Minerva Vs Sekhmet Ransomware
2020 年 12 月 5 日 Minerva のブログから

Sekhmet(セクメト)ランサムウェアについてはそれほど知られていません。この亜種は 2020 年 5 月くらいから広がってきました。Sekhmet は身代金を支払わないと窃取したファイルを世間に公表すると脅迫します。

インターネット上で Sekhmet の感染手法などについての情報も参考になりますが、Minerva ユーザーは実際にこのランサムウェアがリモートデスクトップ経由でサーバーへ接続する際にドメイン認証情報を窃取され、ランサム攻撃を仕掛けようとしました。

Minerva はメモリーインジェクション攻撃手法で侵入を試みる Sekhmet ランサムウェアを先制防御しました。マルウェア自身がインメモリコードの自己解凍を試みた時、Minerva は先制防御しました。今回はこのイベントはお見せすることはできませんが、下記にあるイベントは、他のクライアントで Sekhmet ランサムウェアと同じ系統である Egregor ランサムウェアが攻撃を試みる際に Minerva が先制防御したイベントです。

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。