TSIT01 Datasäkerhetsmetoder

Föreläsning 4 bonus: Bot crisis

Ingemar Ragnemalm

Exempel på malware och svårt säkerhetsproblem: TF2 "Bot crisis"

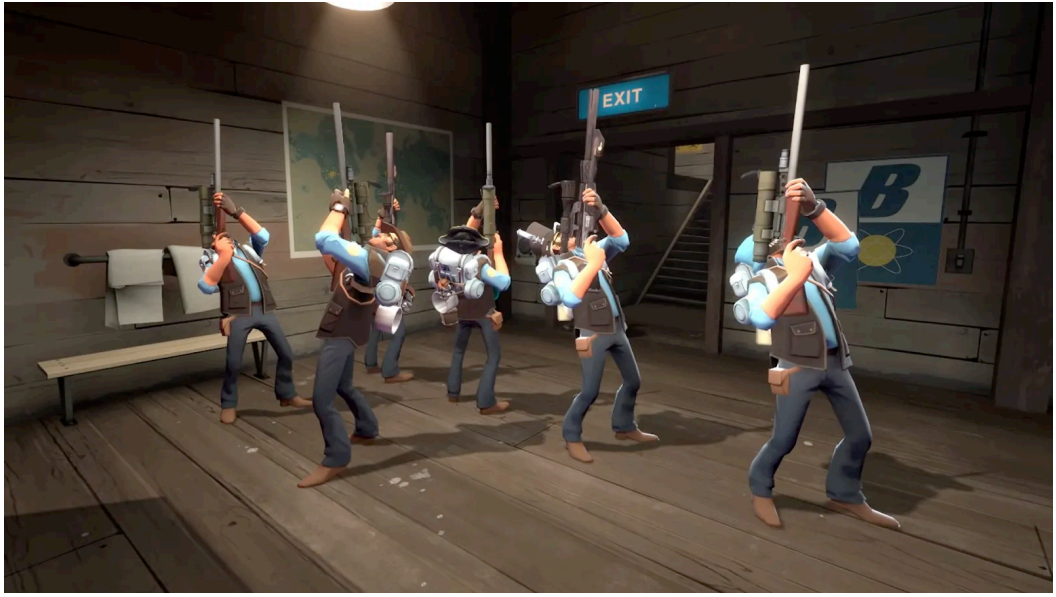
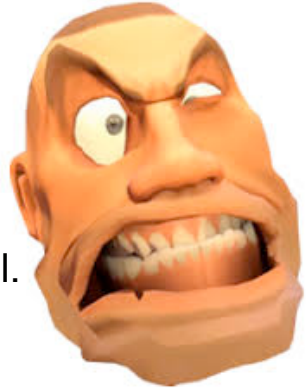


Bild från https://theglobalgaming.com/gaming/are-there-bots-in-team-fortress-2

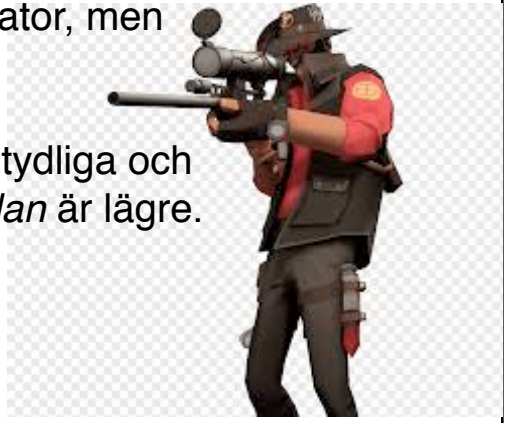
Team Fortress 2: Fusk-botar



Spelet svårt drabbat av "sniper-bots", automater som slår ut andra spelare med ett skott på långt håll.

Spelet blir ospelbart, en typ av denial-of-service.

Attacken görs lokalt, på angriparens egen dator, men resultatet förstör spelet för spelare globalt.



