halcyon

ROC STAR レポート：2026年4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

4月の主要数値

$315M+

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

99.3%+

データ窃取・暗号化前に
阻止

暗号化やデータ窃取の前に
攻撃を阻止することが
事業継続の鍵

98.4%

攻撃の最初期段階で
脅威を阻止

Halcyonは攻撃の98.4%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

98.4%

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

.9%

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

0.7%

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0.7%：そのすべてを実行前にブロック。

99.3%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 – EvilAIダウンローダーを利用した攻撃

検知

大規模キャンペーンを特定

EvilAIダウンローダーを50以上のネットワークで8週連続で検知。SEOポイズニングされた偽ユーティリティサイト経由で配布。すべてのサンプルに署名が施されており、シグネチャベースの防御を無力化。

防止

全亜種を実行前にブロック

Halcyonは全Prevention Mode環境でEvilAIダウンローダーを実行前に阻止。50以上の影響を受けたテナントネットワークにおいて、足場の構築もセカンダリペイロードの配信も許しませんでした。

調査

9系統、5つのハッシュ

ROCアナリストがキャンペーンの進化を継続的に追跡。ファイル名のローテーション、新たなSHA256亜種、2種類のパッケージ形式（Electron/NSIS）、さらにPDFSnap亜種では新しいセカンドステージドロップ（ogg.dll）の導入を確認。

対応

ROCが日次で対応

ROCは日々発生する複数の感染に対応。影響を受けた業種は11に及ぶ：ヘルスケア、教育、金融、行政、製造、小売、ホスピタリティ、公共事業、航空宇宙、法務、芸術。

封じ込め

初期アクセスチェーンを遮断

50件以上の全検知において、横展開・認証情報の窃取・後続の侵害は確認されず。攻撃チェーンの最初期段階でブロックし、ランサムウェア配信の足場となる侵入を未然に防止。

署名付きのEvilAIダウンローダーが8週連続で拡散。
Halcyonの多層防御が、50以上の顧客ネットワークでそのすべてをブロックしました。

正規ツールの武器化

Top 12: 4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** 前月比±0（変動なし） | リモートアクセス | D3	235 組織	
2	**LogMeIn / GoTo** 前月比±0（変動なし） | リモートアクセス | D3	211 組織	
3	**AnyDesk** 前月比±0（変動なし） | リモートアクセス | D3	188 組織	
4	**Splashtop** 前月比±0（変動なし） | リモートアクセス | D3	147 組織	
5	**N-Able** ▲ +6 | リモートアクセス | D3	100 組織	
6	**MobaXterm** ▼ −1 | リモートアクセス | D3	78 組織	
7	**VNC** ▼ −1 | リモートアクセス | D3	66 組織	
8	**RustDesk** ▲ +1 | リモートアクセス | D3	44 組織	
9	**Atera** ▼ −1 | リモートアクセス | D3	42 組織	
10	**FileZilla** ★ 新規 | データ窃取 | D2	29 組織	
11	**WMIC** ▼ −4 | LOLBas（環境寄生型攻撃） | D2	28 組織	
12	**Rclone** 前月比±0（変動なし） | データ窃取 | D2	17 組織	

ツールカテゴリー合計：2026年4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

4月はRMMツールが13種類・3,878件で突出し、前月比+23.5%。データ窃取ツールは前月比+116.7%と最も急激な増加を記録。LOLBAS（環境寄生型攻撃）および攻撃的セキュリティツールの活動も大幅に増加しました。

1	リモート監視（RMM）	3月: 3,141 → 4月: 3,878 件 | 13 ツール	3,878 件	+23.5% 前月比
2	LOLBas（環境寄生型攻撃）	3月: 54 → 4月: 85 件 | 4 ツール	85 件	+57.4% 前月比
3	データ窃取ツール	3月: 30 → 4月: 65 件 | 4 ツール	65 件	+116.7% 前月比
4	攻撃的セキュリティツール	3月: 32 → 4月: 49 件 | 6 ツール	49 件	+53.1% 前月比

