# Výzkum a nové technologie v kybernetické a informační bezpečnosti

## "Air-Fi" útok pomocí Wi-Fi přenosu

(23. 12. 2020; portswigger.net, arxiv.org) Mordechai Guri – výzkumník z University of Negev v Izraeli představil způsob jak zkompromitovat počítače, které jsou součástí fyzicky izolovaných sítí (nejsou připojeny k internetu ani k jiným volně přístupným nebo napadnutelným sítím - tzv. *Air-gapping*). A to za pomocí Wi-Fi přijímače. V počátku představené metody útoku je třeba cílový počítač infikovat specifickým malwarem (např. skrze útok přes dodavatelský řetězec nebo pomocí fyzického přístupu k síti…). Cílové zařízení navíc nemusí mít pro tento typ útoku ani žádný prostředek k připojení nebo vysílání Wi-Fi signálu. Malware poté v infikovaném počítači využívá elektromagnetické záření generované operační pamětí (DDR SDRAM), které spadá do frekvencí využívaných Wi-Fi sítěmi. Jakýkoliv Wi-Fi přijímač poté může přijímat data z infikovaného počítače. Rychlost přenosu je však velmi malá (1-100 bitů za sekundu) a tato metoda útoku se tak nejspíše ujme pro přenos dat jako jsou přihlašovací údaje, malé soubory nebo biometrická data.

**Komentář:** Představená metoda útoku má spíše demonstrativní charakter, že je něco podobného možné. Vzhledem k malým přenosovým rychlostem se však nejspíše příliš neujme. Navíc vyžaduje i relativně blízkou fyzickou přítomnost Wi-Fi přijímače k infikovanému zařízení.

## Nový web dedikovaný zveřejňování bezpečnostních zranitelností malwaru

(14. 01. 2021, portswigger.net, Malvuln.com) Dne 2. ledna 2021 byly uvedeny v provoz webové stránky Malvuln.com, které se zaměřují výlučně na sdílení a výzkum zranitelností v samotném malwaru. Jejich tvůrce John Page uvedl, že jejich hlavní přínos vidí v tom, že mohou pomoci *incident response* týmům v bezpečném odstraňování malwaru z infikovaných zařízení. Autor dokonce poté spekuluje, že by podobná data mohla být v budoucnu využita k tvorbě „dobrého" malwaru, který využívá zveřejněné zranitelnosti a útočí na „špatný" malware.

**Komentář:** Podobné projekty se ve své podstatě snaží o „dobrou variantu" různých stránek na kterých jsou k dostání informace o zranitelnostech v legitimním softwaru. Znalost zranitelností malwaru navíc může být využita nejen k jeho odstranění ale také případně i k vyhledání toho, kdo je jeho tvůrcem. Přestože je jejich užitečnost nezpochybnitelná tak mohou mít i nežádoucí efekt. Především ve formě, že tvůrci malwaru mohou na podobných webech nalézt informace o zranitelnostech ve svém malwaru, kterých si nebyli vědomi a opravit je nebo se jim vyhnout do budoucna při tvorbě malwaru nového.

PETR MARTINEK; p.martinek@nukib.cz

Oddělení výzkumu a evropské spolupráce, NÚKIB