ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 49 / 30 · ENTERPRISE EXPLOITATION

Exposed Kiosks and RMM Shares
Files, Root-Like Paths, and Relays

How five misconfigured open directories expose payment-kiosk drivers, root-like cloud Linux web paths, MSP RMM installers, and medical DICOM tools alongside 250 TacticalRMM endpoints

Two-week observation window ending 21 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

17,255
Combined files reported or listed across five owner shares (925 sampled entries, 582 unique paths)

5 + 0
Misconfigured owner hosts (Host A to Host E, 0 published IPs) with 0 overlap against 250 TacticalRMM rows

25
Static Linux DCMTK 3.6.9 medical imaging binaries exposed on an unauthenticated HTTP listener (Host E)

0
Published indicators of compromise

What Is in This Report. 10 chapters and two appendices.

How five misconfigured open directories expose payment-kiosk drivers, root-like cloud Linux web paths, MSP RMM installers, and medical DICOM tools alongside 250 TacticalRMM endpoints

01	Executive Summary	04
02	Five Open Directories and 250 TacticalRMM Endpoints	07
03	Exposed Payment Kiosks and Root-Like Web Paths	10
04	Exposed MSP RMM Shares and Medical DICOM Binaries	14
05	Separating Lure-Labeled TacticalRMM Candidates From Standard MSP Servers	18
06	What Defenders Should Do	22
07	Detection Rules	24
08	Indicators	27
09	Scope and Limits	29
10	Sources	31
A	Indicators of compromise (0)	33
B	Detection rules (4 files)	34

IN SHORT

In a two-week observation window ending 21 November 2026, Odin by Brandefense observed five misconfigured open web directories reporting 17,255 files alongside 250 internet-wide TacticalRMM endpoints. All five directories belong to misconfigured owners or MSP administrators with zero cross-host links. They expose payment-kiosk card-reader drivers, paths resembling a Linux root tree, organization-named NinjaOne and Action1 installers, and medical DICOM binaries. Two TacticalRMM endpoints carry webmail-lure certificate labels, but their abuse remains unconfirmed. Close open web shares, disable FollowSymLinks, gate RMM installers, and require behavioral evidence before blocking.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 21 November 2026, Odin by Brandefense observed five misconfigured open web directories reporting 17,255 files alongside 250 internet-wide TacticalRMM endpoints. All five directories belong to misconfigured owners or MSP administrators with zero cross-host links. They expose payment-kiosk card-reader drivers, paths resembling a Linux root tree, organization-named NinjaOne and Action1 installers, and medical DICOM binaries. Two TacticalRMM endpoints carry webmail-lure certificate labels, but their abuse remains unconfirmed. Close open web shares, disable FollowSymLinks, gate RMM installers, and require behavioral evidence before blocking.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Payment kiosks, cloud virtual machines, healthcare gateways, and MSP shares hold sensitive drivers, system files, and RMM installers. Leaving directory indexing open or exposing a root-like path inside a web root makes those files readable over HTTP. We reviewed directory metadata statically, installed zero packages, and contacted zero consoles. We withheld all five owner addresses (`Host A` through `Host E`), all file hashes, and all 250 TacticalRMM endpoints (248 hosts).

1. **Open kiosk and cloud directories expose hardware drivers and root-like paths.**
   One dual-listener server (`Host A`) exposes 180 payment-kiosk entries, including `.NET` debug symbols, motorized smart-card and RFID libraries, 134 invoice logs, and camera JPEGs. In Canada, an Apache server (`Host B`) lists 10,000 reported paths resembling Linux root files under a symlink-named web path, including a cloud guest-agent binary and TLS material.

2. **Open MSP shares expose organization-named RMM installers and a 20.4 GB backup ISO.**
   Two United States web shares (`Host C` reporting 684 files and `Host D` reporting 6,366 files) expose eight `NinjaOne` `.msi` installers and one mirrored `Action1` `.msi` installer. `Host C` also lists a 20.40 GB `Veeam 13.0.1` backup ISO. If those RMM packages contain reusable enrollment credentials and the console allows automatic enrollment, an outside party could register an unapproved agent.

3. **Two of 250 TacticalRMM endpoints carry webmail-lure certificate labels without confirmed abuse.**
   Although 117 of 250 examined TacticalRMM endpoints sit on commercial cloud VPS providers, 115 use standard custom-domain TLS certificates consistent with normal MSP deployments. Two cloud VPS endpoints (0.80%) have webmail-lure certificate labels in the source register. Their abuse remains unconfirmed; withhold both addresses until independent protocol or behavioral evidence supports blocking.

Three Decisions for Leaders

1. **Move MSP RMM installers behind authenticated portals and rotate any reusable tokens.** Delete organization-named `NinjaOne`, `Action1`, and remote-support `.msi` files from public HTTP or FTP folders. If a package carries a reusable tenant token, rotate it and require manual console approval for new agent registrations.
2. **Disable web symbolic-link traversal and isolate kiosk and medical shares.** Set `Options -Indexes -FollowSymLinks -SymLinksIfOwnerMatch` on Apache and `disable_symlinks on;` on Nginx, and verify that zero symbolic links inside `DocumentRoot` point outside the web root. Restrict the payment-kiosk listeners and close the unauthenticated HTTP directory serving `DCMTK` binaries.
3. **Require independent behavioral evidence before blocking dual-use RMM infrastructure.** Keep the two webmail-lure TacticalRMM endpoints and the 115 custom-domain cloud RMM servers on review watchlists until protocol or endpoint telemetry confirms abuse. Monitor cloud RMM activity through endpoint `msiexec` logs rather than single-signal IP blocklists.

The Study in Numbers

Number	What it is
17,255	Combined files reported or listed across five owner shares (925 sampled entries, 582 unique paths)
5 + 0	Misconfigured owner hosts (`Host A` to `Host E`, 0 published IPs) with 0 overlap against 250 TacticalRMM rows
180 & 10,000	Payment-kiosk entries across 4 sub-trees (`Host A`) and root-like web paths reported on `Host B` (`CA`)
9 + 20.40 GB	Eight `NinjaOne` and one organization-named `Action1` `.msi` files, plus a 20.40 GB `Veeam 13.0.1` ISO
25	Static Linux `DCMTK 3.6.9` medical imaging binaries exposed on an unauthenticated HTTP listener (`Host E`)
39,887 / 250	Global TacticalRMM sightings across 119 countries (340 feed-verified) and 250 examined endpoints (248 hosts)
2 (0.80%) / 0	Webmail-lure TacticalRMM endpoints (abuse unconfirmed) and 0 published blocklist IPs or hashes in Appendix A

How to use this report.

Leaders and MSP directors can start with Chapters 1, 5, and 6. Cloud, point-of-sale, healthcare, and IT platform engineers should review Chapters 3 and 4, then run the checklist in Chapter 6. SOC analysts and threat hunters should go to Chapters 5, 7, and 8, plus Appendix B and Appendix A. Attribution boundaries and limits sit in Chapter 9.

CHAPTER 02

Five Open Directories and 250 TacticalRMM Endpoints

IN SHORT

Five open web directories listed 17,255 files (925 sampled entries and 582 unique paths across 11 slices) in the two-week window ending 21 November 2026. Paired with 250 TacticalRMM endpoints (248 hosts, 0 shared hosts), they show how accidental owner exposure differs from unconfirmed dual-use RMM candidates. Audit your own perimeter for open shares and require behavioral evidence before blocking RMM endpoints.

INSIDE THIS CHAPTER

Five misconfigured owner and MSP shares (`Host A` through `Host E`) 07

Connecting exposed MSP shares to internet-wide TacticalRMM observations 08

02 Five Open Directories and 250 TacticalRMM Endpoints

Treating every open directory or dual-use RMM server as hostile disrupts legitimate MSPs, clinics, and retail operators. Ignoring world-readable shares that defenders can find through external attack surface management leaves RMM installers, debug symbols, and root-like Linux paths exposed (`T1190`, `T1219`, `T1552.001`).

We grouped the five open directories (`Host A` through `Host E`) as an analytical five-surface defensive model alongside a 250-endpoint TacticalRMM comparison. Nothing links the five open-directory servers to one another (0 shared IPs, certificates, or tenant IDs). In addition, 0 hosts overlap between the five shares and the 250 TacticalRMM rows.

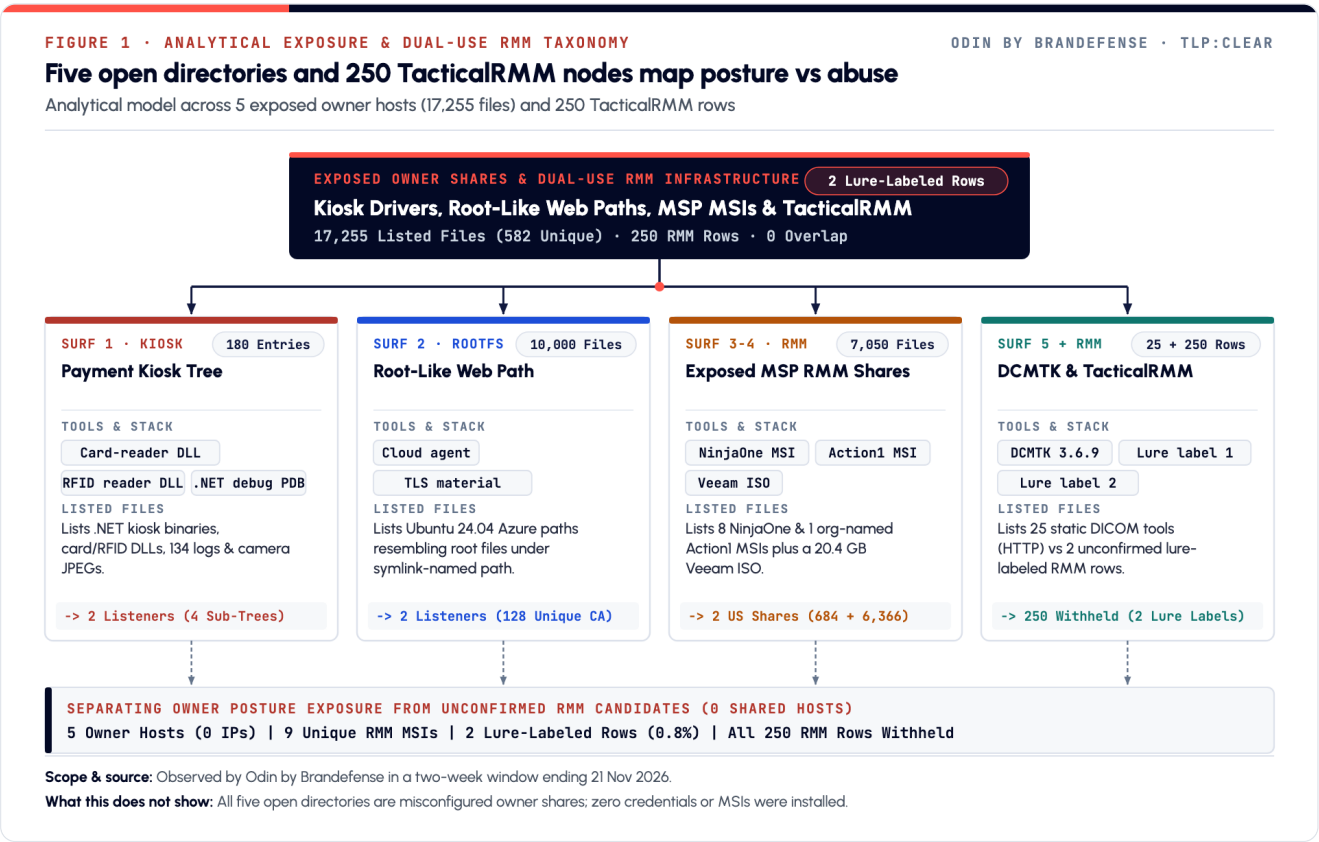


Figure 1: Five open directories and 250 TacticalRMM nodes map posture vs abuse

Five misconfigured owner and MSP shares (`Host A` through `Host E`)

Across 11 directory slices, the five hosts list 17,255 combined per-host files, yielding 925 sampled rows and 582 unique paths (568 sized plus 14 unsized entries on `Host E`). Every server reflects an unattended kiosk, cloud virtual machine, MSP/IT share, or medical utility folder left open over HTTP rather than adversary infrastructure.

The directory listings do not establish defects in the named software or hardware libraries. Those products include `NinjaOne`, `Action1`, `Veeam`, `Splashtop`, `Datto RMM`, `SonicWALL`, `Cisco`, `Apache`, `Nginx`, `Microsoft WALinuxAgent`, and `OFFIS DCMTK`. The listings show public HTTP exposure; Odin did not verify the web-server directives, symlink construction, or folder permissions.

Host alias	Listeners & country	Slices	Listed / unique	Sampled size	Key exposed operational files
`Host A` (kiosk)	Two listeners	4	180 / 180	10,128,354 B (10.13 MB)	`.NET` kiosk binaries, `.pdb` debug symbols, card-reader and RFID DLLs, 134 invoice logs, 3 camera JPEGs
`Host B` (root-like path)	Two listeners (`CA`)	2	10,000 / 128	133,399,463 B (133.40 MB)	Cloud guest agent, TLS material, Python library files, and cloud Linux kernel images under a root-like web path
`Host C` (MSP share)	Two listeners (`US`)	2	684 / 120	141,992,037,486 B (141.99 GB)	8 `NinjaOne` `.msi` packages (6 at 72.35 MB) and a `Veeam 13.0.1` backup ISO (20.40 GB)
`Host D` (Action1 FTP)	Two listeners (`US`)	2	6,366 / 129	3,187,066,013 B (3.19 GB)	Mirrored `Action1` `.msi` (6.65 MB, 3 paths), Cisco VPN predeploy `.zip`, 43 ARM SBC `.xz` images
`Host E` (DCMTK tools)	One HTTP listener	1	25 / 25	54,099,776 B (11 sized)	Static Linux `DCMTK 3.6.9` binaries (image codec tools, clinical document converters, and DICOM network utilities)

Connecting exposed MSP shares to internet-wide TacticalRMM observations

`Host C` and `Host D` show how legitimate RMM administration packages leak when organization-named `.msi` installers sit in public web folders. Meanwhile, threat actors deploy self-hosted `TacticalRMM` servers on rented cloud VPS instances for post-intrusion access (`T1219`).

In the two-week window ending 21 November 2026, `TacticalRMM` (`management` category) generated 39,887 global sightings across 119 countries (340 feed-verified). We reviewed 250 `confirmed`-status endpoints across 248 hosts (0 overlap with `Host A` through `Host E`). The results show why defenders using cyber threat intelligence must pair hosting type with X.509 certificate themes before blocking dual-use RMM servers.

Study population	Scope	Examined rows	Hosts	Published IPs	Withheld rows	Action
Five open shares (`Host A` to `Host E`)	17,255 files	925 (582 unique)	5	0	5 hosts (100%)	Self-audit & gate installers
Webmail-lure TacticalRMM candidates	(39,887 global)	2 (0.80%)	2	0	2 (100%)	Withheld; review before blocking
Dual-use cloud VPS TacticalRMMs	(340 verified)	115 (46.00%)	115	0	115 (100%)	Hunt via `msiexec` logs
Regional & MSP hosting candidates	(119 countries)	111 (44.40%)	110	0	111 (100%)	Watchlist only
Subscriber & mail collisions	(ISP / CDN)	22 (8.80%)	21	0	22 (100%)	Do not block

CHAPTER 03

Exposed Payment Kiosks and Root-Like Web Paths

IN SHORT

Unprotected maintenance listeners on physical payment terminals and root-like web paths on cloud Linux servers expose hardware command libraries, debug symbols, and system files. `Host A` exposes 180 kiosk entries across two listeners, including `.NET` debug symbols, card-reader and RFID DLLs, 134 invoice logs, and camera JPEGs. In Canada, `Host B` reports 10,000 paths resembling Linux root files under a root-like web path. Isolate kiosk listeners and disable `FollowSymLinks`.

INSIDE THIS CHAPTER

Motorized card-reader drivers, `.pdb` symbols, and invoice logs on `Host A` 10

Root-like web path exposure on a Canada cloud VM (`Host B`) 11

03 Exposed Payment Kiosks and Root-Like Web Paths

Cyber-physical terminals and cloud virtual machines rarely trigger CVE-only vulnerability scans when misconfigured. However, open HTTP directories on these assets expose peripheral drivers and OS file paths (`T1190`, `T1552.001`).



Figure 4: Open directories expose kiosk drivers, root-like paths, and MSP MSIs

Motorized card-reader drivers, `.pdb` symbols, and invoice logs on `Host A`

`Host A` (address and ports withheld) exposes four sub-trees across a primary HTTP listener (177 entries) and an HTTPS listener (3 entries). Together they total 180 unique sized paths (10,128,354 B / 10.13 MB, observed on 21 November 2026). Its four Spanish-language application, utility, invoice-log, and camera folders belong to an unattended payment and invoicing kiosk.

One kiosk application sub-tree lists 11 entries totaling 396,501 B, including a .NET client and debug host. The client measures 187,904 B and the debug host measures 22,696 B. The folder also lists five XML and application configuration files (3,128 B, 1,163 B, 835 B, 490 B, and 34 B) and a 27 B shutdown batch script.

Beside them sits a `.NET` debug-symbol file (106,496 B) whose contents Odin did not inspect. The directory also serves two Windows DLLs (40,960 B and 32,768 B) for motorized smart-card readers and dispensers.

A second primary-listener sub-tree lists 32 entries totaling 9,434,398 B. It exposes the main kiosk executable (238,648 B), a companion Java archive (212,536 B), and a reset archive (7,818 B). It pairs those binaries with two contactless RFID reader and communications DLLs (307,712 B and 257,024 B). Nine Java archives in a library subfolder map the peripheral stack and cover JNA, media, JDBC, webcam, barcode, and serial support.

Beside those libraries sit two printer and application configuration files (984 B and 88 B) and three batch scripts (64 B, 64 B, and 24 B). The folder also lists 13 legacy log files dated 2020-3-10 to 2022-11-9 on disk (33 B to 1,237 B).

The third primary-listener sub-tree exposes 134 electronic invoice monitor logs (7,508 B total, 32 B to 456 B). Those files span 131 calendar dates on disk from 2024-6-22 to 2025-1-8. They consist of 131 daily log files, two configuration logs (270 B and 161 B), and one error log dated 2024-7-2 (116 B).

On the HTTPS listener, a fourth sub-tree (3 entries, 289,947 B) serves three kiosk camera JPEG captures (156,672 B, 133,120 B, and 155 B). All 2020 to 2025 log dates are local file dates on disk, not Odin's observation period.

Root-like web path exposure on a Canada cloud VM (`Host B`)

In Canada (`CA`), `Host B` (address and ports withheld) serves an Apache tree across two web listeners, reporting 10,000 files per listener on 20 November 2026. The directory record carries an initial discovery date of 9 August 2026.

We sampled 240 rows, or 120 per listener, and found 128 unique sized paths. They total 133,399,463 B (133.40 MB), with file sizes from 72 B to 49,386,400 B. The listeners share 112 paths; each has eight listener-specific paths.

The sampled paths resemble Linux root files under a symlink-named web path on an Ubuntu 24.04 Azure VM; Odin did not verify the link target (`CWE-59`, `T1190`, `T1552.001`). Odin also did not inspect the Apache configuration or establish how the path tree was created:

- **System library subtree under the root-like web path (92 unique paths).** The listing includes TLS material, six Python files, and 11 Ubuntu Pro scripts. The TLS bundle measures 180,744 B, the Python 3.12 module measures 1,984 B, and a hardware database binary measures 12,292,121 B. The subtree also lists 62 shared libraries, including 433,152 B TLS and 1,258,291 B NSS files.
- **System configuration subtree under the root-like web path (22 unique paths).** The listing includes cloud-init shell profile scripts, service init scripts, runlevel links, a kernel-module configuration file, and a Python startup customization script.
- **Runtime binary subtrees under the root-like web path (10 unique paths).** The listing includes Python 3.12 (8,020,928 B), PHP 8.3 (5,833,168 B), text-editor (4,130,640 B), Perl `5.38.2` (4,023,408 B), and dynamic-linker (236,616 B) binaries.
- **Boot and system-administration subtrees under the root-like web path (4 unique paths).** The listing includes an initial ramdisk (49,386,400 B), an Azure Linux kernel (16,777,216 B), a kernel symbol map (10,380,902 B), and the Azure Guest Agent (252,384 B).

Security tests often use a symlink folder name when checking link-following flaws. Because 0 webshells or implants sit in the 128 sampled paths, directory metadata cannot separate an uncleaned owner test from an earlier upload check. We therefore withhold `Host B`'s address.

Host & listener	Sub-tree or root group	Unique paths	Size range (`B`)	Key exposed files	Posture risk
`Host A` (primary listener)	Kiosk terminal suite sub-tree	11	27 to 187,904	`.NET` client (187,904 B), `.NET` debug symbols (106,496 B), two motorized card-reader DLLs (40,960 B and 32,768 B)	`.NET` symbol file & card-dispenser DLL exposure
`Host A` (primary listener)	Payment kiosk application sub-tree	32	24 to 2,681,931	Main kiosk executable (238,648 B), two RFID reader and communications DLLs (307,712 B and 257,024 B), 9 Java archives	RFID protocol mapping, JDBC recon & 13 (2020 to 2022) logs
`Host A` (primary listener)	Electronic invoice log sub-tree	134	32 to 456	131 daily log files (2024-6-22 to 2025-1-8 file dates), 2 config logs, 1 error log	Electronic invoicing activity & config disclosure
`Host A` (HTTPS listener)	Kiosk camera capture sub-tree	3	155 to 156,672	Three kiosk camera JPEG captures (156,672 B, 133,120 B, and 155 B)	Privacy leak from physical kiosk camera captures
`Host B` (two listeners)	Boot & system-binary subtrees (`CA`)	4	252,384 to 49,386,400	Cloud guest agent (252,384 B), initial ramdisk (49.39 MB), cloud Linux kernel image, and kernel symbol map	Azure Guest Agent read, ramdisk & kernel symbols
`Host B` (two listeners)	System library & config subtrees (`CA`)	114	72 to 12,292,121	TLS material (180,744 B), six Python 3.12 files (1,984 B), 11 Ubuntu Pro scripts, 62 shared libraries	Root-like config & TLS bundle disclosure

CHAPTER 04

Exposed MSP RMM Shares and Medical DICOM Binaries

IN SHORT

Staging organization-named MSP RMM `.msi` installers on world-readable HTTP or FTP servers exposes client deployment packages alongside backup media and virtual disks. Two US shares (`Host C` with 684 files and `Host D` with 6,366 files) expose eight `NinjaOne` `.msi` files, one mirrored `Action1` `.msi` file, and a 20.40 GB `Veeam` ISO. `Host E` exposes 25 static `DCMTK` tools over HTTP. Gate RMM shares and rotate any reusable tokens.

INSIDE THIS CHAPTER

Organization-named `NinjaOne` MSIs and a 20.40 GB `Veeam` ISO on `Host C` (`US`) 14

Mirrored `Action1` RMM installer and embedded Linux archives on `Host D` (`US`) 15

Static medical imaging `DCMTK` binary directory on `Host E` 16

04 Exposed MSP RMM Shares and Medical DICOM Binaries

MSPs and corporate IT teams generate `.msi` packages from cloud RMM portals (`NinjaOne`, `Action1`, `Datto RMM`, `Splashtop`) for endpoint onboarding (`T1219`, `T1552.001`). Leaving client-named `.msi` shares on open HTTP or FTP directories exposes those installers to external visitors.

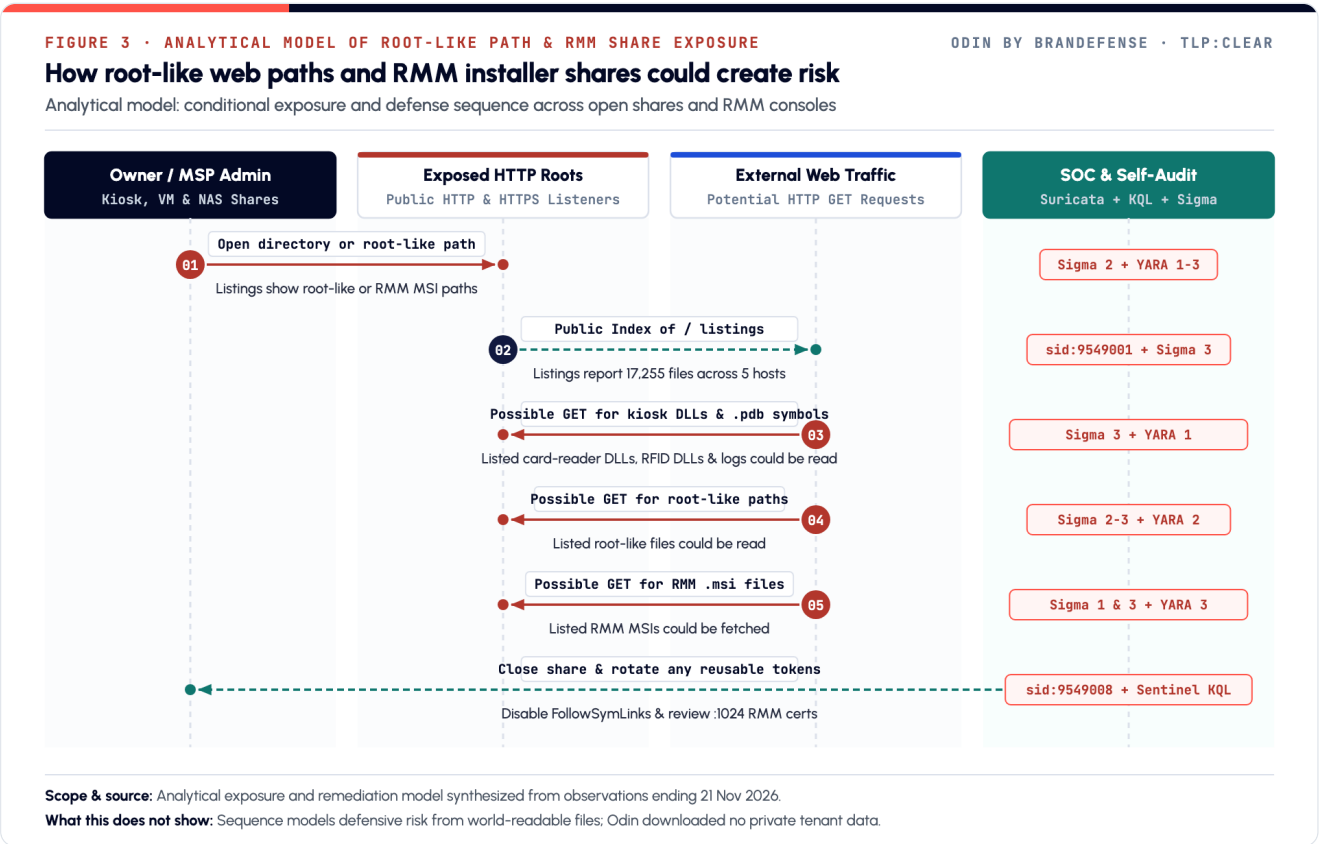


Figure 3: How root-like web paths and RMM installer shares could create risk

Organization-named `NinjaOne` MSIs and a 20.40 GB `Veeam` ISO on `Host C` (US)

In the United States, `Host C` (address and ports withheld) serves identical public directory trees over two Apache listeners. Each listener reported 684 files on 20 November 2026 (record discovery date 11 August 2026), and NAS indexing metadata indicates a NAS-backed share. Across 120 unique paths (141,992,037,486 B / 141.99 GB), `Host C` exposes 66 `.exe` installers, 20 `.msi` packages, 14 scripts, 6 `.iso` images, and 2 `.vhdx` disks:

- **Six 72,351,744 B (72.35 MB) client-folder `NinjaOne` MSIs.** Six client subfolders (tenant names withheld) each expose a 72,351,744 B 64-bit `NinjaOne` agent `.msi` installer under a client-office path.
- **Two 51,380,224 B (51.38 MB) repair MSIs and six scripts.** Repair and removal subfolders expose two 51,380,224 B `NinjaRMM` `.msi` files. Beside them sit six PowerShell and shell cleanup scripts (14,338 B, 9,059 B, 6,656 B, 1,262 B, 983 B, and 91 B). The folders also list a 209.72 MB network management installer and a 35.65 MB remote-control installer.
- **Backup ISOs, Hyper-V virtual disks, and VPN installers (141.99 GB).** Co-hosted folders expose a 20,401,094,656 B (20.40 GB) `Veeam 13.0.1.1071` backup ISO and two Hyper-V Windows `.vhdx` virtual disks (48.32 GB and 20.40 GB). Adjacent folders serve a `Splashtop Streamer` binary, `Datto RMM` uninstallers, four `DNSFilter` `.msi` packages (2.00 MB to 15.61 MB), and two `SonicWALL NetExtender` `.msi` files. They also list an

`OpenVPN Connect` `.msi` (71.30 MB), a password-recovery `.msi` (285.21 MB), and a SQL backup script `.zip` archive.

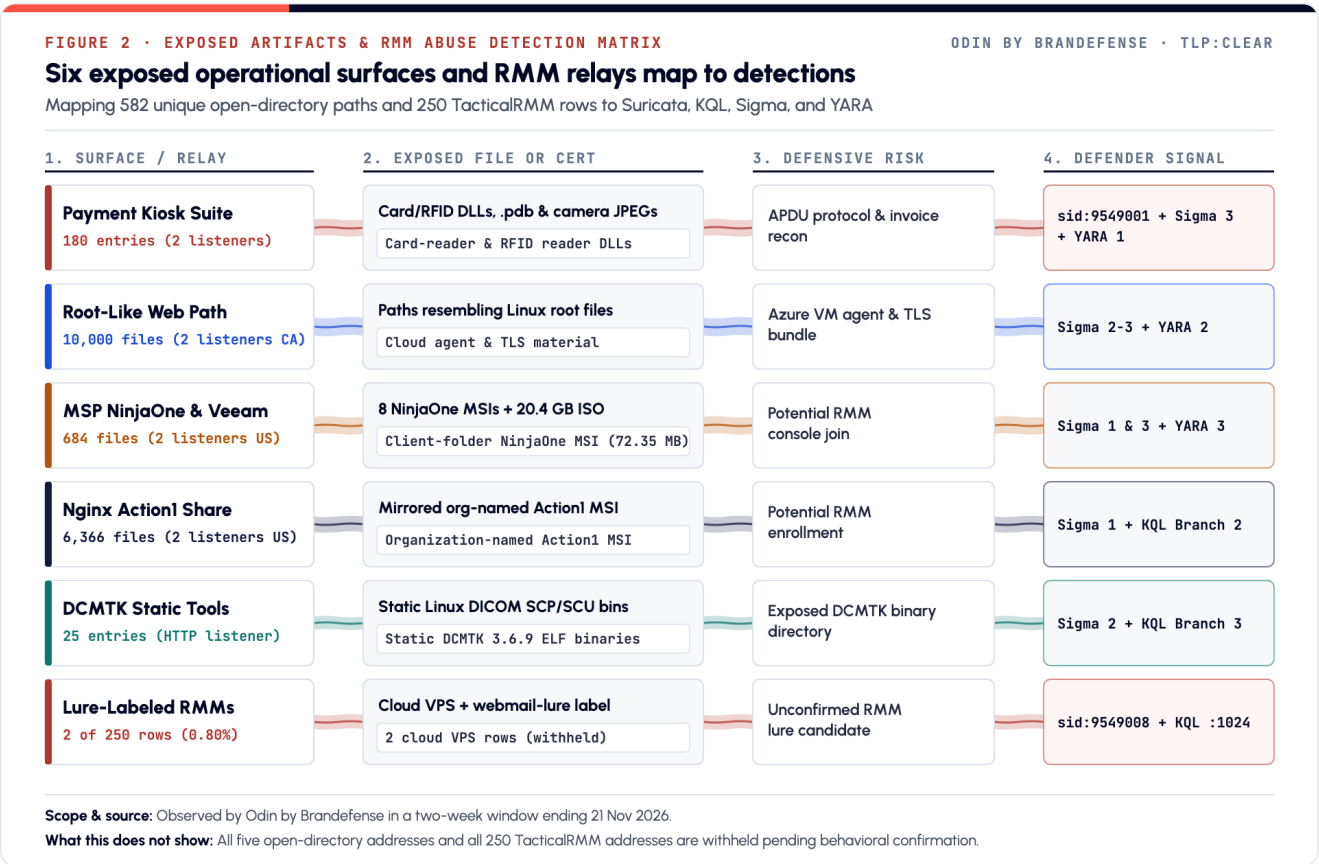


Figure 2: Six exposed operational surfaces and RMM relays map to detections

Why world-readable MSP RMM installers create risk.

The exposed `NinjaOne` and `Action1` `.msi` paths carry client folder or organization names, though Odin did not inspect the packages or verify tenant parameters (`T1552.001`, `T1219`). If the packages contain reusable enrollment credentials and the console allows automatic enrollment, an outside party could register an unapproved agent. Odin did not test either condition. Co-hosted folders also reveal client names, `DNSFilter` agents, `SonicWALL` and `OpenVPN` clients, and `Veeam 13.0.1.1071` backup media.

Mirrored `Action1` RMM installer and embedded Linux archives on `Host D` (`US`)

In the United States, `Host D` (address and ports withheld) serves Nginx directory listings across two web listeners. Each listener reported 6,366 files on 20 November 2026, with an initial record discovery date of 12 August 2026. We sampled 240 rows (120 per listener) and found 129 unique sized paths. They total 3,187,066,013 B (3.19 GB), with file sizes from 6 B to 158,902,046 B.

Most of `Host D` serves embedded ARM single-board computer archives. These include 43 `.xz` rootfs and USB images (21.46 MB to 25.68 MB, dated 2022 to `July 2026`) and 15 `.sh` Yocto/Poky toolchains (up to 158.90 MB). Beside 4 Debian 12/13 software bill-of-materials manifests and 15 C-language Modbus utilities, administrators staged internal IT packages under mirrored HTTP and FTP subfolders:

- **Organization-named `Action1` RMM `.msi` (6,647,808 B).** An organization-named `Action1` agent `.msi` installer (6.65 MB, organization name withheld) sits across three mirrored HTTP and FTP paths. The filename

contains an organization name. Odin did not inspect the package or test whether the name affects console enrollment.

- **VPN predeploy bundle and customer test file.** Alongside the `Action1 .msi`, a sibling subfolder exposes a 135,925,569 B (135.93 MB) Cisco Windows VPN predeploy `.zip` archive. A neighboring customer subfolder exposes a 6 B test text file mirrored across the HTTP and FTP directories.

Static medical imaging `DCMTK` binary directory on `Host E`

`Host E` (address and port withheld) exposes a static Linux `DCMTK 3.6.9` binary directory over an unauthenticated HTTP listener (observed on 21 November 2026). The directory lists 25 entries (24 extensionless Linux ELF paths plus 1 partial download file). Eleven sized static `x86_64` executables total 54,099,776 B (54.10 MB, 2,105,432 B to 8,158,056 B), alongside 14 unsized binary entries.

Exposed utilities include three clinical document and structured-report converters (3,762,760 B, 3,762,760 B, and one unsized XML converter). Diagnostic image codec binaries include three compression and rendering tools (8,158,056 B, 7,125,608 B, and 6,716,008 B). The folder also lists a decompression tool (6,703,720 B) and a 4,980,736 B image-scaling binary. Smaller codec and display helpers measure 4,282,952 B, 3,795,528 B, 2,706,216 B, and 2,105,432 B.

The 14 unsized entries include DICOM network storage, query-retrieve, and print SCP/SCU utilities. Zero patient DICOM studies sit in the folder, yet an open HTTP binary directory flags an unhardened medical-imaging integration host.

Host & listener	Exposed directory group	Unique paths	Size (`B`)	Representative packages or binaries	Posture risk
`Host C` (two listeners, `US`)	RMM client subfolders (6 tenants)	11	213 to 209,715,200	6 client-folder `NinjaOne .msi` (72,351,744 B) and 2 management `.exe` installers	Potential unapproved agent registration if credentials remain active
`Host C` (two listeners, `US`)	RMM repair and removal subfolders	9	91 to 51,380,224	2 repair `NinjaRMM .msi` (51,380,224 B) and 6 cleanup scripts (91 B to 14,338 B)	Repair MSI reuse & removal script study
`Host C` (two listeners, `US`)	Backup, virtual-disk, and support folders	100	0 to 48,318,382,080	`Veeam 13.0.1` backup ISO (20.40 GB) and 2 Hyper-V `.vhdx` virtual disks (48.32 GB & 20.40 GB)	Base VM inspection (68.72 GB VHDXs) & stack recon
`Host D` (two listeners, `US`)	Mirrored HTTP and FTP IT subfolders	9	6 to 135,925,569	Organization-named `Action1 .msi` (6,647,808 B, 3 paths) and Cisco VPN `.zip` (135.93 MB)	Potential unapproved `Action1` enrollment if credentials are active & VPN bundle leak
`Host D` (two listeners, `US`)	Embedded ARM SBC & Modbus folders	120	44 to 158,902,046	43 `.xz` SBC images, 15 `.sh` Poky toolchains, 4 SBOM manifests, 15 C Modbus tools	Engineering mirror mixed with internal IT MSIs
`Host E` (HTTP listener)	Static Linux `DCMTK 3.6.9` binary folder	25	2,105,432 to 8,158,056 (11 sized)	Image codec binaries (8.16 MB and 7.13 MB), document converters (3.76 MB), and DICOM network tools	Unauthenticated HTTP directory serving DCMTK binaries

05

CHAPTER 05

Separating Lure-Labeled TacticalRMM Candidates From Standard MSP Servers

IN SHORT

Global TacticalRMM observations total 39,887 sightings across 119 countries (340 feed-verified), making single-signal IP blocking unsafe for defenders. Across 250 examined `confirmed`-status endpoints (248 hosts, 0 overlap with `Host A` to `Host E`), 117 sit on commercial cloud VPS providers. Two endpoints (0.80%) carry webmail-lure certificate labels in the source register, but their abuse remains unconfirmed. Withhold all 250 addresses and hunt RMM usage through behavioral telemetry.

INSIDE THIS CHAPTER

Why cloud VPS hosting alone does not make a TacticalRMM server malicious 18

Regional MSP candidates and telecom or mail-port collisions 19

05 Separating Lure-Labeled TacticalRMM Candidates From Standard MSP Servers

Self-hosted `TacticalRMM` combines a Django administration API, a MeshCentral remote relay, and signed Windows and Linux agents. That architecture makes the tool popular both with legitimate MSPs and with threat actors seeking persistent C2 (`T1219`).

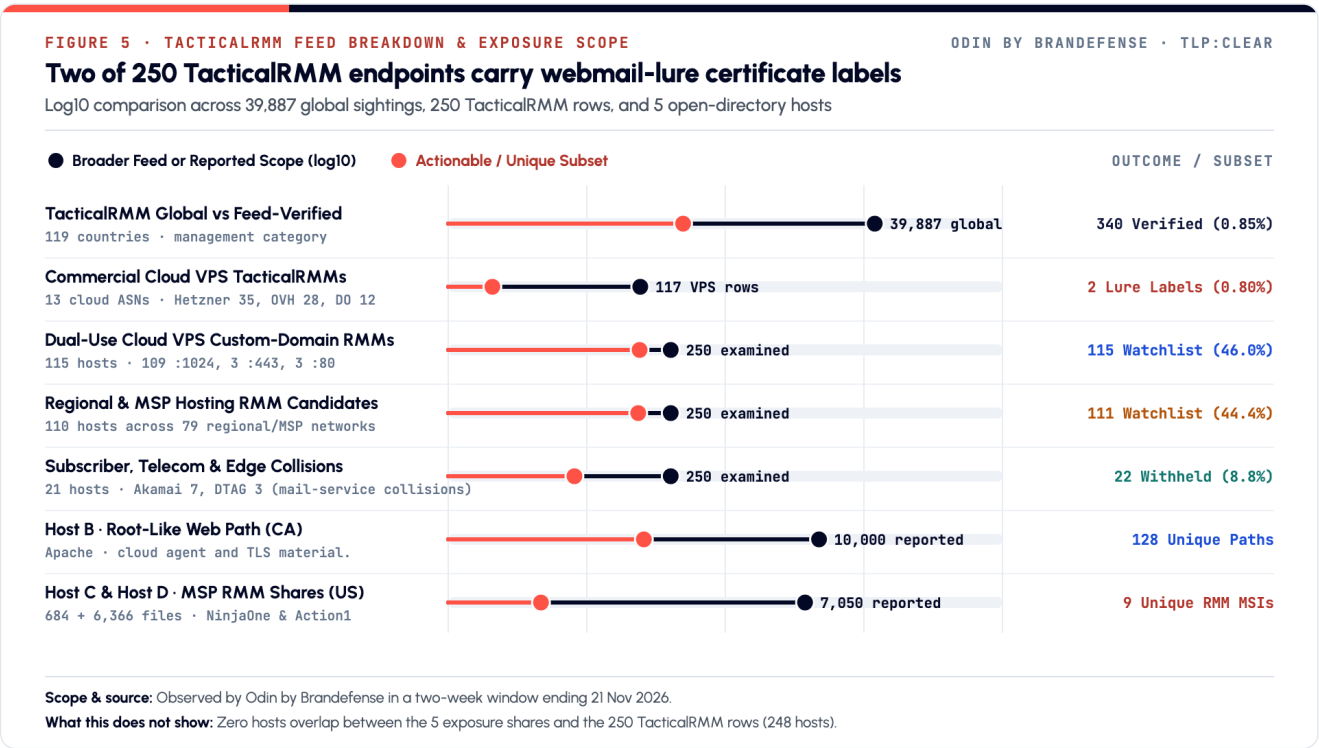


Figure 5: Two of 250 TacticalRMM endpoints carry webmail-lure certificate labels

Why cloud VPS hosting alone does not make a TacticalRMM server malicious

All 250 comparative TacticalRMM endpoints (248 distinct hosts observed from 13 to 19 November 2026) carried an upstream `confirmed` service status. Port 1024 accounts for 227 rows (90.80%), followed by port 80 (14, 5.60%) and port 443 (3, 1.20%). Six ports (587, 800, 993, 8000, 8080, and 8088) carry 1 row each (0.40%).

Leading countries in the sample are the United States (57), Germany (57), Brazil (45), France (23), and the Netherlands (11). Canada (8), Finland (8), the United Kingdom (7), and 21 other countries (34 rows) account for the rest.

Within that sample, 117 endpoints (46.80%, 117 hosts) sit on 13 commercial cloud and VPS providers. Leading networks include `Hetzner Online GmbH` (35), `OVH SAS` (28), `Hostinger` (16), `DigitalOcean` (12), and `Contabo GmbH` (11). Smaller cloud shares appear on `Amazon.com, Inc.` (4), `Contabo Inc.` (3), `Microsoft` (2), `Contabo Asia` (2), and four single-row providers (`Kamatera` , `LeaseWeb` , `M247` , and `IONOS SE`).

Blocking all 117 cloud VPS hosts would disrupt legitimate IT teams. Amidaware's official `TacticalRMM` documentation directs MSPs to deploy on Hetzner, DigitalOcean, Vultr, OVH, AWS, or Azure with custom DNS certificates. Checking X.509 certificate themes splits those 117 cloud VPS rows into two groups:

- **Two unconfirmed cloud VPS endpoints with webmail-lure certificate labels (0.80% of 250).** Two cloud VPS endpoints (addresses and ports withheld, observed 13 November 2026) carry webmail-lure certificate labels in the source register. Because the records hold no raw certificate, protocol response, beacon, or behavior log, their abuse remains unconfirmed and both addresses are withheld.
- **One hundred fifteen dual-use cloud VPS servers with custom domains (46.00% of 250).** The other 115 commercial VPS hosts (109 on :1024, 3 on :443, and 3 on :80) use standard custom-domain TLS certificates with zero phishing lure themes, so all 115 addresses are withheld on a watchlist.

Regional MSP candidates and telecom or mail-port collisions

The remaining 133 TacticalRMM rows (131 distinct hosts, 0 network overlap with the 13 cloud VPS providers) fall into two non-blocking groups. Defenders should keep these addresses off perimeter IP blocklists:

- **One hundred eleven regional and MSP hosting candidates (44.40%, 110 hosts).** These rows span 79 regional networks, led by `netcup GmbH` (6), `Locaweb` (5), `Brasil Site Informatica` (5), and `Telefonica Brasil` (4, including 1 dual-port host). Three rows each sit on `HostPapa`, `Scaleway`, `EVEO`, and `Constant Company`, while top countries are Brazil (28), the US (25), Germany (15), and the Netherlands (10). One hundred rows use :1024, seven use :80, and four use :800/:8000/:8080/:8088 (110 custom-domain CNs, 1 empty CN; addresses withheld).
- **Twenty-two subscriber, telecom, and CDN collisions (8.80%, 21 hosts).** These rows sit on 14 broadband, telecom, and edge networks (`Akamai Technologies, Inc.` 7, `Deutsche Telekom AG` 3, `Verizon Business` 1, `Vodafone Portugal` 1, `CLARO S.A.` 1, and 9 regional ISPs). One telecom host matched on mail-service ports. That match shows how mail-port TLS banners on ISP lines collide with service signatures (addresses withheld).

TacticalRMM group	Rows (250)	Share	Hosts (248)	Certificate theme	Ports	Action
Unconfirmed webmail-lure candidates	2	0.80%	2	Webmail-lure certificate label	Withheld (2)	Withheld; review before blocking
Dual-use cloud VPS servers	115	46.00%	115	Custom-domain CN (115)	:1024 (109), :443 (3), :80 (3)	Watchlist; correlate `msiexec`
Regional & MSP candidates	111	44.40%	110	Custom-domain (110), empty (1)	:1024 (100), :80 (7), 4 other	Watchlist; withheld
Subscriber & mail collisions	22	8.80%	21	Custom-domain CN (22)	:1024 (16), :80 (4), 2 mail ports	Do not block; withheld

Commercial cloud / VPS provider	Cloud rows (117)	Lure-labeled (unconfirmed)	Dual-use watchlist	Countries in sample
Hetzner Online GmbH	35	1 (withheld)	34	DE (26), FI (7), US (2)
OVH SAS	28	0	28	FR (16), CA (5), GB (4), DE / PL / SG (3)
Hostinger International Limited	16	0	16	BR (8), US (5), FR / GB / LT (3)
DigitalOcean, LLC	12	0	12	US (6), DE (3), BR / GB / SG (3)
Contabo GmbH	11	0	11	DE (7), BR (4)
Amazon.com, Inc.	4	0	4	US (4)
Contabo Inc.	3	1 (withheld)	2	US (3)
Microsoft Corporation & Contabo Asia	4	0	4 (2 + 2)	US (2), SG / BR (2)
Kamatera, LeaseWeb, M247, IONOS SE	4	0	4 (1 each)	US (1), NL (1), FR (1), DE (1)

06

CHAPTER 06

What Defenders Should Do

IN SHORT

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

06 What Defenders Should Do

Managed service providers and IT deployment teams

- [ ] Remove organization-named `NinjaOne`, `Action1`, `Splashtop`, and VPN `.msi` or `.exe` packages from public HTTP folders, public NAS shares, and anonymous FTP mirrors. Move `Veeam` ISOs and `.vhdx` disks to authenticated storage.
- [ ] If an RMM installer exposed in a public folder contains a reusable enrollment token, rotate it. Require expiring onboarding links and manual technician approval before newly registered RMM agents receive scripts or policies.

Cloud web operations

- [ ] Audit Apache and Nginx settings across cloud virtual machines. Set `Options -Indexes -FollowSymLinks -SymLinksIfOwnerMatch` in Apache and `autoindex off; disable_symlinks on;` in Nginx, and verify that zero symbolic links inside `DocumentRoot` point outside the web root.

Payment-kiosk and healthcare asset owners

- [ ] Isolate unattended payment-kiosk listeners on private VLANs or APNs, and close the unauthenticated HTTP directory serving `DCMTK` binaries. Strip `.pdb` debug symbols from production builds and store kiosk camera captures outside web roots.

SOC and threat hunting teams

- [ ] Keep all 250 TacticalRMM endpoints off single-signal perimeter IP blocklists until independent protocol or behavioral telemetry confirms abuse. Hunt unapproved RMM activity through `TCP 1024` TLS certificate checks and endpoint `msiexec` logs using the rules in Chapter 7.

07

CHAPTER 07

Detection Rules

IN SHORT

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

INSIDE THIS CHAPTER

How the Suricata signatures work 24

How the KQL, Sigma, and YARA rules work 24

07 Detection Rules

The full rules are in Appendix B. Static syntax checks (`lint_suricata.py` with 0 problems across `sid:9549001` and `sid:9549008` and Sigma modifier checks) passed cleanly. Suricata, YARA, Sigma, and Kusto engines were not installed in our environment, and the rules were not replayed against live traffic or tested against actual captured directory-index pages. Validate and tune them in staging before production use.

Rule file	What it catches
`odin_exposed_kiosks_symlink_roots_and_rmm_shares.rules`	Suricata 7: two generic rules for open-directory HTTP responses serving installer, debug-symbol, virtual-disk, ISO, or DLL files (`sid:9549001`) and `TCP 1024` TLS server certificates (`sid:9549008`)
`sentinel_kiosk_symlink_and_rmm_installer_hunt.kql`	Sentinel and Defender XDR: outbound `TCP 1024` TacticalRMM port sessions, `msiexec.exe` execution of remote or downloaded `.msi` files, and web-root symlink or ad-hoc HTTP server processes
`sigma_rmm_msi_enrollment_and_symlink_exposure.yml`	Sigma (3 rules): Windows `msiexec` remote or downloaded `.msi` installs, Linux web-root `ln` or ad-hoc HTTP server commands, and web `GET` requests for exposed `.msi`, `.pdb`, `.vhdx`, `.iso`, or Linux root-like paths
`odin_kiosk_symlink_and_rmm_share_artifacts.yar`	YARA (3 rules): open-directory HTML indexes exposing `.NET` debug-symbol and DLL suites, Linux FHS root-like directory trees, or `.msi` installer and disk-image shares

How the Suricata signatures work

SID	Looks for	Why
9549001	Outbound 200 with `Index of /` and `.msi`, `.pdb`, `.vhdx`, `.iso`, or `.dll` file links	Self-audit alert when an internal web server exposes an open directory serving installers, debug symbols, disk images, or libraries
9549008	Inbound TLS server certificate (`CN=`) from `$EXTERNAL_NET` on port 1024	Flags TLS sessions on the default TacticalRMM port (:1024) for certificate and host correlation (hunt only)

We removed the six host-specific URI rules (`sid:9549002` to 9549007) so the public ruleset contains no owner-derived filenames or path fragments. Keep both `sid:9549001` and `sid:9549008` in alert mode for self-audit and certificate review. Treat any `sid:9549001` alert on your own perimeter as a posture incident: close the open directory, strip `.pdb` debug symbols, and rotate any reusable RMM enrollment tokens.

How the KQL, Sigma, and YARA rules work

The Sentinel KQL query looks back 7 days across `DeviceNetworkEvents` and `DeviceProcessEvents` in three branches. Branch 1 flags outbound connections to `RemotePort == 1024` outside two exact approved hosts (`msp-repo-prod-01.corp[.]example` and `sec-posture-audit-01.corp[.]example`). Branch 2 catches `msiexec.exe` command lines referencing `.msi` alongside `http://`, `https://`, `ftp://`, `\Downloads\`, or `\Temp\` outside those same two approved distribution hosts.

Branch 3 inspects `ln`, `python`, `python3`, `httpd`, `apache2`, or `nginx` commands referencing `http.server`, `SimpleHTTPServer`, `/var/www`, `DocumentRoot`, or `FollowSymLinks`. It correlates those processes within 15 minutes of port `80, 443, or 1024` network activity outside the two approved hosts.

Sigma rule 1 flags Windows `msiexec.exe` commands installing `.msi` packages from HTTP, HTTPS, FTP, `Downloads`, or `Temp` paths outside exact servers `MSP-DEPLOY-SRV01` and `IT-SCCM-DIST01`. Sigma rule 2 flags Linux `ln` commands targeting `/var/www/`, `/srv/http/`, or `/usr/share/nginx/html` and ad-hoc `http.server` or `SimpleHTTPServer` processes outside `SEC-POSTURE-AUDIT-01`; a match does not establish external HTTP exposure.

Sigma rule 3 flags web `GET` requests ending in `.msi`, `.pdb`, `.vhdx`, or `.iso`, or containing `/etc/passwd`, `/etc/shadow`, `/boot/vmlinuz`, or `/boot/initrd`. Three file-size-bounded YARA rules (512 KB and 1 MB caps) inspect captured HTML directory indexes for `.pdb` and DLL suites, Linux FHS directory trees, and `.msi` installer shares.

CHAPTER 08

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

Unconfirmed webmail-lure TacticalRMM candidates (addresses withheld) 27
Self-audit exposure categories (text-only) 27
Withheld TLS fingerprints 27

08 Indicators

Appendix A holds **0 published indicators: 0 network addresses and 0 file hashes**. All five misconfigured open-directory addresses (`Host A` through `Host E`) and all file digests on those shares are withheld. All 250 TacticalRMM addresses (2 unconfirmed webmail-lure cloud VPS endpoints, 115 dual-use cloud VPS servers, 111 regional MSP candidates, and 22 telecom collisions) are also withheld because none carries independent behavioral confirmation of abuse. Eleven self-audit patterns stay in the table below, while four TLS fingerprints from non-confirmed rows are withheld.

Unconfirmed webmail-lure TacticalRMM candidates (addresses withheld)

Two unconfirmed webmail-lure endpoints were observed; addresses, ports, and host-level details are withheld.

Self-audit exposure categories (text-only)

Exposure surface	Artifact category to audit on your own perimeter	Listener scope	Defensive use
Payment kiosk (`Host A`)	Kiosk `.NET` client and `.pdb` debug-symbol files	Primary HTTP listener	Audit kiosk subnets & strip `.pdb` debug symbols
Payment kiosk (`Host A`)	Motorized smart-card reader and dispenser DLLs (2 files)	Primary HTTP listener	Block external HTTP access to card-reader DLLs
Payment kiosk (`Host A`)	Contactless RFID reader and communications DLLs (2 files)	Primary HTTP listener	Block external HTTP access to RFID DLLs
Payment kiosk (`Host A`)	Electronic invoice log folder (134 log files)	Primary HTTP listener	Restrict kiosk invoice logs to private VLANs
Payment kiosk (`Host A`)	Kiosk camera capture folder (3 JPEG files)	HTTPS listener	Remove & block public kiosk camera JPEGs
Root-like web path (`Host B`)	Symlink-named web path exposing Linux system directories	Two web listeners	Disable `FollowSymLinks` & block root-like paths at proxies
Root-like web path (`Host B`)	Cloud Linux guest-agent binary under a root-like web path	Two web listeners	Audit cloud Linux VMs for root-like web paths
MSP share (`Host C`)	Client-folder `NinjaOne` agent MSIs (72.35 MB)	Two web listeners	Remove public MSIs & rotate any reusable tokens
MSP share (`Host C`)	Backup ISO (20.40 GB) and Hyper-V `.vhdx` disks	Two web listeners	Move backup media and virtual disks to private storage
Nginx/FTP share (`Host D`)	Mirrored organization-named `Action1` MSI (6.65 MB)	Two web listeners	Remove mirrored `Action1` MSIs & rotate any reusable tokens
Medical imaging (`Host E`)	Static Linux `DCMTK 3.6.9` binary directory (25 entries)	HTTP listener	Close the unauthenticated HTTP directory serving DCMTK binaries

Withheld TLS fingerprints

Four TLS fingerprints were observed on non-confirmed rows. Their values and host-level context are withheld.

09

CHAPTER 09

Scope and Limits

IN SHORT

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

09 Scope and Limits

All observations in this report come from a two-week observation window ending 21 November 2026. Five key limits apply to the analysis:

1. **Owner-versus-operator separation.** `Host A` through `Host E` are misconfigured owner or MSP file shares rather than adversary infrastructure, and nothing links them to one another or to the 250 TacticalRMM rows (0 shared hosts). All owner addresses, client or municipal folder names, and victim-specific file paths are withheld.
2. **Neutral vendor posture.** None of the observations imply a defect in `NinjaOne`, `Action1`, `Veeam`, `Splashtop`, `Datto RMM`, `SonicWALL`, `Cisco`, `Apache`, `Nginx`, `Microsoft WALinuxAgent`, `OFFIS DCMTK`, or card-reader and RFID libraries. The listings show public HTTP exposure; Odin did not verify the underlying web-server directives, symlink targets, or folder permissions.
3. **Unestablished origin and target of the web-root symlink path on `Host B`.** Directory metadata cannot show how the web-root symlink path on the Canada Ubuntu 24.04 Azure VM was created. Odin did not verify whether it resolved to a live root filesystem or which Apache options were set (0 webshells or implants observed).
4. **Zero installer testing or file content inspection.** Odin installed 0 `.msi` files, contacted 0 RMM consoles, and opened 0 backups, logs, or camera JPEGs beyond directory listing metadata.
5. **Pre-November file and record dates.** Kiosk log filenames from 2020 to 2025 (`Host A`) and archive build dates from 2022 to `July 2026` (`Host C` and `Host D`) are file timestamps on disk. Initial directory-record discovery dates of 9 to 12 August 2026 (`Host B` to `Host D`) are record metadata, not Odin's monitoring period, and our rules were checked statically without live engines.

10

CHAPTER 10

Sources

IN SHORT

This chapter lists the public references used in the report.

10 Sources

1. **CISA**, Joint Cybersecurity Advisory AA23-025A: Protecting Against Malicious Use of Remote Monitoring and Management (RMM) Software: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a (verified on 21 November 2026).
2. **Apache Software Foundation**, Apache HTTP Server 2.4 Core Features: Options FollowSymLinks and SymLinksIfOwnerMatch: https://httpd.apache.org/docs/2.4/mod/core.html (verified on 21 November 2026).
3. **Apache Software Foundation**, Apache Module mod_autoindex Documentation: https://httpd.apache.org/docs/2.4/mod/mod_autoindex.html (verified on 21 November 2026).
4. **Microsoft Learn**, Azure Linux Virtual Machine Agent (WALinuxAgent / waagent) Overview: https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/agent-linux (verified on 21 November 2026).
5. **MITRE ATT&CK**, Technique T1219: Remote Access Software: https://attack.mitre.org/techniques/T1219/ (verified on 21 November 2026).
6. **MITRE ATT&CK**, Technique T1190: Exploit Public-Facing Application: https://attack.mitre.org/techniques/T1190/ (verified on 21 November 2026).
7. **MITRE ATT&CK**, Sub-technique T1552.001: Unsecured Credentials - Credentials In Files: https://attack.mitre.org/techniques/T1552/001/ (verified on 21 November 2026).
8. **MITRE CWE**, CWE-59: Improper Link Resolution Before File Access ('Link Following'): https://cwe.mitre.org/data/definitions/59.html (verified on 21 November 2026).
9. **OFFIS e.V.**, DICOM Toolkit (DCMTK) Official Source Repository: https://github.com/DCMTK/dcmtk (verified on 21 November 2026).
10. **Amidaware**, Tactical RMM Official Documentation: https://docs.tacticalrmm.com/ (verified on 21 November 2026).

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

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

INSIDE

A. Indicators of compromise (0) 33

B. Detection rules (4 files) 34

A Indicators of Compromise

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

B Detection Rules

Each rule file loads in its own engine (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_exposed_kiosks_symlink_roots_and_rmm_shares.rules

SURICATA

```
# Odin by Brandefense - Monograph 49 Detection Suite (Suricata 7.x)
# Scope: Open HTTP directory listings serving installer, debug-symbol, virtual-disk, ISO, or DLL files,
# and TacticalRMM default-port (TCP 1024) TLS server certificates.
# Validation: Static syntax lint passed (0 problems); keep in alert mode for self-audit and certificate review.

alert http $HOME_NET any -> any any (msg:"ODIN POSTURE Outbound Open Directory Serving Installer Debug-Symbol
Disk-Image or DLL Files"; flow:from_server,established; http.stat_code; bsize:3; content:"200";
http.response_body; content:"Index of /"; fast_pattern; pcre:"/\.(msi|pdb|vhdx|iso|dll)\b/i"; classtype:policy-
violation; sid:9549001; rev:2;)
alert tls $EXTERNAL_NET 1024 -> $HOME_NET any (msg:"ODIN HUNT Inbound TLS Server Certificate on TacticalRMM
Default Port 1024"; flow:from_server,established; tls.cert_subject; bsize:>3; content:"CN="; fast_pattern;
classtype:misc-activity; sid:9549008; rev:1;)
```

odin_kiosk_symlink_and_rmm_share_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 49 YARA Posture & Artifact Rules
   Detects captured HTML open-directory listings exposing .NET debug-symbol
   and DLL suites, Linux FHS root-like directory trees, or MSI installer
   and disk-image shares.
*/

rule ODIN_Exposed_Payment_Kiosk_Directory_Index {
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-21"
        description = "Detects open-directory listings exposing .NET debug-symbol files alongside executable,
DLL, or configuration links"
        tlp = "CLEAR"
    strings:
        $idx1 = "Index of /" ascii nocase
        $idx2 = "Directory listing for /" ascii nocase
        $ext1 = ".exe\"" ascii nocase
        $ext2 = ".pdb\"" ascii nocase
        $ext3 = ".dll\"" ascii nocase
        $ext4 = ".config\"" ascii nocase
    condition:
        filesize < 512KB and 1 of ($idx*) and $ext2 and 2 of ($ext1, $ext3, $ext4)
}

rule ODIN_Apache_Root_Symlink_Traversal_Index {
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-21"
        description = "Detects open-directory listings exposing Linux FHS top-level system directories"
        tlp = "CLEAR"
    strings:
        $idx1 = "Index of /" ascii nocase
        $idx2 = "Directory listing for /" ascii nocase
        $fhs1 = "href=\"etc/\"" ascii nocase
        $fhs2 = "href=\"bin/\"" ascii nocase
        $fhs3 = "href=\"boot/\"" ascii nocase
        $fhs4 = "href=\"sbin/\"" ascii nocase
        $fhs5 = "href=\"lib/\"" ascii nocase
    condition:
        filesize < 1MB and 1 of ($idx*) and 3 of ($fhs*)
```

```
}

rule ODIN_Exposed_MSP_RMM_Share_Index {
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-21"
        description = "Detects open-directory shares exposing Windows MSI installers alongside executables, ISO
media, or VHDX virtual disks"
        tlp = "CLEAR"
    strings:
        $idx1 = "Index of /" ascii nocase
        $idx2 = "Directory listing for /" ascii nocase
        $pkg1 = ".msi\"" ascii nocase
        $pkg2 = ".exe\"" ascii nocase
        $pkg3 = ".iso\"" ascii nocase
        $pkg4 = ".vhdx\"" ascii nocase
    condition:
        filesize < 1MB and 1 of ($idx*) and $pkg1 and 1 of ($pkg2, $pkg3, $pkg4)
}
```

sentinel_kiosk_symlink_and_rmm_installer_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 49 Sentinel & Defender XDR Hunt Query
// Hunts outbound TacticalRMM default-port (TCP 1024) sessions, msiexec execution of
// remote or downloaded MSI installers, and web-root symlink or ad-hoc HTTP server processes.
let Lookback = 7d;
let ApprovedDeploymentHosts = dynamic(["msp-repo-prod-01.corp.example", "sec-posture-audit-01.corp.example"]);
let ExposedPorts = dynamic([80, 443, 1024]);
let TacticalRmmPortHits =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedDeploymentHosts))
    | where RemotePort == 1024
    | project Timestamp, DeviceId, DeviceName, DetectionBranch = "TACTICALRMM_PORT_1024_HUNT",
              ActionDetail = strcat(RemoteIP, ":", tostring(RemotePort)), InitiatingProcessCommandLine;
let RemoteOrDownloadedMsiExec =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedDeploymentHosts))
    | where FileName =~ "msiexec.exe"
    | where ProcessCommandLine has ".msi" and ProcessCommandLine has_any ("http://", "https://", "ftp://", "\
\Downloads\\", "\\Temp\\")
    | project Timestamp, DeviceId, DeviceName, DetectionBranch = "REMOTE_OR_DOWNLOADED_MSI_EXECUTION",
              ActionDetail = FileName, InitiatingProcessCommandLine = ProcessCommandLine;
let WebRootOrAdhocHttpHostProc =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedDeploymentHosts))
    | where FileName in~ ("ln", "python", "python3", "httpd", "apache2", "nginx")
    | where ProcessCommandLine has_any ("http.server", "SimpleHTTPServer", "/var/www", "DocumentRoot",
"FollowSymLinks")
    | join kind=inner (
        DeviceNetworkEvents
        | where Timestamp >= ago(Lookback)
        | where LocalPort in (ExposedPorts) or RemotePort in (ExposedPorts)
        | project DeviceId, NetTime = Timestamp, LocalPort, RemoteIP, RemotePort
    ) on DeviceId
    | where abs(datetime_diff("minute", Timestamp, NetTime)) <= 15
    | project Timestamp, DeviceId, DeviceName, DetectionBranch = "WEBROOT_OR_ADHOC_HTTP_SERVER_HOST",
              ActionDetail = strcat("LocalPort=", tostring(LocalPort), " Remote=", RemoteIP, ":",
tostring(RemotePort)),
              InitiatingProcessCommandLine = ProcessCommandLine;
union TacticalRmmPortHits, RemoteOrDownloadedMsiExec, WebRootOrAdhocHttpHostProc
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(),
            SampleDetails = make_set(ActionDetail, 5), SampleCommands = make_set(InitiatingProcessCommandLine, 3)
            by DeviceName, DetectionBranch
| order by FirstSeen desc
```

sigma_rmm_msi_enrollment_and_symlink_exposure.yml

SIGMA

```
title: Windows Msiexec Execution of Remote or Downloaded MSI Packages Outside Approved Servers
id: 6d4910a1-8c1e-4b32-9d41-01f490000101
status: experimental
description: Detects msiexec execution of MSI packages from HTTP, HTTPS, FTP, Downloads, or Temp paths outside
approved software distribution servers.
author: Odin by Brandefense
date: 2026/11/21
references:
  - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a
  - https://attack.mitre.org/techniques/T1219/
logsource:
  category: process_creation
  product: windows
detection:
  selection_msiexec:
    Image|endswith: '\msiexec.exe'
  selection_msi:
    CommandLine|contains: '.msi'
  selection_source:
    CommandLine|contains:
      - 'http://'
      - 'https://'
      - 'ftp://'
      - '\Downloads\'
      - '\Temp\'
  filter_approved_hosts:
    Computer:
      - 'MSP-DEPLOY-SRV01'
      - 'IT-SCCM-DIST01'
  condition: selection_msiexec and selection_msi and selection_source and not filter_approved_hosts
falsepositives:
  - Authorized technician manual onboarding on endpoints not yet enrolled in central deployment
level: high
tags:
  - attack.command_and_control
  - attack.t1219
---
title: Linux Web-Root Symlink Creation or Ad-Hoc HTTP Directory Server Execution
id: 6d4910a1-8c1e-4b32-9d41-01f490000102
status: experimental
description: Flags ln commands linking into web roots or ad-hoc Python HTTP directory servers outside approved
audit hosts; a process match does not establish external HTTP exposure.
author: Odin by Brandefense
date: 2026/11/21
references:
  - https://httpd.apache.org/docs/2.4/mod/core.html
  - https://cwe.mitre.org/data/definitions/59.html
logsource:
  category: process_creation
  product: linux
detection:
  selection_symlink:
    Image|endswith: '/ln'
    CommandLine|contains:
      - '/var/www/'
      - '/srv/http/'
      - '/usr/share/nginx/html'
  selection_adhoc_http:
    CommandLine|contains:
      - 'http.server'
      - 'SimpleHTTPServer'
  filter_approved_audit:
    Computer:
      - 'SEC-POSTURE-AUDIT-01'
  condition: (selection_symlink or selection_adhoc_http) and not filter_approved_audit
falsepositives:
  - Controlled lab testing on isolated hosts
level: high
```

```
  tags:
    - attack.initial_access
    - attack.t1190
    - attack.credential_access
    - attack.t1552.001
  ---
  title: Web Server Access to Exposed Installer Debug-Symbol Virtual-Disk or System Paths
  id: 6d4910a1-8c1e-4b32-9d41-01f490000103
  status: experimental
  description: Detects inbound HTTP GET requests targeting exposed MSI installers, PDB debug symbols, VHDX virtual
  disks, ISO images, or root-like Linux system subtrees on web servers.
  author: Odin by Brandefense
  date: 2026/11/21
  references:
    - https://httpd.apache.org/docs/2.4/mod/mod_autoindex.html
    - https://attack.mitre.org/techniques/T1552/001/
  logsource:
    category: webserver
  detection:
    selection_method:
      cs-method: 'GET'
    selection_extensions:
      cs-uri-stem|endswith:
        - '.msi'
        - '.pdb'
        - '.vhdx'
        - '.iso'
    selection_rootlike:
      cs-uri-stem|contains:
        - '/etc/passwd'
        - '/etc/shadow'
        - '/boot/vmlinuz'
        - '/boot/initrd'
    condition: selection_method and (selection_extensions or selection_rootlike)
  falsepositives:
    - Internal vulnerability or attack-surface posture audits
  level: high
  tags:
    - attack.credential_access
    - attack.t1552.001
    - attack.command_and_control
    - attack.t1219
```

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/exposed-kiosks-and-rmm-shares/
Short Read · brandefense.io/odin-research/blog/how-exposed-kiosks-root-like-web-paths-and-msp-rmm/
Defense Kit · brandefense.io/odin-research/defense-kit/