[2021년 2분기]

(요약서) 국내·외 의료분야 타겟형 사이버 공격그룹 분석 및 대응방안

진료정보침해대응센터
Korea Healthcare Computer Emergency Response Team

보건복지부
SSiS 한국사회보장정보원

◈ 진료정보침해대응센터(KHCERT)에서 2021년 2분기 심층 분석 보고서로 "**국내·외 의료분야를 주요 공격 대상으로 해킹을 수행하는 공격그룹**"에 대한 분석한 결과와 대응방법을 제공합니다.

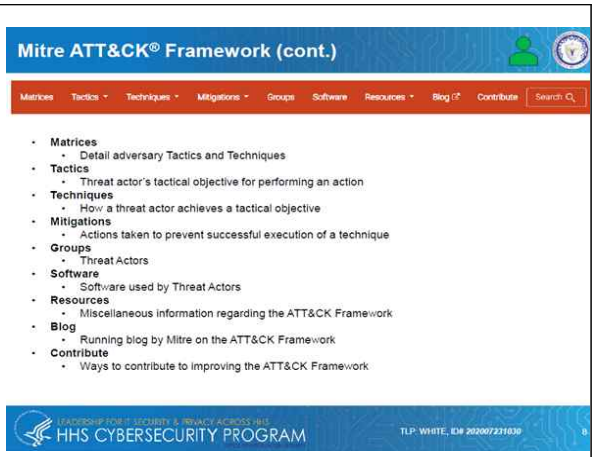
I (현황) 의료분야 타겟형 공격이 확산되는 상황으로 해당 공격을 수행하는 공격그룹에 대한 맞춤형 대응이 필요한 상황입니다.

▶ 미 보건복지부(HHS), 의료분야 타겟형 공격그룹에 대한 분석 보고서 발표 및 랜섬웨어, 웹서버 정보 탈취 등 국내 의료분야 해킹 공격 확산

⊙ 2020년 7월 23일, HHS 산하 HC3(의료분야 사이버 보안 협력 센터)에서 **의료분야 대상 해킹 공격을 수행하는 공격그룹에 대한 분석**[1] **결과 발표**

⊙ 글로벌 보안업체 카스퍼스키랩에서도 과거 공격 기법, 대상 등을 기반으로 **앞으로 발생할 수 있는 공격과 대상을 예측**할 수 있다고 밝힘

1) HC3는 MITRE ATT&CK을 기반으로 의료분야 공격그룹 분석 결과를 제공
* MITRE ATT&CK는 사이버 공격에서 발견된 해킹 전술과 기법에 대한 전 세계적인 지식 기반 모델



< HPH-Sector Cyber Threat Actor Modeling with Mitre ATT&CK®(출처: HC3)>

< 북한 해킹 그룹 공격에 대한 특징 분석(출처: 바이라인 네트워크, 카스퍼스키랩) >

Ⅱ (주요위협) 의료분야 타겟형 공격으로 코로나19 검사 및 일반 진료 서비스가 중단되었고, 수사기관에서도 관련 위협을 경고하고 있습니다.

▶ 해외 의료기관에서 의료기관 타겟형 공격그룹에 의한 **의료서비스 공격으로 의료기록 접근 및 의료서비스 중단 발생**, FBI는 관련 공격에 대한 긴급권고 발표

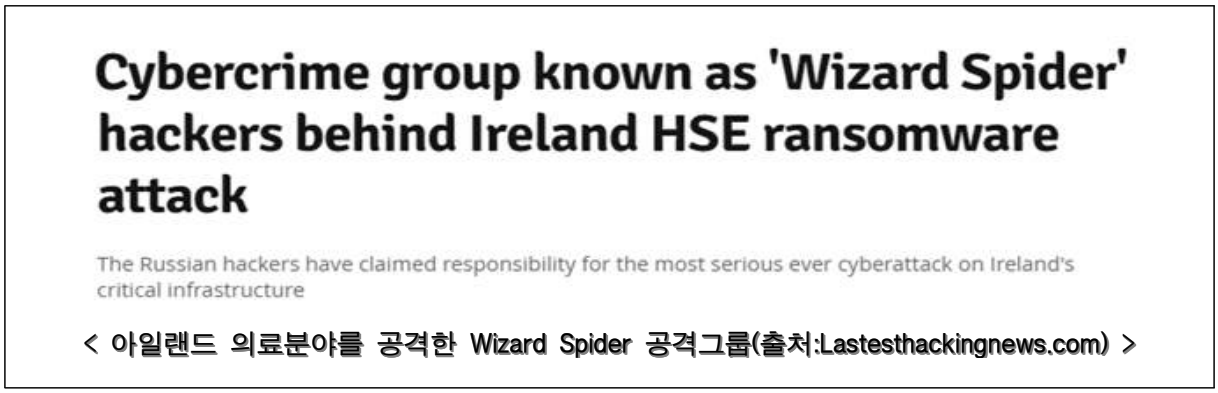
⊙ 2021년 5월 14일 로이터 통신에 따르면 **아일랜드 의료 서비스(HSE)가 Wizard Spider[2] 라는 공격그룹에 의해 공격**당해 환자의 의료기록 접근이 불가한 상태가 지속되었다고 발표

