halcyon

ROC STAR REPORT: March 2026

Real-world 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

March By The Numbers

$355M+

Est. breach costs from ransomware prevented

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

99.9%+

Stopped before exfiltration or encryption

Despite the number of attacks in March, only 0.1% progressed to an encryption attempt – all were stopped.

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

1.2%

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 - Datto RMM Phishing Campaign

DETECTION

Weaponized RMM Tool Identified

Four executables disguised as routine files detected across four customer networks. All signed with a legitimate Datto, LLC certificate to bypass signature-based defenses.

PREVENTION

All Four Blocked Pre-Execution

Halcyon stopped all four samples before any process could run. Three attempted NT AUTHORITY\SYSTEM execution — the highest Windows privilege level. No agent service established.

INVESTIGATION

Coordinated Campaign

Four distinct SHA256 hashes confirmed individually packaged deployments. C2 targeted *.centrastage[.]net over HTTPS.

RESPONSE

Customers Alerted Immediately

All four customers were notified of the malicious activity. No execution observed: no remote access channel, no persistence, no C2 communication established.

CONTAINMENT

Ransomware Risk Eliminated

Pre-execution blocking eliminated ransomware, credential theft, and lateral movement risk. Over 50% of RMM abuse cases progress to ransomware.

Halcyon Detected and Blocked All Four Threats Pre-Execution Across Four Customer Networks

The Weaponization of Legitimate Tools

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

1	**ConnectWise / ScreenConnect**	D3 | Remote Access	228 Orgs	7	**WMIC**	D3 | LOLBAS	46 Orgs
2	**LogMeIn / GoTo**	D3 | Remote Access	163 Orgs	8	**Atera**	D3 | Remote Access	41 Orgs
3	**AnyDesk**	D3 | Remote Access	163 Orgs	9	**RustDesk**	D3 | Remote Access	31 Orgs
4	**Splashtop**	D3 | Remote Access	155 Orgs	10	**RemotePC**	D3 | Remote Access	25 Orgs
5	**MobaXterm**	D3 | Remote Access	71 Orgs	11	**N-Able**	D3 | Remote Access	16 Orgs
6	**VNC**	D3 | Remote Access	55 Orgs	12	**Rclone**	D2 | Exfiltration	15 Orgs

Tool Category Totals: Feb vs Mar 2026

Totals: Aggregate alert counts across all monitored tool categories.

March saw a surge in attack activity, but early detection at the initial access phase (RMM tools) prevented adversaries from advancing driving sharp declines in LOLBAS, offensive security, and exfiltration alerts downstream.

1	**Remote Monitoring (RMM)**	Feb: 2,935 → Mar: 3,141 Alerts	88.5% Usage	+7.0% MoM
2	**LOLBAS (Living Off the Land)**	Feb: 202 → Mar: 54 Alerts	9.8% Usage	-73.3% MoM
3	**Offensive Security Tools**	Feb: 47 Alerts → Mar: 32 Alerts	0.9% Usage	-31.9% MoM
4	**Exfiltration Tools**	Feb: 42 Alerts → Mar: 30	0.8% Usage	-28.6% MoM

Top Ransomware Families Blocked

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	150 victims
2	Akira	85 victims
3	TheGentlemen	76 victims
4	DragonForce	56 victims
5	IncRansom	55 victims
6	LockBit	48 victims
7	Play	46 victims
8	Coinbasecartel	28 victims
9	Nightspire	28 victims
10	Ailock	23 victims
11	Payload	18 victims
12	Genesis	15 victims
13	Worldleaks	15 victims
14	Lapsus	10 victims
15	Gunra	9 victims

Top Industries Targeted by Ransomware

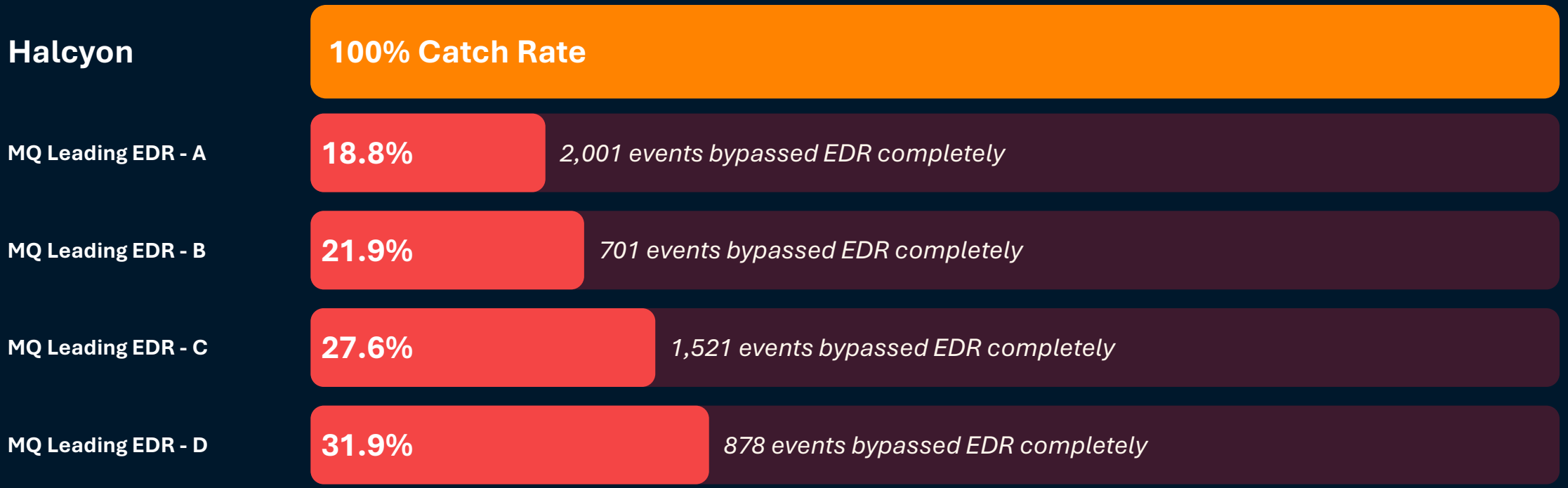
Top 10 industries by ransomware victim count, identified and monitored by Halcyon's research team to surface sector-specific threats and targeting patterns.

Manufacturing continues to be the most popular target for ransomware attackers

1	Manufacturing	208 Claims	6	Retail	47 Claims
2	Business Services	97 Claims	7	Healthcare Services	41 Claims
3	Construction	67 Claims	8	Transportation	31 Claims
4	Law Firms and Legal Services	57 Claims	9	Finance	29 Claims
5	Software	49 Claims	10	Government	27 Claims

Catching What Others Miss

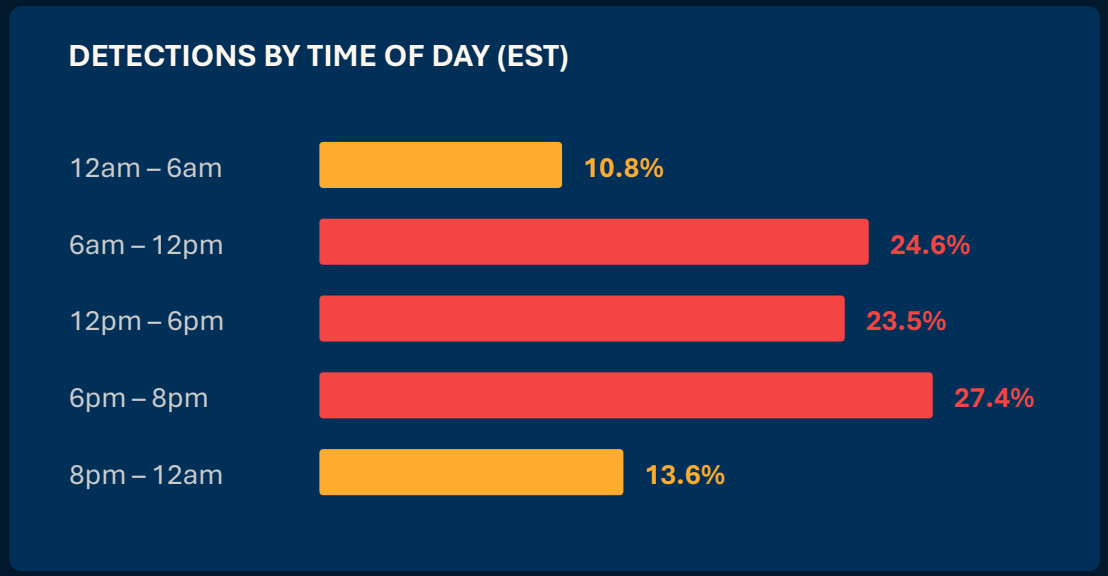
Highest-severity events (DEFCON 3 to 1) that bypassed leading EPP/EDR tools from the Gartner, Inc. Magic Quadrant™ (MQ) but were caught by Halcyon.

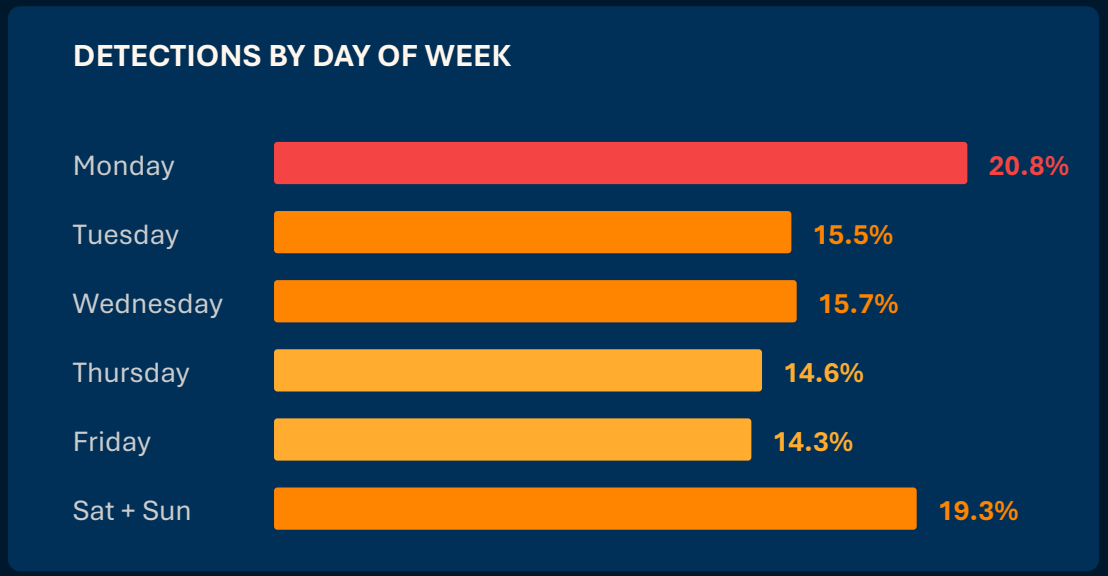


Attack Timing Analysis

Detections spread evenly across weekdays, but spike at shift-change hours when IT and security staffing is thinnest.

19.3%	7 PM	Monday
Weekend Alerts	Peak Alert Hour	Busiest Day





In March, the ROC team saw a trend of attacks peaking on Monday. **Monday alone (20.8%) exceeds Saturday + Sunday combined (19.3%)**, driven by a massive **12 PM spike** as attackers strike when staff return from lunch. The **7 PM peak** hits every day of the week equally — a signature of automated, scheduled campaigns that launch after hours.

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**