ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 28 / 30 · C2 INFRASTRUCTURE

Templated C2 at Scale

ARTEX and DarkSword Clusters on Regional Hosting

How 2,674 ARTEX and DarkSword endpoints reuse certificates, port pairs and a few lease providers

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

2,674
Endpoints with an ARTEX or DarkSword label, on 2,468 distinct IPv4 hosts

526
Confirmed C2 endpoints on 516 hosts (19.7%), ready to block

2,312
ARTEX endpoints on 2,157 hosts; 1,272 of them on port 8787

362
DarkSword endpoints on 313 hosts; 189 (52.2%) on CNServer LLC

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

How 2,674 ARTEX and DarkSword endpoints reuse certificates, port pairs and a few lease providers

01	Executive Summary	04
02	Two Families, Four Clusters	07
03	ARTEX: Two Certificate Clusters and a Port 8787 Fleet	10
04	DarkSword: CNServer and High-Port Hubs	14
05	Multi-Port Hosts and Shared TLS Stacks	17
06	What Not to Block	20
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 (20)	35
B	Detection rules (4 files)	36

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 2,674 endpoints on 2,468 hosts that carry the ARTEX or DarkSword family labels. Of these, 526 endpoints on 516 hosts are confirmed command-and-control (C2) servers. ARTEX controllers reuse one certificate per hosting provider. DarkSword gathers on CNServer LLC. Nothing confirmed links the two families. Block the confirmed endpoints in Appendix A and hunt non-browser traffic to ports 8787, 8790, 8888 and 2000.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 2,674 endpoints on 2,468 hosts that carry the ARTEX or DarkSword family labels. Of these, 526 endpoints on 516 hosts are confirmed command-and-control (C2) servers. ARTEX controllers reuse one certificate per hosting provider. DarkSword gathers on CNServer LLC. Nothing confirmed links the two families. Block the confirmed endpoints in Appendix A and hunt non-browser traffic to ports 8787, 8790, 8888 and 2000.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 04

01 Executive Summary

ARTEX and DarkSword are two high-volume C2 family labels. Both sit on cheap virtual private servers (VPS) leased in bulk from a few regional resellers. This report maps where they sit, what they reuse, and what is safe to block.

1. **Two providers host 82.7% of confirmed ARTEX controllers.**
   YANCY LIMITED holds 237 confirmed ARTEX controllers and PEG TECH INC holds 175. Every controller in each group presents the same TLS certificate and almost always the same JARM fingerprint. Around them sit 1,272 unconfirmed listeners on port 8787 and 108 on port 8790.

2. **DarkSword puts over half its endpoints on one provider.**
   CNServer LLC hosts 189 of the 362 DarkSword endpoints (52.2%). Of these, 186 are suspected listeners on port 443, and 174 share one JARM value. The 28 confirmed DarkSword endpoints sit elsewhere, on 19 hosts that often pair ports 80, 443, 8443, 8888 and 2000.

3. **Most endpoints should be watched, not blocked.**
   Only 526 of the 2,674 endpoints (19.7%) are confirmed. The rest include shared Cloudflare and Traefik certificates, open directories, dynamic telecom addresses and uncorroborated listeners. Blocking them outright would hit shared infrastructure and unrelated tenants.

Three Decisions for Leaders

1. **Block confirmed controllers and review the list every 30 days.** Start with Appendix A. Leased VPS addresses change hands after an operator rotates, so a block that never expires will age badly.
2. **Hunt non-browser egress to the cluster ports.** Ports 8787, 8790, 8888 and 2000 carry most of the fleet. Alert when a script, shell or service process talks to them across these hosting networks.
3. **Ask for a second signal before blocking shared infrastructure.** Shared CDN certificates, mail ports and telecom subscriber ranges belong on short watchlists until a URI, certificate or process match backs them up.

The Study in Numbers

Number	What it is
2,674	Endpoints with an ARTEX or DarkSword label, on 2,468 distinct IPv4 hosts
526	Confirmed C2 endpoints on 516 hosts (19.7%), ready to block
2,312	ARTEX endpoints on 2,157 hosts; 1,272 of them on port 8787
362	DarkSword endpoints on 313 hosts; 189 (52.2%) on CNServer LLC
82.7%	Share of the 498 confirmed ARTEX controllers on YANCY LIMITED and PEG TECH INC (412)
186	Hosts that expose two to four of these listeners at once
2	Hosts that carry both families; both are unconfirmed candidates

How to use this report.

Security leaders can read Chapter 1 and Chapter 7. SOC and detection engineers should start with Chapters 7 to 9. CTI analysts will find the cluster, port and TLS detail in Chapters 2 to 6.

02

CHAPTER 02

Two Families, Four Clusters

IN SHORT

The 2,674 endpoints fall into four clusters by family, port and hosting provider. The clusters are an analytical model: shared certificates link hosts inside a cluster, but almost nothing links one cluster to another.

INSIDE THIS CHAPTER

What the labels mean 07

Counts by family 07

The four clusters 08

Where the endpoints sit 08

ATT&CK mapping 08

02 Two Families, Four Clusters

What the labels mean

ARTEX is the family label for ARTEX, the autonomous red-team console described in Monographs 04 and 11. Its default console port is 8787, and it also listens on 443, 80 and 7878. The confirmed YANCY LIMITED and PEG TECH INC controllers in this report are the same certificate clusters counted in those monographs (237 and 175).

"DarkSword" is a family label that comes from an upstream threat feed. We did not tie it to any published vendor report, so the label is not attribution. We use it only to group the endpoints the feed tags that way.

Each endpoint below is an IP, port and family combination.

Counts by family

Family	Endpoints	Hosts	Endpoints per host	Confirmed	Suspected	Candidate	Other watchlist
ARTEX	2,312	2,157	1.07	498 (497 hosts)	14	1,787	12 open directory, 1 dynamic ISP
DarkSword	362	313	1.16	28 (19 hosts)	212	121	1 dynamic ISP
Total	**2,674**	**2,468**	**1.08**	**526 (516 hosts)**	**226**	**1,908**	**14**

ARTEX makes up 86.5% of the endpoints. The per-family host counts add up to 2,470, two more than the 2,468 distinct hosts. Those two hosts carry listeners of both families (Chapter 5).

