

Fake Huorong security site infects users with ValleyRAT

 malwarebytes.com/blog/scams/2026/02/huorong

Stefan Dasic

February 23, 2026



A convincing lookalike of the popular Huorong Security antivirus has been used to deliver ValleyRAT, a sophisticated [Remote Access Trojan \(RAT\)](#) built on the Winos4.0 framework, to users who believed they were improving their security.

The campaign, attributed to the Silver Fox APT group—a Chinese-speaking threat group known for distributing trojanized versions of popular Chinese software—uses a typosquatted domain to serve a trojanized NSIS installer that deploys a full-featured backdoor with advanced user-mode stealth and injection capabilities.

A fake site built to catch security-conscious users

Huorong Security—known in Chinese as 火绒—is a free antivirus product developed by Beijing Huorong Network Technology Co., Ltd., and widely used across mainland China.

The attackers registered [huoronga\[.\]com](#)—note the extra “a” at the end—as a near-perfect imitation of the legitimate [huorong.cn](#). This [typosquatting](#) technique catches users who mistype the address or arrive via search engine poisoning or phishing links. The fake site looks convincing enough that most visitors would have no obvious reason to suspect anything is wrong.

火绒安全软件6.0

畅享纯粹终端防护

轻快运行，静享守护，全面防御

免费下载

64位版 | 32位版 | ARM版



干净



轻巧



强大



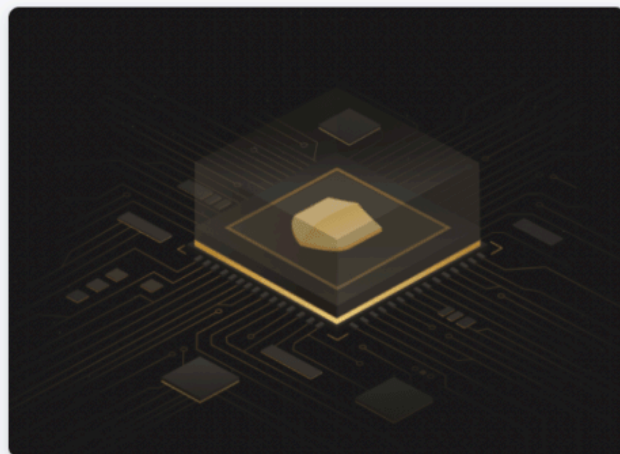
易用

Fake Huorong Security site

火绒

企业级终端安全防护解决方案

火绒安全打造专业终端防护体系，融合病毒查杀、网络防护和隐私保护功能，为您提供可靠的数字安全环境。

[立即下载](#)

火绒安全首选产品

Another fake Huorong Security site

When a visitor clicks the download button, the request is silently routed through an intermediary domain (hndqiebgibuiwqdh[r].cyou) before the final payload is served from Cloudflare R2 storage—a legitimate cloud service chosen for its trusted reputation and availability. The file is named BR 火绒445[.zip], using the Chinese name for Huorong to maintain the disguise up to the moment of execution.

What happens after you click download

Inside the ZIP archive is a trojanized NSIS installer (Nullsoft Scriptable Install System), a legitimate open-source framework used by many real applications. Its use here is deliberate: an NSIS-built executable raises fewer red flags than a custom packer, and the installation experience feels normal.

When executed, the installer drops a desktop shortcut named 火绒.lnk (Huorong.lnk), reinforcing the illusion that the antivirus installed successfully.

At the same time, it extracts a cluster of files into the user's Temp directory. Most are genuine supporting libraries or decoy executables meant to mimic a real installation, including copies of FFmpeg multimedia DLLs, a file posing as a .NET repair tool, and another mimicking a Huorong diagnostic utility.

The malicious components include:

- WavesSvc64.exe: the main loader, disguised as a Waves audio service process
- DuiLib_u.dll: a hijacked DirectUI library used for DLL sideloading
- box.ini: an encrypted file containing shellcode

How Windows is tricked into loading malware

The core technique is DLL sideloading, a technique attackers use to trick Windows into loading a malicious file instead of a legitimate one.

WavesSvc64.exe appears legitimate—its PDB path references a gaming application code directory—so Windows loads it without complaint. When it runs, Windows automatically loads DuiLib_u.dll alongside it. That DLL has been replaced with a malicious version that reads encrypted shellcode from box.ini, decrypts it, and executes it directly in memory.

Rather than dropping a single monolithic backdoor executable, the chain culminates in in-memory shellcode execution loaded from files dropped to disk (e.g., box.ini) via DLL sideloading. The shellcode-based chain is consistent with the Catena loader pattern documented by Rapid7, where signed or legitimate-looking executables bundle attack code in .ini configuration files and use reflective injection to execute it while leaving a minimal forensic footprint.

How the backdoor becomes permanent

Behavioral analysis shows a methodical infection chain:

1. Defender exclusions

The malware spawns PowerShell at high integrity level and instructs Windows Defender to ignore its persistence directory (`AppData\Roaming\trvePath`) and its main process (WavesSvc64.exe). After these commands execute, Windows Defender is less likely to scan the malware's chosen path/process, materially reducing native detection.