Andra typer av fusk finns men de är mindre tydliga och förstör därmed inte spelet lika mycket. *Skadan* är lägre.

Team Fortress 2: Angripare

Två typer av angripare: Experter, som analyserar lokala data och skapar botarna, och "script kids" som laddar ner resultatet och kör det utan att veta hur det fungerar.

TF2 är svårt drabbat av script kids som hittar botkod på nätet. Å andra sidan... detta gör att Valve också kommer åt denna kod.

Team Fortress 2: Motivation

Ett mysterium! Troligen maktkänsla, men det är fullt möjligt att vi även har aktivister som vill förstöra spelet. Smärre ekonomiska motiv finns (säljbara objekt som botarna får under spelandet) men är mindre troliga.

Team Fortress 2: En enkel CIA-analys

Grundsituationen är praktiskt taget enbart en fråga om availability: Spelet är visserligen tillgängligt men spelandet är inte tillgängligt.

Är det ett integritetsproblem när botarna kopierar ditt namn? Det ger också risken att du anmäls för fusk som någon annan utför!

Vissa åtgärder (som vi kommer till) kan dock störa integriteten, och vissa kräver också konfidentialitet.

Team Fortress 2: Åtgärder

Intressant problem på grund av alla försök att lösa det, som måste förkastas! Svårigheten är att hitta rätt åtgärder.

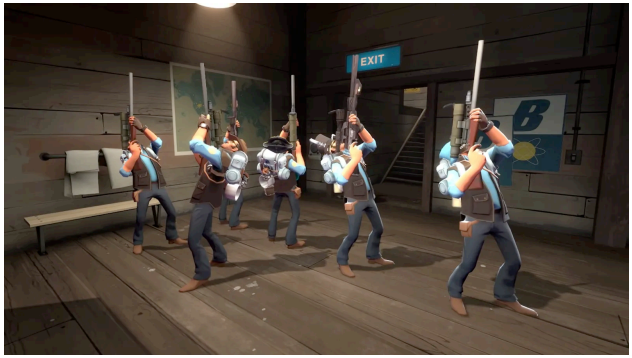
Video från konferens går igenom många förslag för hur problemet kan lösas.

"Threadmill", ett problem måste lösas om och om igen och blir aldrig klart.

Svårt problem eftersom källan är angriparens dator!

Captcha: Fungerar inte! Captchas knäcks med lärande system.

Team Fortress 2: Åtgärder

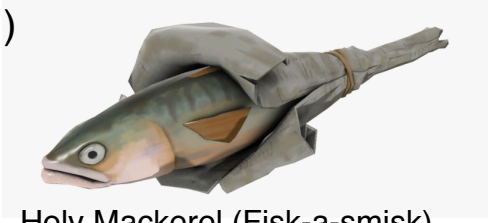


Lärande system. Identifiera fuskare på beteende.

Snipers som siktar i taket är lätta att identifiera. Men... hur långt räcker detta?

Metoder för att identifiera fuskare riskerar att göra "false positives" och drabba skickliga spelare. Även människor gör false positives. Exempel: Duktig "fish scout" blev anklagad för fusk bara för att han var så skicklig! (Dock inte av systemet - än.)

Slutsats: False positives = hög kostnad! För hög!



Holy Mackerel (Fisk-a-smisk)

Team Fortress 2: Åtgärder

Blockera namn? "Omegatronic" mfl vanliga. Namn byts lätt. Botar kopierar namn av andra användare!

Blockera på IP? IP-nummer byts och delas av flera.

Blockera på ID-nummer i hårdvaran? Detta kan manipuleras, lättast med viruella maskiner.

"Fake targets", osynliga låtsasspelare. Detta kan detekteras.

Identifikation (Steam guard)? Det finns emulatorer för detta.

Slutsats: Ingen eller liten effekt för samtliga.

Team Fortress 2: Ändra spelet helt?

