ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 02 / 30 · C2 INFRASTRUCTURE

Port and Certificate Camouflage
Separating Real C2 From Feed Collisions

How C2 fleets reuse ports, TLS stacks and certificate names, and why raw threat feeds flag databases and labs as hostile

Two-week observation window ending 18 November 2026 · Data cutoff 15 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

7,934
Feed-labeled C2 endpoint records on 5,889 IPv4 hosts, in 81 countries and 697 BGP autonomous systems (657 hosting organizations)

93.9%
Brute Ratel C4 records (506 of 539) that share one Nginx reverse-proxy JARM

82.2%
ARTEX endpoints (412 of 501) that present one of two repeated certificate names

3 + 29
High-signal patterns and review patterns in the indicator set, all published at network level

What Is in This Report. 11 chapters and two appendices.

How C2 fleets reuse ports, TLS stacks and certificate names, and why raw threat feeds flag databases and labs as hostile

01	Executive Summary	04
02	How C2 Hides in Ports	07
03	TLS Stack and Hosting Monocultures	10
04	Certificate Camouflage	14
05	Benign Collisions That Inflate the Feed	18
06	What Passive Monitoring Misses	21
07	What Defenders Should Do	23
08	Detection Rules	25
09	Indicators	28
10	Scope and Limits	31
11	Sources	33
A	Indicators of compromise (0)	35
B	Detection rules (3 files)	36

IN SHORT

In a two-week window, with data up to 15 November 2026, Odin by Brandefense analysed 7,934 feed-labeled C2 endpoint records on 5,889 hosts. C2 fleets reuse a few TLS stacks, hosting providers and certificate names. One JARM covers 93.9% of Brute Ratel C4 records, and two certificate names cover 82.2% of ARTEX. Yet 1,876 records are benign collisions: MySQL auto-certificates, hosting panels and a vendor demo lab. Require two independent non-ASN signals before any automatic block.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week window, with data up to 15 November 2026, Odin by Brandefense analysed 7,934 feed-labeled C2 endpoint records on 5,889 hosts. C2 fleets reuse a few TLS stacks, hosting providers and certificate names. One JARM covers 93.9% of Brute Ratel C4 records, and two certificate names cover 82.2% of ARTEX. Yet 1,876 records are benign collisions: MySQL auto-certificates, hosting panels and a vendor demo lab. Require two independent non-ASN signals before any automatic block.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Command-and-control (C2) servers try to look ordinary. They listen on web ports, present certificates that name trusted brands or default appliances, and sit on cheap hosting. Threat feeds that label these servers often catch harmless systems in the same net. This report shows both sides: the camouflage patterns that defenders can hunt, and the collisions that turn into false positives.

1. **A few TLS stacks and hosting providers dominate several C2 fleets.**
   One Nginx reverse-proxy JARM covers 93.9% of feed-labeled Brute Ratel C4 records (506 of 539). Single hosting providers hold up to 98.8% of a family. The same reverse-proxy JARM also appears on commercial proxy nodes and a vendor simulation lab, so a JARM match alone is not enough to block.

2. **ARTEX reuses two certificate names across 82.2% of its fleet.**
   Two repeated certificate names, withheld because they may belong to third parties, cover 412 of 501 ARTEX endpoints. Default appliance names are harder to read. Droplets presenting the Ubiquiti name `unifi.local` show no overlap with the hosts that run CyberStrikeAI's four-port layout, so that name is a lead for review.

3. **Most port-3306 Daybreak hits are ordinary MySQL servers, not C2.**
   Of 1,701 Daybreak records, 1,592 sit on TCP 3306 and carry MySQL startup certificates. Across 59 Daybreak hosts we examined, candidate secondary C2 appeared on 26.7% of non-database candidates but only 8.0% of port-3306 hosts. Separately, 99.6% of MITRE Caldera records sit inside one security vendor's network.

Three Decisions for Leaders

1. **Require two independent non-ASN signals before an automatic block.** Hold a lone certificate-name or reverse-proxy JARM match at analyst review. Block only when it is backed by a verified self-signed certificate, a framework-specific TLS stack, a C2 port or a multi-port layout.
2. **Treat appliance-certificate alerts as enrichment, and add TLS 1.3 coverage.** Check the URI or endpoint context behind external Ubiquiti and non-VoIP Mumble certificate alerts over TLS 1.2. Pair TLS 1.3 rules on port 31337 with endpoint data.
3. **Restrict workstation egress to C2 implant, operator and database ports.** Block direct outbound connections from user segments to TCP 1337, 3306, 4321, 5001 to 5003, 8001, 8082, 8888, 9999, 31337 and 43211 unless there is a business need.

The Study in Numbers

Number	What it is
7,934	Feed-labeled C2 endpoint records on 5,889 IPv4 hosts, in 81 countries and 697 BGP autonomous systems (657 hosting organizations)
93.9%	Brute Ratel C4 records (506 of 539) that share one Nginx reverse-proxy JARM
82.2%	ARTEX endpoints (412 of 501) that present one of two repeated certificate names
72.2% / 73.7%	DarkSword (174 of 241) and SuperShell (126 of 171) records that share one TLS stack
26.7% / 8.0%	Examined Daybreak hosts with a candidate secondary C2: non-database candidates (4 of 15) versus port-3306 MySQL hosts (2 of 25)
1,831 + 45	Collision-prone records: 239 vendor lab records, 1,592 MySQL certificates on TCP 3306, and 45 hosting-panel records
3 + 29	High-signal patterns and review patterns in the indicator set, all published at network level

How to use this report.

Security leaders can read Chapter 1, Chapter 7 and Chapter 10. Detection engineers should start with the JARM analysis in Chapter 3, the certificate taxonomy in Chapter 4 and the rules in Chapter 8. Network teams can use the checklist in Chapter 7.

02

CHAPTER 02

How C2 Hides in Ports

IN SHORT

C2 frameworks either blend into web ports such as 443 and 8080 or bind their own listener and admin ports. The raw feed also mixes real C2 with databases, hosting panels, home routers and dual-use tools.

INSIDE THIS CHAPTER

The data set 07

Four port strategies 08

What the raw feed contains 08

02 How C2 Hides in Ports

The data set

Odin by Brandefense analysed 7,934 endpoint records. Each record is an IP, a port and a family label from upstream threat feeds. The feeds label 5,256 records confirmed, 2,454 suspected and 224 as management-port candidates (21 Daybreak and 203 AdaptixC2). These are the feeds' labels, not our verdicts.

Most records are single snapshots. For 7,700 of the 7,934 records (97.1%), the first-seen and last-seen times are the same. Counts in this report are therefore counts of records, not of deployments or growth.

FIGURE 1 · UPSTREAM-LABELED ENDPOINT CORPUS

ODIN BY BRANDEFENSE · TLP:CLEAR

Daybreak and CyberStrikeAI Lead Raw Volume, While Collisions Inflate Two Top Ranks

Records by labeled family across 697 BGP ASNs, most last seen 13-15 Nov 2026, n = 7,934



Scope & source: 7,934 endpoints across 5,889 IPs, 81 countries, 697 BGP ASNs / 657 orgs (#13 mitmproxy 157, #14 GoPhish 133, #16 Mirai 112).
What this does not show: Counts are records, not deployments or growth; *Daybreak/Caldera include collisions (Figs 3-4).

Figure 1: Daybreak and CyberStrikeAI lead raw volume, while collisions inflate two top ranks

Daybreak tops the raw ranking with 1,701 records, and MITRE Caldera sits ninth with 240. Both ranks are inflated by benign collisions, which Chapter 5 takes apart.

Four port strategies

Frameworks fall into four port strategies. Using a port that does not match the protocol is MITRE ATT&CK T1571, Non-Standard Port.

