JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 4, pp. 75-81, April 2023
https://doi.org/10.9708/jksci.2023.28.04.075

A Study on the Risk and Countermeasures of Hacking Cable

Hea-Jun Kim*, Young-Bok Cho**

*Student, Dept. of Information Security, Daejeon University, Daejeon, Korea
**Professor, School of Information Security, Daejeon University, Daejeon, Korea

[Abstract]

Since the introduction of smartphones, the introduction of charging cable infrastructure that can be used for public use is underway. Thanks to this, people use public cables comfortably without doubt, but most people are not aware of the dangers of public cables. These public cables can lead to infringement accidents such as personal information exposure due to the development of hacking cables, and in the worst case, hackers can take control of smartphones and laptops. This study analyzed the operating principles and attack principles of hacking cables that seem like these general charging cables, but contain malicious scripts or hardware inside. In addition, physical and logical countermeasures were considered based on the analysis.

▸ **Key words**: Mobile, Cable, Hacking, Keystroke, Injection

[요 약]

스마트폰 도입 이후로 공용으로 사용할 수 있는 충전 케이블 인프라 도입이 진행 중이다. 이로 인해, 사람들은 공용 케이블을 의심 없이 편하게 이용하지만, 공용 케이블의 위험성에 대해서는 대부분 인지하지 못하고 있다. 이러한 공용 케이블은 해킹 케이블의 발전으로 개인 정보 노출 등의 침해 사고가 일어날 수 있고, 최악의 경우에는 해커가 스마트폰, 노트북 등을 장악할 수 있다. 본 연구는 이러한 일반적인 충전 케이블처럼 보이지만, 내부에 악성 스크립트 또는 하드웨어가 포함된 해킹 케이블의 동작 원리와 공격 원리를 분석하였다. 또한, 분석 내용을 바탕으로 물리적, 논리적 대응 방안을 고찰해본다.

▸ **주제어**: 모바일, 케이블, 해킹, 키스트로크, 주입

• First Author: Hea-Jun Kim, Corresponding Author: Young-Bok Cho
*Hea-Jun Kim (ravenkim97@naver.com), Dept. of Information Security, Daejeon University
**Young-Bok Cho (ybcho@dju.ac.kr), School of Information Security, Daejeon University
• Received: 2023. 03. 14, Revised: 2023. 04. 21, Accepted: 2023. 04. 21.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

대한민국의 스마트폰 사용률은 2012년 53.4%에서 시작하여 현재 2022년 6월에는 97.1%에 이르렀다[1]. 그러나 개인들이 모두 이를 충전하기 위한 충전용 케이블을 휴대하지는 않는다. 이를 위해 터미널, 카페, 호텔 등에 충전 케이블이 구비되어 있는 것을 자주 접하게 될 수 있다. 그러나 우리는 디바이스에 대한 해킹 위험성은 널리 인지하고 있지만, 케이블에 대한 위험은 인식하지 못하고 쉽게 이용하고 있다. 2019년 사이버 보안 컨퍼런스인 데프콘에서 보안 연구원 마이크 그로버가 해킹 공격용 O.MG 케이블을 공개한 이후, 2021년 하반기에는 우리나라에서도 뒤늦게 해킹 케이블에 대한 위험이 화제가 되었다[2]. 초기에는 개인 하드웨어 학습 프로젝트로 시작되었으며, 다른 사람들이 DIY 방식으로 복제할 수 있는 오픈소스를 갖는 데 중점을 두고 하위 수준 코드의 다양한 부분을 정밀 검사하기 시작했다. 현재 해킹 케이블은 200달러의 금액으로 일반인도 쉽게 구매할 수 있으며, 정상 케이블과 외관이 똑같아 의심 없이 사용하게 되어 악용의 여지가 있다.

