STEAM BROWSER PROTOCOL VULNERABILITY

Daniel Rossell

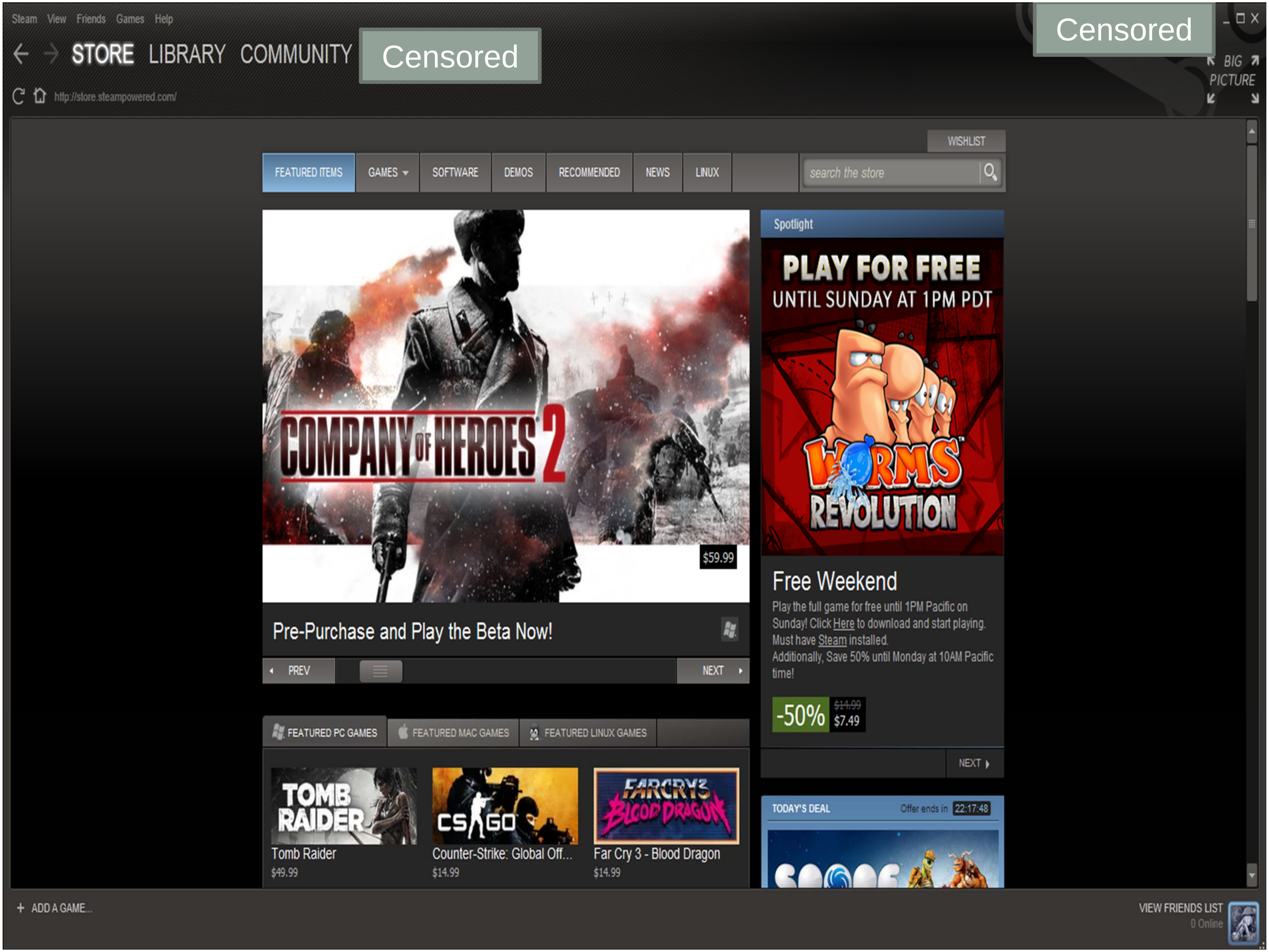
Outline

- Steam Software
- Browser Protocol
- External URLs
- Vulnerabilities
- Fixes

Steam Software

- Digital Distribution Platform mainly used for video games

- EA Origin is Steam’s major competitor and has a similar vulnerability



Pre-Purchase and Play the Beta Now!

