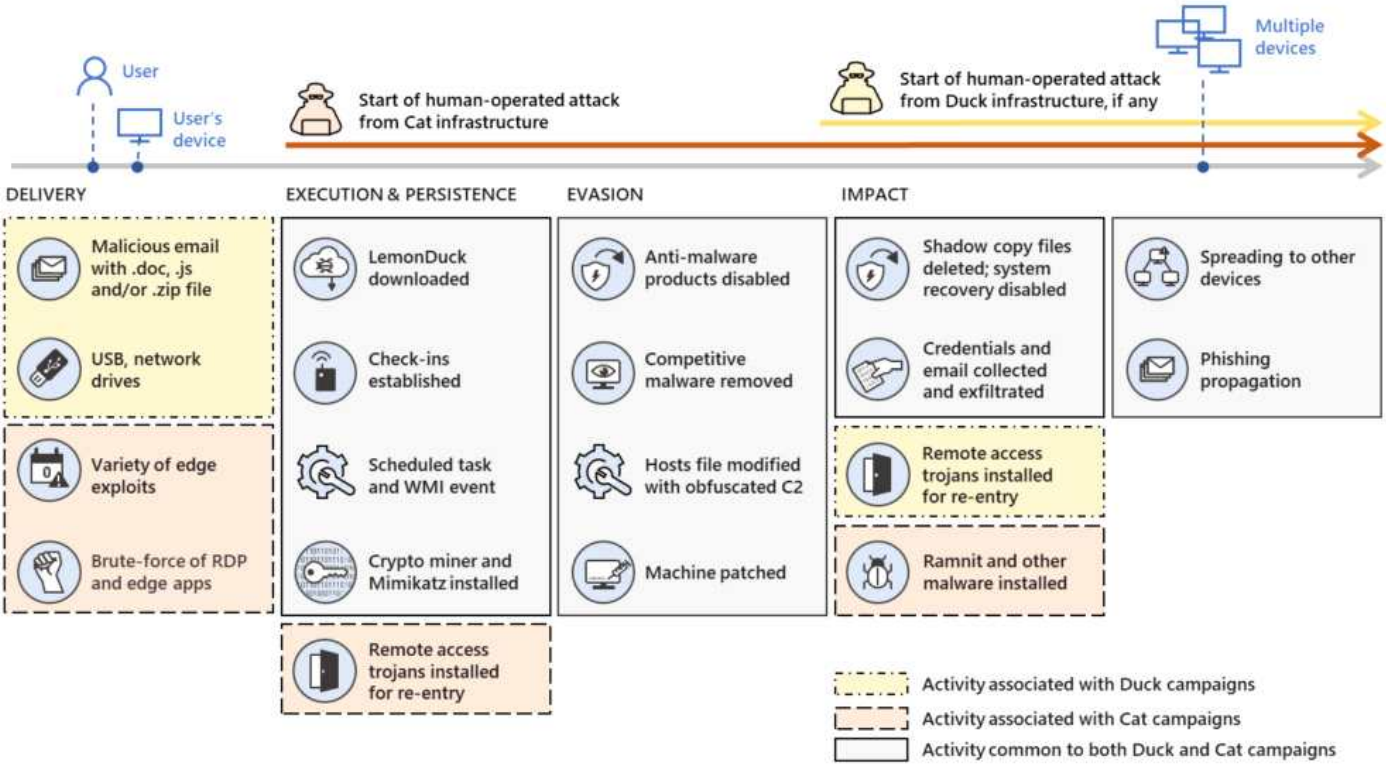
APT 모의해킹



1. 악성코드 배포

- 메일의 악성코드 첨부파일
  : .doc, .hwp, .js, .zip 등
- 물리적인 USB 연결, 네트워크 통신을 통한 감염
- 브라우저 취약점을 이용한 자동 배포
  : 제로데이 취약점, PDF 등
- 원격 접속 프로그램의 공격
  : RDP, VPN 등

2. 실행 & 유지

- LemonDuck
  : 감염된 네트워크 전체에 빠르게 확산되어 정보 탈취를 용이하게 함.
  : 크리덴셜 탈취 및 랜섬웨어를 포함한 다양한 악성 위협을 실행할 수 있는 게이트웨이 역할을 하는 차세대 임플란트를 설치하고, 관련 후속 공격을 진행하는 로더 역할을 함.
- Check-ins established
  : 설치한 악성코드들을 서로 연결
- Scheduled task
  : 악성코드를 작업 스케줄러에 등록하여 매일 실행되게 함.
- WMI
  : 윈도우의 리소스에 접근하여 여러 가지 설정을 구성할 수 있고, 다양한 부분을 관리할 수 있음.
- Crypto miner
  : 코인 체굴
- Mimikatz
  : 윈도우즈 계정정보 탈취 목적의 공격 도구
  : 많은 악성코드에 포함되어있음.

3. 우회

- Anti-malware products disabled
    : 바이러스가 백신 프로그램에 탐지되기 직전에 자체적으로 삭제하여 탐지 우회하기
    : 백신 프로그램이 실행되지 않게 하기
- Competitive malware removed
    : 다른 악성코드나 비슷한 형태의 악성코드 제거
    : 다른 악성코드가 걸리게 되면 담당자에게 보고되어 공격자가 심은 악성코드가 걸릴 확률이 높아짐.
- Hosts file modified with obfuscated C2
    : 호스트 파일을 수정 -> 악성 서버 등록하여 지속적으로 접속하도록 유도
- Machine patched
    : OS가 패치되면 악성코드 실행이 안 될 수도 있음.
    : 패치를 막거나 패치된 것들을 지우기.

4. 영향

- 랜섬웨어, 시스템 파괴, 삭제
- 정보 수집 및 유출

5. Multiple devices

- 다른 디바이스에 접근
- 피싱 메일

APT 대응

- 공격 소요 시간 지연
    : 시스템 패치, 인증 강화, 네트워크 망 분리, 중요정보 암호화, 허니팟 등
- 탐지 및 제거
    : 샌드박스, 행위기반 탐지 등
- 보안 인식 강화

프로젝트 주제 선정 목적

해커가 특정 기업이나 조직의 네트워크를 고도화된 다양한 보안 위협을 만들어 지속적으로 공격을 가하여 더욱 탐지 및 차단하기 어려워졌다. 2004년부터 우리나라도 꾸준히 공격을 받는 APT 모의해킹을 통해서 악성코드 배포와 해킹 전개 과정을 이해하고 어떻게 대응할 수 있는지 알아볼 수 있다.

프로젝트 목표

- 악성코드 배포, 실행 및 유지, 탐지 및 차단 우회, 공격목표 달성, 다른 디바이스 감염
- 공격자의 공격 소요 시간을 지연, 공격에 대한 탐지 및 제거

R&R

진행 계획(WBS)