Port strategy	Ports	Frameworks and endpoint counts	What it means for defenders
Web and alt-web blending	TCP 443, 8080, 8443, 80	Brute Ratel C4 (256 on 443, 255 on 8080, 3 with TLS on 80), ARTEX (421 on 443), DarkSword (216 on 443), SuperShell (169 on 443), HypeAgent (118 on 443)	Passes web proxies easily, but the TLS stack stays visible to internet-wide JARM fingerprinting
Four-port orchestration	TCP 5001, 5002, 5003, 8082	CyberStrikeAI (237 endpoints on each port, 236 hosts with all four, plus 156 on 443)	Operator UI, API, WebSocket stream and agent listener on one host make a distinct four-port fingerprint
High-port implant and operator listeners	TCP 9999, 8888, 4321, 43211, 31337, 1337, 8001	VShell (219 on 9999), AdaptixC2 (82 on 4321, 11 on 43211), Sliver (20 operator gRPC on 31337; default implant mTLS uses 8888), Daybreak (13 on 1337, 1 on 8001), Cobalt Strike (10001 to 55555)	Avoids conflict with a decoy site on 443, but stands out in endpoint socket logs
Admin, RMM, panel and database overlap	TCP 1024, 3306, 1500, 1501	TacticalRMM (313 on 1024), Daybreak (28 on 1500, 17 on 1501, 1,592 raw hits on 3306)	Collides with RMM, hosting-panel and MySQL ports, so it causes false positives without application-layer checks

> **Watch both web ports.**
>
> Brute Ratel C4 records span 283 hosts, split evenly between TCP 443 (256 endpoints) and TCP 8080 (255 endpoints). Both ports appear together on 252 hosts. A TLS inspection policy that covers only port 443 misses half of these channels.

What the raw feed contains

Not every record is C2. The table below splits the 7,934 records by function.

Slice	Records	Share	What is inside
C2 and offensive tools	7,337	92.5%	Teamservers, plus 1,316 open-source AI red-team records (CyberStrikeAI 1,290, PentAGI 26), 525 dual-use RMM and phishing records (TacticalRMM 392, GoPhish 133) and 448 scanner and OAST records
IoT botnets and home routers	203	2.6%	Mirai (112), Hajime (49), Mozi (42); 18 records on one telecom network share a subscriber certificate name that likely reflects router defaults
Traffic distribution (TDS)	200	2.5%	Keitaro redirectors, including 45 `CN=SolidityGameServer` records on 20 hosts
Malware panels, scanners and ASM	194	2.4%	Malware panels (151, including Emotet 37 and AdaptixC2 22), OpenVAS (28), Daybreak candidates (14) and 1 attack-surface node

The scanner and OAST group covers mitmproxy (157), ARL (99), Burp (72), Nessus (46), Interactsh (27), Acunetix (24) and reNgine (23). With the 28 OpenVAS records counted under scanners elsewhere, the feed holds 476. These are dual-use tools, not proof of hostile use.

Some records need extra care. 180 records sit on consumer ISP networks (136 IPs across 43 networks); their addresses and certificate names are withheld. Another 54 records (0.7%, including 22 of 125 Cobalt Strike records) are flagged as contested.

03

CHAPTER 03

TLS Stack and Hosting Monocultures

IN SHORT

A single JARM fingerprint covers up to 93.9% of a C2 family, and a single hosting provider up to 98.8%. But generic reverse-proxy JARMs also appear on commercial proxies and labs, so pair every JARM match with a protocol or host signal.

INSIDE THIS CHAPTER

What JARM measures 10

Hosting concentration 10

Six families compared 11

The Brute Ratel C4 JARM is not unique 11

DarkSword and SuperShell share one stack 12

03 TLS Stack and Hosting Monocultures

What JARM measures

JARM sends ten crafted TLS `ClientHello` messages and hashes the server's replies into a 62-character fingerprint. Servers with the same TLS library and configuration produce the same JARM. That makes it good for clustering, but it describes the TLS stack, not the program behind it.

Hosting concentration

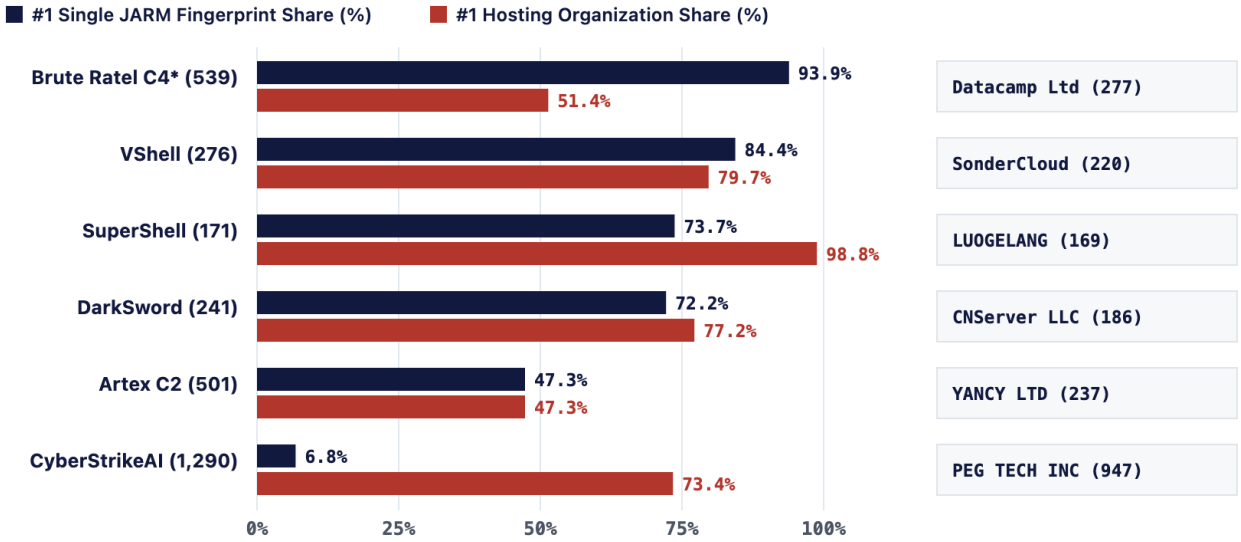
The records span 697 BGP autonomous systems and 657 hosting organizations. Three providers spread their records across sibling networks.

Hosting organization	Records	Networks	Main families
PEG TECH INC	1,144 (6 ASNs)	AS398823 (947), AS54600 (186), 4 others (11)	947 CyberStrikeAI on AS398823; 175 ARTEX on AS54600
Shenzhen Tencent	832 (2 ASNs)	AS45090 (800), AS132203 (32)	288 HypeAgent; 399 Daybreak
Datacamp Limited	283 (2 ASNs)	AS212238 (275), AS60068 (8)	277 Brute Ratel C4 (269 on AS212238, 8 on AS60068)

FIGURE 2 · TLS STACK & HOSTING MONOCULTURES — ODIN BY BRANDEFENSE · TLP:CLEAR

Dominant JARMs and Hosting Providers Concentrate Across Six Labeled Fleets

Share (%) of each upstream-labeled fleet accounted for by its #1 JARM hash vs. #1 hosting org, n = 3,018



Scope & source: Provider shares group sibling BGP ASNs (e.g., BRC4 Datacamp: AS212238 [269] + AS60068 [8]; PEG TECH: AS398823/AS54600).
What this does not show: *BRC4 Nginx-proxy JARM also appears on 90 AS40934 Caldera labs and 322 commercial proxy-node certificates (Ch. 3).

Figure 2: Dominant JARMs and hosting providers concentrate across six labeled fleets

Six families compared

Framework (records / IPs)	Top JARM share	Top hosting organization	Note
Brute Ratel C4 (539 / 283)	**93.9%** (506)	Datacamp Limited (277, 51.4%)	Datacamp, M247 (95) and Cogent (75) host 82.9% (447). The JARM is a generic proxy profile; see below
VShell (276 / 270)	**84.4%** (233)	SonderCloud Limited (220, 79.7%)	Go `crypto/tls` RSA listener on TCP 9999 for 219 of 276 endpoints (AS133199)
SuperShell (171 / 171)	**73.7%** (126)	LUOGELANG FRANCE (169, 98.8%)	170 of 171 suspected; almost all on AS135097, TCP 443
DarkSword (241 / 225)	**72.2%** (174)	CNServer LLC (186, 77.2%)	213 suspected, 28 confirmed; same JARM as SuperShell, on AS7488
ARTEX (501 / 500)	**47.3%** (237)	YANCY LIMITED (237, 47.3%)	Two turnkey blocks, YANCY AS138415 (237) and PEG TECH AS54600 (175), hold 82.2%
CyberStrikeAI (1,290 / 528)	**6.8%** (88)	PEG TECH INC (947, 73.4%)	Plain HTTP on the four-port layout dilutes the JARM share; 73.4% sit on PEG TECH AS398823

The full JARM values are below, for hunting.

