

ValleyRAT: A Chinese APT's Rust Loader, a Cardiff University GovRoam Relay, and a Hong Kong C2 With a Gmail Abuse Contact

 intel.breakglass.tech/post/valleyrat-cardiff-university-govroam-rust-loader-hong-kong-c2

Breakglass Intelligence

April 22, 2026



MEDIUM

THREAT INTEL

ValleyRAT: A Chinese APT's Rust Loader, a Cardiff University GovRoam Relay, and a Hong Kong C2 With a Gmail Abuse Contact

Malware analysis · C2 infrastructure · APT attribution

@BreakGlassIntel

TL;DR

Two ValleyRAT samples surfaced on MalwareBazaar within days of each other. Both target Chinese-speaking users through trojanized software. Both belong to the same campaign family — but their infrastructure tells two very different stories.

The first sample, [malware64.dll](#), is a KCP-based C2 communication module that phones home to 103.215.77[.]17:4488 in Hong Kong. The hosting provider is LANLIAN INTERNATIONAL HOLDING GROUP LIMITED. The abuse contact is a Gmail address. The server has WinRM (port 5985) open to the internet. VirusTotal shows 78+ related malware samples communicating with this same IP. The C2 is live as of this writing.

The second sample is a Rust-compiled loader disguised as "Microsoft OneDrive Sync Engine." It runs multi-layer sandbox evasion, decrypts an embedded payload with AES-256-CBC, and drops a full ValleyRAT core DLL. Its C2 address is not an IP or a throwaway domain — it is [v52-83fbf297.govroam.cf.ac.uk](#), a hostname on Cardiff University's GovRoam network. The

hostname pattern suggests a VPN-authenticated or 802.1x-enrolled device — likely a compromised researcher or student laptop that was repurposed as a C2 relay. Those ports are now closed, suggesting the device was cleaned or disconnected from the network.

The convergence of a live Hong Kong C2 with a compromised British university endpoint illustrates how Chinese APT groups layer disposable academic infrastructure on top of persistent commercial hosting.

What This Report Adds to the Public Record

- Documents a ValleyRAT C2 relay operating from Cardiff University's GovRoam (eduroam-adjacent) network — a compromised academic endpoint used as disposable relay infrastructure
- Identifies the specific hostname pattern (`v52-83fbf297`) as consistent with 802.1x/VPN-authenticated devices, suggesting a compromised researcher or student laptop
- Recovers the Rust loader's full sandbox evasion chain: username checks, environment string detection, and filesystem artifact scanning
- Extracts the AES-256-CBC encrypted stage-2 ValleyRAT core DLL from the Rust loader's `.rdata` section
- Maps 78+ related samples on the Hong Kong C2 (103.215.77[.]17) via VirusTotal
- Confirms the Hong Kong C2 runs WinRM on port 5985, indicating a compromised or actor-controlled Windows host
- Links both samples through shared Chinese-language artifacts and ValleyRAT behavioral signatures
- Provides YARA rules and IOCs for detection

If any of this overlaps with your prior work — particularly the Cardiff GovRoam relay or this specific LANLIAN-hosted C2 — please reach out. We will update this post and credit the earlier source.

Sample 1: malware64.dll — The KCP C2 Module

Property	Value
SHA256	<code>d47aac6bf3946c1fd7b88106af11dfd32c7af3d9a72089e40ffef6555c9182ba</code>
File type	PE32+ DLL (x64)
Size	196 KB
Compile time	2026-04-07
Protocol	KCP (reliable UDP)

Property	Value
C2	103.215.77[.]17:4488
VT detection	16/76

This DLL is a C2 communication module. It implements the KCP protocol — a reliable, low-latency transport layer built on UDP, popular in Chinese gaming and tunneling software and increasingly adopted by Chinese malware authors for its NAT-traversal properties and lower visibility compared to TCP.

The C2 address is stored as a reversed wide string in the `.rdata` section. Flipping it yields the connection target: `103.215.77[.]17` on port `4488`.

The most telling artifact is the parent module import name: `上线模块.dll` — literally "Online Module DLL" in Chinese. This is a hallmark of ValleyRAT and its associated loader ecosystem. The Chinese-language internal naming is consistent across ValleyRAT tooling and reflects the operational language of the development team.

The C2 at `103.215.77[.]17` is allocated to LANLIAN INTERNATIONAL HOLDING GROUP LIMITED (Hong Kong). Shodan confirms port 5985 (WinRM) is open. The abuse contact is `Kchan2789@gmail[.]com` — a Gmail address, not a hosting abuse desk. VirusTotal shows 78+ malware samples communicating with this IP across multiple campaigns. The C2 is live as of this investigation.

