NÉGY APRÓ KIBERFEGYVER

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

nki.gov.hu

1. FLIPPER ZERO

Ezt a kis kütyüt rengetegen ismerhetik, hiszen hatalmas port kavart, amikor **2020-ban 4,8 millió dolláros támogatást kapott** Kickstarteren.

Az alaprendszer lehetőségei pedig tovább bővíthetők, hiszen a **GPIO** porton keresztül többféle kiegészítő, például **Wi-Fi** vagy **GPS** modul is csatlakoztatható hozzá.

KÉPESSÉGEI

RFID és NFC

125 kHz-es RFID-modulja és 13,56 MHz-es NFC-chipje lehetővé teszi különféle beléptetőkártyák, szállodai ajtók, valamint tömegközlekedési kártyák adatainak kiolvasását, és bizonyos esetekben azok klónozását vagy visszajátszását is.

INFRAVÖRÖS FUNKCIÓK

Képes a legtöbb szabványos infravörös távirányító jelének felismerésére, tárolására és visszajátszására. Támogatja a gyakori protokollokat (pl. NEC, Sony), és 38 kHz-es vivőfrekvencián működik, így alkalmas tévék, projektorok, klímák vezérlésére vagy IR-kommunikációk tesztelésére.

KÉPESSÉGEI

USB HID-emuláció

USB-n keresztül billentyűzetként vagy egérként azonosítja magát, és képes előre beprogramozott parancsokat végrehajtani – például fájlokat küld, URL-eket nyit meg, vagy rendszerszintű műveleteket indít el felhasználói jogosultsággal.

Bluetooth Low Energy (BLE)

Bővítőmodul használatával képes BLE-eszközök felderítésére, és megjeleníti azok alapadatait, például a MAC-címet, az eszköz nevét és a jelerősséget (RSSI).

2. RUBBER DUCKY

Ez az eszköz tökéletes példája annak, miért nem szabad ismeretlen forrásból származó USB-meghajtót számítógéphez csatlakoztatni.

A látszat ellenére ugyanis **nem egy egyszerű pendrive**, hanem egy **programozható HID-eszköz,** amely automatikusan parancsokat hajt végre a rendszerben.

KÉPESSÉGEI

Képes **adatokat gyűjt**eni, **automatizált támadásokat indí**tani, **kártevőt telepít**eni a csatlakoztatott számítógépre, vagy akár **teljes hozzáférést szerez**ni a rendszerhez.
Mindezt úgy valósítja meg, hogy USB-n keresztül **billentyűzetként (HID-eszközként) azonosítja magát** – a legtöbb modern operációs rendszer pedig az ilyen eszközöket automatikusan megbízható bemeneti perifériaként kezeli.

Ez a bizalom könnyen kihasználható:
a Ducky **előre beprogramozott karakterleütéseket emulál**, mintha a felhasználó maga gépelné be azokat.
Így akadálytalanul képes például PowerShell- vagy CMD-parancsokat futtatni, amelyekkel gyakorlatilag bármilyen művelet végrehajtható a célgépen.

3. WIFI PINEAPPLE

A WiFi Pineapple egy speciálisan **penetrációs tesztekhez és oktatási célokra fejlesztett eszköz**, amelyet gyakran használnak a **vezeték nélküli hálózatok biztonsági gyengeségeinek vizsgálatára**.

Ugyanakkor megfelelő ismeretek birtokában támadási célokra is alkalmazható, különösen a nyilvános vagy kevésbé védett hálózatok esetében.

KÉPESSÉGEI

Képes azonosítani a közeli Wi-Fi eszközök által keresett hálózatokat, majd ezek nevében **hamis hozzáférési pontokat (hotspotokat) hoz létre**. Ennek hatására a felhasználók észrevétlenül csatlakoznak a támadó eszközére, abban a hitben, hogy egy ismert és megbízható hálózathoz kapcsolódnak.
A támadó ezáltal **teljes mértékben hozzáférhet az áthaladó adatforgalomhoz**: lehallgathatja, módosíthatja, hamis weboldalakra irányíthatja a felhasználót, illetve érzékeny adatokat gyűjthet.

Fejlettebb támadások során akár azt is **elhitetheti a felhasználóval, hogy biztonságos, titkosított HTTPS kapcsolatot használ**, miközben valójában titkosítatlan HTTP protokollon keresztül zajlik a kommunikáció. Ez a technika **SSL stripping** néven ismert, és különösen veszélyes, mivel a felhasználó sokszor nem is észleli, hogy a kapcsolat nem biztonságos.

4. O.MG CABLE

Ahogy korábban már említettük, nem ajánlott ismeretlen forrásból származó USB-meghajtót csatlakoztatni az eszközeinkhez.
De mi a helyzet a töltőkábelekkel?

Az O.MG Cable megmutatta, hogy még a kölcsönkapott vagy „talált” **USB-kábelek sem feltétlenül ártalmatlanok**.
A hétköznapi töltőkábelnek álcázott eszköz valójában **rejtett elektronikát tartalmaz**, amely képes adatátvitelre, billentyűleütések emulálására vagy akár vezeték nélküli (pl. Wi-Fi) vezérlésre is.

KÉPESSÉGEI

Az O.MG Cable a Rubber Ducky-hoz hasonlóan **billentyűzetként (HID-eszközként) azonosítja magát**, és **előre programozott szkriptek** futtatására képes billentyűleütések emulálásával.

További sajátossága, hogy Wi-Fi-kapcsolaton keresztül kommunikálhat a támadóval, aki így távolról is **parancsokat küldhet**, **kártevőt telepíthet**, **adatokat szivárogtathat**, vagy akár **teljes hozzáférést szerezhet** a célrendszerhez – mindezt egy első ránézésre ártalmatlan töltőkábel segítségével.