

지속성 : 공격자가 다시 시작, 자격 증명 변경 및 액세스를 차단할 수 있는 기타 중단을 통해 시스템에 대한 액세스를 유지하기 위해 사용하는 기술로 구성

### \* 기법

Account Manipulation

BITS Jobs

Boot or Logon Autostart Execution

Boot or Logon Initialization Scripts

Browser Extensions

Compromise Client Software Binary

Create Account

Create or Modify System Process

Event Triggered Execution

External Remote Services

Hijack Execution Flow

Implant Internal Image

Modify Authentication Process

Office Application Startup

Pre-OS Boot

Scheduled Task/Job

Server Software Component

Traffic Signaling

Valid Accounts

**계정 조작** 자격 증명 또는 권한 그룹 수정과 같이 손상된 계정에 대한 공격자의 액세스를 유지하는 모든 작업으로 구성됨

> 계정 생성 및 조작을 위해 공격자는 이미 시스템 또는 도메인에 대한 권한이 있어야 함

#### 1) Additional Cloud Credentials (추가 클라우드 자격 증명)

: 클라우드 계정에 공격자가 제어하는 자격 증명을 추가하여 환경 내의 피해자 계정 및 인스턴스에 대한 지속적인 액세스 유지 가능

#### 2) Exchange Email Delegate Permissions (이메일 대리인 권한 교환)

: 공격자는 공격자가 제어하는 이메일 계정에 대한 지속적인 액세스를 유지하기 위해 ReadPermission 또는 FullAccess와 같은 추가 권한 수준 부여 가능

#### 3) Add Office 365 Global Administrator Role (Office 365 전역 관리자 역할 추가)

: 충분한 권한이 있으면 손상된 계정은 전역 관리자 역할을 통해 데이터 및 설정(다른 관리자의 비밀번호 재설정 기능 포함) 액세스 가능

#### 4) SSH Authorized Keys (SSH 인증 키)

: 피해자 호스트에서 지속성을 유지하기 위해 SSH "authorized\_keys" 파일을 수정

Persistence

## 2. BITS Jobs

**BITS Jobs** BITS 작업을 악용해서 악성 페이로드를 실행하거나 정리 가능

\*BITS(Background Intelligent Transfer Service) : 파일 전송 메커니즘, 다른 프로그램을 방해하지 않고 백그라운드에서 작동하는 프로그램에서 사용됨

Persistence

## 3. Browser Extensions

**브라우저 확장** 인터넷 브라우저 확장을 악용하여 피해자 시스템에 지속적으로 액세스 가능

일반적으로 브라우저가 액세스할 수 있는 모든 것에 대한 액세스 및 권한이 있음

Persistence

## 4. Compromise Client Software Binary

**클라이언트 소프트웨어 바이너리 손상** 클라이언트 소프트웨어를 통해 서버에서 제공하는 서비스에 액세스 가능

[클라이언트 소프트웨어 유형] SSH Client, FTP Client, E-mail Client 및 Web-browser

## Persistence

### 5. External Remote Services

**외부 원격 서비스** VPN, Citrix 등의 원격 서비스를 통해 외부 위치에서 내부 엔터프라이즈 네트워크 리소스에 연결 가능  
Windows 원격 관리와 같은 서비스도 외부에서 사용 가능

## Persistence

### 6. Implant Internal Image

**임플란트 내부 이미지** Amazon Web Services(AWS) Amazon 머신 이미지(AMI), Google Cloud Platform(GCP) 이미지, Azure 이미지는 물론 Docker와 같은 인기 있는 컨테이너 런타임을 이식하거나 백도어링 가능  
공격자가 피해자 환경 내의 레지스트리에 이미지를 넣는 데 중점

**부팅 또는 로그인 자동 시작 실행** 시스템 부팅 또는 로그인 중에 프로그램을 자동으로 실행하여 지속성을 유지하거나 손상된 시스템에서 더 높은 수준의 권한을 얻도록 시스템 설정을 구성

### 1) Registry Run Keys / Startup Folder (레지스트리 실행 키 / 시작 폴더)

레지스트리 또는 시작 폴더의 "실행 키"에 항목을 추가하면 사용자가 로그인할 때 참조된 프로그램이 실행

### 2) Authentication Package (인증 패키지)

시스템 부팅 시 DLL을 실행하기 위해 인증 패키지 사용 가능

### 3) Time Providers (시간 제공자)

시스템 부팅 시 DLL을 실행하기 위해 시간 공급자 사용 가능

### 4) Winlogon Helper DLL (Winlogon 도우미 DLL)

### 5) Security Support Provider (보안 지원 제공자)

### 6) Kernel Modules and Extensions (커널 모듈 및 확장)

### 7) Re-opened Applications (다시 열린 응용 프로그램)

### 8) LSASS Driver (LSASS 드라이버)

### 9) Shortcut Modification (바로가기 수정)

### 10) Port Monitors (포트 모니터)

### 11) Plist Modification (Plist 수정)

### 12) Print Processors (인쇄 프로세서)

### 13) XDG Autostart Entries (XDG 자동 시작 항목)

### 14) Active Setup (활성 설정)

부팅 또는 로그인 자동 시작 실행 시스템 부팅 또는 로그인 중에 프로그램을 자동으로 실행하여 지속성을 유지하거나 손상된 시스템에서 더 높은 수준의 권한을 얻도록 시스템 설정을 구성

### 1) Registry Run Keys / Startup Folder (레지스트리 실행 키 / 시작 폴더)

레지스트리 또는 시작 폴더의 "실행 키"에 항목을 추가하면 사용자가 로그인할 때 참조된 프로그램이 실행  
악성코드를 시작 프로그램 경로에 생성할 경우 재부팅 시마다 악성코드가 자동으로 실행

< 시작 프로그램으로 등록한 악성코드 확인 명령어 >

```
cmd.exe /c dir "C:\Users\[유저명]\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\javaw.exe"
```

< 대응 전략 >

시작 프로그램 폴더 경로 및 시작 프로그램으로 등록된 프로그램 모니터링  
C:\Users\[유저명]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

## Persistence

### 8. Boot or Logon Initialization Scripts

**부팅 또는 로그인 초기화 스크립트** 다른 프로그램을 실행하거나 내부 로깅 서버에 정보를 보낼 수 있는 관리 기능을 수행하는 데 사용하는 초기화 스크립트를 사용

1) Logon Script(Windows) (로그온 스크립트(Windows))

2) Logon Script(Mac) (로그온 스크립트(Mac))

3) Network Logon Script (네트워크 로그인 스크립트)

4) RC Scripts (RC 스크립트)

5) Startup Items (시작 항목)

## Persistence

### 9. Create Account

**계정 만들기** 피해자 시스템에 대한 액세스를 유지하기 위해 계정을 만들

1) Local Account (로컬 계정)

3) Cloud Account (클라우드 계정)

2) Domain Account (도메인 계정)

**시스템 프로세스 생성 또는 수정** 지속성의 일부로 악성 페이로드를 반복적으로 실행하기 위해  
시스템 수준 프로세스(서비스)를 생성하거나 수정 가능

1) Launch Agent (에이전트 시작)

2) Systemd Service (시스템화된 서비스)

3) Windows Service (윈도우 서비스)

4) Launch Daemon (데몬 실행)

- New Service : 서비스를 이용하여 악성코드를 등록할 경우 재부팅 시마다 악성코드 자동 실행



**이벤트 트리거 실행** 특정 이벤트를 기반으로 실행을 트리거하는 시스템 메커니즘을 사용하여 지속성을 설정하거나 권한 상승 가능

1) Change Default File Association (기본 파일 연결 변경)

2) Screensaver (화면 보호기)

3) Windows Management Instrumentation Event Subscription (WMI 이벤트 구독)

4) Unix Shell Configuration Modification (Unix 셸 구성 수정)

5) Trap (덫)

6) LC\_LOAD\_DYLIB Addition (추가)

7) Netsh 도우미 DLL

8) Accessibility Features (접근성 기능)

9) AppCert DLL

10) AppInit DLL

11) Application Shimming (응용 프로그램 시밍)

12) Image File Execution Options Injection

(이미지 파일 실행 옵션 주입)

13) PowerShell Profile

14) Emond (에몬드)

15) Component Object Model Hijacking

(컴포넌트 객체 모델 하이재킹)