被害件数上位のランサムウェアグループ

被害件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** 前月比±0（変動なし）	113件			
2	**DragonForce** ▲ +2	64件	9	**Lamashtu** 新規	17件
3	**TheGentlemen** 前月比±0（変動なし）	61件	10	**Payload** ▲ +1	16件
4	**Akira** ▼ −2	48件	11	**Nightspire** ▼ −2	15件
5	**IncRansom** 前月比±0（変動なし）	38件	12	**Worldleaks** ▲ +1	12件
6	**LockBit** 前月比±0（変動なし）	36件	13	**Pear** 新規	12件
7	**Krybit** 新規	20件	14	**Everest** 新規	11件
8	**ShinyHunters** 新規	20件	15	**Coinbasecartel** ▼ −7	10件

ランサムウェアの標的となった上位業種

ランサムウェア被害件数に基づく業種別上位10。Halcyonリサーチチームが業種固有の脅威と標的パターンを把握するために特定・監視しています。製造業は引き続きランサムウェア攻撃者にとって最大の標的です。

1	製造業 前月比±0（変動なし）	110件
2	医療サービス ▲ +5	67件
3	ビジネスサービス ▼ −1	58件
4	ソフトウェア ▲ +1	55件
5	建設業 ▼ −2	53件
6	小売業 前月比±0（変動なし）	52件
7	法律事務所・法務サービス ▼ −3	33件
8	Energy Utilities And Waste 新規	23件
9	運輸業 前月比±0（変動なし）	23件
10	金融業 前月比±0（変動なし）	22件

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がすべて検知。

攻撃タイミング分析

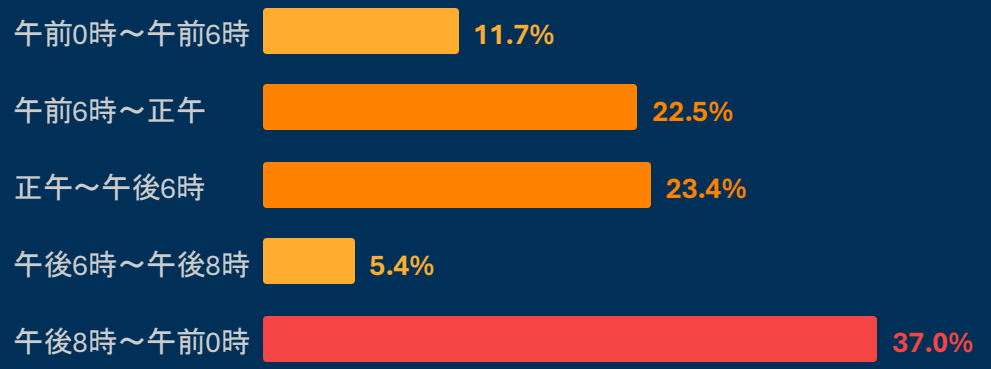
4月の攻撃活動は水曜日と木曜日に集中しました。午後8時（米国東部時間）に検知がピークを迎えていますが、これはUTC午前0時に当たり、以前のレポートで確認された深夜帯の攻撃パターンと同じ傾向です。

14.0%
週末のアラート

午後8時
ピークアラート時間帯

水曜日
最も忙しい曜日

時間帯別の検知状況（米国東部夏時間）



曜日別の検知状況

⚠4月2日の異常値: グッドフライデー前日の攻撃量は月間平均の約3倍、他のどの日と比べても2倍に達しました。これは、休日の連休前にIT・SOCの体制が手薄になることを見越して、攻撃者が活動を前倒しにするパターンと一致しています。

halcyon

事業継続の要

Halcyon ランサムウェアオペレーションセンター（ROC）が、
ランサムウェアからお客様の事業を守り抜きます。

資料請求： halcyon.ai/jp/shiryo-seikyu