Lateral Movement(시스템 내부 이동)

Lateral Movement(시스템 내부 이동)은 공격자가 네트워크의 원격 시스템에 진입하고 제어하는 데 사용하는 기술로 구성된다. 주요 목표를 달성하려면 종종 네트워크를 탐색하여 목표를 찾은 다음 액세스 권한을 얻어야 한다. 목표를 달성하기 위해서는 여러 시스템과 계정을 통해 피벗을 해야 하는 경우가 많다. 공격자는 자신의 원격 액세스 도구를 설치하여 Lateral Movement(시스템 내부 이동)을 수행하거나 더 은밀할 수 있는 기본 네트워크 및 운영 체제 도구와 함께 합법적인 자격 증명을 사용할 수 있다.

- Exploitation of Remote Services

공격자는 원격 서비스를 악용하여 네트워크 내부에 들어가면 내부 시스템에 무단으로 액세스할 수 있다. 소프트웨어 취약점의 악용은 공격자가 프로그램, 서비스 또는 운영 체제 소프트웨어 또는 커널 자체의 프로그래밍 오류를 이용하여 공격자가 제어하는 코드를 실행할 때 발생한다. 원격 서비스의 침해 후 악용에 대한 공통 목표는 원격 시스템에 대한 액세스를 가능하게 하는 Lateral Movement(시스템 내부 이동)이다.

공격자는 원격 시스템이 취약한 상태에 있는지 확인할 수 있다. 이는 네트워크 서비스 스캐닝 또는 네트워크에 배포될 수 있는 일반적이고 취약한 소프트웨어를 찾는 기타 검색 방법을 통해 수행될 수 있다. 서버는 Lateral Movement(시스템 내부 이동) 악용의 높은 가치 대상일 가능성이 높지만, 엔드포인트 시스템이 추가 리소스에 대한 이점이나 액세스를 제공하는 경우에도 위험에 처할 수 있다.

SMB 및 RDP 와 같은 공통 서비스와 MySQL 및 웹 서버 서비스와 같은 내부 네트워크 내에서 사용될 수 있는 애플리케이션에 존재하는 몇 가지 잘 알려진 취약점이 있다.

취약한 원격 서비스의 권한 수준에 따라 공격자는 Lateral Movement(시스템 내부 이동) 악용의 결과로 권한 상승을 위한 악용을 달성할 수도 있다.

- Internal Spearphishing

공격자는 내부 스피어피싱을 사용하여 추가 정보에 대한 액세스 권한을 얻거나 해당 환경 내의 계정 또는 시스템에 이미 액세스 권한이 있는 동일한 조직 내의 다른 사용자를 악용할 수 있다. 내부 스피어피싱은 이전에 설치된 맬웨어로 사용자의 장치를 제어하거나 사용자의 계정 자격 증명을 손상시켜 이메일 계정을 소유하는 다단계 공격이다. 공격자는 신뢰할 수 있는 내부 계정을 이용하여 대상을 속여서 피싱 시도에 빠질 가능성을 높인다.

공격자는 내부 스피어피싱의 일부로 스피어피싱 첨부 파일 또는 스피어피싱 링크를 활용하여 페이로드를 전달하거나 외부 사이트로 리디렉션하여 이메일 로그인 인터페이스를 모방하는 사이트에서 입력 캡처를 통해 자격 증명을 캡처할 수 있다.

내부 스피어피싱이 사용된 주목할만한 사건이 있었다. Eye Pyramid 캠페인은 피해자 간의 Lateral Movement(시스템 내부 이동)을 위해 악성 첨부 파일이 포함된 피싱 이메일을 사용했으며 이 과정에서 거의 18,000 개의 이메일 계정이 손상되었다. SEA(Syrian Electronic Army)는 FT(Financial Times)의 이메일 계정을 해킹하여 추가 계정 자격 증명을 훔쳤다. FT 가 공격을 알고 직원들에게 위협에 대해 경고하기 시작하자 SEA 는 Financial Times IT 부서를 모방한 피싱 이메일을 보냈고 더 많은 사용자에게 피해 입힐 수 있었다.

