halcyon

ROC STAR REPORT: July 2026

Stats, Trends, and Results: What Halcyon's Ransomware Operations Center (ROC) detected, attacker tooling trends, detection gap analysis, and lessons from the front lines.

halcyon

halcyon.ai

July By The Numbers

$105M+

Est. breach costs from ransomware prevented

Based on a $4.99 M average cost of a data breach based on the latest IBM cost of a data breach report.

99.8%+

Stopped before exfiltration or encryption

Stopping attacks before encryption or exfiltration is what keeps businesses running.

99%

Threats stopped at the earliest attack stages

Halcyon stopped 99% of attacks at Defcon 3 or earlier.
(initial access, enumeration, lateralization)

Attack Chain Interception

< DEFCON 3 Early Stage

99%

of threats stopped here

Initial Access · Remote Access · Enumeration · Credential Harvesting · Privilege Escalation

Thousands of malicious events blocked before the attacker could establish a foothold.

DEFCON 2 Mid Stage

0.8%

of threats stopped here

Lateral Movement · Security Bypass · Data Exfiltration

15.5% were from Demo and POC testing and 3.5% came from Halcyon being brought in to support an existing IR engagement

DEFCON 1 Boom!

0.2%

of real threats hit Defcon 1 (All Blocked)

Data Destruction · Encryption

52% of Defcon 1 alerts in July were from Demo and POC testing. the other 48% of real attacks were blocked before impact.

99%+ of *real* ransomware attacks did not make it to Defcon 1

MeshAgent Posed as Windows Security. Halcyon Wasn't Fooled.

Fake Windows Service

MeshAgent RMM is downloaded from an attacker-controlled MeshCentral server and installed as a Windows service renamed to resemble the legitimate Microsoft Windows Security Health Service so it blends in.

Persistent Remote Access

It auto-starts as a SYSTEM-level Windows service, opening an encrypted MeshCentral channel for remote desktop, command execution, and file transfer — while each unique binary slips past hash-based detection.

Caught on Execution

Halcyon flagged the masquerading binary on execution and blocked it in prevention mode; ROC confirmed a legitimate MeshAgent RMM being abused for unauthorized remote access.

Contained & Escalated

ROC placed the asset into High Enforcement and escalated by phone, briefing the customer's IT staff — prevention mode had already blocked execution, and clean-up followed.

Blocked in Under an Hour

End to end in under an hour: detection, containment, customer briefing, and confirmed block — stopping remote access before persistence or ransomware could follow.

A MeshAgent RMM binary masquerading as the Windows Security Health Service was detected and blocked on execution — Halcyon disrupted the attack chain before remote access could be established, with the full incident handled in under an hour.

The Weaponization of Legitimate Tools

Attackers overwhelmingly favor legitimate RMM tools to blend in with normal IT activity, with the top four platforms alone accounting for 673 affected tenants. Offensive-security and exfiltration utilities round out the list.

1	**AnyDesk** ▲ +1 | RMM | D3	217 Tenants
2	**ConnectWise / ScreenConnect** ▼ −1 | RMM | D3	193 Tenants
3	**Splashtop** ▲ +1 | RMM | D3	136 Tenants
4	**LogMeIn / GoTo** ▼ −1 | RMM | D3	127 Tenants
5	**MobaXterm** — No Change | RMM | D3	125 Tenants
6	**VNC** — No Change | RMM | D3	51 Tenants
7	**Atera** ▲ +1 | RMM | D3	34 Tenants
8	**ProcDump** ▲ +4 | Offsec | D3	24 Tenants
9	**Rclone** New Entry | Exfil | D2	17 Tenants
10	**FileZilla** ▼ −1 | Exfil | D2	15 Tenants
11	**VSSAdmin / Shadow Copy** New Entry | Lolbas | D3	13 Tenants
12	**RustDesk** ▼ −5 | RMM | D3	10 Tenants

Tool Category Totals: July vs June 2026

Totals: Aggregate alert counts across all monitored tool categories.

RMM tools dominated July activity with 3,262 alerts across 12 tools (96% of all category volume), up 10.6% month-over-month. LOLBAS rose the most at +47.1%, while Offensive Security fell 23.1% and Exfiltration dropped 49.3%.

1	**RMM**	Jun: 2,949 → Jul: 3,262 | 905 Tenants | 12 Tools	3,262 Alerts	+10.6% MoM
2	**Exfiltration**	Jun: 71 → Jul: 36 | 32 Tenants | 4 Tools	36 Alerts	−49.3% MoM
3	**Offensive Security**	Jun: 65 → Jul: 50 | 28 Tenants | 6 Tools	50 Alerts	−23.1% MoM
4	**LOLBAS**	Jun: 34 → Jul: 50 | 16 Tenants | 4 Tools	50 Alerts	+47.1% MoM

Top Ransomware Families Tracked

The Gentlemen held #1 for a second month above Qilin; seven groups dropped out, replaced by six new entries, signaling continued heavy churn: (LockBit, Settra, ShinyHunters, Play, 3AM, Payload, WorldLeaks)

1	**The Gentlemen** — No Change	170 Victims
2	**Qilin** — No Change	124 Victims
3	**DeadLock** New Entry	82 Victims
4	**DragonForce** ▲ +2	42 Victims
5	**INC Ransom** — No Change	39 Victims
6	**SafePay** ▲ +2	31 Victims
7	**CRPxO** New Entry	30 Victims
8	**Global Secret Group** New Entry	28 Victims
9	**Krybit** ▲ +1	24 Victims
10	**Akira** ▼ −6	21 Victims
11	**Nova** ▼ −2	21 Victims
12	**NightSpire** New Entry	16 Victims
13	**Chaos** New Entry	15 Victims
14	**ExfilSquad** New Entry	15 Victims
15	**Genesis** New Entry	14 Victims

Top Industries Targeted by Ransomware

The rankings reshuffled sharply this month, with several sectors climbing and two new entries (Organizations, Healthcare Services) pushing in as Software and Law Firms dropped off. However, manufacturing continues to be the most popular target for ransomware attackers, holding the top spot by a wide margin with nearly double the claims of the next-ranked sector.

1	Manufacturing	— No Change	215 Claims	6	Government	▲ +3	36 Claims
2	Business Services	▲ +3	122 Claims	7	Organizations	New Entry	36 Claims
3	Retail	— No Change	88 Claims	8	Transportation	▼ −1	36 Claims
4	Construction	▼ −2	67 Claims	9	Finance	▲ +1	33 Claims
5	Hospitals And Physicians Clinics	▲ +1	37 Claims	10	Healthcare Services	New Entry	31 Claims

Catching What Others Miss

Highest-severity ransomware events (DEFCON 3 to 1) that bypassed leading EPP/EDR tools from the Gartner, Inc. Magic Quadrant™ (MQ) but were caught by Halcyon.

Attack Timing Analysis - Global

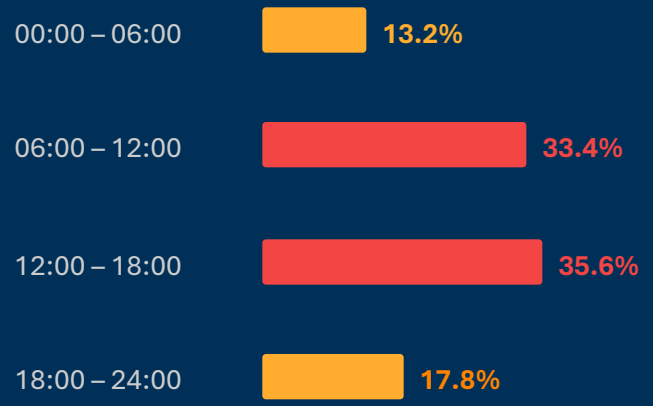
Normalized to each region's local clock, alert timing follows the target's working day, with encryption attempts the one stage that waits until users are logged off.

8.8%
Weekend Alerts

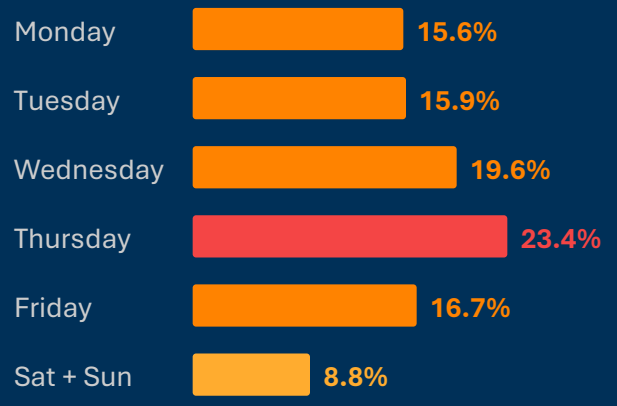
12:00 – 18:00 local
Peak Alert Window

Thursday
Busiest Day

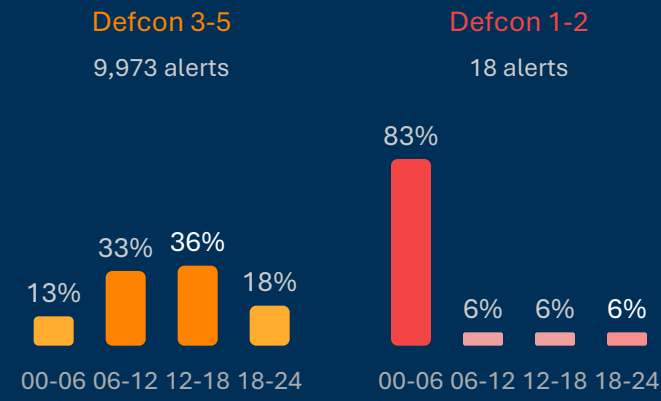
TIME OF DAY (LOCAL)



DAY OF WEEK



DEFCON BY TIME



One curve on four clocks: Every region traces the same daytime hump: volume climbs through the morning, peaks midday (69% in 06:00–18:00 local) and falls off sharply overnight and on weekends, so timing is driven by the local business rhythm of the target environment. The one deliberate exception is final-stage encryption, which inverts to 89% off-hours, 15 of 18 events firing in the 00:00–06:00 block while users are logged off.

halcyon

Key to Resilience.

Discover how the Halcyon ROC team can strengthen your ransomware defenses.

Reach out to us at: **halcyon.ai/get-a-demo**