Cluster (matching records)	JARM
Brute Ratel C4 (506 of 539)	`2ad2ad0002ad2ad00042d42d00000000f78d2dc0ce6e5bbc5b8149a4872356`
VShell (233 of 276)	`3fd21b20d00000021c43d21b21b43de0a012c76cf078b8d06f4620c2286f5e`
DarkSword and SuperShell	`21d14d00021d21d00042d43d00000091f9827a8676a9d9f27d421962a09b5d`
ARTEX, certificate name A (withheld) (237 of 501)	`29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787`
ARTEX, certificate name B (withheld) (173 of 501; 173 of its 175 records return a JARM)	`3fd3fd16d3fd3fd21c42d42d00000078e356c38fb85055d97a8bed930c8956`
CyberStrikeAI (88 of 1,290)	`3fd3fd0003fd3fd00042d42d0000002059a3b916699461c5923779b77cf06b`

The Brute Ratel C4 JARM is not unique

Within the 539 Brute Ratel C4 records, 322 (59.7%, on 162 IPs across 50 city names) carry certificates that name nodes of a commercial proxy service. The pattern is `<city>-rack<NNN>.nodes.<proxy domain>`, with the domain withheld. Most other named certificates follow `<city><NNN>` and expose both 443 and 8080 across Datacamp, M247 and Cogent.

The same `2ad2ad...a4872356` JARM also appears on 90 vendor-lab MITRE Caldera records across 85 hosts, 4 ARTEX records and 3 TacticalRMM records. A rule that keys on reverse-proxy behaviour can confuse a commercial VPN or proxy exit network with Brute Ratel redirectors. We treat this JARM as a generic proxy profile and hold these endpoints at review, with addresses withheld.

DarkSword and SuperShell share one stack

"DarkSword" is a family label that comes from an upstream threat feed. It covers 241 records, 88.4% of them suspected. Google Threat Intelligence Group (GTIG) has documented an iOS exploit kit of that name. We did not check these endpoints against GTIG's published indicators, so the label is not attribution.

One confirmed DarkSword panel on AS45102, port 443, presents a certificate name (withheld). Of the 241 DarkSword records, 174 (72.2%, all on CNServer AS7488) share JARM `21d14d...62a09b5d`. On SuperShell, 126 of 171 records (73.7%, all on LUOGELANG AS135097) share the identical JARM, for 300 records in total.

Most of these records are suspected (213 of 241 DarkSword, 170 of 171 SuperShell), and they split cleanly by provider. The shared JARM fits either a shared C2 bundle or a provider's standard OS and Nginx image.

04

CHAPTER 04

Certificate Camouflage

IN SHORT

A self-made TLS certificate can claim any name, and no authority checks it. Certificate names in the feed fall into three C2 patterns (portal lures and appliance defaults, framework defaults, and repeated campaign names) plus one collision group.

INSIDE THIS CHAPTER

Category A: appliance, VoIP and portal names 14

Category B: cloud ingress and framework defaults 15

Category C: repeated campaign names 16

04 Certificate Camouflage

Under RFC 5280, an operator who builds a custom certificate can write any Common Name (CN) or Organization into it. The feed records the subject CN and the JARM. It does not record certificate hashes, serial numbers or issuers. Repeated CN counts therefore show naming and template reuse, not shared private keys or verified self-signatures. Creating such certificates is MITRE ATT&CK T1587.003, Develop Capabilities: Digital Certificates.

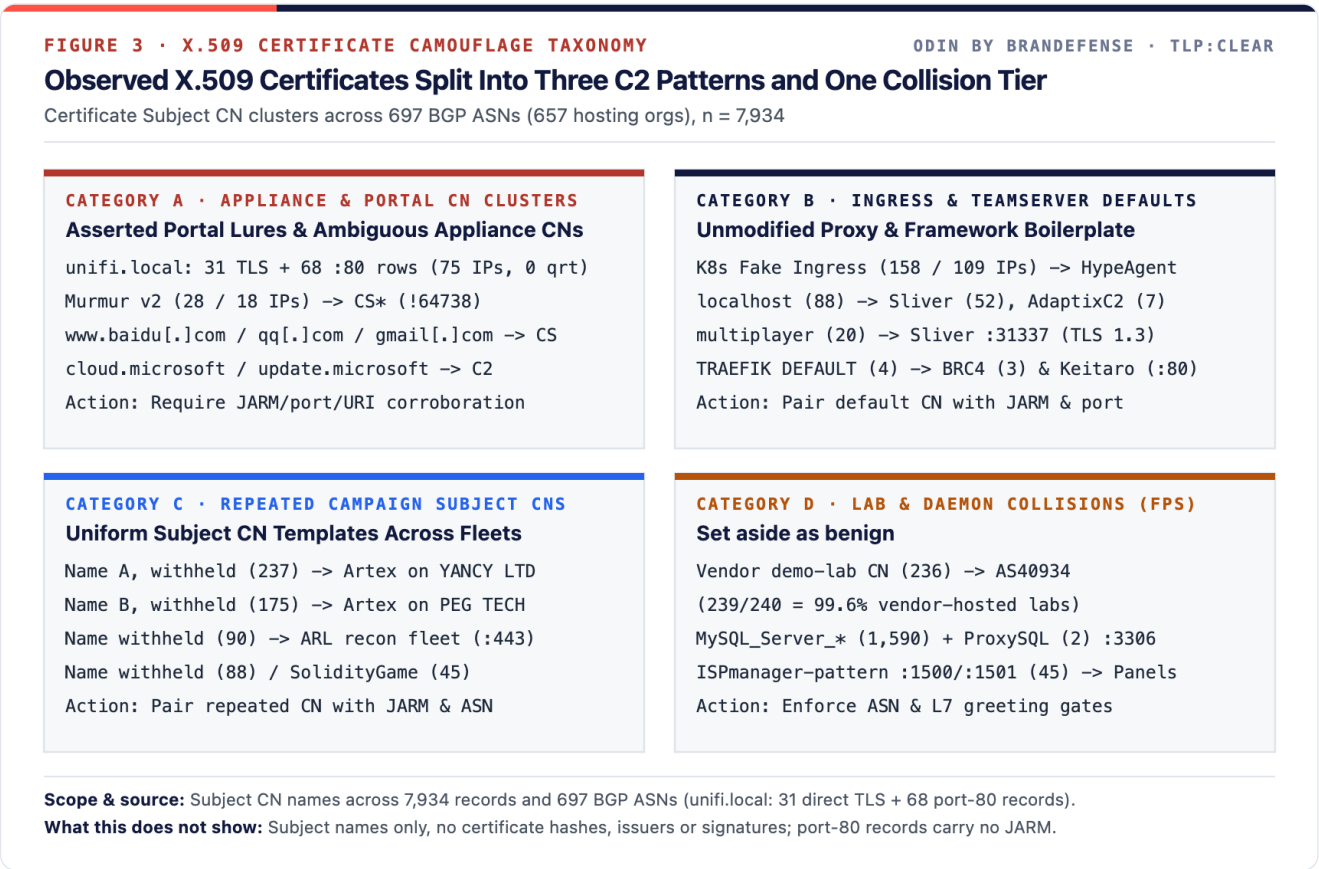


Figure 3: Observed X.509 certificates split into three C2 patterns and one collision tier

Category A: appliance, VoIP and portal names

The `unifi.local` cluster. 99 CyberStrikeAI-labeled records on 75 hosts carry `CN=unifi.local`, the default name of a Ubiquiti console. Of these, 92 (92.9%) sit on DigitalOcean (AS14061).

Part of the cluster	Records	Detail
Direct TLS	31	29 on TCP 443, 1 on 7443, 1 on 8443; generic Nginx or UniFi JARM `29d29d...6c007d93`
Port-80 records with no JARM	68	Across 23 dual-port droplets and 45 hosts without a matching TLS record
Non-DigitalOcean records	7	Including 5 consumer or telecom hosts; same JARM as genuine UniFi OS consoles

None of the 75 hosts expose CyberStrikeAI's four-port layout (5001 to 5003 and 8082). DigitalOcean droplets also host real UniFi controllers. `CN=unifi.local` is therefore an enrichment signal for review, and these addresses are withheld.

The Murmur cluster. 28 Cobalt Strike-labeled records on 18 hosts present `CN=Murmur Autogenerated Certificate v2`, the default of the Mumble voice server. That is 22.4% of the Cobalt Strike slice (125 endpoints on 87 hosts). The records use 19 non-default ports, led by 10010 (7), 10002 (3) and 10004 (2), and none uses the Mumble default 64738.

