halcyon

ROC STAR レポート: 2026年2月

ランサムウェア脅威インテリジェンス: Halcyonのランサムウェアオペレーションセンター（ROC）が検知した脅威、攻撃ツールの動向、検知ギャップ分析、そして最前線からの教訓。

halcyon

halcyon.ai

2月の主要数値

$67.5M+

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

97%

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

99%

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%

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

<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

2月に観測された暗号化試行の99%以上は**顧客のレッドチームテスト**によるもの。

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 – 遠隔操作型トロイの木馬(RAT)＆認証情報窃取攻撃

検知

幹部のGmailへのフィッシングメール

攻撃者管理ドメイン経由で悪意ある.msiファイルを含むフィッシングメールが幹部宛に送信され、不正なScreenConnectセッションが開始された。

防止

HalcyonがRATを実行前にブロック

RemoteTrojan.exeが未署名として検出され、認証情報窃取として分類。FakeLogin.EXEはWindowsログイン画面を模倣してドメイン認証情報の窃取を試みた。

調査

攻撃チェーン全体を解明

約7分以内に攻撃者はSYSTEM権限に昇格し、永続化DLLを登録、ファイアウォールルールを変更、EDRのスケジュールタスクを改竄。顧客のEDRはアラートを出さなかった。

対応

緊急対策本部＆ネットワーク隔離

メールと電話で顧客に通知。緊急対策本部を開設し、システムを隔離、フォレンジックデータを取得し、攻撃チェーンの全体像を調査。

封じ込め

脅威を無力化、データを保護

詳細なレポートと修復パスを提供。侵害されたホスト上の複数の特権アカウントが環境全体への横展開リスクとして特定された。

Halcyonが、顧客のEDRがアラートを出さなかった脅威を検知し無力化した

正規ツールの武器化

Top 12: 2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	ScreenConnect	D3 | リモートアクセス	205 組織	7	Atera	D3 | リモートアクセス	34 組織
2	Splashtop	D3 | リモートアクセス	146 組織	8	FileZilla	D2 | データ窃取	25 組織
3	LogMeIn / GoTo	D3 | リモートアクセス	140 組織	9	WMIC	D3 | LOLBAS	25 組織
4	AnyDesk	D3 | リモートアクセス	125 組織	10	RustDesk	D3 | リモートアクセス	24 組織
5	MobaXterm	D3 | リモートアクセス	68 組織	11	RemotePC	D3 | リモートアクセス	23 組織
6	VNC	D3 | リモートアクセス	41 組織	12	PsExec / RemCom	D2 | 横展開	17 組織

ツールカテゴリ合計：2026年1月 vs 2月

全監視対象ツールカテゴリのアラート集計。RMMツールが量で首位、攻撃的セキュリティツールが最も急成長。

1	リモート監視(RMM)	1月: 2,095 → 2月: 2,935 Alerts	+40% 前月比
2	攻撃的セキュリティツール	J月: 16 → 2月: 47 Alerts	+194% 前月比
3	データ窃取ツール	1月: 50 → 2月: 42 Alerts	-16% 前月比
4	LOLBAS (環境寄生型攻撃)	1月: 234 → 2月: 202 Alerts	-14% 前月比

ランサムウェア亜種

ランサムウェアファミリー

以下の5つのランサムウェアファミリーは、当社の顧客を標的とした最も活発なキャンペーンです。
いずれもHalcyonプラットフォームによって検知・無力化されました。

1. **Abyss** — 2,212 サンプル
   HelloKitty派生のRaaS。ESXi、VPN アプライアンス、 NASデバイスを標的とした二重恐喝。
2. **LockBit 3.0** — 608 サンプル
   世界で最も多発するRaaSフランチャイズ。自己拡散型、StealBitによるデータ窃取。2024年2月にインフラ押収。
3. **RAGroup/RAWorld** — 209 サンプル
   Babukベースの二重恐喝。医療・製造業を標的。中国のスパイツールセットとの関連。
4. **Akira** — 207 サンプル
   VPNの脆弱性を悪用して初期アクセスを取得。 Windows・Linux/ESXiを標的。元Contiアフィリエイト。
5. **Black Basta** — 201 サンプル
   元Conti系RaaS。ScreenConnect、Cobalt Strike、BloodHoundによるAD 列挙を使用。

