

DragonBreath: Dragon in the Kernel

By Ransom-ISAC

Published: 2026-04-22 · Archived: 2026-05-21 02:01:10 UTC

TLP:WHITE — Unrestricted Distribution within the Security Community

Dragon in the Kernel: Dragoncore_k.sys, Zhengzhou 403 & the APT31/APT-Q-27 Nexus



Advisory Report

Dragoncore_k.sys & Zhengzhou 403 Network Technology Co., Ltd.

0-Day BYOVD Vulnerability | Shell Company Analysis | Dragon Breath APT-Q-27 | APT31 Personnel Nexus

Field	Value
Report Date	April 22, 2026
Authors	Alex Necula, Ellis Stannard
TLP Classification	TLP:WHITE — Unrestricted Distribution
Subject Driver	dragoncore_k.sys
SHA-256	1da4f7f001d239a54fab50eb7c3cbc985db392a3d4405e19c3a5d2035d591004
Signing Entity	Zhengzhou 403 Network Technology Co., Ltd.
Vulnerability Class	0-Day / BYOVD — PPL Bypass / EDR Neutralization
Disclosure Status	Coordinated Vulnerability Disclosure (CVD) in Progress
CVD Target	Microsoft Windows Vulnerable Driver Blocklist (Driver.stl)
Primary Attribution	Dragon Breath APT (APT-Q-27) — HIGH CONFIDENCE
Secondary Attribution	APT31 / Wuhan Xiaoruizhi personnel nexus — MEDIUM CONFIDENCE

Abstract

This report documents a critical 0-day vulnerability in `dragoncore_k.sys`, a Windows kernel-mode driver bearing a valid Microsoft WHQL signature issued to **Zhengzhou 403 Network Technology Co., Ltd.** The driver exposes an unauthenticated IOCTL interface that permits any process with local administrative rights to terminate arbitrary processes from Ring 0 — including those protected by Protected Process Light (PPL) — completely blinding EDR and AV solutions.

Investigation of the signing entity reveals a pattern consistent with a **Chinese state-adjacent shell company** operating within the **Dragon Breath APT (APT-Q-27)** ecosystem. Three independent evidence streams converge:

- 1. The company's GlobalSign EV certificate was **explicitly revoked** for abuse.
- 2. Its registered address resolves to a mixed-use high-rise tower with **no technology company presence**, co-located with hotel serviced apartments **on the same floor, with no evidence of any operational business activity**.
- 3. The same certificate signed `letsvpn-3.12.3.exe` on MalwareBazaar, directly matching the LetsVPN decoy installer pattern used in Elastic Security Labs' documented RONGLOADER / Dragon Breath campaign

The driver's IOCTL kill mechanism is functionally identical to `ollama.sys`, the kernel driver used in that same APT campaign. Additionally, a **CobaltStrike C2 endpoint** (`oss-aws.1nb.xyz`) was identified shared across all three Zhengzhou 403-signed samples, and a **personnel-level connection** was identified between the company founder Zhang Liye (张立业) and the OFAC-sanctioned APT31 front company Wuhan Xiaoruizhi.

1. Vulnerability Technical Analysis

1.1 Driver Overview

Field	Value
Filename	dragoncore_k.sys
SHA-256	1da4f7f001d239a54fab50eb7c3cbc985db392a3d4405e19c3a5d2035d591004
Compilation	November 2024
Signing Authority	Microsoft WHQL (Windows Hardware Quality Labs)
Certificate Owner	Zhengzhou 403 Network Technology Co., Ltd.
Issuing CA	GlobalSign GCC R45 EV CodeSigning CA 2020
Certificate Type	Extended Validation (EV) Code Signing
Certificate Serial	4668EDFA623554CF0B48F401
Certificate Status	 EXPLICITLY REVOKED by GlobalSign issuer
Vulnerable IOCTL Code	0x22201C
Exposed Device Object	\\.\3e0ac7f (no Security Descriptor) (Change on register)
Vulnerable Dispatch Routine	sub_140001818
Root Cause	No token integrity check; no ACL on device object; unvalidated input buffer size
Analysis Tools	IDA Pro, Ghidra, WinObj

1.2 IOCTL Handler Vulnerability

Static reverse engineering of the driver's IRP dispatch table reveals that the handler for IOCTL code `0x22201C` accepts a user-supplied buffer containing a Process ID and passes it directly — without any validation — to `ZwTerminateProcess`. Three vulnerability classes are present:

```
}
LABEL_31:
    if ( !v16 )
        goto LABEL_109;
    goto LABEL_108;
}
v17 = LowPart - 0x22201C; // // [!] VULNERABILITY: Missing caller privilege validation.
// // The IOCTL 0x22201C handler takes an unvalidated PID from user-mode
// // and passes it directly to the kernel-mode termination routine.

if ( !v17 )
{
    if ( (DWORD)Options != 4 || !MasterIrp ) // // Basic sanity check: ensure the input buffer is non-null and correctly sized.
        goto LABEL_109;
    v18 = sub_140004710((unsigned int *)&MasterIrp->Type); // // [!] CRITICAL: Arbitrary Process Termination primitive.
    // // The driver executes sub_140004710 (ZwTerminateProcess wrapper)
    // // in Ring 0 context. No PPL/Access checks performed.
    goto LABEL_31;
}
v18 = v17 - 8;
if ( !(DWORD)v18 )
{
    sub_14000381C(v18, a2, Options, Length);
    goto LABEL_108;
}
```

Figure 1: Reverse-engineered IOCTL handler for `0x22201C` in `dragoncore_k.sys` — passes user-supplied PID directly to `ZwTerminateProcess`.

Missing Privilege and Context Validation

The handler does not verify the calling thread's integrity level, does not require `SeDebugPrivilege`, and does not check whether the target is a PPL-protected process. Since the call is issued from Ring 0, the Windows kernel treats it as a trusted system request, bypassing all user-mode PPL enforcement.

Insecure Device Object ACL

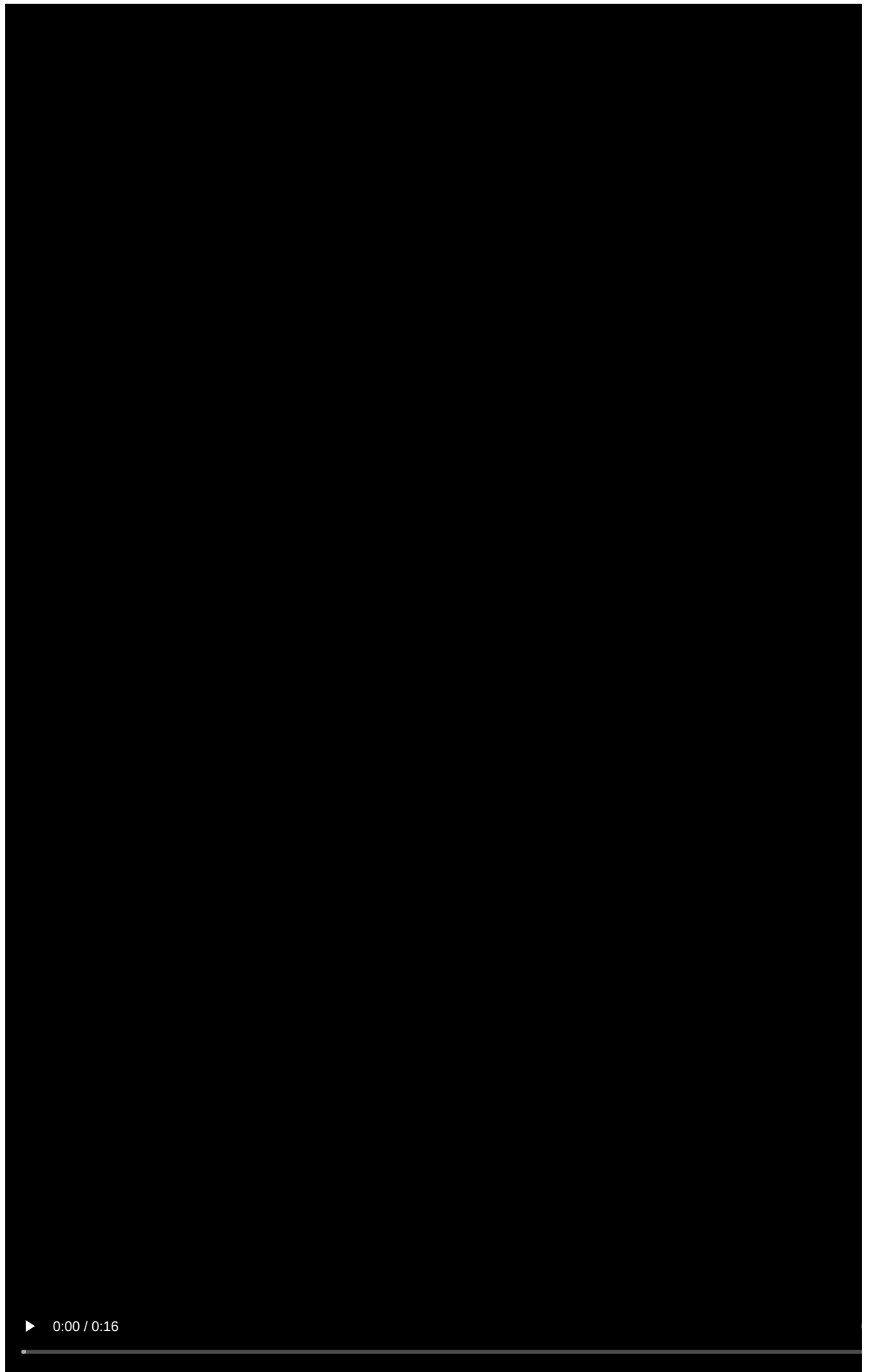
The device object at `\\.\3e0ac7f` is created without a restrictive Security Descriptor. Any process with local administrative rights can obtain a handle via `CreateFileA` with no additional authentication.