Sample 2: The Rust Loader and Its Embedded ValleyRAT Core

Property	Value
SHA256	<code>4cf32bd41a17e51520ddd0b0aea06e9792ceb9c3dcb039f166324e6c73c7a65c</code>
File type	PE32 EXE (x86)
Size	263 KB
Language	Rust (PDB: <code>loader.pdb</code>)
Disguise	"Microsoft OneDrive Sync Engine"
Stage-2 encryption	AES-256-CBC
Stage-2 SHA256	<code>7d48049da5a7f33f4cc6a45a62b2b3a972ffd934403d9cb956c40ff28bfdab9e</code>
C2	<code>v52-83fbf297.govroam.cf.ac[.]uk:8044, :9044, :98</code>
Campaign ID	<code>x9y8z7w6v5u4t3s2r1q0p9o8n7m6l5k4</code>

Property	Value
VT detection	34/76

The Rust loader is the more technically interesting of the two samples. A 263KB executable with the PDB path `loader.pdb`, compiled with Rust and presenting itself as Microsoft's OneDrive synchronization engine. It carries an encrypted stage-2 payload in its `.rdata` section — 107KB of data at entropy 7.671, effectively indistinguishable from random without the key.

The Cardiff University Connection

This is the finding that prompted this writeup.

The stage-2 ValleyRAT core DLL does not connect to a bulletproof hoster in Hong Kong or a disposable VPS. Its C2 address is:

`v52-83fbf297.govroam.cf.ac[.]uk`

Let's break that down:

- `cf.ac.uk` — the domain registered to Cardiff University, Wales, United Kingdom
- `govroam.cf.ac.uk` — Cardiff's deployment of [GovRoam](#), the UK government and academic roaming WiFi federation (similar to eduroam but extended to government departments)
- `v52-83fbf297` — a hostname pattern consistent with VPN or 802.1x-authenticated devices. The `v52` prefix and hex suffix `83fbf297` suggest a dynamically assigned hostname for an authenticated endpoint — a laptop, workstation, or mobile device that joined the GovRoam network with institutional credentials

DNS resolution confirms this hostname resolves (or resolved) to 131.251.242.151, which falls within Cardiff University's allocated IP space.

What This Means

A device on Cardiff's GovRoam network was compromised and repurposed as a C2 relay. A researcher, student, or government visitor's device — already compromised or infected on-network — was configured as a relay, exploiting the university's clean IP reputation. The device has since disconnected or been remediated; all three C2 ports are now closed.

Academic networks are attractive for C2 relay: university IP ranges are broadly allowlisted, GovRoam/eduroam endpoints cycle frequently making attribution difficult, and network monitoring tends to focus on bandwidth abuse rather than C2 beaconing. The choice of three fallback ports (8044, 9044, 98) suggests the operators anticipated intermittent connectivity — exactly what you'd expect from a relay that depends on a user's laptop being powered on and connected to campus WiFi.

The Hong Kong C2: 103.215.77.17

Property	Value
IP	103.215.77[.]17
ASN	LANLIAN INTERNATIONAL HOLDING GROUP LIMITED
Location	Hong Kong
Abuse contact	Kchan2789@gmail[.]com
Open ports	4488 (KCP/UDP), 5985 (WinRM)
Status	LIVE
VT relations	78+ communicating malware samples

Unlike the ephemeral Cardiff relay, this Hong Kong IP is persistent infrastructure. Seventy-eight or more samples have phoned home to it across months of activity. The abuse contact is a personal Gmail address rather than a hosting provider's abuse desk — suggesting either a small operation with limited abuse response, or an actor-controlled registration. Port 5985 (WinRM) confirms this is a Windows host with remote management exposed to the internet.

Sandbox Evasion: What the Rust Loader Checks

The Rust loader runs a multi-layer environment check before decrypting its payload. If any check triggers, execution terminates silently — no crash, no error message, no artifacts. The checks include:

- Username blocklist — Compares the current Windows username against known sandbox and analyst names (sandbox, malware, virus, test, sample, and automated platform defaults)
- Environment string detection — Checks for environment variables associated with VMware, VirtualBox, Hyper-V, and common analysis tools
- File system checks — Scans for directories and files associated with debugging software, AV installations, and monitoring agents

If any check triggers, execution terminates silently. The Rust compilation adds an additional layer of difficulty — Rust binaries are notoriously tedious to reverse-engineer due to complex control flow graphs from the ownership model, monomorphized generics, and panic-handling boilerplate.

