ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 12 / 30 · DELIVERY INFRASTRUCTURE

Before the Payload Lands
Dual-Use Gates, RMM Servers and Relays

How Keitaro traffic gates, TacticalRMM, Hak5 Cloud C2, FRP and ReverseSSH can stage access, and how to tell them from legitimate use

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

5,892
Deduplicated endpoints in the study set (an estimate from aggregate summaries)

526
Estimated priority candidates and relays across the five tools

57
Keitaro cloaking-gate candidates

338
TacticalRMM fleet candidates on disposable or self-signed setups

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

How Keitaro traffic gates, TacticalRMM, Hak5 Cloud C2, FRP and ReverseSSH can stage access, and how to tell them from legitimate use

01	Executive Summary	04
02	How the Pieces Can Fit	07
03	Traffic Gates: Keitaro TDS	10
04	Persistence: TacticalRMM and Hak5 Cloud C2	13
05	Relays: FRP and ReverseSSH	16
06	Telling Hostile From Legitimate	19
07	What Defenders Should Do	21
08	Detection Rules	23
09	Indicators	27
10	Scope and Limits	30
11	Sources	32
A	Indicators of compromise (3)	34
B	Detection rules (4 files)	35

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense studied five dual-use tools that attackers can stage before a payload lands. Of 5,892 endpoints, an estimated 526 deserve attention. Each tool also serves marketers, IT providers or developers, so most hosts stay on watchlists. Three hosts are confirmed adversary infrastructure. Block those three, allowlist your approved remote-management domains, and alert when a browser visit is followed by an installer launch.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense studied five dual-use tools that attackers can stage before a payload lands. Of 5,892 endpoints, an estimated 526 deserve attention. Each tool also serves marketers, IT providers or developers, so most hosts stay on watchlists. Three hosts are confirmed adversary infrastructure. Block those three, allowlist your approved remote-management domains, and alert when a browser visit is followed by an installer launch.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 04

01 Executive Summary

The five tools are Keitaro, a commercial traffic direction system (TDS), and TacticalRMM, an open-source remote monitoring and management (RMM) suite. The other three are Hak5 Cloud C2, a controller for Hak5 implant devices, and two tunneling tools, Fast Reverse Proxy (FRP) and ReverseSSH. None of them is malware. Each has legitimate users, and each can also give an attacker a step in an access chain.

1. **An estimated 57 Keitaro gates look like cloaking gates, not marketing.**
   Only an estimated 57 Keitaro servers fit cloaking-gate patterns; most Keitaro installs serve ordinary marketing. They fall into three clusters: templated `CN=SolidityGameServer` servers, fresh default-certificate VPS gates, and fake CDN or tracker domains. Their redirects are visible, but not where they lead, so all stay on watchlists.

2. **TacticalRMM on fresh disposable domains offers signed, persistent remote access.**
   An estimated 338 TacticalRMM servers sit on new `.online`, `.xyz`, `.top` or `duckdns[.]org` domains. A signed MeshCentral agent gives an operator a shell over HTTPS port 443. Hostile use is not shown, so these stay on watchlists.

3. **Relays hide backends; three hosts are confirmed adversary infrastructure.**
   We found 114 FRP relays, and 86 of them (75.4%) expose a dashboard on port 7500. Four open directories held relay configs, a key dump and an exploit playbook. Only three hosts pass the bar for blocking: a Hak5 Cloud C2 server next to GoPhish, and two TLS-wrapped ReverseSSH listeners.

Three Decisions for Leaders

1. **Allowlist remote-management tools by domain.** Block unapproved TacticalRMM, MeshCentral and out-of-band SSH management traffic by default. Permit only documented corporate or managed service provider (MSP) subdomains.
2. **Link browser clicks to installer launches.** Join workstation connections to unapproved redirector or disposable domains with Windows Installer, PowerShell or RMM agent launches within five minutes.
3. **Never block a dual-use banner on its own.** Require a second signal, such as a co-hosted phishing kit or an IP-literal reverse-shell certificate. Hold everything else on watchlists, and ignore matches on mail ports.

The Study in Numbers

Number	What it is
5,892	Deduplicated endpoints in the study set (an estimate from aggregate summaries)
526	Estimated priority candidates and relays across the five tools
57	Keitaro cloaking-gate candidates
338	TacticalRMM fleet candidates on disposable or self-signed setups
114	FRP relays; 86 (75.4%) expose the port 7500 dashboard
3	Hosts confirmed as adversary infrastructure and published for blocking

How to use this report.

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

02

CHAPTER 02

How the Pieces Can Fit

IN SHORT

We measured the five tool populations separately. The four-layer access chain below is an analytical model of how they can combine, not one observed campaign.

INSIDE THIS CHAPTER

An analytical access model 07

Populations and candidates 08

02 How the Pieces Can Fit

An analytical access model

Many initial-access operations split their work across separate servers. One server attracts traffic, another filters it, a third keeps access to the victim, and a fourth relays traffic out of sight. The five tools in this report map onto those roles.

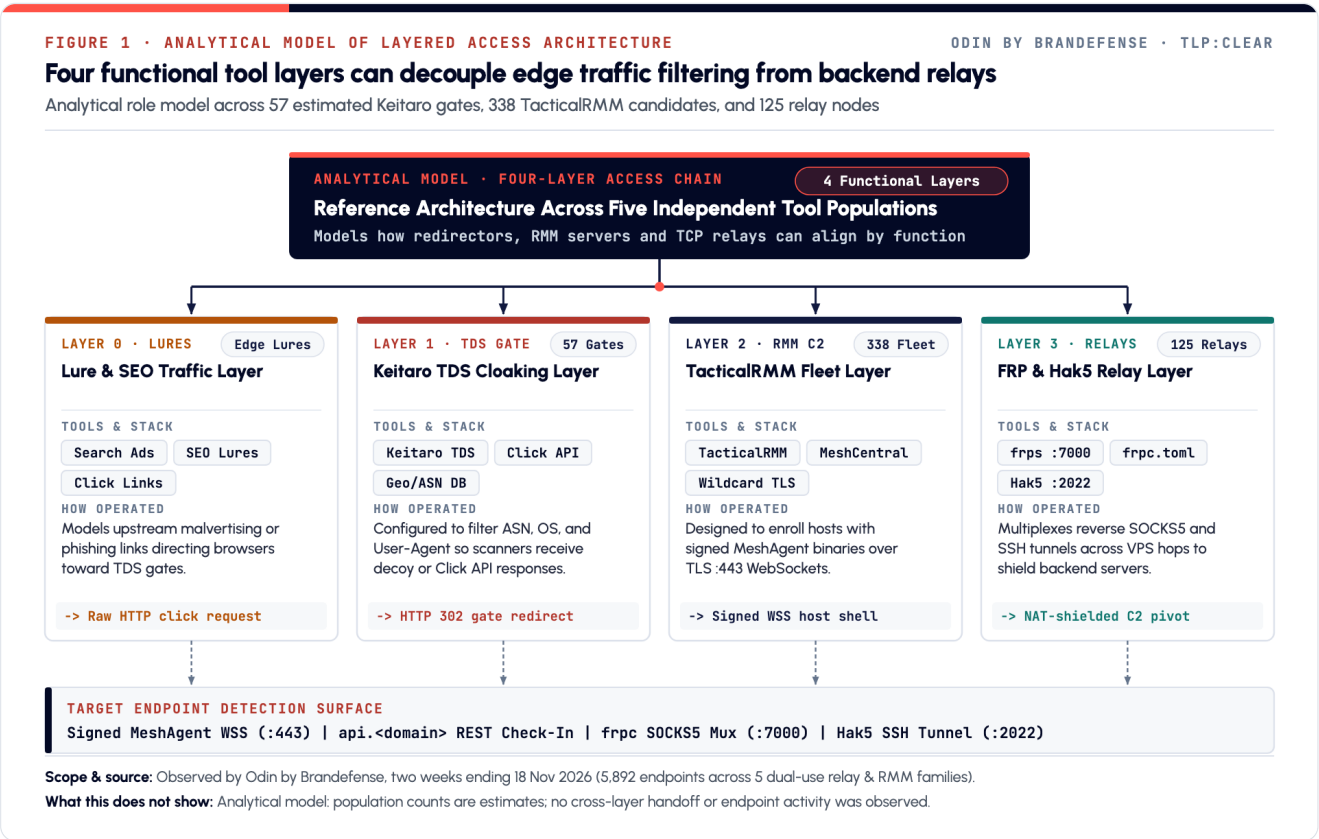


Figure 1: Four functional tool layers can decouple edge traffic filtering from backend relays

Layer	Role	Tools	What it gives an operator
0 Lures	Bring browsers in	Search ads, SEO lures, phishing links	Raw HTTP clicks
1 Traffic gate	Filter visitors and redirect the chosen ones	Keitaro TDS, Click API	HTTP 302 redirects that skip sandboxes
2 Remote management	Keep access to an enrolled host	TacticalRMM, MeshCentral, wildcard TLS	A signed agent with a WebSocket shell on 443
3 Relays	Hide the backend behind NAT-crossing tunnels	`frps` on 7000, `frpc.toml`, Hak5 on 2022, ReverseSSH	SOCKS5 and SSH tunnels across cheap VPS hops

This is a model. Outside a few shared servers, such as Hak5 Cloud C2 and GoPhish on 146.190.211[.]163, nothing links a specific Keitaro gate to a specific TacticalRMM or FRP server.

Populations and candidates

These tools are popular with legitimate users, so most installs are benign. The table gives each population and its estimated candidates.

Tool	Layer	Endpoints (hosts)	Estimated candidates	Main ports and hosting
Keitaro TDS	Traffic gate	3,092 (2,368)	57	443, 80; DigitalOcean and Vultr (US, NL, DE)
TacticalRMM	Remote management	2,634 (2,157)	338	443, 1024, 4430; Hetzner and OVH (US, DE, BR)
FRP (`frps`)	Relay	114 (114)	114	7500, 7000; Alibaba and Tencent (CN 70.2%)
Hak5 Cloud C2	Relay and implant control	22 (16)	11	8080, 9090 plus 2022; AWS and DigitalOcean (US, NL)
ReverseSSH	Relay	30 (23)	6	3232, 8082; 8 POP3S 995 mail collisions removed

The 5,892 endpoint and 526 candidate totals are estimates from aggregate summaries. Endpoint-level records for these populations are withheld because most hosts are dual-use. Chapter 9 lists a selected set of 28; only its 3 confirmed endpoints are published, and 25 are withheld.

"Software confirmed" names the tool. It does not mean the operator is hostile.

03

CHAPTER 03

Traffic Gates: Keitaro TDS

IN SHORT

Keitaro decides in milliseconds which visitor sees which page. An estimated 57 of 3,092 Keitaro endpoints look like cloaking gates, but none shows where its redirect leads, so all stay on watchlists.

INSIDE THIS CHAPTER

How a cloaking gate works 10

Three clusters that stand apart from marketing 11

Why these gates are not blocked 11

03 Traffic Gates: Keitaro TDS

How a cloaking gate works

Keitaro was built for affiliate marketing. It reads each visitor's network (ASN), country, operating system and browser, then routes the visitor to one of several weighted campaign streams. An attacker can use the same filters to send sandboxes and security scanners to a harmless page, while real targets get a redirect to an installer.

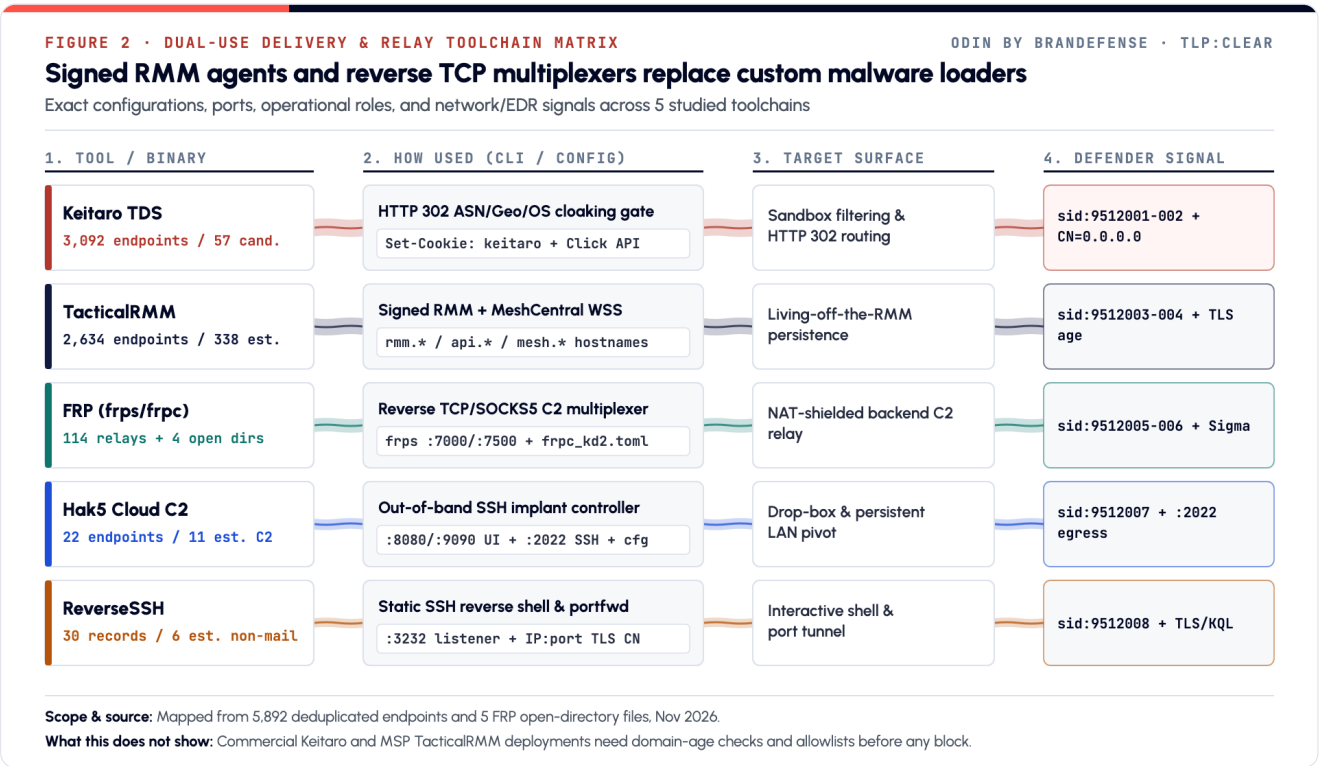


Figure 2: Signed RMM agents and reverse TCP multiplexers replace custom malware loaders

Operators run Keitaro in two ways:

- **Direct redirectors** answer with HTTP 302 and a `Set-Cookie: keitaro` header. They listen on 443 (1,802 endpoints) and 80 (1,218 endpoints).
- **Backend Click API v3 engines** sit behind WordPress or malvertising landing pages. Those pages call `/click_api/v3` and receive an `X-KClick-Token` header.

The gate sits upstream of the payload. A defender who sees the 302 chain can act before an installer lands.

Three clusters that stand apart from marketing

Commercial agencies usually bind Keitaro to aged brand domains behind Cloudflare (219 such records). The 57 candidates look different. They fall into three clusters.

Cluster	Certificates seen	Estimated gates	Hosting and fingerprint
Default `CN=0.0.0.0` TLS	973	21	Newly issued self-signed certificate, HTTP 302 with `X-KClick-Token`, JARM prefix `2ad2ad16d2ad2ad00042`
`SolidityGameServer` dual-port	45	24	Paired 8081 and 8082 listeners, mostly on The Constant Company in Germany, JARM prefix `2ad2ad16d00000022c2a`
CDN and tracker masquerade	Short-lived	12	Privacy or offshore hosts such as Privex Inc. and Melbikomas UAB, on domains that mimic ad or CDN services

The `SolidityGameServer` gates share certificate names, JARM values and one provider. The sampled ones were first seen on 13 and 14 November 2026. That uniformity suggests templated or automated setup rather than manual work.

Why these gates are not blocked

A gate's visible response shows the 302 and the Click API markers. It does not show the downstream `.msi` or `.ps1` destination. Without that, a gate cannot be told apart from an aggressive ad tracker. All eight sampled Keitaro gates in Chapter 9 are on watchlists, and their addresses are withheld.

CHAPTER 04

Persistence: TacticalRMM and Hak5 Cloud C2

IN SHORT

Signed remote-management agents get past controls that would stop an unsigned loader. An estimated 338 TacticalRMM servers and 11 Hak5 Cloud C2 controllers fit the pattern, and one Hak5 server shares its host with a phishing kit.

INSIDE THIS CHAPTER

Living off the RMM 13

How a TacticalRMM server is laid out 13

Disposable domains versus MSP domains 14

Hak5 Cloud C2 and a phishing neighbor 14

04 Persistence: TacticalRMM and Hak5 Cloud C2

Living off the RMM

Endpoint protection blocks many unsigned commodity loaders. A signed, legitimate RMM installer pointed at an attacker's own server raises fewer alarms. CISA advisory AA23-025A describes this abuse of remote monitoring and management software.

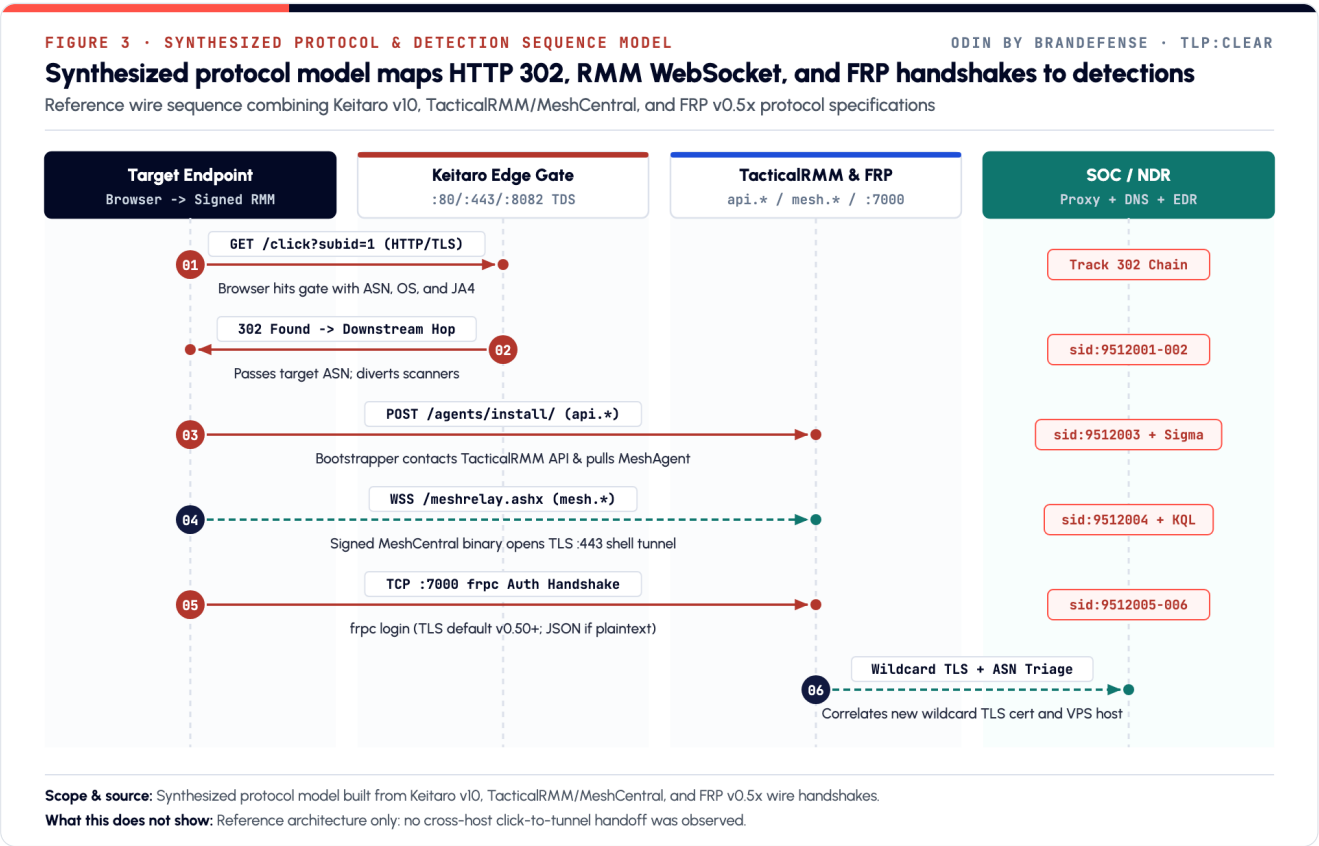


Figure 3: Synthesized protocol model maps HTTP 302, RMM WebSocket, and FRP handshakes to detections

Figure 3 is a protocol model built from the public specifications. It shows where each step appears on the wire and which rule sees it. No single host was seen doing all of these steps.

How a TacticalRMM server is laid out

A standard TacticalRMM install uses three DNS names behind Nginx. The official install covers them with one Let's Encrypt wildcard certificate (`*.<domain>`), though custom certificates also work.

Hostname	Service	Common ports	Records
`rmm.<domain>`	Vue operator console	443	Not split out
`api.<domain>`	Django `uWSGI` REST backend; agents enroll through `POST /agents/install/`	443 or 1024	405
`mesh.<domain>`	MeshCentral relay; remote shells and desktops run through `WSS /meshrelay.ashx`	443 or 4430	232

Once enrolled, the signed `MeshAgent.exe` opens a WebSocket over port 443. That gives an operator PowerShell and desktop access that looks like normal HTTPS.

Disposable domains versus MSP domains

Legitimate MSPs run TacticalRMM on corporate domains that are years old. The 338 candidates instead sit on newly registered disposable domains and dynamic DNS services.

Eight sampled servers sit on fresh wildcard certificates. Five are shown below, with addresses and domains withheld.

Certificate pattern	Hosting provider (country)	What stands out
`*.<withheld>.online`	Rackvolt Cloud (US)	New offensive-themed wildcard certificate; API on 1024 as well as 443
`*.<withheld>.top`	M247 Europe SRL (US)	New `.top` wildcard on a commercial VPS network
`*.<withheld>.xyz`	Sollutium EU (NL)	New `.xyz` wildcard on a commercial VPS network
`*.<withheld>.duckdns.org`	Blatant Tech (SC)	New dynamic DNS wildcard on an offshore VPS
`*.<withheld>.online`	Cherry Servers (US)	New wildcard exposing both the 1024 API and the 4430 relay

The certificates are single wildcards. We did not see an explicit three-name certificate list, and we saw no interaction with a victim. All eight stay on watchlists.

Hak5 Cloud C2 and a phishing neighbor

Hak5 Cloud C2 manages Hak5 hardware implants, such as the LAN Turtle, Packet Squirrel and WiFi Pineapple. It also manages Linux persistence clients (`cc-client`) set up through `/etc/device.config`. A controller shows a web console on 8080, 9090, 8088 or 443, plus port 2022 for device SSH tunnels.

Of 22 Hak5 endpoints on 16 IPs, an estimated 11 are controllers. Port 2022 belongs to Hak5 itself, so a console plus 2022 alone is not enough to block. The two standalone controllers in Chapter 9, on Amazon AWS and DigitalOcean, stay on watchlists.

One server is different. 146.190.211[.]163 on DigitalOcean (US) runs Hak5 Cloud C2 on 8088 and 2022. The same host runs a separate GoPhish phishing server on 3333, with the certificate `CN=*.maquitacushunfin[.]site`. A phishing kit next to an implant controller is a second, independent offensive signal. This host is confirmed and published for blocking.

05

CHAPTER 05

Relays: FRP and ReverseSSH

IN SHORT

Reverse proxies let an operator reach inside a network through a cheap cloud relay instead of a core server. We found 114 FRP relays, four open directories with relay files, and two TLS-wrapped ReverseSSH listeners confirmed for blocking.

INSIDE THIS CHAPTER

How FRP shields the backend 16
Where the relays run 17
What the open directories held 17
ReverseSSH on non-standard ports 17

05 Relays: FRP and ReverseSSH

How FRP shields the backend

FRP has two parts. The server, `frps`, runs on a cloud VPS. The client, `frpc`, runs inside the target network and dials out. Traffic then flows back through the relay, so the operator's own machine never faces the target. FRP can carry RDP, SMB and SOCKS5 traffic.

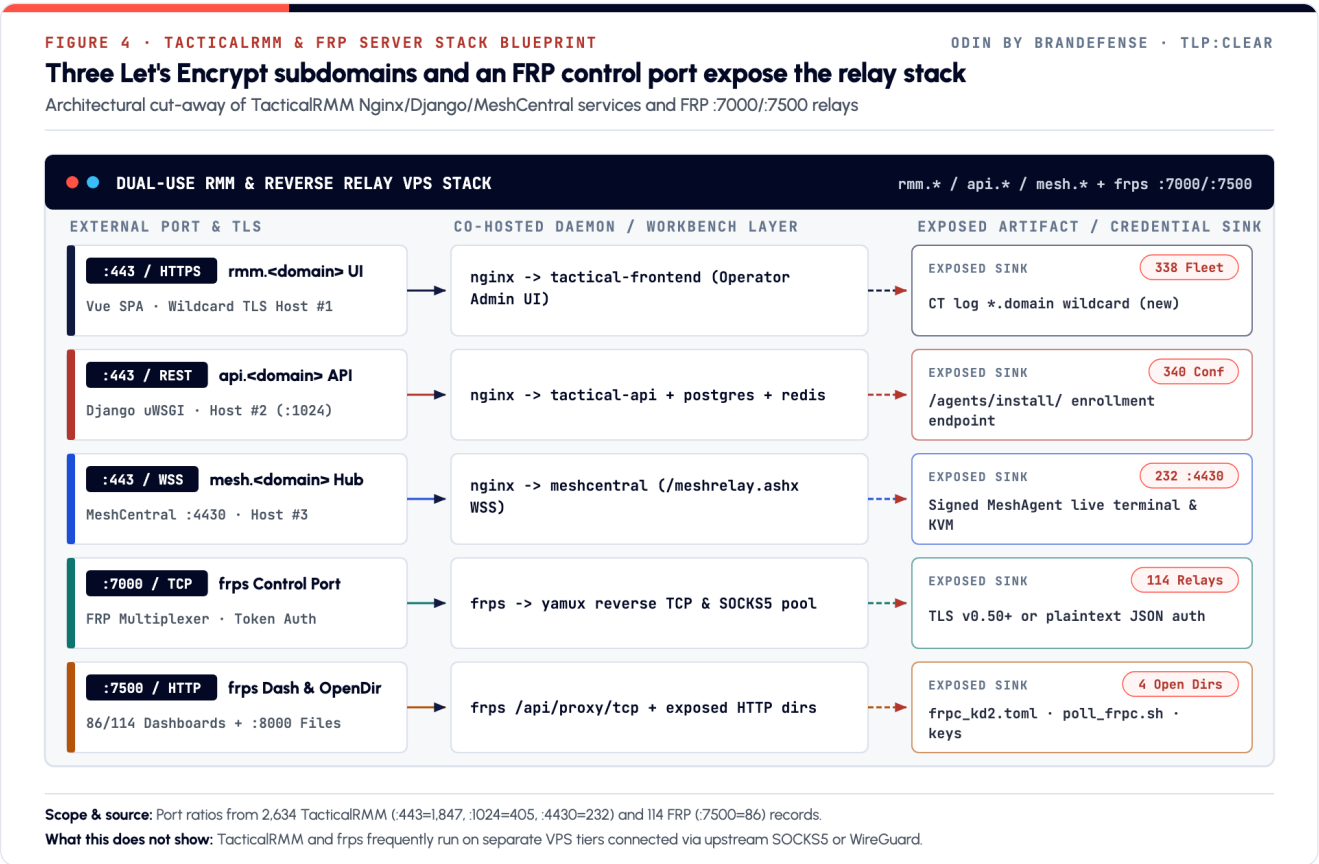


Figure 4: Three Let's Encrypt subdomains and an FRP control port expose the relay stack

Port	Service	What a defender sees
7000	`frps` control port; streams multiplexed with `yamux`	A JSON login with `version`, `privilege_key`, `timestamp` and `run_id`, but only when TLS is off
7500 (sometimes 17500)	`frps` web dashboard, with the `/api/proxy/tcp` API	An HTTP dashboard listing active tunnels

The `privilege_key` is an MD5 digest of the `auth.token` and a timestamp. From FRP v0.50.0, transport TLS is on by default (`transport.tls.enable = true`). The plaintext login is visible only on older builds, when TLS is turned off, or behind TLS inspection.

Where the relays run

Of the 114 relays, 86 (75.4%) leave the 7500 dashboard reachable. China hosts 70.2% of them, led by 61 nodes on Alibaba Cloud and 9 on Tencent. Developers also use FRP to expose test services, and ports and providers alone cannot tell the two apart. All 114 relay addresses are withheld and held on watchlists.

What the open directories held

Four open HTTP directories exposed five relay-related files. Some sit next to a 7000 relay. Whether their owners are attackers or lab administrators is unknown, and no separate C2 framework was found on them. All four hosts stay on watchlists.

Exposed file	Port	Hosting (country)	What it is
`/frpc_kd2.toml`	8000	Huawei Cloud (CN)	FRP v0.5x client config with an `auth.token` (secret withheld)
`/poll_frpc.sh`	18080	Alibaba Cloud (CN)	Cron watchdog script that restarts `frpc` tunnels when they drop
`/keydump.txt`	8000	Oracle Cloud (SG)	Dump of extracted keys, next to a 7000 relay
`/blind-rce-exploit/PLAYBOOK.md`	9999	Tencent (CN)	Remote code execution playbook next to a 7000 relay (2 records)

Three of these records were first listed before our window opened. The `frpc_kd2.toml` record was first seen on 17 November 2026.

ReverseSSH on non-standard ports

ReverseSSH is a static binary that accepts reverse SSH shells and port forwards over firewall-friendly ports. We saw 30 records on 23 IPs. Of these, 11 listen on the default port 3232: 4 as plaintext SSH and 7 behind self-signed `CN=:3232` TLS certificates.

Plaintext listeners on 3232, 8082 or 8443 send their SSH banner (`SSH-2.0-Go` or `SSH-2.0-OpenSSH`) straight to the client. Suricata SID 9512008 catches that.

The two hosts confirmed for blocking hide the banner inside TLS. Each uses a certificate whose common name is its own `IP:port`:

Endpoint	Hosting (country)	Certificate	JARM prefix
77.111.101[.]84:8082 (also 8443)	Latitude.sh (BR)	`CN=77.111.101[.]84:8082`	`3fd3fd0003fd3fd00043`
165.154.199[.]52:443	Scloud Pte Ltd (SG)	`CN=165.154.199[.]52:443`	`3fd3fd0003fd3fd00043`

TLS hides the inner SSH handshake from wire signatures. Find these hosts through the IP-literal certificate and JARM, egress hunting in KQL, and `ssh -R` process events in Sigma.

CHAPTER 06

Telling Hostile From Legitimate

IN SHORT

Blocking every Keitaro or TacticalRMM server would break marketing analytics and outsourced IT support. Four common lookalikes explain why most hosts in this report stay on watchlists.

INSIDE THIS CHAPTER

Four lookalikes 19

What it takes to block 19

06 Telling Hostile From Legitimate

An exposed TacticalRMM login page shows that the software is present. It does not show intent.

Four lookalikes

Lookalike	What we saw	How it is handled
MSPs and marketers	158 TacticalRMM records on aged MSP domains; Keitaro behind enterprise CDNs	Set aside and logged only, when the domain is old, the certificate is clean and no offensive tool shares the host
Mail servers	8 ReverseSSH records were POP3S mail servers at an Italian hosting provider (ports 995 and 110); 5 Hak5 records sat on mail ports of a Dutch VPS	Matches on mail ports 110, 143, 465, 993 and 995 are ignored
Authorized testers	Two suspected Hak5 Cloud C2 instances on Microsoft Azure (IE) and Amazon AWS (DE) present `CN=pentest` certificates	Analyst review; never auto-blocked or published
Home broadband	One TacticalRMM host sits on a dynamic Brazilian subscriber network; 30 TacticalRMM records are on dynamic ISPs	Watchlist entries that expire after 24 hours, so reassigned customer addresses are never blocked for good

What it takes to block

Everything else in this report needs a second, independent signal before a block. The three confirmed hosts have one each:

- **A co-hosted offensive tool.** 146.190.211[.]163 pairs Hak5 Cloud C2 with GoPhish.
- **An IP-literal reverse-shell certificate.** 77.111.101[.]84 and 165.154.199[.]52 wrap SSH in TLS under their own `IP:port` names.

A captured installer redirect from a Keitaro gate would also qualify. None of the sampled gates showed one.

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 three confirmed hosts: 146.190.211[.]163:8088, 77.111.101[.]84:8082 and 165.154.199[.]52:443.
- [ ] Keep watchlist indicators (Keitaro gates, wildcard TacticalRMM servers, standalone Hak5 controllers, FRP open directories, `CN=pentest` hosts) out of automatic block feeds.
- [ ] Exclude mail-port matches (995 POP3S and the other mail ports) from ReverseSSH hunting.

Within 72 hours

- [ ] List every approved RMM tool. Allow `rmm.*`, `api.*` and `mesh.*` traffic, including `/meshrelay.ashx`, only to documented corporate or MSP names, at DNS and the TLS proxy.
- [ ] Add WDAC or AppLocker rules that block unapproved `tacticalrmm.exe`, `MeshAgent.exe` and `frpc.exe`, even when the files carry a valid Authenticode signature.
- [ ] Restrict workstation egress on relay ports 2022, 3232, 4430, 7000, 7500 and 17500.

Within 7 to 30 days

- [ ] Inspect HTTP 302 chains with `keitaro` cookies. Correlate browser visits to domains registered in the last 30 days on `.xyz`, `.top`, `.online` or `duckdns[.]org` with `.msi`, `.vbs` or `.ps1` launches.
- [ ] Deploy Suricata SIDs 9512001 to 9512008, the Sentinel KQL hunt and the three Sigma rules.
- [ ] Alert on plaintext `SSH-2.0` banners from relay ports and on IP-literal TLS certificates.
- [ ] Rotate any token found in an exposed `frpc.toml`.

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 23

How the KQL query works 23

How the Sigma and YARA rules work 24

How to sort a host 24

Before you deploy 25

08 Detection Rules

The full rules are in Appendix B. Each file targets one layer of the model.

Rule file	What it catches
`odin_keitaro_tacticalrmm_frp.rules`	Suricata 7: eight signatures for Keitaro redirects, TacticalRMM enrollment and relay traffic, plaintext FRP logins, Hak5 consoles and ReverseSSH banners
`sentinel_unapproved_rmm_and_tds_redirect_chain.kql`	Microsoft Sentinel and Defender for Endpoint: browser-to-installer chains, unapproved RMM or FRP processes, and relay egress
`sigma_tacticalrmm_frpc_unauthorized_execution.yml`	Sigma (3 rules): unapproved TacticalRMM or MeshCentral agents, `frpc` tunnels, and Hak5 or ReverseSSH tunnels
`odin_tds_rmm_frp_staging_configs.yar`	YARA (4 rules): Keitaro gate configs, TacticalRMM bootstrap manifests, FRP client configs, and Hak5 or ReverseSSH provisioning files

How the Suricata signatures work

SID	Looks for	Tactic
9512001	A server 302 response whose cookie contains `keitaro` and a `subid`, `_subid` or `stream` marker	Initial Access
9512002	An internal client requesting `/click_api/v3`	Initial Access
9512003	An internal client calling TacticalRMM enrollment at `/agents/install/`	Persistence
9512004	A WebSocket upgrade to `/meshrelay.ashx`	Command and Control
9512005	An outbound plaintext FRP login with `privilege_key`, `version` and `timestamp` or `run_id`	Command and Control
9512006	Access to the FRP dashboard API `/api/proxy/tcp` on 7500, 17500, 8080 or 9527	Command and Control
9512007	`Hak5 Cloud C2` branding in an HTTP response body (unmodified consoles only)	Command and Control
9512008	A server response starting `SSH-2.0-Go` or `SSH-2.0-OpenSSH` from ports 3232, 8082 or 8443	Command and Control

The HTTPS rules (9512001 to 9512004 and 9512007) need TLS inspection or offload. The TCP rules (9512005 and 9512008) belong on perimeter egress. SID 9512005 sees only FRP builds older than v0.50.0 or sessions with TLS turned off. Bypass 9512003 and 9512004 for your documented MSP `api.` and `mesh.` names, and exclude sanctioned jump hosts from 9512008.

How the KQL query works

The Sentinel query uses a 14-day lookback and has three branches.

1. **Browser to installer.** It joins a browser connection to a confirmed host, a `click_api/v3` URL or a disposable domain with a later process launch. It looks for `msiexec.exe`, PowerShell, script hosts, `tacticalrmm.exe` or `MeshAgent.exe` on the same device within five minutes.
2. **Unapproved RMM or FRP process.** It flags `tacticalrmm.exe`, `MeshAgent.exe` or `frpc`, or command lines that mention `meshrelay.ashx`, `/agents/install/`, `frpc.toml`, `frpc.ini`, `privilege_key` or `device.config`.

3. **Relay egress.** It flags connections to the three confirmed hosts or to `rmm.`, `api.` or `mesh.` names on disposable domains. It also flags RMM, FRP or SSH processes that reach relay ports 2022, 3232, 4430, 7000, 7500 or 17500.

Fill the `ApprovedMspDomains` list before use. Treat the disposable-domain branch as a hunting lead, not an isolation trigger. Endpoint network events do not carry certificate details, so check domain age and certificate names in certificate transparency or passive TLS data first.

How the Sigma and YARA rules work

Rule	Fires when
Sigma: Unapproved TacticalRMM or MeshCentral Agent Execution	`tacticalrmm.exe` or `MeshAgent.exe` runs, or a command line names RMM enrollment or relay paths, outside approved MSP names
Sigma: FRP Reverse Relay Client Execution or Tunnel Multiplexing	`frpc` runs, or a command line references `frpc.toml` or `serverPort = 7000`; this works even when FRP traffic is encrypted
Sigma: Hak5 Cloud C2 or ReverseSSH Outbound Tunnel Invocation	A Linux command references Hak5 `/etc/device.config`, or `ssh -R` targets port 2022, 3232, 8082, 8443 or 443
YARA: `ODIN_Keitaro_TDS_Cloaking_Gate_Config`	`keitaro` appears with `X-KClick-Token`, `click_api/v3` or `object=campaigns`, plus `stream_id=` or `302 Found`
YARA: `ODIN_TacticalRMM_Agent_Bootstrap_Manifest`	Two TacticalRMM markers (`/agents/install/`, `/meshrelay.ashx`, `tacticalagent`) appear with two of the `api.`, `mesh.` and `rmm.` prefixes
YARA: `ODIN_FRP_Reverse_Relay_Client_Config`	A file has a server address, `serverPort = 7000`, an `auth.token` or `privilege_key`, and a `socks5` or `[[proxies]]` entry
YARA: `ODIN_Hak5_CloudC2_And_ReverseSSH_Provisioning`	Two Hak5 markers appear with 2022, or `device.config` appears with :3232

How to sort a host

The triage logic turns these signals into an action. It never blocks on one dual-use signal.

What the host shows	Action
An approved MSP or enterprise asset	Allow
A match on a standard mail port	Ignore as a collision
An aged domain, a clean business certificate and no co-hosted offensive tool	Log only
A `CN=pentest` certificate	Analyst review
A dynamic subscriber ISP address	Watchlist for 24 hours
A Keitaro gate with no captured installer, a wildcard RMM server on a new disposable domain, a standalone Hak5 controller, or an FRP relay or open directory	Watchlist and analyst review
A co-hosted offensive tool, a captured installer redirect, or an IP-literal reverse-shell certificate	Block

Before you deploy

Only the KQL query carries an allowlist, and it matches exact hostnames. The Sigma, Suricata and YARA rules have none, so suppress sanctioned MSP agents by exact host and agent ID first. 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. The YARA rules matched four sample config files and did not fire on two benign controls. Test all rules 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

Confirmed endpoints to block 27

Watchlist entries 27

ATT&CK tactics 28

09 Indicators

Appendix A holds the 3 confirmed endpoints. The other 25 records in the selected set are withheld.

Type	Count
Confirmed adversary endpoints to block (IP and port)	3
Watchlist endpoints, addresses withheld	24
Excluded mail-server collision, address withheld	1

Confirmed endpoints to block

Endpoint	Tool	Hosting (country)	Key fingerprint	First seen
146.190.211[.]163:8088	Hak5 Cloud C2	DigitalOcean (US)	Hak5 console on 8088 and 2022; GoPhish on 3333 with `CN=*.maquitacushunfin[.]site`	13 Nov 2026
77.111.101[.]84:8082	ReverseSSH	Latitude.sh (BR)	TLS-wrapped SSH on 8082 and 8443, `CN=77.111.101[.]84:8082`, JARM prefix `3fd3fd0003fd3fd00043`	14 Nov 2026
165.154.199[.]52:443	ReverseSSH	Scloud Pte Ltd (SG)	TLS-wrapped SSH, `CN=165.154.199[.]52:443`, same JARM prefix	13 Nov 2026

Watchlist entries

These 24 entries are for enrichment and analyst triage, not for blocking. Addresses and domains are withheld.

Group	Entries	Hosting (country)	Fingerprint to hunt
Keitaro gates	8	The Constant Company (DE, 3), Ultahost (DE), ROUTE 95 LLC (NL), Privex Inc. (NL), Melbikomas UAB (DE), Mulgin A.S. (UA)	`CN=SolidityGameServer` on 8081, 8082 and 443; `CN=0.0.0.0` with `X-KClick-Token`; `.life`, `.site` and lookalike domains with `/click_api/v3`
TacticalRMM servers on new wildcards	8	Rackvolt Cloud (US), M247 Europe (US), Sollutium EU (NL, 2), Blatant Tech (SC), Ultahost (NL), Amazon AWS (US), Cherry Servers (US)	New wildcards on `.online`, `.top`, `.xyz`, `.art`, `.site` and `duckdns[.]org`; API on 1024; one with `/meshrelay.ashx` on 443
TacticalRMM on dynamic broadband	1	Dynamic telecom network (BR)	24-hour watchlist only
Standalone Hak5 controllers	2	Amazon AWS (US), DigitalOcean (US)	Console on 8080 or 9090 plus 2022
FRP open directories	4	Tencent (CN), Oracle Cloud (SG), Alibaba Cloud (CN), Huawei Cloud (CN)	The relay files listed in Chapter 5
`CN=pentest` host	1	Microsoft Azure (IE)	`CN=pentest` with 3389 open; the second `CN=pentest` host (AWS, DE) is outside the selected set

Most entries were first seen between 13 and 18 November 2026. Three FRP open-directory records were first listed before our window.

Withheld: all 114 FRP relay addresses, the 24 watchlist addresses and domains, the `frpc_kd2.toml` token, the mail-server collision host, and all other candidate addresses.

ATT&CK tactics

Tactic	How the tools fit	Detection
Initial Access	Keitaro gates filter visitors and redirect the chosen ones	SIDs 9512001 and 9512002; KQL branch 1; YARA Keitaro rule
Persistence	Signed TacticalRMM and MeshCentral agents enroll and hold access	SID 9512003; KQL branch 2; Sigma rule 1; YARA TacticalRMM rule
Command and Control	MeshCentral WebSockets, FRP tunnels, Hak5 SSH and ReverseSSH listeners	SIDs 9512004 to 9512008; KQL branch 3; Sigma rules 2 and 3; YARA FRP and Hak5 rules

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

- **Window.** The findings cover a two-week observation window ending 18 November 2026. Three FRP directory records were first listed before the window; no dates are given for them.
- **Population totals are estimates.** The 5,892 endpoints, 526 candidates, 57 gates and 338 TacticalRMM servers come from aggregate summaries. Only 3 confirmed endpoints are published at endpoint level.
- **The access chain is a model.** The five tools were measured separately. Apart from shared hosts such as the Hak5 and GoPhish server, nothing links one layer to another.
- **Software present is not hostile intent.** Most hosts run legitimate tools for marketing, IT support or development. Only three hosts are confirmed adversary infrastructure.
- **Redirect targets are unseen.** No sampled Keitaro gate showed where its redirect leads, and no installer download was seen.
- **Open directories show staging, not use.** The relay configs, key dump and playbook are staged files. Whether their owners are attackers or lab administrators is unknown.
- **Rule testing.** Every published rule file loads without errors in its engine (Suricata 7.0.12, YARA-X, pySigma and Microsoft's Kusto.Language analyzer, checked on 20 November 2026). The rules were not replayed against live traffic, so test and tune 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. MITRE ATT&CK Enterprise tactics: Initial Access, Persistence, Command and Control. https://attack.mitre.org/tactics/enterprise/ (verified 18 November 2026)
2. CISA. Joint Cybersecurity Advisory AA23-025A, Protecting Against Malicious Use of Remote Monitoring and Management Software. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a (verified 18 November 2026)
3. Keitaro TDS documentation: campaign streams, filters, redirects and Click API v3. https://docs.keitaro.io/ (verified 18 November 2026)
4. TacticalRMM documentation, How It All Works: `rmm`, `api` and `mesh` hostnames, wildcard TLS, Django and MeshCentral. https://docs.tacticalrmm.com/howitallworks/ (verified 18 November 2026)
5. fatedier. Fast Reverse Proxy (FRP) repository: `frps`, `frpc.toml`, default TLS from v0.50.0, token authentication. https://github.com/fatedier/frp (verified 18 November 2026)
6. Hak5 Cloud C2 documentation: deployment, ports and `device.config`. https://docs.hak5.org/cloud-c2/ (verified 18 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 (3) 34

B. Detection rules (4 files) 35

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
R12-IOC-01	IPv4	146.190.211[.]163	8088	Hak5 Cloud C2 controller	BLOCK
R12-IOC-02	IPv4	77.111.101[.]84	8082	ReverseSSH listener	BLOCK
R12-IOC-03	IPv4	165.154.199[.]52	443	ReverseSSH listener	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_keitaro_tacticalrmm_frp.rules

SURICATA

```
# Odin by Brandefense - Report #12 Suricata 7.x Keitaro TDS, Candidate TacticalRMM, FRP & Hak5 Suite
# Classification: TLP:CLEAR
# Scope Note: Network HTTP/TLS offload and TCP relay handshake signatures (sid:9512001-9512008).
#             Pair RMM and TDS detections with enterprise MSP domain allowlists and host process telemetry.

# 1. Keitaro TDS HTTP 302 cloaked redirect with keitaro session/subid cookie marker
alert http any any -> $HOME_NET any (msg:"ODIN-TDS Keitaro HTTP 302 Cloaked Redirect Gate";
flow:established,from_server; http.stat_code; content:"302"; http.cookie; content:"keitaro"; nocase;
fast_pattern; pcre:"/(subid|_subid|stream)/i"; metadata:created_at 2026_11_18, tactic initial_access;
classtype:trojan-activity; sid:9512001; rev:1;)

# 2. Keitaro TDS Click API v3 Gate Query (/click_api/v3)
alert http $HOME_NET any -> any any (msg:"ODIN-TDS Keitaro Click API v3 Cloaking Gate Request";
flow:established,to_server; http.uri; content:"/click_api/v3"; nocase; fast_pattern; pcre:"/\/click_api\/v3(?:\/|
\?|$)/i"; metadata:created_at 2026_11_18, tactic initial_access; classtype:trojan-activity; sid:9512002; rev:2;)

# 3. TacticalRMM Agent Bootstrapper Enrollment URI (/agents/install/ or tacticalagent)
alert http $HOME_NET any -> any any (msg:"ODIN-RMM TacticalRMM Agent Enrollment Bootstrap Request";
flow:established,to_server; http.uri; content:"/agents/install/"; nocase; fast_pattern; metadata:created_at
2026_11_18, tactic persistence; classtype:policy-violation; sid:9512003; rev:1;)

# 4. TacticalRMM MeshCentral WebSocket Relay Upgrade (/meshrelay.ashx)
alert http $HOME_NET any -> any any (msg:"ODIN-RMM MeshCentral WebSocket Relay Upgrade (/meshrelay.ashx)";
flow:established,to_server; http.uri; content:"/meshrelay.ashx"; nocase; fast_pattern; http.header;
content:"Upgrade: websocket"; nocase; metadata:created_at 2026_11_18, tactic command_and_control;
classtype:trojan-activity; sid:9512004; rev:1;)

# 5. FRP (frpc -> frps) Legacy or Plaintext TCP JSON Authentication Handshake (TLS disabled or pre-v0.50)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-RELAY FRP Plaintext Client JSON privilege_key Handshake";
flow:established,to_server; content:"\"privilege_key\":"; fast_pattern; content:"\"version\":"; pcre:"/
\"(timestamp|run_id)\"\s*:/"; metadata:created_at 2026_11_18, tactic command_and_control; classtype:trojan-
activity; sid:9512005; rev:3;)

# 6. FRP Server (frps) Dashboard TCP Proxy Enumeration (/api/proxy/tcp)
alert http any any -> any [7500,17500,8080,9527] (msg:"ODIN-RELAY FRP Server Dashboard TCP Proxy API Access";
flow:established,to_server; http.uri; content:"/api/proxy/tcp"; fast_pattern; metadata:created_at 2026_11_18,
tactic command_and_control; classtype:policy-violation; sid:9512006; rev:1;)

# 7. Hak5 Cloud C2 Web Controller Branding in an HTTP Response Body (branded, unmodified controller pages only)
alert http any any -> $HOME_NET any (msg:"ODIN-C2 Hak5 Cloud C2 Web Controller Branding in Response";
flow:established,from_server; file.data; content:"Hak5 Cloud C2"; fast_pattern; metadata:created_at 2026_11_18,
tactic command_and_control; classtype:trojan-activity; sid:9512007; rev:2;)

# 8. ReverseSSH Plaintext Server Identification Response Over Non-Standard C2 Relay Ports
alert tcp $EXTERNAL_NET [3232,8082,8443] -> $HOME_NET any (msg:"ODIN-RELAY ReverseSSH Plaintext Server SSH-2.0
Banner on C2 Relay Port"; flow:established,from_server; content:"SSH-2.0-"; depth:8; fast_pattern; pcre:"/
^SSH-2\.0-(?:Go|OpenSSH)/"; metadata:created_at 2026_11_18, tactic command_and_control; classtype:trojan-
activity; sid:9512008; rev:2;)
```

odin_tds_rmm_frp_staging_configs.yar

YARA

```
/*
   Odin by Brandefense - Report #12 YARA Staging & Config Suite
   Classification: TLP:CLEAR
   Scope: Detects exposed Keitaro TDS cloaking configs, TacticalRMM bootstrapper manifests,
          FRP (frpc) reverse relay TOML/INI configs, and Hak5 Cloud C2 / ReverseSSH descriptors.
```

```
*/

rule ODIN_Keitaro_TDS_Cloaking_Gate_Config
{
    meta:
        author = "Odin by Brandefense"
        report = "Monograph 12 - Keitaro TDS, TacticalRMM, and FRP Relays"
        classification = "TLP:CLEAR"
        tactic = "Initial Access"
    strings:
        $k1 = "keitaro" ascii wide nocase
        $k2 = "X-KClick-Token" ascii wide nocase
        $k3 = "click_api/v3" ascii wide nocase
        $k4 = "object=campaigns" ascii wide nocase
        $c1 = "stream_id=" ascii wide nocase
        $c2 = "302 Found" ascii wide
    condition:
        filesize < 512KB and ($k1 and ($k2 or $k3 or $k4) and ($c1 or $c2))
}

rule ODIN_TacticalRMM_Agent_Bootstrap_Manifest
{
    meta:
        author = "Odin by Brandefense"
        report = "Monograph 12 - Keitaro TDS, TacticalRMM, and FRP Relays"
        classification = "TLP:CLEAR"
        tactic = "Persistence"
    strings:
        $t1 = "/agents/install/" ascii wide nocase
        $t2 = "/meshrelay.ashx" ascii wide nocase
        $t3 = "tacticalagent" ascii wide nocase
        $s1 = "api." ascii wide nocase
        $s2 = "mesh." ascii wide nocase
        $s3 = "rmm." ascii wide nocase
    condition:
        filesize < 1MB and (2 of ($t*) and 2 of ($s*))
}

rule ODIN_FRP_Reverse_Relay_Client_Config
{
    meta:
        author = "Odin by Brandefense"
        report = "Monograph 12 - Keitaro TDS, TacticalRMM, and FRP Relays"
        classification = "TLP:CLEAR"
        tactic = "Command and Control"
    strings:
        $f1 = "serverAddr" ascii wide
        $f2 = "server_addr" ascii wide
        $p1 = "serverPort = 7000" ascii wide
        $p2 = "server_port = 7000" ascii wide
        $a1 = "auth.token" ascii wide
        $a2 = "privilege_key" ascii wide
        $x1 = "socks5" ascii wide nocase
        $x2 = "[[proxies]]" ascii wide
    condition:
        filesize < 256KB and (1 of ($f*) and 1 of ($p*) and 1 of ($a*) and 1 of ($x*))
}

rule ODIN_Hak5_CloudC2_And_ReverseSSH_Provisioning
{
    meta:
        author = "Odin by Brandefense"
        report = "Monograph 12 - Keitaro TDS, TacticalRMM, and FRP Relays"
        classification = "TLP:CLEAR"
        tactic = "Command and Control"
    strings:
        $h1 = "device.config" ascii wide
        $h2 = "CLOUDC2_" ascii wide
        $h3 = "Hak5 Cloud C2" ascii wide nocase
```

```
        $r1 = "2022" ascii wide
        $r2 = ":3232" ascii wide
    condition:
        filesize < 256KB and ((2 of ($h*) and $r1) or ($h1 and $r2))
}
```

sentinel_unapproved_rmm_and_tds_redirect_chain.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Report #12 Microsoft Sentinel & Defender XDR Hunting Query
// Classification: TLP:CLEAR
// Correlates browser network egress to TDS gates or disposable TLDs with downstream MSI/script/RMM
// process execution within 5 minutes, and performs preliminary unapproved TacticalRMM / MeshCentral
// domain hunts and outbound FRP / Hak5 / ReverseSSH relay tunnel detection (pair with Suricata sid:
9512001-9512002).

let Lookback = 14d;
let CorrelationWindow = 5m;
// Exact hostnames of your sanctioned MSP; replace the placeholders.
let ApprovedMspDomains = dynamic(["rmm.authorized-msp.example", "api.authorized-msp.example", "mesh.authorized-
msp.example"]);
let VerifiedHostileNodes = dynamic(["146.190.211.163", "77.111.101.84", "165.154.199.52"]);
let DisposableTlds = dynamic([".xyz", ".top", ".online", ".site", ".art", ".life", "duckdns.org", "sslip.io"]);
let RelayPorts = dynamic([2022, 3232, 4430, 7000, 7500, 17500]);
let BrowserProcesses = dynamic(["chrome.exe", "msedge.exe", "firefox.exe", "brave.exe", "iexplore.exe"]);
let BrowserGateClicks =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback) and ActionType == "ConnectionSuccess"
    | where InitiatingProcessFileName in~ (BrowserProcesses)
    | extend RemoteHost = tolower(tostring(parse_url(iff(RemoteUrl contains "://", RemoteUrl, strcat("https://",
RemoteUrl))).Host))
    | where RemoteIP in (VerifiedHostileNodes)  // confirmed hostile addresses are never excluded
        or (RemoteHost !in (ApprovedMspDomains) and (RemoteUrl has_any ("click_api/v3") or RemoteUrl has_any
(DisposableTlds)))
    | project DeviceName, ClickTime = Timestamp,
              GateTarget = strcat(RemoteIP, ":", tostring(RemotePort), " (", coalesce(RemoteUrl, "direct_ip"),
")");
let DownstreamInstallers =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where FileName in~ ("msiexec.exe", "powershell.exe", "pwsh.exe", "wscript.exe", "cscript.exe",
"tacticalrmm.exe", "MeshAgent.exe")
    | project DeviceName, ProcTime = Timestamp, InitiatingProcessFileName, FileName, ProcessCommandLine;
union isfuzzy=true
(
    BrowserGateClicks
    | join kind=inner (DownstreamInstallers) on DeviceName
    | where ProcTime between (ClickTime .. (ClickTime + CorrelationWindow))
    | extend Timestamp = ProcTime,
             HuntSignal = "Browser_Gate_Egress_To_Installer_Or_RMM_Chain",
             ArtifactDetail = strcat("Gate=", GateTarget, " -> ", FileName, ": ", ProcessCommandLine)
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName, ArtifactDetail
),
(
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where FileName in~ ("tacticalrmm.exe", "MeshAgent.exe", "frpc.exe", "frpc")
        or ProcessCommandLine has_any ("meshrelay.ashx", "/agents/install/", "frpc.toml", "frpc.ini",
"privilege_key", "device.config")
    | extend HuntSignal = "Unapproved_TacticalRMM_Or_FRP_Process_Execution",
             ArtifactDetail = ProcessCommandLine
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName, ArtifactDetail
),
(
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback) and ActionType == "ConnectionSuccess"
    | where RemoteIPType == "Public"
    | extend RemoteHost = tolower(tostring(parse_url(iff(RemoteUrl contains "://", RemoteUrl, strcat("https://",
RemoteUrl))).Host))
```

```
    | where RemoteIP in (VerifiedHostileNodes)  // confirmed hostile addresses are never excluded
         or (RemoteHost !in (ApprovedMspDomains) and (false
         or RemoteUrl has_any ("meshrelay.ashx", "/agents/install/")
         or ((RemoteUrl startswith "rmm." or RemoteUrl startswith "api." or RemoteUrl startswith "mesh.") and
RemoteUrl has_any (DisposableTlds))
         or (InitiatingProcessFileName in~ ("MeshAgent.exe", "tacticalrmm.exe", "frpc.exe", "frpc", "ssh.exe",
"ssh") and RemotePort in (RelayPorts))))
    | extend HuntSignal = case(
             RemoteIP in (VerifiedHostileNodes), "Verified_R12_TDS_RMM_Or_Relay_IP_Egress",
             RemoteUrl has_any ("meshrelay.ashx", "/agents/install/") or RemoteUrl has_any (DisposableTlds),
"Preliminary_Unapproved_RMM_Domain_Or_MeshRelay_Hunt",
             "Outbound_FRP_Hak5_Or_ReverseSSH_Relay_Port"
         ),
         ArtifactDetail = strcat(RemoteIP, ":", tostring(RemotePort), " (", coalesce(RemoteUrl, "raw_tcp"), ")")
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName = InitiatingProcessFileName,
ArtifactDetail
)
| summarize
    FirstSeen = min(Timestamp),
    LastSeen = max(Timestamp),
    EventCount = count(),
    SampleIndicators = make_set(ArtifactDetail, 5)
    by DeviceName, HuntSignal, InitiatingProcessFileName, FileName
| order by EventCount desc
```

sigma_tacticalrmm_frpc_unauthorized_execution.yml

SIGMA

```
title: Unapproved TacticalRMM or MeshCentral Agent Execution
id: 6d9b4f12-84c1-4e7a-9b21-120000000001
status: experimental
description: Detects installation or execution of TacticalRMM and MeshCentral agents. Suppress sanctioned MSP
agents by exact host and agent ID in the SIEM.
author: Odin by Brandefense
date: 2026-11-18
tags:
  - attack.initial_access
  - attack.persistence
  - attack.command_and_control
logsource:
  category: process_creation
  product: windows
detection:
  selection_bin:
    Image|endswith:
      - '\tacticalrmm.exe'
      - '\MeshAgent.exe'
  selection_cli:
    CommandLine|contains:
      - '/agents/install/'
      - 'meshrelay.ashx'
      - '-m install --api https://api.'
  # No substring allowlist: a command line can name an approved domain and still reach another host.
  # Suppress sanctioned MSP agents by exact host and agent ID in your SIEM instead.
  condition: selection_bin or selection_cli
falsepositives:
  - Newly onboarded MSP TacticalRMM agents prior to allowlist registration
level: high
---
title: FRP Reverse Relay Client Execution or Tunnel Multiplexing
id: 6d9b4f12-84c1-4e7a-9b21-120000000002
status: experimental
description: Detects Fast Reverse Proxy client (frpc) execution or inline TOML/INI tunnel invocation exposing
internal services or SOCKS5 pivots to external frps relays.
author: Odin by Brandefense
date: 2026-11-18
tags:
  - attack.command_and_control
logsource:
```

```
    category: process_creation
    product: windows
  detection:
    selection_img:
      Image|endswith:
        - '\frpc.exe'
    selection_cfg:
      CommandLine|contains:
        - 'frpc.toml'
        - 'frpc.ini'
        - 'frpc_kd'
        - 'privilege_key'
        - 'serverPort = 7000'
        - 'server_port = 7000'
    filter_dev_tunnel:
      ParentImage: 'C:\Program Files\ApprovedDevTunnel\runner.exe'
    condition: (selection_img or selection_cfg) and not filter_dev_tunnel
  falsepositives:
    - Explicitly sanctioned developer NAT-traversal testing hosts
  level: high
  ---
  title: Hak5 Cloud C2 or ReverseSSH Outbound Tunnel Invocation
  id: 6d9b4f12-84c1-4e7a-9b21-120000000003
  status: experimental
  description: Detects Hak5 Cloud C2 provisioning descriptors (device.config / port 2022) or static ReverseSSH
  reverse-shell tunnel flags targeting non-standard C2 ports.
  author: Odin by Brandefense
  date: 2026-11-18
  tags:
    - attack.persistence
    - attack.command_and_control
  logsource:
    category: process_creation
    product: linux
  detection:
    selection_hak5:
      CommandLine|contains:
        - '/etc/device.config'
        - 'cc-client'
    selection_revssh:
      Image|endswith:
        - '/ssh'
        - '/reversessh'
      CommandLine|contains: ' -R'
      CommandLine|re: '(?:-R\s*(?:\S+:)?(?:2022|3232|8082|8443|443):|-p\s*(?:2022|3232|8082|8443|443)\b|[@:](?:
  2022|3232|8082|8443|443)\b)'
    # No command-line substring exception: suppress sanctioned bastions by exact source host in the SIEM.
    condition: selection_hak5 or selection_revssh
  falsepositives:
    - Sanctioned physical penetration testing drop-boxes with documented change tickets
  level: high
```

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/before-the-payload-lands/
Short Read · brandefense.io/odin-research/blog/before-the-payload-lands/
Defense Kit · brandefense.io/odin-research/defense-kit/