2. Persistence

It creates a scheduled task named Batteries (observed as `C:\Windows\Tasks\Batteries.job`). On every subsequent boot, the task launches `WavesSvc64.exe /run` from the persistence directory, reapplies Defender exclusions, and reconnects to command and control (C2).

3. File refresh

To evade signature-based detection, the malware deletes and re-writes WavesSvc64.exe, DuiLib_u.dll, libexpat.dll, box.ini, and vcruntime140.dll. Deletion of these files alone may not fully remediate the infection, as the malware demonstrates the ability to re-write core components during execution.

4. Registry storage

Configuration data, including the encoded C2 domain yandibaiji0203.[.]com, is written to `HKCU\SOFTWARE\IpDates_info`. A secondary key at `HKCU\Console\0\451b464b7a6c2ced348c1866b59c362e` stores encrypted binary data likely used for malware configuration or payload staging.

How it avoids detection

Beyond disabling Defender, ValleyRAT takes steps to avoid detection and analysis.

It checks for debuggers and forensic tools by looking for characteristic window titles. It probes BIOS version, display adapters, and VirtualBox registry keys to detect virtual machines—the sandboxes researchers use to analyze malware safely. It also checks available memory and disk capacity, and inspects locale and language settings, likely as a geofencing measure to confirm it is running on a Chinese-language system before fully deploying.

Command-and-control communications

The Winos4.0 stager connects to its C2 server at 161.248.87.250 over TCP port 443. Using TCP 443 provides camouflage at the port level; however, inspection revealed a custom binary protocol rather than standard TLS-encrypted HTTPS.

Network intrusion detection systems triggered Critical-severity alerts for Winos4.0 CnC login and server-response messages, and a high-severity alert for ProcessKiller C2 initialization.

C2 traffic was observed originating from `rundll32.exe`, which executed with the command line “rundll32.exe”—lacking the typical <DLL>, <Export> argument structure. In environments with command-line and parent-child process monitoring, this execution pattern is a high-confidence anomaly. Sandbox analysis extracted multiple WinosStager plugin DLLs from the rundll32 process, confirming the modular architecture that makes ValleyRAT particularly dangerous: capabilities are not bundled in a single monolithic binary but downloaded on demand.

The ProcessKiller component is particularly concerning. Network telemetry indicates ProcessKiller C2 initialization, consistent with a module associated in prior reporting with terminating security software. Previous ValleyRAT/Winos4.0 campaigns targeted security products from Qihoo 360, Huorong, Tencent, and Kingsof—indicating the potential to terminate security software, including the product it impersonated as a lure.

Post-compromise capabilities

In short, once it's installed, attackers can monitor the victim, steal sensitive information, and remotely control the system. Sandbox analysis confirmed the following behaviors once the malware has a foothold:

- Keylogging via a system-wide keyboard hook installed through SetWindowsHookExW in the rundll32 process, capturing every keystroke.
- Process injection: WavesSvc64.exe creates suspended processes and writes to the memory of other processes for stealth code execution.
- Credential access: the malware reads credential-related registry keys and touches browser cookie files.
- System reconnaissance: queries hostname, username, keyboard layout, locale, running processes, and physical drives.
- RWX memory regions created inside rundll32.exe consistent with in-memory execution, reducing reliance on additional dropped payload executables.
- Self-cleanup: deletes its own executed files and performs deletion of 10 or more additional files to obstruct forensic recovery.
- The malware creates mutexes including the dated string 2026. 2. 5 and the path C:\ProgramData\DisplaySessionContainers.log, and writes a log file at that location.

Who's behind this campaign?

This campaign fits the established pattern of Silver Fox operations. The group has repeatedly used trojanized installers of widely trusted Chinese software to distribute ValleyRAT and the Winos4.0 framework. Previous lures included QQ Browser, LetsVPN, and gaming applications.

Impersonating a security product raises the stakes. The victims are not just casual users—they are actively looking for protection.

The targeting remains consistent. Chinese-language filenames, the Huorong lure, and built-in locale checks all point to a geographically focused campaign.

However, the public leak of the ValleyRAT builder on GitHub in March 2025 significantly lowered the barrier to entry. Researchers identified approximately 6,000 related samples between November 2024 and November 2025, with 85% appearing in the latter half of that period. That increase suggests the tooling is spreading beyond a single operator.

How to stay safe

This campaign shows how easily trust can be turned against users. The attackers didn't need a zero-day exploit. They needed a convincing website, a realistic installer, and the knowledge that many people will search for a product name and click the first result.

When the lure is a security product, the deception is even more effective.

