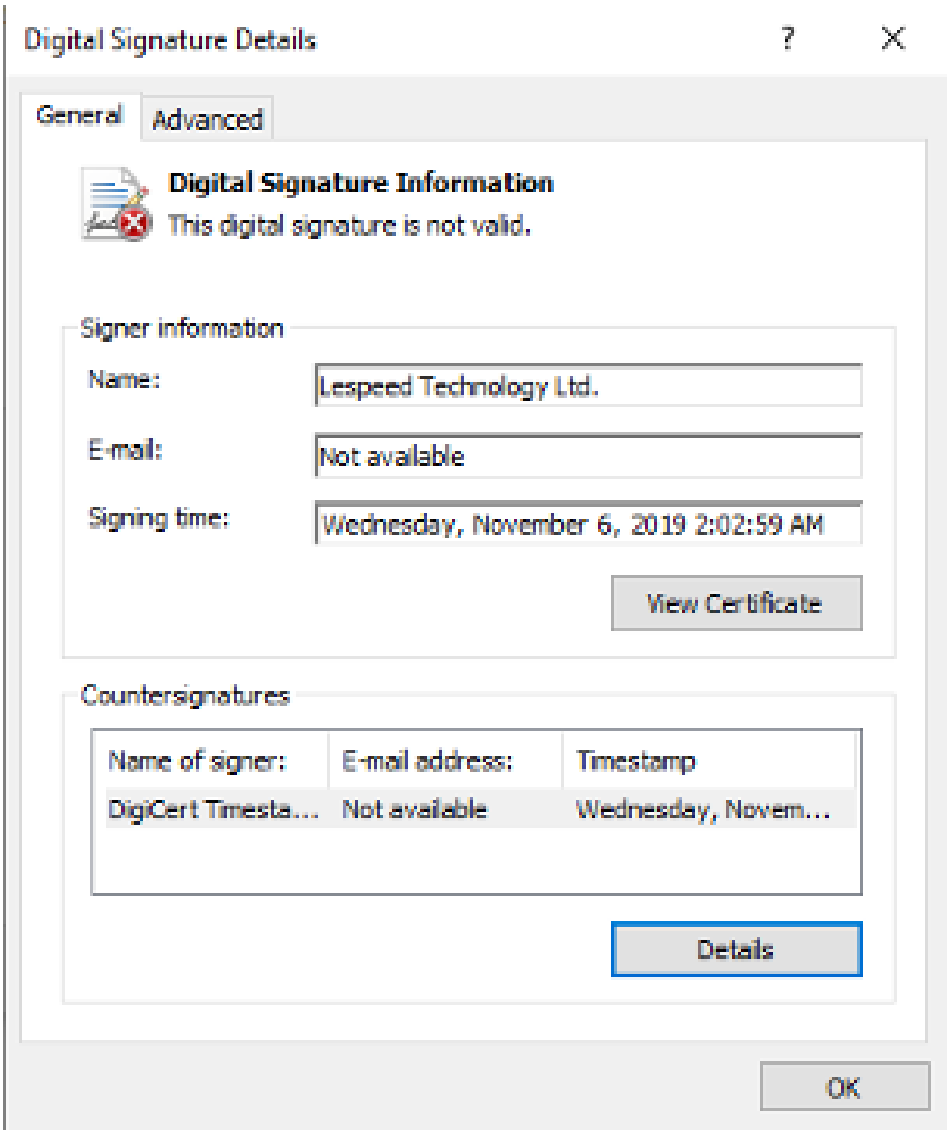
偽物インストーラーに仕組まれたマルウェアからの攻撃を先制防御
2020 年 10 月 20 日 Minerva のブログから

昨今、偽物インストーラーが増えてきており、遭遇する機会が増えてきています。開発するにも手間がかからず手離れの良いペイロード攻撃は典型的なマルウェアと位置付けられました。アンチウィルスベンダーの製品はこの種のマルウェアは早くて数時間、巧みなもので数日間後に検知されて登録されています。

最近の例として LideEx Converter というマルウェアで、偽物のインストーラーなどに埋め込まれています。Minerva 調査チームは、このマルウェアが Among Us というオンラインゲームの偽物インストーラーに埋め込まれていたのを確認しています。

バイナリーを分析すると Programs Files のディレクトリー内に LideEx Converter ディレクトリーが生成されていてペイロード攻撃を実行する LideEx.exe が格納されています。
攻撃が開始されると、この悪意あるソフトウェアは、感染している端末情報を C2 サーバーへ送信し、更にこのサーバーから付加的な悪意ペイロードを送り込みます。

偽物インストーラーは、Lespeed Technology 社発行の偽デジタル署名がされていました。



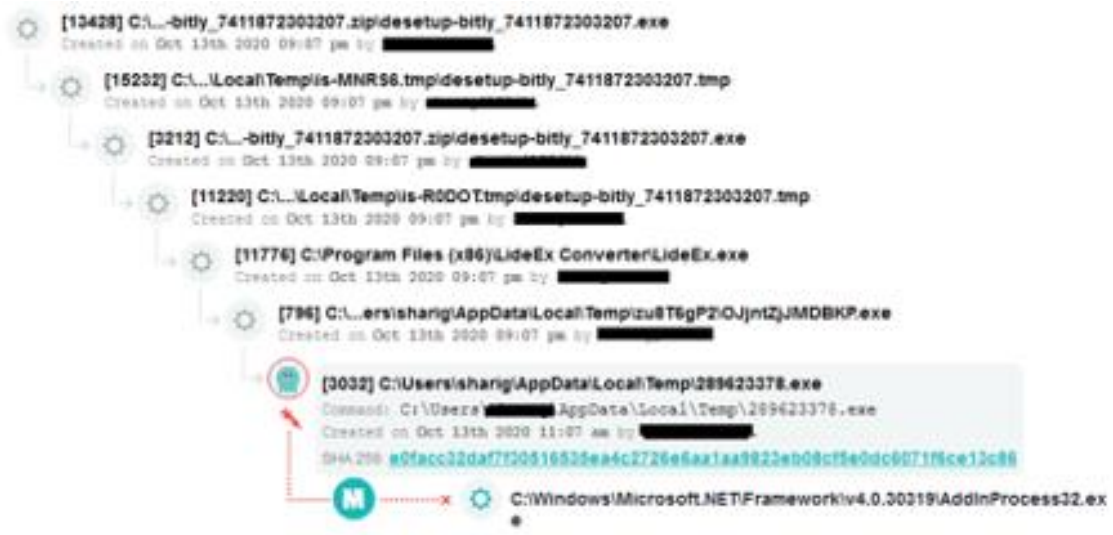
今回のケースではインストーラーは RedLineStealer というブラウザー上の認証情報や暗号資産を盗む悪名高いマルウェアが仕組まれていました。

この RedLineStealer ペイロード攻撃のテクニカル分析詳細については、Proofpoint 社のレポートが発表されています。

RedLineStealer は .NET インストーラーディレクトリー内に格納された addinprocess32.exe を調査すると子プロセスのインスタンスにペイロード攻撃を注入していることがわかります。注入されたペイロードは機密情報などを収集し、C2 サーバーへ送信

されます。サーバーアドレスはマルウェアのバイナリー上にハードコーディングされていました。

Minerva 製品は RedLineStealer のメモリーインジェクション攻撃を先制防御しました。



更に下の図の攻撃タイムラインには、Minerva がダウンローダーからの攻撃をマルウエアワクチン防御手法で先制防御しました。

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。