케이블을 통한 해킹은 모바일 기기뿐만 아니라 PC, 태블릿 등 입력이 가능한 모든 기기가 대상이 될 수 있으며, 케이블이 정상적인 것처럼 보이지만 실제로는 해킹이 이루어져 몇 초 만에 피싱 사이트에 접속하고 피싱 어플리케이션을 배포하는 등의 악용이 가능하다. 이로 인해 우리가 모르는 사이에 문자, 통화, 사진 데이터뿐만 아니라 우리가 입력하는 모든 내용이 공격자에게 노출되어 피해를 입을 수 있으며, 피해자는 해당 사실을 알 방법이 없어 치명적인 피해를 입을 수 있다.

본 연구는 해킹 케이블의 작동 원리 및 공격 기법 등을 분석하여, 공격자가 해킹 케이블을 악용할 때 피해자가 겪을 수 있는 피해 사실을 모든 이가 인지하고 주의할 수 있도록 경각심을 심어주는 것을 목표로 한다. 또한, 해킹 케이블에 대응하는 방안에 대해 논의한다.

II. Related research

1. Outline

해킹 케이블은 백그라운드에서 악의적인 활동이 이루어지는 동시에 충전 및 데이터 전송과 같은 정상적인 기능도 수행하기에 피해자가 해킹 케이블을 통해 공격을 당하고 있다는 사실을 인지하기가 어렵다. <그림 1>은 병원에서 사용되는 X-ray를 통하여 케이블 내부를 나타낸 것이다.

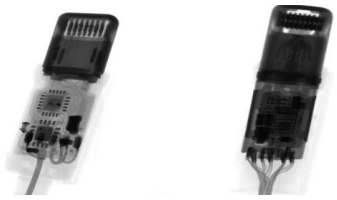

Fig. 1. Inside the cable identified by X-ray

<그림 2>와 같이 해킹 케이블은 다른 USB 케이블과 외관상 차이점은 없지만, X-ray로 촬영하면 차이점을 발견할 수 있다. 해킹 케이블에는 일반 케이블과 달리 악성 칩이 내장되어 있고, 이 칩을 통해 피해자의 기기에서 악성 스크립트를 실행시킬 수 있다.

Fig. 2. Hacking Cable Malicious Chips

2. Function

해킹 케이블의 기능으로는 Payloads 전송, Keylogger, Concealment가 있다. 각각의 기능에 대한 설명은 다음과 같다[3].

2.1 Send Payloads

해킹 케이블은 'Ducky Script' 언어로 짜인 공격 구문을 피해자의 기기에 전송할 수 있다. <그림 3>은 DuckyScript를 캡쳐한 화면으로 프로그래밍 경험이 거의 없어도 쉽게 작성할 수 있는 스크립트 언어로 이를 이용하면 간단한 문자열 명령을 통해 다양한 기능을 수행할 수 있다.

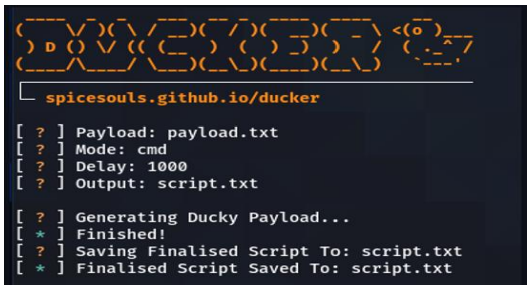

Fig. 3. DuckyScript

이러한 스크립트 언어는 파일 전송도 없이 작성만 하면 되기 때문에 개발이 빠르고, 공격 구문을 작성하기 쉽다.

이러한 기능은 모바일에서도 동일하게 작동하며, O.MG 장치에 스마트폰과 태블릿에서 실행 가능한 Keystroke Injection이 포함될 경우 쉽게 페이로드를 전송할 수 있게 된다. 이때 확인해야 할 점은 활성 USB-C 쪽만 스마트폰이나 태블릿에 연결되어 있어야 한다는 것이다. 여기서 Keystroke Injection은 특수하게 설계된 장치가 연결된 모든 호스트 디바이스에서 자동으로 코드를 실행하는 것을 의미한다[4].