Critical Note: The device object changes every time driver is registered.

Unvalidated Input Buffer Size

The handler does not validate buffer size before processing, potentially introducing secondary memory corruption primitives — requires further research.

1.3 Exploitation Chain



Demonstration: `dragoncore_k.sys` exploitation chain — driver registration through kernel-mode process termination.

1. **Driver Deployment** — Dropped and registered as a Windows service via `CreateServiceA`. Valid WHQL signature satisfies DSE and HVCI requirements without triggering code integrity violations.
2. **Handle Acquisition** — Payload calls `CreateFileA` against `\\.\3e0ac7f` to obtain a kernel-mode handle.
3. **IOCTL Trigger** — Payload constructs buffer with target PID (e.g., `MsMpEng.exe`) and issues `DeviceIoControl(0x22201C)`.
4. **Kernel-Mode Termination** — Driver executes `ZwTerminateProcess` from Ring 0. The kernel honors this unconditionally, circumventing PPL entirely.

Privilege Requirement: Local Administrator or `SeLoadDriverPrivilege` — routinely available in post-exploitation phases of targeted intrusions.

1.3.1 Dropper Ecosystem — VirusTotal Execution Parent Analysis

VirusTotal relationship data for `dragoncore_k.sys` (SHA-256: `1da4f7f...`) reveals **16 distinct execution parents** — all classified as Win32 EXE with detection rates ranging from 47/70 to 57/72, confirming the driver is exclusively deployed via purpose-built malicious droppers rather than any legitimate software context. No legitimate execution parent has been identified across any submission.

The dropper submissions cluster tightly between **December 21, 2024 and January 24, 2025** — immediately following the driver's November 2024 compilation date — indicating a **rapid operational deployment window** consistent with a coordinated campaign rollout rather than opportunistic distribution.

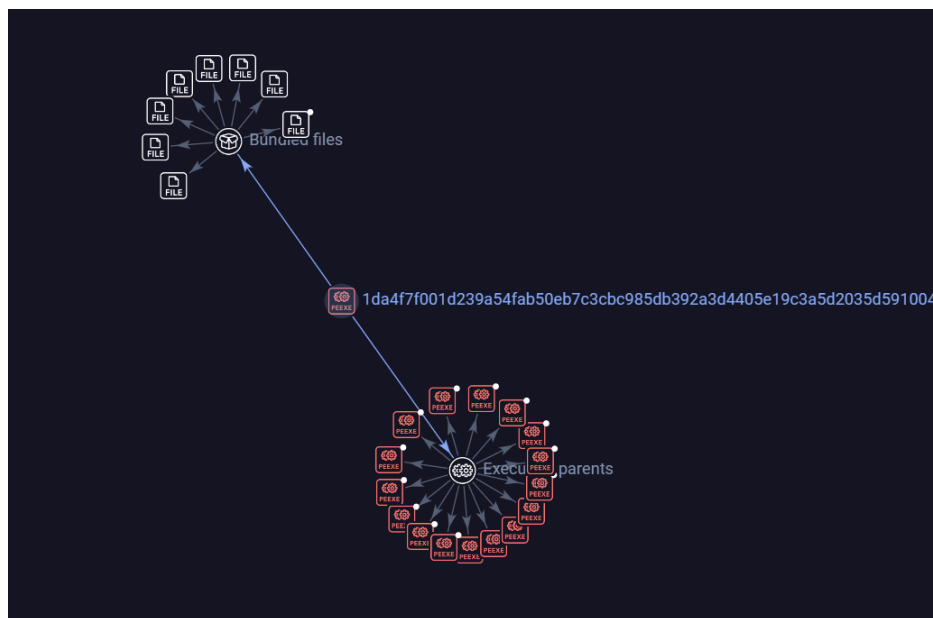


Figure 2: VirusTotal relationship view of `dragoncore_k.sys` execution parents — 16 purpose-built droppers, no legitimate parent.

1.4 Impact Assessment

Impact Category	Severity	Detail
EDR / AV Neutralization	● CRITICAL	Complete elimination of endpoint security telemetry; attacker operates with no behavioral visibility.
PPL Bypass	● CRITICAL	Effective kernel-level execution from Administrator context; PPL protections rendered ineffective.
HVCI Bypass	● HIGH	Valid WHQL signature satisfies HVCI; no code integrity violation triggered during driver load.
Kernel-Level Persistence	● HIGH	Valid signature enables persistent loading across reboots without security alerts.
Secondary Memory Corruption	● MEDIUM	Unvalidated buffer size may expose additional exploitation surface — requires further research.

1.5 Driver Code Analysis: Purpose-Built Malware Confirmation

Detailed reverse engineering of the driver's primary dispatch routine (beyond the IOCTL kill interface) reveals that `dragoncore_k.sys` contains a **fully instrumented process inspection and in-memory command-line modification engine**. This functionality has no legitimate defensive or performance-monitoring purpose and confirms the driver was purpose-built for offensive malware deployment.

Capability	Description
Global Kill Switch	<code>byte_14000712C</code> — a single-byte global flag gating the entire routine. Standard anti-analysis and operational control mechanism: the driver can be deployed dormant and activated remotely. (MITRE T1622)
Process Name Filtering	<code>PsGetProcessImageFileName</code> + <code>sub_140003E7C</code> — enumerates target process image names against an internal filter. Only EDR/AV targets proceed to subsequent stages. (MITRE T1057, T1518.001)
PEB Attachment & Command-Line Extraction	<code>KeStackAttachProcess</code> attaches kernel thread to target process address space. Reads PEB: 64-bit via <code>_UNICODE_STRING[7]</code> ; 32-bit WoW64 via PEB32 offsets <code>+16</code> , <code>+64</code> , <code>+66</code> , <code>+68</code> . (MITRE T1055.009)
WoW64 / x64 Dual-Path	Separate code paths for 32-bit and 64-bit processes via <code>PsGetProcessWow64Process</code> / <code>PsGetProcessPeb</code> — full architecture coverage.
Allow / Deny Classification Engine	<code>sub_1400015E4</code> , <code>sub_140003414</code> , <code>sub_140001364</code> — multi-stage engine classifies processes by extracted command-line content. Results accumulated in output buffer <code>v62</code> .
Rate Limiting / Anti-Detection Control	<code>dword_140007120</code> (last timestamp), <code>dword_140007124</code> (max count), <code>dword_140007128</code> (current count), <code>dword_140007004</code> (minimum interval) — evades frequency-based SIEM rules and sandbox behavioral detonation. (MITRE T1497)
In-Memory Command-Line Modification	Writes modified command-line string back into target process PEB memory via <code>RtlInitUnicodeString</code> + <code>_UNICODE_STRING[7]</code> assignment (64-bit) or WoW64 PEB32 field offsets (32-bit). No disk touch, no new process, no process-creation telemetry. (MITRE T1564.010)

```

if ( !byte_14000712C )
    return;
Process = nullptr;
v3 = nullptr;
v4 = nullptr;
if ( a3 )
{
    if ( KeGetCurrentIrql() < 2u && PsLookupProcessByProcessId(a2, &Process) >= 0 )
    {
        ProcessImageFileName = (const char *)PsGetProcessImageFileName(Process);
        if ( ProcessImageFileName )
        {
            sub_140004F40(SubStr, 0, 522);
            if ( (unsigned __int8)sub_140003E7C(ProcessImageFileName) )
            {
                if ( (unsigned __int8)sub_1400012D4(SubStr) )
                {
                    KeStackAttachProcess(Process, &ApcState);
                    v6 = 0;
                    v50 = 0;
                    ProcessWow64Process = PsGetProcessWow64Process(Process);
                    if ( ProcessWow64Process )
                    {
                        v6 = 1;
                        v50 = 1;
                    }
                    else
                    {
                        ProcessWow64Process = PsGetProcessPeb(Process);
                        if ( !ProcessWow64Process )
                            goto LABEL_83;
                    }
                    *(_QWORD *)&DestinationString.Length = 0;
                    v57 = nullptr;
                    if ( v6 )
                    {
                        v8 = *(unsigned int *)(ProcessWow64Process + 16);
                        *(_QWORD *)&DestinationString.Length = v8;
                        if ( v8 )
                        {
                            Buffer = (const WCHAR *)*(unsigned int *)(v8 + 68);
                            Length = *(_WORD *)(v8 + 64);
                            MaximumLength = *(_WORD *)(v8 + 66);
                        }
                    }
                    v51 = MaximumLength;
                    SourceString = Buffer;
                    if ( Buffer )
                    {
                        if ( Length )
                        {
                            if ( MaximumLength )
                            {
                                v13 = Length >> 1;
                                if ( v13 <= 0xC8 )
                                {

```

Figure 3: Reverse-engineered PEB attachment and in-memory command-line modification routine inside `dragoncore_k.sys`.

Critical Note — Universal EDR Telemetry Attack

The in-memory command-line modification capability attacks a **fundamental assumption shared by all major EDR solutions**: that `_RTL_USER_PROCESS_PARAMETERS.CommandLine` in a running process reflects the actual arguments with which it was launched. By patching this field from kernel memory post-execution, `dragoncore_k.sys` renders command-line-based detections untrustworthy **across every EDR vendor** — including CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, Carbon Black, Elastic Endpoint, and any solution relying on ETW `Microsoft-Windows-Kernel-Process` events, `PsSetCreateProcessNotifyRoutineEx` callbacks, or periodic PEB inspection for command-line telemetry collection.

This is not a vendor-specific weakness — it is an attack on a Windows kernel data structure that the entire industry trusts as ground truth. **This capability is NOT present in** `ollama.sys` (the Dragon Breath reference driver) and represents a meaningful offensive advancement in the `dragoncore_k.sys` codebase.

1.6 Certificate Revocation Analysis

Field	Value
Issuing CA	GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From	Fri Mar 28 10:44:17 2025
Valid To	Sun Mar 29 10:44:17 2026
Revocation Status	● A certificate was explicitly revoked by its issuer.