Decryption: AES-256-CBC and the Embedded Stage-2

The encrypted stage-2 lives in the Rust loader's `.rdata` section as a 107KB blob. The entropy of 7.671 (out of a maximum 8.0) confirms it is encrypted or compressed data — in this case, AES-256-CBC encrypted.

After passing all sandbox checks, the loader derives the AES-256 key and IV from hardcoded values, decrypts the `.rdata` blob, maps the resulting PE into memory, and transfers execution. The decrypted output is a 107KB MSVC C++ DLL — the ValleyRAT core.

The ValleyRAT Core DLL

Property	Value
SHA256	7d48049da5a7f33f4cc6a45a62b2b3a972ffd934403d9cb956c40ff28bfdab9e
Compiler	MSVC C++
Key RTTI classes	CKernelManager, CTcpSocket
C2 ports	8044, 9044, 98
Chinese artifacts	Chinese characters in C2 configuration strings

The core DLL contains RTTI class names consistent with ValleyRAT: CKernelManager (command dispatch, persistence, module management) and CTcpSocket (C2 communication). Chinese characters in the C2 configuration reinforce attribution to a Chinese-speaking actor.

The campaign ID `x9y8z7w6v5u4t3s2r1q0p9o8n7m6l5k4` is a sequential alphanumeric pattern — potentially a placeholder or internal campaign tag. Three fallback ports (8044, 9044, 98) on the same hostname provide redundancy. Port 98 falls in the well-known range and could blend with legitimate traffic on a university network.

Infrastructure Overlap and Campaign Links

These two samples are linked by more than malware family classification:

Indicator	Sample 1 (malware64.dll)	Sample 2 (Rust loader)
Malware family	ValleyRAT (C2 module)	ValleyRAT (loader + core)
Chinese language artifacts	上线模块.dll import	Chinese chars in C2 config
Target audience	Chinese-speaking users	Chinese-speaking users
Distribution	Trojanized Chinese software	Trojanized Chinese software

Indicator	Sample 1 (malware64.dll)	Sample 2 (Rust loader)
C2 protocol	KCP (reliable UDP)	TCP (multi-port fallback)
Infrastructure type	Persistent commercial (HK)	Ephemeral academic relay (UK)

The infrastructure strategy is deliberate: persistent Hong Kong commercial hosting as the backbone, ephemeral academic relays as disposable frontends. When the Cardiff relay goes down, the campaign's core infrastructure remains intact.

ValleyRAT (also tracked as Farfli, Winos, PoisonMouse) targets Chinese-speaking users through trojanized software. The KCP protocol in Sample 1 reflects a broader trend — KCP adoption in Chinese malware has increased since 2025 for its NAT-traversal and low-latency properties.

IOC Table

File Hashes

Hash	Description
d47aac6bf3946c1fd7b88106af11dfd32c7af3d9a72089e40ffef6555c9182ba	malware64.dll — KCP C2 communication module
4cf32bd41a17e51520ddd0b0aea06e9792ceb9c3dcb039f166324e6c73c7a65c	Rust loader (disguised as OneDrive Sync Engine)
7d48049da5a7f33f4cc6a45a62b2b3a972ffd934403d9cb956c40ff28bfdab9e	Decrypted ValleyRAT core DLL (stage-2)

Network Indicators

Indicator	Type	Description
103.215.77[.]17	IPv4	Hong Kong C2, LANLIAN INTL HOLDING GROUP, LIVE
103.215.77[.]17:4488	IP:Port	KCP C2 endpoint
103.215.77[.]17:5985	IP:Port	WinRM (remote management)

Indicator	Type	Description
v52-83fbf297.govroam.cf.ac[.]uk	Hostname	Cardiff University GovRoam relay (ports CLOSED)
131.251.242[.]151	IPv4	Resolved IP for Cardiff relay

Network Ports (Stage-2 C2)

Port	Protocol	Status
8044	TCP	Closed
9044	TCP	Closed
98	TCP	Closed

Campaign Identifiers

Indicator	Context
x9y8z7w6v5u4t3s2r1q0p9o8n7m6l5k4	Campaign ID in Rust loader config
上线模块.dll	Parent module import name (Chinese: "Online Module DLL")
loader.pdb	PDB path in Rust loader

Abuse Contacts

Contact	Context
kchan2789@gmail[.]com	Registered abuse contact for 103.215.77[.]17

MITRE ATT&CK Mapping

Tactic	Technique	ID	Notes
Initial Access	Supply Chain Compromise	T1195.002	Trojanized Chinese software distribution
Execution	Native API	T1106	Direct Windows API calls for payload execution