Free Weekend

Play the full game for free until 1PM Pacific on Sunday! Click Here to download and start playing. Must have Steam installed.
Additionally, Save 50% until Monday at 10AM Pacific time!

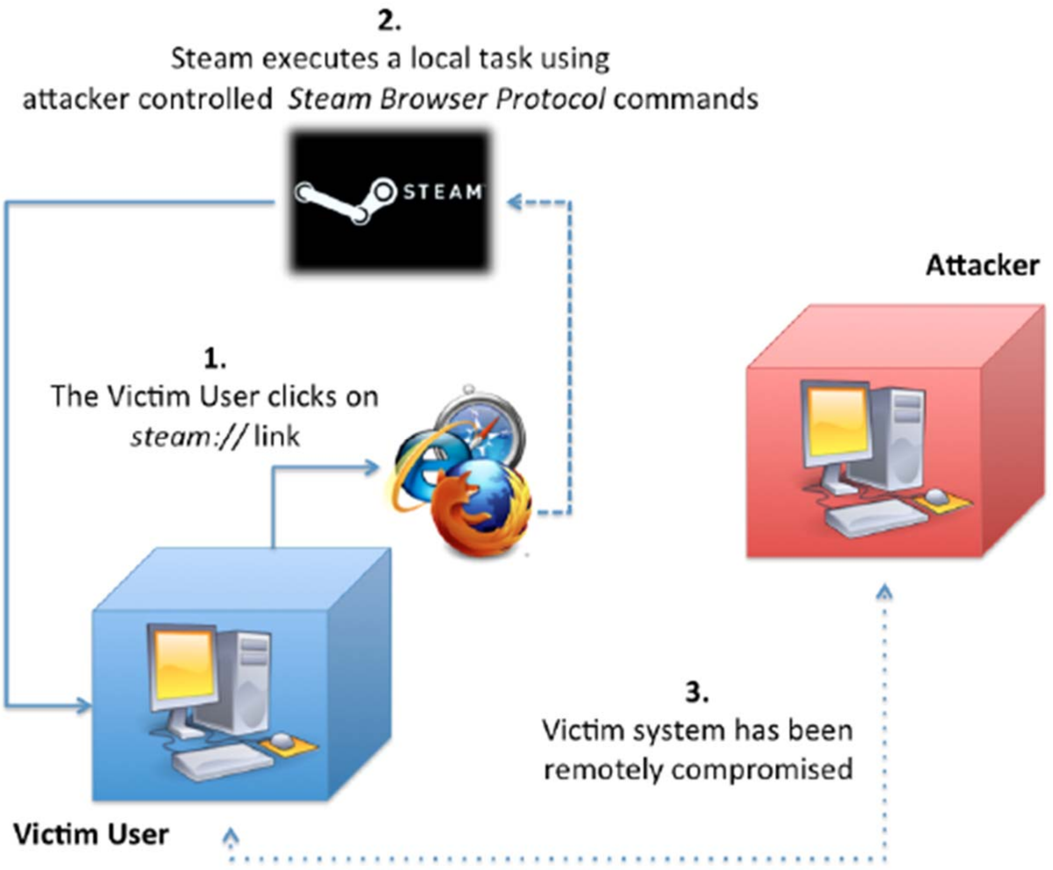
-50% ~~$14.99~~ $7.49

Tomb Raider	Counter-Strike: Global Off...	Far Cry 3 - Blood Dragon
$49.99	$14.99	$14.99

Steam Browser Protocol Vulnerability

- steam:// URL handler Is Used To :
  - Install and Uninstall Software
  - Backup Software
  - Defrag
  - Run Games
  - Navigate Steam