⊙ 2021년 5월 20일 **FBI는 Conti 랜섬웨어[3] 공격이 의료분야와 국가안전망을 공격**하고 있으며 이와 유사한 공격이 발생할 경우 FBI로 신고해 달라고 긴급 보안권고를 발표

⊙ 2021년 2월 의료분야 타겟형 공격그룹이 주로 사용하는 공격기법이 **국내 OO병원, 의료분야 관련 단체 등에서 발견되어 랜섬웨어 감염으로 인한 데이터 암호화** 등 피해 발생

2) Wizard Spider 공격그룹은 공격 대상 네트워크에 무단접근 하는데 악성 이메일 링크, 첨부파일, 원격 데스크탑(RDP) 자격증명을 악용함

3) Conti 랜섬웨어는 공격대상의 정보를 탈취하고 파일을 암호화하여 금전을 요구, 금전을 지불하지 않을 경우 탈취한 데이터를 판매하거나 인터넷에 공개해 버림



Cybercrime group known as 'Wizard Spider' hackers behind Ireland HSE ransomware attack

The Russian hackers have claimed responsibility for the most serious ever cyberattack on Ireland's critical infrastructure

< 아일랜드 의료분야를 공격한 Wizard Spider 공격그룹(출처:Lastesthackingnews.com) >

TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

20 May 2021

Alert Number
CP-000147-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately.**
Email:
cywatch@fbi.gov

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP:WHITE**

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Summary

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a

< Conti 랜섬웨어 관련 FBI 긴급 보안 권고(출처:aha.org) >

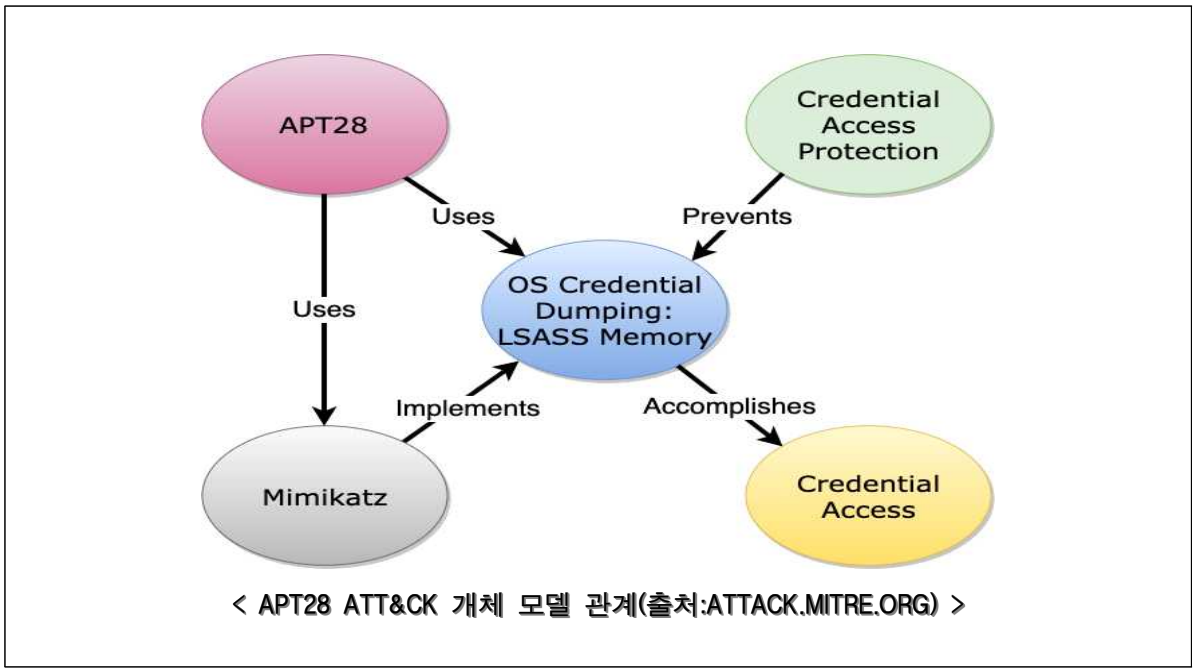
Ⅲ (분석내용) 과거에 발생한 공격 행위의 유사성을 기반으로 공격 수행 주체를 판별, 유사한 공격에 참고 및 예측자료 활용할 수 있습니다.

