Eighth Army

CYBERSECURITY BULLETIN Issue 24-01– November 2023

8군 G6 사이버보안문화캠페인 기획안 24-01

제 목 : 이동식 미디어 및 USB 기기 보안의식 고취 & 모범사례 구성원들의 사이버 보안 의식 고취를 위한 분기별 공고

사이버 보안 모범 사례 – 이동식 미디어 및 USB 장치

이 분기별 8A G6 사이버 보안 문화 캠페인 게시판은 승인되지 않은 USB 장치를 정부 컴퓨터에 ***연결하지 않는 것***과 USB 장치 및 이동식 미디어에 대한 안전 조치 및 모범 사례에 초점을 맞추고 있습니다.

"매일매일 우리는 사이버 영역에서 전투를 벌이는 중이며, 우리 모두가 이 전투에 있어서 중요한 구성원입니다. 우리의 적들은, 우리 팀원들의 행동이나, 대책의 부재가 전투 네트워크에 가장 큰 위협이 된다는 것을 알고 있습니다. 네트워크 사용 시, 경각심의 공백은 종종 생산성에 있어, 상당한 손실을 초래하고, 최악의 경우 정보와 시스템을 손상시킵니다. 사이버 위협이 진화함에 따라, 우리는 어떤 것도 당연하게 받아들일 수 없습니다. 이것은 우리의 행동 양식이며, 우리 모두는 디지털 자산을 보호하기 위해, 우리의 역할을 해야 합니다."

- COL Les Thompson, 8A ACoS G6

Cybersecurity Bulletin Issue 24-01, November 2023

이동식미디어란?

이동식 미디어는 플래시 미디어, 외장 하드 드라이브, 광 디스크, 음악 플레이어 등을 포함하며, 노트북, 태블릿, 블루투스 기기, 스마트폰 등을 포함한 다른 모바일 사용 및 휴대용 전자기기(PED)도 유사한 기능을 가지고 있으며, 플래시 미디어든 모바일 기기든 아래에서 상세히 설명하는 동일한 규칙, 보호, 위험이 적용됩니다.

1. **USB 장치는 사용자와 공격자(ex.해커) 모두에게 편리합니다.** USB 드라이브는 가격이 저렴하고 쉽게 사용할 수 있으며 휴대성이 뛰어나기 때문에 파일 저장 및 전송용으로 사용자에게 인기가 있으며, 공격자에게 매력적인 공격 매개체입니다.

2. **악성 소프트웨어 감염은 쉽게 발생할 수 있습니다.** 공격자들은 USB 드라이브를 사용하여 컴퓨터에 USB 드라이브를 연결할 때 이를 탐지할 수 있는 악성코드를 컴퓨터에 감염시킬 수 있습니다. 악성코드는 USB 드라이브에 악성코드를 다운로드하고 다른 드라이브에 연결할 때 이 악성코드를 퍼뜨립니다. 일부 공격자들은 공급망을 공격 대상으로 삼아 생산 과정에서 전자 액자, USB 드라이브 등의 아이템을 감염시키기도 하는데, 사용자가 이러한 감염된 제품을 구입하여 컴퓨터에 꽂으면 악성코드가 설치됩니다.

3. **데이터는 쉽게 도난당하거나 분실될 수 있습니다.** 공격자는 그들의 USB 드라이브를 사용하여 직접 정보를 훔칠 수 있습니다. 컴퓨터에 물리적으로 액세스한 공격자는 USB 드라이브에 직접 정보를 다운로드할 수 있습니다. 컴퓨터의 전원이 꺼져도 컴퓨터의 메모리는 전원이 공급되지 않은 상태에서 몇 분 동안 활성화되어 있기 때문에 전원이 꺼져 있는 컴퓨터도 취약할 수 있습니다. 공격자가 메모리가 활성화 되어있는동안 USB 드라이브를 컴퓨터에 연결하고 USB 드라이브에서 시스템을 빠르게 재부팅하면 암호와 같은 민감한 데이터 및 암호 키를 포함하여 컴퓨터의 메모리를 가져갈 수 있습니다. 이러한 공격은 탐지하기조차 어려울 수 있습니다. 이러한 공격 매개체뿐만 아니라 USB 드라이브는 쉽게 분실되고 도난 당합니다. 데이터를 백업하지 않으면 USB 드라이브가 손실되어 작업 시간이 손실될 수 있습니다. 마지막으로 암호화되지 않은 드라이브에서는 누구든지 모든 데이터를 찾거나 훔칠 수 있습니다.