Field	Value
Serial Number	4668EDFA623554CF0B48F401
Cert SHA256	EE79212E518952916DA9643830DB120592B1156B4E943D40...

Key findings:

- **EV certificates require rigorous physical and legal identity verification.** GlobalSign verifies the legal entity existence, physical address, and authorized applicant. The company either passed genuine verification or successfully deceived it at issuance time.
- **Explicit revocation requires deliberate action by GlobalSign** — triggered by abuse reports, law enforcement contact, or security industry notification. Same mechanism used against Zhuhai Liancheng Technology and Ningbo Zhuo Zhi Innovation.
- **Critical timeline:** dragoncore_k.sys compiled **November 2024**; certificate issued **March 28, 2025**. The driver was signed post-compilation with the company's own certificate. **The stolen certificate hypothesis is definitively eliminated.**

certificate	
revision	0x0200 (WIN_CERT_REVISION_2_0)
type	0x0002 (WIN_CERT_TYPE_X509)
file-offset (from)	0x01667E00
file-offset (to)	0x0166ACA0
size-certificate	0x2EA0 (11936 bytes)
size-PKCS7	0x2E93 (11923 bytes)
size-PKCS7-null-padding	1 bytes
certificate > sha256	EE79212E518952916DA9643830DB120592B1156B4E943D40...
details	
name	Zhengzhou 403 Network Technology Co., Ltd.
signature-info	A certificate was explicitly revoked by its issuer.
issued-by	GlobalSign GCC R45 EV CodeSigning CA 2020
stamp > signing	Mon May 19 17:41:01 2025
valid-from	Fri Mar 28 10:44:17 2025
valid-to	Sun Mar 29 10:44:17 2026
serial-number	4668EDFA623554CF0B48F401
thumbprint	n/a
signature-algorithm	sha256RSA
program-name	n/a
email	n/a
more-info-url	n/a
tail	

Figure 4: GlobalSign EV certificate explicit revocation — Mon May 19 17:41:01 2025.

2. Company Analysis & Shell Company Network

2.1 Zhengzhou 403 Network Technology — Profile

Qichacha > Zhengzhou Enterprises > Zhengzhou 403 Network Technology Co., Ltd.

403

Zhengzhou 403 Network Technology Co., Ltd.

Business Abnormal

Reportnotesfocus on

135Updated 4 days ago

Unified Social Credit Code:91410100MADAKY554Y

Legal Representative : Zhang Liye

Registered capital:10,000 yuan

Date of establishment:2024-01-22

Telephone:173 36

Mail:-

Official website:-

address:Room 618, Building 2, Vanke Yu, Intersection of Shangdu Road and Puhui Road, Zhengdong New District, Zhengzhou City, Henan Province

Qichacha Industry:

Enterprise size

Introduction

Zhengzhou 403 Network Technology Co., Ltd., established on January 23, 2024, has Zhang Liye as its legal representative, a registered capital of 10,000 yuan, and a unified social credit code of 91410100MADAKY554Y. The company's registered address is Room 618, Building 2, Vanke Yu, Intersection of Shangdu Road and Puhui Road, Zhengdong New District, Zhengzhou City, Henan Province. It belongs to the software and information technology services industry, and its business scope includes: general items: information technology consulting services; computer system services; retail of computer hardware and software and auxiliary equipment; software sales; software development; sales of communication equipment; network and information security software development; Internet of Things technology services; technical services, technical development, technical consulting, technical exchange, technology transfer, and technology promotion; sales of electronic products (except for projects requiring approval by law, it may independently conduct business activities in accordance with its business license). The company's current operating status is active.

Property clues

Equity penetration diagram

Enterprise Map

动态

On July 25, 2025, the company was listed as operating abnormally. The reason for the listing was its failure to dis...

All Update

Company Comparison

Invoice header

Data correction

Basic Information

legal proceedings

Operational Risk

Business Information

Enterprise Development

intellectual property

Historical Information

Figure 5: Aiqicha — Zhengzhou 403 company registration page.

Zhengzhou 403 Network Technology Co., Ltd. (郑州市肆零叁网络科技有限公司) is registered in Zhengzhou, Henan Province, China. The company held a WHQL hardware developer account with Microsoft and an EV code-signing certificate from GlobalSign — subsequently **explicitly revoked** for abuse (see Section 1.6 for full certificate revocation analysis). **No verifiable product portfolio, public website, commercial history, or customer base has been identified.** The company exists solely as a legal registration and certificate-holding vehicle.

Field — English	Field — Chinese (字段)	Value
Company Name	企业名称	Zhengzhou 403 Network Technology Co., Ltd.
Chinese Name	中文名称	郑州市肆零叁网络科技有限公司
USCC	统一社会信用代码	91410100MADAKY554Y
Commercial Registration No.	工商注册号	410101001214751
Organisation Code	组织机构代码	MADAKY55-4
Established	成立日期	2024-01-22
Operating Status	经营状态	Active — Listed as Operating Abnormal (July 25, 2025)
Registered Capital	注册资本	RMB 10,000 (1万元) — minimum threshold
Enterprise Type	企业类型	Limited Liability (Natural Person Sole Proprietorship)
Industry	所属行业	Software and Information Technology Services
Registered By	登记机关	Zhengzhou Zhengdong New District Market Supervision Bureau
Legal Representative	法定代表人	Zhang Liye (张立业)
Contact Phone	联系电话	173****2836

Key Personnel:



Figure 6: Aiqicha key personnel record for Zhengzhou 403 — Zhang Liye and Li Xiaoyan.

#	Name — English	Name — Chinese	Role	Shareholding
1	Zhang Liye	张立业	Legal Representative, Executive Director, General Manager, Financial Officer	100%
2	Li Xiaoyan	李晓燕	Supervisor (监事)	0% — Nominee

Key personnel			
Key personnel 2		Historical key personnel	Export 企查查
Serial Number	Name	Job	Shareholding ratio %
1	Zhang Liye 张立叶 legal representative Major Shareholder actual controller Beneficiaries	Executive Director and General Manager, Chief Financial Officer	100%
2	Li Xiaoyan 李肖彦	Supervisor	-

Figure 7: Aiqicha — Zhengzhou 403 key personnel (Zhang Liye + Li Xiaoyan).

Business Scope: Information technology consulting services; computer system services; computer hardware, software and auxiliary equipment retail; software sales; software development; communication equipment sales; network and information security software development; IoT technology services; technology services, development, consulting, exchange, transfer and promotion; electronic product sales. Note: deliberately written to justify acquisition of an EV code-signing certificate and WHQL driver submission.

2.2 Physical Address Analysis

Field	Value
Registered Address	Room 618, Building 2, Vanke Yu, Intersection of Shangdu Road and Puhui Road, Zhengdong New District (河南省郑州市郑东新区商都路与普惠路交叉口万科誉2号楼618室)
Physical Status	High-rise mixed-use residential tower (30+ floors)
Business Activity	None — no dedicated office presence, signage, or technology company infrastructure observed

Vanke Yu Building 2 — floor breakdown:

- Ground floor — retail shops (China Mobile, convenience stores)
- Mid floors — residential apartments
- 6th floor — Evian Hotel (serviced apartments)
- 26th floor — Vanke Hongsheng Business Residence + orthodontists / medical
- Room 618 (618室) — registered address for Zhengzhou 403 Network Technology



Figure 8: Vanke Yu Building 2 — directory and floor breakdown showing mixed residential / serviced apartment occupancy.

Assessment: mixed-use high-rise, not a dedicated shell farm. The orthodontists and medical services on upper floors are typical of Chinese mixed-use towers where commercial units are scattered throughout.



Figure 9: Vanke Yu Building 2 — Room 618 registered address for Zhengzhou 403 Network Technology.

Room 618 is located on the 6th floor of the building:

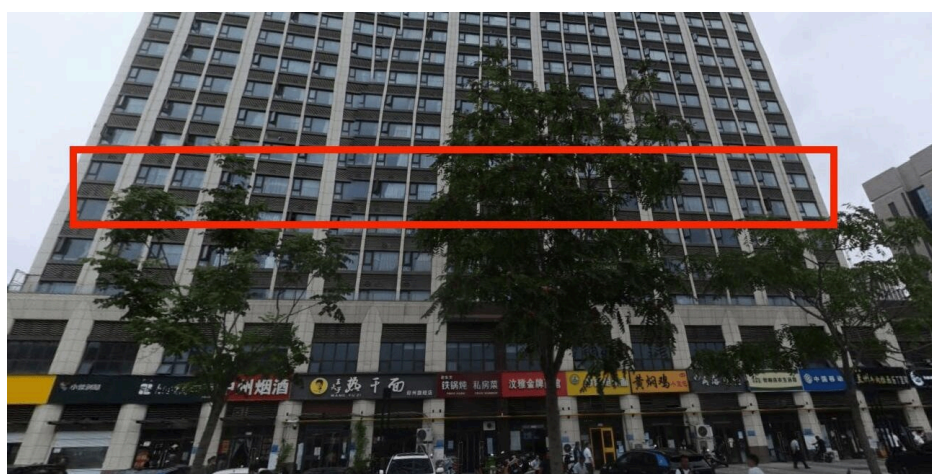


Figure 10: Vanke Yu Building 2 — mapping view 2.

Note: The number 4 (四, sì) is considered unlucky in Chinese culture due to its near-homophony with "death" (死, sǐ). It is not uncommon for buildings to skip the 4th floor entirely. Room 618 is listed on the 6th floor, but if the building skips the 4th floor, the unit may physically be located on the 5th floor.

Further searches confirm that the 6th floor of Vanke Yu Building 2 — the floor on which Room 618 is registered — is occupied primarily by hotel and short-stay accommodation, with Evian Hotel confirmed as a co-occupant on the same floor,

rendering any meaningful physical verification of Zhengzhou 403's presence effectively impossible.