Fifteen of the 28 records sit in one OVH /24 network (AS16276), across consecutive ports 10001 to 10025, with 9 ports on one IP. The 28 records also show 5 different JARMs. This layout fits multi-tenant game-voice hosting. We hold Murmur certificates at review unless a separate C2 signal appears.

Portal names. Endpoints in four families present the names of major web and update portals, outside the brand owner's network.

Asserted CN	Family	Endpoints	Hosting
`www.baidu[.]com`	Cobalt Strike	5	Shenzhen Tencent, CNServer, Alibaba
`qq[.]com`	Cobalt Strike	4	Shenzhen Tencent
`gmail[.]com`	Cobalt Strike	1	Privex Inc. (AS210083)
`baidu[.]com`	HypeAgent	2	Shenzhen Tencent
`cloud.microsoft`	CyberStrikeAI	1	Cloudie Limited (AS906)
`update.microsoft[.]com`	AdaptixC2	1	Alibaba (AS37963), TCP 4321

Category B: cloud ingress and framework defaults

Fake Kubernetes ingress certificates.

Across 510 suspected HypeAgent endpoints (171 hosts), 288 (56.5%) sit on Shenzhen Tencent Cloud. A sub-cluster of 158 endpoints (109 hosts, 31.0% of HypeAgent) presents `CN=Kubernetes Ingress Controller Fake Certificate`. It sits mainly on Microsoft Azure (AS8075, 48 endpoints, 30.4%), DigitalOcean (19, 12.0%) and Alibaba (19, 12.0%). Smaller shares are on AWS (11), Hetzner (7), FPT Telecom (3) and ALEXHOST (2).

Every unconfigured Kubernetes `ingress-nginx` deployment shows this exact name. On 443 or 8443 it is not enough on its own; it needs a C2 port or co-hosting signal.

Teamserver and proxy defaults.

CN	Endpoints	Where it appears
`CN=localhost`	88 on 82 hosts	Sliver (52 of 100), PentAGI (8), AdaptixC2 (7), OpenVAS (5)
`CN=multiplayer`	20	All Sliver operator gRPC listeners on TCP 31337; all 16 that answer JARM negotiate TLS 1.3 only, as Sliver's mTLS default does
`CN=TRAEFIK DEFAULT CERT`	4	None on 8080 or 8443. Three Brute Ratel C4 records and 1 Keitaro record on DigitalOcean (AS14061) serve live TLS on TCP port 80

TLS on port 80 is a protocol mismatch worth hunting, because ordinary web servers speak plain HTTP there.

Category C: repeated campaign names

Industrial-scale deployments reuse fixed certificate names across whole provider blocks.

CN	Family	Endpoints	Hosting
certificate name A (withheld)	ARTEX	237	YANCY LIMITED (AS138415)
certificate name B (withheld)	ARTEX	175	PEG TECH INC (AS54600)
an ARL certificate name (withheld)	ARL recon	90	TCP 443
a CyberStrikeAI certificate name (withheld)	CyberStrikeAI	88	AROSSCLOUD INC. (AS400619)
`SolidityGameServer`	Keitaro TDS	45 on 20 hosts	Ports 8082, 8081 and 443

ARTEX has 501 endpoints on 500 hosts, and its two names cover 412 of them (82.2%). Confirming that these endpoints share a private key or a self-signature needs certificate thumbprints, which the feed does not carry.

05

CHAPTER 05

Benign Collisions That Inflate the Feed

IN SHORT

Raw feed volume is not adversary volume. Most port-3306 Daybreak records are MySQL servers, ports 1500 and 1501 match a hosting panel, and 99.6% of Caldera records sit in a security vendor's network.

INSIDE THIS CHAPTER

Daybreak and MySQL 18

Ports 1500 and 1501: a hosting panel 19

MITRE Caldera in a vendor lab 19

05 Benign Collisions That Inflate the Feed

Two large clusters needed testing before any defensive advice: 1,701 Daybreak records and 240 MITRE Caldera records.

Daybreak and MySQL

Daybreak ranks first by raw count with 1,701 records. Of these, 1,592 (93.6%) sit on TCP 3306. They carry 1,590 auto-generated `MySQL_Server_*` certificates and 2 `ProxySQL` certificates. MySQL 5.7.44 (365) and 8.0.45 (148) lead the versions.

Modern MySQL servers (5.7.5 and later, 8.0 and 8.4) can create their own CA and server certificate at startup when the `auto_generate_certs` conditions are met. Any feed that labels "self-signed TLS on an unusual port" will catch them.

To test this, we compared the feed labels on other ports of 59 Daybreak hosts, drawn from three groups. A host counts as a candidate secondary C2 when another port carries a C2 family label. Every such label in this set is candidate-level.

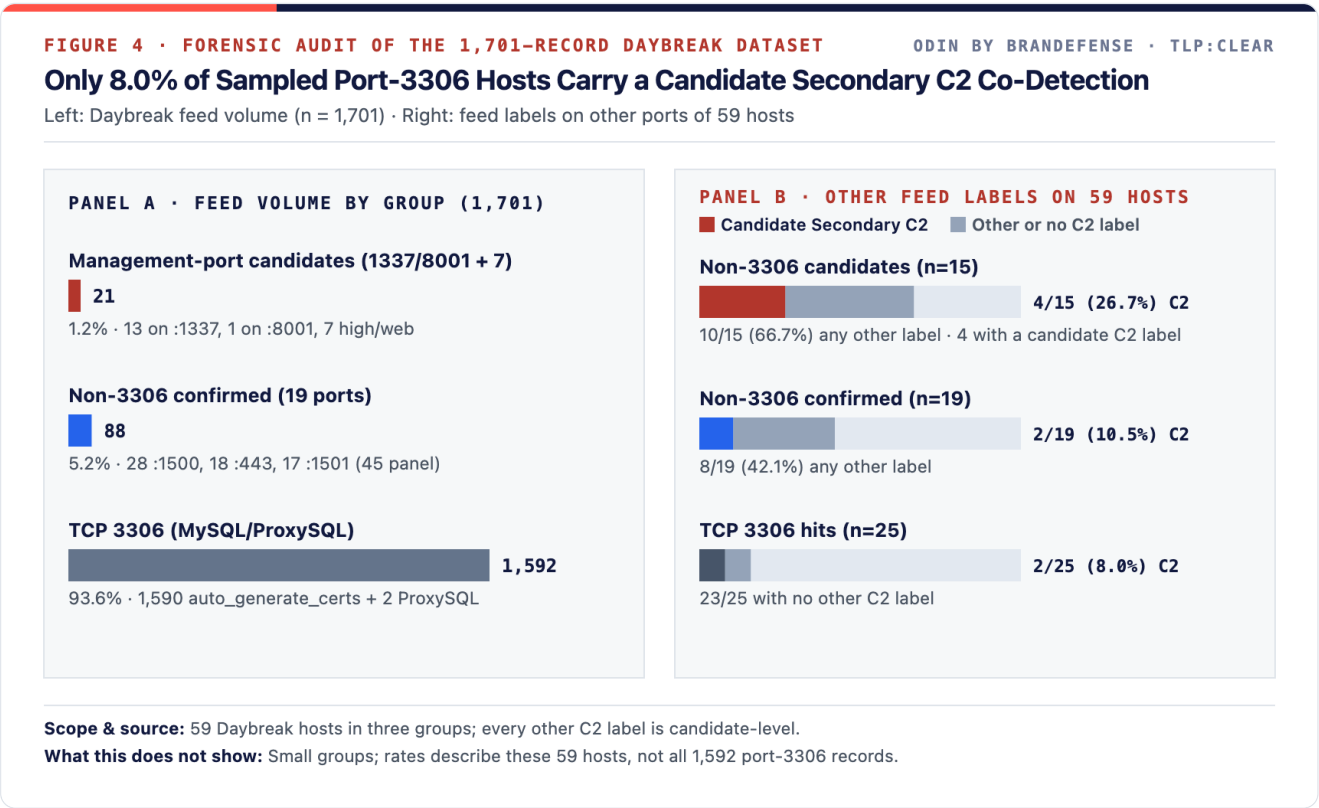


Figure 4: Only 8.0% of sampled port-3306 hosts carry a candidate secondary C2 co-detection

Daybreak group	Records (port split)	Hosts examined	Candidate secondary C2	Any other hit
Non-3306 candidates	21 (13 on 1337, 1 on 8001, 7 on other ports)	15	**4 of 15 (26.7%)**	10 of 15 (66.7%)
Non-3306 confirmed	88 (28 on 1500, 18 on 443, 17 on 1501, 25 on 16 other ports)	19	**2 of 19 (10.5%)**	8 of 19 (42.1%)
TCP 3306	1,592 (1,590 MySQL, 2 ProxySQL)	25	**2 of 25 (8.0%)**	4 of 25 (16.0%)

What sat next to Daybreak in each group:

- **Non-3306 candidates.** Four hosts carried candidate VShell (8084 and 8887), Sliver (8080), Metasploit (33970, SSH banner only) or ARTEX and JavaChains (8787 and 8011). Three carried ARL or AutoHunter recon hits. Three showed only Daybreak itself.
- **Non-3306 confirmed.** Two hosts on 443 carried candidate Ramnit or ARTEX labels. Four of the 8 raw hits were Daybreak's own labels on ports 1500 and 1501.
- **TCP 3306.** Two hosts carried candidate VShell or Sliver next to open MySQL, along with GoWebSSH or GoPhish. Two matched only Acunetix or Nessus scanners. The other 21 (84.0%, typically MySQL 8.4) showed no other detection.