이동식 미디어 및 USB 장치 사용 모범 사례

모범 사례를 시행하고 따르는 것은 잠재적인 사이버 공격의 영향을 줄이는 데 도움이 될 수 있습니다. 다음은 개인 또는 조직 보안에 영향을 미칠 수 있는 재앙적인 결과를 최대한 줄이고 피하기 위해 적용하고 따라야 할 몇 가지 방안과 조치들입니다.

1. **출처가 불분명하거나 의심스러운 기기를 조심해야 합니다.** 직장에서 출처 불명의 장치를 발견한 경우 해당 기관(조직의 사이버 보안 팀)에 장치를 제공합니다. 컴퓨터에 연결하여 내용을 보거나 소유자를 식별하지 마십시오.

2. **개인 PC와 노트북이 적절하게 보호되고 있는지 확인합니다.** 자동 실행 기능을 비활성화하는 것과 같은 적절한 환경설정은 감염된 USB 드라이브의 악성 코드가 자동으로 열리는 것을 방지할 수 있습니다. 또한 바이러스 백신 소프트웨어인 방화벽을 사용하고 유지하며 바이러스 정의 및 소프트웨어 업데이트를 최신 상태로 유지하므로써 장치가 USB 장치와 이동식 미디어와 관련된 공격에 덜 취약하게 됩니다.

3. **공공장소에서 모바일 기기를 가지고 이동하거나 사용할 때는 주의해야 합니다.** 특히 공항 보안 검색대를 통과할 때는 항상 기기의 시각적 또는 물리적 제어를 유지해야 합니다. 공용 Wi-Fi 연결을 통해 전송된 정보는 도난에 노출될 수 있으며 기기는 악성 프로그램에 노출될 수 있음을 유의하십시오. VPN(Virtual Private Network)을 사용하면 공용 Wi-Fi와 관련된 위험을 줄이는데 도움이 될 수 있습니다. 공공장소에서 기기를 사용할 때는 기기에 보이는 정보에 주의해야 하며 보안 장치를 사용하더라도 공공장소에서는 중요한 정보에 대해 절대 논의하지 마십시오.

4. **이동식 미디어, PED 및 USB 장치의 데이터가 적절하게 보호되었는지 확인합니다.** 사용하지 않을 때는 장치를 잠그고 화면 보호기를 활성화해야 합니다. 가능한 경우 모든 장치의 중요한 데이터가 암호화되어 있는지 확인하고, 가능한 경우 장치가 생체 인식 또는 일회용 비밀번호(OTP)와 같은 두 가지 요소 인증을 사용하고 있는지 확인합니다.

5. **근거리 무선 통신(NFC)을 지원하는 장치를 사용할 때는 주의해야 하며 모바일 장치에서는 GPS를 주의해야합니다.** NFC는 스마트폰에 적용되는 무선 기술로서, 기기가 매우 근접해 있을 때 정보 교환을 가능하게 하며, 신용카드 결제 정보(예를 들어, 비접촉식 결제)의 전송을 위해 일반적으로 사용됩니다. 마찬가지로, GPS는 모바일 기기에서 자주 사용되며, 사용자가 알지 못하거나 동의하지 않아도 위치를 추적할 수 있는 많은 애플리케이션에 의해 접근됩니다. 이러한 기술과 관련된 위험을 최소화하기 위해 애플리케이션 허가를 검토할 뿐만 아니라 기기와 앱을 업데이트하는 것이 중요합니다.

6. **스마트폰을 업무용 컴퓨터에 꽂지 마십시오.** 정부 소유 컴퓨터의 경우, 조직에서 명시적으로 승인하지 않는 한 USB 드라이브, 스마트폰 또는 기타 PED를 USB 포트에 꽂지 마십시오. 여기에는 워크스테이션, 씬 클라이언트, 도킹 스테이션 및 허브, 모니터 등에 있는 USB 포트가 포함됩니다. 데이터가 전송되지 않고, 장치를 충전하기 위한 목적으로만 사용하더라도 승인되지 않은 USB 장치가 감지되어 철저하게 조사되고 공식적으로 처리해야하는 사이버 보안 사고가 발생합니다. 조직의 사이버 보안 사고의 원인이 되지 마십시오!

Cybersecurity Awareness와 관련된 추가 정보나 질문에 대해서는 전 세계에 있는 사이버보안처에 문의하시기 바랍니다:

USARMY Camp Humphreys 8 Army List Cybersecurity Information Request
usarmy.humphreys.8-army.list.cybersecurity-information-request@army.mil