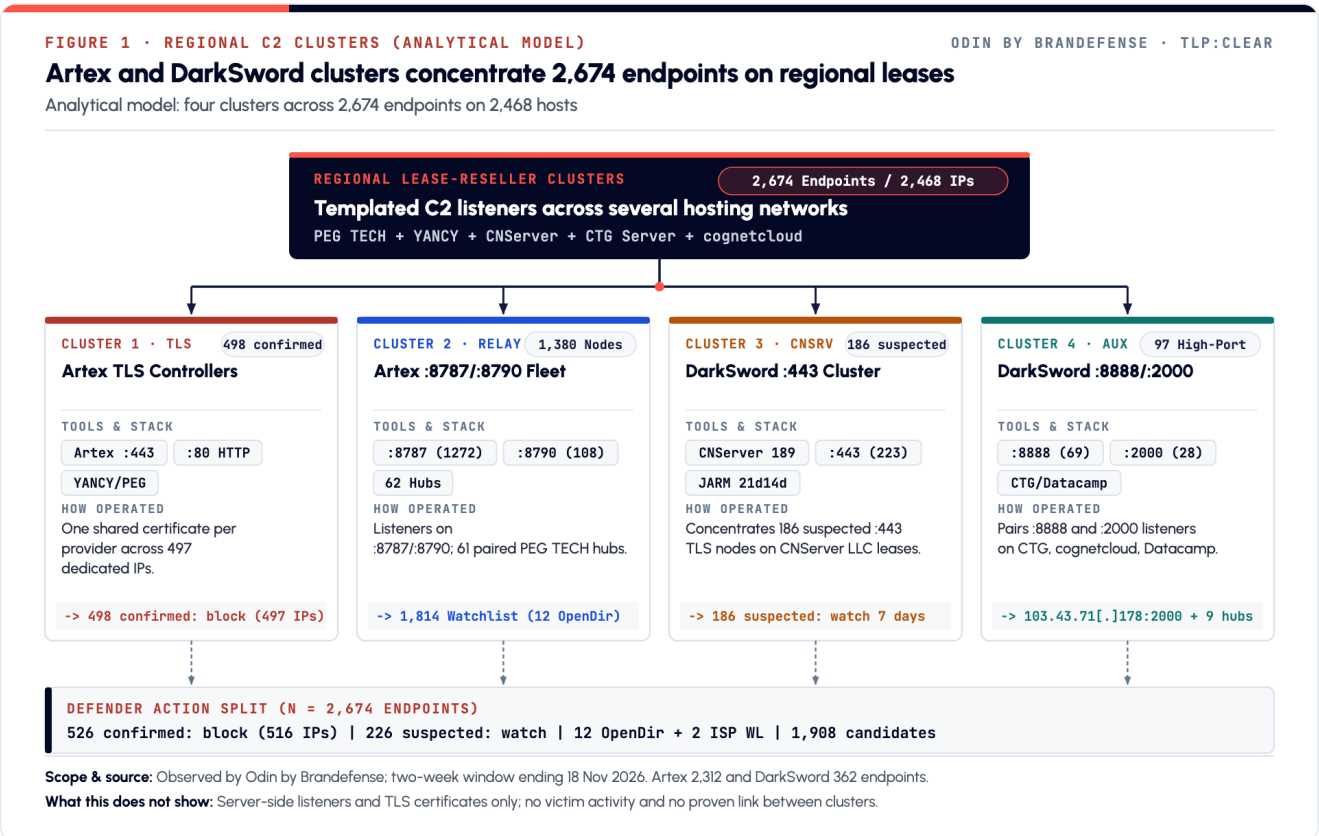


Figure 1: Artex and DarkSword clusters concentrate 2,674 endpoints on regional leases

The four clusters

Cluster	What defines it	Size	Confirmed
1. ARTEX TLS controllers	Confirmed controllers, mostly on ports 443 and 80; 412 sit on YANCY LIMITED and PEG TECH INC behind one shared certificate per provider	498 confirmed endpoints on 497 hosts	498
2. ARTEX port 8787 and 8790 fleet	Listeners on the ARTEX default port and its companion port	1,380 endpoints (1,272 on 8787, 108 on 8790)	None
3. DarkSword CNServer cluster	Port 443 listeners on CNServer LLC sharing one JARM value	189 endpoints	None (186 suspected)
4. DarkSword high-port hubs	Listeners on 8888 and 2000, often paired, on CTG Server, cognetcloud and Datacamp	97 endpoints (69 on 8888, 28 on 2000)	Includes 103.43.71[.]178:2000

Inside clusters 1 and 3, one certificate or one JARM value repeats across hundreds of servers. Between clusters, the only shared element is the hosting provider. Two candidate hosts carry both families, and nothing else links ARTEX to DarkSword.

Where the endpoints sit

Country	Endpoints	Share
United States	1,283	48.0%
Hong Kong	698	26.1%
China	301	11.3%
Singapore	89	3.3%
Japan	87	3.3%

The Netherlands (34), Germany (31), South Korea (21) and Malaysia (19) follow.

US and Hong Kong locations may reflect where resellers announce their address space rather than where the operators sit. PEG TECH INC, YANCY LIMITED, CNServer LLC, CTG Server Limited and cognetcloud INC all sell VPS capacity in both places.

ATT&CK mapping

Technique	ID	Where it shows
Acquire Infrastructure: Virtual Private Server	T1583.003	Bulk VPS leases on a few regional resellers
Non-Standard Port	T1571	Listeners on 8787, 8790, 8888, 2000, 7676 and 18787
Application Layer Protocol: Web Protocols	T1071.001	HTTP and HTTPS controllers on 80, 443 and 8443

CHAPTER 03

ARTEX: Two Certificate Clusters and a Port 8787 Fleet

IN SHORT

Confirmed ARTEX controllers listen mostly on port 443 (421) and port 80 (63). The unconfirmed majority sits on port 8787 (1,272) and port 8790 (108), often on the same providers and behind the same certificates.

INSIDE THIS CHAPTER

Ports 10

One certificate per provider 11

Provider footprint 11

The port 8787 and 8790 fleet 11

Confirmed controllers off the two big providers 12

How these counts relate to Monographs 04 and 11 12

03 ARTEX: Two Certificate Clusters and a Port 8787 Fleet

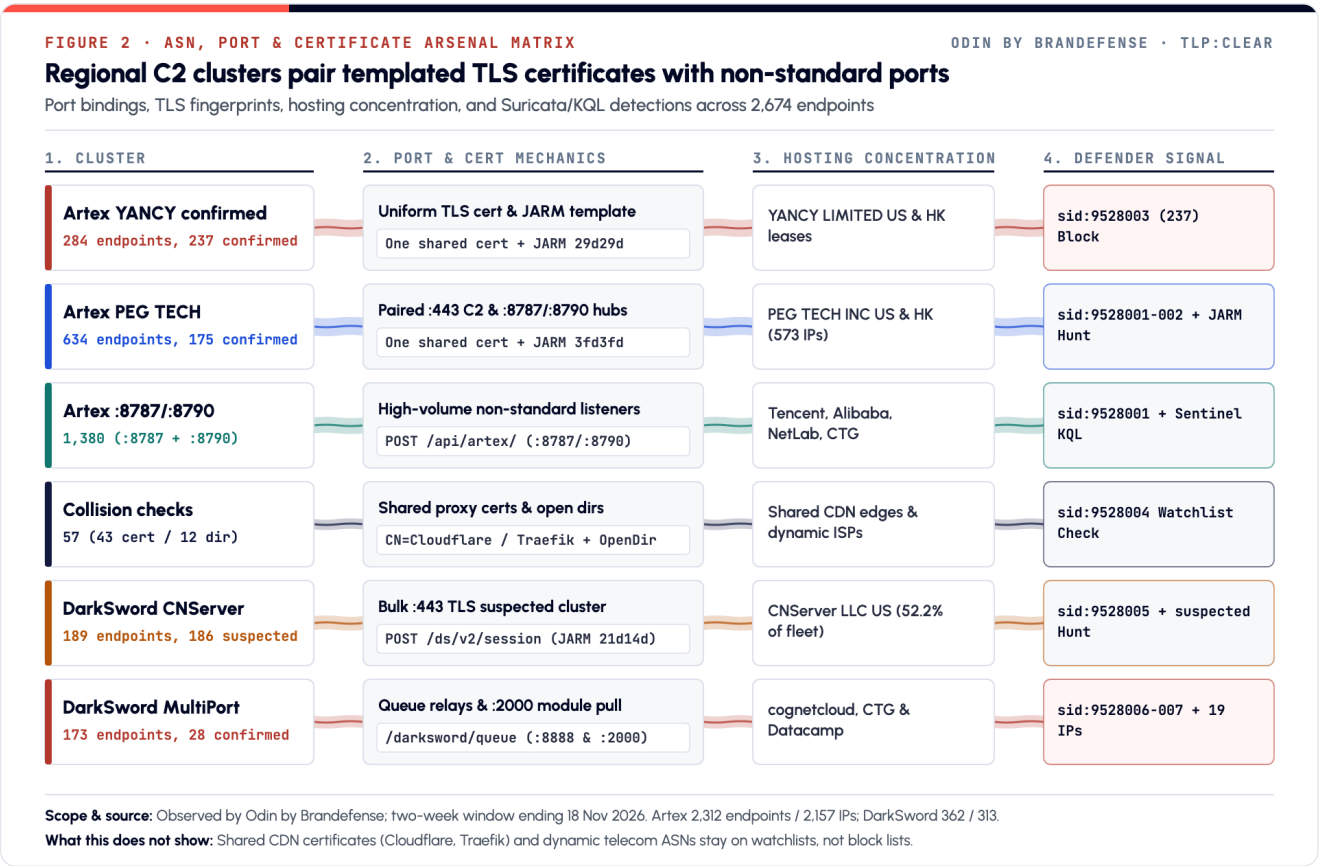


Figure 2: Regional C2 clusters pair templated TLS certificates with non-standard ports

