# 사이버 공격

## 설명

즉각적인 조치를 촉구하는 물리적 위협과 달리 사이버 위협과 공격은 대체로 식별 또는 파악하기가 어렵습니다. 사이버 보안은 사이버 인시던트를 예방, 검색하고 그에 대응하는 것과 관련합니다. 정부 기관, 병원, 기업, 은행, 공익사업자를 비롯하여 지금의 거의 모든 조직은 컴퓨터 시스템에 운영 및 데이터 관리를 맡기며 그에 따라 사이버 공격에 영향받기 쉽습니다.

악당에게 노출되어 있는 이른바 "공격 표면"으로는 컴퓨터 하드웨어, 태블릿, 휴대전화 등 많은 웹 사용 장치와 소위 "사물 인터넷"에 연결된 가전기기 등이 있습니다. 사이버 공격의 위험 중에서 잘 알려진 것으로는 침입자가 전체 시스템을 지우고, 데이터나 운영 체제를 인질로 삼고서 대가를 요구하고, 기밀이나 신상 정보를 탈취하고, 시스템에 침입해서 파일을 변경하고 혹은 특정 컴퓨터나 장치를 사용해서 연락처 목록에 액세스한 후 다른 상대를 공격하거나 감염시키는 것 등이 있습니다.

## 주요 용어

- **사이버 공격**은 개인, 네트워크 조직, 테러리스트 집단 또는 국가로부터 비롯될 수 있으며 정부, 비즈니스, 공공시설, 공중에 심각한 (동시에 위험한) 문제를 초래할 수도 있습니다.
- **해킹**은 사람이든 "봇"이든 공격자가 보안/제한된 데이터 또는 운영에 직접 액세스할 수 있는 권한을 획득하는, "전신선을 통해" 특정 시스템에 가하는 직접적인 공격입니다. 일반적으로 그러한 해킹을 가능하게 하는 통로는 "피싱"이나 다운로드 스캠을 통해 열립니다.
- **IoT(사물 인터넷)**은 웹 사용 장치 및 냉장고, 음향 기기, 시계, 자동 온도 조절기, 보안 시스템, 커피 메이커 등을 비롯한 가전기기를 아우릅니다.
- **피싱**은 불특정한 몇 명의 받는 사람이 바이러스나 기타 멀웨어를 활성화하는 메시지의 어떤 곳(예컨대 첨부 파일, 링크, "매크로 사용" 단추 등)을 클릭하겠지 하는 바람으로 광범위하게 유포하는 이메일 또는 텍스트 통신으로 구성됩니다. 예를 들어 특정한 정부나 유틸리티 등 대상이 지정된 피싱 캠페인은 스피어 피싱이라고 합니다.
- **사회 공학**은 IT 보안 방책을 우회하고자 시스템보다 사용자의 취약성을 이용하는 것과 관련이 있습니다. 그 예로는 피싱, 이메일 스캠 등의 사기가 있습니다. 사용자는 대체로 IT 보안 아키텍처에서 가장 쉽게 뚫리는 요소입니다.

## 행동 지침

### 재난 발생 전(대비/완화)

- ❑ 방화벽을 켜 두고 늘 업데이트합니다.
- ❑ 바이러스 백신/스파이웨어 방지 소프트웨어를 설치 또는 업데이트합니다.
- ❑ 강력한 고유 암호를 사용하되 정기적으로 암호를 변경합니다.
- ❑ 모든 업데이트를 주의 깊게 찾아서 운영 체제, 펌웨어, 소프트웨어, 바이러스 백신 등에 즉시 설치합니다.
- ❑ 다운로드를 조심하십시오. 원치 않는 이메일이나 문자에 포함된 첨부 파일, 링크 또는 매크로를 절대 클릭하지 마십시오.
- ❑ 컴퓨터를 사용하지 않을 때는 컴퓨터를 끕니다.
- ❑ 이메일의 원본을 늘 확인하되, 의심이 들면 삭제합니다.
- ❑ 틀린 철자, 이상한 구문이나 단어 사용, 자리 표시자가 있는 언어, 수상한 링크 URL 등 "꺼짐"(퇴근이나 휴가)으로 보이는 알려진 연락처로부터 수신된 이메일은 의심하십시오. 많은 경우 해커들은 잘 알려진 이메일을 사용한다는 점을 주의하십시오.
- ❑ 의심 가는 콘텐츠를 삭제하기 전에 분석에 필요한 스크린샷을 찍어 둡니다.
- ❑ 외부 하드 드라이브 또는 Cloud에 사용자의 모든 데이터를 정기적으로 백업합니다. Mac 사용자는 "Time Machine (타임머신)" 기능을 사용할 수 있습니다.

### 재난 발생 시(대응)

- ❑ 감염된 장치는 네트워크에서 분리합니다.
- ❑ 직장에 있는 경우 장치에 미심쩍거나 확인된 공격이 있다면 어떤 공격이든 IT 직원에게 알리고, 스크린샷을 제공합니다.
- ❑ 인시던트가 금융, 신상 또는 의료 정보의 손실을 초래하는 경우 경찰에 신고서를 정식 제출합니다.

### 재난이 지나간 후(복구)

- ❑ 악영향을 받을 수도 있는 신용 거래처, 은행 거래처, 고객, 직원, 가족, 친구 등 모든 이에게 공격 피해 사실을 알립니다. 계정과 모든 암호를 변경합니다.
- ❑ 해당 검사와 유틸리티를 사용해서 혹시 모를 감염을 제거합니다.
- ❑ 신용 평가서, 은행 입출금 내역, 투자 내역 및 신용카드 사용 내역을 모니터링합니다.
- ❑ 장치가 감염되지 않았는지 확인하고, 그래도 의심이 든다면 하드 드라이브를 초기화한 후 모든 소프트웨어를 다시 설치합니다.