ブロックしたランサムウェアファミリー上位

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。

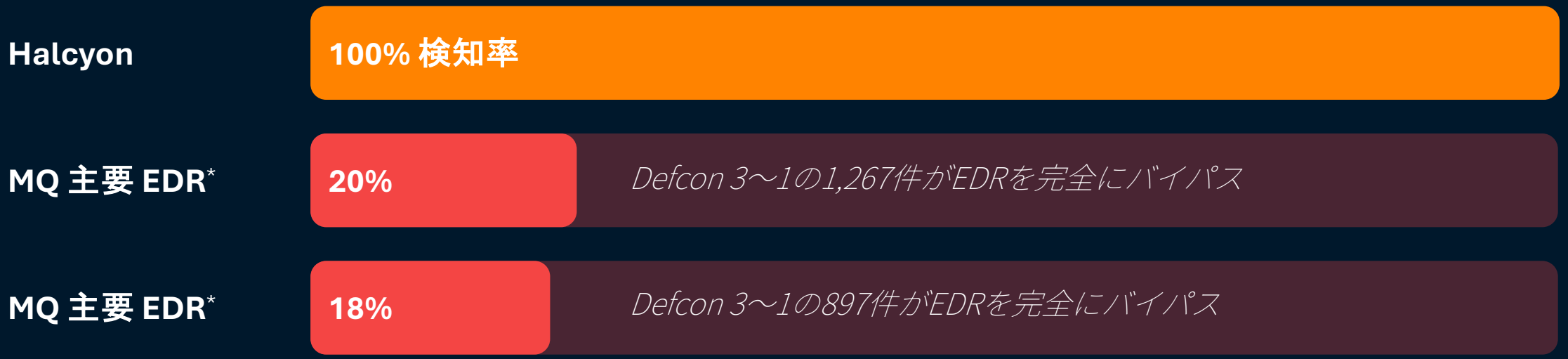
1	Qilin	2,298 組織
2	Akira	1,721 組織
3	Clop	1,091 組織
4	Play	1,026 組織
5	RansomHub	971 組織
6	SafePay	804 組織
7	Lynx	667 組織
8	DragonForce	504 組織
9	IncRansom	467 組織
10	Medusa	420 組織
11	Sinobi	415 組織
12	INC Ransom	410 組織
13	FunkSec	347 組織
14	KillSec3	334 組織
15	Everest	313 組織

EDR バイパス検知

すり抜けた脅威も、逃がさない

VirusTotal検知率が低い最高重要度サンプル（DEFCON 3〜1）を、Gartner社マジック・クアドラント（ Magic Quadrant™ ）掲載の主要EPP/EDRツールと比較検証。

※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

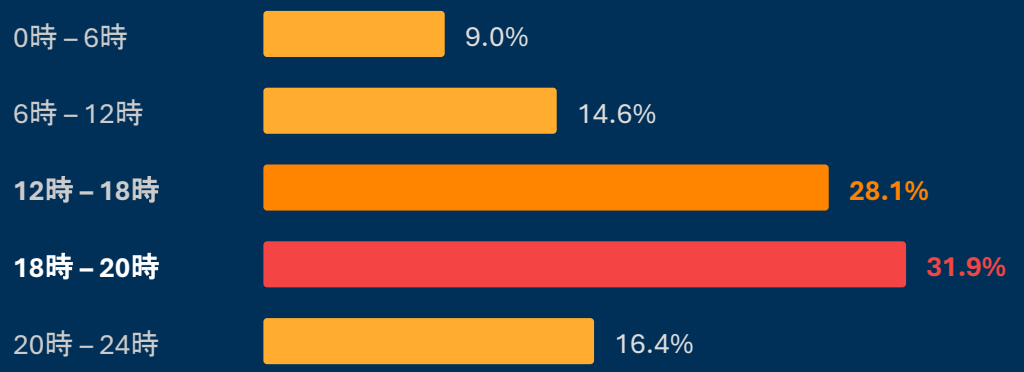
検知は平日を通じてほぼ均等に分布するが、ITおよびセキュリティ担当者が最も手薄になる交代時間帯に急増する。

17%
週末のアラート

午後7時
ピークアラート時間帯 (EST)

水曜日
最も多い曜日(18.6%)

時間帯別検知数 (EST)



曜日別検知数

Halcyon ROCが24時間365日監視するので、御社のチームが張り付く必要はありません。

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