Ports

Port	ARTEX endpoints	Note
8787	1,272 (55.0%)	ARTEX default console port; also RStudio Server's default
443	563	421 confirmed
80	168	63 confirmed
8790	108 (4.7%)	Companion port, often paired with 8787
8443	19	
8080	16	
18787	14	Offset variant of 8787
7878	13	ARTEX default
8899	12	
8081	12	
8788	4	

One certificate per provider

Of the 498 confirmed ARTEX endpoints, 412 (82.7%) sit on two providers. Inside each provider, every controller presents the same TLS certificate. This points to one provisioning template per provider, applied to hundreds of servers.

Provider	Confirmed controllers	Certificate	JARM	Unconfirmed listeners with the same certificate
YANCY LIMITED (US, HK)	237, all on 443	One shared certificate on all 237 (100%); certificate name withheld	`29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787` on all 237	29 of 47 port 8787 candidates; 266 endpoints in total carry it
PEG TECH INC (US, HK)	175, all on 443	One shared certificate on all 175 (100%); certificate name withheld	`3fd3fd16d3fd3fd21c42d42d00000078e356c38fb85055d97a8bed930c8956` on 173	167 port 8787 candidates; 343 endpoints in total carry it

Certificate name withheld for both clusters. The shared certificate ties many unconfirmed port 8787 listeners to confirmed controllers on the same provider.

The other 86 confirmed ARTEX controllers spread across smaller networks. CTG Server Limited holds 9, Hangzhou Alibaba 8, HostPapa 6, NetLab Global 5, Shenzhen Tencent 4 and Oracle 4.

Provider footprint

PEG TECH INC is the largest single home for ARTEX: 634 ARTEX endpoints on 573 hosts (635 endpoints in total). Besides the 175 confirmed controllers, it carries 357 candidates on 8787 and 100 on 8790.

YANCY LIMITED appears under two network names. Together they carry 284 ARTEX endpoints: the 237 confirmed controllers plus 47 port 8787 candidates. They also carry 6 DarkSword endpoints, for 290 in total. In all, 918 ARTEX endpoints sit on PEG TECH INC (634) and the YANCY networks (284).

The port 8787 and 8790 fleet

The 1,380 listeners on 8787 and 8790 are unconfirmed and sit on the same budget providers.

Provider	Listeners on 8787 or 8790
PEG TECH INC	357 on 8787, 100 on 8790
Shenzhen Tencent	102
Hangzhou Alibaba	77
NetLab Global	70
cognetcloud INC	51
Yancy Limited	47

Sixty-two hosts bind 8787 and 8790 together, and 61 of them sit on PEG TECH INC. The pairing looks like a primary and fallback port set by the same template.

Seven port 8787 listeners also serve an open directory, and 41 on 8787 or 8790 sit behind shared Cloudflare or Traefik certificates (Chapter 6).

Confirmed controllers off the two big providers

Several confirmed ARTEX controllers use other ports and providers. Examples include 8.216.54[.]254 on Alibaba US Technology in Japan (ports 80 and 443) and 64.90.1[.]153:8083 on NetLab Global (JARM prefix `1dd40d40d`). Another is 110.42.238[.]147:7676 on Shenzhen Tencent. Chapter 9 lists the 12 published ARTEX endpoints in Appendix A.

How these counts relate to Monographs 04 and 11

The 237 YANCY and 175 PEG TECH controllers match Monographs 04 and 11. Monograph 04 counted 501 ARTEX endpoints including suspected ones, and Monograph 11 counted 2,121. Each study draws a different set, so the totals differ while the two certificate clusters stay the same.

04

CHAPTER 04

DarkSword: CNServer and High-Port Hubs

IN SHORT

DarkSword has 362 endpoints on 313 hosts. Over half sit on CNServer LLC as suspected port 443 listeners. The 28 confirmed endpoints sit on other providers and pair standard ports with 8443, 8888 and 2000.

INSIDE THIS CHAPTER

The CNServer LLC cluster 14

Confirmed DarkSword hubs 15

Ports 8888 and 2000 15

04 DarkSword: CNServer and High-Port Hubs

DarkSword listens on 443 (223 endpoints, 61.6%), 8888 (69, 19.1%), 2000 (28, 7.7%), 80 (23), 3000 (5) and 8443 (3).

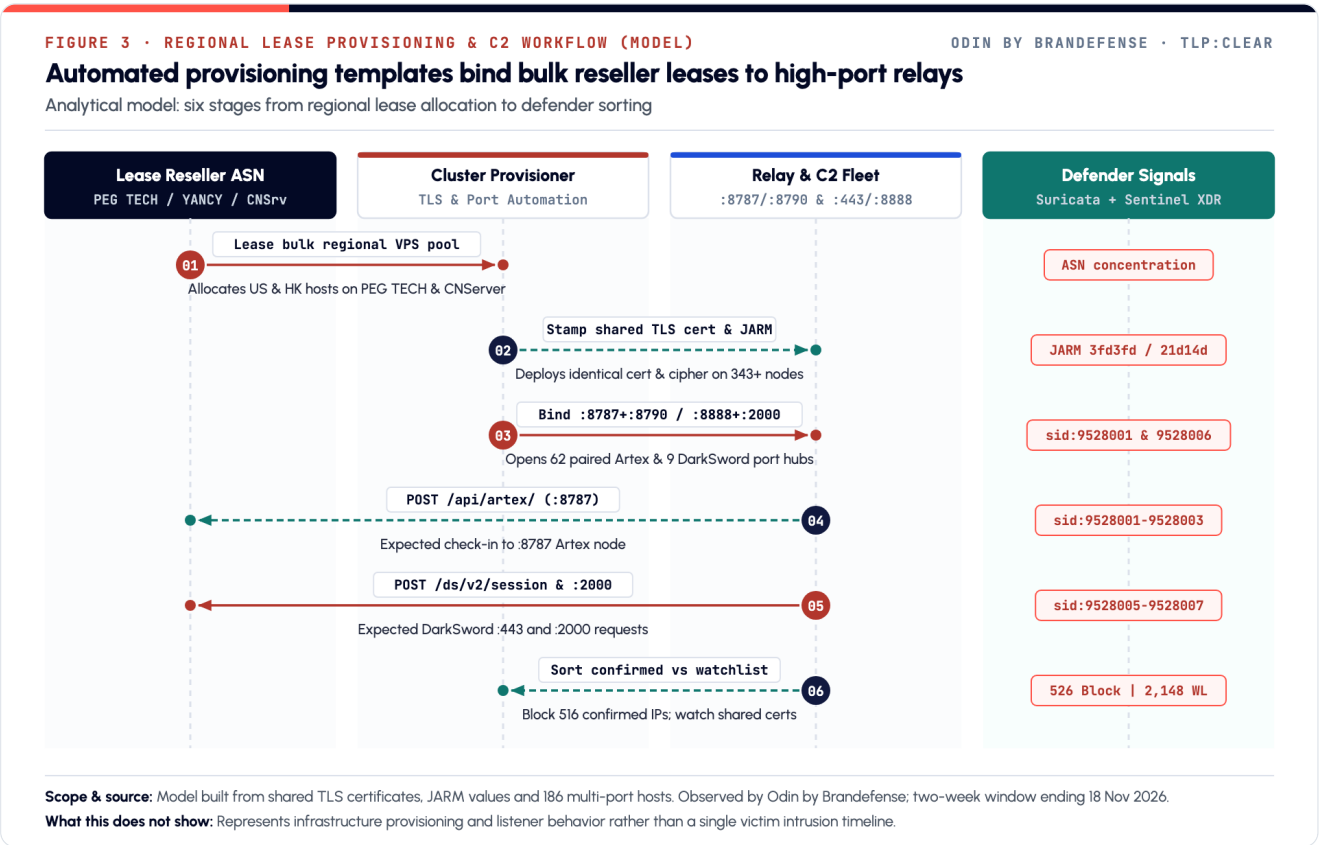


Figure 3: Analytical model of how bulk reseller leases are bound to high-port listeners

Figure 3 is an analytical model inferred from shared certificates, JARM values and port pairs. The HTTP paths in steps 04 and 05 are the strings our rules look for, not captured traffic.

