Keylogger a Phishing

Zpracoval: Denis Lokaj

Popis problému

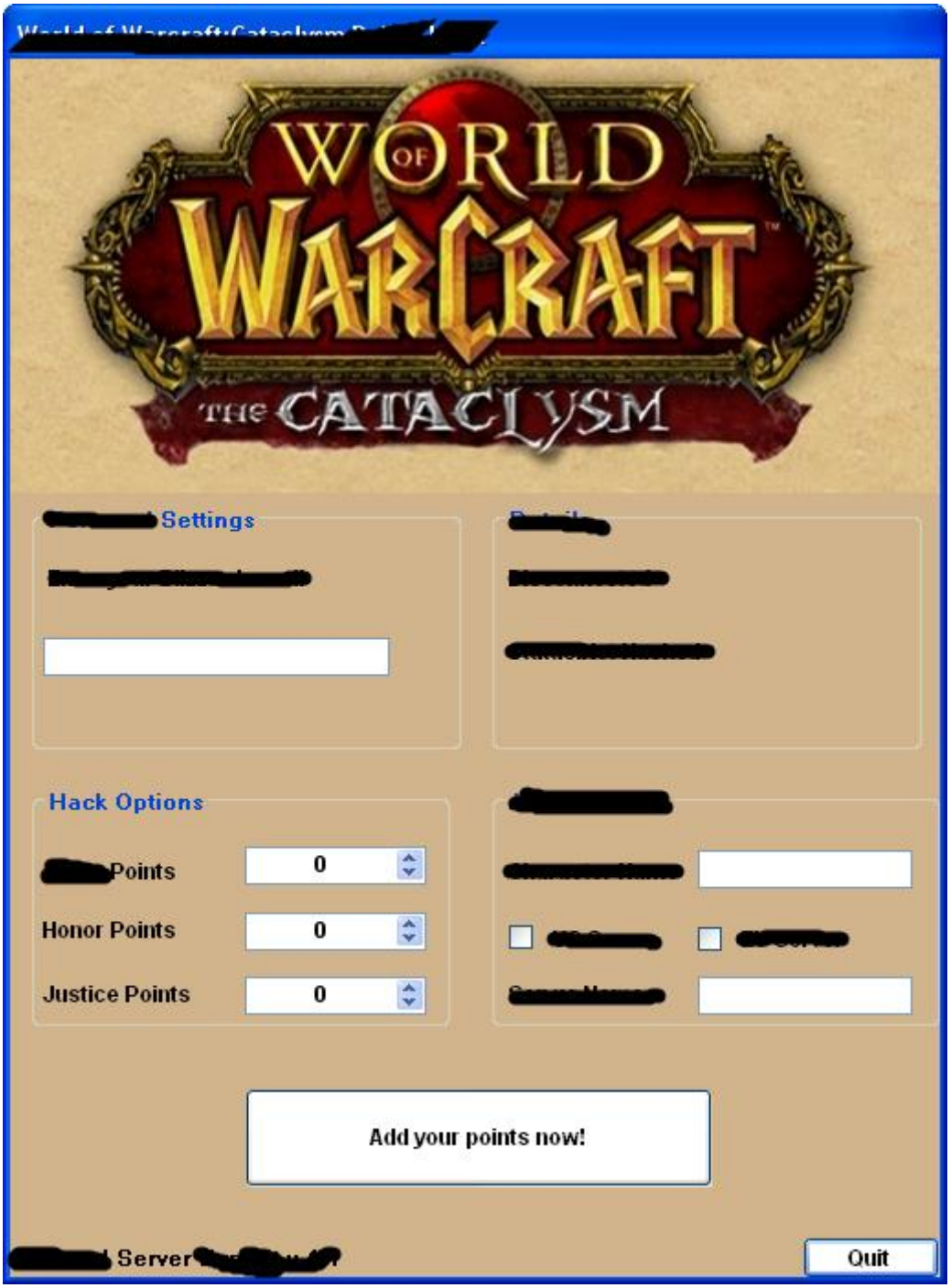
Jedná se o nejstarší a poměrně nejznámější způsob jak získat citlivé údaje od obětí tohoto viru. Cílem těchto nástrojů je povětšinou vždy od oběti něco získat – nejlépe něco co se dá zpeněžit. Phishing staví svou činnost na získávání účtů – ať už bankovních nebo klidně herních, případně různé elektronické peněženky, které se dají také zpeněžit. Trochu propracovanější metodou získávání citlivých údajů je Keylogger, který může fungovat jak softwarově tak i hardwarově a poskytuje větší výběr údajů od uživatele, zde se dají zpeněžit i jedny z nejcitlivějších údajů. Příkladem může být vydírání na základě nějaké činnosti, kterou byste nechtěli aby lidé z vašeho nejbližšího kruhu věděli, tedy na základě informací co od vás hacker dostane, je schopen zanalyzovat co jste za člověka a zvolit strategii takovou aby vás zahnal takříkajíc „do kouta“ a dostal od vás co potřebuje. Většinou takhle člověk poskytne útočníkovi více svých osobních údajů v domění, že ho už hacker nechá na pokoji, ovšem povětšinou tihle lidé jenom vaří z vody a tvrdí, že např. mají intimní video s vámi, přitom jenom ví, že jste intimní video sledoval a v tuhle chvíli pokud poskytnete útočníkovi další informace může být těžké se dostat ze spirály vydírání.