- Vulnerability
  - Local tasks can be executed using Steam URL Commands

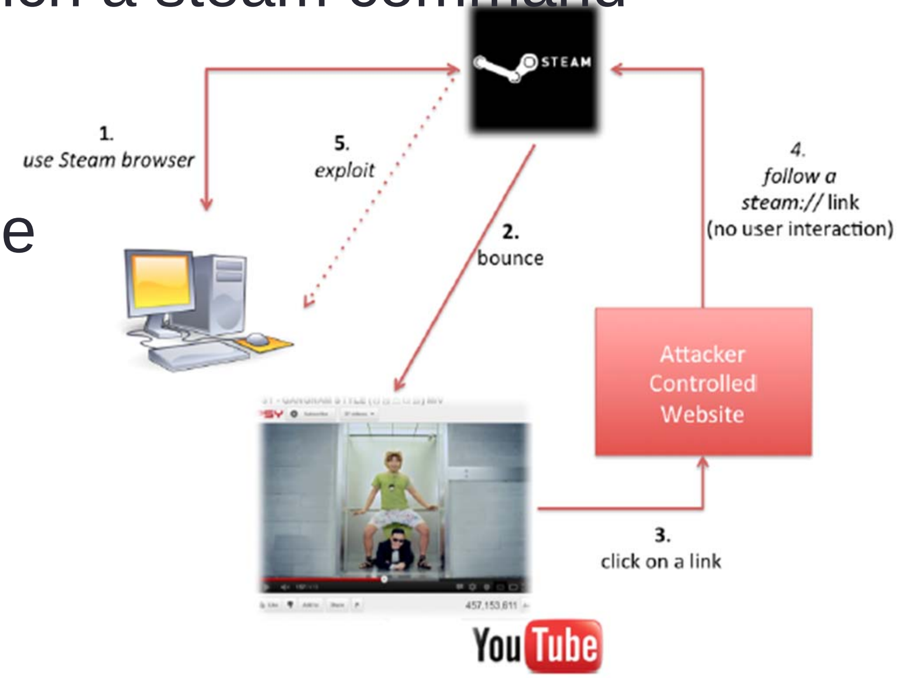

2.
Steam executes a local task using
attacker controlled *Steam Browser Protocol* commands
STEAM
Attacker
1.
The Victim User clicks on
steam:// link
3.
Victim system has been
remotely compromised
Victim User

How the Vulnerability Works

- steam:// is a 3rd party URL to web browsers
  - Only IE9 and Chrome generate a warning and it can be turned off
  - Most browsers (including Firefox) do not generate a warning

- User clicking on link will launch a steam command
  - Example : steam://nav/games

