

「即調査」詳細解説レポート — 香港 AS9269・ポート4444 クラスタ

asset-observatory | scan#004 要調査キュー上位3件 | 対象: 183.179.230.x / 183.179.141.x / 183.178.96.x | 判定: FP (C2非該当)

要旨: 週次観測で最高スコア (120点・Tier1/即調査) に達した香港の3ホストを人手で精査した。発火要因は **cert_shared_multi_ip** (証明書共有) と **cluster_density** (クラスタ密集) の二重ヒット。調査の結果、共有されていた TLS 証明書は **pfSense** の初期自己署名証明書であり、本件は **C2 (指令サーバ)** ではなく、同一テンプレートから複製されたファイアウォール機器群と判定した (フォールスポジティブ)。ただし「同一構成の量産ホスト群」という観測事実は記録価値があるため保持する。

1. 検出内容 (何がキューに上がったか)

3ホストは以下の共通属性を持ち、いずれも合計スコア **120点** (証明書共有80+クラスタ密集40) で **Tier1 / 即調査** に分類された。

属性	値
IP:ポート	183.179.230.x:4444 / 183.179.141.x:4444 / 183.178.96.x:4444
ASN・国	AS9269 (香港)
共有 TLS 証明書	d2f2a774...
証明書 Subject	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6a79...
発火ルール	cert_shared_multi_ip (80点) + cluster_density (40点)

ASN (エーエスエヌ/Autonomous System Number=自律システム番号)

インターネットを構成する「ネットワークのかたまり」に割り振られた番号。ISP やホスティング事業者などが単位。同一 ASN 上に対象が集中していれば「同じ事業者のネットワークに並んでいる」ことを示す。AS9269 は香港の一事業者。

ポート (port=通信の出入口番号)

1台のホストは番号付きの多数の通信窓口を持つ。443=HTTPS、22=SSH など用途が慣習化している。**4444** は侵入テストフレームワーク **Metasploit (メタスプロイト)** の既定リスナーポートとして知られ、攻撃インフラの疑い符号として最初に注目される番号。

2. 発火要因の技術的解説

2-1. cert_shared_multi_ip（証明書共有）－ 80点

複数の異なる IP が**同一の TLS 証明書**を提示している状態を検出するルール。攻撃基盤の相関分析（ピボット）で最も強い手がかりの一つ。

TLS証明書（ティーエルエス証明書／Transport Layer Security certificate）

暗号化通信（HTTPS 等）で、サーバが「自分が何者か」を示すために提示するデジタル証明書。内部に発行者・主体（Subject）・有効期限・**フィンガープリント（指紋）**などを含む。

フィンガープリント（fingerprint＝指紋。SHA-256 等のハッシュ値）

証明書全体を一定の計算（ハッシュ関数）で短い固定長の値に変換したもの。証明書が同一なら指紋も一致する。d2f2a774... がそれ。**別々の IP が同じ指紋を出す＝物理的に同じ証明書ファイルを使い回していることを意味する。**

ピボット（pivot＝軸足を移した横断調査）

1つの指標（証明書・ドメイン・JARM 等）を軸に、関連する別の資産へ次々にたどる相関手法。「証明書 X を共有する IP 群」を芋づる式に洗い出すのが典型例。単体スキャンでは見えない“同一運用”を可視化する。

本件では、地理的・ASN 的に別個に見える 3 IP が同一証明書を共有していたため、「同一の主体が一括運用するインフラ」の疑いとして高スコアが付いた。**この判断ロジック自体は正しく機能している。**

2-2. cluster_density（クラスタ密集）－ 40点

同一 ASN 上に同一ポートが一定数以上（既定 6 台以上）集中している状態を検出するルール。ボットネットや量産型の攻撃基盤は、同一事業者上に似た構成を大量展開する傾向があるため、その密度を加点する。

ボットネット（botnet＝乗っ取られた機器群の集合）

攻撃者に制御された多数のホストの集合。指令は **C2** から配られる。同一構成が広域に分散するのが特徴で、「同一 ASN・同一ポートの密集」はその兆候になり得る。

C2（シーツ－／Command and Control＝指令統制サーバ）

攻撃者がマルウェアやボットに指令を送り、結果を受け取る中枢サーバ。**Cobalt Strike**（ポート50050）、**Metasploit**（ポート4444）などのフレームワークが既定ポートを持つため、それらのポート＋証明書/JARM の一致で C2 を推定する。

本件は AS9269 上にポート4444が8台集中しており、この条件にも合致した。証明書共有との二重ヒットで 120 点に達した。

3. 人手調査の所見

共有証明書の **Subject（主体情報）** を精査したところ、決定的な手がかりが得られた。

0=pfSense GUI default Self-Signed Certificate / CN=pfSense-6a79...