Ports 1500 and 1501: a hosting panel

All 8 examined hosts on ports 1500 and 1501 returned `"Authorization"` on 1500, and 4 of 8 exposed `nginx` on 1501. This matches the ISPsystem ISPmanager shared-hosting control panel, which binds web listeners to those ports and redirects to `/ispmgr`. The feed holds 45 such records. ISPConfig and FASTPANEL also appear.

MITRE Caldera in a vendor lab

The 240 MITRE Caldera records sit on ports 443 (118), 80 (114), 16018 (5) and 8080 (3). Of these, 236 present one vendor demo-lab certificate name (withheld), and 3 present `192.168.100.4`. Routing data puts 239 of 240 (99.6%) inside one security vendor's network, AS40934, with one external DigitalOcean instance.

The pattern is consistent with a Fortinet demo lab, a benign collision. Exclude vendor-hosted demo labs like this from automatic WAN block lists, but keep internal callback monitoring.

CHAPTER 06

What Passive Monitoring Misses

IN SHORT

Internet-wide TLS data describes server configuration, not victim compromise. TLS 1.3 hides the certificate, JARM hides the backend behind a proxy, and many C2 families are also normal security tools.

06 What Passive Monitoring Misses

> **TLS 1.3 hides the certificate.**
>
> Under TLS 1.2, the `ServerHello` and `Certificate` messages travel in clear text. A passive Suricata deployment can read the certificate subject and issuer. Under TLS 1.3 (RFC 8446, NIST SP 800-52 Rev. 2), everything after `ServerHello` is encrypted, including the certificate.

Certificate rules therefore stay blind on TLS 1.3 flows. All 16 Sliver `multiplayer` listeners on 31337 that answer JARM return a TLS 1.3-only JARM (`00000000000000000043d43d...`), matching Sliver's default mutual TLS profile. The rule set covers this with a TLS 1.3 session rule on port 31337, paired with JA4S and endpoint process data.

> **JARM measures the TLS stack, not the program.**
>
> Reverse proxies such as Nginx, Caddy and Traefik hide the teamserver behind a generic profile. The `2ad2ad...` JARM shared by Brute Ratel C4 and 90 vendor-lab Caldera records on 85 hosts shows this. A feed that exports only the subject CN, without issuer or signature, also cannot confirm self-signing. A JARM match alone should never trigger an automatic firewall block.

Dual-use tools. TacticalRMM (392), GoPhish (133), Sliver (100), CyberStrikeAI (1,290), PentAGI (26) and 476 scanner, proxy and OAST endpoints serve authorized security teams and MSPs as well as attackers. The study covers network handshakes and service banners only, with no malware samples, so file-based YARA rules are out of scope. C2 behind a CDN ends TLS at the Cloudflare or CloudFront edge and needs endpoint data instead.

07

CHAPTER 07

What Defenders Should Do

IN SHORT

This chapter lists the actions defenders should take, in priority order.

07 What Defenders Should Do

Within 24 hours

- [ ] Configure SOAR so that no lone certificate name, JARM or ASN match triggers an automatic block. Require two independent non-ASN signals.
- [ ] Exclude the vendor demo-lab records (AS40934, 239 records) from automatic WAN block lists.
- [ ] Block direct workstation egress to implant ports (8888, 9999, 43211, 5001 to 5003, 8082), admin ports (1337, 4321, 8001, 31337) and 3306, unless there is a business need.

Within 72 hours

- [ ] Deploy the Suricata certificate rules for TLS 1.2, with the Mumble port 64738 excluded and consumer ISP ranges tuned out.
- [ ] Deploy the TLS 1.3 session rule for port 31337.
- [ ] Alert on non-MySQL certificates on inspectable TCP 3306 handshakes, and check `/ispmgr` banners on TCP 1500 and 1501.

Within 7 to 30 days

- [ ] Hunt endpoint network events for the full CyberStrikeAI four-port layout, TLS 1.3 callbacks to high ports, and port-3306 egress from processes that are not database clients.
- [ ] Add the JARM values in this report to external attack surface hunting, as leads for review.
- [ ] Inspect TLS on both 443 and 8080, since Brute Ratel C4 splits evenly across the two.

The table suggests an owner for each control. Record its status and the evidence that it works in production.

Control	Owner
Two-signal gate before SOAR blocking, vendor lab excluded	CTI and SOAR engineering
Non-MySQL certificate on 3306, ISPmanager check on 1500 and 1501	Network detection and SOC
Suricata TLS 1.2 rules and TLS 1.3 rule on 31337	Perimeter NDR team
Workstation egress block on C2 and database ports	Firewall operations
Endpoint hunting for four-port layouts, TLS 1.3 high-port callbacks and non-database 3306 egress	Threat hunting and EDR

08

CHAPTER 08

Detection Rules

IN SHORT

This chapter describes each published rule and where to deploy it.

INSIDE THIS CHAPTER

How the Suricata signatures work 25

How the KQL hunt works 25

How the Sigma rules work 26

How to sort an endpoint 26

08 Detection Rules

The full rules are in Appendix B. Each file targets a signal that holds up after a C2 operator changes the surface details.

Rule file	What it catches
`suricata_c2_tls_jarm_camouflage.rules`	Suricata 7: six server-to-client TLS signatures for camouflage certificates, TLS on port 80, non-MySQL certificates on 3306 and TLS 1.3 on 31337
`sentinel_wan_c2_certificate_and_port_hunt.kql`	Microsoft Sentinel and Defender XDR: workstation egress to C2 and database ports, with the CyberStrikeAI four-port layout and database-client checks
`sigma_c2_nonstandard_port_egress.yml`	Sigma (3 rules): outbound connections to public 3306, staging-folder binaries reaching C2 ports, and LOLBins reaching CyberStrikeAI or VShell ports

How the Suricata signatures work

All six signatures inspect the server's side of the handshake (`flow:established,to_client`). SIDs 9202601 to 9202603, 9202606 and 9202607 read the certificate subject, so they work only on cleartext TLS 1.2 or decrypted traffic. Matching a subject and issuer name does not prove a cryptographic self-signature.

SID	Looks for	Feed records it covers
9202601	`CN=unifi.local` in both subject and issuer, from an external IP	25 non-consumer direct-TLS records (of 31)
9202602	`CN=Murmur Autogenerated Certificate v2` on any port except 64738	28
9202603	`CN=multiplayer` on TCP 31337, not issued by Let's Encrypt	TLS 1.2 downgrade only; pair with 9202608
9202606	`CN=TRAEFIK DEFAULT CERT` served as live TLS on TCP 80	4
9202607	A TLS certificate on TCP 3306 that is not `MySQL_Server_` or `ProxySQL_`	Pair with KQL and Sigma for TLS 1.3
9202608	Any TLS 1.3 session from external TCP 31337	16 responsive Sliver records

These counts are upper bounds. The feed holds the subject CN and port but no issuer, so it cannot show which records would also match the issuer condition.

How the KQL hunt works

The Sentinel query looks back 14 days at successful connections to public addresses. It ignores private IPv4 ranges and IPv6 link-local and unique-local addresses. It watches TCP 1337, 4321, 5001 to 5003, 8001, 8082, 8888, 9999, 31337, 43211 and 3306.

Each hit gets a plain label. A device that reaches all four CyberStrikeAI ports (5001, 5002, 5003, 8082) on one IP is always kept, even at low volume. Port 9999 is labelled VShell, 8888 Sliver implant mTLS, 4321 and 43211 AdaptixC2, and 1337, 8001 and 31337 operator consoles. Except for the full four-port layout, a destination needs 3 or more connections before it is reported.

