

Beware of Fake 7zip Installer: upStage Proxy

 blog.lukeacha.com/2026/01/beware-of-fake-7zip-installer-upstage.html

Luke Acha

January 24, 2026



Over the past couple weeks [analysts have been looking](#) at a suspicious 7zip installer which turns the host into a residential proxy (proxyware). I'm playfully calling this upStage Proxy (with a heroquest boardgame theme). More on the name will become clear in this article.

The installer comes from 7zip[.]com, which, while looking professional, and having been around for quite some time, is in fact not the official site for the 7zip tool. The official site is 7-zip.org.

**Update February 10, 2026: At this time the download link is now pointing to the official 7-zip.org download.*

The installer is signed by (now revoked) certificate:

"JOZEAL NETWORK TECHNOLOGY CO., LIMITED". The installer drops a version of [7zfm.exe](#) that is also signed with this signer.

This version of 7zfm.exe differs from the official build in an important way, it has embedded within it 3 files ([upHreo.exe](#), [hero.exe](#), and [hero.dll](#)).



Download

Download 7-Zip 25.01 (2025-08-03) for Windows:

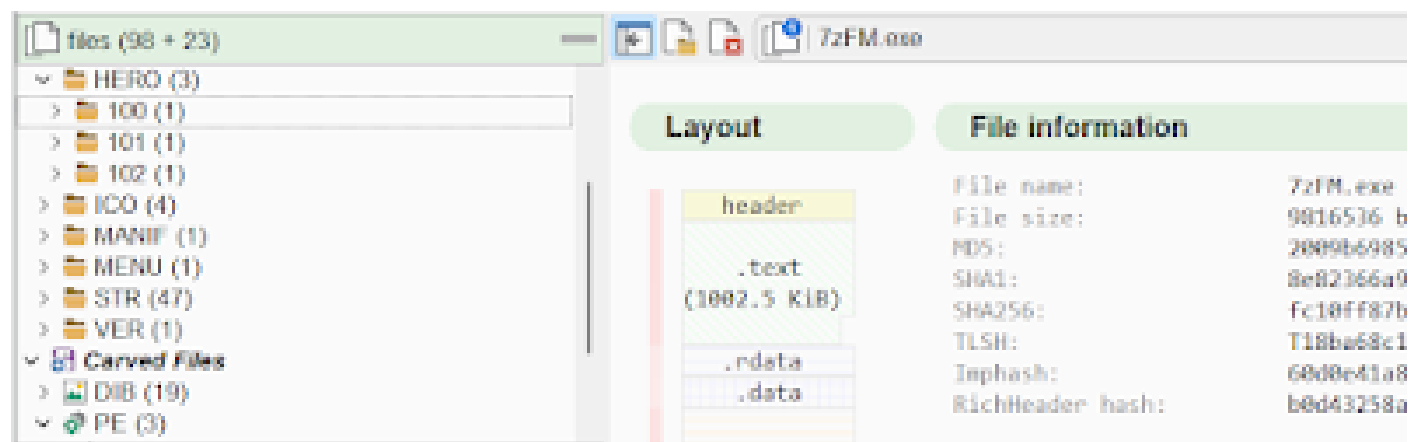
Link	Type	System
Download	.exe	64-bit Windows x64
Download	.exe	32-bit Windows x86
Download	.exe	64-bit Windows arm64
Download	.msi	64-bit Windows x64
Download	.msi	32-bit Windows x86
Download	.7z	Windows x86 / x64
https://update.7zip.cloud/7zipinstall.exe	.ar.xz	64-bit Linux x86-64

Analysis of this has been interesting, the main payloads are Go compiled binaries, which are dropped in C:\Windows\SysWOW64\hero.

upHero.exe appears to "upStage" hero.exe (which loads hero.dll), by punching a hole in the windows firewall for hero.

hero.exe is run and installed as a service on the machine, and cycles through multiple domains which have patterns like smshero before finally making direct IP connections to ports 1000 or 1002 (observed at the time of this writing).

Another interesting aspect of this is some relations to wirevpn, isharkvpn, and embedded strings related to many other samples. A pivot on a [YARA rule](#) I built will find many of these interesting binaries with commons string structures.



Even more interesting is how little attention this has received at the time of this writing. Most of the initial public analysis has been by myself, [s1dhy](#), and [Andrew Danis](#).

There are a couple good sandbox runs of this: Including [app.any.run](#), and [joe sandbox](#). More recently, Japanese researchers have begun to notice this: [Qiita](#) and [WizSafe Security](#) have some writeups on this.

Some of the biggest breakthroughs in understanding this suspicious behavior come from s1dhy who shared a [script](#), and [screenshots](#) to demonstrate how hero pulls it's config to connect to the direct IP:PORT.

