halcyon

ROC STAR REPORT: June 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

June By The Numbers

$131M+

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.

99.0%

Threats stopped at the earliest attack stages

Halcyon stopped 99.0% of attacks at Defcon 3 or earlier.
(initial access, enumeration, lateralization)

Attack Chain Interception

< DEFCON 3 Early Stage

99.0%

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

0.9%

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 – Rugmi Loader Blocked

DETECTION

Malicious Loader Flagged on Endpoint

Halcyon flagged a Rugmi loader on a customer asset, delivered over a WebDAV-style network path. The file used a Right-to-Left Override trick to disguise an executable as a PDF.

PREVENTION

Sideloading Chain Cut Off

The DLL sideloading chain was blocked before completion, stopping any secondary payload from downloading or executing and preventing the signed binaries and malicious DLL from being staged.

INVESTIGATION

Signed Binary Abuse Uncovered

The loader dropped renamed, legitimately signed binaries from trusted vendors beside a malicious DLL, so a trusted process sideloaded attacker code. The spoofed filename defeated name-based inspection.

RESPONSE

Isolated and Customer Notified

The threat was contained to a single asset and the customer was notified immediately. Linked tooling on the same domain indicated intent for remote access and lateral movement beyond simple data theft.

CONTAINMENT

Credential Theft Averted

Contained to one endpoint with no further spread. Left unchecked, Rugmi has delivered infostealers and RATs, risking wholesale credential theft, account takeover, lateral movement, and follow-on ransomware.

A Rugmi loader disguised as a PDF via RLO spoofing, using DLL sideloading through a signed vendor binary, was blocked before its infostealer or RAT payload could run.

The Weaponization of Legitimate Tools

Attackers overwhelmingly favor legitimate remote monitoring and management (RMM) tools to blend in with normal IT activity, with the top four platforms alone accounting for over 700 affected tenants. ProcDump's arrival as a new entry signals credential-dumping and offensive-security utilities creeping into the mix.

1	**ConnectWise / ScreenConnect** — No Change | RMM | D3	209 Tenants	
2	**AnyDesk** — No Change | RMM | D3	186 Tenants	
3	**LogMeIn / GoTo** — No Change | RMM | D3	170 Tenants	
4	**Splashtop** — No Change | RMM | D3	154 Tenants	
5	**MobaXterm** — No Change | RMM | D3	67 Tenants	
6	**VNC** — No Change | RMM | D3	60 Tenants	
7	**RustDesk** ▲ +1 | RMM | D3	47 Tenants	
8	**Atera** ▼ −1 | RMM | D3	39 Tenants	
9	**FileZilla** — No Change | Exfil | D2	36 Tenants	
10	**RemotePC** — No Change | RMM | D3	23 Tenants	
11	**N-Able** — No Change | RMM | D3	23 Tenants	
12	**ProcDump** New Entry | Offsec | D3	22 Tenants	

Tool Category Totals: June vs May 2026

Totals: Aggregate alert counts across all monitored tool categories.

RMM tools dominated June activity with 2,949 alerts across 13 tools, roughly flat month-over-month. Offensive Security saw the sharpest surge at +51.2%, while Exfiltration fell 29.0% and RMM held steady.

1	**RMM**	May: 2,953 → Jun: 2,949 alerts | 13 Tools Seen	2,949 Alerts	−0.1% MoM
2	**Exfiltration**	May: 100 → Jun: 71 alerts | 4 Tools Seen	71 Alerts	−29.0% MoM
3	**Offensive Security**	May: 43 → Jun: 65 alerts | 7 Tools Seen	65 Alerts	+51.2% MoM
4	**LOLBas**	May: 29 → Jun: 34 alerts | 3 Tools Seen	34 Alerts	+17.2% MoM

Top Ransomware Families Tracked

Qilin has been overtaken for the first time all year, with The Gentlemen taking the top spot. Another wave of new entries this month, following last month's, signals heavy churn and activity across the landscape.

1	The Gentlemen ▲ +1	73 Victims
2	Qilin ▼ −1	72 Victims
3	LockBit New Entry	57 Victims
4	Akira — No Change	30 Victims
5	INC Ransom — No Change	29 Victims
6	DragonForce ▼ −3	27 Victims
7	Settra New Entry	22 Victims
8	SafePay ▼ −2	21 Victims
9	Nova ▼ −2	21 Victims
10	Krybit New Entry	19 Victims
11	ShinyHunters New Entry	18 Victims
12	Play ▼ −3	16 Victims
13	3AM New Entry	14 Victims
14	Payload New Entry	12 Victims
15	WorldLeaks New Entry	12 Victims

Top Industries Targeted by Ransomware

The rankings reshuffled sharply this month, with several sectors climbing and three new entries pushing their way in, a sign of attackers broadening their targeting across the economy. However, manufacturing continues to be the most popular target for ransomware attackers with more claims than the next 3 combined.

1	Manufacturing — No Change	151 Claims	6	Hospitals And Physicians Clinics ▲ +4	29 Claims
2	Construction ▲ +1	64 Claims	7	Transportation New Entry	28 Claims
3	Retail ▲ +1	46 Claims	8	Law Firms And Legal Services ▼ −2	28 Claims
4	Software ▲ +1	33 Claims	9	Government New Entry	27 Claims
5	Business Services ▼ −3	29 Claims	10	Finance New Entry	26 Claims

Catching What Others Miss

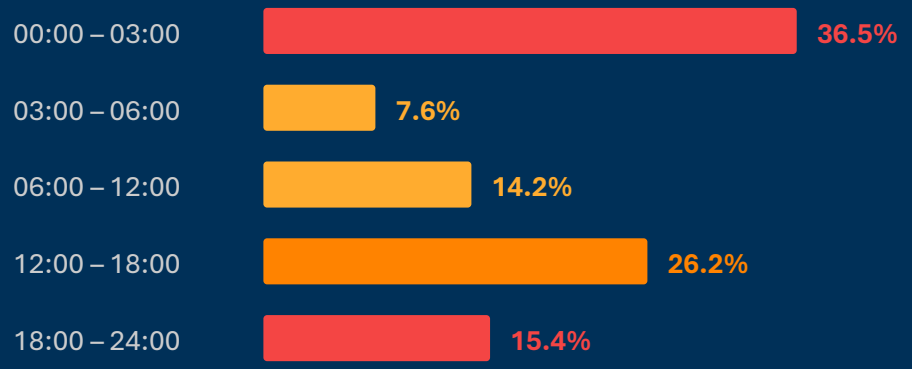
Highest-severity ransomware events (DEFCON 3 to 1) that bypassed leading EPP/EDR tools from the Gartner, Inc. Magic Quadrant™ (MQ) but were caught by Halcyon.

Attack Timing Analysis

Attack activity in June was heaviest on weekdays, with Monday and Thursday carrying the largest share and volume tapering off through the weekend. Peak alert time remains 00:00 UTC or 8:00pm EDT

16.2%	00:00 UTC	Monday
Weekend Alerts	Peak Alert Hour	Busiest Day

DETECTIONS BY TIME OF DAY (UTC)



DETECTIONS BY DAY OF WEEK

⚠ **June 18 Anomaly:** Thursday, June 18 saw 2,142 alerts, 1.8x the monthly daily average of 1,213, the highest single-day volume in the dataset. Two other days spiked well above baseline, June 12 (Friday) at 1.6x and June 15 (Monday) at 1.2x, indicating isolated surge events spread across the week rather than a consistent weekday pattern.

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**