For port 3306, a known database client name alone is not trusted. The query checks the process hash, or a trusted signer such as Oracle, MariaDB, DBeaver, JetBrains, PremiumSoft or Datadog. A known name without that check is flagged as an unverified database client, and any other process as a non-database process reaching public 3306.

How the Sigma rules work

The three Sigma rules use Sysmon Event ID 3 network events and exclude RFC 1918, CGNAT and private IPv6 ranges.

Rule	Fires when	Note
1	Any process connects to public TCP 3306	Event ID 3 has no hash or signer, so correlate with Event ID 1 by `ProcessGuid`
2	A binary in a staging folder (`\AppData\Local\Temp\`, `\Users\Public\`, `\ProgramData\`, `\Windows\Temp\`, `\Downloads\`) reaches a high C2 port	Catches dropped implants
3	A Windows LOLBin reaches CyberStrikeAI ports (5001 to 5003, 8082) or VShell port 9999	Catches living-off-the-land callbacks

How to sort an endpoint

The triage logic never blocks on uncorroborated evidence. It treats self-signing as unknown until certificate evidence is checked.

What the endpoint shows	Action
Inside the vendor lab network AS40934	Benign vendor lab
A verified MySQL greeting or ISPmanager banner	Low signal
Dual-use labels (TacticalRMM, GoPhish, CyberStrikeAI, PentAGI)	No co-hosting credit without independent service checks

Test every rule in your own environment before production use.

09

CHAPTER 09

Indicators

IN SHORT

This chapter lists the published indicators and explains what stays withheld.

INSIDE THIS CHAPTER

VShell pattern 28

Other patterns 28

MITRE ATT&CK mapping 29

09 Indicators

No individual address is published for this study, so Appendix A is empty. The selected set has 32 records across 11 families. It contains no vendor-lab records, no 3306, 1500 or 1501 collisions, and no consumer-ISP or contested records.

Type	Count
Network-level patterns (VShell on port 9999)	3
Other network-level patterns	29
Full JARM values for hunting	6 (Chapter 3)
Default certificate names	See Chapters 4 and 8; campaign names are withheld

All 32 are published at network level. Their individual IP addresses are withheld, because their feed label is suspected or because self-signing or hostile use is not verified. Cloud and VPS addresses change hands quickly, so check the live handshake before any permanent block.

VShell pattern

Records	Framework	Network	Port	Certificate	JARM
3	VShell	AS133199 SonderCloud	9999	None	`3fd21b20d0000002...c2286f5e`

These three share TCP 9999 and the VShell Go TLS fingerprint.

Other patterns

Records	Framework	Network	Port	Certificate	JARM	Needs
2	Brute Ratel C4	AS14061 DigitalOcean	80	`TRAEFIK DEFAULT CERT`	`3fd3fd0000000000...ff7899fb`	Self-signature check
2	Brute Ratel C4	AS45671 Servers Australia (8080); AS212238 Datacamp (443)	8080, 443	`<city><NNN>` ; proxy-node name	`2ad2ad0002ad2ad0...a4872356`	Second signal (generic proxy JARM)
2	CyberStrikeAI	AS14061 DigitalOcean	443	`unifi.local`	`29d29d00029d29d0...6c007d93`	Second signal
1	CyberStrikeAI	AS400619 AROSSCLOUD	443	a CyberStrikeAI certificate name (withheld)	`3fd3fd0003fd3fd0...b77cf06b`	Self-signature check
2	CyberStrikeAI	AS398823 PEG TECH	5001, 5002	None	No TLS	Four-port check
4	ARTEX	AS138415 YANCY (2); AS54600 PEG TECH (2)	443	certificate name A (withheld); certificate name B (withheld)	`29d29d...c55d6787` ; `3fd3fd16...930c8956`	Self-signature check

Records	Framework	Network	Port	Certificate	JARM	Needs
3	HypeAgent	AS18403 FPT Telecom; AS200019 ALEXHOST; AS14061 DigitalOcean	443	`Kubernetes Ingress Controller Fake Certificate`	Several `29d29d...`	Second signal
2	Cobalt Strike	AS16276 OVH	10004, 10025	`Murmur Autogenerated Certificate v2`	`29d08d00029d0000...b2392e62`	Non-Mumble protocol
2	Cobalt Strike	AS45090 Shenzhen Tencent; AS7488 CNServer	443	`www.baidu[.]com`	`3fd3fd20...ddbaefa8`; `3fd3fd00...ff7899fb`	Second signal
2	Sliver	AS16509 Amazon; AS396982 Google	31337	`multiplayer`	TLS 1.3 only, or no JARM reply	Self-signature check (one record)
3	DarkSword	AS7488 CNServer (2); AS45102 Alibaba US (1)	443	None (2); a certificate name (withheld) (1)	`21d14d...62a09b5d`; `40d40d40d00040d0...9311926e`	Second signal; self-signature check for the panel
1	SuperShell	AS135097 LUOGELANG FRANCE	443	None	`21d14d00021d21d0...62a09b5d`	Second signal
1	AdaptixC2	AS57043 HOSTKEY	4321	None	No TLS	Hunt lead
2	Daybreak	AS139203 Guizhou GuiAn IDC; AS45090 Shenzhen Tencent	1337	None	No TLS	Candidate co-detection

Withheld: every individual IP in the set, the campaign certificate names (they may belong to third parties), the commercial proxy domain, the vendor demo-lab certificate name, subscriber certificate names, and all 180 consumer-ISP records.

MITRE ATT&CK mapping

Technique	How it shows up	Detection
T1571 Non-Standard Port	Four-port CyberStrikeAI layout, VShell on 9999, AdaptixC2 on 4321 and 43211, Sliver on 31337, TLS on 80	KQL hunt; Sigma rules 2 and 3; SIDs 9202606 and 9202608
T1587.003 Develop Capabilities: Digital Certificates	Portal-name certificates, appliance and framework defaults, repeated campaign names	SIDs 9202601 to 9202603 and 9202607

10

CHAPTER 10

Scope and Limits

IN SHORT

This chapter sets out what the evidence can show and what it cannot.

10 Scope and Limits

- **Dates.** Last-seen dates on the records run from 17 October to 15 November 2026, and most fall on 13 to 15 November. Some first-seen dates go back to 2024. Those are the earliest dates attached to records in source feeds, not the start of our observation. The research cutoff is 15 November 2026.
- **Feed labels are not verdicts.** Family names and confirmed, suspected and candidate labels come from upstream feeds. "DarkSword" in particular is a feed label, not a link to GTIG's reporting.
- **Configuration, not compromise.** The data describes how external servers are set up. It does not show any victim compromise.
- **Names, not keys.** The feed holds certificate subject names and JARMs, not certificate hashes, issuers or signatures. Repeated names show template reuse, not a shared private key.
- **Small samples.** The Daybreak rates come from 59 examined hosts in three groups. They describe those hosts, not the whole 1,592-record port-3306 set.
- **No growth claims.** Most records are single snapshots, so the data supports counts, not trends.
- **Network only.** No malware samples were analysed, so file-based detection is out of scope. C2 behind a CDN needs endpoint data.
- **Rule testing.** Each rule file loads without errors in its engine (Suricata 7.0.12, pySigma and Microsoft's Kusto.Language analyzer). The rules were not replayed against live traffic, so test them in your own environment before production use.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. Salesforce Engineering (Althouse, Smart, Nunnally and Brady). Easily Identify Malicious Servers on the Internet with JARM. https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a/ (verified 18 November 2026)
2. Google Threat Intelligence Group. The Proliferation of DarkSword: iOS Exploit Chain Adopted by Multiple Threat Actors. https://cloud.google.com/blog/topics/threat-intelligence/darksword-ios-exploit-chain (verified 18 November 2026)
3. MySQL 8.0 Reference Manual. Creating SSL and RSA Certificates and Keys using MySQL. https://dev.mysql.com/doc/refman/8.0/en/creating-ssl-rsa-files-using-mysql.html (verified 18 November 2026)
4. MITRE ATT&CK. T1587.003 Develop Capabilities: Digital Certificates. https://attack.mitre.org/techniques/T1587/003/ (verified 18 November 2026)
5. MITRE ATT&CK. T1571 Non-Standard Port. https://attack.mitre.org/techniques/T1571/ (verified 18 November 2026)
6. NIST Special Publication 800-52 Rev. 2. Guidelines for the Selection, Configuration, and Use of TLS Implementations. https://csrc.nist.gov/pubs/sp/800/52/r2/final (verified 18 November 2026)
7. IETF RFC 5280. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. https://datatracker.ietf.org/doc/html/rfc5280 (verified 18 November 2026)
8. IETF RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. https://datatracker.ietf.org/doc/html/rfc8446 (verified 18 November 2026)

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

No individual indicators are published for this study; Appendix A explains why. Appendix B carries every published detection rule in full.