- Link can be hidden anywhere
  - E-Mail
  - Website
  - Steam User Profile



1. use Steam browser

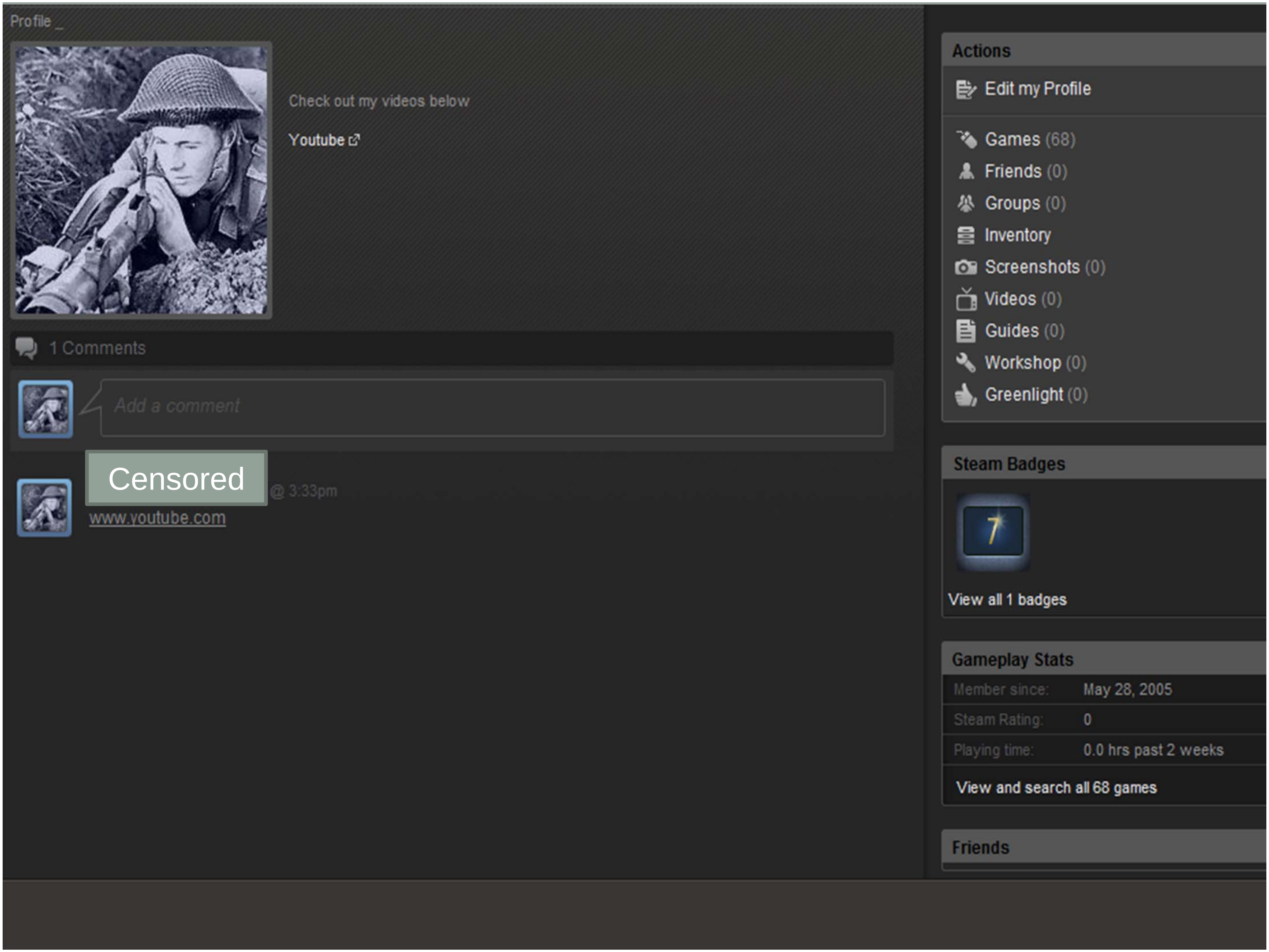
2. bounce

3. click on a link

4. follow a steam:// link (no user interaction)

5. exploit

Attacker Controlled Website



Profile _

Check out my videos below

Youtube

1 Comments

Add a comment

Censored @ 3:33pm

www.youtube.com

Gameplay Stats

Member since:	May 28, 2005
Steam Rating:	0
Playing time:	0.0 hrs past 2 weeks

View and search all 68 games

Friends

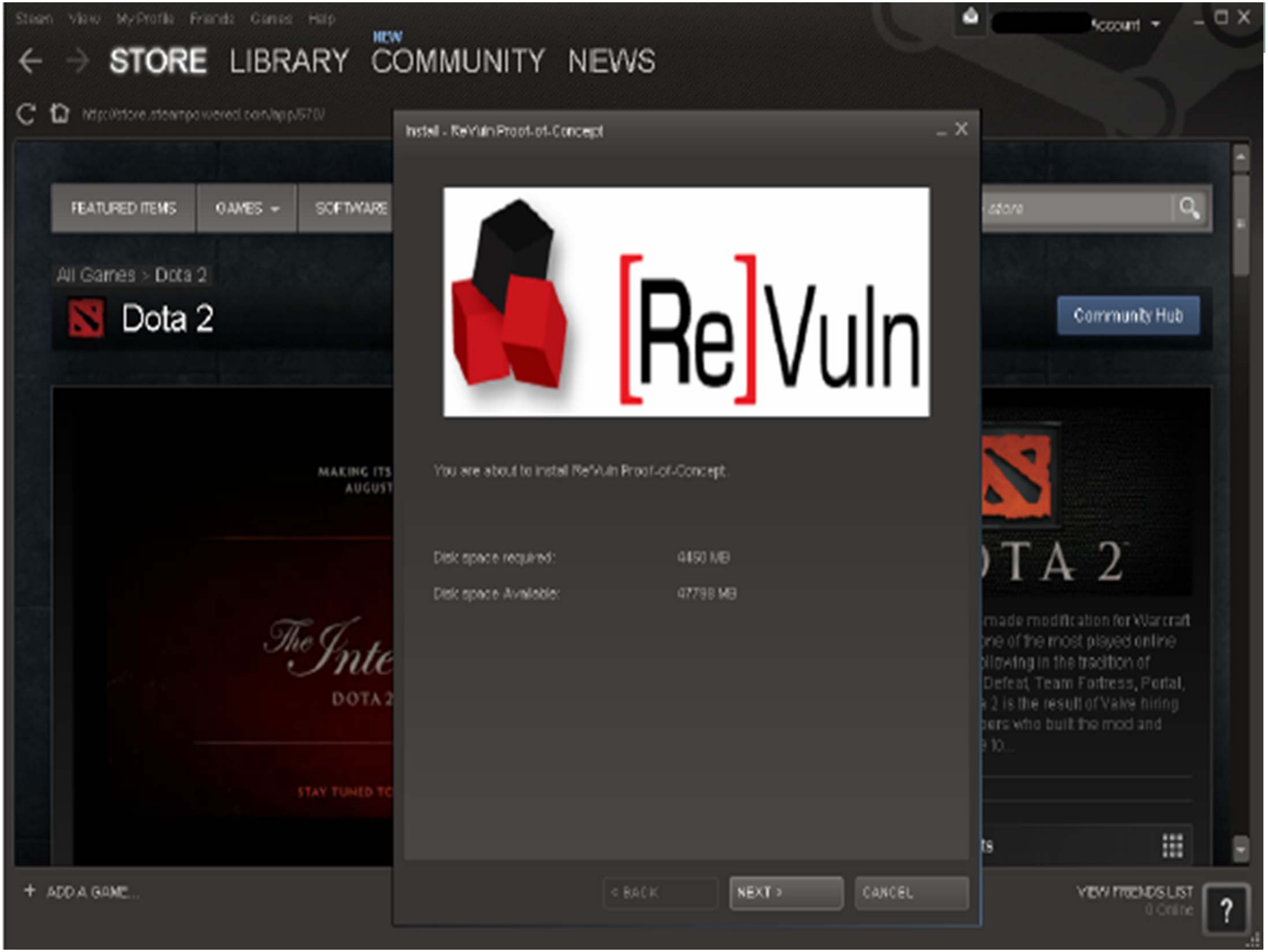
Vulnerability Allows Execution of Steam Commands

