[2021년 1분기]

(요약서) 의료기관 대상 고도화된 원격접속 공격 대응방안

- 원격데스크톱(RDP) 터널링 공격 분석 및 대응방법 -

한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE

진료정보침해대응센터
Korea Health Computer Emergency Response Team

◈ 진료정보침해대응센터(KHCERT)에서 2021년 1분기 심층 분석 보고서로 최근 발생 빈도가 증가하고, 향후에도 발생 가능성이 높은 "**고도화된 원격접속 공격(RDP 터널링)**"에 대해 분석한 결과와 대응방법을 제공합니다.

I (현황) 고위험 공격으로 분류되는 원격접속 공격이 COVID-19 등의 영향으로 급증하여, 의료분야에서도 관련 위협에 대비가 필요합니다.

▶ 원격접속 공격은 의료분야에서도 고위험 공격이며, 최근 공격시도가 급격히 증가

⊙ ECRI[1]는 **원격접속 시스템 해킹이 환자의 안전을 위협하는 1번째 위험**이라고 발표

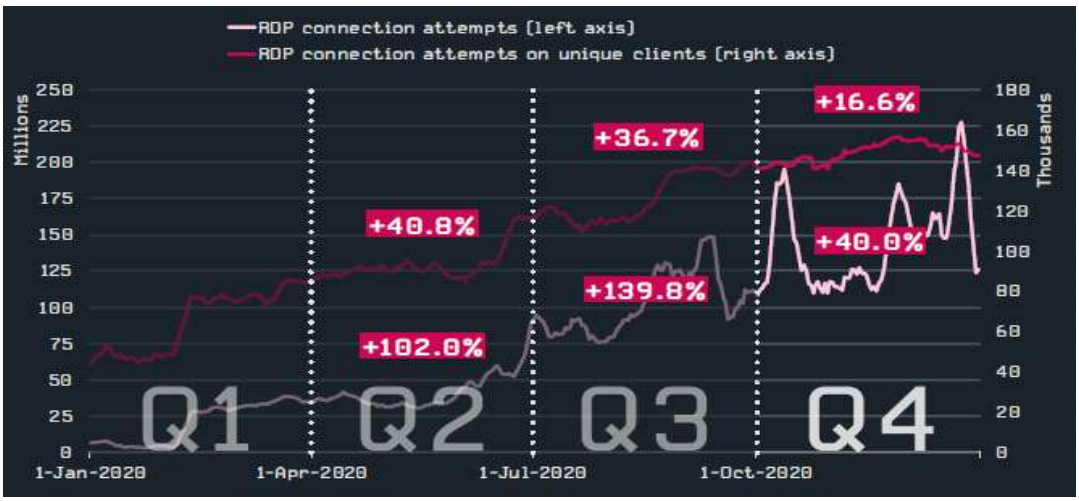
⊙ ESET社는 **`20년 4분기 RDP[2] 접속 시도**가 1분기 대비 **768% 증가**했다고 발표

1) ECRI(Emergency Care Research Institute): 전 세계 의료 환경에서 치료의 안전, 품질 및 비용 효율성 등을 개선하는 활동을 수행하는 비영리 조직
2) RDP(Remote Desktop Protocol): MS社의 Windows OS의 구성요소로 네트워크를 통해 원격에서 컴퓨터에 접속하여 제어가 가능한 통신 규약

Remote Access System Hacking Is No. 1 Patient Safety Risk

Hackers attacking healthcare through remote access systems and disrupting operations is the number one patient safety risk.

< 원격접속 해킹은 환자의 안전을 위협하는 1번째 위험 (출처:ECRI) >



< '20년 1분기~4분기 RDP 접속 시도 현황 (출처:ESET社) >

Ⅱ (주요위협) RDP 공격의 확산에 따라 고도화된 RDP 터널링 공격 발생이 우려되는 상황으로, 취약한 RDP 사용에 대한 보안조치가 요구됩니다.

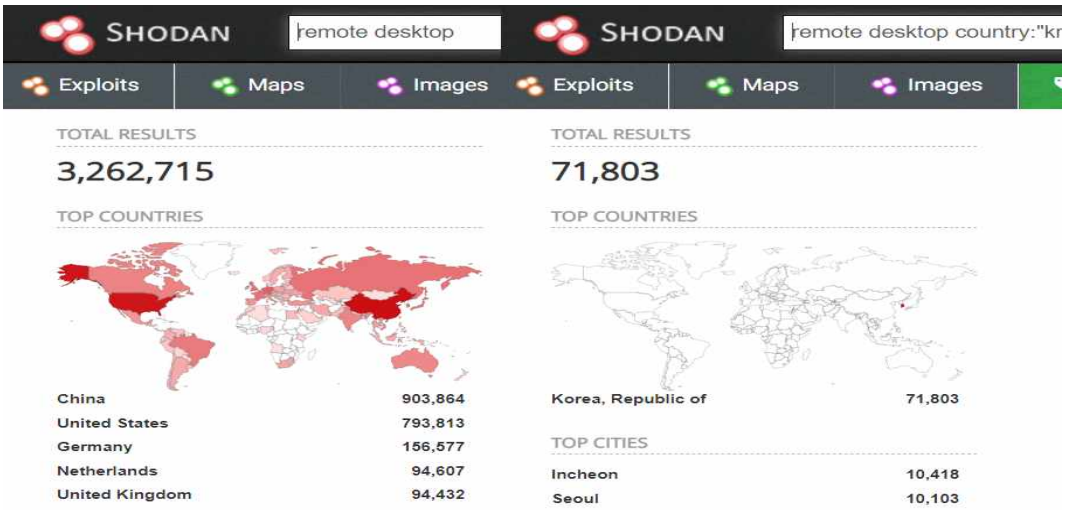
▶ 국내·외 의료분야 해킹사고에서, RDP를 악용한 초기침투 및 내부전파 확인

