halcyon

ROC STAR レポート：2026年3月

Halcyonのランサムウェアオペレーションセンター（ROC）が検知した実際の統計・トレンド・成果をもとに、攻撃者のツール動向、検知ギャップの分析、そして最前線から得られた教訓をお届けします。

halcyon

halcyon.ai

3月の主要数値

$355M+

ランサムウェア防止による推定侵害コスト削減額

1インシデントあたり
平均修復コスト450万ドルに
基づく推計

99.9%+

データ窃取・暗号化前に阻止

2月に観測された暗号化試行の
99.9%以上は顧客の
レッドチームテストによるもの

98.6%

攻撃の最初期段階で脅威を阻止

Halcyonは攻撃の97%を
Defcon 3*以前の段階で阻止。
（初期アクセス、偵察、横展開）

*日本語版注記：DEFCONは米軍の防衛準備態勢に由来する脅威レベル指標。数字が小さいほど深刻度が高い。

攻撃を阻止したタイミング

攻撃チェーンの遮断

< DEFCON 3　初期段階

98.6%

の脅威をここで阻止

初期アクセス・リモートアクセス・偵察・認証情報窃取・権限昇格

攻撃者が足掛かりを築く前に、数千の悪意あるイベントをブロック。

DEFCON 2　中期段階

1.2%

の脅威をここで阻止

横展開・セキュリティ回避・データ窃取

横展開、データ窃取、セキュリティ回避に進行した脅威はすべてブロック。

DEFCON 1　最終段階

~0.1%

の実際の脅威がDefcon 1に到達（すべてブロック済み）

データ破壊・暗号化

暗号化フェーズに到達した攻撃はわずか0.1%：そのすべてを実行前にブロック。

99.9%以上の実際のランサムウェア攻撃はDefcon 1に到達しなかった

*日本語版注記：DEFCONは米軍の防衛準備態勢に由来する脅威レベル指標。数字が小さいほど深刻度が高い。

ROC現場事例 - Datto RMM 悪用型フィッシング攻撃

検知

武器化されたRMM ツールを特定

4つの顧客ネットワークにおいて、通常のファイルに偽装された4つの実行ファイルを検知。すべてDatto, LLCの正規の証明書で署名されており、署名ベースの防御を回避する意図がありました。

防止

4件すべてを実行前にブロック

Halcyonは、プロセスが実行される前に4つのサンプルすべてを阻止。そのうち3件はNT AUTHORITY¥SYSTEM（Windowsの最高権限レベル）での実行を試みていました。エージェントサービスは確立されませんでした。

調査

組織的なキャンペーン

4つの異なるSHA256ハッシュにより、個別にパッケージ化された展開が確認されました。C2通信先は*.centrastage[.]net（HTTPS経由）でした。

対応

顧客への即時通知

4社すべての顧客に悪意ある活動を通知。実行は確認されず、リモートアクセスチャネル、永続化、C2通信のいずれも確立されていませんでした。

封じ込め

ランサムウェアリスクの排除

実行前のブロックにより、ランサムウェア、認証情報の窃取、横展開のリスクを排除しました。RMM悪用事例の50%以上がランサムウェアに進行します。

Halcyonは4つの顧客ネットワークにおいて、4件の脅威すべてを実行前に検知・ブロック

正規ツールの武器化

Top 12: 3月に影響を受けた組織数別の悪用ツールランキング（DEFCON*レベルとキルチェーンカテゴリ付き）

*日本語版注記：DEFCONは米軍の防衛準備態勢に由来する脅威レベル指標。数字が小さいほど深刻度が高い。

1	ConnectWise / ScreenConnect	D3 | リモートアクセス	228 組織	7	WMIC	D3 | LOLBAS	46 組織
2	LogMeIn / GoTo	D3 | リモートアクセス	163 組織	8	Atera	D3 | リモートアクセス	41 組織
3	AnyDesk	D3 | リモートアクセス	163 組織	9	RustDesk	D3 | リモートアクセス	31 組織
4	Splashtop	D3 | リモートアクセス	155 組織	10	RemotePC	D3 | リモートアクセス	25 組織
5	MobaXterm	D3 | リモートアクセス	71 組織	11	N-Able	D3 | リモートアクセス	16 組織
6	VNC	D3 | リモートアクセス	55 組織	12	Rclone	D2 | データ窃取	15 組織

ツールカテゴリー合計：2026年2月 vs 3月

総計：監視対象の全ツールカテゴリにおけるアラート件数の集計

3月は攻撃活動が急増しましたが、初期アクセスフェーズ（RMMツール）での早期検知により攻撃者の侵入進行を阻止。その結果、LOLBAS・攻撃的セキュリティツール・データ窃取関連のアラートは大幅に減少しました。

1	リモート監視(RMM)	2月: 2,935 → 3月: 3,141 Alerts	88.5% Usage	+7.0% 前月比
2	LOLBAS (Living Off the Land)	2月: 202 → 3月: 54 Alerts	9.8% Usage	-73.3% 前月比
3	攻撃的セキュリティツール	2月: 47 → 3月: 32 Alerts	0.9% Usage	-31.9% 前月比
4	データ窃取ツール	2月: 42 → 3月: 30 Alerts	0.8% Usage	-28.6% 前月比

ブロックしたランサムウェアグループ上位

被害組織数に基づくランサムウェアグループ上位15。Halcyonリサーチチームが新興脅威と攻撃者トレンドの変化を把握するために特定・監視しています。

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

ランサムウェアの標的となった上位業種

Halcyonのリサーチチームが特定・監視しているランサムウェア被害件数別の上位10業種。セクター固有の脅威と標的パターンを把握するためのものです。製造業は引き続きランサムウェア攻撃者にとって最も人気の高い標的です。