pfSense（ピーエフセンス）

FreeBSD ベースのオープンソースファイアウォール／ルーター OS。企業・個人で広く使われる正規ソフトウェアであり、攻撃ツールではない。Web 管理画面（GUI）を持ち、導入時に管理用の証明書を自動生成する。

自己署名証明書（じこしょめい／Self-Signed Certificate）

公的な認証局（CA）ではなく**自分自身で発行した証明書**。pfSense は初期状態でこれを自動生成し、GUI の HTTPS に用いる。正規かつ一般的な運用であり、それ自体は不審ではない。

3-1. なぜ3台が同一証明書だったのか

pfSense は本来インストールごとに異なる証明書（CN のランダム部が変わる）を生成する。にもかかわらず 3 台が CN=pfSense-6a79... で完全一致していた。これは次を強く示唆する。

- 1 台を構築後、**ディスクイメージ／VM を複製**して 3 台に増やした（証明書を再生成していない）。
- 結果として、本来ユニークであるはずの証明書指紋まで複製され、3 台が同一 fingerprint を持つに至った。

ポートが 3 台とも 4444 のみである点も、量産テンプレートの一律設定と整合する（pfSense GUI の既定は 443 のため、4444 は運用者が意図的に変更した非標準構成）。

4. 判定と根拠

判定：フォールスポジティブ（False Positive／FP＝誤検知）

共有されていたのは攻撃基盤の証明書ではなく **pfSense の初期自己署名証明書**であり、ポート4444も C2 リスナーではなく複製された管理画面であった。したがって本 3 件は **C2 には該当しない**。

フォールスポジティブ（False Positive／FP＝偽陽性・誤検知）

「危険」と判定したが実際は無害だったケース。逆に、危険を見逃すのは **フォールスネガティブ（False Negative／FN）**。検知システムは両者のバランス調整が要点で、FP は除外ルール（suppress）の学習で減らす。

記録価値：C2 ではないが、「香港 AS9269 上に、同一テンプレートから複製された pfSense 群が並存する」事実は観測記録として保持する。量産 VPS 環境・一括構築されたゲートウェイ群などを示す可能性があり、将来の傾向分析の素材になる。

5. システムへの反映（学習）

本調査により、**pfSense 初期証明書は正常ホストが日常的に提示するノイズ源**であることが確認された。これを除外ルール（suppress）に登録すれば、同種の FP が自動的にスコア対象外となり、**真正な C2 証明書共有のみが即調査に残る**。人手調査の結果を継続的に規則へ還元することで、キューの精度は週ごとに向上する。

suppress (サプレス=抑制・除外リスト)

正常な揺らぎや既知の無害パターンをスコア対象から外す仕組み。CDN・主要クラウド・既知の正規証明書などを登録し、分母から除くことで要調査キューの S/N 比 (信号対雑音比) を高める。

6. 用語集 (本レポート初出順)

ASN (エーエスエヌ / Autonomous System Number)

ネットワークのかたまりに割り振られた番号。事業者単位の識別子。

ポート (port)

ホストの通信窓口番号。4444=Metasploit 既定、50050=Cobalt Strike 既定、443=HTTPS など。

TLS 証明書 (Transport Layer Security certificate)

暗号通信でサーバの身元を示すデジタル証明書。

フィンガープリント (fingerprint)

証明書をハッシュ化した固定長の指紋値。一致=同一証明書。

ピボット (pivot)

1 指標を軸に関連資産を横断的にたどる相関手法。

C2 (シーツ / Command and Control)

攻撃者の指令統制サーバ。

ボットネット (botnet)

攻撃者に制御された多数ホストの集合。

Metasploit (メタスプロイト)

侵入テスト用フレームワーク。既定リスナーがポート4444。

Cobalt Strike (コバルトストライク)

商用の攻撃シミュレーション基盤。既定ポート50050。悪用も多い。

pfSense (ピーエフセンス)

オープンソースのファイアウォール/ルーター OS。正規ソフト。

自己署名証明書 (Self-Signed Certificate)

認証局を介さず自分で発行した証明書。pfSense が初期生成する。

フォールスポジティブ (False Positive / FP)

誤検知。危険と判定したが無害だったケース。

suppress (サプレス)

既知の無害パターンをスコア対象から外す除外リスト。

本レポートは asset-observatory scan#004 要調査キュー上位3件に対する人手調査の詳細記録である。判定：FP (C2非該当) / 記録区分：pfSense 複製クラスタとして保持 / 推奨対応：suppress へ pfSense 初期証明書を登録。