While I was analyzing the traffic PCAPs from multiple systems, it became clear to me that these are not VPN connections, the protocols don't match up, and there was repeated characters and some clear text. I began to suspect a custom http communications was being employed. I quickly recognized what looks like XOR encoding in some of the payload and was reward with uncovering multiple domains when applying XOR key 70.

435	236.768083	84.17.37.1	192.168.1.2	TCP	66 1802 → 49716 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM WS=2048
436	236.768246	192.168.1.2	84.17.37.1	TCP	54 49716 → 1802 [ACK] Seq=1 Ack=1 Win=65536 Len=0
437	236.768438	192.168.1.2	84.17.37.1	TCP	60 49716 → 1802 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=6
438	237.007881	84.17.37.1	192.168.1.2	TCP	54 1802 → 49716 [ACK] Seq=1 Ack=7 Win=43808 Len=0
439	237.007918	84.17.37.1	192.168.1.2	TCP	221 1802 → 49716 [PSH, ACK] Seq=1 Ack=7 Win=43808 Len=167
440	237.072058	192.168.1.2	84.17.37.1	TCP	54 49716 → 1802 [ACK] Seq=7 Ack=168 Win=65280 Len=0
441	237.173154	192.168.1.2	84.17.37.1	TCP	1514 49716 → 1802 [ACK] Seq=7 Ack=168 Win=65280 Len=1460
442	237.173162	192.168.1.2	84.17.37.1	TCP	1514 49716 → 1802 [ACK] Seq=1467 Ack=168 Win=65280 Len=1460
443	237.173166	192.168.1.2	84.17.37.1	TCP	1230 49716 → 1802 [PSH, ACK] Seq=2927 Ack=168 Win=65280 Len=1176
444	237.175156	192.168.1.2	84.17.37.1	TCP	768 49716 → 1802 [PSH, ACK] Seq=4103 Ack=168 Win=65280 Len=714
445	237.419574	84.17.37.1	192.168.1.2	TCP	54 1802 → 49716 [ACK] Seq=168 Ack=2927 Win=43808 Len=0
446	237.428684	84.17.37.1	192.168.1.2	TCP	54 1802 → 49716 [ACK] Seq=168 Ack=4817 Win=43808 Len=0

se 441: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0, Ethernet II, Src: Intel_62:e5:74 (00:15:17:62:e5:74), Dst: a0:82:50:2f:2c:b2 (a0:82:50:2f:2c:b2), Internet Protocol Version 4, Src: 192.168.1.2, Dst: 84.17.37.1, Transmission Control Protocol, Src Port: 49716, Dst Port: 1802, Seq: 7, Ack: 168, Len: 1460 (bytes)

```

0000 a0 82 50 2f 2c b2 00 15 17 62 e5 74 00 00 45 00  --P/-...-b-t-t-E-
0010 05 dc 39 5b 00 00 80 06 c1 04 c0 a8 01 02 54 11  --9[.....T-
0020 25 01 c2 34 03 ea 36 dd 8e 57 27 fd 4f 81 50 10  %-4-6-W'-O-P-
0030 00 ff 5b 13 00 00 66 73 73 70 35 72 70 70 31 73  --[-...f- sp5rpp1
0040 73 04 b4 b4 d7 31 29 67 f6 34 b5 07 45 ec a8 95  s---1)g -4-t...
0050 1f 48 3a 51 94 13 f6 1e 46 33 01 3e f7 5d 69 74  -H:Q... F3>...it
0060 2c 70 b0 5f 70 70 69 8f 71 70 71 70 70 70 70 70  -p_ppi- qpqpqpqp
0070 70 7b 70 74 73 70 71 72 70 53 70 70 67 70 70 70  p[ptspqr p5pppppp
0080 66 73 73 61 31 7b 70 61 4d 70 61 4a 70 76 25 40  fssal[pa Mpa]pv8@
0090 f2 76 21 40 f2 75 49 d0 73 72 71 72 72 7c 25 a2  -v!@-uI- srqr[X-
00a0 ce b5 2f cc 4e 98 b3 c8 84 90 40 7d 76 79 5a f6  -/-N--- -@]vyZ-
00b0 38 f6 87 7d 71 71 7b 75 70 40 25 41 7b 40 79 76  8-...)qq(u p@A[ @yv
00c0 73 25 74 76 63 72 32 35 41 69 40 67 76 73 25 74  s$tvcr25 Aigvgs$
00d0 7a 63 60 37 1c 1f 12 11 1c 23 19 17 1e 50 1e 06  zc'7--- -#...P..
00e0 5d 03 11 41 5b 40 59 76 73 25 74 73 63 52 37 1c  ]-A[ @yv s$tsCR7-
00f0 1f 12 11 1c 23 19 17 1e 50 37 33 33 50 22 46 50  -...#--- P733P"EP
0100 31 1c 00 18 13 23 23 3c 50 33 31 50 42 40 42 45  1----##@ P31PD@E
0110 40 6e 67 7d 42 45 40 47 41 45 40 47 42 46 43 44  @ng)BE@GC AE@GBGCD
0120 2a 67 7d 42 46 40 47 43 41 41 44 45 49 45 49 2a  *g)BF@GC AAOEIEI*
0130 40 65 41 63 40 61 76 73 25 74 73 7c 7a 5a 5e 1e  @eAc@avs $ts|zZ^
0140 11 8d 15 5e 11 1f 1d d0 f2 71 52 d0 7d 76 79 5a  ---^---@ -aB@!uv7