- Lateral Tool Transfer

공격자는 손상된 환경에서 시스템 간에 도구 또는 기타 파일을 전송할 수 있다. 작업 과정에서 적의 도구나 다른 파일을 준비하기 위해 파일을 한 시스템에서 다른 시스템으로 복사할 수 있다. 공격자는 SMB 를 통해 연결된 네트워크 공유로의 파일 공유 또는 SMB/Windows Admin Shares 또는 원격 데스크톱 프로토콜을 통한 인증된 연결과 같은 고유한 파일 공유 프로토콜을 사용하여 Lateral Movement(시스템 내부 이동)을 지원하기 위해 내부 피해자 시스템 간에 파일을 측면으로 복사할 수 있다. scp, rsync 및 sftp 와 같은 기본 도구를 사용하여 Mac 및 Linux 에서 파일을 복사할 수도 있다.

- Remote Service Session Hijacking

[서브 기술] SSH Hijacking, RDP Hijacking

공격자는 환경에서 Lateral Movement(시스템 내부 이동)하기 위해 원격 서비스가 있는 기존 세션을 제어할 수 있다. 사용자는 유효한 자격 증명을 사용하여 텔넷, SSH 및 RDP 와 같은 원격 연결을 허용하도록 특별히 설계된 서비스에 로그인할 수 있다. 사용자가 서비스에 로그인하면 해당 서비스와의 지속적인 상호 작용을 유지할 수 있는 세션이 설정된다.

공격자는 원격 시스템에서 작업을 수행하도록 이러한 세션을 지휘할 수 있다. 원격 서비스 세션 하이재킹은 유효한 계정을 사용하여 새 세션을 생성하는 대신 기존 세션을 하이재킹한다는 점에서 원격 서비스 사용과 다르다.

- Remote Services

[서브 기술] Remote Desktop Protocol, SMB/Windows Admin Shares,
Distributed Component Object Model, SSH, VNC,
Windows Remote Management

공격자는 유효한 계정을 사용하여 telnet, SSH 및 VNC 와 같은 원격 연결을 허용하도록 특별히 설계된 서비스에 로그인할 수 있다. 그런 다음 공격자는 로그온한 사용자로 작업을 수행할 수 있다.

엔터프라이즈 환경에서 서버와 워크스테이션은 도메인으로 구성될 수 있다. 도메인은 중앙 집중식 ID 관리를 제공하여 사용자가 전체 네트워크에서 하나의 자격 증명 세트를 사용하여 로그인할 수 있도록 한다. 공격자가 일련의 유효한 도메인 자격 증명을 얻을 수 있는 경우 SSH(Secure Shell) 또는 RDP(원격 데스크톱 프로토콜)와 같은 원격 액세스 프로토콜을 사용하여 다양한 시스템에 로그인할 수 있다.

- Replication Through Removable Media

공격자는 맬웨어를 이동식 미디어에 복사하고 미디어가 시스템에 삽입되어 실행될 때 자동 실행 기능을 이용하여 연결이 끊겼거나 에어갭이 있는 네트워크에 있는 시스템으로 이동할 수 있다. Lateral Movement(시스템 내부 이동)의 경우 이동식 미디어에 저장된 실행 파일을 수정하거나 멀웨어를 복사하고 합법적인 파일처럼 보이도록 이름을 변경하여 사용자를 속여 별도의 시스템에서 실행할 수 있다. 초기 액세스의 경우 미디어 수동 조작, 미디어를 처음 포맷하는 데 사용되는 시스템 수정 또는 미디어 펌웨어 자체 수정을 통해 발생할 수 있다.

- Software Deployment Tools

공격자는 관리, 모니터링 및 배포 시스템과 같은 엔터프라이즈 네트워크 내에 설치된 타사 소프트웨어 제품군에 액세스하고 이를 사용하여 네트워크를 가로질러 이동할 수 있다. 타사 응용 프로그램 및 소프트웨어 배포 시스템은 관리 목적으로 네트워크 환경에서 사용 중일 수 있다(ex SCCM, HBSS, Altiris 등).

타사 네트워크 또는 전사적 소프트웨어 시스템에 대한 액세스는 공격자가 그러한 시스템에 연결된 모든 시스템에서 원격 코드 실행을 가능하게 할 수 있다. 액세스는 다른 시스템으로 횡적으로 이동하거나, 정보를 수집하거나, 모든 엔드포인트에서 하드 드라이브를 지우는 것과 같은 특정 효과를 일으키는 데 사용될 수 있다.

