halcyon

ROC STAR REPORT: April 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

April By The Numbers

$315M+

Est. breach costs from ransomware prevented

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

99.3%+

Stopped before exfiltration or encryption

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

98.4%

Threats stopped at the earliest attack stages

Halcyon stopped 98.4% of attacks at Defcon 3 or earlier.
(initial access, enumeration, lateralization)

Attack Chain Interception

< DEFCON 3 Early Stage

98.4%

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

.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!

0.7%

of real threats hit Defcon 1 (All Blocked)

Data Destruction · Encryption

Only 0.7% of attacks made it to the encryption phase and all were blocked before execution.

99.3%+ of *real* ransomware attacks did not make it to Defcon 1

Stories from the ROC – EvilAI Downloader Campaign

DETECTION

Widespread Campaign Identified

EvilAI Downloader detected across 50+ networks over 8 consecutive weeks. Distributed via SEO-poisoned fake utility sites. All samples are signed, defeating signature-only defenses.

PREVENTION

All Variants Blocked Pre-Execution

Halcyon stopped EvilAI Downloader pre-execution in all Prevention mode environments. No foothold established, no secondary payloads delivered across any of the 50+ affected tenant networks.

INVESTIGATION

Nine Families, Five Hashes

ROC analysts tracked active campaign evolution — rotating filenames, new SHA256 variants, dual packaging formats (Electron/NSIS), and introduction of a new second-stage drop (ogg.dll) in the PDFSnap variant.

RESPONSE

ROC Responded Daily

ROC responded to multiple infections daily. 11 sectors impacted: Healthcare, Education, Finance, Government, Manufacturing, Retail, Hospitality, Utilities, Aerospace, Legal, and Arts.

CONTAINMENT

Initial Access Chain Severed

No lateral movement, credential theft, or follow-on compromise observed across all 50+ detections. Initial access blocked at the earliest stage of the chain — preventing the foothold that enables ransomware delivery.

Halcyon's layered detection blocked a persistent, signed EvilAI Downloader campaign across 50+ customer networks over eight consecutive weeks

The Weaponization of Legitimate Tools

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

1	**ConnectWise / ScreenConnect** — No Change | RMM | D3	235 Tenants	
2	**LogMeIn / GoTo** — No Change | RMM | D3	211 Tenants	
3	**AnyDesk** — No Change | RMM | D3	188 Tenants	
4	**Splashtop** — No Change | RMM | D3	147 Tenants	
5	**N-Able** ▲ +6 | RMM | D3	100 Tenants	
6	**MobaXterm** ▼ −1 | RMM | D3	78 Tenants	
7	**VNC** ▼ −1 | RMM | D3	66 Tenants	
8	**RustDesk** ▲ +1 | RMM | D3	44 Tenants	
9	**Atera** ▼ −1 | RMM | D3	42 Tenants	
10	**FileZilla** New Entry | Exfil | D2	29 Tenants	
11	**WMIC** ▼ −4 | LOLBas | D2	28 Tenants	
12	**Rclone** — No Change | Exfil | D2	17 Tenants	

Tool Category Totals: Apr vs Mar 2026

Totals: Aggregate alert counts across all monitored tool categories.

RMM tools dominated April activity with 3,878 uses across 13 tools — up 23.5% MoM. Exfiltration tools saw the sharpest month-over-month surge at +116.7%, while LOLBas and OffSec activity also climbed significantly.

1	**RMM**	Mar: 3,141 → Apr: 3,878 uses | 13 tools	3,878 Uses	+23.5% MoM
2	**LOLBas**	Mar: 54 → Apr: 85 uses | 4 tools	85 Uses	+57.4% MoM
3	**Exfiltration**	Mar: 30 → Apr: 65 uses | 4 tools	65 Uses	+116.7% MoM
4	**Offensive Security**	Mar: 32 → Apr: 49 uses | 6 tools	49 Uses	+53.1% 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	113 Victims	
2	**DragonForce** ▲ +2	64 Victims	
3	**TheGentlemen** — No Change	61 Victims	
4	**Akira** ▼ −2	48 Victims	
5	**IncRansom** — No Change	38 Victims	
6	**LockBit** — No Change	36 Victims	
7	**Krybit** New Entry	20 Victims	
8	**ShinyHunters** New Entry	20 Victims	
9	**Lamashtu** New Entry	17 Victims	
10	**Payload** ▲ +1	16 Victims	
11	**Nightspire** ▼ −2	15 Victims	
12	**Worldleaks** ▲ +1	12 Victims	
13	**Pear** New Entry	12 Victims	
14	**Everest** New Entry	11 Victims	
15	**Coinbasecartel** ▼ −7	10 Victims	

Top Industries Targeted by Ransomware

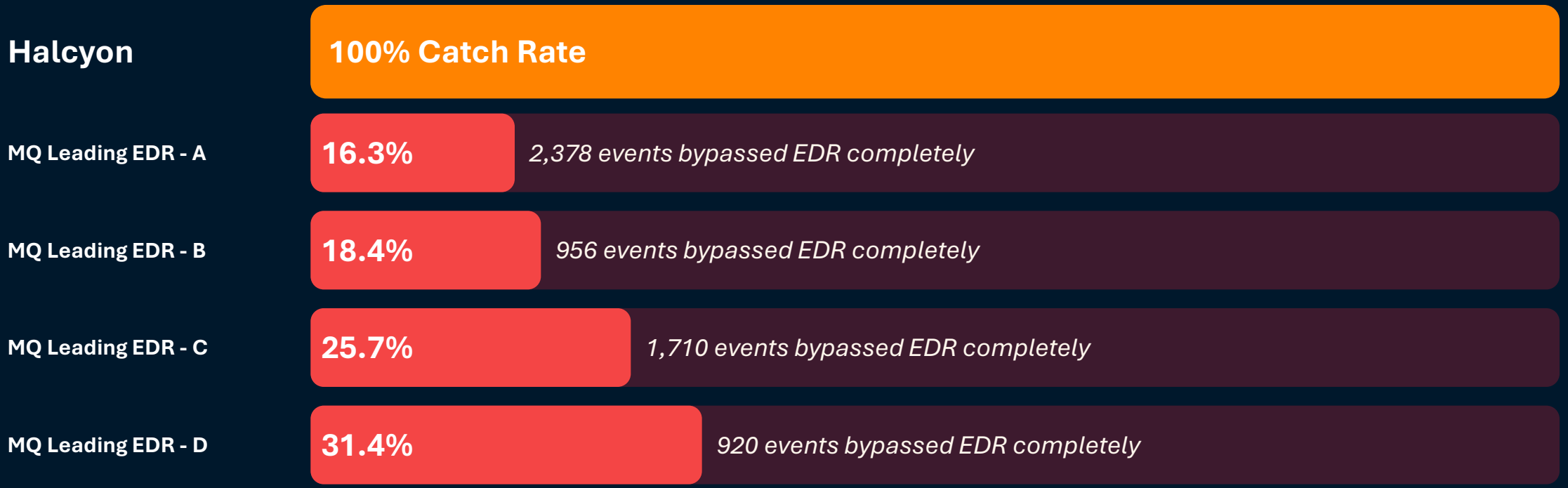
Top 10 industries by ransomware victim count, identified and monitored by Halcyon's research team to surface sector-specific threats and targeting patterns.

Manufacturing continues to be the most popular target for ransomware attackers

1	Manufacturing — No Change	110 Claims
2	Healthcare Services ▲ +5	67 Claims
3	Business Services ▼ −1	58 Claims
4	Software ▲ +1	55 Claims
5	Construction ▼ −2	53 Claims
6	Retail — No Change	52 Claims
7	Law Firms And Legal Services ▼ −3	33 Claims
8	Energy Utilities And Waste New Entry	23 Claims
9	Transportation — No Change	23 Claims
10	Finance — No Change	22 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.

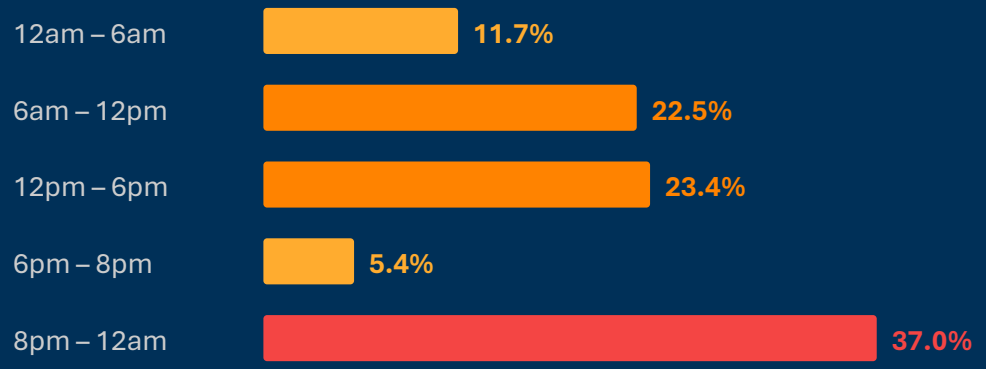


Attack Timing Analysis

Attack activity in April 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.

14.0%	8 PM	Wednesday
Weekend Alerts	Peak Alert Hour	Busiest Day

DETECTIONS BY TIME OF DAY (EDT)



DETECTIONS BY DAY OF WEEK

⚠ **Apr 2 Anomaly:** The day before Good Friday saw nearly 3× the monthly average and 2× any other single day, consistent with attackers front-loading activity ahead of a holiday weekend when IT and SOC coverage predictably thins.

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**