2.2 Keylogger

키로거를 통해 사용자의 키보드 이용 로그를 기록하고 공격자에게 이를 전달할 수 있다. 키로깅을 성공적으로 하기 위해서는 로깅하려는 키보드와 키보드가 연결된 기기 사이에 물리적으로 O.MG 기기를 연결해야 한다. 따라서, O.MG 케이블은 케이블이 분리가 가능한 키보드에서만 사용할 수 있다. 이때, 악성 칩이 포함된 부분을 USB 호스트에 연결해야 한다. 현재 Full Speed USB 키보드 캡처를 지원하며, 키로거 기능을 통해 최대 650,000번의 키 입력을 저장할 수 있다. 이러한 키로거 기능은 모든 로그인 및 전자상거래 환경에서 큰 위협이 될 수 있다. 키로거는 계정 탈취를 위한 타 기법들과 비교했을 때, 많은 정보를 손쉽게 탈취할 수 있으며, 피해자가 알아차리기 어려워 공공장소와 같은 많은 사람이 사용하는 공간에서는 피해가 더욱 커질 우려가 있다[5].

2.3 Concealment

Concealment는 페이로드를 전송하지 않을 때는 표준 USB 2.0 케이블처럼 데이터를 전달해 충전용 케이블로 인식하는 기능이다. 이 상태에서는 호스트가 케이블을 감지할 수 없는 상태로 유지된다. 만일의 경우에는 원격으로 플래시를 초기화하거나 O.MG 케이블이 더 이상 데이터를 전달하지 않도록 임의로 자기 자신을 파손시킬 수 있다. 또한, 위치를 감지하여 자동으로 동작을 수정, 페이로드를 트리거 및 삭제하는 등의 작업을 수행할 수 있다. 이를 통해 케이블이 공격자와 거리가 멀어지면 일반 케이블로 위장할 수 있고, USB 식별자를 변경하여 신뢰할 수 있는 장치로 위장할 수도 있다.

3. Anticipated damage

스마트폰에서 케이블 사용 시 예상되는 피해는 다음과 같다[6].

- 키보드 자판 입력 조정 권한 탈취
- 파일 관리자 비밀번호 등 중요정보 탈취
- 파일 열람, 파일 변경 및 파일 유출
- 인터넷 접속 시 악성 사이트로 우회
- 네트워크 카드 스푸핑, 컴퓨터 DNS 경로 조작
- PC boot loader 감염
- USB 드라이브에 Hidden partition 조작

III. Attack Scenario

일반적으로 원격의 공격자가 타겟을 설정하고 해킹을 위한 공격을 시도할 경우 <그림 5>와 같은 방법을 이용하게 된다.

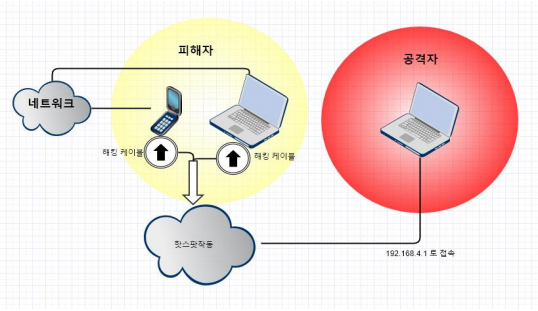

Fig. 4. Structural chart of the attack process

해킹 케이블의 악성 칩으로 모바일 및 PC에 연결하는 동시에 전력이 공급되어 O.MG WiFi가 작동하게 된다. <그림 4>의 노란 부분에서 알 수 있듯 피해자 장치에 해킹 케이블이 연결되면 별도의 Hot-spot이 작동된다. 공격자는 Hot-spot에 연결하면 키로깅 기능과 페이로드 전송이 가능한 192.168.4.1이라는 <그림 4>와 같은 공격자용 URL에 접속하게 된다.

