

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 ji 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](#)

Odkaz na konkrétní file: [File](#)

Cuckoo task ID: [5432709](#)

The screenshot shows the FitGirl Repacks website. The main content is a download page for "GHOST OF TSUSHIMA DIRECTOR'S CUT, V1053.0.0515.2048 + DLC + BONUS CONTENT + MULTIPLAYER". It includes a thumbnail image of the game, download links for direct links and torrent mirrors, and a sidebar with popular repacks of the week.

FitGirl Repacks

The ONLY official site for FitGirl Repacks. Every single FG repack installer has a link inside, which leads here. Do not fall for fake and scam sites, which are using my name.

POPULAR REPACKS ▾ ALL MY REPACKS, A-Z ▾ UPDATES LIST ▾ FAQ DONATE CONTACTS REPACKS TROUBLESHOOTING

LOSSLESS REPACK

GHOST OF TSUSHIMA DIRECTOR'S CUT, V1053.0.0515.2048 + DLC + BONUS CONTENT + MULTIPLAYER

⌚ 17/05/2024 FITGIRL 13067 COMMENTS

#4424 Ghost of Tsushima DIRECTOR'S CUT v1053.0.0515.2048 + DLC + Bonus Content + Multiplayer

Genres/Tags: Action, Open world, Stealth, Third-person, 3D
Companies: Sucker Punch Productions, Nixxes Software, Sony Interactive Entertainment
Languages: RUS/ENG/MULTI26
Requires Windows 10/11
Original Size: 59.7 GB
Repack Size: from 31.2 GB [Selective Download]

Download Mirrors (Direct Links)

- Filehoster: DataNodes (Speed & Usability) [Use IDM]
+ Click to show direct links
- Filehoster: FuckingFast (REALLY Fucking Fast 😊)
+ Click to show direct links
- Filehoster: MultiUpload (10+ hosters, interchangeable) [Use iDownloader2]
- Filehoster: OneDrive (Uploaded by DyR0t(-_-t), compatible with torrent mirrors)

Download Mirrors (Torrent)

- 1337x [magnet] [torrent file only]

Please support my site

Most Popular Repacks of the Week

Summary

File GhostOfTsushima.exe

Summary	Download Submit sample
Size	27.9MB
Type	PE32+ executable (GUI) x86-64, for MS Windows
MDS	961b94c24aabd717a045d4b9154f7712
SHA1	24157a5bd4c9ae06f10c5660e2c05d2df404b60
SHA256	9fe24cc952e33803afbe63979343c0e3f29314b7a250a519b5e734ae8c5bc036
SHA512	Show SHA512
CRC32	C050F8A1
ssdeep	None
PDB Path	d:\g1\code\bin\ship_steam.pdb
Yara	<ul style="list-style-type: none"> GlassesCode - Glasses code features Glasses - Glasses family ThreadControl_Context - (no description) SEH_vectored - (no description) Check_OutputDebugStringA_iat - (no description) DebuggerCheck_MemoryWorkingSet - Anti-debug process memory working set size check anti_dbg - Checks if being debugged antisb_threatExpert - Anti-Sandbox checks for ThreatExpert network_tcp_listen - Listen for incoming communication network_tcp_socket - Communications over RAW socket

Score

This file shows numerous signs of malicious behavior.

The score of this file is **3.4 out of 10**.

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

File has been identified by at least one AntiVirus engine on IRMA as malicious (1 event)

Microsoft Defender ATP (Linux) Trojan:Win32/LummaStealer!MTB

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.

Signatures			
Yara rules detected for file (10 events)			
description	Glasses code features	rule	GlassesCode
description	Glasses family	rule	Glasses
description	(no description)	rule	ThreadControl_Context
description	(no description)	rule	SEH_vectored
description	(no description)	rule	Check_OutputDebugStringA_iat
description	Anti-debug process memory working set size check	rule	DebuggerCheck_MemoryWorkingSet
description	Checks if being debugged	rule	anti_dbg
description	Anti-Sandbox checks for ThreatExpert	rule	antisb_threatExpert
description	Listen for incoming communication	rule	network_tcp_listen
description	Communications over RAW socket	rule	network_tcp_socket
This executable has a PDB path (1 event)			
pdb_path	d:\g1\code\bin\ship_steam.pdb		
The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)			
section		_RDATA	
The file contains an unknown PE resource name possibly indicative of a packer (1 event)			
resource name		AFX_DIALOG_LAYOUT	

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.

