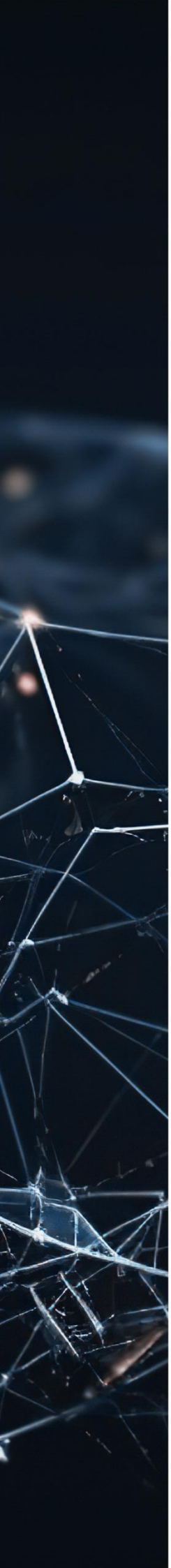

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie o službe

ANALÝZA ŠKODLIVÉHO KÓDU

od **VJ CSIRT**

oAKH

Oddelenie analýzy kybernetických hrozieb

Charakteristika služby

Analýza škodlivého kódu predstavuje špecializovanú činnosť zameranú na detailné preskúmanie spustiteľných súborov, skriptov alebo iných digitálnych objektov, pri ktorých existuje podozrenie na škodlivé správanie. Hlavným cieľom služby je zistiť, aké aktivity analyzovaný kód vykonáva, akým spôsobom môže ovplyvniť napadnutý systém a aké riziká predstavuje pre organizáciu. Výsledkom analýzy je lepšie pochopenie fungovania hrozby a získanie technických poznatkov potrebných na jej identifikáciu, detekciu a elimináciu.

Služba je určená najmä na skúmanie vzoriek zachytených počas riešenia bezpečnostných incidentov, pri preverovaní podozrivých súborov alebo pri overovaní bezpečnostných upozornení generovaných ochrannými technológiami. V prípade potreby môže byť využitá aj na podporu ďalších činností v oblasti kybernetickej bezpečnosti, threat hunting alebo tvorbu detekčných pravidiel.

Kedy službu využiť

Potreba analýzy škodlivého kódu vzniká najmä v situáciách, keď organizácia identifikuje neznámy alebo podozrivý súbor a potrebuje určiť jeho charakter. Typickým príkladom sú podozrivé e-mailové prílohy, súbory stiahnuté z nedôveryhodných zdrojov, neznáme procesy spustené v systéme alebo objekty zachytené bezpečnostnými riešeniami bez jednoznačnej klasifikácie. Služba nachádza uplatnenie aj pri vyšetrovaní ransomvérových útokov, kompromitácie pracovných staníc alebo serverov, podozrenia na vzdialené ovládanie zariadení útočníkom či pri preverovaní nových hrozieb, pre ktoré ešte nie sú dostupné dostatočné informácie z verejných zdrojov.

Priebeh analýzy škodlivého kódu a súčinnosť organizácie

Proces analýzy začína prevzatím vzorky a jej bezpečným spracovaním v izolovanom prostredí určenom na skúmanie potenciálne nebezpečného obsahu. Následne sa vykonávajú technické činnosti zamerané na identifikáciu štruktúry kódu, použitých technológií a funkcionalít vzorky. Podľa typu a komplexity vzorky sa zvolia vhodné analytické postupy.

Pri statickej analýze sa analyzuje samotný kód vzorky. Pri dynamickej analýze sa tento kód kontrolovane spúšťa pomocou softvéru, ktorý umožňuje podrobnú inšpekciu a prípadnú modifikáciu artefaktov počas behu vzorky.

Počas skúmania prostredníctvom behaviorálnej analýzy sa vyhodnocujú zmeny vykonávané v operačnom systéme, vytvárané alebo modifikované súbory, komunikácia so sieťou, využívané systémové prostriedky a ďalšie aktivity, ktoré môžu naznačovať škodlivý zámer. Pri komplexnejších vzorkách môže byť potrebné vykonať aj hlbšiu analýzu jednotlivých komponentov alebo dekompiláciu a reverzné inžinierstvo.

Pre dosiahnutie čo najpresnejších výsledkov je vhodné, aby organizácia poskytla dostupné informácie o okolnostiach zachytenia vzorky, identifikovaných príznakoch kompromitácie a súvisiacich technických údajoch. Tieto informácie umožňujú lepšie zasadiť zistenia do kontextu konkrétneho incidentu.

Predmet analýzy

Predmetom skúmania môžu byť spustiteľné súbory, skripty, dokumenty obsahujúce aktívny obsah, archívy, odkazy na webové stránky alebo iné digitálne objekty, pri ktorých existuje podozrenie na škodlivú funkcionalitu. Analýza nie je obmedzená na konkrétny operačný systém alebo platformu a môže zahŕňať operačné systémy Windows či Unix-like systémy.

V závislosti od povahy prípadu môžu byť skúmané aj súvisiace artefakty, ako napríklad sieťová komunikácia, konfiguračné súbory, komponenty využívané na komunikáciu s riadiacou infraštruktúrou útočníka alebo ďalšie objekty potrebné na pochopenie fungovania analyzovanej hrozby.

Výstupy

Kľúčovým výsledkom analýzy sú identifikované indikátory kompromitácie (Indicators of Compromise – IoC), ktoré predstavujú prakticky využiteľné technické artefakty slúžiace na detekciu, monitorovanie a elimináciu danej hrozby v prostredí organizácie.

Ďalším výsledkom služby je odborná technická správa sumarizujúca zistenia získané počas analýzy. Dokument obsahuje opis správania analyzovaného kódu, identifikované funkcionality, potenciálne bezpečnostné riziká a technické charakteristiky dôležité pre pochopenie jeho činnosti. Správa môže obsahovať aj odporúčania na blokovanie hrozby, odstránenie jej následkov a zvýšenie úrovne ochrany dotknutých systémov.

Obmedzenia

Možnosti analýzy sú ovplyvnené viacerými faktormi, predovšetkým kvalitou a úplnosťou poskytnutej vzorky (napr. pri viacstážovom alebo viacprvkovom malvéri). Niektoré moderné hrozby využívajú techniky, ktoré komplikujú alebo znemožňujú úplné odhalenie ich funkcionality. Ide napríklad o silnú obfuskáciu, šifrovanie, viacvrstvové mechanizmy ochrany alebo použitie softvéru na ochranu kódu proti reverznému inžinierstvu.

Prínosy služby

Analýza škodlivého kódu umožňuje organizácii získať detailný pohľad na povahu identifikovanej hrozby a pochopiť jej potenciálny vplyv na informačné systémy. Získané poznatky podporujú efektívnejšie riešenie bezpečnostných incidentov, zlepšujú schopnosť detegovať podobné útoky a poskytujú podklady pre prijímanie primeraných bezpečnostných opatrení.

Dlhodobým prínosom je rozširovanie znalostí o aktuálnych hrozbách, zvyšovanie pripravenosti organizácie na budúce incidenty a posilňovanie celkovej úrovne kybernetickej bezpečnosti.