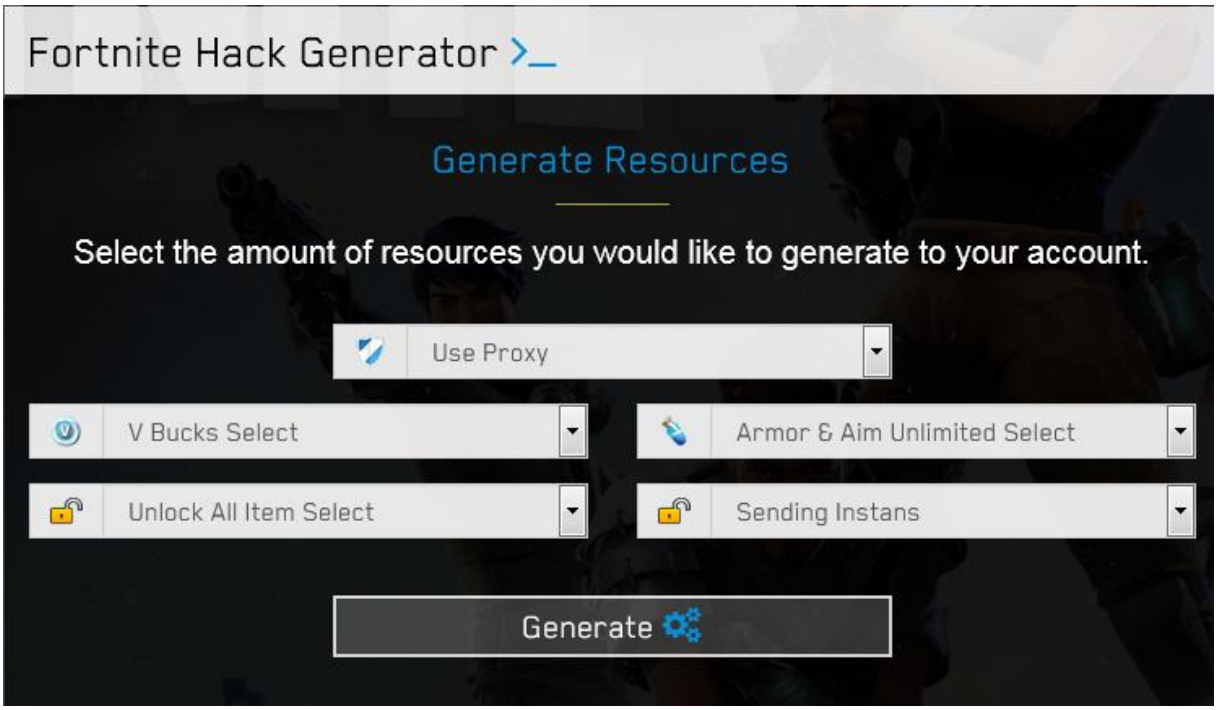
Jak fungujou?