Tactic	Technique	ID	Notes
Defense Evasion	Masquerading	T1036.005	Rust loader disguised as "Microsoft OneDrive Sync Engine"
Defense Evasion	Obfuscated Files or Information: Encrypted/Encoded File	T1027.013	AES-256-CBC encrypted stage-2 in .rdata
Defense Evasion	Virtualization/Sandbox Evasion: System Checks	T1497.001	Username, environment, and filesystem checks
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	Runtime decryption of ValleyRAT core DLL
Command and Control	Application Layer Protocol	T1071	KCP over UDP (Sample 1), TCP multi-port (Sample 2)
Command and Control	Non-Standard Port	T1571	Ports 4488, 8044, 9044, 98
Command and Control	Proxy: Multi-hop Proxy	T1090.003	Cardiff University relay as intermediate C2 hop
Command and Control	Fallback Channels	T1008	Three fallback ports on Cardiff relay
Resource Development	Compromise Infrastructure: Server	T1584.004	Compromised Cardiff GovRoam endpoint as relay

YARA Rule

```
rule ValleyRAT_RustLoader_CardiffRelay
{
    meta:
        author = "Breakglass Intelligence"
        description = "Detects ValleyRAT Rust loader with AES-256-CBC encrypted stage-2"
        date = "2026-04-20"
        reference = "https://intel.breakglass.tech/post/valleyrat-cardiff-university-govroam-rust-loader-hong-kong-c2"
        hash1 = "4cf32bd41a17e51520ddd0b0aea06e9792ceb9c3dcb039f166324e6c73c7a65c"
        hash2 = "d47aac6bf3946c1fd7b88106af11dfd32c7af3d9a72089e40ffef6555c9182ba"

    strings:
        $pdb = "loader.pdb" ascii
        $onedrive = "Microsoft OneDrive Sync Engine" wide
        $campaign = "x9y8z7w6v5u4t3s2r1q0p9o8n7m6l5k4" ascii
        $govroam = "govroam" ascii wide
        $cardiff = "cf.ac.uk" ascii wide
        $module_cn = { 0A 4E BF 7E 6A 6B 2E 00 64 00 6C 00 6C 00 } // 上线模块.dll in UTF-16LE
        $kcp_init = { 4B 43 50 00 } // "KCP\x00"
        $rtti_kernel = "CKernelManager" ascii
        $rtti_socket = "CTcpSocket" ascii

    condition:
        uint16(0) == 0x5A4D and
        filesize < 500KB and
        (
            ($pdb and $onedrive) or
            ($campaign) or
            ($govroam and $cardiff) or
            ($module_cn and $kcp_init) or
            ($rtti_kernel and $rtti_socket)
        )
}
```

Recommendations

For Cardiff University / Jisc:

- Investigate device **v52-83fbf297** in GovRoam authentication logs to identify the compromised user
- Review NetFlow logs for connections on ports 8044, 9044, and 98 from 131.251.242[.]151

For network defenders:

- Block 103.215.77[.]17 — live C2 serving 78+ malware families
- Monitor for KCP (reliable UDP) traffic on non-standard ports, particularly 4488

- Alert on outbound connections to *.govroam.*.ac.uk on ports 8044, 9044, or 98
- Deploy the YARA rule above against PE files entering your environment

For threat intelligence teams:

- Pivot on kchan2789@gmail[.]com in registration data for additional infrastructure
- Monitor LANLIAN INTERNATIONAL HOLDING GROUP LIMITED allocations — preferred hosting for this actor cluster
- Campaign ID x9y8z7w6v5u4t3s2r1q0p9o8n7m6l5k4 may appear in other ValleyRAT configs

Acknowledgments

Both samples were sourced from [abuse.ch MalwareBazaar](#), which continues to be an indispensable resource for the threat intelligence community. The researchers and submitters who contribute samples to MalwareBazaar make work like this possible.

ValleyRAT has been extensively documented by researchers at Fortinet, Zscaler, Proofpoint, and others. This report builds on their foundational work in tracking this malware family and its Chinese APT operators.

If you have additional context on these samples, the Cardiff GovRoam relay, or the LANLIAN hosting infrastructure — or if we've missed prior art — reach out via [DM on X](#) or at jeffery@breakglass.tech. We will update this post with proper credit.

Tags: ValleyRAT, Farfli, Winos, Chinese APT, Cardiff University, GovRoam, KCP Protocol, Rust Malware, AES-256-CBC, Hong Kong C2, Academic Infrastructure Compromise

Share  

Related Reports

[high](#)

[Multi-RAT Operation Dismantled: WaterHydra APT Nexus, Five AES Keys Recovered, and Live C2 Infrastructure Mapped Across Three Continents](#)

[3/7/2026](#)