하이재킹 실행 흐름 운영 체제가 프로그램을 실행하는 방식을 가로채서 자체 악성 페이로드를 실행 가능

- 1) DLL Search Order Hijacking (DLL 검색 순서 하이재킹)
- 2) DLL Side-Loading (DLL 사이드 로딩)
- 3) Dylib Hijacking (딜립 하이재킹)
- 4) Executable Installer File Permissions Weakness (실행 가능한 설치 프로그램 파일 권한 약점)
- 5) Dynamic Linker Hijacking (동적 링커 하이재킹)
- 6) Path Interception by PATH Environment Variable (PATH 환경 변수에 의한 경로 가로채기)
- 7) Path Interception by Search Order Hijacking (검색 순서 하이재킹에 의한 경로 가로채기)
- 8) Path Interception by Unquoted Path (인용되지 않은 경로에 의한 경로 가로채기)
- 9) Services File Permissions Weakness (서비스 파일 권한 약점)
- 10) Services Registry Permissions Weakness (서비스 레지스트리 권한 약점)
- 11) COR\_PROFILER

## Persistence

## 13. Modify Authentication Process

**인증 프로세스 수정** 인증 메커니즘과 프로세스를 수정하여 사용자 자격 증명에 액세스하거나 계정에 대한 부당한 액세스를 허용 가능

- 1) Domain Controller Authentication (도메인 컨트롤러 인증)
- 2) Password Filter DLL (비밀번호 필터 DLL)
- 3) Pluggable Authentication Modules (플러그형 인증 모듈)
- 4) Network Device Authentication (네트워크 장치 인증)

## Persistence

## 14. Valid Accounts

**유효한 계정** 초기 액세스, 지속성, 권한 상승 또는 방어 회피를 얻기 위한 수단으로 기존 계정의 자격 증명을 획득하고 사용할 수 있음

- 1) Default Accounts (기본 계정)
- 2) Domain Accounts (도메인 계정)
- 3) Local Accounts (로컬 계정)
- 4) Cloud Accounts (클라우드 계정)

## Persistence

### 15. Office Application Startup

Office 응용 프로그램 시작 Microsoft Office 기반 애플리케이션 활용

- 1) Office Template Macros (Office 템플릿 매크로)
- 2) Office Test (사무실 시험)
- 3) Outlook Forms (Outlook 양식)
- 4) Outlook Home Page (Outlook 홈페이지)
- 5) Outlook Rules (Outlook 규칙)
- 6) Add-ins (추가 기능)

## Persistence

### 16. Pre-OS Boot

OS 이전 부팅 Pre-OS Boot 메커니즘

- 1) System Firmware (시스템 펌웨어)
- 2) Component Firmware (구성 요소 펌웨어)
- 3) Bootkit (부트킷)
- 4) ROMMONkit (롬몬킷)
- 5) TFTP Boot (TFTP 부팅)

**예약된 작업/작업** 작업 예약 기능을 악용하여 악성 코드의 초기 또는 반복 실행을 용이하게 할 수 있음

1) At (Linux) (리눅스에서)

2) At (Windows) (Windows에서)

3) Cron (크론)

4) Launchd (출시)

5) Scheduled Task (예약된 작업)

6) Systemd Timers (시스템 타이머)

7) Container Orchestration Job (컨테이너 오케스트레이션 작업)

**교통 신호** 트래픽 신호는 닫힌 포트를 열거나 악의적인 작업을 실행하는 것과 같은 특수 응답을 얻어내기 위해 시스템에 보내야 하는 값 또는 시퀀스의 사용을 포함

1) Port Knocking (포트 노킹)

포트를 활성화하기 위해 공격자는 일련의 시도된 연결을 미리 정의된 닫힌 포트 시퀀스로 보냄

시퀀스 완료 후 포트를 여는 것은 호스트 기반 방화벽에 의해 수행되지만 사용자 지정 소프트웨어로 구현 가능

서버 소프트웨어 구성 요소 Microsoft Office 기반 애플리케이션 활용

1) SQL Stored Procedures (SQL 저장 프로시저)

2) Transport Agent (운송 에이전트)

3) Web Shell

- 웹 서버를 백도어하여 시스템에 지속적인 액세스 가능
- 공격자가 웹 서버를 네트워크의 게이트웨이로 사용할 수 있도록 공개적으로 액세스할 수 있는 웹 서버에 배치되는 웹 스크립트
- 웹 서버를 호스팅하는 시스템에서 실행할 기능 집합이나 명령줄 인터페이스 제공 가능
- 주로 사용하는 Web Shell : Redhat, WSO, Venus, Code Hunters