The CNServer LLC cluster

CNServer LLC hosts 189 of the 362 DarkSword endpoints (52.2%). It is the densest single pairing of provider and family in this study.

CNServer LLC DarkSword group	Endpoints
Suspected listeners on 443	186
...of which share JARM `21d14d00021d21d00042d43d00000091f9827a8676a9d9f27d421962a09b5d`	174
Candidate web consoles on 3000, same JARM	3

A shared JARM value fits either a shared C2 bundle or the provider's standard server image. We therefore keep all 186 port 443 listeners on a 7-day watchlist and do not publish their addresses. Block a subnet here only with a second signal, such as a matching URI.

Confirmed DarkSword hubs

The 28 confirmed DarkSword endpoints sit on 19 hosts, so a confirmed host often exposes more than one port. CTG Server Limited holds 7 of them, Datacamp Limited 4, YANCY LIMITED 3 and SOLLUTIUM 2.

Endpoint	Provider (country)	Pattern
27.124.7[.]56:80, :443, :8443	CTG Server Limited (HK)	Three confirmed ports on one host; same certificate on 443 and 8443
103.43.71[.]178:2000	CyberForest LLC. (KR)	Confirmed listener on port 2000
193.218.201[.]146:443	Spartan Host Ltd (US)	TLS controller
206.187.214[.]37:443	cognetcloud INC (HK)	TLS controller; JARM also seen on Cloudflare-fronted hosts
43.229.112[.]254:443	YANCY LIMITED (US)	One of 3 confirmed DarkSword endpoints on YANCY
85.137.62[.]160:443	SOLLUTIUM EU (NL)	One of 2 confirmed in the Netherlands
86.38.247[.]228:80, :443	Datacamp Limited (SG)	Confirmed on both ports

Seven confirmed hosts bind ports 80 and 443 together. Six of them are not in the table above. They appear in this report only, not in Appendix A.

Host	Provider (country)
118.107.21[.]193	CTG Server Limited (HK)
181.215.18[.]87	Datacamp Limited (HK)
191.40.44[.]243	CORENET CLOUD SDN. BHD. (US)
47.85.134[.]152	Alibaba US Technology (US)
52.237.90[.]192	Microsoft Corporation (SG)
64.90.7[.]155	NetLab Global (HK)

Ports 8888 and 2000

DarkSword's 97 high-port listeners split into 69 on 8888 and 28 on 2000. They sit mostly on CTG Server Limited, cognetcloud INC and Datacamp Limited. Nine candidate hosts expose 8888 and 2000 together.

Only one port 2000 listener, 103.43.71[.]178, is confirmed. Treat the rest as leads, because routers and proxies also use these ports (Chapter 6).

05

CHAPTER 05

Multi-Port Hosts and Shared TLS Stacks

IN SHORT

Of the 2,468 hosts, 186 (7.5%) expose two to four of these listeners at once. Three JARM values cover 850 endpoints (31.8%), so the TLS stack stays visible even when the addresses rotate.

INSIDE THIS CHAPTER

Port pairs 17

JARM clusters 18

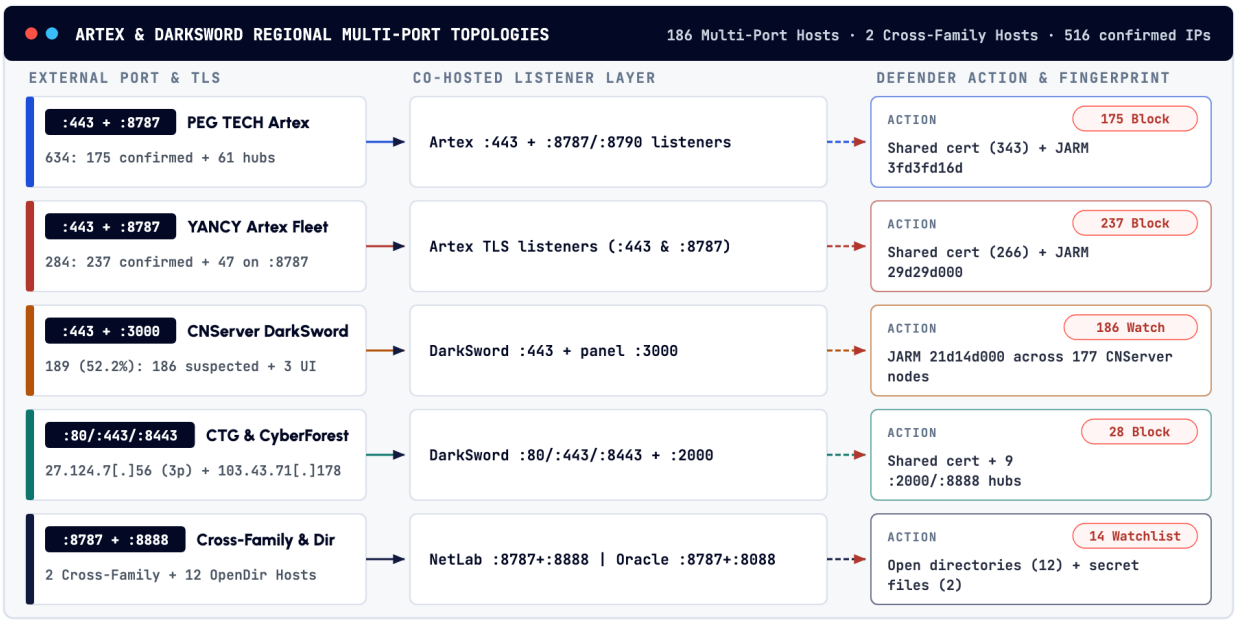
The two hosts that carry both families 18

05 Multi-Port Hosts and Shared TLS Stacks

FIGURE 4 · MULTI-PORT HUB & CLUSTER STACK BLUEPRINT
ODIN BY BRANDEFENSE · TLP:CLEAR

Paired listener ports and reused TLS certificates expose cluster templates

Observed port pairings, listener roles, and certificate/JARM artifacts across 186 multi-port hosts (n = 2,674)



Scope & source: Composite of multi-port, ASN-clustered and cross-family hosts. Observed by Odin by Brandefense; two-week window ending 18 Nov 2026.
What this does not show: Addresses of the 2,148 watchlist endpoints and all certificate names are withheld.

Figure 4: Paired listener ports and reused TLS certificates expose cluster templates

Port pairs

The 186 multi-port hosts expose 392 endpoints between them. Of these hosts, 170 have two ports, 12 have three and 4 have four.