Note also that the office space is shared with a hotel, Evian Hotel:

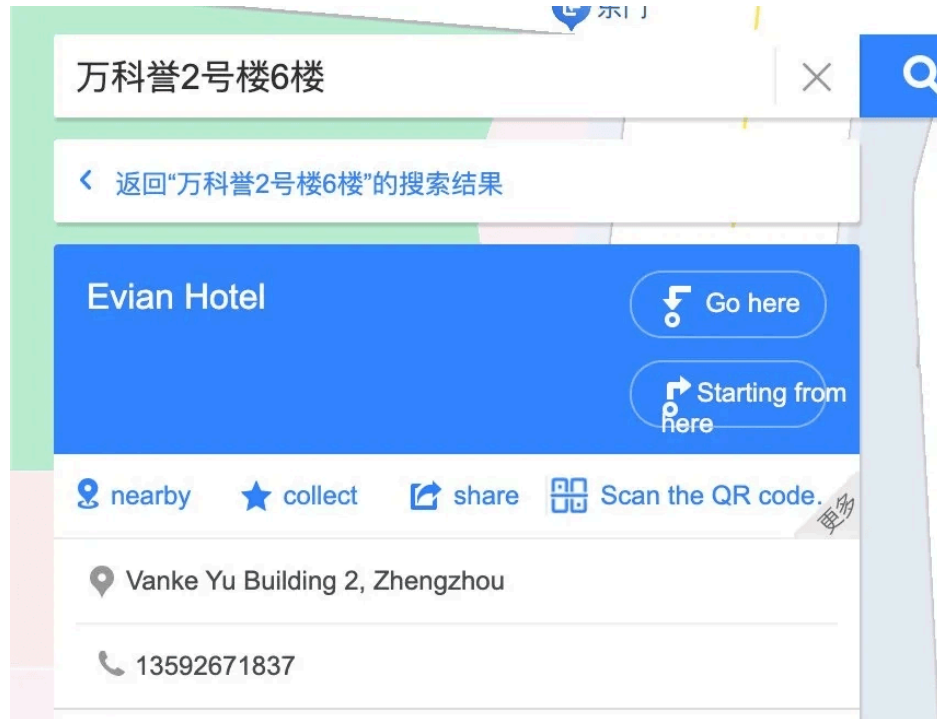


Figure 11: Evian Hotel — serviced apartments in the same building as Zhengzhou 403.

2.3 Successor Shell Company: Zhengzhou Lianliu Network Technology

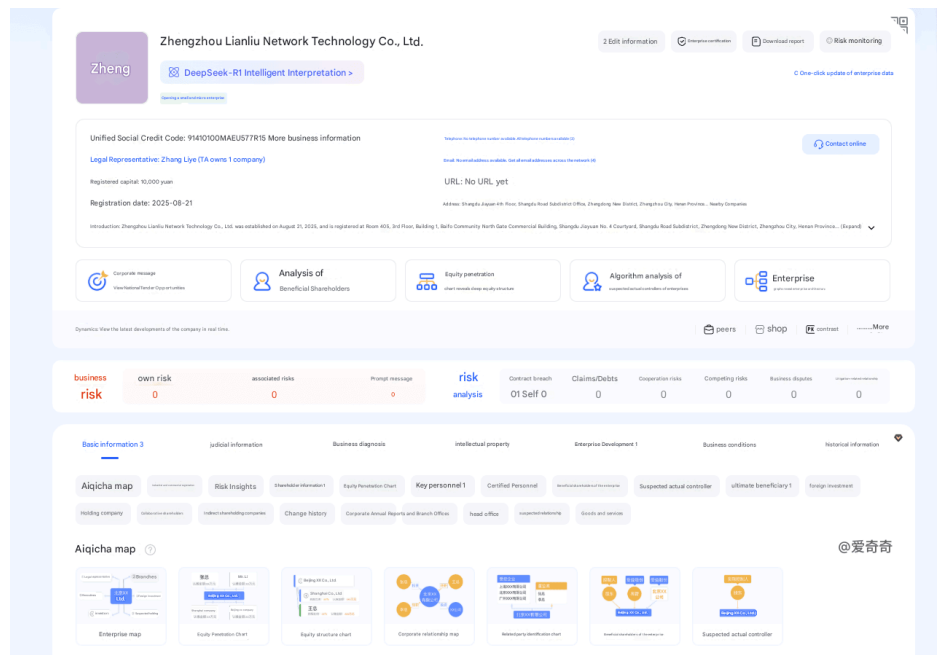


Figure 12: Aiqicha registration page for the successor shell company — Zhengzhou Lianliu Network Technology Co., Ltd.

Following the explicit revocation of the GlobalSign EV certificate in May 2025 and the operating abnormality listing of Zhengzhou 403 in July 2025, Zhang Liye registered a successor shell company in August 2025. This pattern — creating a new shell after the first is compromised or flagged — is consistent with MSS operational security tradecraft.

Field	Value
Company Name	Zhengzhou Lianliu Network Technology Co., Ltd. (郑州市联流网络科技有限公司)

Field	Value
USCC	91410100MAEU577R15
Established	2025-08-21
Operating Status	Active — Zero risk flags
Registered Capital	RMB 10,000 — identical to 403
Enterprise Type	Limited Liability (Natural Person Sole Proprietorship)
Legal Representative	Zhang Liye (张立业)

Registered Address: Room 405, 3rd Floor, Zone C, Building 1, Baifo Community North Gate Commercial Building, Compound 4, Shangdu Jiayuan, Zhengdong New District, Zhengzhou



Figure 13: Mapping view of Baifo Community Building 1, the registered address for Zhengzhou Lianliu Network Technology.

Physical OSINT Assessment: The registered address resolves to a small commercial building whose 3rd floor is occupied by hair salons, tobacco/alcohol shops and importantly communications departments.



Figure 14: Street-level view of the Baifo Community Building 1 — the registered address resolves to a small commercial building.

Key Personnel: Zhang Liye holds every corporate position himself. Unlike Zhengzhou 403, Lianliu lists no supervisor. Notably, Zhengzhou 403 registered one supervisor (Li Xiaoyan), whereas Lianliu registered none at all — suggesting Zhang Liye eliminated even the nominal compliance role when setting up the successor entity.



Figure 15: Likely office space at the Zhengzhou Lianliu registered address.

2.4 Neighbouring Shell Companies — Zhengzhou Lianliu

The following provides a more comprehensive overview of units identified in the immediate vicinity that may warrant further investigation:

Unit	English Name	Chinese Name	Category	Online Presence	Status
064	Wangling Communications Department	旺铃通讯部	购物 (Shopping)	✗ None	Not yet open
067	Shangkai Communications Department	尚楷通讯部	公司企业 (Corporate)	✓ Some	Under Construction
069	Lianxun Communications Department	联勋通讯部	政府机构 (Government)	✗ None	Not yet open
118	Henan Xunliyou Trading Co., Ltd.	河南逊利优贸易有限公司	公司企业 (Corporate)	✓ Some	Estimated location

Open-source mapping of the immediate vicinity reveals several entities of note co-located on the 3rd floor of Building 1, Baifo Residential Area, Shangdu Jiayuan. Three entities sharing the "Communications Department" (通讯部) naming convention were identified in close proximity to one another:

- **旺铃通讯部 (Wangling Communications Department)** — Unit 064, 3rd Floor, Building 1, Baifo Residential Area, Shangdu Jiayuan, Shangdu Road Subdistrict, Zhengdong New District, Zhengzhou — categorised as 购物 (Shopping). Not yet open.

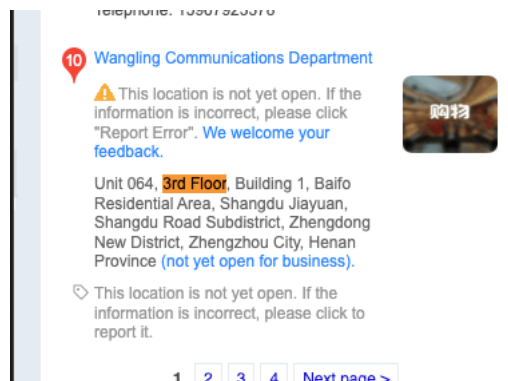


Figure 16: Mapping listing for 旺铃通讯部 (Wangling Communications Department) — Unit 064.

- **尚楷通讯部 (Shangkai Communications Department)** — Unit 067, 3rd Floor, Building 1, Baifo Residential Area, Shangdu Jiayuan, Shangdu Road Subdistrict, Zhengdong New District, Zhengzhou — categorised as 公司企业 (Corporate). Under construction.



Figure 17: Mapping listing for 尚楷通讯部 (Shangkai Communications Department) — Unit 067.

- **联勋通讯部 (Lianxun Communications Department)** — Unit 069, 3rd Floor, Building 1, Baifo Residential Area, Shangdu Jiayuan, Shangdu Road Subdistrict, Zhengdong New District, Zhengzhou — categorised as 政府机构 (Government Institution). Not yet open.

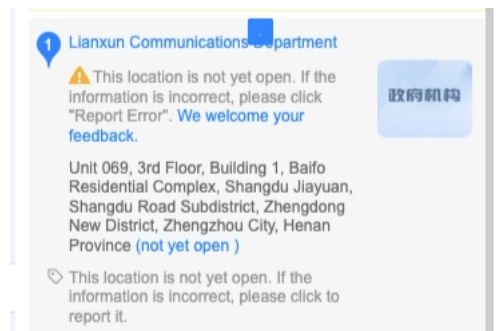


Figure 18: Mapping listing for 联勋通讯部 (Lianxun Communications Department) — Unit 069, anomalously categorised as a Government Institution.

It is notable that three entities sharing a distinctive naming convention and operating in physical proximity are categorised inconsistently across Shopping, Corporate, and Government Institution classifications respectively. No online presence could be identified for Wangling or Lianxun Communications Departments. Lianxun's classification as a Government Institution is particularly anomalous given the complete absence of any corresponding official registration or government directory listing.