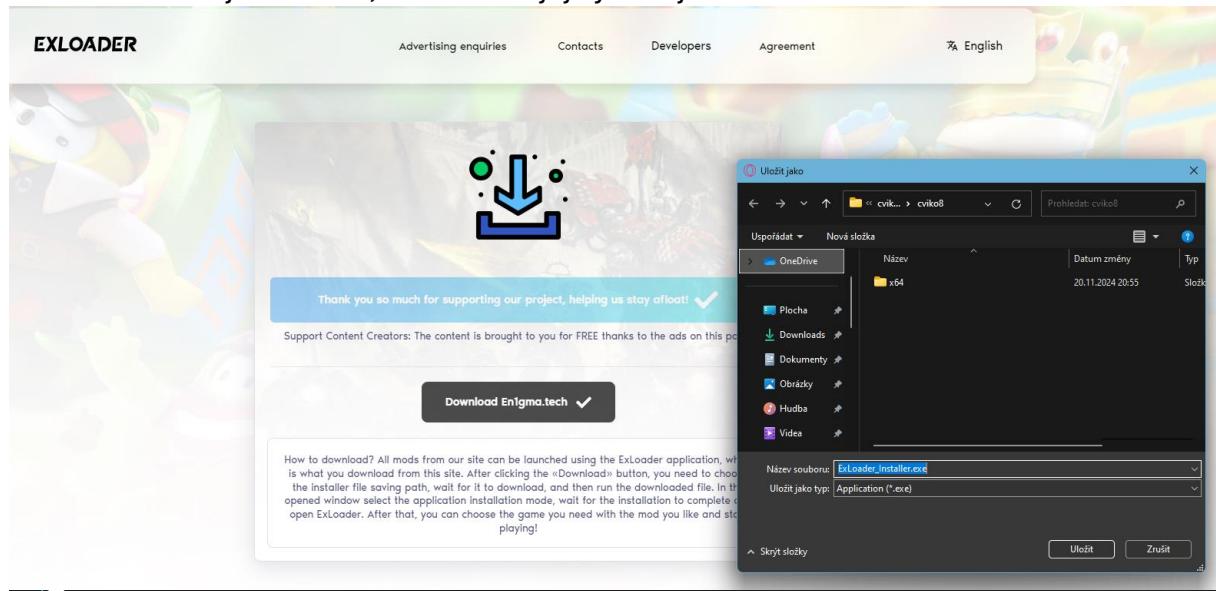
Neznámé názvy PE sekcí a PE resource name (jako _RDATA a AFX_DIALOG_LAYOUT): Neobvyklé názvy sekcí a zdrojů jsou typické pro soubory, které byly zabalené nebo zakódovány packery. Tento packer může sloužit k obcházení antivirových detekcí a ztížení analýzy souboru

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

<https://cuckoo.cert.ee/submit/post/5152284>

Cheaty do her

Cheat se hledal velice obtížně, upřímně to zabralo dost času. To je způsobeno tím, že stránky se snaží vytěžit maximum. Často se tak bez registrace nikam nedostanete a nikdo vám nedá cheaty na pár kliknutí. Cheaty často hledají mladší hráči, což je zároveň zranitelná skupina, která si neuvědomuje jak moc je nutná obezřetnost. Cheaty už jsou dávno komerční věc. Kdysi jste našli .exe soubor někde na fóru, bez přihlášení jej během pár sekund stáhli, spustili. Já jsem při hledání narazil spíš na velké platformy, které dokonce nabízejí launcher, dokonce si jej vynucují.



A screenshot of the anyx.gg website. The top navigation bar includes links for "Forums", "Store", "Discord", "FAQ", "Log in", "Register", and a search icon. Below the navigation, a banner reads "CS2 Cheats & Undetected Free CS2 Hacks". A sub-banner below it says "Get our amazing CS2 Cheats - the best on the market. We develop our cs2 hacks very carefully and take care about your security. Our counter-strike 2 hacks are undetected." On the left, a sidebar lists categories: "Free CS2 Cheats" (1), "CS2 Hacks" (4), "CS:GO Cheats" (4), and "CS2 Commandbot" (2). A "Top rated products" section highlights three items: "Free CS2 Cheats | Undetected Free CS2 Hacks" (Premium CS2 Hacks | Undetected v3.0.0.6) with a 5-star rating and "From: €12.99"; "CS2 Cheat | Premium CS2 Hacks | Undetected v3.0.0.6" with a 5-star rating and "From: €12.99"; and "CS2 Commandbot - Ingame commands (friendly teacher leader)" with a 5-star rating and "From: €2.99". Each product card includes a "Purchase" button and update information like "Updated: Thursday at 12:57 PM" or "Released: Mar 20, 2024".

