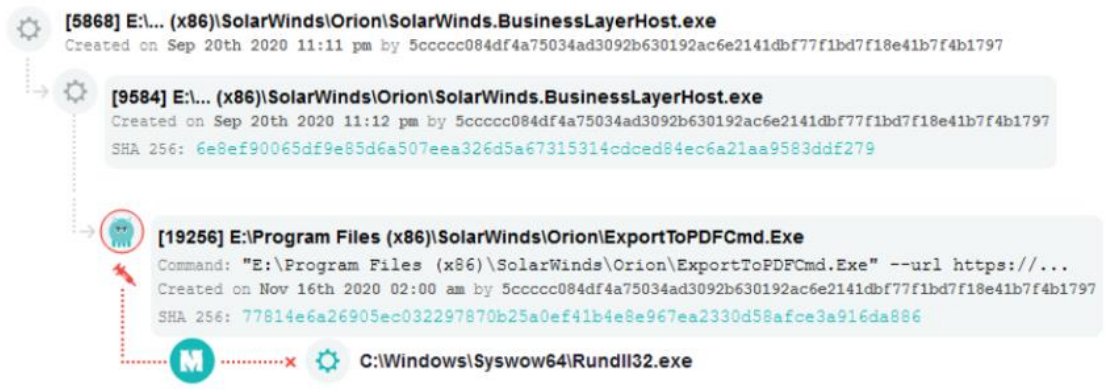

SolarWinds 社サイバー攻撃を Minerva が防御！
2020 年 12 月 20 日 Minerva ブログから

2020 年 8 月以来の数々のメモリーインジェクション攻撃を防御：Minerva 防御手法が改めて功を奏しました。

Minerva Labs 社は SolarWinds 社のサイバー攻撃について徹底的にレビューを行いました。リサーチの結果、過去数か月間で“SolarWinds.BusinessLayerHost.exe”というファイルから由来する数々の攻撃を封じ込めています。

Minerva リサーチチームによると、今回の攻撃は、現在のサイバー脅威として注視されるべきもので他社のセキュリティベンダーにも注意喚起を行いました。Minerva は 2020 年 8 月以来にこの攻撃を防御することに成功しました。

以下のプロセスイベントが実際にメモリーインジェクション攻撃試行であった例です。

Example #1:

Example #2:

セキュリティベンダーFireEye 社のレポートによると、ある特定のブラックリストプロセスがOS 上に発見された際に、悪意のバックドアーは攻撃実行を回避したとのことです。これはMinerva のマルウェア敵対環境モジュールによる先制防御結果です。

このモジュールは何万もの生成物(アーティファクト)はマルウェアが攻撃を実行する前にセキュリティ製品あるいはフォーレンジックツールなどをネットワーク内に仮想化して攻撃を仕掛けてくるのを防御するモジュールです(特許取得済)。

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。