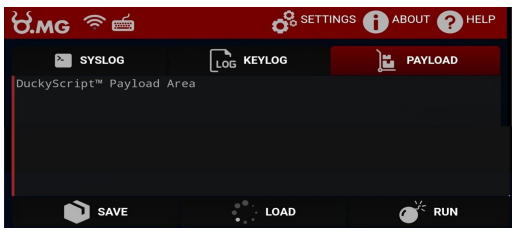

Fig. 5. Attackers Page (192.168.4.1)

공격은 매우 간단하다. 공격자는 해당 WiFi 접속을 통해 <그림 5>의 빨간 부분에서와 같이 홈페이지로 이동한 다음 페이로드를 전송하는 공격을 진행하는 방식이다. 해당 웹에 접속하면 키로깅 부분과 페이로드 전송 부분으로 나뉘는데 <그림 5>의 상단에 위치한 키로그 부분에 접속

하면, 피해자의 키보드와 연결되어 입력 발생 시 입력 값을 확인할 수 있다. 공격자가 <그림 5>의 페이로드 부분으로 들어가게 되면 페이로드를 입력할 수 있는 텍스트 영역이 나타난다. 즉, 이 텍스트 영역이 앞서 설명한 Ducky Script를 입력하는 곳이다. 해당 영역에 악성 스크립트를 작성하여 전송하면 해킹 케이블에 연결된 장치로 전송된다. 피해자 장치에서는 페이로드를 받게 되면 스크립트에 해당하는 내용이 실행된다.

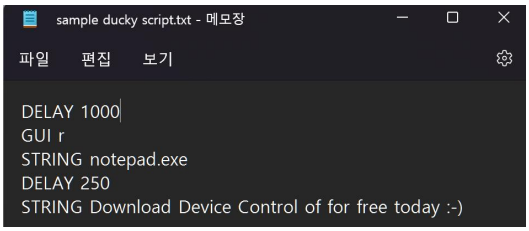

Fig. 6. Example of DuckyScript
(Enter a specific string after running Notepad)

<그림 6>은 다음과 같은 공격을 피해자 PC에서 수행한다. 우선 첫 줄은 1000ms 동안, 즉 1초를 기다리고 윈도우와 함께 'r'을 누르라는 의미인 다음 문장을 실행시킨다. 이를 통해 실행 창이 나오면 메모장을 입력하고 엔터를 누르고, 이후 창이 뜨는 것을 기다리기 위해 대기시간을 잠깐 넣고 문자열을 입력 후 엔터를 입력한다. 이와 같은 기능을 응용하면 피해자의 기기를 특정 악성 웹사이트에 강제로 접속하게 하는 등의 공격 또한 가능하다. 해커의 공격은 장치는 컴퓨터가 키보드를 신뢰한다는 전제로 작동하게 되는데 컴퓨터는 기본적으로 내려받은 실행 파일을 신뢰하지 않아서 소스의 의도를 확인하기 위해 스캔을 실행한다. 실행 파일이 알 수 없는 개발자의 것이거나 잘못된 의도를 나타내는 경우 컴퓨터에서 실행을 차단한다. 하지만 표준 사용자가 명령 프롬프트를 열고 명령을 입력하면 컴퓨터는 의도를 판단하지 않고 맹목적으로 실행한다. 공격자는 피해자의 장치에 가상의 키보드를 생성하여 시스템이 입력값을 실제 사용자가 입력하는 것으로 인식하도록 만들고 장치는 대상 시스템에 연결되면 수행할 작업을 알려주는 스크립트 언어를 사용한다. 이러한 장치 대부분은 상당히 간단한 스크립트를 사용하지만, 일부 장치는 JavaScript와 같은 더 복잡한 프로그램과도 호환이 된다.

IV. Experiments and countermeasures

1. Detection Tools

악성 페이로드 전송은 악성 칩에서 AP로 전송하기에 공격자 PC에서 WiFi를 통해 피해자 PC로 들어오거나 나가는 페이로드를 분석을 위해 네트워크 분석에 쉬운 오픈소스 프로그램인 와이어샤크를 이용했다. 피해자 PC에서 악성 페이로드를 받았을 때 일어나는 내부 일을 살펴보기 위해 실시간 파일 시스템, 레지스트리 및 프로세스 작업 등을 모두 볼 수 있는 윈도우용 고급 모니터링 도구 "Process Monitor"를 이용하여 악성 스크립트의 특징을 분석했다.

1.1 Wireshark

본 논문에서는 탐지 시도를 확인하기 위해 와이어샤크를 이용해 <그림 7>과 같이 공격자 PC의 패킷과 <그림 8>의 피해자 컴퓨터의 통신 패킷을 캡쳐 했다.

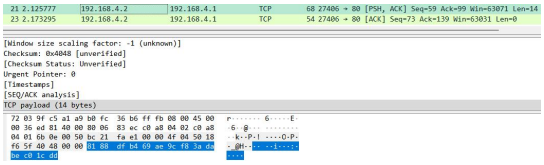

Fig. 7. Attacker PC Packets

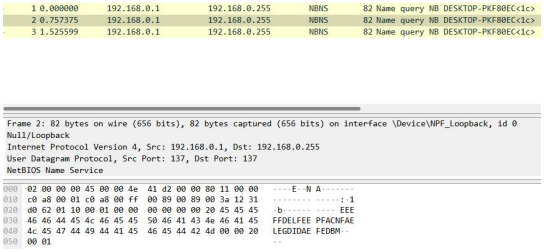

Fig. 8. Victim PC Packets

공격 시도는 192.168.4.2 는 일반적으로 휴대폰, 데스크탑, 랩톱, TV, 스마트 스피커 및 기타 장치에 할당되는 인트라넷 IP 주소다. 인트라넷에는 일반적으로 외부 게이트웨이로 사용되는 다른 IP 192.168.4.1 이 있을 수 있다.

공격자 PC에서는 <그림 7>과 같이 192.168.4.1에 접속한 웹에서 피해자에게 페이로드를 전송할 때의 패킷 상태이다. <그림 7>의 패킷을 보면 공격자 IP에서 시작하는 것이 아닌 192.168.4.2 인트라넷 IP 주소에서 출발하여 192.168.4.1 게이트웨이 주소로 이동한다. 공격자 IP에서 직접 움직이는 것이 아니라 접속해 있는 웹 192.168.4.2에서 게이트웨이가 피해자까지의 경로를 지정해서 보낸다는

것을 알 수 있다. 피해자 PC에서는 <그림 8>과 같이 악성 페이로드가 담긴 패킷이 오는 것을 확인할 수 없다. 피해자 PC의 패킷 프로토콜인 NBNS는 NetBIOS 네임 서버 프로토콜(NBNS 프로토콜), NBT(NetBIOS over TCP/IP)계열의 일부로 윈도우 시스템에서는 WINS(Windows Internet Name Service)로 구현되어 있다. 설계상으로는 NBNS는 네트워크에 연결된 다른 컴퓨터들 상호 간의 이름이 충돌되지 않도록 도와주는 역할을 하고 있으므로 네트워크 패킷으로 해킹 케이블의 악성 행위를 판단할 수 없다. 이러한 예상 원인으로는 해킹 케이블이 사용하는 패킷이 일반적인 네트워크 트래픽과 다를 경우, 예를 들어 사용하는 프로토콜, 포트, 프로토콜 버전 등이 다르다면, 패킷 필터링 규칙에 따라 무시되는 경우나 패킷의 양이 너무 적거나 무작위성이 높기 때문이다.

1.2 Process Monitor

<그림 9>은 공격이 들어오는 약 3초간의 로그를 캡처한 것이다. 3초 동안에 10만 개에 달하는 로그가 기록되었다. 하지만 그 어느 로그에서도 페이로드가 실행되는 것으로 보이는 로그가 남지 않았다. 케이블에 내장된 악성 칩에 자체 프로세서가 있기에 연결된 호스트 컴퓨터에서는 프로세스가 표시되지 않는다.

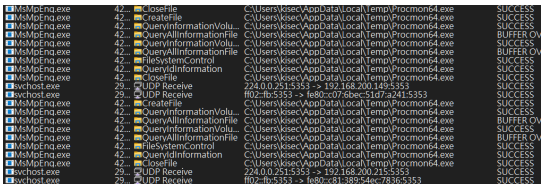

Fig. 9. Victim PC Log

이는 해킹 케이블이 하드웨어 또는 펌웨어를 수정하는 방식으로 작동하기 때문에 시스템 내의 프로세스와 파일 활동을 모니터링하는 프로세스 모니터와 같은 운영체제 수준의 도구로는 탐지가 어렵다.

2. Countermeasures of Hacking cable

2.1 Port Blocker

포트 차단기는 사용자가 모르는 사이에 악성 페이로드를 포함한 승인되지 않은 장치가 연결되는 것을 막는 도구이다. BadUSB(해킹 케이블) 경우 공격자가 포트 차단기가 설치된 장치를 표적으로 삼을 가능성이 작다는 장점이 있다. 포트 차단기는 민감한 파일이 포함된 네트워크의 중요한 시스템에 설치할 수 있으며 설치 후 장치를 잠금 해제하고 잠그는 특수 키와 함께 제공된다. 예를 들어 포트가 보이지 않는 네트워크의 데스크톱 컴퓨터에 포트 차단기를 설치할 수 있다. 그러나 포트 차단기의 경우 모니터링이 제대로 되지 않으면 공격자가 몇 가지 기본 도구만으로 대상 시스템에서 포트 차단기를 쉽게 제거할 수 있다는 단점이 있다[7].

해킹에서 대표적인 포트 차단기로는 Microsoft의 주변 장치 감사를 수행하는 Intune Endpoint Protection 기능이 있으며 이는 특정 공급업체의 장치, 모델 번호 또는 연결할 특정 일련번호의 장치 클래스만 허용한다. 이를 통해 대부분의 공격을 막을 수 있지만, 알려진 장비 번호를 수집할 수 있다면 유효한 장치로 가장하고 공격할 수 있다. 따라서 케이블의 일련번호, 데이터 속도, 전력 소비량 및 요청된 역할도 식별할 수 있는 OS의 최신 USB 장치 진단 기능을 구글 크롬에서 개발 중이지만 아직은 12세대 Intel 이상에만 해당 기능을 사용할 수 있다. 모바일의 경우 사용자가 암호를 사용하여 주변 장치를 명시적으로 신뢰하지 않는 한 충전 이외에는 USB를 비활성화하는 기능이 있다. 대상의 암호를 알고 있더라도 HID 주입을 사용하여 포트의 잠금을 해제할 수 없으며 코드를 입력하거나 기존 신뢰할 수 있는 주변 장치를 사용하려면 HID 주입을 물리적으로 터치해야 한다. 기업의 경우 주요 업무용 핸드폰에는 악성 케이블 검출기를 제공해야 한다. PC USB 포트를 막아놓듯이 장치가 데이터를 사용하려고 하는지, 연결된 것이 없을 때 전력을 끌어당기는지 등을 확인하는 필터 장치의 설치가 필요하다.

2.2 Monitor typing speed

악성 스크립트를 가진 페이로드가 도착하면 피해자 PC에서는 최대 650.000번의 키 입력 속도로 빠르게 입력하는 스크립트가 실행된다. 타이핑 속도 모니터링은 이러한 특징을 이용하여 초당 기준값을 넘는 키 입력을 차단하는 방법으로 DuckHunter와 같은 특정 프로그램은 백그라운드에서 실행 중일 때 타이핑 속도를 주시하여 사람이 입력할 수 없는 속도의 입력 공격이 감지되면 키보드 입력을 차단한다[8]. 이 예방 방법을 사용할 때의 단점은 이러한 프로그램이 공격을 탐지하는 데 몇 밀리초(ms)가 걸리기에 페이로드의 길이가 짧으면 프로그램으로 의해 차단되기 전에 대상 컴퓨터로 들어갈 수 있다는 점이다. 또한, 일반 사용자가 정상적인 프로그램을 실행할 때도 명령 프롬프트가 열리며 각종 정상 스크립트를 자동 입력하는 때도 있기에 제약이 있다.

2.3 Restrict access to elevated command prompts

중요한 공격을 하기 위해서는 관리자 권한이 필요한 경우가 많다. 그래서 공격자는 Window에서는 먼저 실행 명령에 "CMD"를 입력한 다음 Ctrl+Shift+Enter↵를 이용해 상승된 명령 프롬프트에 액세스하는 방식을 자주 사용하는데, 이 방법은 이를 예방하고자 CMD를 관리자로 실행하기 위해서는 암호를 설정해두는 것이다. 그렇게 된다면 트랙에서 죽은 관리 권한을 찾도록 프로그래밍된 모든 Keystroke Injection이 중지되고, 이와 유사한 방법으로 윈도우에서 바로 가기 키(key)를 제한하는 것이 있다. 잠금 화면 바로 가기 키는 (Win + L)이므로 레지스트리에서 이를 비활성화한다면 Keystroke Injection을 예방할 수 있다[9].

2.4 Firmware lock and TMSUI

해킹 케이블이 공격 코드를 저장하기 위해서는 펌웨어를 조작한다. 그렇기에 하드웨어적인 방법으로 펌웨어가 수정되는 것을 막으면 이러한 공격을 예방할 수 있다. 하지만 펌웨어 기능을 추가하거나 오류 정정하지 못하는 단점이 발생한다[10].

TMSUI(Trust Management Scheme for USB Interfaces)라는 신뢰 관리 체계가 제안되었다. TMSUI는 특정 보호된 단말기에서만 특정 시간 동안 USB 저장 장치의 연결을 허용하여 ICS(Industry Control System)를 보호한다[11].

2.5 Disable Finder function in mobile

대부분의 공격은 모바일에서 파인더를 통해서 이루어진다. 그렇기에 사용자는 파인더 기능을 사용하지 않을 시 각 버전에 맞는 방법으로 기능을 비활성화하며 기기를 보호한다. 혹은 인터넷과 같은 공격 가능성이 큰 앱들을 미리 검색목록에서 제외 설정을 해 놓을 수 있다.

V. Conclusion

본 연구에서 해킹 케이블의 작동 원리 및 공격과 방어 기법에 대해 분석했다. 이에 대한 대응 방안을 모색하기 위해 악성 스크립트 차단을 목적으로 하는 스크립트 블랙리스트를 작성하려고 하였으나 분석한 도구 Wireshark, Process Monitor에서는 악성 스크립트의 특징을 찾을 수 없었다. 그러나 본 논문에서 알아본 대응 방안을 통해 악성 스크립트의 특징을 발견할수 있으나 사전에 대비한 해킹 케이블의 특성은 불가능했거나 타이핑 속도 모니터링은 악성 스크립트만을 차단하는 것이 아닌 정상적인 프로그램마저 차단하여 정상적으로 시스템을 운영하지 못할 가능성이 있어 완벽한 차단은 어려울 것이다. 따라서 현재로서는 해킹 케이블에 대한 완전한 대응방안을 찾기는 어렵기 때문에 공용으로 사용되는 케이블의 사용을 보다 주의해야 할것으로 판단된다. 본 연구를 기반으로 향후 연구 방향으로는 해킹 케이블의 물리적/논리적 특성을 고려한 대응방안을 고려하는 것이 필요하다. 공공장소 및 개인 소유의 케이블 사용 시 항상 의심하고 사용을 지양하는 것을 권장하며, 사업체도 정상적으로 공용 케이블을 갖춘 곳이라도 케이블 교체 여부를 수시로 확인하거나, 잠금장치를 설치하여 타 케이블이 설치되지 않게 하는 등의 대비를 강화해야 한다. 기존 탐지 도구 이외에도 악성 스크립트를 탐지하기 위한 새로운 기술 및 도구를 개발하여 스크립트 블랙 리스트를 더욱 효과적으로 작성할수 있는 방법의 연구가 필요하다.

