Esport – Cvičení číslo 1

V rámci tohoto cvičení budete pracovat s herními cracky a cheaty, abyste pochopili jejich fungování a bezpečnostní rizika spojená s jejich používáním. Postupujte podle následujících kroků:

1. **Vyhledání herního cracku:** najděte a stáhněte alespoň jeden herní crack pro libovolnou počítačovou hru.
2. **Vyhledání herního cheatu:** najděte a stáhněte alespoň jeden herní cheat pro libovolnou počítačovou hru.
3. **Testování v sandboxu Cuckoo:**
   * Otestujte stažené soubory v sandboxu Cuckoo dostupném na adrese <https://cuckoo.cert.ee/>.
   * Analyzujte chování těchto souborů a identifikujte případné bezpečnostní hrozby.
4. **Diskuse a analýza:**
   * Jak obtížné bylo najít herní crack a cheat?
   * Kde jste tyto soubory našli a jak jsou zmíněné weby či fóra vytížené?
   * Lze zjistit počet uživatelů těchto stránek nebo fór?
   * Jaké bezpečnostní riziko představují tyto soubory pro uživatele?
   * Jaké jsou právní a etické důsledky používání herních cracků a cheatů?

**Poznámka:** Při práci s herními cracky a cheaty buďte obezřetní, protože mohou obsahovat škodlivý software. Používejte výhradně zabezpečené prostředí pro testování a nikdy nespouštějte tyto soubory na svém osobním počítači.

# Crack na hru Ghost Of Tsushima

Jedná se o relativně novou hru. Na PC vyšla v květnu 2024, předtím byla pouze jako Play Station exclusive.

Fitgirl Repack je známá stránka, která nabízí torrenty na většinu her. Tato stránka je obecně považována za „bezpečnou“ protože je velmi známá. Našel jsem jí na redditu v několika vláknech označovanou jako bezpečný zdroj cracků. Občas jsem sám z těchto stránek stahoval a někdy byl virus odhalen už prohlížečem, jindy byl bez virů. Podle všeho však na stránce najdeme pouze repacky jiných cracků, takže tato stránka není původním zdrojem souborů.

Odkaz na stránku s cracky: [Fitgirl Repack](https://fitgirl-repacks.site)

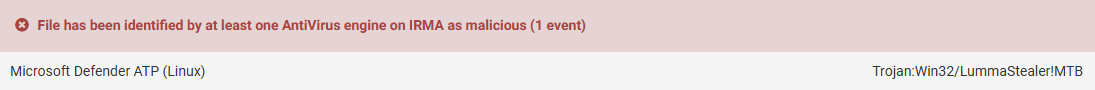
Odkaz na konkrétní file: [File](https://fitgirl-repacks.site/ghost-of-tsushima-directors-cut/)

Cuckoo task ID: [5432709](https://cuckoo.cert.ee/submit/post/5147439)

Obsah obrázku text, elektronika, počítač, snímek obrazovky

Popis byl vytvořen automaticky

Obsah obrázku text, Písmo, číslo, snímek obrazovky

Popis byl vytvořen automaticky 

LummaStealer je malware kategorie „stealer,“ který se zaměřuje na krádež osobních dat, například přihlašovacích údajů, platebních informací, historii prohlížení nebo cookies z napadeného zařízení. Detekce signalizuje, že analyzovaný .exe soubor je považován za potenciálně nebezpečný trojský kůň, který může tyto informace sbírat. Obsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automaticky

**network\_tcp\_listen, network\_tcp\_socket**

Tato pravidla naznačují, že soubor obsahuje kód pro naslouchání na síťových připojeních a komunikaci přes TCP sockety. Tento druh funkcionality je typický pro backdoory nebo malware, který čeká na příkazy z vnějšího zdroje.

**Neznámé názvy PE sekcí a PE resource name** (jako \_RDATA a AFX\_DIALOG\_LAYOUT): Neobvyklé názvy sekcí a zdrojů jsou typické pro soubory, které byly zabaleny nebo zakódovány packery. Tento packer může sloužit k obcházení antivirových detekcí a ztížení analýzy souboru

Celkově tento soubor vykazuje vlastnosti malwaru zaměřeného na krádež dat a obcházení bezpečnostních opatření. Kombinace anti-debug a anti-sandbox kontrol, spolu s možností síťové komunikace, naznačuje, že tento crack/cheat není pouze neškodným nástrojem, ale potenciálně závažným bezpečnostním rizikem pro uživatele, kteří by jej spustili