- Steam Commands executed locally on users system
    - Possibly without user knowledge
- Provides access to a number of tools to make exploiting other vulnerabilities easier
- Fortunately there are many available
    - Some built into Steam itself
    - Many based off of the games that Steam manages

Retailinstall Vulnerability

- Command built into steam that restores backups from a local directory
  - Command line argument specifies directory
  - Directory stores a TGA image and backup files
  - vgui2_s.dll loads the TGA image when command is called
  - Vulnerable to heap based buffer overflow using a malformed TGA image

- Buffer overflow allows the writing of any arbitrary code to any location on the victim’s PC


Steam View My Profile Friends Games Help
[redacted] Account
STORE LIBRARY NEW COMMUNITY NEWS
http://store.steampowered.com/app/570/
FEATURED ITEMS
GAMES
SOFTWARE
store
All Games > Dota 2
Dota 2
Community Hub
MAKING ITS
AUGUST
The Inte
DOTA 2
STAY TUNED TO
OTA 2
made modification for Warcraft
one of the most played online
ollowing in the tradition of
Defeat, Team Fortress, Portal,
2 is the result of Valve hiring
bers who built the mod and
to...
+ ADD A GAME...
VIEW FRIENDS LIST
0 Online
?
[Re]Vuln
< BACK
NEXT >
CANCEL

Install - ReVuln Proof-of-Concept

You are about to install ReVuln Proof-of-Concept.

Disk space required: 4450 MB

Disk space Available: 47798 MB

Game Based Vulnerabilites

- Steam allows games to be ran with command line arguments that can be used to exploit game engines
  - Example : steam://run/id/language/url_encoded_parameters

- Source Engine
  - Use for Half Life Games, Team Fortress 2, Left for Dead, Dota 2, …
  - Commands within the Engine can be exploited :
    - +con_logfile – Specifiy file to copy the game console to
    - +echo – Put custom data into the console
    - -hijack – In case the game is currently running
  - Combined allows writing custom file to location of choice on target's system
  - Author's created a .bat file to execute malicious scripts

Fixes

- Individual Vulnerabilities
  - Steam TGA file loading
  - Source engine console write
  - Unreal engine buffer overflow

- Steam distributes a lot of software, need to fix core problem that allows execution
  - Do not allow passing of command line arguments to games
  - Browsers should check or limit execution of steam:// URL

References

- http://revuln.com/files/ReVuln_Steam_Browser_Protocol_Insecurity.pdf
- http://arstechnica.com/security/2012/10/steam-vulnerability-can-lead-to-remote-insertion-of-malicious-code/
- https://developer.valvesoftware.com/wiki/Steam_browser_protocol