

Fake 7-Zip downloads are turning home PCs into proxy nodes

malwarebytes.com/blog/threat-intel/2026/02/fake-7-zip-downloads-are-turning-home-pcs-into-proxy-nodes

Stefan Dasic

February 9, 2026



A convincing lookalike of the popular 7-Zip archiver site has been serving a trojanized installer that silently converts victims' machines into residential proxy nodes—and it has been hiding in plain sight for some time.

“I’m so sick to my stomach”

A PC builder recently turned to Reddit’s r/pcmasterrace community in a panic after realizing they had downloaded 7-Zip from the wrong website. Following a YouTube tutorial for a new build, they were instructed to download 7-Zip from 7zip[.]com, unaware that the legitimate project is hosted exclusively at 7-zip.org.

In their Reddit post, the user described installing the file first on a laptop and later transferring it via USB to a newly built desktop. They encountered repeated 32-bit versus 64-bit errors and ultimately abandoned the installer in favor of Windows’ built-in extraction tools. Nearly two weeks later, Microsoft Defender alerted on the system with a generic detection:

Trojan:Win32/Malgent!MSR.

The experience illustrates how a seemingly minor domain mix-up can result in long-lived, unauthorized use of a system when attackers successfully masquerade as trusted software distributors.

A trojanized installer masquerading as legitimate software

This is not a simple case of a malicious download hosted on a random site. The operators behind 7zip[.]com distributed a trojanized installer via a lookalike domain, delivering a functional copy of functional 7-Zip File Manager alongside a concealed malware payload.

The installer is Authenticode-signed using a now-revoked certificate issued to Jozeal Network Technology Co., Limited, lending it superficial legitimacy. During installation, a modified build of **7zfm.exe** is deployed and functions as expected, reducing user suspicion. In parallel, three additional components are silently dropped:

- **Uphero.exe**—a service manager and update loader
- **hero.exe**—the primary proxy payload (Go-compiled)
- **hero.dll**—a supporting library

All components are written to **C:\Windows\SysWOW64\hero**, a privileged directory that is unlikely to be manually inspected.

An independent update channel was also observed at **update.7zip[.]com/version/win-service/1.0.0.2/Uphero.exe.zip**, indicating that the malware payload can be updated independently of the installer itself.

Abuse of trusted distribution channels

One of the more concerning aspects of this campaign is its reliance on third-party trust. The Reddit case highlights YouTube tutorials as an inadvertent malware distribution vector, where creators incorrectly reference 7zip.com instead of the legitimate domain.

This shows how attackers can exploit small errors in otherwise benign content ecosystems to funnel victims toward malicious infrastructure at scale.

Execution flow: from installer to persistent proxy service

Behavioral analysis shows a rapid and methodical infection chain:

1. **File deployment**—The payload is installed into SysWOW64, requiring elevated privileges and signaling intent for deep system integration.
2. **Persistence via Windows services**—Both **Uphero.exe** and **hero.exe** are registered as auto-start Windows services running under System privileges, ensuring execution on every boot.

3. Firewall rule manipulation—The malware invokes `netsh` to remove existing rules and create new inbound and outbound allow rules for its binaries. This is intended to reduce interference with network traffic and support seamless payload updates.

4. Host profiling—Using WMI and native Windows APIs, the malware enumerates system characteristics including hardware identifiers, memory size, CPU count, disk attributes, and network configuration. The malware communicates with `iplogger[.]org` via a dedicated reporting endpoint, suggesting it collects and reports device or network metadata as part of its proxy infrastructure.

Functional goal: residential proxy monetization

While initial indicators suggested backdoor-style capabilities, further analysis revealed that the malware's primary function is proxyware. The infected host is enrolled as a residential proxy node, allowing third parties to route traffic through the victim's IP address.

The `hero.exe` component retrieves configuration data from rotating "smshero"-themed command-and-control domains, then establishes outbound proxy connections on non-standard ports such as 1000 and 1002. Traffic analysis shows a lightweight XOR-encoded protocol (key `0x70`) used to obscure control messages.

This infrastructure is consistent with known residential proxy services, where access to real consumer IP addresses is sold for fraud, scraping, ad abuse, or anonymity laundering.

Shared tooling across multiple fake installers

The 7-Zip impersonation appears to be part of a broader operation. Related binaries have been identified under names such as `upHolla.exe`, `upTikTok`, `upWhatsapp`, and `upWire`, all sharing identical tactics, techniques, and procedures:

- Deployment to SysWOW64
- Windows service persistence
- Firewall rule manipulation via `netsh`
- Encrypted HTTPS C2 traffic

Embedded strings referencing VPN and proxy brands suggest a unified backend supporting multiple distribution fronts.