Phishing funguje tak, že vám nabídne nějaký falešný nástroj, případně falešně sdělení od např. vaší bankovní společnosti, že je něco v nepořádku s vaším účtem a potřebujou nějaké údaje, mnohdy tyto sdělení dokážou vypadat až trapně, ale někdy jsou hodně sofistikované, v tom smyslu že je těžké rozeznat jestli se jedná o reálné nebo falešné sdělení. V oblasti her se využívají hodně nástroje, které hráčům mají pomoct ve hrách, tedy můžeme do nich zařadit nějaké pluginy nebo klidně i cheaty u kterých je vedlejším účinkem to, že získají přístup k vašemu hernímu účtu nebo hernímu obchodu.

Keylogger je povětšinou řešen softwarově a zde platí, že pokud stáhnete něco neověřeného z internetu, můžete se lehce stát obětí keyloggeru, funguje na principu toho, že zaznamenává všechny stisknutí kláves. V oblasti her a esportu se dá využít praktičtěji a nabízí větší škálu možností, jelikož by se v hodně „hardcore“ scénaři dalo tohoto nástroje využít pro simulaci pozice daného hráče z nepřátelského týmu, tedy nejspíše v žánru FPS, jako např. CS:GO nebo Valorant. Tímto způsobem by tým využívající této metody získal navrh a měl by realtime přehled o pozici hráčů z nepřátelského týmu, nýbrž existuje zde řada komplikací, např. jak vědět že zrovna hráč dělá to co by podle keyloggeru měl dělat? A taktéž komplikace v podobě jak dostat zmíněný keylogger do počítače druhých hráčů. Jedná se o komplexní využití keyloggeru, které by v reálném světě vyžadovalo moc práce pro takové řešení, ale i přesto se jedná o zajímavý nápad.

Příklady z praxe:





Rozhodl jsem se rozebrat tenhle typ phishingu, kdy vám např. ve hře World of Warcraft nebo Fortnite podobné aplikace nabídnou, že vám nějakým způsobem „dají“ herní měnu, případně jiné vymoženosti bez potřebné námahy, mnoho lidí, zejména dětí se na tenhle způsob phishingu snadno chytí, jelikož interface dané aplikace je velmi jednoduchý a přímočarý, nevyžaduje komplexní informace a pro laika, který tomu nerozumí, příjdou i tyto požadované informace jako opodstatněné. Hry typu Fortnite a World of Warcraft neoperujou s lokálními daty, veškeré citlivé informace se nacházejí na databázovém serveru společnosti provozující tyto hry, tudíž neexistuje způsob jak by tento „cheat“ mohl fungovat. Pokud pomineme nedůvěryhodnost pramenicí z inteligence a určité intuice jedná se o typ hacku, který si vždy najde své oběti. Řešením by byla osvěta, která by měla probíhat už i na základních školách a hlavně do hloubky a s expertama, nyní výuka probíhá dost vágně, kdy se opakujou ty stejné „mantry“ v podobě „Nikdy nikomu nedávej své heslo“ atd. které nejsou pro reálnou praxi moc vypovídající.

Jak se bránit?

1. Nestahovat aplikace z neověřených zdrojů
2. Mít aktivní antivirus
3. Než na něco kliknu/vyplním zkontrolovat zdroj (např. odesílatele emailu)
4. Pokud pracuji na jiném počítači, zkontrolovat co vše je k němu napojené
5. Pokud něco chce mé údaje, použít selský rozum a 2x si rozmyslet jestli ho opravdu potřebuje
6. Použít software, který používá komplexnější způsoby autentifikace – např. měnič hesel nebo dvoufázové autentifikátory

Zdroje :

https://sites.google.com/site/fortnitehackonline999/_/rsrc/1528584854143/home/Screenshot_1.png

https://1.bp.blogspot.com/-BDSw8mgpeDU/UyQfHnL9GGI/AAAAAAAAAHc/9ACljvkaKzQ/s1600/WOW+POINTS.png

https://cs.wikipedia.org/wiki/Keylogger

https://www.spyshop24.cz/blog_cz/jak-funguje-keylogger/

https://cs.wikipedia.org/wiki/Phishing