CYLANCE CONSULTING

# ランサムウェアの予防と修復

次の被害者にはならないために

## この脅威には次の特性があります。

- 通常は従来のスピアフィッシングや水飲み場型の攻撃ベクトルを使用しない
- 脆弱な公開サービスが利用されるため、攻撃者は手動で横移動して持続性を維持できる
- 数台のホストのみではなく、ネットワーク全体を覆って暗号化する
- ネットワーク内のバックアップシステムを標的にし、アーカイブを暗号化するのではなく削除して、被害者がリソースをほとんどまたはまったく使用できないようにする [1]

SamSam ( 別名 Samas、Samsa) ランサムウェアは業種固有ではない新世代のランサムウェア

[1] 2016 年 3 月 25 日に FBI が特定の団体 (TLP:GREEN) に配布した FBI FLASH MC-000070-MW

## 今日のランサムウェア脅威環境

今日のランサムウェア攻撃は、従来のものとはかなり異なります。ランサムウェアはハッキングスキルがほとんど、またはまったくない攻撃者でも簡単に入手してうまく使用できるため、Ransomware as a Service (RaaS) と呼ばれることがあります。その一方で、ランサムウェアが単なる身代金要求以外にも使用される事例が見られます。たとえば、相手の気をそらすために使用されたケースがあります。まず、後で使用するために認証情報を奪い、次にドライブを暗号化して IT スタッフが対応にかかりきりになるようにし、その間に攻撃者は自分の足跡を消し、より悪質な目的を達成するというものです。さらに最近では、組織のネットワーク全体を暗号化し、暗号化前にホストのバックアップを削除し、組織全体を人質に取って業務ができないようにするという、きわめて日和見的な攻撃も見られます。

Cylance® では、企業がこの進化する脅威に対処できるように 2 つの補完的サービスを提供しています。

## 事前予防および対応準備

Cylance は、予防、ネットワークアーキテクチャ、社内 IR ワークフロー、脆弱性およびパッチ管理のベストプラクティスと、攻撃者が足がかりに使用する社内ホストと公開サービスの両方について評価を提供します。

ランサムウェアに関して言えば、最良の対策は予防と対応準備です。ひとたび実行されると、ビジネス上のコストとリスクが急激に高まります。ランサムウェアに対して十分な準備をしている組織は、総じて IT インシデントによるビジネスへの影響を最小化できています。

ランサムウェア感染への対応に特化された Cylance の事前予防および対応準備サービスの特長 :

- 機械学習と人工知能 (AI) の能力を活かして、予測 / 自律型の実行前予防が可能
- 深い専門知識を持つ、世界で高い評価を受けているコンサルタントがランサムウェア攻撃の修復を促進
- 攻撃が発生する前に、最適な準備、予防テクノロジー、およびワークフローを整えられるように知識移転

## 関連サービスおよび製品

### 産業制御システム

- ICS インフラストラクチャ評価
- ICS セキュリティ侵害評価
- ビルディングオートメーションシステム
- 制御システム向けインシデント対応サービス

### IoT/ 組み込み

- IoT および組み込みシステムのインシデント対応
- 組み込みシステムの侵入テスト

### ThreatZERO™

- ThreatZERO+ セキュリティ侵害評価
- ThreatZERO 専任エキスパート

### ヘルスケア

- 臨床情報セキュリティプログラム開発
- 臨床アプリケーションセキュリティ評価
- 医療機器リスク評価
- 政府のコンプライアンス

### トレーニング

- カスタムインシデント対応およびフォレンジックトレーニング
- ICS セキュリティの基礎 インシデント対応およびセキュリティ侵害評価
- マルウェアおよびインシデント対応リテーナーサービス
- インシデント対応準備評価
- 緊急インシデント対応

### エンタープライズセキュリティサービス

- 社内 / 社外侵入テスト
- ソーシャルエンジニアリング
- Web アプリケーション評価

## 今日のランサムウェア脅威環境

ランサムウェアはそれぞれ異なります。亜種が 1 つリリースされるとすぐに、大量の「模倣」亜種が出現します。その中には、まったく異なる暗号化アルゴリズムと鍵交換を使用するものや、依然として新しいコマンド & コントロールインフラや異なる攻撃ベクトルを使用するものもあります。場合によっては、組織が IR サービスを要求する必要が生じます。このような場合に判断を迅速に下し、すばやく封じ込めを行うには、組織化されたプロセスとカスタム開発されたツールが用意された環境で経験のある担当者が対応することが重要です。

Cylance IR チームが処理した IR 案件は、昨年だけでも数百件に上ります。このチームは、現在行われている攻撃についてセキュリティ侵害を示す重要な指標を突き止めるエキスパートであり、Cylance の機械学習と AI エンジンを直接利用して IR プロセス中に即時封じ込めを行います。そのためにエージェントをインストールしたり、背後にいる攻撃者に情報が漏れたりすることは一切ありません。

ランサムウェア侵害に対応する際の目標は同じです。組織のリスクとコストを軽減し、できるだけ早く業務を復旧することです。さらにこのすべてを水面下で目立たずに、迅速かつ断固として行います。

Cylance Consulting は、マネージドサービスプロバイダの関与やネットワーク上に常駐するエージェントなしで即時封じ込めに注力します。脆弱性を除去し、永久に外部にさらされないようにします。将来的にお客様がインシデントを含む組織を迅速に検知し、発生を予防できるようにします。

ランサムウェア侵害に対する Cylance のインシデント対応、迅速な封じ込め、およびリスク軽減の特長 :

- 年間数百件もの IR 案件を処理するこの分野のエキスパートが担当
- カスタム開発されたツールで今日の高度なランサムウェアに特化して対応
- 組織化された独自の対応ワークフローで迅速に攻撃を識別して封じ込め
- ランサムウェア分析により特定の側面が侵入可能かどうか判断し、身代金支払いを回避
- 攻撃の終盤では背後にいる攻撃者との交渉を支援
- AI の利用により、背後にいる攻撃者に情報を与えかねないホストベースのエージェントのインストールが不要

Cylance Japan株式会社
〒100-6510
東京都千代田区丸の内1-5-1　新丸の内ビルディング10F
www.cylance.co.jp
03-6386-0061 (代表)



20160623-1804