初期アクセス	実行	権限昇格	防御回避	認証情報取得	偵察	水平移動・内部活動	データ流出	コマンド＆コントロール	影響
T1190 - 公開向けアプリケーションの脆弱性悪用 主に Ivanti Connect Secure アプリケーションの既知の複数脆弱性を悪用します。 T1189 - ドライブバイ侵害 ユーザが複数のクラックソフトをダウンロードしており、信頼できない供給元からのマルウェア感染の可能性を示しています。 T1078 - 有効なアカウント 侵害したアカウントを用いて悪意ある活動を継続的に行っています。	T1059.003 - コマンドおよびスクリプトインタプリタ：Windows コマンドシェル 攻撃者はコマンドラインを利用して、Cobalt Strike 等のツールからコマンドやペイロードを実行しています。	T1078.002 - 有効なアカウント：ドメインアカウント DragonForceは盗まれたドメイン管理者資格情報を悪用してアクセスを維持しています。これらのアカウントによりシステム横断的な持続的アクセスが可能となり、新規ユーザ作成、ポリシー変更、マルウェア展開がアラートを上げずに実行され得ます。	T1562.001 - 防御機能の阻害：ツールの無効化または変更 BYOVD手法の利用により、攻撃者は脆弱なドライバを悪用してセキュリティプロセスを停止し、検出を回避しています。	T1003.002 - OS認証情報ダンプ：Security Account Manager (SAM) T1003.001 - OS認証情報ダンプ：LSASSメモリ MIMIKATZやLaZagneを用いた認証情報のダンプが行われています。	T1595.002 - アクティブスキャン：脆弱性スキャン 特定のIPアドレスから脆弱性スキャンが実行されており、悪用準備が行われていることを示しています。 T1087 - アカウントの検出 攻撃者は AdFind を使用してアカウント、リモートシステム、グループの探索を行いました。 T1018 - リモートシステム検出 ネットワーク上の他コンピュータを発見するために AdFind や Advanced IP Scanner が継続的に使用されました。 T1069.002 - 権限グループの検出：ドメイントラスト 攻撃者は AdFind を利用してドメイントラストや組織単位を列挙しました。 T1016 - システムネットワーク構成の検出 AdFind や Netscanold.exe のようなツールを用いたネットワークおよびアカウントの検出、PassView やレジストリハイブダンプによる認証情報の探索が行われました。	T1021.001 - リモートサービス：リモートデスクトッププロトコル（RDP） RDPを用いたリモートアクセスおよび横移動が行われています。	T1567.002 - クラウドストレージへの流出 攻撃者は MEGA 等のファイルストレージを悪用し、盗取情報をクラウド上にアップロードしている報告があります。	T1105 - ツールの持ち込み (Ingress Tool Transfer) 攻撃者はスクリプトや偵察ツールを侵害されたシステムへ転送し使用しました。 T1071.001 - アプリケーション層プロトコル：Webプロトコル HTTP/HTTPS 等を用いて各種コマンド＆コントロール（C2）サーバへリクエストを送信しています。	T1486 - 影響を与えるためのデータ暗号化 ランサムウェアバイナリを実行してシステム上のデータを暗号化します。 T1490 - システム復旧の阻害 ボリュームシャドウコピーの削除や起動時復旧機能の無効化を行い、システム復旧を困難にします。 T1489 - サービス停止 BYOVD を使用してサービスを停止し、検出を回避する可能性があります。