

表 1. APTグループ「Earth Preta」の攻撃キャンペーンから観測された主な事例のタイムライン

対象期間	主要な出来事
2012 – 2016	<p>Earth Preta グループの初期の攻撃活動と用いた基本ツール</p> <p>Earth Pretaグループは、当初PlugX/Korplug RATを用いた攻撃活動を開始し、標的型フィッシングメールに不正ファイルやおとり文書を添付して送信しました。同グループが用いたC&Cサーバの構成は単純で、最小限の難読化を施したC&Cサーバに直接接続し、実行処理や不正活動の永続化には、ごく一般的なDLLサイドローディングを用いました。当時は主にアジア太平洋地域のNGO（非政府組織）、政策研究機関、政府関連機関を標的としていました。</p>
2017 – 2019	<p>より巧妙化した配信チェーン</p> <p>左記の期間、Earth Pretaグループは、政策・外交を主題としたフィッシング攻撃を仕掛けるようになりました（これについて、サイバーセキュリティ企業「ReliaQuest社」が解説しています）。初期侵入の手口としては、ZIP/RARアーカイブや悪意あるショートカットファイルを度々用いました。インフラ面では、C&Cサーバ（IPアドレス）の変更が増加したほか、モジュール型ローダの採用により、ステルス性の高まりが若干確認されました。</p>
2020 – 2022	<p>複数地域における攻撃範囲の拡大と強化されたC&Cサーバインフラ</p> <p>Earth Pretaグループは、ヨーロッパ地域にも攻撃範囲を拡大させたほか、ローダを多段階に展開する攻撃チェーンを高度化させました。具体的には、C&Cサーバとの暗号化通信、難読化レイヤー、PlugXの変種（Hodurなど）が追加されました。左記の期間は、標的型かつ長期的な諜報活動を主とした攻撃キャンペーンへの移行期と言えます。TrendAIの公開記事（2023年5月18日）では、同グループが用いるPlugXの高度化などについて解説しました。</p>
2023	<p>モジュラー型バックドアと長期的な不正アクセス</p> <p>Stately Taurusグループなどが実施した攻撃キャンペーンでは、モジュラー型ペイロードを実行するためにマルウェア「DOPLUGS」やローダ「PubLoad」を用いて東南アジア地域の政府機関へと侵入する手口が浮き彫りとなりました（これについて、サイバーセキュリティ企業「Cyfirma社」が解説しています）。これらの攻撃者集団の情報収集対象範囲は拡大し、エネルギー業、製造業、大学業界、海事産業など、政策・戦略的価値に関連するシステムも標的となりました。</p>
2024	<p>プロキシベースのインフラとステルス性の高まり</p> <p>Earth Pretaグループは、Beacon通信の隠蔽やC&Cサーバの通信経路の変更にマルウェア「StarProxy」を採用しました。FakeTLSによる暗号化通信を用いるバックドア「ToneShell」と併用することで検出を困難にしました。当C&Cサーバのスタックは、階層化されたバックドア構造を持つプロキシへと高度化しました。TrendAIの公開記事（2025年3月3日）では、マルウェア「DOPLUGS」/バックドア「ToneShell」が採用された攻撃キャンペーンやステルス活動について解説しました。</p>
2025	<p>USBワームとエアギャップ環境への侵入能手口</p> <p>Earth Pretaグループが最近実施した攻撃活動では、USB経由で自己拡散するワーム「SnakeDisk」が確認されました（これについて、IT企業「IBM社」が解説しています）。当マルウェアは、バックドア「Yokai」や更新版バックドア「ToneShel」を拡散させるためのもので、エアギャップ環境やアクセス制限されたネットワークへの侵入を可能にします。初期侵入は、依然として標的型フィッシングメールの添付ファイル経由が一般的で、次いで、DLLサイドローディング、コマンド/スクリプトインタープリタによる実行、そしてステルス性を高めるためにC&Cサーバには暗号化通信が用いられました。</p>