Pattern	Hosts	Detail
ARTEX 8787 + 8790	62	61 on PEG TECH INC
ARTEX 80 + 8787	19	
ARTEX 443 + 8787	17	
ARTEX 80 + 443	12	Includes confirmed hub 8.216.54[.]254
ARTEX 80 + 443 + 8080 + 8787	4	Four-port hosts
DarkSword 80 + 443	10	7 confirmed two-port hubs plus the three-port hub 27.124.7[.]56
DarkSword 2000 + 8888	9	Candidates
DarkSword 443 + 8888	7	
DarkSword 443 + 3000	3	All on CNServer LLC

JARM clusters

JARM is an active TLS fingerprint. Servers that share a TLS library and configuration return the same 62-character value. A shared JARM can mean one operator's template or one provider's default image, so it is a hunting lead, not proof on its own.

JARM	Endpoints (ARTEX / DarkSword)	Where it concentrates
`3fd3fd16d3fd3fd21c42d42d00000078e356c38fb85055d97a8bed930c8956`	368 (368 / 0)	PEG TECH INC: 173 confirmed 443 controllers plus 195 listeners on 8787 or 80
`29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787`	278 (278 / 0)	YANCY LIMITED: 237 confirmed 443 controllers plus port 8787 candidates
`21d14d00021d21d00042d43d00000091f9827a8676a9d9f27d421962a09b5d`	204 (21 / 183)	CNServer LLC: 174 suspected DarkSword 443 listeners and 3 on 3000; 15 PEG TECH 8787 listeners
`3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763`	101 (84 / 17)	Mixed; includes Cloudflare-fronted hosts and confirmed 206.187.214[.]37
`40d40d40d00040d00042d42d000000831b6af40378e2dd35eeac4e9311926e`	20 (0 / 20)	DarkSword confirmed TLS stack: 11 of the 15 confirmed 443 endpoints, including 27.124.7[.]56

The first three values cover 850 endpoints, 31.8% of the study. The fourth mixes in shared Cloudflare edges, so do not block on it.

The two hosts that carry both families

Two hosts carry an ARTEX listener and a DarkSword listener side by side. One is on NetLab Global in Hong Kong (ARTEX on 8787, DarkSword on 8888). The other is on Oracle Corporation in the United States (ARTEX on 8787, DarkSword on 8088).

Both are unconfirmed candidates, so their addresses are withheld. They are the only cross-family link in the data. Two hosts out of 2,468 do not show that one group runs both families.

CHAPTER 06

What Not to Block

IN SHORT

Port and banner matches on 8787, 443, 8888 and 2000 also hit reverse proxies, data-science servers, routers and telecom subscribers. Of the 2,674 endpoints, 2,148 (80.3%) on 1,952 hosts stay on watchlists for that reason.

INSIDE THIS CHAPTER

Shared CDN and ingress certificates 20
Unrelated services on the same ports 20
Open directories 20
Dynamic telecom addresses 20
How the endpoints sort 21

06 What Not to Block

Shared CDN and ingress certificates

Forty-three candidate endpoints (41 ARTEX, 2 DarkSword) present a certificate that many unrelated tenants share.

Certificate subject	Endpoints
`CN=Cloudflare`	26
`CloudFlare Origin Certificate`	8
`TRAEFIK DEFAULT CERT`	7
`Kubernetes Ingress Controller Fake Certificate`	2

Blocking one can cut off every site behind the same edge, so route them to a 48-hour review. Do the same for any listener on a mail port (25, 110, 143, 465, 587, 993, 995).

There is one exception. Two ARTEX HTTP controllers on dedicated Alibaba VPS addresses use a Cloudflare Origin Certificate pinned to their own origin. They stay confirmed, because the address belongs to the server, not to a shared edge.

Unrelated services on the same ports

RStudio Server listens on 8787 by default, and Jupyter often uses 8888. MikroTik routers answer on 2000 for bandwidth tests. Enterprise proxies use 8888 as well. A port match alone cannot tell these apart from a C2 listener.

Open directories

Twelve ARTEX candidates also serve a browsable directory index. Seven sit on 8787, three on 8081 inside CNServer LLC (sharing one certificate), one on 8443 and one on 50549. Two of the port 8787 hosts, on POWER LINE DATACENTER in Hong Kong, also expose files that hold secrets. Their addresses are withheld, and they stay on a 7-day watchlist.

Dynamic telecom addresses

Two listeners sit on subscriber telecom networks. One is a confirmed ARTEX controller on China Telecom. The other is a suspected DarkSword listener on JT TELECOM INTERNATIONAL PTE.LTD. in Japan. Addresses on these networks pass between customers, so they get 24-hour watchlists, not permanent blocks.

How the endpoints sort

Group	Endpoints	Action
Confirmed on dedicated hosting	526 (516 hosts)	Block, review every 30 days
Suspected	226 (186 of them DarkSword on CNServer)	Watch for 7 days, look for a second signal
Candidates	1,908 (mostly 8787, 8790, 8888 and 2000 listeners)	Watch for 3 days, look for a URI or process match
Open-directory candidates	12	Watch for 7 days, hunt with SID 9528004
Dynamic telecom	2	Watch for 24 hours
Shared CDN or ingress certificate (within the groups above)	43	Review for 48 hours; never block automatically

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

- [ ] Block the 20 confirmed endpoints in Appendix A and the six confirmed hubs in Chapter 4 at the firewall and secure web gateway. Set a 30-day review.
- [ ] Put the two dynamic telecom listeners on a 24-hour watchlist and keep shared CDN addresses off automated block lists.

Within 72 hours

- [ ] Restrict workstation and server egress to ports 8787, 8790, 18787, 8888 and 2000 outside documented development subnets.
- [ ] Deploy Suricata SIDs 9528001 to 9528008. Send SID 9528004 (open-directory index) to a hunting queue, not an inline drop.
- [ ] Schedule the Sentinel query and the three Sigma rules. Name any sanctioned RStudio (8787) or Jupyter (8888) servers in the allowlists by exact host.

Within 7 to 30 days

- [ ] Pivot across proxy and NDR logs on JARM `3fd3fd16d...8956` (368 ARTEX endpoints) and `21d14d000...5d` (204 endpoints) on PEG TECH, YANCY and CNServer ranges.
- [ ] Ask for a second signal (URI, certificate or process) before blocking any suspected or candidate address.
- [ ] Add the pass rules your environment needs, such as internal RStudio servers, before enabling Suricata inline blocking.

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 other rules work 25

08 Detection Rules

The full rules are in Appendix B. Every rule file loads without errors in its engine (Suricata 7.0.12, YARA-X, pySigma, Kusto.Language); the rules were not replayed against live traffic. This report includes no captured ARTEX or DarkSword traffic, so test the HTTP strings in your own environment before blocking on them.

Rule file	What it catches
`odin_artex_and_darksword_clusters.rules`	Suricata 7: eight signatures for ARTEX and DarkSword check-ins, tasking responses, module requests, panel requests and open-directory indexes
`sentinel_artex_8787_and_darksword_cluster_hunt.kql`	Microsoft Sentinel and Defender XDR: contact with the 19 confirmed addresses, and non-browser traffic to the cluster ports joined with process command lines
`sigma_artex_darksword_implant_and_beaconing.yml`	Sigma (3 rules, Linux process creation): ARTEX listener or agent processes, DarkSword worker processes, and certificate or firewall provisioning scripts for the cluster ports
`odin_artex_darksword_cluster_implants.yar`	YARA (4 rules): ARTEX listener and controller configs, DarkSword controller configs, and panel or staging manifests

How the Suricata signatures work

SID	Looks for	Ports
9528001	Outbound `POST` to `/api/artex/` with `"node_uuid"` and `"beacon_int"` in the body	8787, 8790, 18787, 7878
9528002	Inbound 200 response with `"artex_task"` and `"jitter_ms"` in the body	From 8787, 8790, 18787
9528003	Request to `/artex/v1/sync` with an `X-Artex-Session:` header	80, 443, 8443
9528004	Directory listing (`Index of /`) that contains `artex_` ; policy alert for hunting	From 8787, 8081, 8443, 50549
9528005	`POST` to `/ds/v2/session` with an `X-DarkSword-ID:` header	443, 8443, 80
9528006	`POST` to `/darksword/queue` with `"task_opcode"` in the body	8888, 18888, 8088
9528007	Request to `/ds/module/pull` with a user agent that starts `DarkSword-Node/`	2000, 22000
9528008	Request to `/api/syndicate/health` with an `X-Syndicate-Token:` header	3000, 8080, 8787, 8888

Rules on port 443 or 8443 see the HTTP content only where TLS is decrypted. Where it is not, pair the rules with the JARM values in Chapter 5 and the Sentinel query.