Undetected CS2 Cheats & Free CS2 Cheats

By registering with us, you'll be able to try our free **CS2 Cheat** or to buy the premium!

 SIGNUP NOW!

CS2 CHEATS & HACKS

Get now the Project: Infinity CS2 Cheats and get a better gaming experience. With our CS2 Hacks you get the full control of the game. We also offer Free CS2 Cheats.

CATEGORIES

CS2 Cheats & Hacks 1

CS:GO Cheats & Hacks 3

CS2 Command-Bot 1

Valorant Cheats 1

Steam Points 1

Forum Upgrades 2

REDEEM KEY

You need to be logged in to view this page.



PREMIUM CS2 CHEAT

Get our undetected Premium CS2 Cheat. Undetected Counter-Strike 2 Cheats since release.

 From: €14.99

Filters ▾

Na všech výše zobrazených stránkách je nutná **registrace i launcher**.

Zajímavostí je, že když jsem nemohl nic najít, napadlo mě podívat se rovnou na GitHub, kde by to šlo snadno stáhnout. Tam jsou k nalezení cheaty především ve formě CPP projektů. Nenajdeme tam nic spustitelného. Museli bychom si spustit cheat externě, sami si buildnout projekt a vytvořit něco spustitelného. Výhodou je, že pokud umíte CPP, můžete proletět všechny soubory a zjistit, zda neobsahuje nějaký škodlivý software.

Github link

[CS2_External / CS2_External /](#) 

 **forcemilk** Update Bunnyhop.hpp

Name

Last commit message

 ..

[Update] Updated menu style, added FovCircle, a toggle for OBSBypass.

 Radar

[Update] Move radar to window.

 Utils

added static folder for configs

 AimBot.hpp

[Fixed] Fixed smooth calc error.

 AntiFlashbang.hpp

[Move] Move "AntiFlashbang.hpp" to "Cheats" Filter.

 Bone.cpp

添加项目文件。

 Bone.h

[Update] Added weapon ESP, aimbot RCS.

 Bunnyhop.hpp

Update Bunnyhop.hpp

 CS2_External.vcxproj

added anti flashbang

 CS2_External.vcxproj.filters

[Move] Move "AntiFlashbang.hpp" to "Cheats" Filter.

 Cheats.cpp

fixed

 Cheats.h

added anti flashbang

 Entity.cpp

[Fixed] Fixed esp not working when holding some weapons.

Původně jsem si myslel že může být problém v prohlížeči, VPN nebo něčem jiném. Ale ani po hledání na jiném prohlížeči, cheaty na jinou hru, bez VPN se mi prostě ani po 2h nepodařilo najít jediný soubor bez registrace. A jelikož stránky nabízející cheaty mi nepřipadají jako důvěryhodná entita do které budu sypat svoje loginy, tak jsem nic nenašel. Snažil jsem se najít v Cuckoo sandboxu něco podle jména. Ale jejich search fukce nefunguje a po dlouhých minutách spadne web.

Výsledkem tedy je, že najít cheaty není vůbec snadné. Provideři se snaží často vydojit maximum. Ukradou vám přihlašovací údaje, vezmou si od vás peníze za jejich skvělý nedetekovatelný cheat, vy dostanete ban a oni ještě mají Trojana ve vašem PC 😊 . A tak to obvykle dopadá.

Závěr k oběma částem:

Na internetu nelze věřit ničemu a nikomu. Obzvlášť pokud je to zdarma. Když něčemu dáte nálepku „free“, tak to přiláká hodně lidí. V tomto kontextu na to hakeři spoléhají. Dají se najít i legitimní softwary. Častěji ale například crack funguje a vy sice hrajete, ale crack s sebou přivezl černého pasažéra. Cheaty ani cracky se nevyplatí, radši si zaplatit těch pár dolarů za oficiální distribuci a hrát poctivě.