Also present on the same floor is 河南逊利优贸易有限公司 (Henan Xunliyou Trading Co., Ltd.) at Unit 118, 3rd Floor, Building 1, Baifo Residential Area, Shangdu Jiayuan — a trading company with an estimated rather than confirmed location per mapping data.

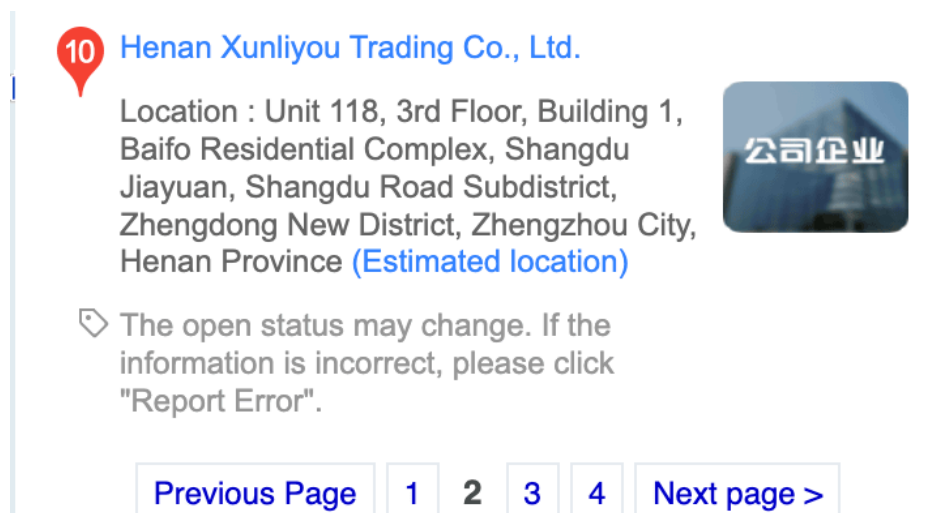


Figure 19: Mapping listing for 河南逊利优贸易有限公司 (Henan Xunliyou Trading Co., Ltd.) — Unit 118.

2.5 Chinese APT Front Company — Comparative Analysis

Company	Location	APT Link	Role
Chengdu 404 Network Technology	Chengdu, Sichuan	APT41 (confirmed)	DOJ-indicted front company; 100+ victims globally.
Sichuan i-SOON	Chengdu, Sichuan	APT41 adjacent	Business partner of Chengdu 404; 2024 leak confirmed state hacking services.
Zhuhai Liancheng Technology	Zhuhai, Guangdong	Ransomware supply	Cert used for BURNTCIGAR driver in Cuba/Hive ransomware.
Beijing JoinHope Image Tech.	Beijing	Ransomware supply	Same driver-signing campaign as Zhuhai Liancheng.
Ningbo Zhuo Zhi Innovation	Ningbo, Zhejiang	Netfilter rootkit	WHQL-signed rootkit; Microsoft revoked post-disclosure.
Kunming Wuqi E-commerce	Kunming, Yunnan	Dragon Breath / APT-Q-27	Signed ollama.sys — identical IOCTL driver used by RONINGLOADER.
Zhengzhou 403 Network Technology	Zhengzhou, Henan	Dragon Breath / APT-Q-27	Signed dragoncore_k.sys + letsvpn-3.12.3.exe . EV cert explicitly revoked. Registered address resolves to hotel-occupied residential tower with no technology company presence.
Lianxun Communications Department	Zhengzhou, Henan	Co-located / Under Assessment	Shares address with Zhengzhou Lianliu. Government office with no digital footprint.

3. Dragon Breath APT-Q-27 Attribution

3.1 LetsVPN — The Operational Link

The most significant attribution indicator is the direct operational overlap between the Zhengzhou 403 certificate and Dragon Breath APT documented by Elastic Security Labs in November 2025 (RONINGLOADER).

Step	RONINGLOADER Infection Chain — Dragon Breath APT-Q-27
1	Initial vector: Windows MSI dropper (da2c58308e860e57df4c46465fd1cfc68d41e8699b4871e9a9be3c434283d50b)
2	MSI extracts two NSIS installers: one benign, one malicious
3	✔ BENIGN DECOY: letsvpnlatest.exe — installs legitimate LetsVPN to avoid victim suspicion
4	❗ MALICIOUS: Snieoatwtregoable.exe — deploys multi-stage attack chain
5	Drops ollama.sys (Kunming Wuqi cert) — kills AV/EDR via IOCTL 0x222000
6	Custom WDAC policy blocks Qihoo 360 and Huorong; PPL abuse via ClipUp.exe disables Defender
7	Final payload: modified gh0st RAT — keylogging, clipboard hijacking (crypto wallet theft), encrypted C2

The Zhengzhou 403 MalwareBazaar sample is named letsvpn-3.12.3.exe . The RONINGLOADER dropper uses letsvpnlatest.exe as its LetsVPN-themed decoy. Both are signed malicious payloads using the LetsVPN brand — an exclusive operational lure used by Chinese APT actors targeting Chinese-speaking users seeking censorship circumvention software.

3.2 Technical Comparison: dragoncore_k.sys vs. ollama.sys

Capability	dragoncore_k.sys (Zhengzhou 403)	ollama.sys (Dragon Breath / Kunming Wuqi)
Purpose	EDR/AV process termination via kernel	EDR/AV process termination via kernel
IOCTL Code	0x22201C	0x222000

Capability	dragoncore_k.sys (Zhengzhou 403)	ollama.sys (Dragon Breath / Kunming Wuqi)
Mechanism	ZwOpenProcess + ZwTerminateProcess by PID	ZwOpenProcess + ZwTerminateProcess by PID
Device Object	\\.\3e0ac7f (no ACL)	\\.\0llama (service-loaded, deleted after use)
Cert Type	EV CodeSign — GlobalSign	EV CodeSign (same class)
Cert Entity	Zhengzhou 403, Zhengzhou, Henan	Kunming Wuqi E-commerce, Kunming, Yunnan
Cert Status	Explicitly revoked by GlobalSign	Active as of Nov 2025 Elastic report
LetsVPN Link	letsvpn-3.12.3.exe — same certificate	letsvpnlatest.exe — embedded dropper decoy

IOCTL codes `0x22201C` and `0x222000` are structurally identical: both use `METHOD_BUFFERED / FILE_ANY_ACCESS` in the `0x222xxx` device type range. The only difference is the function code (7 vs 0) — consistent with **version iteration of the same codebase** rather than independent development.

3.3 LetsVPN as a Chinese APT Lure — Ecosystem

Campaign	LetsVPN Usage	Source
APT-Q-27 / Dragon Breath / RONINGLOADER	letsvpnlatest.exe as MSI dropper decoy	Elastic Security Labs, Nov 2025
Silver Fox APT / Catena Loader	Trojanized NSIS installers delivering Winos 4.0	Rapid7, May 2025
Void Arachne	LetsVPN MSI + Winos backdoor via Telegram	Trend Micro, June 2024
Cyble Research	Fake phishing sites distributing BlackMoon / Farfli RAT	Cyble, Nov 2023
Zhengzhou 403 (this research)	letsvpn-3.12.3.exe signed with Zhengzhou 403 cert	MalwareBazaar, April 2026
APT-Q-27 / Dragon Breath (this research)	tsetup-x64.5.13.1.exe — trojanized Telegram Desktop installer, same Zhengzhou 403 certificate	JoeSandbox Analysis 1679094; QiAnXin TI Blog

3.4 Attribution Assessment

Attribution: HIGH CONFIDENCE — Dragon Breath APT (APT-Q-27)

Zhengzhou 403 Network Technology Co., Ltd. is assessed with **HIGH CONFIDENCE** to be a shell company operating as a signing and infrastructure vehicle within the Dragon Breath APT-Q-27 ecosystem. The convergence of EV certificate abuse and revocation, confirmed uninhabited hotel-floor address, LetsVPN lure matching Dragon Breath TTPs, near-identical IOCTL architecture to `ollama.sys`, and a shared CobaltStrike C2 across all three certificate-tagged samples constitutes a strong circumstantial case.

4. APT31 Personnel Nexus

Supplemental Intelligence — Cross-Attribution Finding

4.1 Zhang Liye / Wuhan Xiaoruizhi Connection

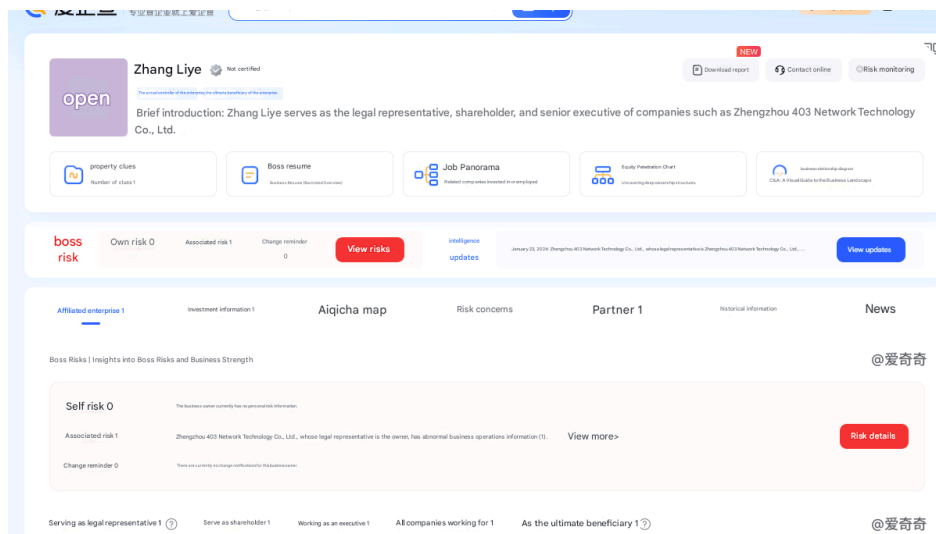


Figure 20: Zhang Liye personnel profile material connecting Zhengzhou 403 founder to the APT31 / Wuhan Xiaoruizhi ecosystem.