How the other rules work

The KQL query looks back 7 days. It flags any contact with the 19 confirmed addresses, with no exclusion on that branch. It also flags non-browser traffic to ten cluster ports, excluding browsers by exact path and scanners by exact device name. It joins these events with command lines that name `artex`, `darksword`, the rule URIs or the cluster ports. Port-only cases need 12 or more connections.

The first Sigma rule needs an ARTEX or Python process with `/api/artex/`, `artex_relay` or a `--listen-port 8787` or 8790 argument. The second flags command lines with `darksword` or the DarkSword URIs. The third flags `openssl req` or `iptables` commands naming the cluster ports. All three exclude only named lab hosts.

YARA rule	Fires when (file under 512 KB)
`ODIN_Artex_8787_8790_Relay_Listener_Config`	`ARTEX_RELAY` or `artex_task`, plus 8787 or 8790, plus `/api/artex/`
`ODIN_Artex_TLS_Controller_Session_Manifest`	`/artex/v1/sync` and `X-Artex-Session`, plus `beacon_int` or `jitter_ms`
`ODIN_DarkSword_MultiPort_Controller_Config`	A matching pair: the session header and path, the queue path and `task_opcode`, or the module path and user agent
`ODIN_Regional_C2_Cohosted_Staging_Panel_Manifest`	The panel health path and token header, or `artex_staging_root` and `cohosted_opendir`

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

Confirmed endpoints in Appendix A 28

JARM fingerprints for hunting (text only) 29

09 Indicators

Appendix A holds 20 published indicators: 20 confirmed C2 endpoints (IP and port, on 19 distinct addresses). The 2 JARM fingerprints appear in this report only. It holds no file hashes. Six watchlist endpoints from the same selection are withheld, because they are suspected or candidate hosts.

Type	Count	Where
Confirmed C2 endpoints (IP and port)	20	Appendix A
JARM fingerprints for hunting	2	This report only
Watchlist endpoints	6	Withheld
Additional confirmed DarkSword hub addresses	6	Chapter 4 text only

The full list of 516 confirmed hosts is not published here. Certificate names, the cross-family hosts and all watchlist addresses are withheld.

Confirmed endpoints in Appendix A

Endpoint	Family	Provider (country)	Seen
38.12.72[.]83:443	ARTEX	PEG TECH INC (US)	14 Nov 2026
38.38.175[.]199:443	ARTEX	PEG TECH INC (US)	14 Nov 2026
103.48.132[.]2:443	ARTEX	YANCY LIMITED (US)	14 Nov 2026
156.234.57[.]93:443	ARTEX	YANCY LIMITED (HK)	14 Nov 2026
8.216.54[.]254:443	ARTEX	Alibaba US Technology (JP)	18 Nov 2026
8.166.116[.]93:80	ARTEX	Hangzhou Alibaba (CN)	18 Nov 2026
8.137.13[.]182:8888	ARTEX	Hangzhou Alibaba (CN)	13 Nov 2026
64.90.1[.]153:8083	ARTEX	NetLab Global (HK)	13 Nov 2026
45.77.24[.]71:8443	ARTEX	The Constant Company (JP)	13 Nov 2026
110.42.238[.]147:7676	ARTEX	Shenzhen Tencent (CN)	13 Nov 2026
103.45.68[.]143:80	ARTEX	CTG Server Limited (HK)	14 Nov 2026
172.245.215[.]3:443	ARTEX	HostPapa (US)	13 Nov 2026
103.43.71[.]178:2000	DarkSword	CyberForest LLC. (KR)	13 Nov 2026
27.124.7[.]56:443	DarkSword	CTG Server Limited (HK)	13 Nov 2026
27.124.7[.]56:8443	DarkSword	CTG Server Limited (HK)	13 Nov 2026
193.218.201[.]146:443	DarkSword	Spartan Host Ltd (US)	13 Nov 2026
206.187.214[.]37:443	DarkSword	cognetcloud INC (HK)	13 Nov 2026
43.229.112[.]254:443	DarkSword	YANCY LIMITED (US)	13 Nov 2026

Endpoint	Family	Provider (country)	Seen
85.137.62[.]160:443	DarkSword	SOLLUTIUM EU (NL)	13 Nov 2026
86.38.247[.]228:443	DarkSword	Datacamp Limited (SG)	13 Nov 2026

45.77.24[.]71 and 172.245.215[.]3 present self-signed certificates that carry their own IP address as the subject.

JARM fingerprints for hunting (text only)

JARM	Use
`3fd3fd16d3fd3fd21c42d42d00000078e356c38fb85055d97a8bed930c8956`	ARTEX on PEG TECH INC, 368 endpoints (173 confirmed)
`21d14d00021d21d00042d43d00000091f9827a8676a9d9f27d421962a09b5d`	Mostly DarkSword on CNServer LLC, 204 endpoints (183 DarkSword, 21 ARTEX)

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

- **Server side only.** The data shows listeners, certificates and TLS fingerprints on internet-facing servers. It shows no victim activity and no proof that any implant reached a target.
- **Family labels come from upstream.** "ARTEX" and "DarkSword" are labels attached to the records. "DarkSword" in particular is a feed label, not attribution to any named group or vendor report.
- **Clusters are a model.** Shared certificates and JARM values link hosts inside a cluster. Only two candidate hosts link the families, so this report makes no claim that one group runs both.
- **Most endpoints are unconfirmed.** Of the 2,674 endpoints, 2,148 are suspected, candidate or held for review. Port 8787, 8888 and 2000 also host benign services.
- **Rule testing.** Every rule file loads without errors in its engine (Suricata 7.0.12, YARA-X, pySigma, Kusto.Language). The rules have not been replayed against live traffic. Their HTTP strings are not drawn from captured traffic in this report.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. MITRE ATT&CK, Non-Standard Port (T1571): attack.mitre.org/techniques/T1571 (verified on 20 November 2026).
2. MITRE ATT&CK, Application Layer Protocol: Web Protocols (T1071.001): attack.mitre.org/techniques/T1071/001 (verified on 20 November 2026).
3. MITRE ATT&CK, Acquire Infrastructure: Virtual Private Server (T1583.003): attack.mitre.org/techniques/T1583/003 (verified on 20 November 2026).
4. Salesforce Engineering, Easily Identify Malicious Servers on the Internet with JARM: engineering.salesforce.com (verified on 20 November 2026).
5. Open Information Security Foundation (OISF), Suricata 7.0 User Guide: HTTP Keywords: docs.suricata.io (verified on 20 November 2026).

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

Appendix A lists the indicators published for this study. Appendix B carries every published detection rule in full.

INSIDE

A. Indicators of compromise (20) 35

B. Detection rules (4 files) 36

A Indicators of Compromise

Values are defanged for display. The CSV, JSON and STIX files on the online edition carry the raw values. Values the report marks as withheld are not listed.

