인 카드와 관련된 모든 사람들과 파트너사들에게는 무료 신용 모니터링 서비스를 제공할 예정입니다." 코그니잔트가 고객에게 알린 내용 중 일부다.

뿐만 아니라 코그니잔트는 문제가 될 수 있는 신용카드 발급사들에게도 이 사실을 알렸고, 관련 계정들에 대한 모니터링을 요청했다. 특히 사기성 거래가 그러한 카드들로부터 발생하는지를 지켜보고 있다고 한다. "하지만 아직까지 별다른 특이 사항이나 사기성 거래 시도 행위가 발생하고 있지는 않습니다. 이는 카드사들과도 상호 확인한 바입니다."

하지만 외신들은 코그니잔트가 발송한 또 다른 사건 고지 서신(메일)을 입수해 도난당한 정보가 개인 식별 정보라고 보도하고 있다. 이름, 사회보장 번호, 납세자 식별 번호, 금융 계좌 정보, 운전자 면허 정보, 여권 정보 등이 여기에 포함되어 있는 것으로 알려져 있다.

한편 메이즈는 파일을 암호화 하기 전에 미리 빼돌리는 수법을 가장 먼저 선보인 랜섬웨어 운영자들로 알려져 있다. 이들은 웹사이트를 다크웹에 따로 개설해 피해자들을 관리한다. 관리란, 돈을 내지 않는 피해자들의 정보를 이 사이트에 그대로 업로드 하는 것을 말한다. 이런 이중 협박 전략은 다른 랜섬웨어 운영자들 사이에서도 유행하고 있다.

[국제부 문가용 기자(globoan@boannews.com)]

<저작권자: 보안뉴스(www.boannews.com) 무단전재-재배포금지>

사이버보안 주요 이슈(ISSUE)

» 북한 해킹그룹으로 추정되는 조직, 청와대 보안 이메일 사칭 APT 공격

북한발 사이버공격으로 추정되는 한국내 타깃공격이 지속적으로 발행하고 있다. 6월 19일 새벽, 대한민국 청와대 로고가 찍힌 보안 이메일 파일이 전파되기 시작했다. 분석결과, 해당 악성 메일은 청와대 보안 메일이 아닌 북한 정부 후원으로 추정되는 해킹그룹 '김수키(Kimsuky)' 조직의 소행인 것으로 분석됐다. APT(지능형지속위협) 공격용 악성파일 변종이 복수로 발견된 것이다. 각별한 주의가 요구되는 시점이다.

ESRC는 해당 악성파일을 긴급 분석한 결과, 특정 정부와 연계된 것으로 알려진 이른바 '김수키(Kimsuky)' 조직의 '블루 에스티메이트' 위협 캠페인의 연장선으로 확인했고, 위협 모니터링 과정 중에 윈도우 스크립트 파일 유형으로 제작된 'bmail-security-check.wsf' 악성 스크립트 코드를 발견했다.
스크립트 코드 내부에는 Base64 코드로 인코딩된 데이터가 포함되어 있고, 디코딩 과정을 거치면 'bmail-security-check.exe', 'AutoUpdate.dll' 파일 등이 생성된다.

특히, 'bmail-security-check.exe' 악성코드는 대한민국 청와대 로고 이미지를 아이콘으로 사용하고 있어 충격을 주고 있다.
악성파일은 UPX로 실행압축되어 있으며, 'bmail-security-check.exe' 파일이 실행되면 악성파일 실행시 보여지는 메시지 창 화면이 보인다.
'bmail-security-check.exe' 파일에는 '보안메일 현시에 안전합니다.'라는 메시지 박스가 나타나는 알림 기능을 가지고 있는데, 여기에 '현시'라는 표현은 북한식 언어 표기법이다.