INSIDE

A. Indicators of compromise (0) 35

B. Detection rules (3 files) 36

A Indicators of Compromise

No individual addresses or file hashes are published for this study. The hosts in this report are exposed or unattributed systems rather than confirmed adversary infrastructure, so they stay anonymous. Use the detection rules in Appendix B.

B Detection Rules

Each rule file loads in its own engine (Kusto, pySigma, Suricata 7). Tune thresholds and allow-lists to your environment before alerting or blocking. The same files can be downloaded from the online edition.

sentinel_wan_c2_certificate_and_port_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense: Report #02 Detection Engineering Suite
// Target: Microsoft Sentinel / Defender XDR (DeviceNetworkEvents)
// Notes:
//   1. DeviceNetworkEvents.RemoteUrl records outbound client SNI / HTTP Host headers, NOT remote server X.509
Subject CNs.
//   2. TCP 31337/1337/8001 hunt rogue operator consoles or jumpboxes; TCP 8888/9999/43211/5001-5003/8082 hunt
implants/agents.
//   3. Retain filename-matched AllowedDatabaseClients on port 3306 until verified via
ApprovedDatabaseClientHashes or DeviceFileCertificateInfo signer data (using InitiatingProcessSHA1 fallback when
InitiatingProcessSHA256 is unpopulated).

let Lookback = 14d;
let QuartetPorts = dynamic([5001, 5002, 5003, 8082]);
let SuspiciousC2Ports = dynamic([1337, 4321, 5001, 5002, 5003, 8001, 8082, 8888, 9999, 31337, 43211]);
let AllowedDatabaseClients = dynamic([
    "mysqld.exe", "mysql.exe", "mysqldump.exe", "workbench.exe", "MySQLWorkbench.exe",
    "dbeaver.exe", "datagrip64.exe", "navicat.exe", "datadog-agent.exe",
    "mysqld", "mysql", "mysqldump", "dbeaver", "datagrip"
]);
let ApprovedDatabaseClientHashes = dynamic([]);
let ApprovedDatabaseSigners = dynamic(["Oracle America", "MariaDB", "DBeaver", "JetBrains", "PremiumSoft",
"Datadog"]);
let SignedBinaries = DeviceFileCertificateInfo
| where Timestamp > ago(Lookback) and IsTrusted == true
| summarize Signer = any(Signer), IsTrustedSigner = true by DeviceId, SHA1;
let BaseEvents = DeviceNetworkEvents
| where Timestamp > ago(Lookback) and ActionType == "ConnectionSuccess" and RemoteIPType == "Public"
| where coalesce(ipv4_is_private(RemoteIP), false) == false
    and not(RemoteIP startswith "fe80:" or RemoteIP startswith "fc" or RemoteIP startswith "fd" or RemoteIP ==
"::1")
| where RemotePort in (SuspiciousC2Ports) or RemotePort == 3306
| extend ProcessHash = iff(isnotempty(InitiatingProcessSHA256), InitiatingProcessSHA256, InitiatingProcessSHA1)
| join kind=leftouter SignedBinaries on DeviceId, $left.InitiatingProcessSHA1 == $right.SHA1
| extend IsFilenameMatchedDBClient = InitiatingProcessFileName in~ (AllowedDatabaseClients)
| extend IsVerifiedDBClientIdentity = IsFilenameMatchedDBClient and (
    (isnotempty(ProcessHash) and ProcessHash in~ (ApprovedDatabaseClientHashes))
    or (coalesce(IsTrustedSigner, false) and Signer has_any (ApprovedDatabaseSigners))
)
| where RemotePort in (SuspiciousC2Ports) or (RemotePort == 3306 and not(IsVerifiedDBClientIdentity));
let QuartetByTarget = BaseEvents
| where RemotePort in (QuartetPorts)
| summarize DistinctQuartetPorts = dcount(RemotePort) by DeviceName, RemoteIP;
BaseEvents
| join kind=leftouter QuartetByTarget on DeviceName, RemoteIP
| extend PortAnomalyType = case(
    RemotePort == 3306 and IsFilenameMatchedDBClient, "UnverifiedDBClientNameToPublic3306",
    RemotePort == 3306, "NonDBProcessToPublic3306",
    RemotePort in (QuartetPorts) and DistinctQuartetPorts == 4, "CyberStrikeAI_FullQuartet_4Ports",
    RemotePort in (QuartetPorts), "CyberStrikeAI_QuartetCandidatePort",
    RemotePort == 9999, "VShell_DefaultPort9999",
    RemotePort == 8888, "Sliver_DefaultImplant_mTLSPort",
    RemotePort in (4321, 43211), "AdaptixC2_ListenerOrAdminPort",
    RemotePort in (1337, 8001, 31337), "OperatorConsole_Or_AdminPort",
    "Other"
)
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), ConnectionCount = count(),
            DistinctHosts = dcount(DeviceName), SampleProcesses = make_set(InitiatingProcessFileName, 5),
```

```
            Signers = make_set_if(Signer, isnotempty(Signer), 5),
            ObservedClientSniOrHost = make_set_if(RemoteUrl, isnotempty(RemoteUrl), 5)
        by RemoteIP, RemotePort, PortAnomalyType, InitiatingProcessFolderPath, ProcessHash
| where ConnectionCount >= 3 or PortAnomalyType == "CyberStrikeAI_FullQuartet_4Ports"
| order by DistinctHosts desc, ConnectionCount desc
```

sigma_c2_nonstandard_port_egress.yml

SIGMA

```
title: Outbound Endpoint Egress to External Public TCP 3306 (Require Hash or Signer Correlation)
id: 6a19c4d2-11b8-4f29-9c01-8e4f7a210201
status: experimental
description: >
  Detects processes initiating outbound connections to public WAN IPv4/IPv6 addresses over TCP port 3306.
  Because Sysmon Event ID 3 (network_connection) does not record file hashes or code-signing certificates,
  this rule intentionally omits filename-only exclusions (which renamed binaries can bypass) and requires
  downstream ProcessGuid correlation against Sysmon Event ID 1 Hashes/Signature or Defender
  DeviceFileCertificateInfo to suppress hash- or signer-verified database clients.
author: Odin by Brandefense
date: 2026-11-16
logsource:
  category: network_connection
  product: windows
detection:
  selection:
    Initiated: 'true'
    DestinationPort: 3306
  filter_private:
    DestinationIp|cidr:
      - '10.0.0.0/8'
      - '172.16.0.0/12'
      - '192.168.0.0/16'
      - '127.0.0.0/8'
      - '169.254.0.0/16'
      - '100.64.0.0/10'
      - '::1/128'
      - 'fe80::/10'
      - 'fc00::/7'
  condition: selection and not filter_private
falsepositives:
  - Approved database clients (mysql.exe, MySQLWorkbench.exe, dbeaver.exe, datagrip64.exe) and application
servers verified via Sysmon Event ID 1 ProcessGuid hash/signature correlation or DeviceFileCertificateInfo
level: high
tags:
  - attack.command_and_control
  - attack.t1571
---
title: Staging or Transient-Directory Binary Connecting to High-Port C2 Implant or Operator Listeners
id: 7b28d5e3-22c9-4a38-8d12-9f5a8b320202
status: experimental
description: >
  Detects processes executing from transient or public staging directories initiating outbound
  connections to public endpoints on Sliver implant mTLS (8888), AdaptixC2 listeners (4321, 43211),
  or operator/jumpbox administration ports (31337 Sliver multiplayer, 1337 and 8001 Daybreak).
author: Odin by Brandefense
date: 2026-11-16
logsource:
  category: network_connection
  product: windows
detection:
  selection_port:
    Initiated: 'true'
    DestinationPort:
      - 1337
      - 4321
      - 8001
      - 8888
      - 31337
      - 43211
```