ID	Type	Indicator	Port	Context	Action
R28-IOC-01	IPv4	38.12.72[.]83	443	artex	BLOCK
R28-IOC-02	IPv4	38.38.175[.]199	443	artex	BLOCK
R28-IOC-03	IPv4	103.48.132[.]2	443	artex	BLOCK
R28-IOC-04	IPv4	156.234.57[.]93	443	artex	BLOCK
R28-IOC-05	IPv4	8.216.54[.]254	443	artex	BLOCK
R28-IOC-06	IPv4	8.166.116[.]93	80	artex	BLOCK
R28-IOC-07	IPv4	8.137.13[.]182	8888	artex	BLOCK
R28-IOC-08	IPv4	64.90.1[.]153	8083	artex	BLOCK
R28-IOC-09	IPv4	45.77.24[.]71	8443	artex	BLOCK
R28-IOC-10	IPv4	110.42.238[.]147	7676	artex	BLOCK
R28-IOC-11	IPv4	103.45.68[.]143	80	artex	BLOCK
R28-IOC-12	IPv4	172.245.215[.]3	443	artex	BLOCK
R28-IOC-13	IPv4	103.43.71[.]178	2000	darksword	BLOCK
R28-IOC-14	IPv4	27.124.7[.]56	443	darksword	BLOCK
R28-IOC-15	IPv4	27.124.7[.]56	8443	darksword	BLOCK
R28-IOC-16	IPv4	193.218.201[.]146	443	darksword	BLOCK
R28-IOC-17	IPv4	206.187.214[.]37	443	darksword	BLOCK
R28-IOC-18	IPv4	43.229.112[.]254	443	darksword	BLOCK
R28-IOC-19	IPv4	85.137.62[.]160	443	darksword	BLOCK
R28-IOC-20	IPv4	86.38.247[.]228	443	darksword	BLOCK

B Detection Rules

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

odin_artex_and_darksword_clusters.rules

SURICATA

```
# Odin by Brandefense - Monograph 28 / 30 Suricata 7.x Detection Suite
# Coverage: Artex (:8787/:8790/:443/:80) and DarkSword (:443/:8888/:2000) C2 clusters
# Classification: TLP:CLEAR

alert http $HOME_NET any -> $EXTERNAL_NET [8787,8790,18787,7878] (msg:"ODIN [R28] Artex Non-Standard Port C2
Check-In"; flow:established,to_server; http.method; content:"POST"; http.uri; content:"/api/artex/";
fast_pattern; http.request_body; bsize:>24; content:"\"node_uuid\""; content:"\"beacon_int\""; distance:0;
classtype:trojan-activity; sid:9528001; rev:1; metadata:created_at 2026_11_20, deployment perimeter, tactic
command_and_control;)

alert http $EXTERNAL_NET [8787,8790,18787] -> $HOME_NET any (msg:"ODIN [R28] Artex Port 8787 Listener Tasking
Response"; flow:established,from_server; http.stat_code; content:"200"; http.response_body; bsize:>28;
content:"\"artex_task\""; fast_pattern; content:"\"jitter_ms\""; distance:0; classtype:trojan-activity; sid:
9528002; rev:1; metadata:created_at 2026_11_20, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,443,8443] (msg:"ODIN [R28] Artex Leased Controller Session
Heartbeat"; flow:established,to_server; http.uri; content:"/artex/v1/sync"; fast_pattern; http.header; bsize:>18;
content:"X-Artex-Session:"; classtype:trojan-activity; sid:9528003; rev:1; metadata:created_at 2026_11_20,
deployment perimeter, tactic command_and_control;)

alert http $EXTERNAL_NET [8787,8081,8443,50549] -> $HOME_NET any (msg:"ODIN [R28] Hunt Artex Co-Hosted Open-
Directory Staging Index"; flow:established,from_server; http.stat_code; content:"200"; http.response_body;
bsize:>36; content:"Index of /"; content:"artex_"; fast_pattern; distance:0; classtype:policy-violation; sid:
9528004; rev:1; metadata:created_at 2026_11_20, deployment perimeter, policy opendir_hunt;)

alert http $HOME_NET any -> $EXTERNAL_NET [443,8443,80] (msg:"ODIN [R28] DarkSword Primary Controller
Registration Beacon"; flow:established,to_server; http.method; content:"POST"; http.uri; content:"/ds/v2/
session"; fast_pattern; http.header; bsize:>18; content:"X-DarkSword-ID:"; classtype:trojan-activity; sid:
9528005; rev:1; metadata:created_at 2026_11_20, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [8888,18888,8088] (msg:"ODIN [R28] DarkSword Port 8888 Operator Relay
Queue Poll"; flow:established,to_server; http.method; content:"POST"; http.uri; content:"/darksword/queue";
fast_pattern; http.request_body; bsize:>22; content:"\"task_opcode\""; classtype:trojan-activity; sid:9528006;
rev:1; metadata:created_at 2026_11_20, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [2000,22000] (msg:"ODIN [R28] DarkSword Port 2000 Auxiliary Module
Staging Request"; flow:established,to_server; http.uri; content:"/ds/module/pull"; fast_pattern; http.user_agent;
bsize:>15; content:"DarkSword-Node/"; startswith; classtype:trojan-activity; sid:9528007; rev:1;
metadata:created_at 2026_11_20, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [3000,8080,8787,8888] (msg:"ODIN [R28] Regional C2 Management Panel
Health Request"; flow:established,to_server; http.uri; content:"/api/syndicate/health"; fast_pattern;
http.header; bsize:>20; content:"X-Syndicate-Token:"; classtype:trojan-activity; sid:9528008; rev:1;
metadata:created_at 2026_11_20, deployment perimeter, tactic command_and_control;)
```

odin_artex_darksword_cluster_implants.yar

YARA

```
/*
   Odin by Brandefense - Monograph 28 / 30 YARA Artifact Suite
   Scope: Sanitized configuration, relay, and provisioning manifests for Artex (:8787/:8790/:443)
          and DarkSword (:443/:8888/:2000) regional C2 clusters.
   Classification: TLP:CLEAR
*/

rule ODIN_Artex_8787_8790_Relay_Listener_Config
{
```

```
    meta:
        author = "Odin by Brandefense"
        monograph = "28 / 30"
        classification = "TLP:CLEAR"
        description = "Matches Artex non-standard port 8787/8790 relay and beacon listener manifests"
    strings:
        $a1 = "ARTEX_RELAY" ascii
        $a2 = "artex_task" ascii nocase
        $p1 = "8787" ascii
        $p2 = "8790" ascii
        $u1 = "/api/artex/" ascii
    condition:
        filesize < 512KB and ($a1 or $a2) and ($p1 or $p2) and $u1
}

rule ODIN_Artex_TLS_Controller_Session_Manifest
{
    meta:
        author = "Odin by Brandefense"
        monograph = "28 / 30"
        classification = "TLP:CLEAR"
        description = "Matches Artex leased TLS controller sync and session headers"
    strings:
        $s1 = "/artex/v1/sync" ascii
        $s2 = "X-Artex-Session" ascii
        $c1 = "beacon_int" ascii nocase
        $c2 = "jitter_ms" ascii nocase
    condition:
        filesize < 512KB and $s1 and $s2 and ($c1 or $c2)
}

rule ODIN_DarkSword_MultiPort_Controller_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "28 / 30"
        classification = "TLP:CLEAR"
        description = "Matches DarkSword primary (:443), relay (:8888), and module (:2000) controller configs"
    strings:
        $d1 = "X-DarkSword-ID" ascii
        $d2 = "/ds/v2/session" ascii
        $q1 = "/darksword/queue" ascii
        $q2 = "task_opcode" ascii nocase
        $m1 = "/ds/module/pull" ascii
        $m2 = "DarkSword-Node/" ascii
    condition:
        filesize < 512KB and (($d1 and $d2) or ($q1 and $q2) or ($m1 and $m2))
}

rule ODIN_Regional_C2_Cohosted_Staging_Panel_Manifest
{
    meta:
        author = "Odin by Brandefense"
        monograph = "28 / 30"
        classification = "TLP:CLEAR"
        description = "Matches regional C2 management panels or co-hosted staging manifests"
    strings:
        $h1 = "/api/syndicate/health" ascii
        $h2 = "X-Syndicate-Token" ascii
        $o1 = "artex_staging_root" ascii nocase
        $o2 = "cohosted_opendir" ascii nocase
    condition:
        filesize < 512KB and (($h1 and $h2) or ($o1 and $o2))
}
```

sentinel_artex_8787_and_darksword_cluster_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 28 / 30 Microsoft Sentinel & Defender XDR Hunt
// Correlates contact with confirmed Artex/DarkSword C2 addresses and non-browser traffic to non-standard ports
(:8787/:8790/:8888/:2000)
// Classification: TLP:CLEAR
// Exclusions use exact device names and exact browser executable paths only.
// Exclusions never apply to contact with a confirmed C2 address.