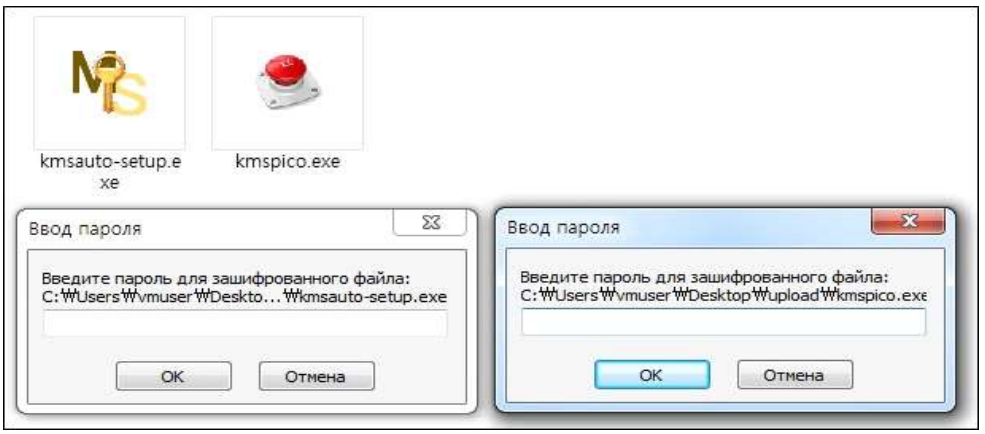
C2 주소로 접속시 청와대 주소로 이동되는 화면 분석 시점 당시 'security-confirm.bmail-org[.]com/pages' 주소로 접속하면, 청와대 홈페이지로 변경되는 것이 확인되었다.

ESRC 측은 "특정 정부의 후원을 받고, 연계된 것으로 확신하는 이른바 '김수키(Kimsuky)' 조직의 APT 활동이 꾸준히 이어지고 있다. 특히, 이들 조직이 최근까지 가장 왕성하게 사용하는 '스모크 스크린(Smoke Screen)'과 '블루 에스티메이트(Blue Estimate)' 캠페인은 대표적인 김수키 조직의 APT 공격 활동"이라며 "최근 김수키 조직이 마치 라자루스(Lazarus)처럼 위장한 기법을 도입하는 등 갈수록 고도화되고 있다. 각별한 주의와 이와 관련 사이버보안 인텔리전스 정보를 활용하는 것도 중요하다"고 강조했다.

출처 : 데일리시큐(https://www.dailysecu.com)

사이버보안 주요 이슈 (ISSUE)

» 불법 '정품인증 툴'로 위장한 악성코드 주의하세요



최근 불법으로 소프트웨어를 이용하려는 사용자를 노려 불법 정품인증 툴로 위장한 악성코드 유포 사례가 발견돼 사용자 주의가 요구된다.

공격자는 P2P사이트, 불법 다운로드 사이트 등 다양한 경로로 MS제품에 대한 불법 정품인증 툴인 'KMSAuto', 'KMSPico' 등(이하 '불법 정품인증 툴')으로 위장한 악성 실행파일을 유포했다. 사용자가 해당 악성 실행파일을 실행하면 비밀번호 입력창이 나타난다(보충자료 참고). 여기에 공격자가 제공한 비밀번호를 입력하고 OK 버튼을 누르면 불법 정품인증 툴과 '비다르(Vidar)' 악성코드가 동시에 설치된다.

비다르(Vidar) 악성코드는 감염 PC내 주요 정보를 외부로 유출한다. 유출 대상 정보는 FTP 클라이언트 내 저장된 사용자 계정정보, 웹 브라우저 내 계정정보 및 자동채우기(Autofill)값, 인터넷 쿠키, 암호화폐 지갑주소 등이다. 정보유출 행위 이후에도 다른 악성코드를 내려받아 추가 악성행위를 수행할 수 있다.

이번 악성코드는 실제 불법 정품인증 툴과 동일한 아이콘과 파일명을 사용하고, 툴 설치까지 진행되기 때문에 사용자는 악성코드 감염을 의심하기 어렵다.

안랩 분석팀 이재진 연구원은 "공격자에게 탈취된 정보는 추후 금전탈취나 계정도용 등 다양한 범죄에 악용될 수 있다"며 "피해를 예방하기 위해선 정품 소프트웨어 사용을 생활화하고 의심스러운 웹사이트나 P2P이용은 자제하는 것이 좋다"고 말했다.

출처 : 데일리시큐(https://www.dailysecu.com)