Thanos ランサムウェアを先制防御
2020 年 9 月 24 日 Minerva のブログから

Thanos ランサムウェアは 2019 年の後半に見られた比較的新種なマルウェアです。ランサムウェアやビルダーはアンダーグラウンドで不法売買されている RaaS（Ransomware as a Service）のタイプになるかと思います。Palo Alto’s Unit 42 の報告によると中東諸国などでよく見かけられ攻撃が報告されています。

初期インジェクションは Powershell スクリプトを利用し、ネットワーク上に拡散していきます。よくある自給自足型の攻撃手法で利用される wmic コマンドを使用しラテラルムーブメント攻撃を達成させます。ランサムウェア攻撃は悪意のあるコードをローディングするために APC インジェクションを使います。

以下のイベントは実際に悪意のある Powershell スクリプトが Minerva Armor でブロックされたスクリーンショットです。

Minerva 製品（Minerva Armor）についてのお問い合わせは Pico Technologies（info@pico-t.co.jp）までお願い致します。