1. 명확한 목표 정하기

- 키오스크 종류(https://www.nicetcm.co.kr/front/sub/sub0206.htm)

- 어떤 목표를 가지고 하는지

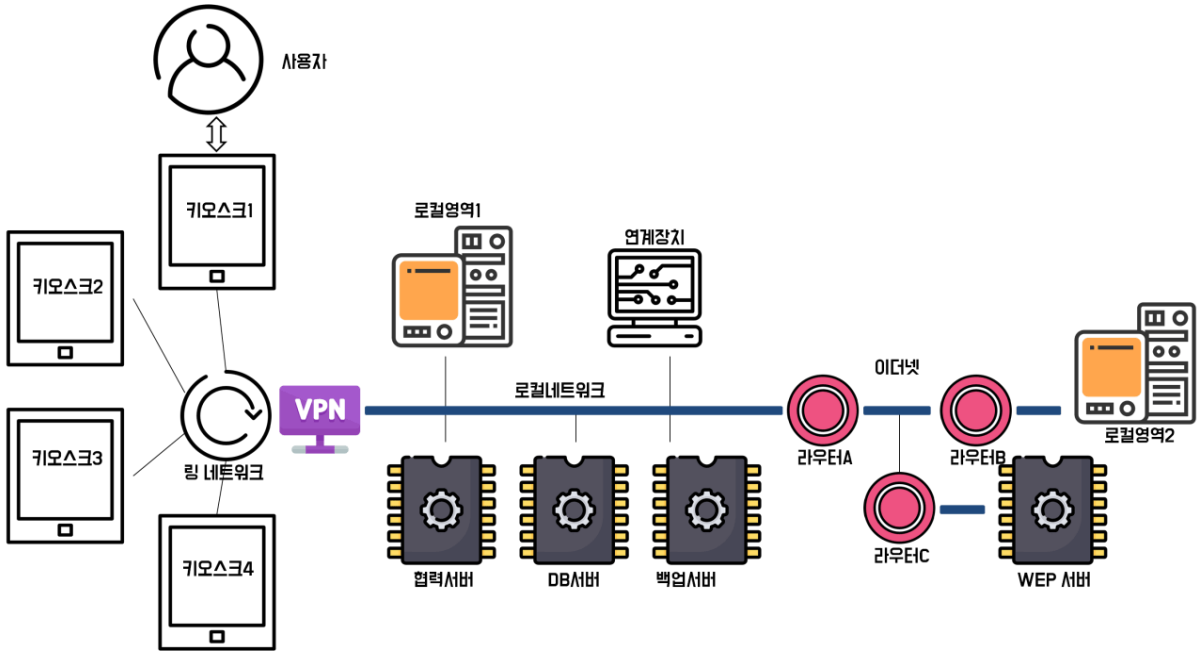
-> 포스단말기 해킹한 후 빈어택 방식을 이용하여 개인정보, 금융정보 탈취

-> 탈취한 이메일 주소, 비밀번호로 팀뷰어 로그인 창에 Credential stuffing 공격 진행

해당 기사에서는 확보한 카드 번호로 물품을 구매하는 대신 주로 '다크 웹' 등에서 팔아넘김

출처 : 연합인포맥스(http://news.einfomax.co.kr)

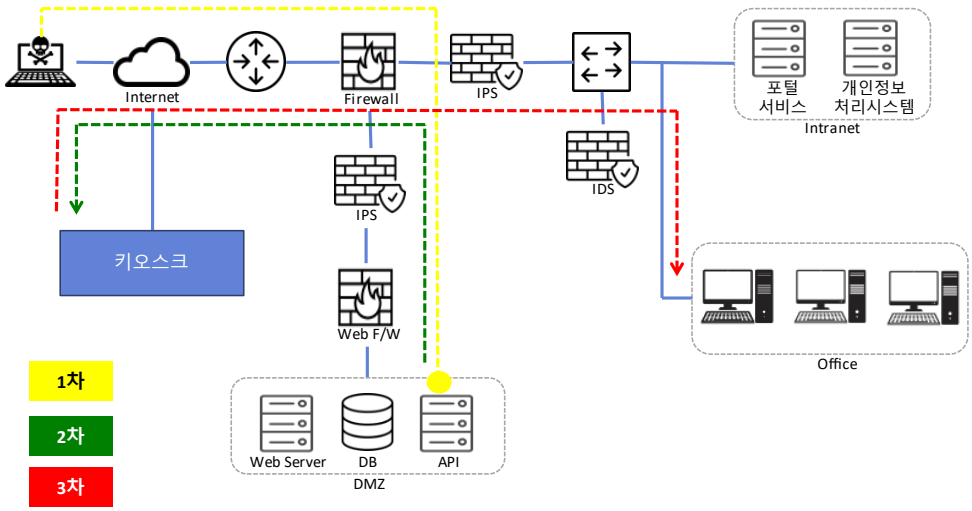
- 회사 시스템(https://doonaint.net/index.php/kiosk-system/)



2. 네트워크 구성도 현실성있게 바꾸기

-> 위에 있는 회사 시스템 구성도를 토대로 네트워크 구성도를 수정(키오스크 개수 줄이기, 중요도 낮은 서버 삭제 등)하면 어떨지..