⊙ 의료분야를 대상으로 고도화된 해킹 공격을 수행하는 FIN8[3] 공격그룹이 **RDP 터널링 공격을 악용하는 것으로 확인**

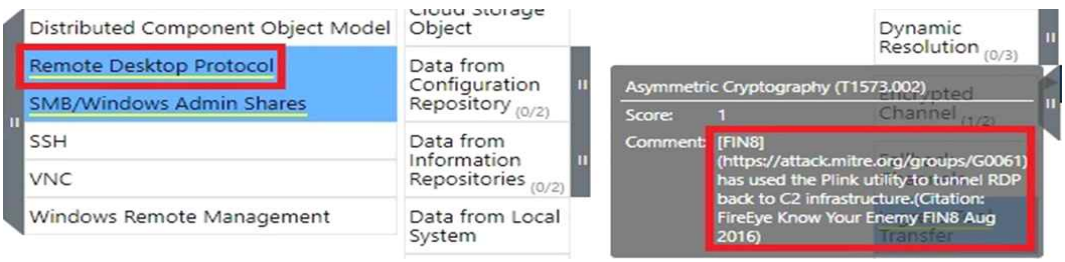
⊙ RDP 공격이 가능한 시스템을 SHODAN[4]에서 검색한 결과 **전세계 약 3백만개, 국내 약 7만개 이상의 취약한 시스템 발견**

⊙ KHCERT(진료정보침해대응센터)는 국내 의료기관에서 **RDP를 악용한 공격** 및 이로 인한 **피해가 지속적으로 발생**하고 있다고 밝힘

3) FIN8 공격그룹: 금전적인 목적으로 맞춤형 공격을 실행하며, 의료, 숙박, 소매, 엔터테인먼트 등을 주로 공격
4) SHODAN: 시스템에 개방된 포트나 취약점 등을 검색하는데 주로 사용하는 검색엔진



< RDP 취약 시스템 SHODAN 검색 결과 >



< FIN8에 대한 MITRE 분석결과(RDP 터널링 악용) >

Ⅲ (공격분석) 관리가 허술한 [내부→외부] 연결을 악용한 RDP 터널링 공격을 통해 시스템을 탈취하고 추가 공격으로 피해를 확산시킵니다.

▶ 공격 대상 네트워크에 거점을 확보하고 **공격자의 C&C 서버로 역방향 SSH 연결**

⊙ 내부 시스템으로 접근하는 인바운드 대비 **아웃바운드 트래픽에 대한 보안관리 허점을 악용**하여 역방향 SSH 연결 설정

⊙ 공격자는 피해 시스템에 연결된(역방향 SSH) C&C 서버[5]를 통해 **터널을 생성하여 RDP 접속 및 공격 수행**

5) C&C(Command & Control) 서버: 악성코드 등에 감염된 좀비PC가 공격자가 원하는 공격을 수행하도록 원격지에서 명령을 내리거나 제어하는 서버