Rotating infrastructure and encrypted transport

Memory analysis uncovered a large pool of hardcoded command-and-control domains using `hero` and `smshero` naming conventions. Active resolution during sandbox execution showed traffic routed through Cloudflare infrastructure with TLS-encrypted HTTPS sessions.

The malware also uses DNS-over-HTTPS via Google's resolver, reducing visibility for traditional DNS monitoring and complicating network-based detection.

Evasion and anti-analysis features

The malware incorporates multiple layers of sandbox and analysis evasion:

- Virtual machine detection targeting VMware, VirtualBox, QEMU, and Parallels
- Anti-debugging checks and suspicious debugger DLL loading
- Runtime API resolution and PEB inspection
- Process enumeration, registry probing, and environment inspection

Cryptographic support is extensive, including AES, RC4, Camellia, Chaskey, XOR encoding, and Base64, suggesting encrypted configuration handling and traffic protection.

Defensive guidance

Any system that has executed installers from 7zip.com should be considered compromised. While this malware establishes SYSTEM-level persistence and modifies firewall rules, reputable security software can effectively detect and remove the malicious components. Malwarebytes is capable of fully eradicating known variants of this threat and reversing its persistence mechanisms. In high-risk or heavily used systems, some users may still choose a full OS reinstall for absolute assurance, but it is not strictly required in all cases.

Users and defenders should:

- Verify software sources and bookmark official project domains
- Treat unexpected code-signing identities with skepticism
- Monitor for unauthorized Windows services and firewall rule changes
- Block known C2 domains and proxy endpoints at the network perimeter

Researcher attribution and community analysis

This investigation would not have been possible without the work of independent security researchers who went deeper than surface-level indicators and identified the true purpose of this malware family.

- **Luke Acha** provided the first comprehensive analysis showing that the Uphero/hero malware functions as residential proxyware rather than a traditional backdoor. His work documented the proxy protocol, traffic patterns, and monetization model, and connected this campaign to a broader operation he dubbed upStage Proxy. [Luke's full write-up is available on his blog.](#)

- **s1dhy** expanded on this analysis by reversing and decoding the custom XOR-based communication protocol, validating the proxy behavior through packet captures, and correlating multiple proxy endpoints across victim geolocations. Technical notes and findings were [shared publicly on X \(Twitter\)](#).
- **Andrew Danis** contributed [additional infrastructure analysis and clustering](#), helping tie the fake 7-Zip installer to related proxyware campaigns abusing other software brands.

Additional technical validation and dynamic analysis were published by researchers at [RaichuLab](#) on Qiita and [WizSafe Security](#) on IIJ.

Their collective work highlights the importance of open, community-driven research in uncovering long-running abuse campaigns that rely on trust and misdirection rather than exploits.

Closing thoughts

This campaign demonstrates how effective brand impersonation combined with technically competent malware can operate undetected for extended periods. By abusing user trust rather than exploiting software vulnerabilities, attackers bypass many traditional security assumptions—turning everyday utility downloads into long-lived monetization infrastructure.

Malwarebytes detects and blocks known variants of this proxyware family and its associated infrastructure.

Indicators of Compromise (IOCs)

File paths

- `C:\Windows\SysWOW64\hero\Uphero.exe`
- `C:\Windows\SysWOW64\hero\hero.exe`
- `C:\Windows\SysWOW64\hero\hero.dll`

File hashes (SHA-256)

- `e7291095de78484039fdc82106d191bf41b7469811c4e31b4228227911d25027` (Uphero.exe)
- `b7a7013b951c3cea178ece3363e3dd06626b9b98ee27ebfd7c161d0bbcfd894` (hero.exe)
- `3544ffefb2a38bf4fa6181aa4374f4c186d3c2a7b9b059244b65dce8d5688d9` (hero.dll)

Network indicators

Domains:

- `soc.hero-sms[.]co`
- `neo.herosms[.]co`
- `flux.smshero[.]co`

- nova.smshero[.]ai
- apex.herosms[.]ai
- spark.herosms[.]io
- zest.hero-sms[.]ai
- prime.herosms[.]vip
- vivid.smshero[.]vip
- mint.smshero[.]com
- pulse.herosms[.]cc
- glide.smshero[.]cc
- svc.ha-teams.office[.]com
- iplogger[.]org

Observed IPs (Cloudflare-fronted):

- 104.21.57.71
- 172.67.160.241

Host-based indicators

- Windows services with image paths pointing to C:\Windows\SysWOW64\hero\
- Firewall rules named Uphero or hero (inbound and outbound)
- Mutex: Global\3a886eb8-fe40-4d0a-b78b-9e0bcb683fb7

We don't just report on threats—we remove them

Cybersecurity risks should never spread beyond a headline. Keep threats off your devices by [downloading Malwarebytes today](#).