REFERENCES

[1] GallupReport, 2012-2022 Smartphone Usage & Brand, Smartwatch, Wireless Earphone Survey on Wireless Earphones, https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1309

[2] H. Lee, “Is there a safe zone?” 8 ways for Smartphone hacking, https://www.ciokorea.com/t/21989/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4/213594.

[3] Hak5, O.MG CABLE, https://shop.hak5.org/products/omg-cable

[4] S. Vouteva “Feasibility and Deployment of Bad USB”, System and Network Engineering Master Research project, February 2015. https://rp.os3.nl/2014-2015/p49/report.pdf

[5] J. Jo, H. Yang, and B. Lee, “Implementation of screen key-logger for virtual keyboard and its countermeasures”, Journal of the Society for Information Protection, June 2013.

[6] J. Choi, “Countermeasures for badusb vulnerability”, Journal of the Korea Institute of Information Security and Cryptology, 25, 3, pp. 559-565, June 2015. DOI: 10.13089/JKIISC.2015.25.3.559

[7] Manage Engine, What is BadUSB Attack and How to Prevent, https://www.manageengine.com/device-control/badusb.html

[8] B. Choi, and T. Suh “A Security Program To Protect against Keyboard-Emulating BadUSB”, Journal of The Korea Institute of Information Security & Cryptology, 26, 5, pp. 1487, December 2016. ISSN 1598-3986(Print)/ISSN 2288-2715(Online). DOI: 10.13089/JKIISC.2016.26.6.1483

[9] A. Kishore, Prevent Access to the Command Prompt in Windows, https://helpdeskgeek.com/how-to/disable-command-prompt-in-win

dows/, April 2011.

[10] S. Nam, I. Oh, K. Lee, and K. Yim, “Study on BAD USB Detection Technique based on User Cognition”, Proceedings of the Korean Society of Computer Information Conference, 24, 2, pp. 93-94, July 2016. https://koreascience.kr/article/CFKO201623070249541.page

[11] S. Neuner, A. G. Voyiatzis, S. Fotopoulos, C. Mulliner, E. R. Weippl, “USBlock: Blocking USB-Based Keypress Injection Attacks”, Data and Applications Security and Privacy XXXII, pp. 278-295, July 2018. DOI: 10.1007/978-3-319-95729-6_18

Authors

Hea-Jun Kim received the A.S. and B.S. degrees in Computer Network Engineering and Information Security. In 2020, he obtained a professional bachelor's degree from the National Lifelong Education Institute, and in 2023, he received his bachelor's degree from Daejeon University. Hea-Jun Kim received his bachelor's degree from Daejeon University in 2023. In 2020, he also obtained a professional bachelor's degree from the National Lifelong Education Institute. He is interested in web development, web security, and mobile technology.

Young-Bok Cho earned her Master's and Ph.D. degrees in Electronic and Computer Engineering from Chungbuk National University in 2005 and 2012, respectively. She has since held positions as a visiting professor at the university and earned Ph.D. degrees in Medicine and Law from other institutions. She is currently an Assistant Professor of Information Security at Daejeon University. Professor Young-Bok Cho, a full member, received her Master's degree in Electronic and Computer Engineering from Chungbuk National University in 2005, and her Ph.D. in the same field from the same university in 2012. She was a visiting professor in the Department of Software at Chungbuk National University from 2012 to 2018. In 2019, she earned a Ph.D. in Medicine from Chungbuk National University, and completed her Ph.D. in Law from Chungnam National University in 2020. Since 2018, she has been serving as an Assistant Professor in the Department of Information Security at Daejeon University, Korea. Her research interests include medical image processing, information security, medical information protection, mobile security.