BINÁRNE

Profesionáli zo spoločnosti Binary House sú pripravení Vám pomôcť v analyzovaní škodlivého kódu, binárneho/spustiteľného súboru pomocou reverzného inžinierstva, alebo napísaním PoC/exploitu.

ANALÝZA ŠKODLIVÉHO KÓDU

V prípade, že Vaša organizácia bola napadnutá škodlivým kódom, táto služba Vám pomôže získať detailné informácie o jeho funkcionalite a risku, ktorý pre Vašu organizáciu predstavuje. Typický škodlivý kód sa nachádza v rôznych skriptoch, mobilných aplikáciách, dokumentoch alebo v spustiteľných súboroch.

Výstupom je detailný report s výsledkami analýzy a zoznam odporúčaní ako reagovať na podobný typ útoku.

REVERZNÉ INŽINIERSTVO

Reverzné inžinierstvo (RE) je proces získavania informácií z dodaných súborov. Táto služba Vám pomôže najmä v nasledujúcich prípadoch:

- Pochopenie proprietárneho sieťového protokolu a súborových formátov
- Identifikácia zmien v systéme alebo aplikácií vykonaných aplikovaním záplaty
- Rekonštrukcia časti funkcionality spustiteľného súboru z dôvodu strateného zdrojového kódu.

Počas projektu používame statickú a dynamickú analýzu na získanie informácií o funkcionalite programu alebo jeho časti. Rozumieme architektúram:

- x86
- x86-64
- ARM
- ARM64
- MIPS

Po skončení analýzy obdržíte detailný report s požadovanými informáciami.

VÝVOJ EXPLOITOV

Pri penetračných testoch alebo aj pri overovaní či zraniteľnosť bola opravená je z času na čas nevyhnutné použiť exploit alebo "proof of concept" (PoC). Exploity/PoC zvyčajne nie sú verejne dostupné a preto ich vieme vyvinúť pre potreby zákazníka.