▶ MITRE ATT&CK에서 **과거 공격 이력을 기반**으로 **의료분야 타겟형 공격그룹을 확인**, 해당 공격 그룹의 주요 공격기법을 분석하여 **공통적인 공격기법을 추출**

⊙ **APT41, FIN4, Wizard Spider 등** 과거 의료분야를 대상으로 사이버 공격을 수행한 공격그룹을 MITRE ATT&CK을 통해 확인

⊙ **의료분야 타겟형 공격그룹**이 수행한 공격 전술 및 기법을 확인하여 **공통적으로 사용한 공격 기법**을 추출한 결과 **원격 서비스 악용, OS 자격 증명 덤핑**[4], **피싱 공격** 등이 확인

4) OS 자격 증명 덤핑(OS Credential Dumping)은 OS 계정 로그인을 위한 자격 증명 데이터를 탈취하는 공격



< APT28 ATT&CK 개체 모델 관계(출처:ATTACK.MITRE.ORG) >

< MITRE ATT&CK에서 공개한 의료분야 공격그룹 일부 발췌 >

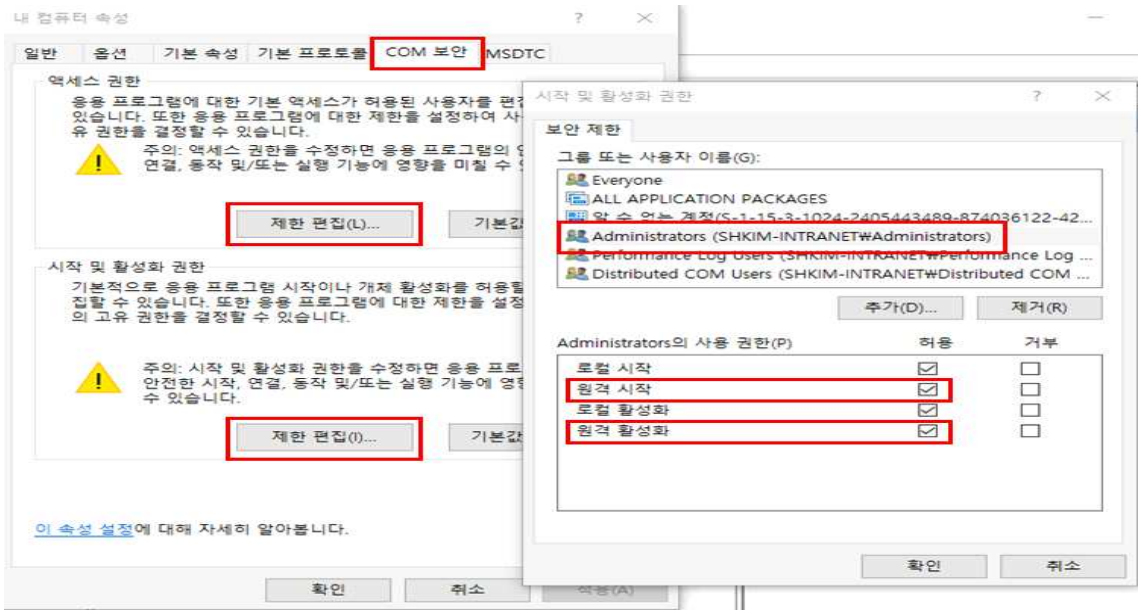
그룹명	설명
APT41	중국의 지원을 받는 스파이 그룹, 금전 목적의 공격 수행, 의료, 통신, 기술, 비디오 게임 등의 분야와 한국을 포함한 14개 국가를 목표한 것으로 관찰됨
FIN4	의료 및 제약 회사와 관련 기밀 정보 및 금전 탈취 목적의 공격 그룹, 이메일 시스템 등에 접근 권한이 있는 자격 증명을 탈취하여 공격에 악용
Tropic Trooper	대만, 필리핀, 홍콩 대상의 공격을 주도한 공격 그룹으로 정부, 의료, 교통, 하이테크 산업을 주요 대상으로 2011년부터 활동함.
Wizard Spider	대기업부터 병원까지 다양한 조직을 대상으로 랜섬웨어 공격을 하여 금전을 요구하는 공격 그룹

