**🔹 registry\_modification\_rule**

**설명:** 시스템 보안 기능을 비활성화하거나 악성코드 지속성을 위해 **레지스트리를 조작**하는 행위를 탐지합니다.  
**탐지 문자열:**

* EnableSmartScreen – SmartScreen 기능 비활성화 시도
* EnableLUA – UAC(User Account Control) 비활성화 시도
* DisableTaskMgr – 작업 관리자 비활성화
* DisableRegistryTools – 레지스트리 편집기 사용 차단
* HKCU\Software\Microsoft\Windows\CurrentVersion\Run – 사용자 영역의 자동 실행 등록
* HKLM\SYSTEM\CurrentControlSet\Services\MyMalService – 서비스로 등록된 악성코드 지속성 확보

**의미:** 공격자가 보안 기능을 우회하거나 부팅 시 자동 실행을 위해 레지스트리를 수정한 경우 탐지합니다.

**🔹 powershell\_encoded\_command\_rule**

**설명:** PowerShell을 이용한 **인코딩된 명령 실행**을 탐지합니다.  
**탐지 문자열:**

* powershell -EncodedCommand – Base64로 인코딩된 명령어 실행
* ExecutionPolicy Bypass – 실행 정책 우회를 통한 무조건 실행

**의미:** 흔히 악성 스크립트에서 탐지를 우회하기 위해 사용되는 기법입니다. 파일 없이 명령어 기반으로 악성 동작을 수행할 때 유용합니다.

**🔹 info\_collection\_rule**

**설명:** 시스템 정보를 수집하는 명령어를 탐지합니다.  
**탐지 문자열:**

* systeminfo – 시스템 환경 정보
* ipconfig /all – 네트워크 인터페이스 정보
* tasklist – 실행 중인 프로세스 목록
* netstat -an – 네트워크 연결 상태
* net user – 사용자 계정 정보

**의미:** 침해자나 악성코드가 내부 정찰 단계에서 시스템 환경을 파악하는 데 사용하는 명령어들입니다.

**🔹 startup\_persistence\_rule**

**설명:** 시스템 재부팅 시 자동으로 실행되는 **지속성 확보 수단**을 탐지합니다.  
**탐지 문자열:**

* HKCU\Software\Microsoft\Windows\CurrentVersion\Run – 레지스트리 기반 자동 실행
* cmd.exe /c echo pwned – 명령 프롬프트 명령 실행 예시
* .mal – 악성 파일 확장자 힌트

**의미:** 공격자가 시스템 재부팅 이후에도 악성코드가 자동 실행되도록 설정한 흔적을 탐지합니다.

**🔹 user\_account\_creation\_rule**

**설명:** **비인가 사용자 계정 생성**을 탐지합니다.  
**탐지 문자열:**

* net user backdooruser – 사용자 계정 생성
* net localgroup administrators backdooruser – 관리자 권한 부여

**의미:** 공격자가 시스템 접근을 지속하기 위해 백도어 계정을 생성하는 행위를 탐지합니다.