```
    selection_staging_dir:
      Image|contains:
        - '\AppData\Local\Temp\'
        - '\Users\Public\'
        - '\ProgramData\'
        - '\Windows\Temp\'
        - '\PerfLogs\'
        - '\Downloads\'
    filter_private:
      DestinationIp|cidr:
        - '10.0.0.0/8'
        - '172.16.0.0/12'
        - '192.168.0.0/16'
        - '127.0.0.0/8'
        - '169.254.0.0/16'
        - '100.64.0.0/10'
        - '::1/128'
        - 'fe80::/10'
        - 'fc00::/7'
    condition: selection_port and selection_staging_dir and not filter_private
  falsepositives:
    - Authorized red-team operator binaries, developer builds or browsers run from Downloads or ProgramData; tune
  in the SIEM
  level: high
  tags:
    - attack.command_and_control
    - attack.t1571
  ---
  title: Windows LOLBin Egress Matching CyberStrikeAI Quartet or VShell Listener Ports
  id: 8c37e6f4-33da-4b47-9e23-a06b9c430203
  status: experimental
  description: >
    Detects Windows living-off-the-land binaries (LOLBins) and scripting interpreters initiating outbound
    connections to public servers listening on CyberStrikeAI orchestration ports (5001, 5002, 5003, 8082)
    or VShell default TLS port (9999).
  author: Odin by Brandefense
  date: 2026-11-16
  logsource:
    category: network_connection
    product: windows
  detection:
    selection_port:
      Initiated: 'true'
      DestinationPort:
        - 5001
        - 5002
        - 5003
        - 8082
        - 9999
    selection_lolbin:
      Image|endswith:
        - '\powershell.exe'
        - '\pwsh.exe'
        - '\cmd.exe'
        - '\rundll32.exe'
        - '\regsvr32.exe'
        - '\mshta.exe'
        - '\certutil.exe'
        - '\curl.exe'
        - '\bitsadmin.exe'
        - '\wscript.exe'
        - '\cscript.exe'
    filter_private:
      DestinationIp|cidr:
        - '10.0.0.0/8'
        - '172.16.0.0/12'
        - '192.168.0.0/16'
        - '127.0.0.0/8'
        - '169.254.0.0/16'
        - '100.64.0.0/10'
        - '::1/128'
        - 'fe80::/10'
```

```
      - 'fc00::/7'
  condition: selection_port and selection_lolbin and not filter_private
falsepositives:
  - Administrative PowerShell or curl scripts managing external Synology DSM appliances on TCP 5001
level: high
tags:
  - attack.command_and_control
  - attack.t1571
```

suricata_c2_tls_jarm_camouflage.rules

SURICATA

```
# Odin by Brandefense: Report #02 Suricata 7.x TLS Masquerade & Port-Protocol Mismatch Suite
# Classification: TLP:CLEAR
# Operational Scope, Subject-CN/Issuer-CN Matching & TLS 1.3 Visibility Boundary:
#   1. Under TLS 1.3 (RFC 8446), the server Certificate message after ServerHello / EncryptedExtensions is
encrypted;
#      passive NDR sensors populate tls.cert_subject / tls.cert_issuer only on inspectable TLS handshakes
(cleartext
#      TLS 1.2 or SSL-decrypted streams where mTLS is absent). Accordingly, sid:9202601-9202603, 9202606 and
9202607 apply strictly to
#      inspectable TLS handshakes (uninspected TLS 1.3 on TCP 3306 requires endpoint KQL/Sigma process-egress
rules).
#      Because 16/16 responsive Sliver :31337 corpus listeners negotiate TLS 1.3 only (consistent with Sliver's
mTLS
#      default), sid:9202608 hunts uninspected TLS 1.3 ServerHello sessions on TCP 31337.
#   2. Matching the same CN=<value> substring in tls.cert_subject and tls.cert_issuer checks Subject-CN and
#      Issuer-CN substring alignment; under RFC 5280, full self-issuance requires full Distinguished Name
equality
#      (Subject DN == Issuer DN), and self-signing additionally requires cryptographic signature verification.
Because
#      the corpus CSV stores Subject CN without Issuer strings, corpus matches represent upper-bound Subject CN +
port coverage.
#   3. Tune $HOME_NET to include all internal LAN ranges; treat sid:9202601 and sid:9202602 as enrichment alerts
#      requiring endpoint/URI or non-VoIP protocol corroboration (suppress consumer ISP ASNs on sid:9202601).

# 1. Matching Subject-CN and Issuer-CN Ubiquiti unifi.local certificate served from external WAN IP (suppress
consumer ISP ASNs; verify URI/agent behavior)
alert tls !$HOME_NET any -> $HOME_NET any (msg:"ODIN-C2 Matching Subject/Issuer CN Ubiquiti unifi.local
Certificate on WAN (Console or Masquerade)"; flow:established,to_client; tls.cert_subject;
content:"CN=unifi.local"; fast_pattern; tls.cert_issuer; content:"CN=unifi.local"; classtype:command-and-control;
sid:9202601; rev:5;)

# 2. Murmur Autogenerated Certificate v2 on non-default port (!64738; verify non-Mumble protocol / JARM before
blocking)
alert tls !$HOME_NET !64738 -> $HOME_NET any (msg:"ODIN-C2 Murmur Autogenerated Certificate v2 on Non-Default
Port (!64738 - Verify Non-Mumble)"; flow:established,to_client; tls.cert_subject; content:"CN=Murmur
Autogenerated Certificate v2"; fast_pattern; tls.cert_issuer; content:"CN=Murmur Autogenerated Certificate v2";
classtype:command-and-control; sid:9202602; rev:4;)

# 3. Sliver C2 multiplayer certificate on TCP 31337 (fires only on legacy TLS 1.2 downgrade; pair with sid:
9202608 for TLS 1.3 mTLS)
alert tls !$HOME_NET 31337 -> $HOME_NET any (msg:"ODIN-C2 Sliver Multiplayer Operator Certificate on TCP 31337
(TLS 1.2 Downgrade Only)"; flow:established,to_client; tls.cert_subject; content:"CN=multiplayer"; fast_pattern;
tls.cert_issuer; content:!"Let's Encrypt"; classtype:command-and-control; sid:9202603; rev:4;)


# 4. Brute Ratel C4 / TDS matching Subject-CN and Issuer-CN Traefik default certificate bound directly as live
TLS on TCP 80 (TLS-on-80 protocol mismatch)
alert tls !$HOME_NET 80 -> $HOME_NET any (msg:"ODIN-C2 Matching Subject/Issuer CN Traefik Default Certificate
Bound Directly to TCP 80 (TLS-on-80 Anomaly)"; flow:established,to_client; tls.cert_subject; content:"CN=TRAEFIK
DEFAULT CERT"; fast_pattern; tls.cert_issuer; content:"CN=TRAEFIK DEFAULT CERT"; classtype:command-and-control;
sid:9202606; rev:5;)

# 5. Non-MySQL TLS certificate on external TCP 3306 (inspectable TLS 1.2 / decrypted handshakes only; pair with
KQL/Sigma for TLS 1.3)
alert tls !$HOME_NET 3306 -> $HOME_NET any (msg:"ODIN-C2 Non-MySQL Certificate on TCP 3306 (Inspectable TLS 1.2
or Decrypted Handshake)"; flow:established,to_client; tls.cert_subject; content:!"MySQL_Server_";
content:!"ProxySQL_"; classtype:command-and-control; sid:9202607; rev:6;)
```

```
# 6. Passive TLS 1.3 visibility companion: external TCP 31337 ServerHello negotiating TLS 1.3 (covers Sliver mTLS
operator consoles)
alert tls !$HOME_NET 31337 -> $HOME_NET any (msg:"ODIN-C2 External TLS 1.3 Session Over TCP 31337 (Sliver
Operator mTLS Candidate)"; flow:established,to_client; tls.version:1.3; classtype:command-and-control; sid:
9202608; rev:3;)
```

About Odin Research

Odin Research is the public research series of Odin by Brandefense. It documents adversary infrastructure seen on the internet and turns each finding into indicators and detection rules that defenders can use. Victims and third parties stay anonymous, addresses appear only for confirmed adversary infrastructure, and no working attack code is published.

Odin is the agentic analyst inside the Brandefense threat intelligence platform, which unifies Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management.

Online edition, indicators and rules · brandefense.io/odin-research/reports/port-and-certificate-camouflage/
Short Read · brandefense.io/odin-research/blog/c2-servers-hide-in-plain-ports-and-threat-feeds-flag/
Defense Kit · brandefense.io/odin-research/defense-kit/