Practical security in computer games

by gynvael.coldwind//vx

Confidence 2.0, Warsaw 2009

Hispasec

http://hispasec.com
http://virustotal.com

Gynvael Coldwind

Vexillium

http://vexillium.org

Is there anyone from the game industry here with us ?

If so, please, do not throw heavy objects in my direction

No, light objects are not OK

Why should we care about some stupid games?

Why should we care about some stupid games?

Games are normal apps

Why should we care about some stupid games?

Games are normal apps

↓

Multi player (network) games are normal network apps

Game vs Web Browser

Game vs Web Browser

√ Connects to foreign servers

- game management server
- game hosting servers
- other game peers
- resource servers

Game vs Web Browser

√ Connects to foreign servers

√ **Downloads foreign content**

- GUI layouts
- animated ads
- various scripts
- maps, images, sfx, savegames

Game vs Web Browser

√ Connects to foreign servers
√ Downloads foreign content
√ Supports many resource types

Game vs Web Browser

√ Connects to foreign servers

√ Downloads foreign content

√ Supports many resource types

√ Executes foreign scripts

Game vs Web Browser

√ Connects to foreign servers

√ Downloads foreign content

√ Supports many resource types

√ Executes foreign scripts

√ Uses various protocols

Why should we care about some stupid games?

Games are normal apps

↓

Multi player (network) games are normal network apps

Why should we care about some stupid games?

Games are normal apps

↓

Multi player (network) games are normal network apps

↓

Most (every?) network apps have vulnerabilities

Over 30 vulnerabilities* in network apps in just one week (10-16 Nov)

*SecurityFocus.com

Why should we care about some stupid games?

Games are normal apps

↓

Multi player (network) games are normal network apps

↓

Most (every?) network apps have vulnerabilities

↓

Vulnerabilities present a threat

What threat?

Botmasters do not exploit games…

What threat?

Botmasters do not exploit games… yet

What threat?

Two ways to become a zombie!

- drive-by download
- scan and exploit

What threat?

Three ways to become a zombie!

- drive-by download
- scan and exploit
- user downloads game-related malware (PPKK)

Who plays these games anyway?

Who plays these games anyway?

kids

Who plays these games anyway?

kids
your employees at home

Who plays these games anyway?

kids
your employees at home
your employees at work

Who plays these games anyway?

kids
your employees at home
your employees at work
your clients

Who plays these games anyway?

kids
your employees at home
your employees at work
your clients
your employer

Who plays these games anyway?

kids
your employees at home
your employees at work
your clients
your employer
your family

Who plays these games anyway?

kids
your employees at home
your employees at work
your clients
your employer
your family

Who plays these games anyway?

kids
your employees at home
your employees at work
your clients
your employer
your family

Know any of these people?
Ever got a pendrive from them?
Ever executed an app they gave you?

Some random stats

PC game sales: $1.1 billion
Console game sales: $6.2 billion
(in USA in 2004)

There are over 20,000 Internet cafes in South Korea

World of Warcraft had over 11.5 million subscriptions (December 2008)

Source: Wikipedia

Some random stats

Games are becoming more and more popular

E-sport and progaming

WCG 2009
GF: 600 players in Chengdu, China

Poland WCG 2009 eliminations:
27,000 fans watching online

Do game makers care about security?

Do game makers care about security?

YES THEY DO!

Do game makers care about security?

YES THEY DO!

- anti-cracking (anti-piracy) security

reverse engineering, cracking/keygens, making copies of DVD/CD disk

Do game makers care about security?

YES THEY DO!

- anti-cracking (anti-piracy) security
- anti-cheating security

wallhacks, maphacks, bots

Do game makers care about security?

YES THEY DO!

- anti-cracking (anti-piracy) security
- anti-cheating security
- game-logic security

10 iron + 1 smiths hammer
->
+1 sword, - 10 iron

Do game makers care about security?

What about “standard” anti-vulnerability stuff ?

Do game makers care about security?

What about “standard” anti-vulnerability stuff ?

Yes... ehm.. maybe?
Well, it's bad because frame-rate is low because of it. And it takes coders too much time. And... who exploits games anyway?

A brief walk through popular multiplayer games

Let's see how the game security looks like...

Some bugtraq, some research...

Research == let's look for an exception

$$P = \mathrm{MIN}\left(\frac{\text{Number of DoS found}}{\text{Time spent testing (h)}}, 0.9\right)$$

A brief walk through popular multiplayer games

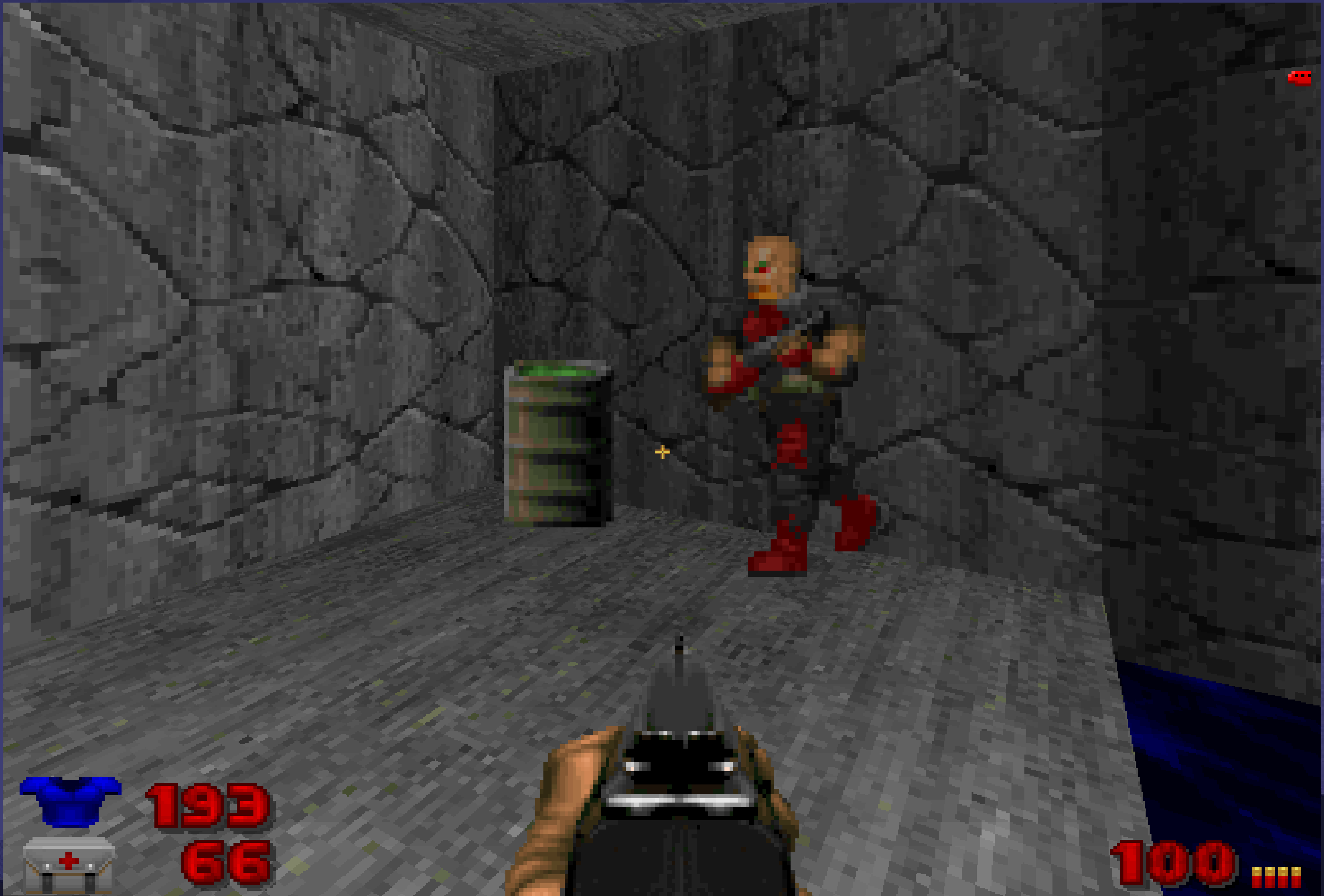
Tools:

SilkProxy
(simple scriptable proxy)

ExcpHook
(kernel-level exception monitor)

GDB, strace

Doom 2 (1994)
by id Software



Doom 2 (1994)
by id Software

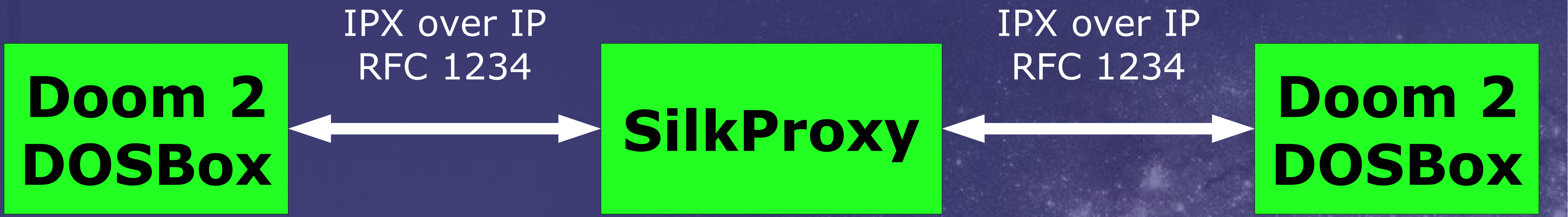
"Shareware registrations turned in $100,000 per day immediately after the release

Doom II's initial release was 600,000 copies. The supply intended to last one quarter, but only lasted one month."

http://doom.wikia.com/wiki/Sales

Doom 2 (1994)
by id Software

Test setup:



IPX over IP
RFC 1234

IPX over IP
RFC 1234

Doom 2
DOSBox

SilkProxy

Doom 2
DOSBox

**black sheep wall
and kill packet**

StarCraft (1998)
by Blizzard Entertainment

StarCraft (1998)
by Blizzard Entertainment

Over 9,000,000 copies sold (over 4,000,000 in South Korea). Who knows how many downloaded...

Many "master servers" (called "battle.net servers"). For example, on ICCUP there are over 60,000 players registered.

http://en.wikipedia.org/ICCUP

StarCraft (1998)
by Blizzard Entertainment

One of few pro gaming games
(players earn up to 200,000$ per year)

Very popular, even after 11 years

StarCraft (1998)
by Blizzard Entertainment

“Have Stim? No, Shield!”
Buffer overflow in map (UMS) loader found by Deathknight 4 years go.

What was the community response for a remote buffer overflow?

StarCraft (1998)
by Blizzard Entertainment

“Have Stim? No, Shield!”
Buffer overflow in map (UMS) loader found by Deathknight 4 years go.

“A new glitch found by Deathknight, a buffer overflow, has opened new limitless possibilities for the UMS map making with Starforge, making Starcraft map editing far superior to even Warcraf3 editing.”

http://sc.gosugamers.net

StarCraft (1998)
by Blizzard Entertainment

“Have Stim? No, Shield!”
Buffer overflow in map (UMS) loader found by Deathknight 4 years go.

It was patched by version 1.13b

“The UMS community did lose a useful tool, as the bug permitted them some nifty legitimate UMS functionality.”

http://sc.gosugamers.net

StarCraft (1998)
by Blizzard Entertainment

SecurityFocus:

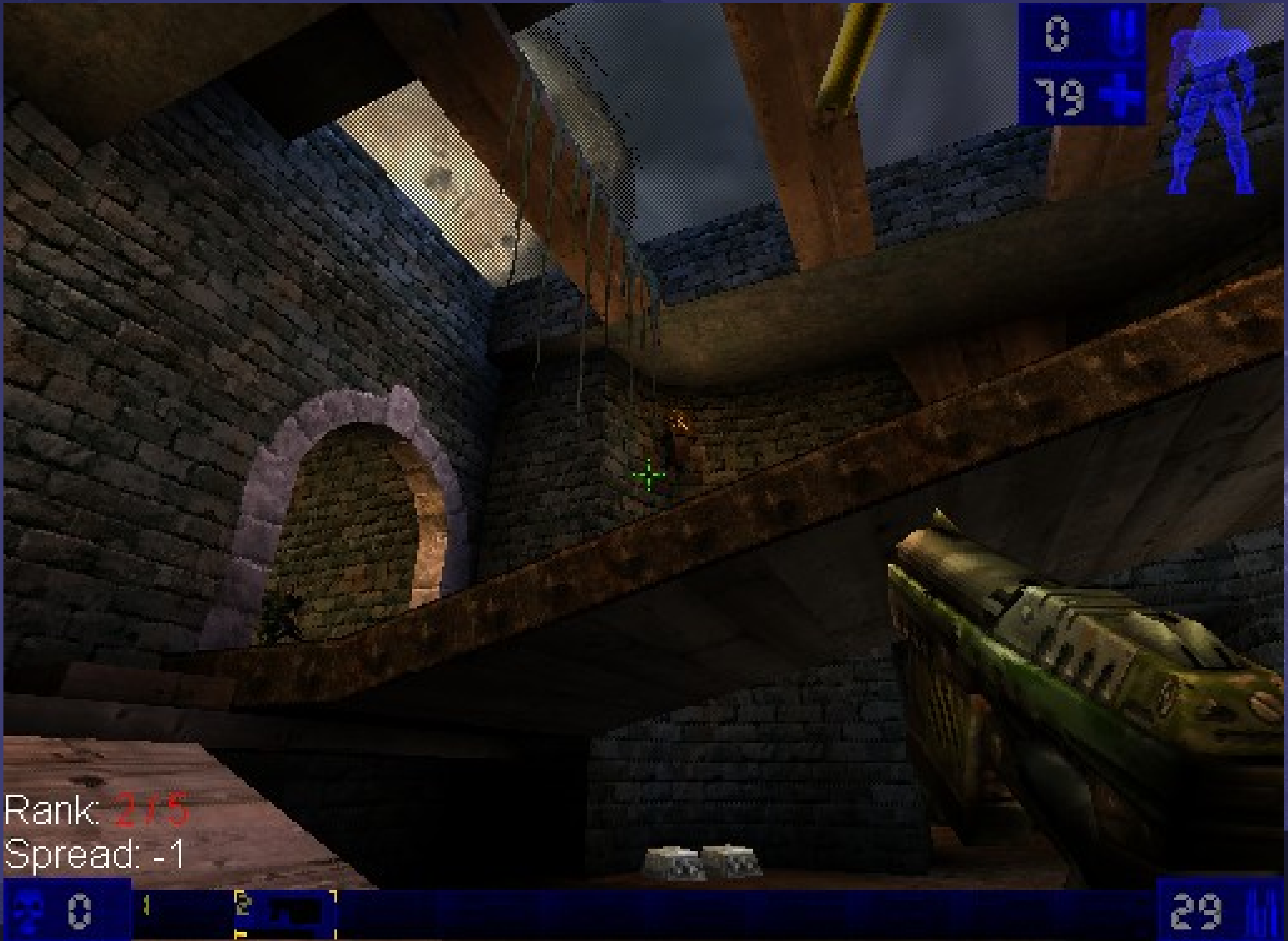
* BID=25478, Blizzard Entertainment StarCraft Brood War Minimap Preview Remote Denial of Service Vulnerability, Gynvael Coldwind

Brief testing results:

black sheep wall
black sheep wall

Unreal Tournament (1999)

by Epic Games



Unreal Tournament (1999)
by Epic Games

Based on Unreal engine.

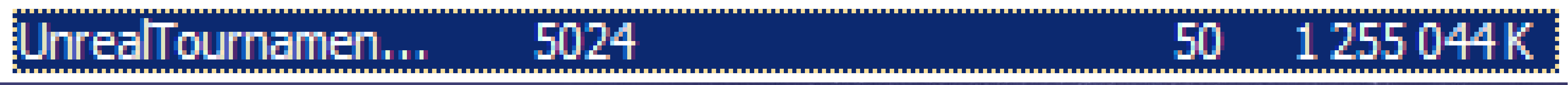
Up to date the master server is online, and there are still around a 100 populated game server.