1	製造業	208 件
2	ビジネスサービス	97 件
3	建設業	67 件
4	法律事務所・法務サービス	57 件
5	ソフトウェア	49 件
6	小売業	47 件
7	医療サービス	41 件
8	運輸業	31 件
9	金融業	29 件
10	政府機関	27 件

EDR バイパスの検知

他ツールが見逃す脅威をキャッチ

Gartner 社マジック・クアドラント（Magic Quadrant™ ）掲載の主要EPP/EDRツールをバイパスした最重要度イベント（DEFCON3〜1）を、Halcyonが全て検知。

*日本語版注記：DEFCONは米軍の防衛準備態勢に由来する脅威レベル指標。数字が小さいほど深刻度が高い。

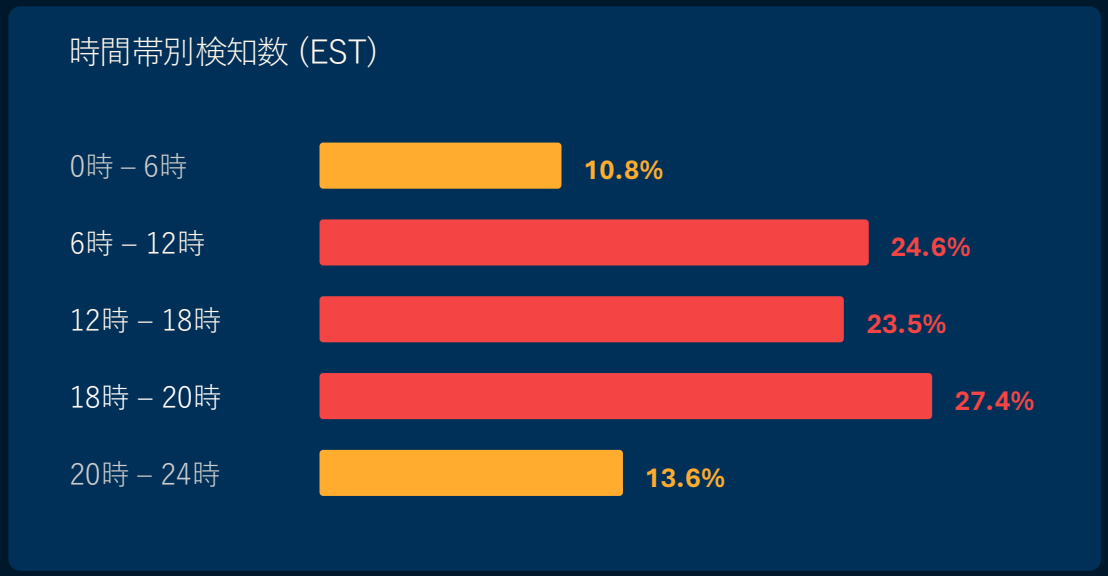
攻撃タイミング分析

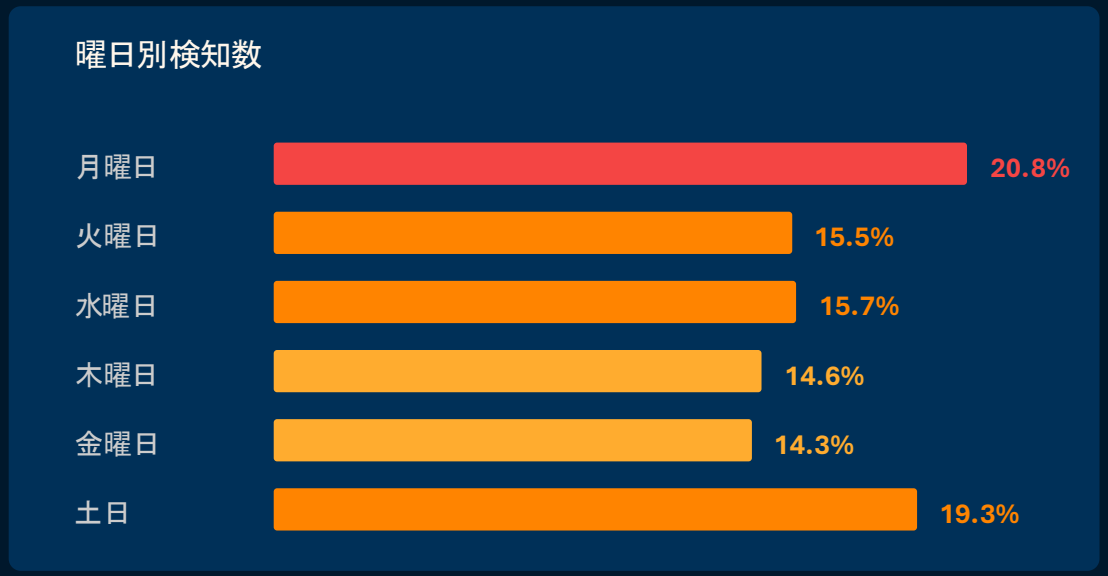
検知は平日を通じてほぼ均等に分布するが、ITおよびセキュリティ担当者が最も手薄になる交代時間帯に急増する。

19.3%
週末のアラート

午後7時
ピークアラート時間帯 (EST)

月曜日
最も多い曜日





3月、ROCチームは月曜日に攻撃がピークを迎える傾向を確認しました。月曜日だけで20.8%を占め、土日の合計（19.3%）を上回っています。これは、スタッフが昼休みから戻る正午の大幅な急増が要因です。午後7時のピークは曜日に関係なく均等に発生しており、業務時間後に開始される自動化・スケジュール型キャンペーンの特徴です。

halcyon

揺るがない防御力の鍵

ランサムウェア対策は、Halcyon ROC（ランサムウェアオペレーションセンター）にお任せください。

halcyon.ai/jp