Here's what to check:

- **Verify download sources.** The legitimate Huorong Security website is `huorong.cn`. Always double-check the domain before downloading security software—a single extra character can lead to a malicious site.
- **Monitor Windows Defender exclusions.** Any `Add-MpPreference` command you did not initiate is a strong indicator of compromise. Audit exclusions regularly.
- **Hunt for persistence artifacts.** Search endpoints for a scheduled task or job named `Batteries` (artifact observed as `C:\Windows\Tasks\Batteries.job`), the `%APPDATA%\trvePath\` directory, and the registry key `HKCU\SOFTWARE\IpDates_info`.
- **Block outbound connections** to `161.248.87.250` at the firewall and deploy IDS rules for Winos4.0 C2 signatures (ET SIDs `2052875`, `2059975`, and `2052262`).
- **Alert on process anomalies.** `Rundll32.exe` without a legitimate DLL argument, and `WavesSvc64.exe` outside a genuine Waves Audio installation, are high-confidence indicators.

Malwarebytes detects and blocks known variants of ValleyRAT and its associated infrastructure.

Indicators of Compromise (IOCs)

Infrastructure

- Fake websites:
 - `huoronga[.]com`
 - `huorongcn[.]com`
 - `huorongh[.]com`
 - `huorongpc[.]com`
 - `huorongs[.]com`
- Redirect domain: `hndqiuebgibuiwqthr[.]cyou`
- Payload host: `pub-b7ce0512b9744e2db68f993e355a03f9.r2[.]dev`
- C2 IP: `161.248.87[.]250` (TCP 443, custom binary protocol)
- Encoded C2 domain: `yandibaiji0203[.]com`

File hashes (SHA-256)

- `72889737c11c36e3ecd77bf6023ec6f2e31aecbc441d0bdf312c5762d073b1f4` (NSIS installer)
- `db8cbf938da72be4d1a774836b2b5eb107c6b54defe0ae631ddc43de0bda8a7e` (WavesSvc64.exe)
- `d0ac4eb544bc848c6eed4ef4617b13f9ef259054fe9e35d9df02267d5a1c26b2` (DuiLib_u.dll)
- `07aaaa2d3f2e52849906ec0073b61e451e0025ef2523dafbd6ae85ddfa587b4d` (WinosStager DLL #1)

- [66e324ea04c4abbad6db4f638b07e2e560613e481ff588e0148e33e23a5052a9](#) (WinosStager DLL #2)
- [47df12b0b01ddca9eb116127bf84f63eb31e80cec33e4e6042dff1447de8f45f](#) (WinosStager DLL #3)

Host-based indicators

- Scheduled task named [Batteries](#) at [C:\Windows\Tasks\Batteries.job](#)
- Persistence directory: [%APPDATA%\trvePath\](#)
- Registry key: [HKCU\SOFTWARE\IpDates_info](#)
- Registry key: [HKCU\Console\0\451b464b7a6c2ced348c1866b59c362e](#)
- Log file: [C:\ProgramData\DisplaySessionContainers.log](#)
- Processes: [WavesSvc64.exe](#), [rundll32.exe](#) (without DLL argument)

MITRE ATT&CK

- [T1189](#) — Drive-by Compromise (Initial Access)
- [T1059.001](#) — PowerShell (Execution)
- [T1053.005](#) — Scheduled Task (Persistence)
- [T1562.001](#) — Impair Defenses: Disable or Modify Tools (Defense Evasion)
- [T1574.002](#) — DLL Side-Loading (Defense Evasion)
- [T1027](#) — Obfuscated Files or Information (Defense Evasion)
- [T1218.011](#) — Rundll32 (Defense Evasion)
- [T1555](#) — Credentials from Password Stores (Credential Access)
- [T1082](#) — System Information Discovery (Discovery)
- [T1057](#) — Process Discovery (Discovery)
- [T1056.001](#) — Keylogging (Collection)
- [T1071](#) — Application Layer Protocol (Command and Control)
- [T1070.004](#) — Indicator Removal: File Deletion (Defense Evasion)

We don't just report on scams—we help detect them

Cybersecurity risks should never spread beyond a headline. If something looks dodgy to you, check if it's a scam using [Malwarebytes Scam Guard](#). Submit a screenshot, paste suspicious content, or share a link, text or phone number, and we'll tell you if it's a scam or legit. Available with [Malwarebytes Premium Security](#) for all your devices, and in the [Malwarebytes app for iOS and Android](#).

About the author

Passionate about antivirus solutions, Stefan has been involved in malware testing and AV product QA from an early age. As part of the Malwarebytes team, Stefan is dedicated to protecting customers and ensuring their security.

[AI](#)



[Public Google API keys can be used to expose Gemini AI data](#)

February 27, 2026

[Researchers found that Google API keys long treated as harmless can now unlock access to Gemini.](#)

[How to](#)



[How to understand and avoid Advanced Persistent Threats](#)

February 26, 2026

[APT stands for Advanced Persistent Threat. But what does that actually mean, and how does it translate into the kind of threat you're facing?](#)

[News](#)



CONDUENT



Humana

ExpertPay®



[The Conduent breach; from 10 million to 25 million \(and counting\).](#)

February 26, 2026

[A third-party breach at Conduent now affects 25 million Americans—many never knew their data flowed through its systems.](#)