이 작업에 필요한 권한은 시스템 구성에 따라 다르다. 로컬 자격 증명으로 타사 시스템에 직접 액세스할 수 있거나 특정 도메인 자격 증명이 필요할 수 있다. 그러나 시스템에 로그인하거나 의도한 목적을 수행하기 위해 관리 계정이 필요할 수 있다.

- Taint Shared Content

공격자는 네트워크 드라이브 또는 내부 코드 저장소와 같은 공유 저장 위치에 콘텐츠를 추가하여 원격 시스템에 페이로드를 전달할 수 있다. 네트워크 드라이브나 다른 공유 위치에 저장된 콘텐츠는 다른 유효한 파일에 악성 프로그램, 스크립트 또는 악용 코드를 추가하여 오염될 수 있다. 사용자가 공유된 오염된 콘텐츠를 열면 악성 부분이 실행되어 원격 시스템에서 공격자의 코드를 실행할 수 있다. 공격자는 오염된 공유 콘텐츠를 사용하여 Lateral Movement(시스템 내부 이동)할 수 있다.

디렉터리 공유 피벗은 사용자가 공유 네트워크 디렉터리에 액세스할 때 맬웨어를 전파하기 위해 여러 다른 기술을 사용하는 기술의 변형이다. Hidden Files and Directories 를 통해 숨겨진 실제 디렉토리처럼 보이도록 Masquerading 을 사용하는 디렉토리 .LNK 파일의 Shortcut Modification 을 사용한다. 악성 .LNK 기반 디렉터리에는 디렉터리에 숨겨진 멀웨어 파일을 실행한 다음 사용자가 예상한 작업이 계속 발생하도록 실제 의도된 디렉터리를 여는 명령이 포함되어 있다. 자주 사용하는 네트워크 디렉터리와 함께 사용하는 경우 이 기술을 사용하면 재감염이 자주 발생하고 시스템과 잠재적으로 새롭고 더 높은 권한을 가진 계정에 광범위하게 액세스할 수 있다.

공격자는 공유 네트워크 디렉터리의 정상적인 바이너리에 코드를 추가하거나 추가하여 바이너리 감염을 통해 공유 네트워크 디렉터리를 손상시킬 수도 있다. 멀웨어는 정상 바이너리의 원래 진입점(OEP)을 수정하여 합법적인 코드보다 먼저 실행되도록 할 수 있다. 원격 시스템에서 실행될 때 새로 감염된 파일을 통해 감염이 계속 확산될 수 있다. 이러한 감염은 .EXE, .DLL, .SCR, .BAT 및/또는 .VBS 를 포함하되 이에 국한되지 않는 확장자로 끝나는 바이너리 및 비 바이너리 형식을 모두 대상으로 할 수 있다.

- Use Alternate Authentication Material

공격자는 환경 내에서 Lateral Movement(시스템 내부 이동)하고 정상적인 시스템 액세스 제어를 우회하기 위해 암호 해시, Kerberos 티켓 및 애플리케이션 액세스 토큰과 같은 대체 인증 자료를 사용할 수 있다.

인증 프로세스에는 일반적으로 하나 이상의 인증 요소(예: 비밀번호, 핀, 물리적 스마트 카드, 토큰 생성기 등)와 함께 유효한 ID(예: 사용자 이름)가 필요하다. 대체 인증 자료는 사용자 또는 애플리케이션이 유효한 ID 와 필수 인증 요소를 제공하여 성공적으로 인증한 후 시스템에서 합법적으로 생성된다. 신원 생성 과정에서 대체 인증 자료가 생성될 수도 있다.

대체 인증 자료를 캐싱하면 시스템에서 사용자에게 인증 요소를 다시 입력하지 않고도 신원이 성공적으로 인증되었는지 확인할 수 있다. 대체 인증은 시스템이 메모리나 디스크에서 유지 관리해야 해서 자격 증명 액세스 기술을 통해 도난당할 위험이 있다. 대체 인증 자료를 훔쳐 공격자는 일반 텍스트 암호나 추가 인증 요소를 알지 못해도 시스템 액세스 제어를 우회하고 시스템을 인증할 수 있다.