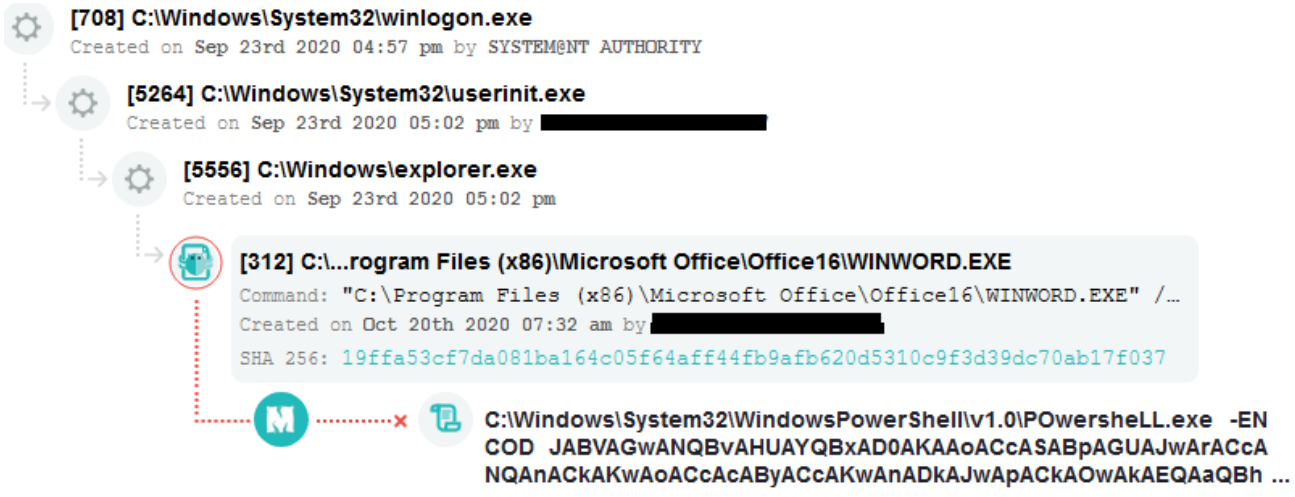
Emotet を即効で先制防御
2020 年 11 月 2 日 Minerva ブログから

Emotet はマルスパム攻撃の中でも最もアクティブに活動しており、Bleeping Computer コミュニティによれば Windows アップデートなどの偽メッセージ上に悪意のあるドキュメントを添付して送りつけてきます。 ドキュメントは PowerShell プロセスを実行させハードコーディングされた C2 サーバーへ接続され、さらに追加のペイロードがダウンロードされる仕組みになっています。このマルウェアの知識なく、Minerva Armor は悪意ペイロードを先制防御し、Emotet ローダーが侵入エンドポイントのディスクへダウンロードさせるのを完全シャットアウトしました。



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。