• Skippa free-to-play
Lite svårt att göra på ett gammalt spel som varit gratis länge

• Tag bort sniper
Blir spelet för lätt för t.ex. heavy? Neej... heavy har fortfarande spy efter sig.

• Försvaga sniper
Ja tack säger jag men den blir nog ospelbar för människor.

Vågar man göra så dramatiska ändringar? Allt retar upp eller jagar bort folk som vill att det skall vara som förut.

Team Fortress 2: Andra åtgärder?

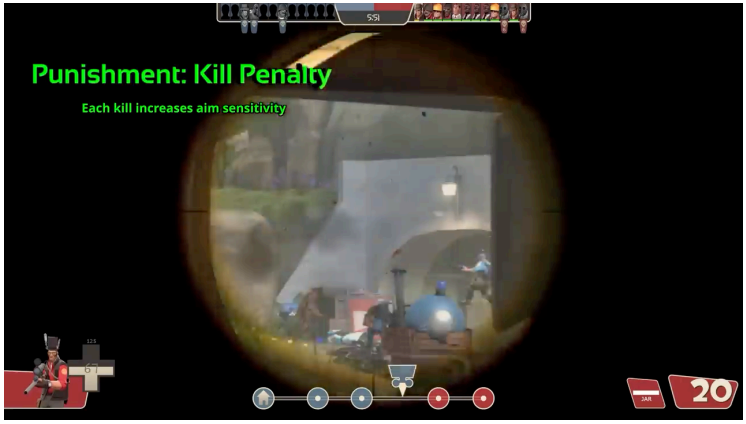
Red hat. Anfall på deras egen planhalva.

Antag att de flesta är script kiddies. Publicera "fusk" som fungerar dåligt. Lura script kiddies att använda dem.

Plötsligt flyttas problemet till dem, de måste lura ut vad som är fusk!

Kostnad: Medel. Retar inte upp legitima spelare.

Effekt: Kan hjälpa.



Team Fortress 2: Andra åtgärder?

Använd kunskap om hur botarna fungerar.

Jobbar botarna med interna hitboxar? Troligt eftersom de skjuter på dolda spioner. Ändra lagringsformatet för hitboxar mm?

Kan detta göras dynamiskt, automatiskt, så får botskaparna ett "threadmill"-problem.

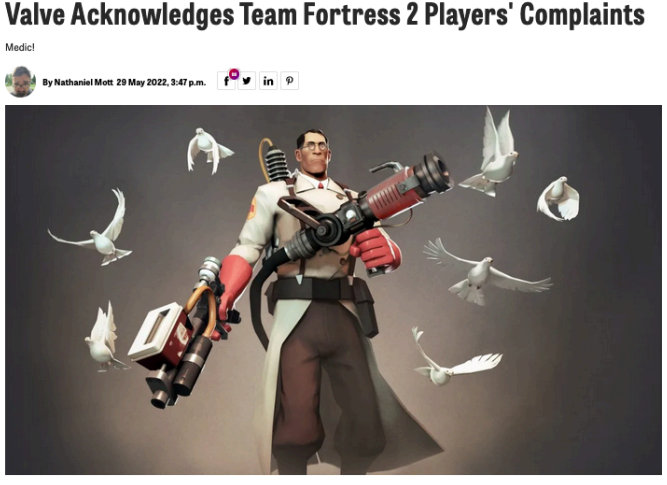
Kostnad: Rätt hög. Kräver betydande insatser i komplex kod.

Effekt: Kan hjälpa.

Team Fortress 2: Bättre idag?

Situationen verkar ha förbättrats. Vad gjorde utvecklaren Valve? Det kan de inte avslöja! Men de har bekräftat att de gjort något, eller i alla fall jobbar på det.

Vad tror du att de kan ha gjort för åtgärder?



Är allt bra igen?

Fusk kommer alltid att finnas. "Threadmill problem"
Men om spelet är spelbart så är mycket vunnet.

Slutsats: Ett problem där svårigheten är att *hitta åtgärderna*