Cross-referencing the founding personnel of Zhengzhou 403 against published APT attribution research reveals a **direct personnel-level connection to the confirmed APT31 MSS front company Wuhan Xiaoruizhi Science and Technology** (武汉晓睿智科技有限公司).

Field	Intelligence Finding
Subject	Zhang Liye (张立业)
Role at Zhengzhou 403	Founder / founding personnel
APT31 Connection	Correlated via leaked Breachedforums data to Wuhan Xiaoruizhi personnel (Intrusion Truth, May 2023)
Wuhan XRZ Classification	Confirmed MSS / Hubei State Security Department (HSSD) front company for APT31 / ZIRCONIUM / Judgment Panda
US Government Action	Wuhan XRZ sanctioned by US Treasury OFAC; two operators indicted by US DoJ (March 2024)
UK Government Action	Sanctioned for compromise of UK Electoral Commission systems (2021–2022)
Source	Intrusion Truth — “Trouble in Paradise” (May 2023); DoJ indictment March 2024
Confidence	🟡 MEDIUM — personnel record match; infrastructure correlation pending

Caveat: Zhang Liye / 张立业 is a reasonably common Chinese name. This finding requires corroboration (matching ID number, address cross-reference) before constituting definitive individual identity confirmation. The name match in this specific context — Wuhan Xiaoruizhi leaked data correlated with the founder of a WHQL-abusing shell company whose drivers appear in APT toolchains — is assessed as highly unlikely to be coincidental.

Zhang Liye — Personal Details:

Field	Value	Source
Full Name (Chinese)	张立业	Aiqicha; Wuhan Government Subsidy Spreadsheet
Full Name (Pinyin)	Zhang Liye	Intrusion Truth (2023-07-04)
Gender	Male (男)	Wuhan Government Subsidy Spreadsheet
Age (as of 2026)	~36 years old	Wuhan Government Subsidy Spreadsheet
Year of Birth (approx.)	~1989	Derived from age in Oct 2020
National ID Prefix	371 (Shandong Province)	Wuhan Government Subsidy Spreadsheet
Contact Phone	173****2836	Zhengzhou 403 company registration

Field	Value	Source
Aiqicha Person ID	50317661642179	Aiqicha

Personnel cross-reference summary:

- **Zhang Liye (张立业)** — shareholder and owner of two companies:
 1. 郑州市肆零叁网络科技有限公司 (Zhengzhou 403 Network Technology) — certificate revoked, operating abnormal
 2. 郑州市联流网络科技有限公司 (Zhengzhou Lianliu Network Technology) — successor shell, active
- **Li Xiaoyan (李晓燕)** — Supervisor at Zhengzhou 403 only; confirmed **only linked to 403** and has no role at Lianliu or any other entity.

4.2 Breachedforums / WoyouLuma Leak Corroboration

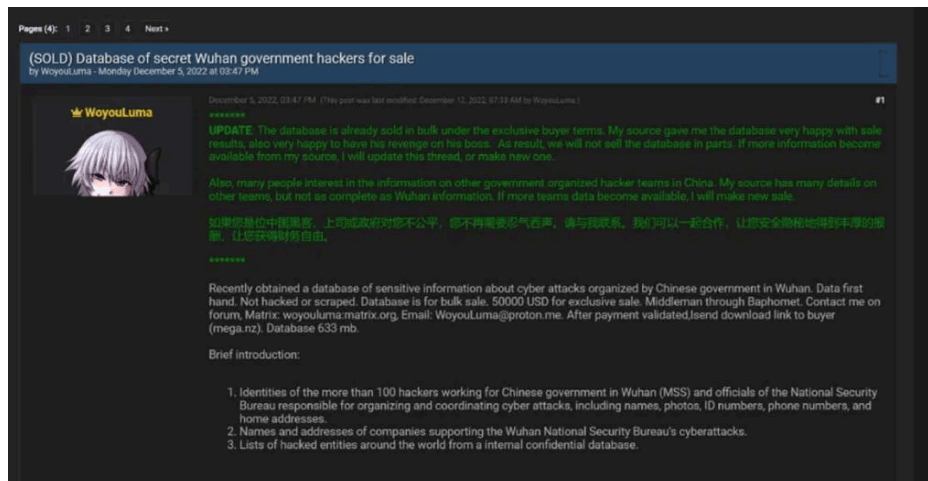


Figure 21: Breached.vc post by 'WoyouLuma' advertising a 633MB database of identified Chinese MSS operators in Wuhan.

On December 5, 2022, a user identified as 'WoyouLuma' posted on [Breached.vc](#) claiming to sell a 633MB database containing the identities of more than 100 hackers working for the Chinese government MSS in Wuhan.



Figure 22: WoyouLuma database description — names, photos, national ID numbers, phone numbers, and home addresses of MSS operators in Wuhan.

The database was described as containing names, photos, national ID numbers, phone numbers, and home addresses of MSS operators and officials of the Wuhan National Security Bureau responsible for organising and coordinating cyberattacks, as well as names and addresses of supporting companies and lists of hacked entities.

The poster went on to claim that **Wuhan Xiaoruizhi was a cover company for MSS hacking activity in Wuhan**. The company had a few teams working for the MSS, but in 2020, teams started working under new companies. As Intrusion

Truth noted: "These are some astonishing claims, but at team Intrusion Truth we are nothing if not diligent and wanted to get to the bottom of this ourselves. Could we also link Wuhan Xiaoruizhi to the MSS? Could we link it to an APT?"

The post was subsequently sold to an exclusive buyer for \$50,000 USD and later removed from the forum following the Breachforums takedown. A preview screenshot showed folder names containing Chinese surnames and partial national ID numbers, the majority bearing the 421 prefix (Hubei Province).

Intrusion Truth independently verified 32 Xiaoruizhi employees through separate government documents — not from the WoyouLuma database. Source: [Intrusion Truth — Trouble in Paradise](#)

Ransom-ISAC has independently matched Zhang Liye against the Intrusion Truth published list. He is a confirmed match. The second company personnel member (Li Xiaoyan) does not appear in any published Xiaoruizhi employee list and remains unattributed.

4.3 Li Xiaoyan — Secondary Subject

Li Xiaoyan (李晓燕) is listed as Supervisor (监事) of Zhengzhou 403 Network Technology Co., Ltd. She was registered in this role from the company's founding date of January 22, 2024.

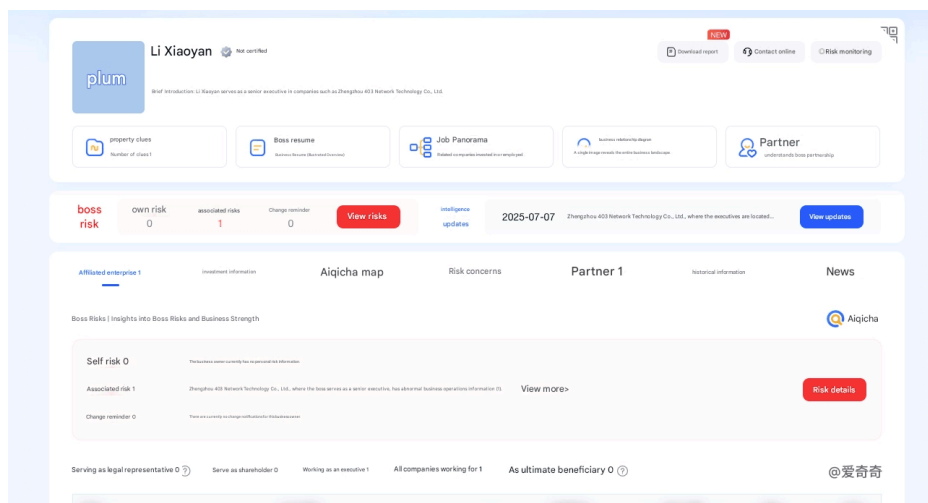


Figure 23: Aiqicha record for Li Xiaoyan — Supervisor (监事) of Zhengzhou 403 Network Technology.

Field	Value	Source
Full Name (Chinese)	李晓燕	Zhengzhou 403 registration; Aiqicha
Full Name (Pinyin)	Li Xiaoyan	Aiqicha
Role at Zhengzhou 403	Supervisor (监事)	Aiqicha company registration
Shareholding	0% — No equity stake	Aiqicha
Legal Representative roles	None (0 companies)	Aiqicha
Total company affiliations	1 (Zhengzhou 403 only)	Aiqicha
Ultimate Beneficiary roles	None	Aiqicha
Business partner	Zhang Liye (1 collaboration)	Aiqicha partner data
Aiqicha Person ID	83c6efa69a81b322e5c7e986f8585cba	Aiqicha

4.4 APT31 Background

APT31 (Violet Typhoon / Judgment Panda / ZIRCONIUM) conducts cyber operations on behalf of the **Hubei State Security Department (HSSD)**, a provincial MSS branch in Wuhan ([US DoJ indictment](#), March 2024; [Rewards for Justice](#)). Documented targets include:

- US White House, DoJ, Commerce, Treasury, State Department
- US Congress members (Democratic and Republican senators)
- Defense Industrial Base, aerospace, telecom, energy, financial sectors
- Norwegian government ([PST attribution](#), 2018), Finnish Parliament ([NBI investigation](#), 2020–2021), Hong Kong pro-democracy activists

In 2010, HSSD established **Wuhan Xiaoruizhi Science and Technology** as a front company. The [US DoJ March 2024 indictment](#) named seven defendants and formally designated Wuhan XRZ as an MSS front company. Concurrent with the indictment, the [US Treasury imposed sanctions](#) on Wuhan XRZ and two of the defendants, and the Department of State announced a [Rewards for Justice bounty of up to \\$10 million](#).

