

# Video Game Hacking Presentations

# The History of Garry's Mod Hacking

- Garry's Mod is a multiplayer sandbox modification for Half Life 2
- The primary focus was on building stuff. [Example](#)
- Released for free between 2004-2005.
- Version 9 added Lua support.
- In 2006 a paid version was released on Steam: Gmod 10
- Developed by a weird British guy called Garry Newman.
- His company is called Facepunch.
- His Forum is also called Facepunch.

# Early “Lua Viruses”

There have been a number of “Lua Viruses” over the years.

Example: “Chrisaster Bindtoggle Exploit” circa 2006-2009

- Used malicious servers with spoofed player counts to infect players.
- Overrode movement commands to make players say “CHRISASTER IS AWESOME!”
- Overrode menu commands so players could not exit the server easily.
- Used the `host_writeconfig` command to make changes permanent.
- Kept a public log of infected users & IPs:  
<http://download.chrisaster.com/garrysmod/ownedlog.txt>
- Several variations/copycats appeared over the years.

I found my username on the list three times. I was not a smart child.

DrogenViech - 87.122.183.211:61371 - STEAM\_0:0:8615861

\*BIOG\*Mad-Parakeet - 72.175.70.12:27005 - STEAM\_0:1:18839805

W33Dman6 - 67.181.62.103:27005 - STEAM\_0:0:8298169

\*BIOG\*Mad-Parakeet - 72.175.70.12:27005 - STEAM\_0:1:18839805

W33Dman6 - 67.181.62.103:27005 - STEAM\_0:0:8298169

[ Â°rzÂ« ]Rippin Rocket - 72.197.237.233:6430 - STEAM\_0:1:17971248

The pie maker - 71.170.63.55:27005 - STEAM\_0:1:20304421

\*BIOG\*Mad-Parakeet - 72.175.70.12:27005 - STEAM\_0:1:18839805

sTo??d WhiTe Boy - 97.127.8.185:53208 - STEAM\_0:1:11771144

# Early “Lua Viruses” (Continued)

Example: "Noxius Trolls" (circa 2008)

- Added payload to end of lua scripts using the following command:
  - `RunConsoleCommand("con_logfile","/lua/autorun/HAX.lua")`
- Later improved to circumvent console command filtering:
  - `RunConsoleCommand("con_logfile\t","/lua/autorun/HAX.lua")`

*Found by Facepunch user aVoN.*

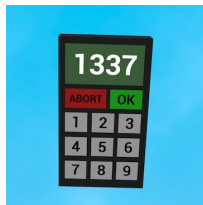


# Seth

- Seth's Diamond Build (2009-2012)
- Sold "SethHack", his Gmod Cheat.
- Banned from Steam for having porn on his profile.
- Also sold a SteamID spoofing tool called "Serenity".
- The Seth-Facepunch War (2012)
  - Sethhack manually blocked by Garry.
  - Sethhack source leaked: <https://github.com/hakusaro/Sethhack>
  - Facepunch was DDOSed many times.
- Evidently arrested in 2013 for the Spamhaus DDOS, among other things.

# In-Game Exploits

- Lag/DoS: More than you can count.
- E2 Keypad “Hackers”



- Wiremod Nailer Exploit
- DarkRP Money Stealers
- Countless Other Greifing E2 Scripts
  - Balls of Steel <https://www.youtube.com/watch?v=L-sXVM0ijYk>
  - Hologram Blinders
  - Turrets
  - Teleporting Cages

# In-Game Exploits (Continued)

## Herpes E2 Virus (2016)

- Flies in front of users trying to use the duplicator tool.
- When a user copies + pastes the E2, it starts running console commands and attempts to infect other players.
- Another user wrote an “antivirus”, also in E2 form.





# Lua Script Stealing

Why stop at stealing contraptions and E2s?

- Scan the files of developers who join your server.
- You can steal a server's clientside files -- they send them to you, after all.
- Using exploits, could read any file on a server.
  - Use it to steal serverside lua!
  - Use it to steal config files!
    - Guess what the config files had in them?
    - Willox (we'll talk more about him later) claims to have done this to Valve's official TF2 servers.
  - This exploit has been patched. Probably.



# Addon Vulnerabilities: NAN Injection (2015)

- The Lua function `tonumber` parses strings and converts them to numbers.
- Pretty standard, right?
- Guess what it does with the string “nan”?



# Addon Vulnerabilities: NAN Injection (2015)

## (Continued)

We get the floating point “Not a Number” value. AKA the result of 0/0.

It has some fun properties!

$x + \text{NaN} = \text{NaN}$        $\text{NaN} \neq x$       *(Every other comparison is always false!)*

$x - \text{NaN} = \text{NaN}$        $\text{NaN} \neq \text{NaN}$       *(This is my favorite!)*

$x * \text{NaN} = \text{NaN}$

$x / \text{NaN} = \text{NaN}$



# Addon Vulnerabilities: NAN Injection (2015) (Continued)

It shouldn't come as a surprise that most mods aren't coded to deal with this insanity.

Example:

```
concommand.Add("dropmoney", function(p,_,s)
    local amount = tonumber(s);
    if(amount <= 0) then return; end
    if(p:GetMoney() < amount) then return; end

    p:SetMoney(p:GetMoney() - amount);

    CreateMoneyEntity(amount):SetPos(p:GetEyeTrace().HitPos));
end);
```

Credit: Meep



# Addon Vulnerabilities: Bad Net Messages

- Some addons will manually write the sender into their network messages.
- There is no way to verify that this is the actual sender.

```
sc_input.OnEnter = function( self )  
    net.Start( "sc_verify" )  
    net.WriteString( self:GetValue() )  
    net.WriteEntity(LocalPlayer())  
    net.SendToServer()  
end
```

```
net.Receive( "sc_verify", function(len)  
    local a = net.ReadString()  
    local b = net.ReadEntity()  
    print(a) -- works  
    print(b:Nick()) -- doesn't work  
    b:Kill() -- same here  
end
```

- Falco's linter actually warns about this.

# Backdoored Addons

Why find vulnerabilities when we can make our addons vulnerable from the start?

There are a lot of these. I'll talk about the more famous cases.

These are particularly scary because Steam Workshop addons can be updated at any time. Users have no choice but to update.




# Backdoored Addons (Continued)

## GFireworks (2015)

- Backdoored and banned a number of times.
- The developer left a “debug command” in his mod.
- Had his fans spam a moderator’s profile when his addon was banned.
- Later versions of his addons had a “permanent wall of shame” included.

This was such an extreme shitfest that later backdoors were jokingly called “baldursgate3 approved”.



# Backdoored Addons (Continued)

## NeuroTec (2016)

- A fairly reputable developers added invisible web advertisements to his addon.
- Some of these invisible ads had very loud audio!
- Nothing has been heard from the developer since this was exposed.

Nobody (that we know of) has figured out how to mine bitcoin with a gmod addon yet, but we're trying to get WebGL and custom shaders added to the game. I strongly suspect either would be abused for this purpose.

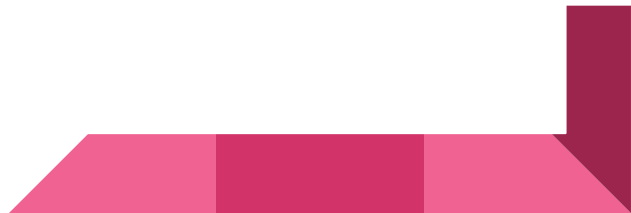




# Anti-Backdoor Efforts

There have actually been some community efforts to curb these.


- Almost weekly threads exposing some backdoor.
- A number of scanning tools exist.
- The “download everything and grep through it” strategy.



# Social Engineering

Writing a good addon to backdoor is too hard, and so is finding exploits!

The plan:

1. Pretend to be a developer.
  2. Offer to “develop” for servers for free.
  3. Install the malicious addon your “hacker friend” wrote.
  4. Get booted from the “development team” because you can’t actually code.
  5. Raid the server with your friends, using the backdoor you uploaded to do mean stuff.
- 

# Paid Addon DRM

*(AKA: Proof that this is the darkest timeline.)*

- Yes, people pay money for Gmod scripts.
  - <https://www.gmodstore.com>
- Naturally people also pirate Gmod scripts.
  - <https://nulledbb.com/forum-Garry-s-Mod-Leaks>
- The solution is obviously DRM: ScriptEnforcer
  - This ended **BADLY!**



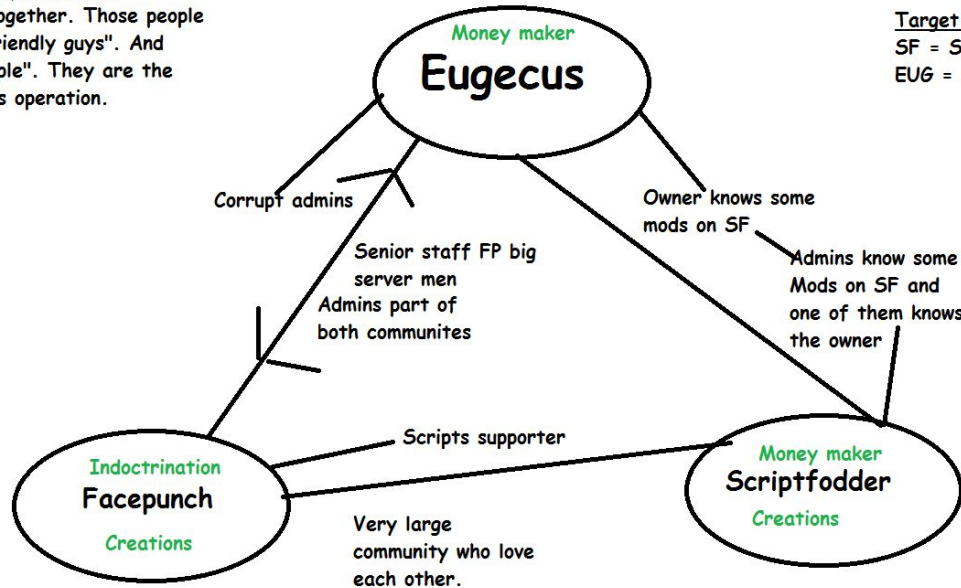
# Paid Addon DRM (Continued)

Alternatively, upload backdoored versions of your addons and post the keys in the glua chat!



# The Serverwatch Conspiracy (2015)

There is a "hive mentality" shown between the people who are connected all together. Those people you know as "friendly guys". And "big server people". They are the ones behind this operation.



£\$\$\$

Target markets

SF = Server owners

EUG = Server players

# The Serverwatch Conspiracy (2015)

Facepunch's response was overwhelming.

<https://steamcommunity.com/groups/BigServerMen>

<https://www.youtube.com/watch?v=YfwXytoVYVs>



# More Spoofing

- At one point the Source Engine only validated commands based on IP.
- You can spoof your IP in the UDP header.
- Voice communications are (were?) peer-to-peer, so an admin's IP could be obtained by intercepting voice packets.
- This could be used to submit commands as an admin.
- Admin mods were updated to add a second stage of authentication.



# More Spoofing (Continued)

Both of our boys weigh in on the subject:

6th March 2011

**Chrisaster**

IS

AWESOME@@@@@@@@

Packet spoofing.

6th March 2011

**^seth**

Lolololololoooooooooooo! La  
la la-laaaaaaaaaaaaah, la la  
laaaaaah, lol, haha.

Good job trying to remove the one bit of fun left in this game that's been ruined by whitehat scum such as yourself.



# More Spoofing (Continued)

- In 2016, FP user Leystryku found a new exploit that allowed users to spoof their SteamIDs.
  - “This spoofing affects all steam products.”
- This was mainly used to impersonate Garry for a few weeks.

”So how do I abuse this to get massive hacker cred with the skiddies by making Serenity 2.0?”

- Totally Not Me, 2016



# Hex & Hex Anti-Cheat


- There was a guy called Hex who really hated cheaters.
  - Like, he really hated them.
- So he coded an anti-cheat. (HAC)
- You have a few options when you detect cheaters.
  - You could just ban them...
  - Or you could make it entertaining...



# Hex & Hex Anti-Cheat (Continued)


- Turn hackers into fireworks.
- Record it every single time it happens.
- <https://www.youtube.com/watch?v=YM1lj2CrjHI>
- Evidently he also had some kind of physical alarm in his house that would go off every time a cheater was banned.

It doesn't stop there!

- Delete their settings.
  - Delete their files.
  - Do more malicious stuff???
- 

# Hex & Hex Anti-Cheat (Continued)

HAC was eventually released. The release page is no longer up, but it was incredibly complex.

- Required a large number of binary modules.
  - “The documentation is 11 pages long, and it's a rough documentation.” - Some Dude on FP
  - “Mac users have different fonts. Make sure to test on Mac OS - OR IT WILL BAN ALL MAC USERS!” - The Readme
  - “READ ALL THE CODE before you even attempt to start it up. Understand how it works.” - Also The Readme
- 

# Hex & Hex Anti-Cheat (Continued)

SkidCheck was Hex's giant, public list of 40,000+ "cheaters".

- Users could be added for being a member of certain Steam groups, downloading certain addons, or being VAC banned in a different game.
- Falco - developer of DarkRP - was added to it, so he decided to disable SkidCheck in DarkRP.

```
113 + -- Malicious addons that kicks players this one person doesn't like.  
114 + if Skid then  
115 +     Skid.Check = fn.Id
```



**Shigbeard** on Aug 30, 2015

Contributor

what even is fn.Id?



**FPTje** via email on Aug 30, 2015

Owner

The identity function

# Screen Grabbing

- The lua function `render.Capture` can be used to take a screenshot.
- The screenshot can then be uploaded to a server, without the player's knowledge.
- It used to capture the Steam UI, so Steam chats and browser windows could be spied on.
- Evidently used by some anticheats.



# How many exploits can I cram into this presentation?

MeepDarknessM  
glua.team



July 2013  
1,594 Posts






```
net.Receive("weapon_smg1", function()
  net.ReadUInt(-0x7fffffff)
  net.ReadUInt(32)
end)

net.Start "weapon_smg1"
net.SendToServer()
```

this also allows memory reading sorta  
© 2016-2017 glua.team

# How many exploits can I cram into this presentation?

1st June 2015

**Willox**  
Willox said I can put anything in here, so I've put "meow"  
  
December 2009  
2,971 Posts  
 

**meharryp posted:**

I assume you could do something like this:

```
CreateConVar( "cv=G", 0 )  
CreateConVar( "cv.print(\"\\\"while(true)do\", 0 )  
CreateConVar( "cv.print(\"\\\"end\", 0 )
```

Then do RunConsoleCommand( "cvarlist cv log lua/autorun/crash.lua" ) and break singleplayer for whoever you run it on.

Write executable file to data/two.txt with file.Write.




Create Convars:




```
"cv1" => "<script>console.log( 'RUNLUA: OpenFolder[[data/one.bat]]' );</script>"  
"cv2" => "<script>console.log( 'RUNLUA: OpenFolder[[data/two.exe]]' );</script>"  
"cv3" => "x!Arename data/two.txt two.exe\x!A"
```

Dump cv3 to data/two.txt with cvarlist.

Dump cv1 to menu/menu.html with cvarlist so that the html/javascript/lua is executed, internally using ShellExecute from the Windows C API and - via one.bat - renaming data/two.txt to data/two.exe (once the menu is reloaded via the "menu\_reload" concommand).

Dump cv2 to menu/menu.html, so that reloading it with "menu\_reload" causes two.exe to be executed.

 Winner x 8  Informative x 1  Funny x 1 (list)



# How many exploits can I cram into this presentation?

There are probably a few dozen other serious vulnerabilities found by Willox, Leystryku, and others over the past few years.

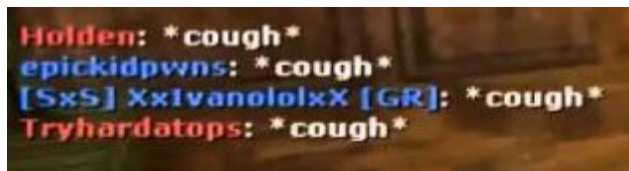
These usually involve memory corruption, or some kind of failure on a filter that allows arbitrary writing to files.

It's worth noting that many of them affected all source games, not just Gmod.

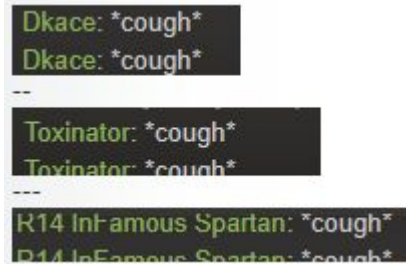


# \*Cough\* \*Cough\* (2014)

- These exploits are pretty cool.
- So how about an actual virus?



Holden: \*cough\*  
epickidpwns: \*cough\*  
[SxS] XxIvanololxX [GR]: \*cough\*  
Tryhardatops: \*cough\*



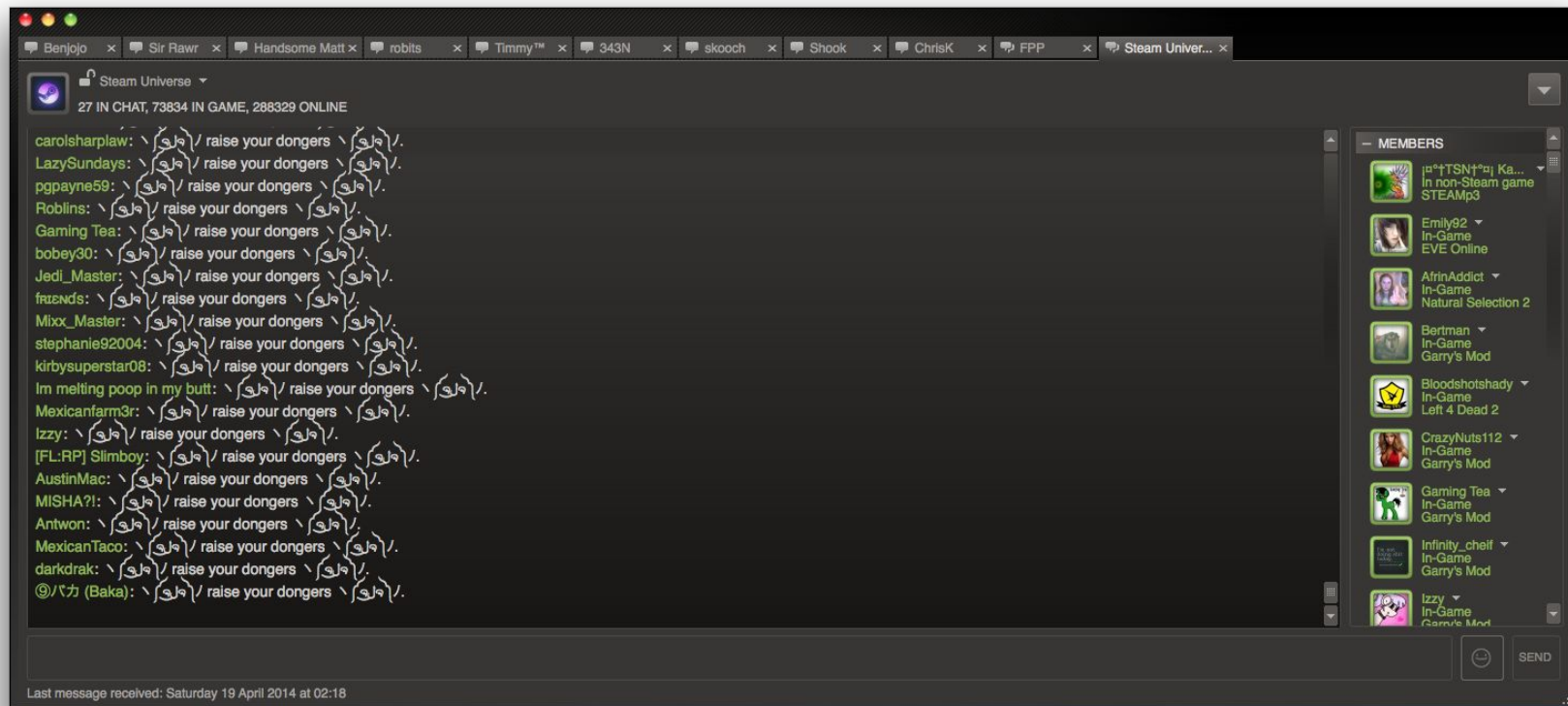
Dkace: \*cough\*  
Dkace: \*cough\*  
---  
Toxinator: \*cough\*  
Toxinator: \*cough\*  
---  
R14 Infamous Spartan: \*cough\*  
R14 Infamous Spartan: \*cough\*



/Winy! Scratch: \*cough\*  
rhmontg: \*cough\*  
/Winy! Scratch: \*cough\*  
rhmontg: \*cough\*  
/Winy! Scratch: \*cough\*  
rhmontg: \*cough\*  
/Winy! Scratch: \*cough\*  
rhmontg: \*cough\*  
/Winy! Scratch: \*cough\*  
rhmontg: \*cough\*



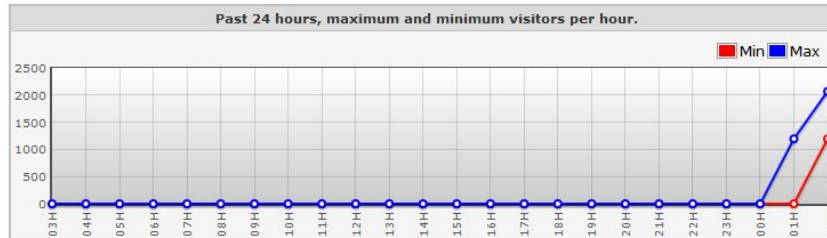
# \*Cough\* \*Cough\* (2014)



# \*Cough\* \*Cough\* (2014)

!!!AsylumZMOD - Minimum Downloads   AsylumCentral.com#	Z_mod	0 / 64
!!!Axis Gaming M9K Weapons   30+ Jobs   Fast DL#	DarkRP	18 / 64
!!!Bill's Sandbox: M9K, WAC, PVP, TDM Cars#	Sandbox	4 / 32
!!!Black Lemon Custom TTT (Pointshop + Rainbow Lazer, etc)#	Trouble in Terrorist T...	0 / 22
!!!Bluemooingaming.enjin.com MPF Needed, Need Staff, NEW, Helpfu	CW: HL2 RP	2 / 15
!!!Bonghits' TTT Server Pointshop Pineapples Cool T Weapons Bet	Trouble in Terrorist T...	11 / 25
!!!Bricksters Sandbox [m9k/tdmcsars]#	Sandbox	5 / 15
!!!Broom Closet Gaming   Sandbox#	Sandbox	9 / 10
!!!Build/Chill/Kill ACF Wire+Extras FA:S Weps SProps TDM#	Sandbox	0 / 16
!!!Centralia - Wirebuild#	Sandbox	0 / 20
!!!Centrifugal  Cinema M9K 20+Printers Lots Of Jobs ATM's Bank	DarkRP	8 / 64
!!!Cervidae TTT#	Trouble in Terrorist T...	0 / 16
!!!Chamb's TTT Server   Fast DL   Jihad   One-Hit Knife#	Trouble in Terrorist T...	4 / 30
!!!Chernobyl Advanced Build Mature Only. Custom ACF/Sprops/Wire	Sandbox	1 / 100
!!!Ciber's Custom Murder Server ~ 24/7 Levels PointShop More Lo	Murder	4 / 18
!!!Clock Town Gaming    PH [Chicago-Vanilla]#	Prop Hunt	0 / 20
!!!ClockworkDR AutoJump Redie ThirdPerson Coinshop FastDL! #	Deathrun	7 / 24
!!!CommunismRP[tdmcars][drugs][40jobs]#	DarkRP	2 / 16

# \*Cough\* \*Cough\* (2014)



# \*Cough\* \*Cough\* (2014)

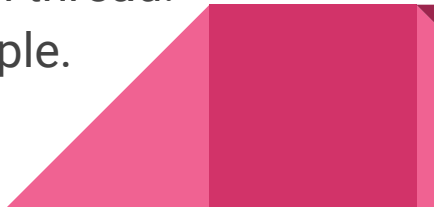
So what exactly was it?

- A virus that could spread bidirectionally (Client  $\rightarrow$  Server and Server  $\rightarrow$  Client)
- Leveraged an exploit in the source engine.
- Only targeted Windows machines.
- Not really malicious.



# \*Cough\* \*Cough\* (2014)

## Features

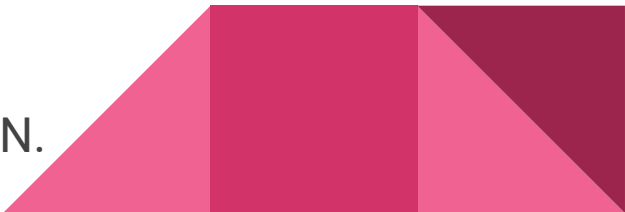
- Live updating via a Github Gist.
  - Spammed steam chats + ingame chats with “\*cough\*” and “FIX IT VINH”.
  - Map of infected users.
  - Forced voice transmission on.
  - Displayed a picture of “VINH”.
  - Set user’s Steam name to “VINH’L FIX IT!”
  - Artificially inflated the guest counter of its own forum thread.
  - Sent friend requests to some seemingly random people.
  - Prefixed server name with “!!!” to make it sort first.
  - Designed to stop working after a day.
- 

# \*Cough\* \*Cough\* (2014)

## How it Worked

- It turns out you could not only read arbitrary files, but also write them.
- You just had to bypass a filter!

## Client

1. Client downloads “cfg/server.cfg\n.txt”.
  2. Client parses server’s RCON password.
  3. Client enables file uploads via RCON.
  4. Client uploads “gmsv\_engine\_windows.dll\n.txt”
  5. Client makes the server execute the payload via RCON.
- 



# \*Cough\* \*Cough\* (2014)

How it Worked

## Server

1. Server sends “game\_shader\_generic\_engine.dll\n.txt” to all clients.
  2. Crash clients so they restart the game and load the payload.
- Described by Handsome Matt, who was actually probably responsible for this, with the exploit provided by Willox.

# \*Cough\* \*Cough\* (2014)

Patched within a few hours by Garry.

Will be remembered forever.

```
1  --[[
2      Copyright Mr. 'Handsome' Matt ©
3  ]]
4
5  -- Steam Wallet Currency is NOT being stolen pls believe
6  -- Source Code to DLLs will be publically released here after the Garry's Mod patch along with binaries which, if you are really worried,
7
8  -- Infected lawl
9  -- Probably more than 30,000 infections
10 -- This could have been silent
11 -- Once spammed, this script will stop working by itself
12 -- sv_allowupload is not required to be enabled on the server, as rcon access allows it to be set
```

# The End

There's more I could talk about but I'm sure we all have better things to do.