Unreal Tournament (1999)
by Epic Games

SecurityFocus:

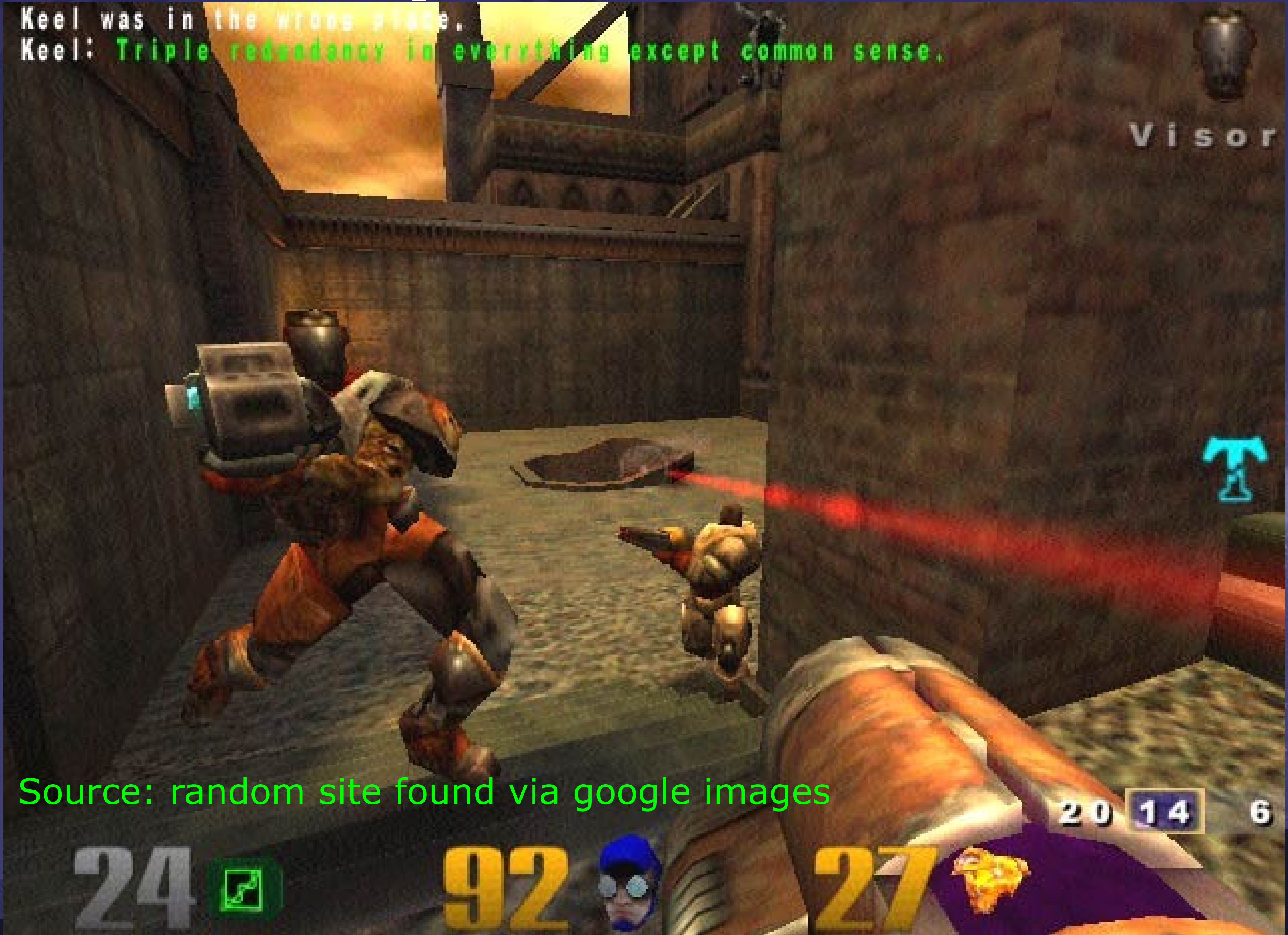
BID=5148, Server DoS Amplifier Vulnerability, Luigi Auriemma
BID=9840, Server Engine Remote Format String Vulnerability, Luigi Auriemma
BID=6770, Memory Consumption DoS, Luigi Auriemma
BID=6775, URL Directory Traversal Vulnerability, Luigi Auriemma
BID=10670, Memory Corruption Vulnerability, Luigi Auriemma
BID=6771, Multiple Players DoS Vulnerability, Luigi Auriemma
BID=6773, Packet Amplification DoS Vulnerability, Luigi Auriemma

Brief testing results:



```
UnrealTournamen...    5024                        50    1 255 044 K
```

Quake 3 (1999)
by id Software



Keel was in the wrong place.
Keel: Triple redundancy in everything except common sense.

Source: random site found via google images

Quake 3 (1999)
by id Software

Over 4,000,000 copies sold

Over 27,000 player online
(checked few days ago)

Release as open source

Many games based on this engine

Quake 3 (1999)
by id Software

SecurityFocus:

BID=3123, Possible Buffer Overflow Vulnerability, Coolest
BID=12976, Message Denial of Service Vulnerability, Luigi Auriemma
BID=12534, Infostring Query Remote DoS Vulnerability, Luigi Auriemma
BID=18777, Multiple Stack Buffer Overflow Vulnerabilities, RunningBon
BID=18685, Multiple Vulnerabilities, Luigi Auriemma
BID=18271, CL_ParseDownload Remote Buffer Overflow Vulnerability, Luigi Auriemma (**huffman decompr in size vs out size**)
BID=17857, remapShader Command Remote Buffer Overflow Vulnerability, landser

Older quake

BID=90, Quake Server Backdoor Vulnerability, Mark Zielinski

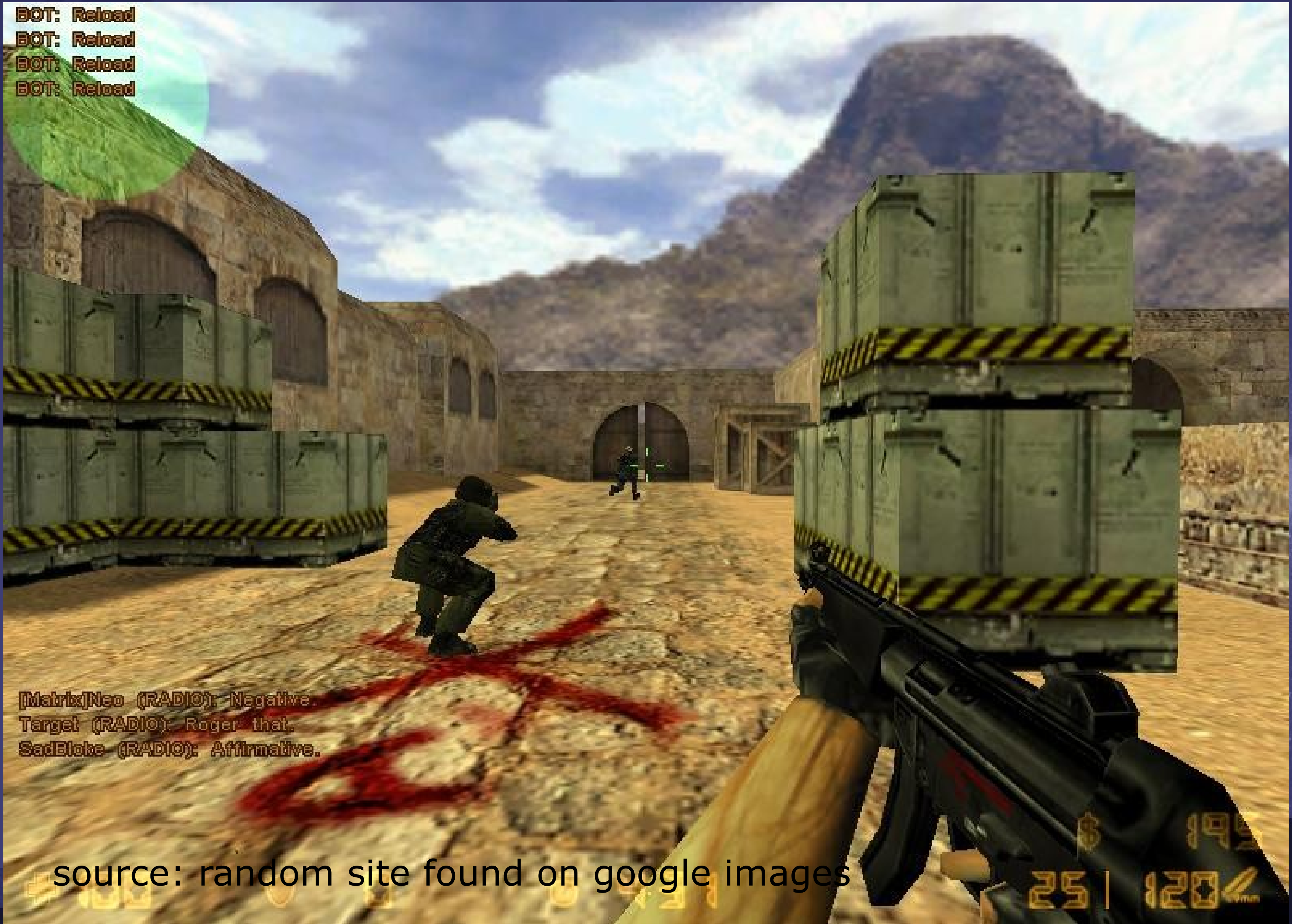
Quake 3 (1999)
by id Software

Luigi Auriemma website:

Format string in the Doom 3 engine through PunkBuster, Luigi Auriemma

Files overwriting through Automatic Downloading (directory traversal)

Counter-Strike (1999)
by Valve Software



BOT: Reload
BOT: Reload
BOT: Reload
BOT: Reload

[Matrix]Neo (RADIO): Negative.
Target (RADIO): Roger that.
SadBloke (RADIO): Affirmative.

source: random site found on google images

Counter-Strike (1999)
by Valve Software

Over 4,200,000 copies sold

Over 1,000,000 players playing on dedicated servers

Pro-gaming
(WCG 2009, Again takes the gold)

Based on Half-life engine

Counter-Strike (1999)
by Valve Software

SecurityFocus:

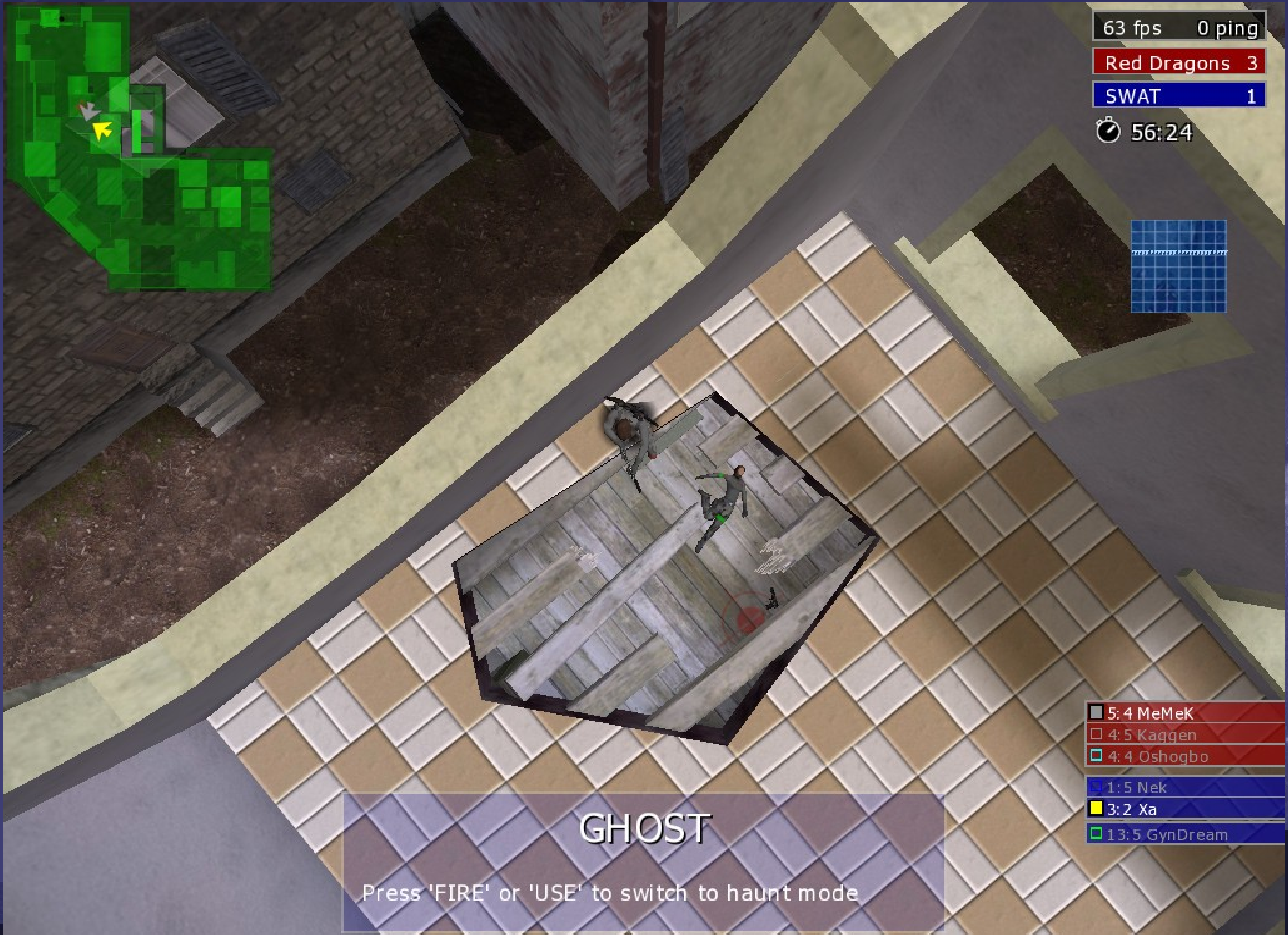
BID=2476, Halflife Map Command Buffer Overflow Vulnerability, Stanley G. Bubrouski

BID=27159, Half-Life Counter-Strike Login Denial of Service Vulnerability, Maxim Suhanov

BID=26077, Counter-Strike 1.6 Multiple Remote Vulnerabilities, Nemessis (web based? code exec, xss, info disc.)

BID=8651, HLSW RCON Console Password Disclosure Weakness, Alexander 'xaitax' Hagenah, Adrian 'p0beL' Waloschyk (plaintext)

Urban Terror (2000)
by Silicon Ice / Frozen Sand



63 fps 0 ping

Red Dragons 3

SWAT 1

56:24

■ 5: 4 MeMeK
□ 4: 5 Kaggen
□ 4: 4 Oshogbo
□ 1: 5 Nek
■ 3: 2 Xa
□ 13: 5 GynDream

GHOST

Press 'FIRE' or 'USE' to switch to haunt mode

Urban Terror (2000)
by Silicon Ice / Frozen Sand

Counter-strike-like mod for Quake 3
Running on ioQuake3 open source compilation.

Free to download and play

Over 82,000 players online on dedicated servers

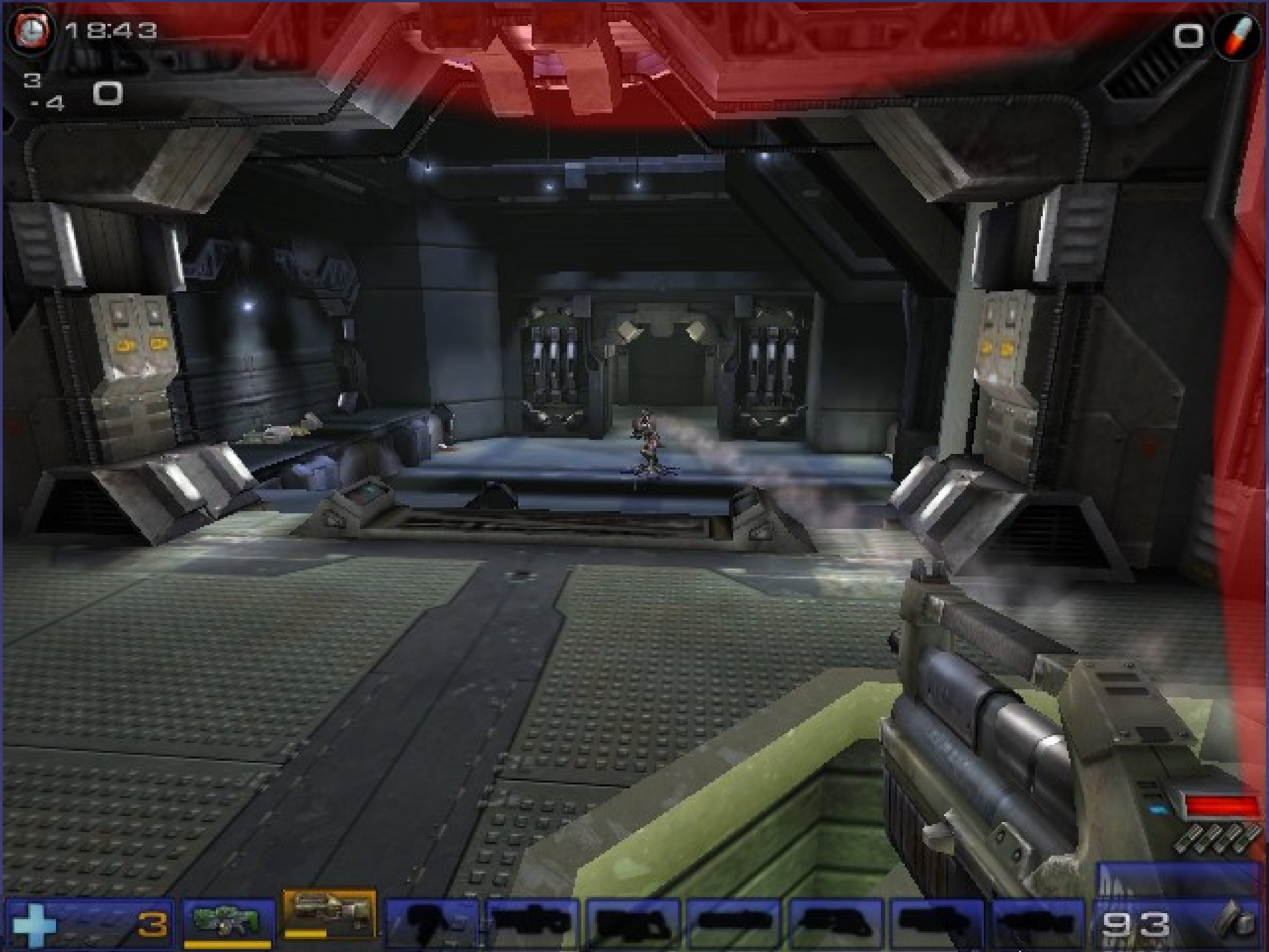
Urban Terror (2000)
by Silicon Ice / Frozen Sand

Brief testing results:

Black
Sheep
Wall

Unreal Tournament 2004

by Epic Games



Unreal Tournament 2004
by Epic Games

Over 11,000,000 copies sold

Over 13,000 players online

Unreal Tournament 2004
by Epic Games

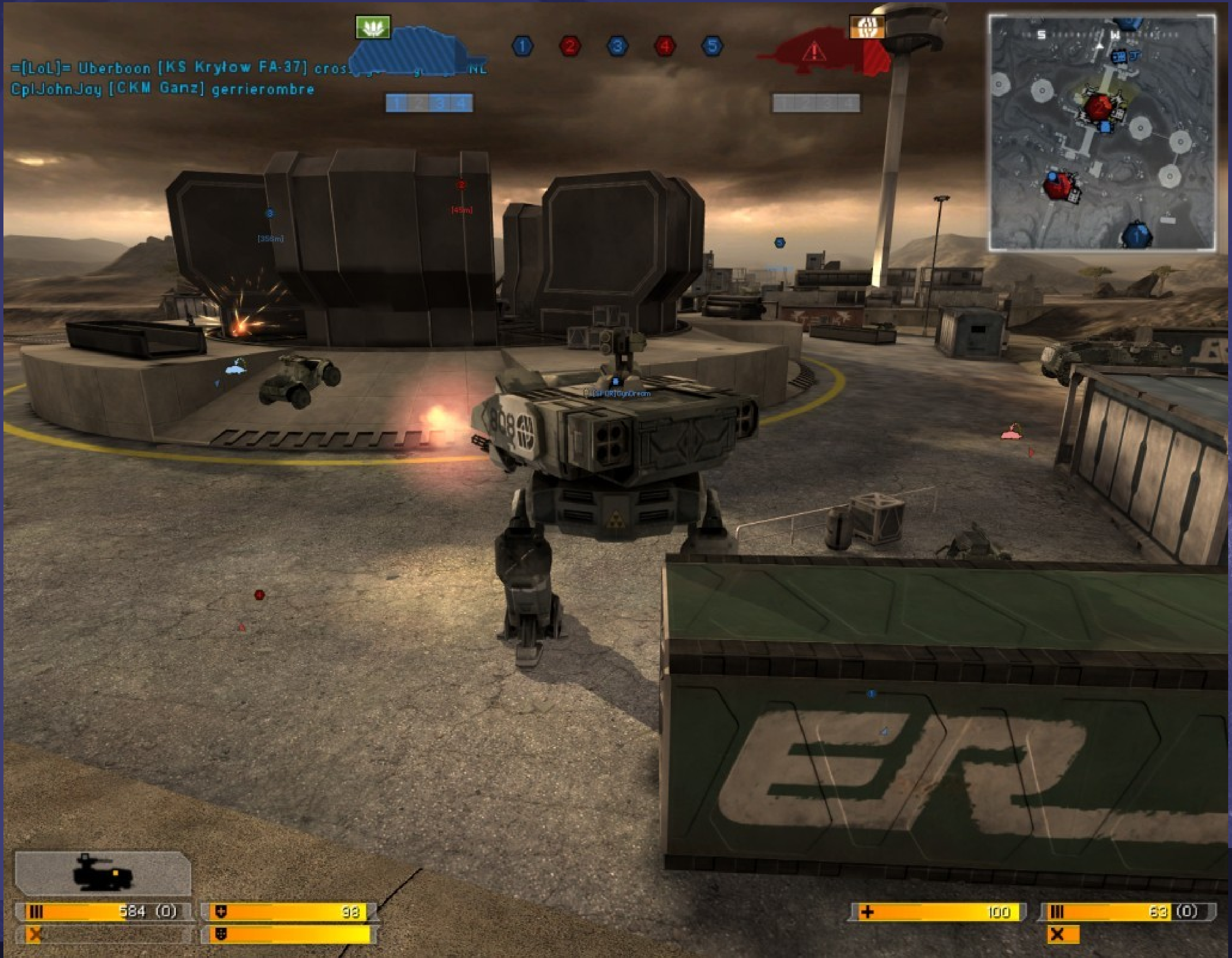
SecurityFocus:

BID=30427, Unreal Tournament 2004 NULL Pointer Remote Denial of Service Vulnerability, Luigi Auriemma

Brief test results:

black sheep wall

Battlefield 2142 (2006)
by DICE


=[LoL]= Uberboon [KS Kryłow FA-37] cros NL
CplJohnJoy [CKM Ganz] gerrierombre
1 2 3 4 5
[356m]
[45m]
S
W
584 (0)
93
100
63 (0)

Battlefield 2142 (2006)

by DICE

Over 24,000 players online

Previous version was sold in over 1,200,000 copies in 4 weeks, and over 2,200,000 in one year.

No info on this version :(

Battlefield 2142 (2006)
by DICE

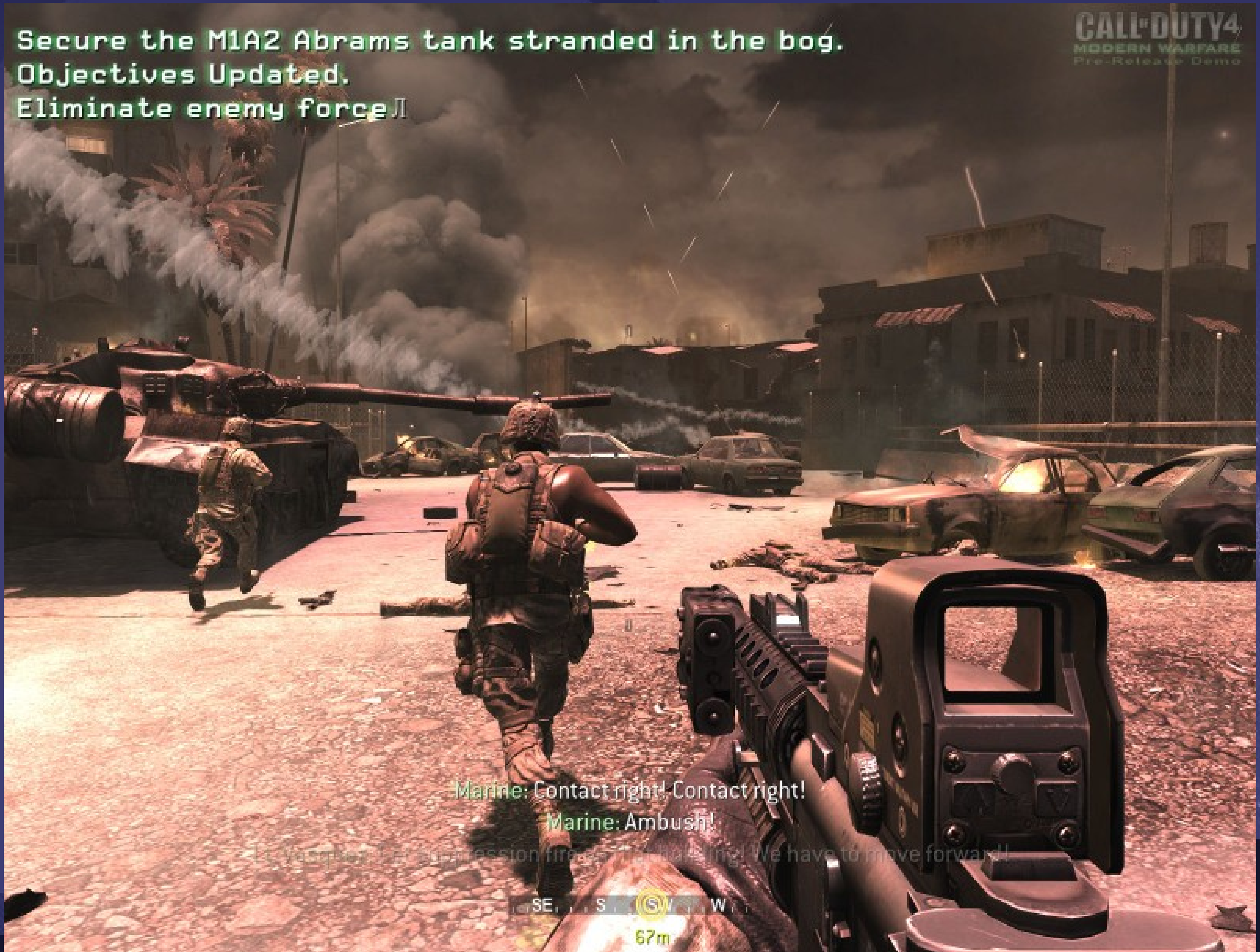
SecurityFocus:
No bugs reported.

Previous game versions:
BID=11838, Multiple Games Remote DoS Vulnerability, Luigi Auriemma

Luigi's home page:
Battlefield 2/2142 invisible Fake Players DoS 0.1.1

Brief test results:
black sheep wall

COD4 Modern Warfare (2007) by Infinity Ward



Secure the M1A2 Abrams tank stranded in the bog.
Objectives Updated.
Eliminate enemy force

Marine: Contact right! Contact right!
Marine: Ambush!
Lt. Vasquez: Get suppression fire on that building! We have to move forward!

COD4 Modern Warfare (2007)

by Infinity Ward

Over 13,000,000 copies sold

Over 10,000 players online

And… nothing reported.
Simple tests also show nothing.

COD4 Modern Warfare (2007)

by Infinity Ward

Over 13,000,000 copies sold

Over 10,000 players online

And... nothing reported.
Simple tests also show nothing.
UPDATE: there are vulns after all!

COD4 Modern Warfare (2007)

by Infinity Ward

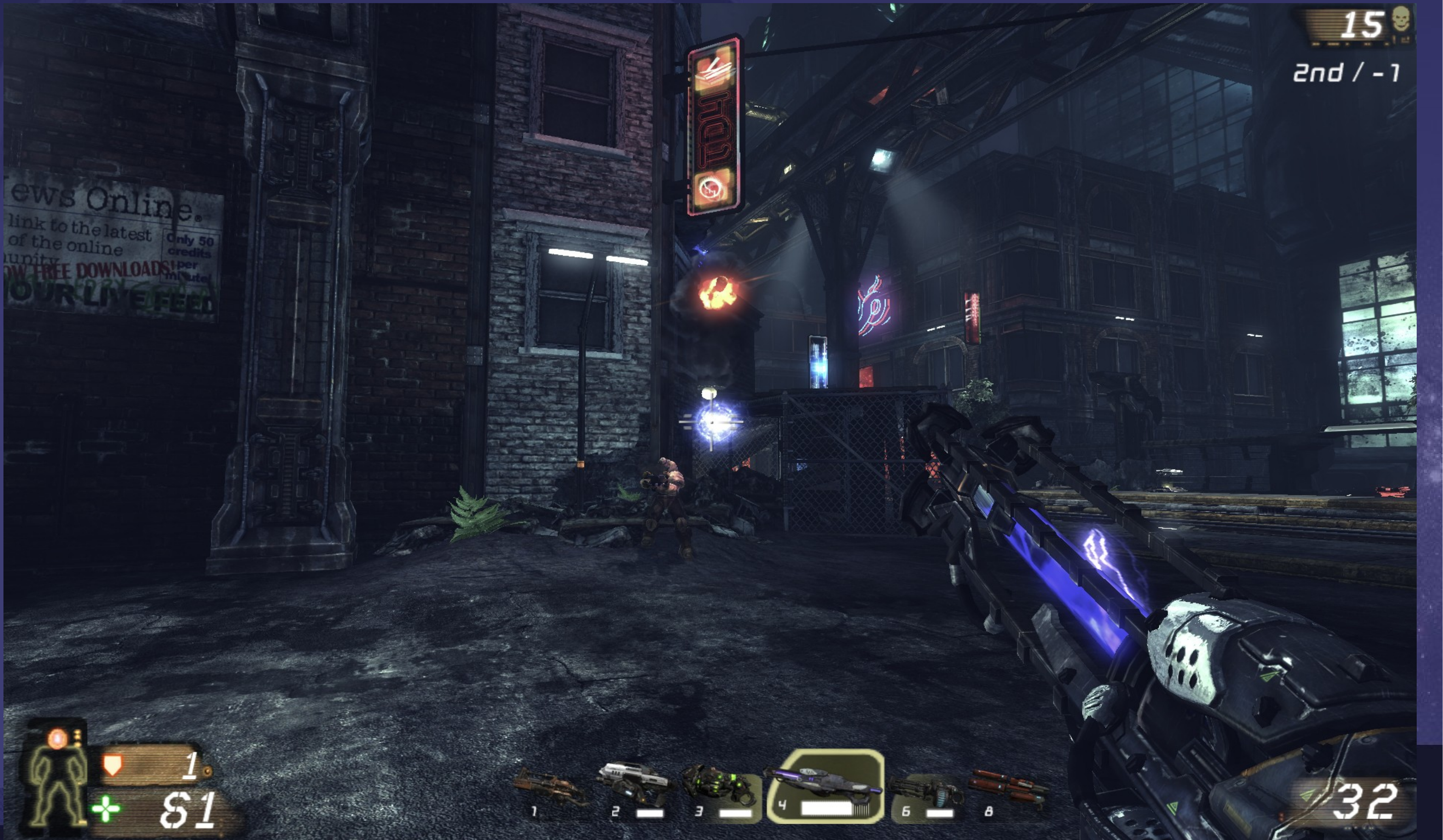
SecurityFocus:
No bugs reported.

Luigi Auriemma website (server bugs):
"Attempted to overrun string in call to va()" DoS
(this is a feature, not a bug!)

"callvote map" Denial of Service (Buffer Overflow)

remote server crash due to a memcpy() with a negative size value
(stats packet id 7)

Unreal Tournament 3 (2007) by Epic Games



Unreal Tournament 3 (2007)

by Epic Games

State of art 3D engine

Over 1,000,000 copies in 3 months

Over 7000 players online

Unreal Tournament 3 (2007)

by Epic Games

SecurityFocus:

BID=31272, Epic Games Unreal Tournament 3 UT3 WebAdmin **Directory Traversal Vulnerability (due to a “fix” in the library, INI vs ini)**, Luigi Auriemma

BID=30430, Unreal Tournament 3 Denial Of Service And Memory Corruption Vulnerabilities, Luigi Auriemma

Brief test results:

some black sheep wall

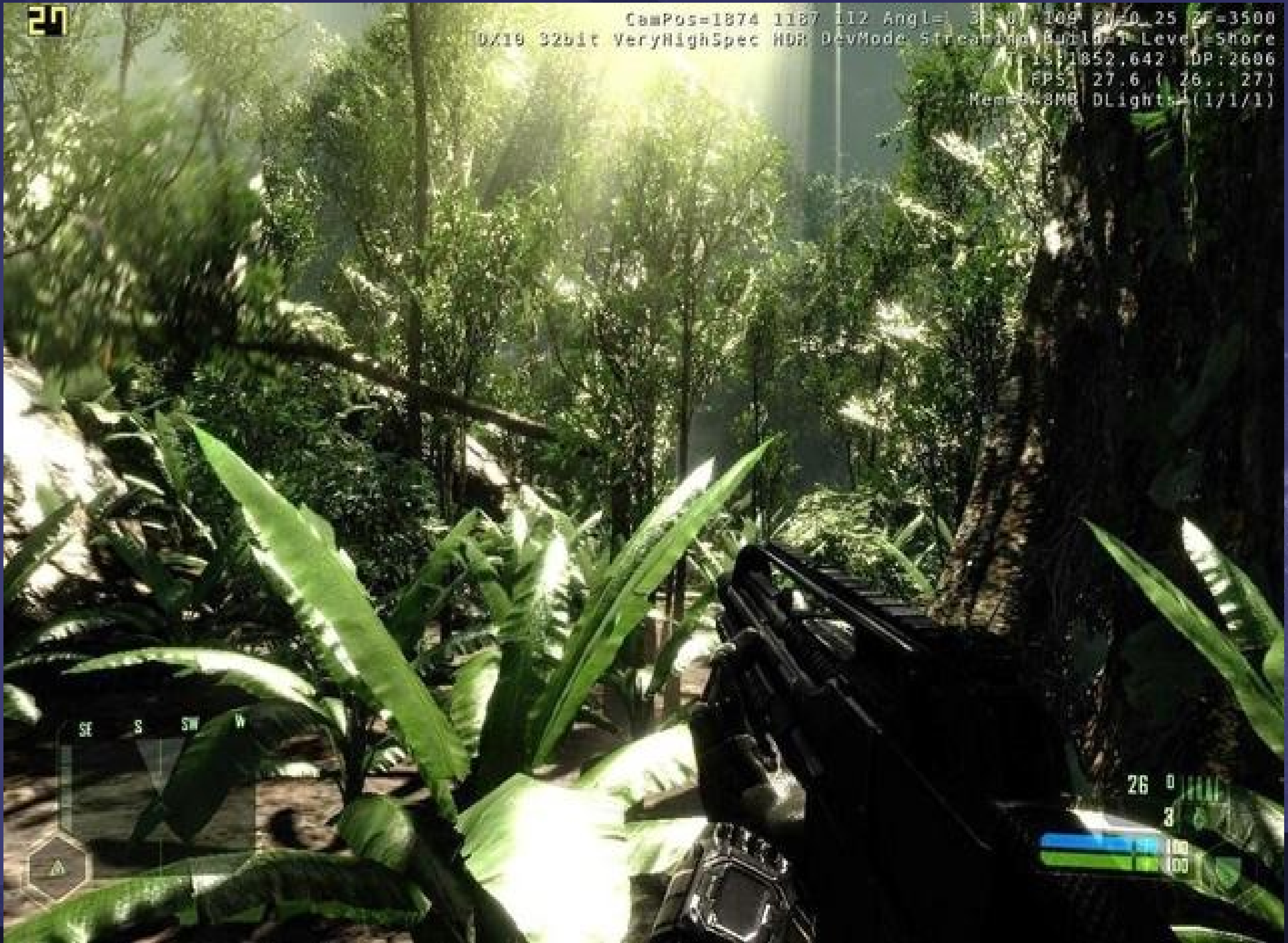
My holiday photos

My holiday photos

My holiday photos

Crysis (2007)

by Crytek



```
     CamPos=1874 1187 112 Angl=  3  0  109 ZN=0.25 ZF=3500
DX10 32bit VeryHighSpec HDR DevMode Streaming Build=1 Level=Shore
                                     T 1s:1852.642  DP:2606
                                      FPS  27.6 ( 26.. 27)
                           Mem=[illegible]8MB DLights=(1/1/1)
```

Crysis (2007)
by Crytek

State of art 3D engine

Over 1,000,000 copies in 3 months

About 1000 players online

Crysis (2007)
by Crytek

SecurityFocus:

BID=28039, **Crysis Username Format String Vulnerability,** LONGPOKE<ATOM> (_vsnprintf(4096, message); from disconnect packet error message from the user)

BID=29720, Crysis 'keyexchange' Packet Information Disclosure Vulnerability, Luigi Auriemma

BID=29759, **Crysis HTTP/XML-RPC Service Remote Denial of Service Vulnerability**, Luigi Auriemma (yes, crysis has a small HTTP server, however it's activated manually, NULL ptr, packet over 4k)

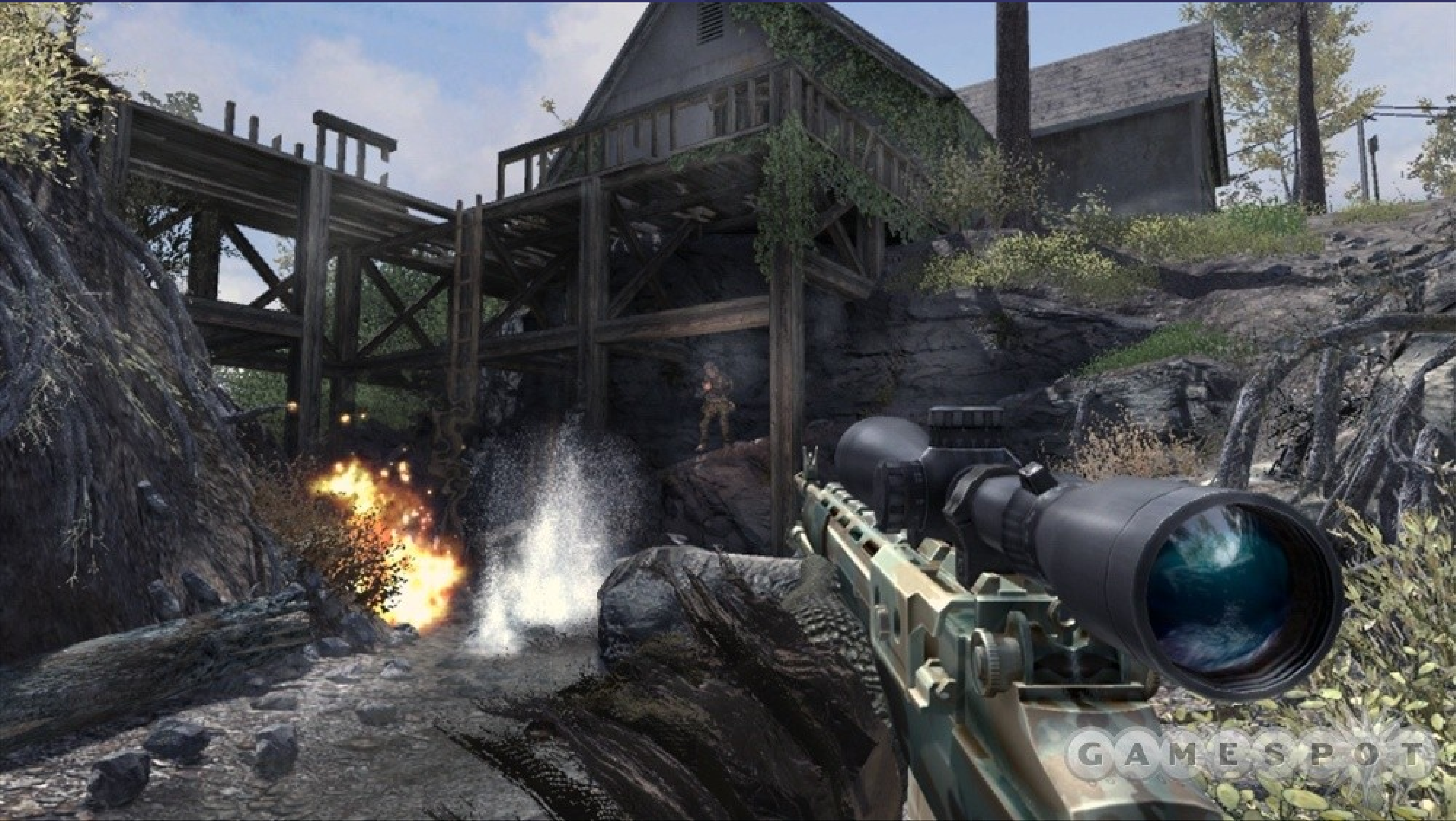
BID=35735, Crysis HTTP/XML-RPC Service Access Violation Remote Denial of Service Vulnerability, Luigi Auriemma (no params in RPC)

Crysis (2007)
by Crytek

BID=29720, Crysis 'keyexchange' Packet Information Disclosure Vulnerability
Luigi Auriemma

[...] containing a "KeyExchange1 with no connection" error message **followed by usually 16 lines of internal logs which include various real-time informations like IP addresses, nicknames and status of the clients (which so can be disconnected through spoofed disconnect packets), details about PunkBuster like paths, screenshosts, bans, checks and GUIDs of the players, status of the Gamespy SDK (stats, failed cdkey checks, communication with the master server and so on) and other plus or less sensitive informations.**

Modern Warfare 2 (2009)
by Infinity Ward



Modern Warfare 2 (2009)
by Infinity Ward

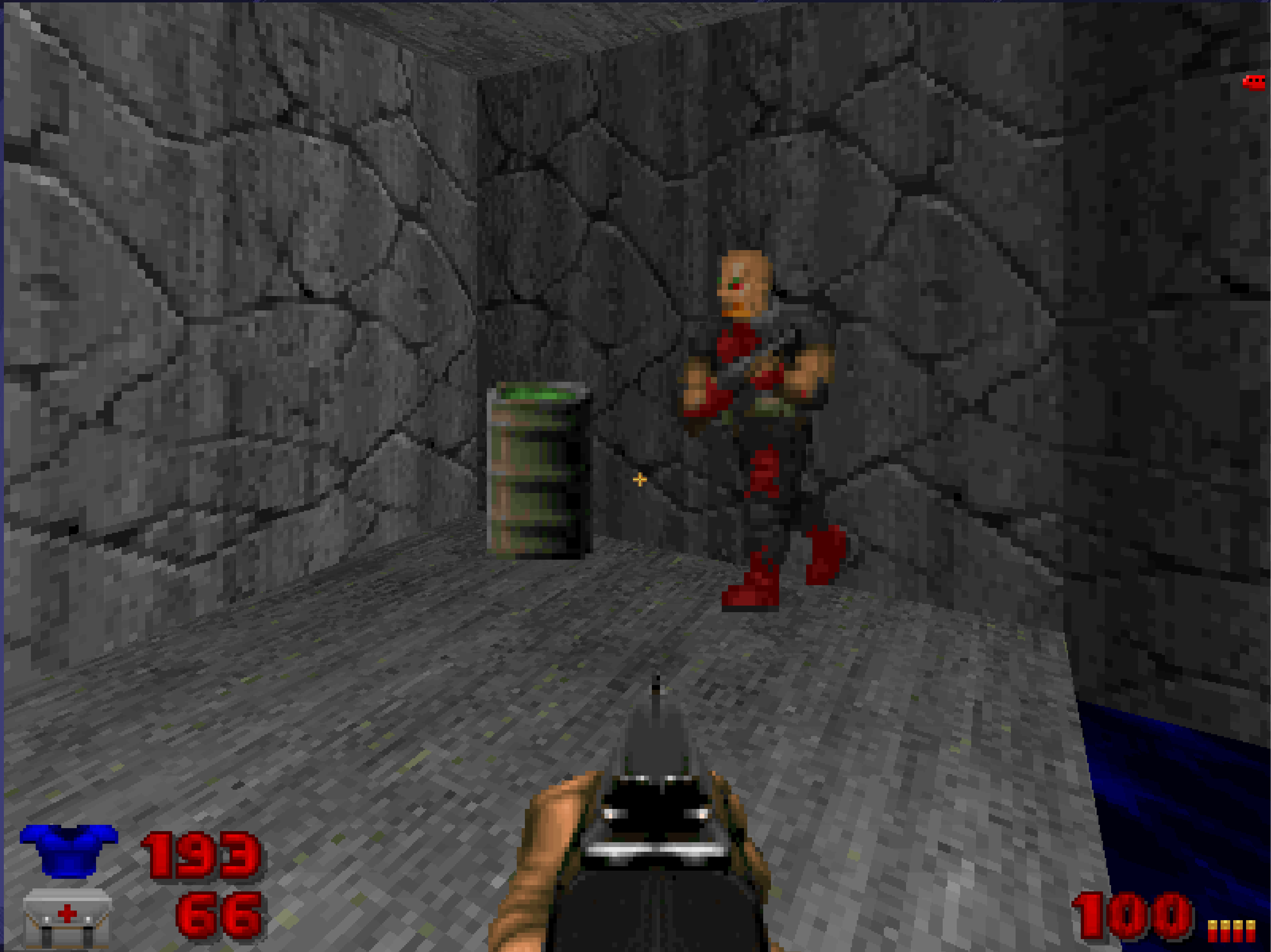
Released 9 days ago

Sold 4,700,000 copies in 24 hours

No dedicated servers

No KNOWN vulnerabilities... yet

What has changed in 15 years ?


193
66
100

What has changed in 15 years ?

Graphics and sound effects!

Security? From bad, to worse

Best vector of attacks:

1. data file loaders:

- images
- sounds
- 3D models
- maps
- packfiles
- save games
- replays

Best vector of attacks:

Standard web browser / VM language like stuff - look for things the programmer was to lazy (or he put too much trust in the docs) to check.

Best vector of attacks:

2. network protocols

- player to player
- player to master server
- player to game host
- player to resource host
- player to update host

both UDP and TCP

Best vector of attacks:

3. scripting engines

- API
- VM

Best vector of attacks:

4. player
- custom_skins.zip.exe
- patch_1_45.exe
- wallhack.exe

There are several million players out there.

Wonder when the malware (zombie/worm) community will start to get interested in them (in another way then stealing tibia accounts ;p)

Thank you for your attention

Questions?

e-mail: gynvael@coldwind.pl
blog: http://gynvael.coldwind.pl