

戦術	手法	説明
初期侵入 (Initial Access)	T1190 - 外部公開されたアプリケーションの悪用	Nmapを介してFortiGateサーバおよび管理者アカウントが侵害される
	T1078.002 - 有効なアカウント: ドメインアカウント	侵害されたドメインアカウント
事前調査 (Discovery)	T1046 - ネットワークサービスの探索	サービスの探索にNmapが用いられる
	T1018 - リモートシステムの探索	ネットワークの関連付けにAdvanced IP Scannerが用いられる
	T1087.002 - アカウントの探索: ドメインアカウント	複数のドメインアカウントを取得するためにバッチスクリプトが用いられる
	T1069.002 - パーミッショングループの探索: ドメイングループ	ドメイングループが列挙される
	T1482 - ドメインの信頼関係の探索	プライマリドメインコントローラを識別するためにPowerShellコマンドが実行される
実行 (Execution)	T1059.003 - コマンドとスクリプトインタプリタ: Windowsコマンドシェル	コマンドプロンプト (cmd.exe) を通じて様々なコマンドが実行される
	T1059.001 - コマンドとスクリプトインタプリタ: PowerShell	セキュリティソフト無効化ツールやランサムウェアを展開するためにPowerShellコマンドが用いられる
検出回避 (Defense Evasion)	T1562.001 - 防御策の無効化: ツールの無効化/変更	セキュリティソフト無効化ツールによりセキュリティプロセスに関連するサービスが停止される
	T1014 - ルートキット	プロセスを強制終了するために脆弱なドライバが展開される
	T1112 - レジストリの変更	認証方法を弱体化させるためにレジストリが変更される
	T1562.004 - 防御策の無効化: システムファイアウォールの無効化/変更	リモートデスクトップ接続のためにファイアウォールの設定が変更される
	T1027 - ファイルまたは情報の難読化	Base64でエンコードされたPowerShellコマンドが実行される
権限昇格 (Privilege Escalation)	T1484.001 - ドメインまたはテナントポリシーの変更: グループポリシーの変更	グループポリシーオブジェクトを通じてドメイン全体のセキュリティ侵害が実行される
不正活動の永続化 (Persistence)	T1219 - リモートアクセスソフトウェア	リモートアクセスのためにAnyDeskがインストールされる
	T1112 - レジストリの変更	不正活動を永続化させるためにレジストリが変更される
内部活動・情報探索 (Lateral Movement)	T1021.002 - リモートサービス: SMB/Windowsの管理共有	内部活動のためにPSEXECが用いられる
	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	レジストリの変更によりリモートデスクトップ接続が有効化される
	T1021.004 - リモートサービス: SSH	Secure Shell (SSH) を介した内部活動にPuTTYが用いられる。
情報収集 (Collection)	T1074.001 - データの一時的保存: ローカルデータの一時的保存	データがC:\ProgramData\data内に一時的に保存される
	T1039 - ネットワーク上の共有ドライブから収集されたデータ	内部リソースに対してWebDAV接続が用いられる

コマンド&コントロール (Command & Control)	T1219 - リモートアクセスソフトウェア	C&Cサーバとのやり取りにAnyDeskが用いられる
	T1071.001 - アプリケーション層のプロトコル: Webプロトコル	C&Cサーバとのやり取り/データ移行のためにWebDAVが用いられる
情報送出 (Exfiltration)	T1048.001 - 代替プロトコルを用いた情報送出: C&C通信経路とは異なる、対称鍵暗号を用いたプロトコルを介した情報送出	データを送出させるためにWinSCPが用いられる
影響被害 (Impact)	T1486 - Data Encrypted for Impact 影響を与えるためにデータの暗号化	NETLOGON共有を介してランサムウェアが展開される
	T1489 - サービスの停止	セキュリティサービスが強制終了される