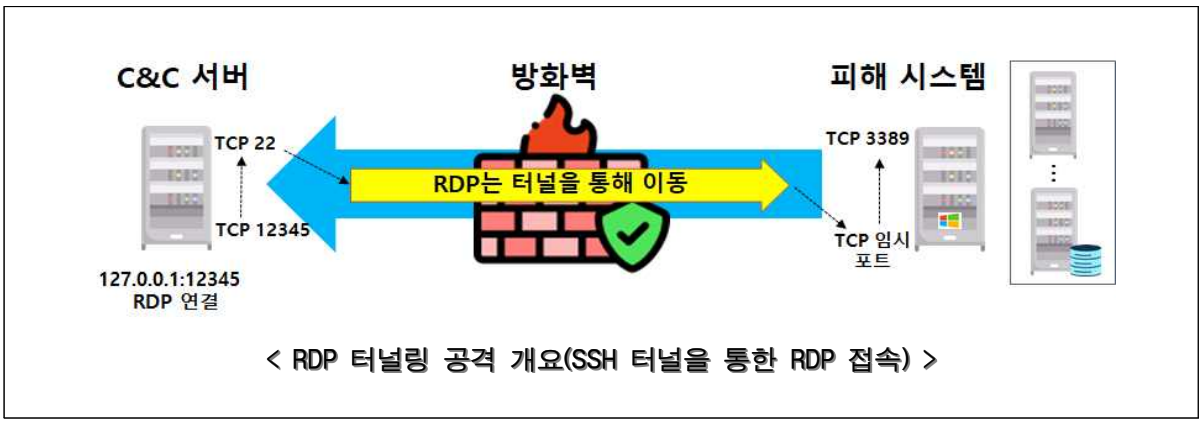
< RDP 터널링 공격 개요(역방향 SSH(TCP22) 연결) >

▶ 공격자는 RDP 터널링을 통해 **보안장비의 탐지를 우회**하여 내부 **시스템 제어권 탈취**

⊙ 내부 네트워크에서 다른 시스템으로 **측면 이동(Lateral Movement)[6]을 통한 피해 확산**

⊙ 내부 시스템 간 허용된 RDP를 통해 **무차별 대입공격, 저장된 자격증명 탈취** 등 추가 공격 시도

6) 측면 이동(Lateral Movement): 내부 네트워크 침투에 성공한 공격자는 공격 목표인 시스템으로 이동하려고 시도하는데 이 과정을 측면 이동(Lateral Movement)라고 한다.



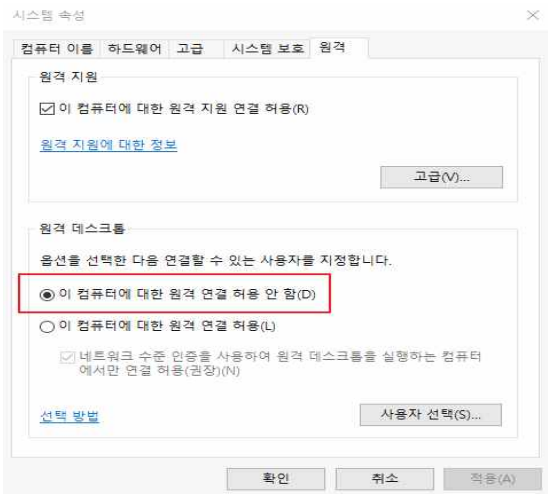
< RDP 터널링 공격 개요(SSH 터널을 통한 RDP 접속) >

Ⅳ (조치권고) RDP 사용 억제 및 공격징후 탐지 등 보안대책을 적용하여 위험성이 큰 RDP 터널링 공격에 선제적으로 대응해야 합니다.

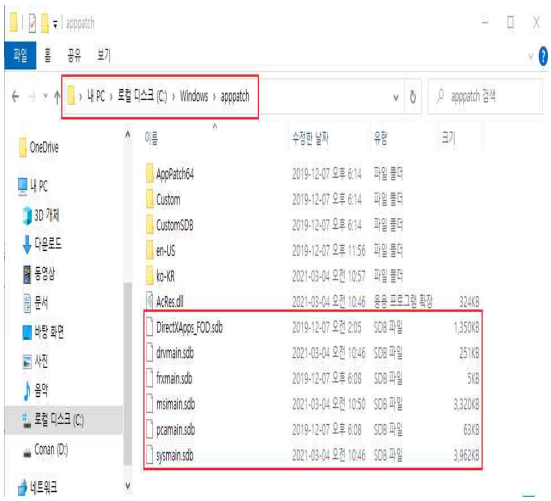
▶ 호스트 기반 보안 대책·탐지 기법을 적용하여 **RDP 접속 원천 차단**

⊙ 윈도우 OS의 **원격 데스크톱 서비스(RDP) 기능 비활성화, 윈도우 방화벽에서 3389 (RDP) 포트 차단, 사용자 계정의 원격 로그인 권한 제거**

⊙ Plink 등 RDP 터널링 악용 프로그램의 **설치·실행 내역 확인 및 윈도우즈 이벤트 로그, 레지스트리 키 검토를 통한 공격 탐지**



< 윈도우 원격 데스크톱 차단 설정 >



< 실행 내역 검토를 위한 ShimCaChe 관련 파일 >

▶ 네트워크 기반 예방·탐지 방법을 적용하여 **RDP 터널링 공격징후 조기 발견·대응**

⊙ 내부 지정 서버·도메인 계정만 RDP 접속을 허용하여 **취약 영역 및 관리 포인트 최소화**

⊙ **포트포워딩 관련 방화벽 규칙 검토, 트래픽 상세 모니터링(보안관제)** 등을 수행하여 RDP 터널링 관련 위협에 선제적 대응

☞ 세부내용은 **"원격데스크톱(RDP) 터널링 공격 분석 및 대응방법"** 보고서 원문 참고

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

진료정보침해대응센터
Korea Health Computer Emergency Response Team

SSiS 한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE