halcyon

ROC STAR REPORT: May 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

May By The Numbers

$252M+

Est. breach costs from ransomware prevented

Based on a $4.5M average remediation cost, per incident.

99.9%+

Stopped before exfiltration or encryption

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

98.6%

Threats stopped at the earliest attack stages

Halcyon stopped 98.6% of attacks at Defcon 3 or earlier.
(initial access, enumeration, lateralization)

Attack Chain Interception

< DEFCON 3 Early Stage

98.6%

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

1.3%

of threats stopped here

Lateral Movement · Security Bypass · Data Exfiltration

Threats that progressed to lateral movement, exfiltration, or security bypass were all blocked.

DEFCON 1 Boom!

0.1%

of real threats hit Defcon 1 (All Blocked)

Data Destruction · Encryption

Only 0.1% of attacks made it to the encryption phase and all were blocked before execution.

99.9%+ of *real* ransomware attacks did not make it to Defcon 1

Stories from the ROC – Triple DLL Sideloading ShellcodeRunner

DETECTION

Behavioral Anomaly Flagged

A trojan delivered via a triple DLL sideloading chain abused a legitimate image viewer by mimicking an audio file that played genuine audio for several seconds before injecting the embedded shellcode into a target process.

PREVENTION

ROC Blocked Pre-Execution

The malicious DLL was blocked before shellcode execution. No foothold, no payload, no lateral movement. ROC notified customer by phone and email immediately.

INVESTIGATION

Three-Stage Chain Unpacked

Discovered 3 sideloaded DLLs each carrying only a partial payload so no single file would trigger a detection on its own. The file was staged in a GUID-named AppData folder and wore spoofed metadata to impersonate a trusted application.

RESPONSE

Customer Isolated Endpoint

Customer reviewed and isolated the affected asset as a precaution after initial contact from the ROC containing the incident before the attacker could progress.

CONTAINMENT

Chain Severed at Entry

The combination of Halcyon's detection and the customer's prompt isolation response closed the window before the attacker could cause any further damage within the customer's environment.

Triple DLL sideloading chain from a malicious audio file detected and blocked before in-memory execution.

The Weaponization of Legitimate Tools

Top 12: Most abused tools by unique orgs affected in May, with DEFCON level and kill chain category.

1	**ConnectWise / ScreenConnect** — No Change | RMM | D3	215 Tenants	
2	**AnyDesk** ▲ +1 | RMM | D3	198 Tenants	
3	**LogMeIn / GoTo** ▼ −1 | RMM | D3	158 Tenants	
4	**Splashtop** — No Change | RMM | D3	141 Tenants	
5	**MobaXterm** ▲ +1 | RMM | D3	70 Tenants	
6	**VNC** ▲ +1 | RMM | D3	57 Tenants	
7	**Atera** ▲ +2 | RMM | D3	46 Tenants	
8	**RustDesk** — No Change | RMM | D3	39 Tenants	
9	**FileZilla** ▲ +1 | Exfil | D2	24 Tenants	
10	**RemotePC** New Entry | RMM | D3	24 Tenants	
11	**N-Able** ▼ −6 | RMM | D3	16 Tenants	
12	**Rclone** — No Change | Exfil | D2	15 Tenants	

Tool Category Totals: May vs Apr 2026

Totals: Aggregate alert counts across all monitored tool categories.

RMM tools dominated May activity with 2,953 alerts across 13 tools. Exfiltration saw the sharpest month-over-month surge at +53.8%, while LOLBas and Offensive Security activity declined.

1	**RMM**	Apr: 3,878 → May: 2,953 alerts | 13 Tools Seen	2,953 Alerts	−23.8% MoM
2	**Exfiltration**	Apr: 65 → May: 100 alerts | 5 Tools Seen	100 Alerts	+53.8% MoM
3	**Offensive Security**	Apr: 49 → May: 43 alerts | 5 Tools Seen	43 Alerts	−12.2% MoM
4	**LOLBas**	Apr: 85 → May: 29 alerts | 4 Tools Seen	29 Alerts	−65.9% MoM

Top Ransomware Families Tracked

Top 15 ransomware groups by victim count, identified and monitored by Halcyon's research team to surface emerging threats and shifting attacker trends.

1	**Qilin** — No Change	108 Victims
2	**The Gentlemen** ▲ +1	80 Victims
3	**DragonForce** ▼ −1	52 Victims
4	**Akira** — No Change	41 Victims
5	**INC Ransom** — No Change	31 Victims
6	**SafePay** New Entry	27 Victims
7	**Nova** New Entry	23 Victims
8	**FulcrumSec** New Entry	21 Victims
9	**Play** New Entry	17 Victims
10	**CMDOrganization** New Entry	17 Victims
11	**Genesis** New Entry	17 Victims
12	**Lamashtu** ▼ −3	15 Victims
13	**MedusaLocker** New Entry	15 Victims
14	**Bavacai** New Entry	15 Victims
15	**Pear** ▼ −2	13 Victims

Top Industries Targeted by Ransomware

Top 10 industries by ransomware victim count, identified and monitored by Halcyon's research team to surface sector-specific threats and targeting patterns.

Manufacturing continues to be the most popular target for ransomware attackers

1	Manufacturing — No Change	133 Claims
2	Business Services ▲ +1	91 Claims
3	Construction ▲ +2	83 Claims
4	Retail ▲ +2	68 Claims
5	Software ▼ −1	47 Claims
6	Law Firms And Legal Services ▲ +1	34 Claims
7	Education New Entry	26 Claims
8	Healthcare Services ▼ −6	26 Claims
9	Nonprofits New Entry	25 Claims
10	Hospitals And Physicians Clinics New Entry	25 Claims

Catching What Others Miss

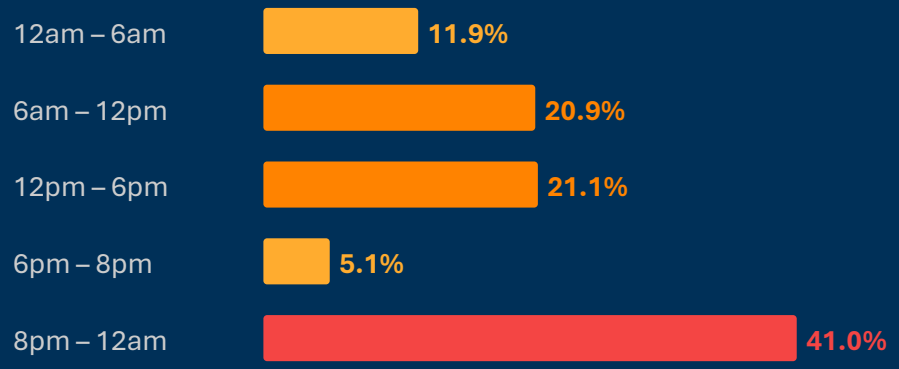
Highest-severity events (DEFCON 3 to 1) that bypassed leading EPP/EDR tools from the Gartner, Inc. Magic Quadrant™ (MQ) but were caught by Halcyon.

Attack Timing Analysis

Attack activity in May concentrated mid-week, with Wednesday and Thursday carrying the heaviest load. The nightly 8 PM EDT spike reflects the same midnight UTC pattern seen previously, just shifted for daylight savings.

17.7%	8 PM	Thursday
Weekend Alerts	Peak Alert Hour	Busiest Day

DETECTIONS BY TIME OF DAY (EDT)



DETECTIONS BY DAY OF WEEK

⚠ **May 7 Anomaly:** Thursday, May 7 saw 1,686 alerts — 1.6× the monthly daily average — the highest single-day volume in the dataset. May 12 (Tuesday) and May 28 (Thursday) also spiked at 1.5× and 1.4× respectively, suggesting mid-week pressure rather than pre-holiday front-loading this month.

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**