let Lookback = 7d;
let ApprovedInfraHosts = dynamic(["INFRA-MON-01", "EASM-SCANNER-01", "SEC-LAB-RUNNER-01"]);
let ApprovedBrowserPaths = dynamic([
    @"C:\Program Files\Google\Chrome\Application\chrome.exe",
    @"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe",
    @"C:\Program Files\Mozilla Firefox\firefox.exe"
]);
let ConfirmedC2IPs = dynamic([
    "38.12.72.83", "38.38.175.199", "103.48.132.2", "156.234.57.93",
    "8.216.54.254", "8.166.116.93", "8.137.13.182", "64.90.1.153",
    "45.77.24.71", "110.42.238.147", "103.45.68.143", "172.245.215.3",
    "103.43.71.178", "27.124.7.56", "193.218.201.146", "206.187.214.37",
    "43.229.112.254", "85.137.62.160", "86.38.247.228"
]);
let NonStandardPorts = dynamic([2000, 7676, 7878, 8083, 8787, 8790, 8888, 18787, 18888, 22000]);
let SuspiciousProcs = DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedInfraHosts))
    | where ProcessCommandLine has_any ("artex", "darksword", "/api/artex/", "/ds/v2/session", "/darksword/
queue")
        or (FileName in~ ("curl", "wget", "python", "python3", "powershell.exe", "rundll32.exe") and
ProcessCommandLine has_any (":8787", ":8790", ":8888", ":2000"))
    | project ProcTime = Timestamp, DeviceId, DeviceName, FileName, ProcessCommandLine;
DeviceNetworkEvents
| where Timestamp >= ago(Lookback)
| where RemoteIP in (ConfirmedC2IPs)
    or (RemotePort in (NonStandardPorts)
        and not(DeviceName in~ (ApprovedInfraHosts))
        and not(InitiatingProcessFolderPath in~ (ApprovedBrowserPaths)))
| summarize
    NetFirstSeen = min(Timestamp),
    NetLastSeen = max(Timestamp),
    DistinctRemoteIPs = dcount(RemoteIP),
    DistinctPorts = make_set(RemotePort, 16),
    MatchedConfirmedIPs = make_set_if(RemoteIP, RemoteIP in (ConfirmedC2IPs), 16),
    ConnectionCount = count()
    by DeviceId, DeviceName, InitiatingProcessFileName
| join kind=leftouter (SuspiciousProcs) on DeviceId, DeviceName
| where array_length(MatchedConfirmedIPs) > 0 or isnotempty(ProcessCommandLine) or ConnectionCount >= 12
| extend AlertDisposition = case(
    array_length(MatchedConfirmedIPs) > 0, "CONFIRMED_C2_CONTACT",
    (set_has_element(DistinctPorts, 8787) or set_has_element(DistinctPorts, 8790)) and ConnectionCount >= 12,
"HUNT_ARTEX_8787_8790_BEACON",
    (set_has_element(DistinctPorts, 8888) or set_has_element(DistinctPorts, 2000)) and ConnectionCount >= 12,
"HUNT_DARKSWORD_MULTIPORT_BEACON",
    "REVIEW_PORT_AND_PROCESS_CORRELATION"
)
| project NetFirstSeen, NetLastSeen, DeviceName, AlertDisposition, MatchedConfirmedIPs, DistinctRemoteIPs,
DistinctPorts, InitiatingProcessFileName, FileName, ProcessCommandLine, ConnectionCount
| sort by ConnectionCount desc
```

sigma_artex_darksword_implant_and_beaconing.yml

SIGMA

```
title: Artex High-Volume Port 8787 and 8790 Relay or Implant Execution
id: 8c41e290-3b17-4d82-9a64-202611192801
status: experimental
description: Detects unapproved execution of Artex C2 relay listeners or endpoint agents binding or connecting to
canonical TCP ports 8787, 8790, or 18787.
author: Odin by Brandefense
date: 2026/11/20
tags:
  - attack.command_and_control
  - attack.t1571
logsource:
  category: process_creation
  product: linux
detection:
  selection_runtime:
    Image|endswith:
      - '/artex-agent'
      - '/artex-relay'
      - '/python3'
      - '/nohup'
  selection_cli:
    CommandLine|contains:
      - '/api/artex/'
      - 'artex_relay'
      - '--listen-port 8787'
      - '--listen-port 8790'
  filter_approved_infra:
    ComputerName:
      - 'INFRA-MON-01'
      - 'EASM-SCANNER-01'
  condition: selection_runtime and selection_cli and not filter_approved_infra
falsepositives:
  - Internal application development services explicitly registered on port 8787
level: high
---
title: DarkSword Multi-Port 443 8888 and 2000 C2 Controller or Node Spawn
id: 4f72a913-6d08-4e51-b312-202611192802
status: experimental
description: Identifies DarkSword C2 controller, queue worker, or implant processes referencing DarkSword URI
paths or paired ports 8888 and 2000.
author: Odin by Brandefense
date: 2026/11/20
tags:
  - attack.command_and_control
  - attack.t1071.001
logsource:
  category: process_creation
  product: linux
detection:
  selection_ds:
    CommandLine|contains:
      - 'darksword'
      - '/ds/v2/session'
      - '/darksword/queue'
      - '/ds/module/pull'
  filter_lab:
    ComputerName:
      - 'SEC-LAB-RUNNER-01'
  condition: selection_ds and not filter_lab
falsepositives:
  - Dedicated adversary-simulation lab hosts registered with security operations
level: high
---
title: Templated Regional C2 TLS Certificate and Multi-Port Provisioning
id: 9b18c645-2a74-49c0-8e33-202611192803
status: experimental
description: Detects automated VPS provisioning scripts templating recurring TLS certificates across paired Artex
(8787/8790) or DarkSword (443/8888/2000) listeners.
```

```
  author: Odin by Brandefense
  date: 2026/11/20
  tags:
    - attack.resource_development
    - attack.t1583.003
  logsource:
    category: process_creation
    product: linux
  detection:
    selection_provision:
      CommandLine|re: '(openssl\s+req.*(8787|8790|darksword|artex)|iptables.*(8787|8790).*(443|8888|2000))'
    filter_lab:
      ComputerName:
        - 'SEC-LAB-RUNNER-01'
        - 'INFRA-MON-01'
    condition: selection_provision and not filter_lab
  falsepositives:
    - Sanctioned reverse-proxy provisioning pipelines documented in change management
  level: medium
```

ODIN

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/templated-c2-at-scale/
Short Read · brandefense.io/odin-research/blog/artex-and-darksword-c2-clusters-sit-on-a-few-lease/
Defense Kit · brandefense.io/odin-research/defense-kit/