Kaseya 社のランサムウェア攻撃は Minerva Armor で防御可能！
2021 年 7 月 4 日 Minerva のブログから

2021 年 7 月 2 日に事件は起こりました。Kaseya 社 VSA という製品は企業組織のソフトウェアをアップデート、ネットワークのリモート監視する製品で、VSA 製品を起動していたコンピューターに Revil ランサムウェアによって攻撃されました。このインシデントに対するインパクトは特に Kaseya 社の製品を担ぐマネージドサービスプロバイダー（MSP）にとって晴天の霹靂でなす術もなくランサム攻撃に晒されました。約 1000～1500 社が攻撃で影響を受け、2020 年 12 月起きた SolarWinds 社以来、大規模なサプライチェーン攻撃となりました。

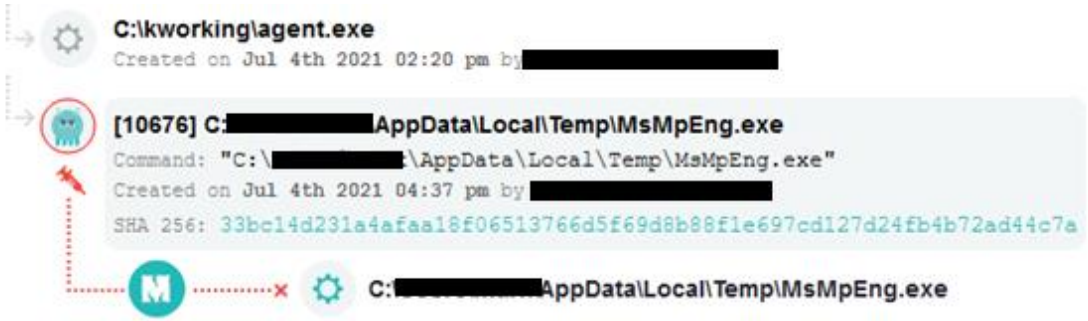
参考：Kaseya 社のランサムウェア攻撃について 1
参考：Kaseya 社のランサムウェア攻撃について 2

MSP が企業組織（エンドユーザー）の IT インフラストラクチャをシームレスに管理及び運用するためには顧客ネットワークへの特権アクセスが必要となります。今回は VSA 製品の脆弱性を突いた要因により攻撃グループはメーカーの VSA サーバーへハッキングに成功し、MSP から各企業組織へランサムウェア攻撃が仕掛けられてしまったという典型的なサプライチェーン攻撃の縮図でした。

攻撃者は“agent.exe”という悪意のファイルを仕掛け、旧 Windows Defender バイナリ

ーと“mpsvc.dll”という悪意のファイルをドロップできるように仕掛けていたようです。旧Windows Defender エクスプロイトが実行されると現行の Windows Defender は無効になり、“mpsvc.dll”内には仕掛けられていたメモリーが注入され攻撃されました。

Kaseya 社のある VSA ユーザーは Minerva Armor ユーザーでもあり、悪意の Defender エクスプロイトが実行される前に先制防御できたことが確認されました。



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。