本レポートの主要な知見

ランサムウェアの脅迫戦術は進化しています。**最も新しい戦術は四重脅迫**ですが、現在のところ最も一般的な戦術は、二重脅迫です。また、ランサムウェアグループは、被害者に圧力をかける、あるいはコンプライアンスを武器に使うなど、利益を生み出すための新たな方法を模索し続けています。

ランサムウェアグループが使用する TrickBot マルウェアファミリーに関連するマルウェアにより、**7 億 2,400 万米ドル以上の暗号資産（仮想通貨）が脅し取られました。** Akamai Hunt Team は最近、5 つの顧客資産上でスケジュールされた 4 つの悪性タスクにこのマルウェアが関連していることを発見しました。

FunkSec のようなグループが示しているように、**生成 AI と LLM を使用することで、**技術的な専門知識があまりない個人でも高度なキャンペーンを開始できるようになり、**ランサムウェア攻撃の頻度が高まり、規模も拡大しています**。

RaaS プラットフォームを活用して影響力を高めているハイブリッド・ランサムウェア・ハクティビスト・グループ（CyberVolk、Stormous、KillSec、Dragon RaaS、DragonForce など）の出現は、ランサムウェアの情勢が大きく変化し、**政治的動機や思想的動機が金銭目的の犯罪と絡み合うようになっている**ことを示しています。

ハクティビストグループである Head Mare、Twelve、NullBulge は、政治的混乱を引き起こすために LockBit ランサムウェア（流出したビルダーまたは公開されているビルダーから構築）を頻繁に使用します。NullBulge は特に、**AI やオンラインゲームツールで動作するオンラインコミュニティやプラットフォームを標的にしています**。

クリプトマイナーには特有の危険がありますが、その目的や実践する戦略は前述のランサムウェアグループと類似しています。注目すべきは、**Akamai が分析したクリプトマイニング攻撃の約 50% が非営利団体や教育機関を標的としていた**ことです。その理由は、これらの組織が多くの計算リソースを所有していることと、他の業界よりもセキュリティが弱いことであると考えられます。