(*api 서버는 intranet 안에 존재 / 키오스크는 화이트리스트 방식 / 접점 자체가 없으며 VPN으로 연결)



이전 시나리오

3. 키오스크가 VPN 사용한다는 가정하에 어떻게 침투할 수 있는지

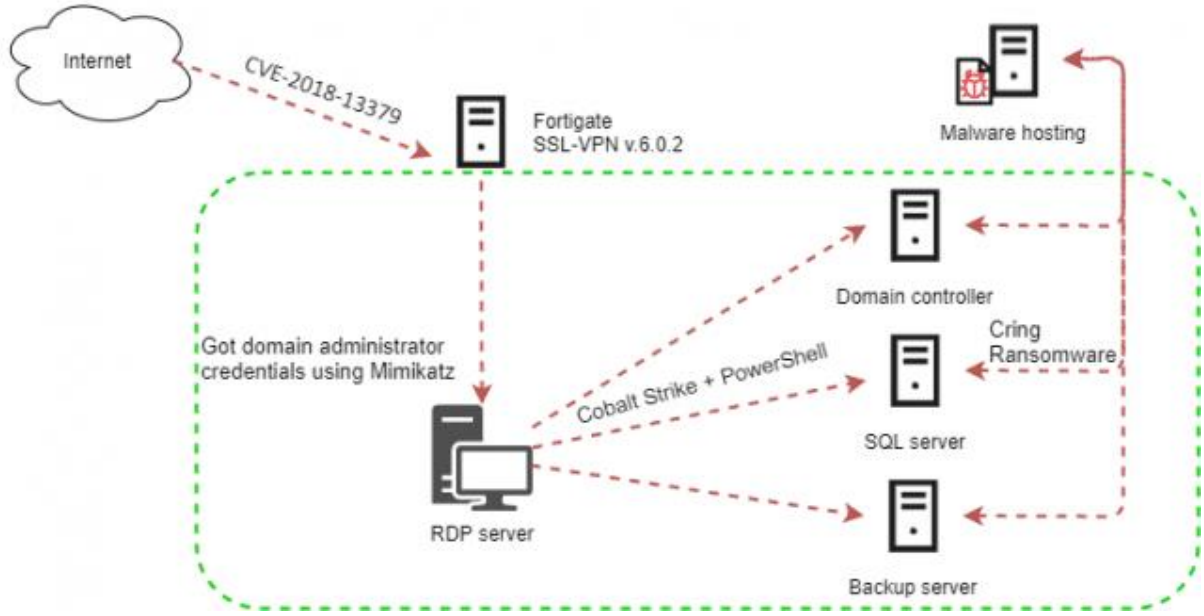
- vpn 관련 취약점 조사 진행(포티넷 VPN 취약점을 악용한 공격)

공통보안취약점공개항목(CVE) 번호는 'CVE-2018-13379'

VPN, 많이 쓰니 해커가 집중 공략했다(https://zdnet.co.kr/view/?no=20210409093837)

VPN 도입이 확산되고 있는 점을 노려 취약점을 악용해 랜섬웨어를 유포

지난 1월 알려진 포티넷 VPN 서버 취약점을 악용해 랜섬웨어 '크링(Cring)'을 유포했다. 해당 취약점에 대한 보안 패치가 제공되고 있으나, 아직 보안 패치를 적용하지 않은 네트워크를 노렸다.



크링 공격 워크 플로우(출처=카스퍼스키)

해커는 이 취약점을 통해 사용자 계정을 탈취한 뒤 내부망에 접속했다. 이후 오픈소스 해킹 도구 '미미카츠'를 악용해 사용자 계정 정보를 추가 탈취하고, '코발트 스트라이크'등 해킹 도구로 권한을 탈취해나갔다.

VPN 해킹도 일상화 우려…이제 대안을 생각 할 때

(http://www.nspna.com/news/?mode=view&newsid=514192)

VPN은 인터넷 등 통신 구간에서 양 접속 지점간 데이터를 암호화하는 터널을 형성하여 외부로부터 해킹을 막아주는 역할

문제가 될 수 있는 부분은 인터넷처럼 오픈 된 환경에서 최초 접속 요구자가 누구인지 확인되기도 전에 내부서버와 연결될 수 있는 통신IP(Internet Protocol)가 노출되어 내부시스템에 대한 공격의 원인을 제공할 수도 있다. 이것은 외부 단말기가 내부와 접속된 이후에 인증(선 접속 후 인증)을 받는다는 것을 기본으로 하는 VPN의 한계 중의 하나이고, 접속자가 외부 해커인지 정상적으로 접속을 요구하고 있는 사용자 인지 구분하기 어렵기 때문에 해킹 고수들의 타겟이 될 가능성은 언제든지 열려 있다고 본다.

원자력연구원의 해킹 통로 전락한 VPN, 공공기관 취약점 점검 나섰다

(https://pplus.co.kr/news/?mod=document&uid=398)

보안업체인 뉴스파이어가 2021년 1분기 악성행위를 분석한 결과 대표적인 VPN 기업인 포티넷과 펄스 시큐어

의 VPN을 노린 공격이 증가했는데, 포티넷은 무려 1,916%, 펄스 시큐어는 1,527% 증가했다고 알려졌습니다. 또한, 디지털 셰도우즈 역시 VPN에 대한 공격이 증가하고 있다며 조사결과를 발표했고, 파이어아이는 중국의 사이버 공격 단체들이 펄스 시큐어의 VPN 취약점을 공략해 미국과 유럽의 국방, 정부, 운송, 금융 기관들을 정찰했다고 밝혔습니다.

* docker

docker 기본 개념 영상

https://www.youtube.com/watch?v=hWPv9LMlme8

https://www.youtube.com/watch?v=tPjpcsgxgWc