Ⅳ (조치권고) 의료분야 타겟형 공격그룹에서 공통적으로 사용하는 공격을 방어하기 위해 주요 공격기법에 대한 선제적 보안대책 적용이 필요 합니다.

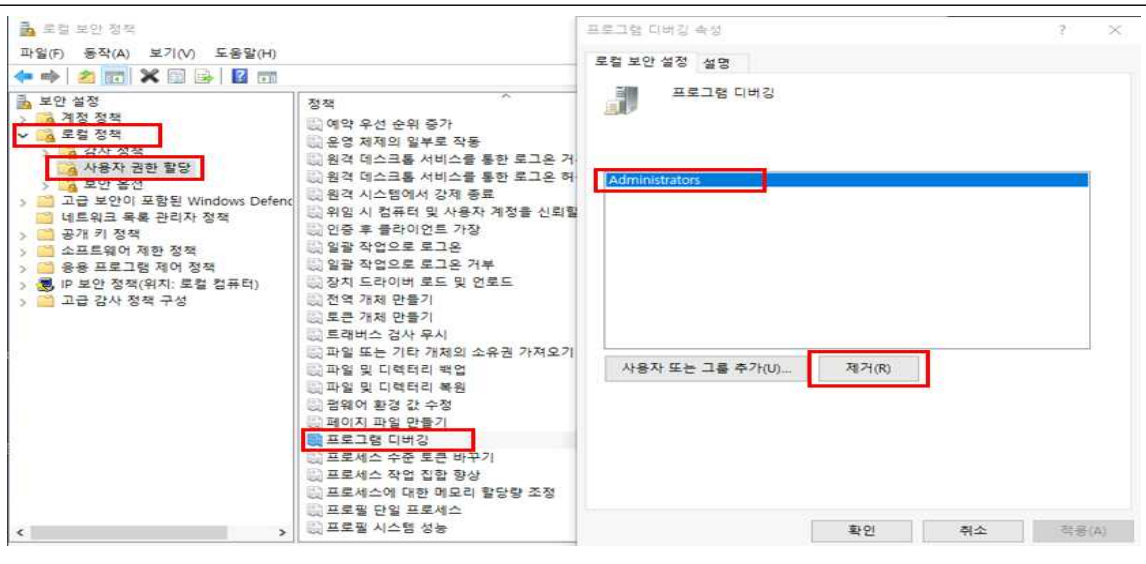
▶ 사용자 계정 관리를 통한 공격 악용 도구의 **원격접속시 실행권한 차단**, **프로그램 디버깅 권한 제어**를 통한 OS 자격증명 덤핑 공격 방지 등 적용

⊙ WMI는 윈도우 관리 프로토콜로 공격에 자주 악용되는 도구로 관리자 권한에서 원격 시작 및 원격 활성화를 해제하여 **공격자의 원격접속시 WMI 실행권한 차단**

⊙ 로컬 보안 정책(secpol.msc)에서 대상이 아닌 사용자의 프로그램 디버깅 권한을 제거하여 **OS 자격증명 덤핑 공격 방지**



< Administrators의 원격 액세스, 시작 및 활성화 권한 해제 >



< 로컬 보안 정책에서 디버그 권한 제거 >

☞ 세부내용은 "**국내·외 의료분야 타겟형 사이버 공격그룹 분석 및 대응방안**" 보고서 원문 참고

※ 본 보고서를 인용할 경우, 반드시 한국사회보장정보원 KHCERT(진료정보침해대응센터)를 명시하여 주시기 바랍니다.

진료정보침해대응센터
Korea Healthcare Computer Emergency Response Team

보건복지부

SSiS 한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE