halcyon

ROC STAR REPORT: February 2026

Real-world Ransomware Threat Intel: What Halcyon's Ransomware Operations Center (ROC) detected, attacker tooling trends, detection gap analysis, and lessons from the front lines.

halcyon

halcyon.ai

February By The Numbers

$67.5M+

Est. breach costs from ransomware prevented

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

99.9%+

Stopped before exfiltration or encryption

99.9+% of encryption attempts in Feb. were customer red team tests.

97%

Threats stopped at the earliest attack stages

Halcyon stopped 97% 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

<1%

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!

<1%

of real threats hit Defcon 1 (All Blocked)

Data Destruction · Encryption

Over 99% of encryption attempts seen in the month of February were from **Customer Red Team Testing**.

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

Stories from the ROC - RAT & Credential Harvesting Attack

DETECTION

Phishing Email to Executive Gmail

A phishing email delivered a malicious .msi file via an attacker-controlled domain to an executive-level employee, initiating an unauthorized ScreenConnect session.

PREVENTION

Halcyon Blocked RAT Pre-Execution

RemoteTrojan.exe was flagged as unsigned and classified as CredentialHarvesting. Companion payload FakeLogin.EXE mimicked a Windows login prompt to steal domain credentials.

INVESTIGATION

Full Attack Chain Uncovered

Within ~7 minutes, attacker escalated to SYSTEM, registered persistent DLLs, modified firewall rules, and tampered with the EDR scheduled tasks. Customer EDR produced zero alerts.

RESPONSE

War Room & Network Isolation

Customer notified via email and phone. War Room initiated, system isolated, forensic data retrieved, and full incident investigation performed to map the attack chain.

CONTAINMENT

Threat Neutralized, Data Protected

Detailed report and remediation path delivered. Multiple privileged accounts on the compromised host were identified as at risk for lateral movement across the environment.

Halcyon Detected and Neutralized The Threat Where The Customer's EDR Produced Zero Alerts

The Weaponization of Legitimate Tools

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

1	**ScreenConnect**	D3 | Remote Access	205 Orgs	7	**Atera**	D3 | Remote Access	34 Orgs
2	**Splashtop**	D3 | Remote Access	146 Orgs	8	**FileZilla**	D2 | Exfiltration	25 Orgs
3	**LogMeIn / GoTo**	D3 | Remote Access	140 Orgs	9	**WMIC**	D3 | LOLBAS	25 Orgs
4	**AnyDesk**	D3 | Remote Access	125 Orgs	10	**RustDesk**	D3 | Remote Access	24 Orgs
5	**MobaXterm**	D3 | Remote Access	68 Orgs	11	**RemotePC**	D3 | Remote Access	23 Orgs
6	**VNC**	D3 | Remote Access	41 Orgs	12	**PsExec / RemCom**	D2 | Lateralization	17 Orgs

Tool Category Totals: Jan vs Feb 2026

Totals: Aggregate alert counts across all monitored tool categories.
RMM tools dominate volume while offensive security tools show the sharpest growth.

1	**Remote Monitoring (RMM)**	Jan: 2,095 → Feb: 2,935 Alerts	**+40% MoM**
2	**Offensive Security Tools**	Jan: 16 → Feb: 47 Alerts	**+194% MoM**
3	**Exfiltration Tools**	Jan: 50 → Feb: 42 Alerts	**-16% MoM**
4	**LOLBAS (Living Off the Land)**	Jan: 234 → Feb: 202 Alerts	**-14% MoM**

Ransomware Families

These five ransomware families represented the most active campaigns targeting our customers. Each was detected and neutralized by the Halcyon platform.

1. **Abyss** — 2,212 Samples
   HelloKitty-derived RaaS. Double extortion targeting ESXi, VPN appliances, and NAS devices.
2. **LockBit 3.0** — 608 Samples
   Most prolific global RaaS franchise. Self-spreading, StealBit exfil. Infrastructure seized Feb 2024.
3. **RAGroup/RAWorld** — 209 Samples
   Babuk-based double extortion. Targets healthcare and manufacturing. Linked to Chinese espionage toolsets.
4. **Akira** — 207 Samples
   Exploits VPN flaws for initial access. Targets Windows and Linux/ESXi. Tied to former Conti affiliates.
5. **Black Basta** — 201 Samples
   Former Conti-affiliated RaaS. Uses ScreenConnect, Cobalt Strike, and BloodHound for AD enumeration.

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	2,298 victims
2	Akira	1,721 victims
3	Clop	1,091 victims
4	Play	1,026 victims
5	RansomHub	971 victims
6	SafePay	804 victims
7	Lynx	667 victims
8	DragonForce	504 victims
9	IncRansom	467 victims
10	Medusa	420 victims
11	Sinobi	415 victims
12	INC Ransom	410 victims
13	FunkSec	347 victims
14	KillSec3	334 victims
15	Everest	313 victims

Catching What Others Miss

Highest-severity samples (DEFCON 3 to 1) with low VirusTotal detection rates, tested against leading EPP/EDR tools from the Gartner, Inc. Magic Quadrant™ (MQ).

Attack Timing Analysis

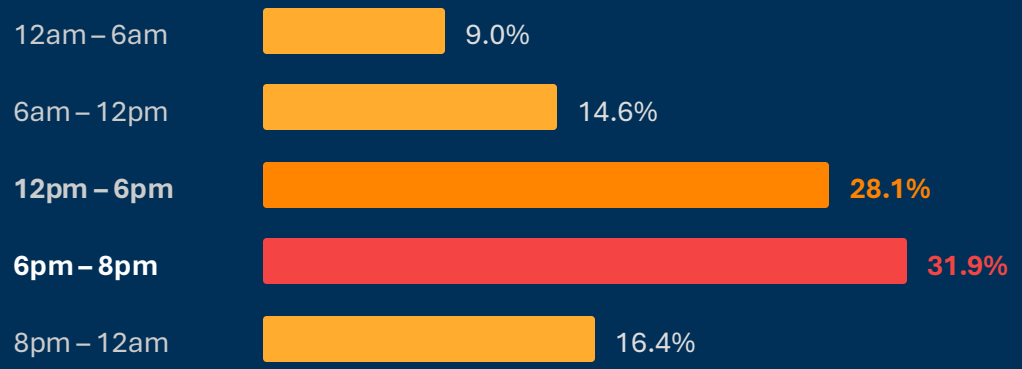
Detections spread evenly across weekdays, but spike at shift-change hours when IT and security staffing is thinnest.

17%
Weekend Alerts

7 PM
Peak Alert Hour (EST)

Wednesday
Busiest Day (18.6%)

DETECTIONS BY TIME OF DAY (EST)



DETECTIONS BY DAY OF WEEK

The Halcyon ROC operates 24/7 so your team doesn't have to.

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**