```



Since the entire communications do not appear to be XOR encoded, I had to assume that there were communication setup markers/flags, and additional payload information I wasn't seeing. I relayed this to others in the [X post](#). S1dhy cracked the rest of this and shared this [X post](#).

Some interesting further notes: Many of the shared strings/domains that's I've observed include similar names like, upHOLA, upWhatsApp (misspelled), upTikTok, and upWire, with similar firewall and sysWOW64 drop locations.

Update 01-25-2026: I had noticed last week that running different region IPs resulted in different IP:Port connections. [S1dhy confirmed](#) this behavior and found several more IP connections, added to the IOCs below.

Conclusion: I agree with S1dhy, this appears to set up the host system as a proxy. Persistence is set via service, firewall is opened using netsh, and certain strings within the binary suggest it looks to see if its running on a VM. The use of ip lookup appears to occur (geolocation?), and some basic system fingerprinting. This, combined with the fact that it's wrapped inside an installer that users believe to be the official installer suggests this isn't merely a PUP in my opinion. I am now curious to see more follow-on with this, and with some of the older samples like upHOLA.exe.

Category	Indicator	Details / Notes
URL	https://update.7zip.cloud/7zipInstall.exe	Trojanized installer distribution URL
URL	https://gg.afn360.com/client_v1/config/http	Config endpoint observed in hero.dll strings
Domain	soc.hero-sms.co	Config / control domain
Domain	neo.herosms.co	Config / control domain
Domain	flux.smshero.co	Config / control domain
Domain	nova.smshero.ai	Config / control domain
Domain	zest.hero-sms.ai	Config / control domain
Domain	apex.herosms.ai	Config / control domain
Domain	mint.smshero.com	Config / control domain
Domain	vivid.smshero.vip	Config / control domain
Domain	spark.herosms.io	Config / control domain
Domain	prime.herosms.vip	Config / control domain
Domain	glide.smshero.cc	Config / control domain
Domain	pulse.herosms.cc	Config / control domain
IP:Port	79.127.221.47:1000	Tunnel / proxy endpoint
IP:Port	84.17.37.1:1002	Alternate tunnel / proxy endpoint
IP:Port	89.187.169.66:1000	Tunnel / proxy endpoint
IP:Port	138.199.12.70:1000	Tunnel / proxy endpoint
IP:Port	156.146.44.213:1002	Tunnel / proxy endpoint
IP:Port	195.181.170.79:1000	Tunnel / proxy endpoint
IP:Port	195.181.175.120:10000	Tunnel / proxy endpoint
IP:Port	43.243.170.20:1000	Tunnel / proxy endpoint
IP:Port	79.127.221.41:1000	Tunnel / proxy endpoint
IP:Port	79.127.221.56:1000	Tunnel / proxy endpoint
IP:Port	79.127.241.51:1000	Tunnel / proxy endpoint
IP:Port	95.173.197.212:1002	Tunnel / proxy endpoint

Category	Indicator	Details / Notes
IP:Port	89.187.169.66:1000	Tunnel / proxy endpoint
IP:Port	84.17.56.88:1002	Tunnel / proxy endpoint
File (SHA256)	7zipInstall.exe	63396fa92aa010e543e21cd8cb1bcccc
File (SHA256)	7zfm.exe	2009b69852a9b20bbbe85061e1ef9186
File (SHA256)	hero.exe	e2022cedcea9b5ea81764996732a9880
File (SHA256)	hero.dll	ddf75cc7e322d75de77b17c8ec887975
File (SHA256)	uphero.exe	c4edf28177e72d1bfc482cf4d05a156b
Certificate Signer	JOZEAL NETWORK TECHNOLOGY CO., LIMITED	EV Code Signing (GlobalSign), observed on related files

[TamperedChef: Suspicious Recipe App is really Malware](#)

[EvilAI: Fake Online Speedtest Application](#)