[민경님]
- Initial Access : 최초 침투 공격자는 공격 대상을 감염시킬 때 두 가지 방법을 사용
첫 번째는 악성 한글 문서 파일을 첨부하는 방법
두 번째는 공격 준비 단계에서 확보한 거점에 취약점 코드를 삽입하고 접속을 유도하는 방식

*최초 침투 방식
1) Spearphishing Attachment : 메일에 악성코드 첨부
2) Spearphishing Link : 메일에 악성 사이트 링크 삽입
3) Drive-by Compromise : 웹 사이트 접속 시 악성코드 감염
4) Exploit Public-Facing Application : 공개된 어플리케이션 취약점 악용

공격자는 주로 홈페이지에 메일 주소가 노출되어있는 영업팀이나 고객관리팀을 대상으로 피싱 메일을 보내는 것으로 확인

- Living off the land
: 해커와 같은 공격자들이, 시스템에 이미 설치되어 있는 Tool 을 사용해서 해킹 공격을 하는 기법
→ 피해자 시스템에 기본으로 설치되어 있는 프로그램을 활용하여 해킹을 수행하기 때문에, AV(안티바이러스) Software 의 탐지를 피할 수 있음
→ fileless 형태 : 시그니처 비교하여 LoL 공격 탐지 불가

최종 Payload(악성코드)를 침투시키기 위한 침투 도구(최종 Payload 의미 x)로 LoL(Living-off-the-land) Tool 을 사용

Windows 에 있는 LotL Tool : regsvr32.exe, mshta.exe, rundll32.exe, certutil.exe

LoL 공격은 다음과 같은 합법적인 도구를 사용
- Windows 장치 관리를 위한 광범위한 기능을 제공하는 스크립트 실행 프레임워크인 PowerShell (공격자는 PowerShell 을 사용하여 악성 스크립트 실행, 권한 상승, 백도어 설치 등을 수행)
- WMI(Windows Management Instrumentation)[UAC(사용자 계정 제어)]
(https://encyclopedia.kaspersky.com/glossary/user-account-control-uac/)
- 공격자가 악성 코드를 삽입하는 데 사용하는 원격 명령 실행 도구인 PsExec
- 사용자 자격 증명을 기록하는 Windows 용 보안 검색 도구인 Mimikatz

LoL 공격에 대응할 수 있는 도구 및 기술 : EDR 솔루션

자료 출처 :
https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=aepkoreanet&logNo=221980190942
https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/