4.5 Dual-Track Attribution

Attribution Track	Confidence	Primary Evidence
Dragon Breath APT (APT-Q-27)	 HIGH	LetsVPN lure match, IOCTL architecture, shared C2, cert revocation
APT31 / Wuhan XRZ personnel nexus	 MEDIUM	Zhang Liye correlated via Breachedforums leaked data to Xiaoruizhi personnel (Intrusion Truth 2023)

The Chinese contractor ecosystem (documented in i-SOON leak) demonstrates individuals routinely work across multiple MSS-affiliated entities. APT-Q-27 and APT31 both operate under MSS tasking. Possible interpretations: (1) Zhang Liye migrated from Wuhan XRZ to establish Zhengzhou 403 as a new signing vehicle; (2) Zhengzhou 403 serves both APT-Q-27 and APT31 as shared infrastructure; (3) the connection is circumstantial. Infrastructure correlation required to resolve.

These tracks are not mutually exclusive — the Chinese contractor ecosystem routinely sees individuals serve multiple MSS-affiliated entities simultaneously, and Zhengzhou 403 may function as shared signing infrastructure spanning both APT-Q-27 operational activity and APT31 personnel networks.

5. MalwareBazaar Samples & C2 Infrastructure

5.1 Certificate-Tagged Sample Catalog

Three samples bearing the Zhengzhou 403 EV certificate (serial `4668EDFA623554CF0B48F401`) are cataloged on [MalwareBazaar](#) under the tag `Zhengzhou-403-Network-Technology-Co-Ltd`. All three are classified as either **CobaltStrike beacons** or **signed loaders** (possibly DonutLoader or Telegram-based loading), and all three communicate with the same CobaltStrike C2 endpoint.

#	Filename	SHA-256	Classification
1	<code>letsvpn-3.12.3.exe</code>	<code>e515a6e0738e699df2b569fafc234c534ac4417f29c2b4684accda275bfec79</code>	CobaltStrike / Signed Loader (LetsVPN decoy)
2	<code>tsetup-x64.5.13.1.exe</code>	<code>ce38c96a69a8a1c6828e11742355c41b878198e08d7efbe73eefa1b5cbe623c5</code>	CobaltStrike / Signed Loader (Telegram Desktop decoy)
3	<code>SearchUpdate.exe</code>	<code>00c250adb21fd14148f963a92fb5ec21d5eac2cd2f67501f03e28c5e7135422e</code>	CobaltStrike / Signed Loader

All three samples are signed with the same explicitly revoked GlobalSign EV certificate and tagged on MalwareBazaar with loader and CobaltStrike indicators. The presence of DonutLoader or Telegram-based loading mechanisms is consistent with Chinese APT multi-stage deployment chains where a signed loader serves as the initial trust-bypass stage before deploying shellcode or retrieving the final payload from a messaging platform channel.

Sample #2 — `tsetup-x64.5.13.1.exe`: Trojanized Telegram Desktop Confirmed

Dynamic analysis of `tsetup-x64.5.13.1.exe` (SHA-256: `ce38c96a69a8a1c6828e11742355c41b878198e08d7efbe73eefa1b5cbe623c5`) conducted via JoeSandbox (Analysis ID: 1679094) confirms this sample is a **trojanized Telegram Desktop installer** bearing the explicitly revoked Zhengzhou 403 EV certificate. The filename `tsetup-x64.5.13.1.exe` is a direct impersonation of the legitimate Telegram Desktop installer naming convention (`tsetup` = Telegram setup). The sample presents as a functional Telegram installer to avoid victim suspicion while executing its malicious payload chain — structurally identical to the dual-installer pattern documented in RONGINGLOADER, where a benign decoy application is installed alongside the malicious component.

This finding directly corroborates QiAnXin's attribution of trojanized Telegram installers to Dragon Breath APT-Q-27, and confirms that Zhengzhou 403 Network Technology Co., Ltd. served as the certificate signing vehicle for both the LetsVPN-themed and Telegram-themed lure families within the same campaign infrastructure. The use of a single compromised EV certificate across multiple lure brands indicates **centralized certificate management at the operator level** rather than per-campaign certificate acquisition.

5.2 Shared C2 Endpoint: oss-aws.1nb.xyz

Investigation of the three MalwareBazaar samples bearing the Zhengzhou 403 certificate reveals a **shared CobaltStrike**

Beacon C2 endpoint: `http://oss-aws.1nb.xyz/`

Field	Value
C2 Domain	<code>oss-aws.1nb.xyz</code>
Protocol	HTTP (CobaltStrike Malleable C2)
Confirmed Across	All three MalwareBazaar Zhengzhou 403-tagged samples
Infrastructure Response	HTTP 403 Forbidden — served by NgxFence WAF/CDN
WAF Provider	NgxFence — Chinese-operated WAF/CDN
Domain Construction	Deliberate mimicry of AWS S3 + Alibaba OSS naming to blend into cloud traffic
Geo-filtering	403 response confirms active geo-IP blocking against non-Chinese / researcher IPs

Domain masquerade analysis: `oss-aws.1nb.xyz` — "oss" references Alibaba Cloud Object Storage Service; "aws" references Amazon Web Services. Engineered to appear as a legitimate cloud storage endpoint in SIEM alerting. Consistent with Dragon Breath / APT-Q-27 documented use of cloud-mimicry domains.

NgxFence significance: Deployment of a Chinese WAF for a CobaltStrike C2 is consistent with Chinese threat actor operational patterns documented by Hunt.io and Rapid7 (2025–2026), where Chinese CDN providers are used to mask C2 origin and return 403/404 to non-beacon requests while routing valid beacon traffic to the actual team server.

Block immediately: `oss-aws.1nb.xyz` — Block at DNS, proxy, and firewall. Any beacon traffic to this domain from within your environment indicates active CobaltStrike compromise. Monitor for outbound HTTP beaconing patterns (periodic intervals, consistent URI, encoded body) to this domain.

5.3 jnsupx.exe — Dropper Analysis & Kill Chain Reconstruction

Dynamic analysis of `jnsupx.exe` (SHA-256: `8fc822b3e285030c6dcb36d7b9a52426e2b3eeaf643a28ef2cfcd1cb0709906f` , 1,014.50 KB, detection: 57/72) reveals the **primary dropper responsible for deploying** `dragoncore_k.sys` into target environments. The sample is UPX-packed, contains debug environment detection, persistence mechanisms, self-deletion capability, and long-sleep anti-sandbox controls — a behavioral profile consistent with a mature, operationally deployed loader.

8fc822b3e285030c6dcb36d7b9a52426e2b3eeaf643a28ef2cfd1cb0709906f			
101.198.192.8	1 / 94	55992	CN
101.200.42.181	0 / 94	37963	CN
101.200.60.14	0 / 94	37963	CN
101.206.209.10	0 / 94	4837	CN
101.226.27.114	0 / 94	4811	CN
101.226.27.115	0 / 94	4811	CN
101.32.212.153	0 / 94	132203	SG
101.33.20.125	1 / 94	139341	SG
...			
Execution Parents (2) ⌵			
Scanned	Detections	Type	Name
2024-12-25	51 / 71	Win32 EXE	8be3d9779092cc07a72594bb77756b7a.virus
2024-12-30	53 / 72	Win32 EXE	2024-12-30_01e00386ecc0739586956f00a5e6addb_icedid
Dropped Files (13) ⌵			
Scanned	Detections	File type	Name
2025-10-02	17 / 72	Win32 EXE	panmapOym.dll
2026-04-23	1 / 72	Win32 EXE	<u>1da4ff001d239a54fab50eb7c3cbc985db392a3d4405e19c3a5d2035d591004.sys</u>
2025-08-18	0 / 72	Win32 EXE	usbhub.sys
2025-12-23	24 / 72	Win32 EXE	iesetupJ.R.dll
2025-07-13	0 / 72	Win32 EXE	CulwinrscmdrELuH.dll
2024-12-21	30 / 71	Win32 EXE	CulCoreMmResp4.dll
2026-04-22	27 / 72	Win32 EXE	CulcomcatQPGUWE.dll
?	?	file	515143abc506146f0050a552379f039d4aee6a1fa24702078ca77f1ad5259ea
?	?	file	5e042db6f62e7446e734b9602c57aaf6c350c212e8fa42ea961c92fe231ac06
?	?	file	92e4fb1fd08a2335a5e4c59250f61a378a6ee7843118fc9f08546c4d6b906e0
...			

Figure 24: Dynamic analysis of `jnsupx.exe` — UPX-packed dropper deploying `dragoncore_k.sys` .

6. MITRE ATT&CK Mapping

Technique ID	Technique	Application
T1068	Exploitation for Privilege Escalation	IOCTL abuse escalates from Administrator to Ring 0 execution.
T1014	Rootkit	Driver loaded at Ring 0 enabling invisible system state modification.
T1562.001	Impair Defenses: Disable or Modify Tools	Terminates EDR/AV via <code>ZwTerminateProcess</code> from kernel context.
T1543.003	Create System Process: Windows Service	Driver deployed via <code>CreateServiceA</code> through SCM.
T1195.001	Supply Chain: Compromise Software Dependencies	WHQL-signed driver used to bypass code integrity enforcement.
T1588.002	Obtain Capabilities: Tool	Acquisition of vulnerable signed driver as BYOVD component.
T1055.009	Process Injection: Process Hollowing	Kernel PEB attachment and manipulation via <code>KeStackAttachProcess</code> .
T1564.010	Hide Artifacts: Process Argument Spoofing	In-memory PEB CommandLine modification to deceive EDR telemetry.
T1057	Process Discovery	Process name enumeration via <code>PsGetProcessImageFileName</code> .
T1518.001	Security Software Discovery	Filter targets EDR/AV process list.
T1497	Virtualization/Sandbox Evasion	Rate-limiting anti-detection control via timestamp gating.
T1622	Debugger Evasion	Global kill switch flag for dormant deployment.

7. Indicators of Compromise

7.1 Files

Filename	SHA-256	Notes
dragoncore_k.sys	1da4f7f001d239a54fab50eb7c3cbc985db392a3d4405e19c3a5d2035d591004	Vulnerable BYOVD kernel driver
letsvpn-3.12.3.exe	e515a6e0738e699df2b569fafc234c534ac4417f29c2b4684accda275bfec79	LetsVPN-branded payload, same certificate
tsetup-x64.5.13.1.exe	ce38c96a69a8a1c6828e11742355c41b878198e08d7efbe73eefa1b5cbe623c5	CobaltStrike / Signed Loader — Telegram Desktop decoy
SearchUpdate.exe	00c250adb21fd14148f963a92fb5ec21d5eac2cd2f67501f03e28c5e7135422e	CobaltStrike / Signed Loader — cert tag match
RONINGLOADER MSI dropper	da2c58308e860e57df4c46465fd1cfc68d41e8699b4871e9a9be3c434283d50b	Dragon Breath APT-Q-27 (Elastic, Nov 2025)
jnsupx.exe	8fc822b3e285030c6dcb36d7b9a52426e2b3eeaf643a28ef2cfcd1cb0709906f	Primary dropper for dragoncore_k.sys ; UPX-packed, anti-sandbox
ollama.sys (Dragon Breath)	Retrieve from Elastic / VirusTotal	Kunming Wuqi cert — identical IOCTL pattern

7.2 Certificate

Field	Value	Action
Serial Number	4668EDFA623554CF0B48F401	Block ALL files bearing this serial
Subject CN	Zhengzhou 403 Network Technology	Flag any file signed by this entity
Issuing CA	GlobalSign GCC R45 EV CodeSigning 2020	GlobalSign confirmed abuse revocation
Cert SHA256	EE79212E518952916DA9643830DB120592...	Block by certificate thumbprint
Status	EXPLICITLY REVOKED by issuer	Do not trust even within validity window

7.3 Network

Indicator	Type	Notes
oss-aws.1nb.xyz	CobaltStrike C2 domain	Block at DNS/proxy/firewall; geofiltered behind NgxFence WAF

7.4 Behavioral Indicators

- CreateService events referencing dragoncore_k.sys or drivers signed by certificate serial 4668EDFA623554CF0B48F401
- CreateFile calls targeting \\.\3e0ac7f
- DeviceIoControl calls with code 0x22201C
- Abrupt termination of EDR/AV processes (MsMpEng.exe , CrowdStrike Falcon, Carbon Black, SentinelOne) without a preceding uninstall event
- Service registration for kernel-mode drivers signed by unrecognized Chinese entities not in the Microsoft Vulnerable Driver Blocklist
- Outbound HTTP beaconing to oss-aws.1nb.xyz at periodic intervals

7.5 YARA Rule

```
rule BYOVD_dragoncore_k_sys {
  meta:
    description = "Detects dragoncore_k.sys BYOVD driver - Zhengzhou 403 / Dragon Breath APT"
    author      = "Alex Necula"
```

```

date      = "2026-04-22"
tlp       = "WHITE"

strings:
  $device = { 5C 00 5C 00 2E 00 5C 00 66 00 33 00 65 00
              30 00 61 00 63 00 37 00 66 00 }
  $ioctl  = { 1C 20 22 00 }

condition:
  uint16(0) == 0x5A4D and filesize < 500KB and ($device or $ioctl)
}

```

8. Disclosure & Defensive Recommendations

8.1 Coordinated Vulnerability Disclosure

This vulnerability is being addressed via **CVD**. Primary remediation target: inclusion of `dragoncore_k.sys` in the **Microsoft Windows Vulnerable Driver Blocklist (Driver.stl)**. Reported to MSRC at <https://msrc.microsoft.com/report/> under Windows Hardware Developer Program abuse.

8.2 Immediate Actions

- **Block by hash:** Deploy WDAC or AppLocker policy blocking `dragoncore_k.sys` by SHA-256 `1da4f7f001d239a54fab50eb7c3cbc985db392a3d4405e19c3a5d2035d591004`
- **Block by cert serial:** Add `4668EDFA623554CF0B48F401` to EDR block rules and SIEM alerting
- **Enable Microsoft Vulnerable Driver Blocklist:** Settings → Windows Security → Device Security → Core Isolation → Microsoft Vulnerable Driver Blocklist: **ON**
- **Block C2:** Add `oss-aws.1nb.xyz` to DNS blocklist and firewall rules immediately

8.3 Detection Rules

- Alert on `CreateService` events for kernel-mode drivers signed by novel unrecognized Chinese entities
- Alert on `CreateFile` calls to `\\.\3e0ac7f` and `DeviceIoControl(0x22201C)`
- Hunt retroactively for driver hash across endpoint telemetry
- Monitor for `PEB.CommandLine` field modification events via kernel ETW providers (MDE Advanced Hunting)

8.4 Strategic Measures

- Enforce **HVCI** on all endpoints
- Restrict `SeLoadDriverPrivilege` to minimum necessary accounts
- Subscribe to **MalwareBazaar** / **VirusTotal feeds** filtered by signing certificate CN for proactive driver threat intelligence
- **Treat the signing entity as a threat indicator** — any file signed by an unrecognized Chinese technology company with no verifiable commercial history should be treated with extreme suspicion

9. Conclusion

`dragoncore_k.sys` represents a credible, immediately weaponizable threat to enterprise endpoint security. Its zero-input-validation IOCTL interface, combined with a valid WHQL signature from Zhengzhou 403 Network Technology Co., Ltd., makes it an effective BYOVD component for EDR neutralization in targeted intrusions.

The surrounding intelligence elevates this finding well beyond a routine driver vulnerability:

- EV certificate explicitly revoked by GlobalSign
- Registered address confirmed as an uninhabited hotel-floor address.
- `letsvpn-3.12.3.exe` signed by the same certificate directly matches the Dragon Breath **RONINGLOADER** LetsVPN lure pattern
- IOCTL architecture (`0x22201C` vs `0x222000`) supports version iteration of the same codebase
- Shared CobaltStrike C2 (`oss-aws.1nb.xyz`) across all three certificate-tagged samples confirms active operational infrastructure
- In-memory command-line modification engine confirms purpose-built offensive tooling, not accidental vulnerability
- Personnel-level connection between founder Zhang Liye and OFAC-sanctioned APT31 front company Wuhan Xiaoruizhi introduces a dual-track APT attribution assessment

This research demonstrates that BYOVD threat intelligence must not stop at the technical vulnerability. The signing entity is a first-class intelligence artifact. Shell company structures, EV certificate acquisition patterns, revocation

histories, co-signed payload families, and personnel records are underutilized attribution signals that can bridge kernel-level vulnerability analysis with APT campaign tracking.

10. References

1. Elastic Security Labs — [RONINGLOADER: DragonBreath's New Path to PPL Abuse](#) (Jia Yu Chan, Salim Bitam, November 15, 2025)
 2. US DOJ Indictment — APT41 / Chengdu 404 Network Technology (August 2020)
 3. Mandiant — *Hunting for Attestation Signed Malware* (Google Cloud Blog, 2022)
 4. Sophos — *Signed Driver Malware Moves Up the Software Trust Chain* (December 2022)
 5. Rapid7 — *Winos 4.0 via Trojanized LetsVPN Installers / Catena Loader* (May 2025)
 6. Cyble Research — *New Malware Campaign Targets LetsVPN Users* (November 2023)
 7. Trend Micro — *Void Arachne / LetsVPN / Winos Backdoor* (June 2024)
 8. Microsoft Security Advisory ADV230001 — *Maliciously Signed WHQL Drivers* (2023)
 9. Intrusion Truth — [Trouble in Paradise: Wuhan Xiaoruizhi Science and Technology](#) (May 2023)
 10. [malware.news](#) — [Trouble in Paradise](#) (APT31 / Zhang Liye analysis, 2023)
 11. US Treasury OFAC — *Sanctions: Wuhan Xiaoruizhi Science and Technology Co., Ltd. and APT31 operators* (March 2024)
 12. US DoJ — *Indictment: Seven APT31 Operators / Wuhan Xiaoruizhi* (March 2024)
 13. UK Government — *Sanctions: APT31 / Wuhan XRZ / UK Electoral Commission intrusion* (2024)
 14. [Hunt.io](#) — [Inside China's Hosting Ecosystem: 18,000+ Malware C2 Servers Mapped](#) (January 2026)
 15. MalwareBazaar — [Tag: Zhengzhou-403-Network-Technology-Co-Ltd](#)
 16. ReliaQuest — *Anxun and Chinese APT Activity* (2025)
 17. SecurityOnline — *Dragon Breath APT Deploys RoningLoader* (November 2025)
 18. JoeSandbox — Analysis ID 1679094: `tsetup-x64.5.13.1.exe` dynamic analysis (trojanized Telegram Desktop installer)
 19. QiAnXin Threat Intelligence Blog — *Dragon Breath APT-Q-27 trojanized Telegram installer attribution*
 20. US Department of State — *Rewards for Justice: [APT31 / Wuhan Xiaoruizhi Science & Technology Company, Ltd.](#)*
 21. Norway Police Security Service (PST) / Cyber Defense Magazine — [Norway Blames China-Linked APT31 for 2018 Government Hack](#) (June 2021)
 22. The Hacker News — [Finland Blames Chinese Hacking Group APT31 for Parliament Cyber Attack](#) (March 2024)
-

— END OF REPORT —

TLP:WHITE — Approved for unrestricted distribution within the security community.

Disclaimer: For educational and defensive research purposes only. Unauthorized exploitation of described techniques is illegal and unethical.

If you or your organisation have been impacted by an incident of this nature or similar, please reach out to the Ransom-ISAC team at ransom-isac.org or contact us at contact@ransom-isac.org.

Source: <https://ransom-isac.com/blog/dragonbreath-dragon-in-the-kernel/>