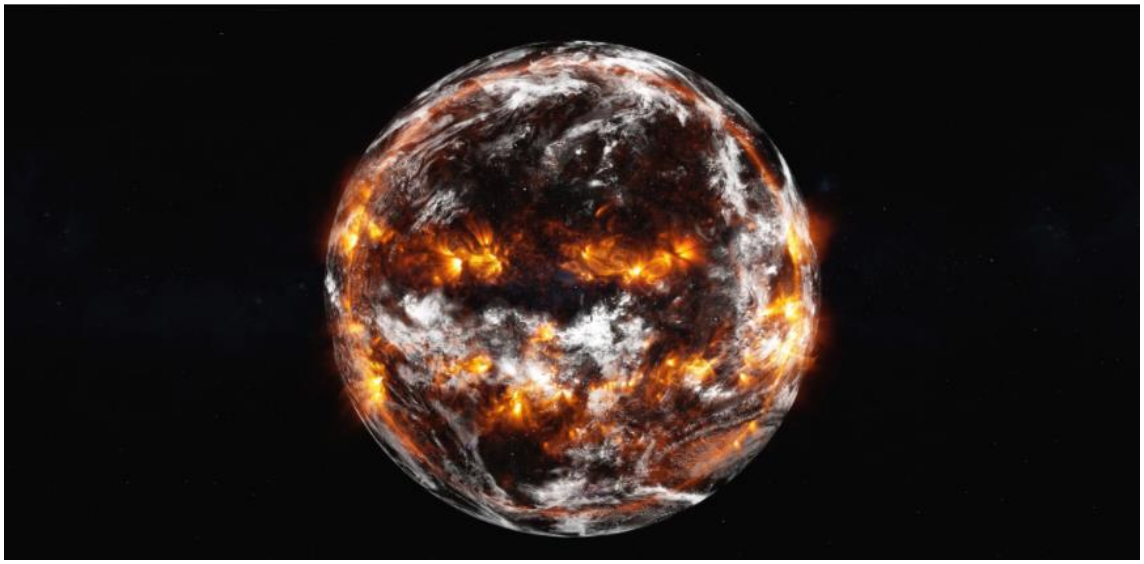

Jupyter Stealer マルウェアを難なく防御
2021 年 8 月 9 日 Minerva のブログから

Jupyter Stealer とは一般的に知られているバックドアを利用して機密情報などを盗む（Stealer）マルウェアが進化したものです。この Jupyter Stealer の最新バージョン版に出会う機会がありました。攻撃者はターゲットデバイスに対しペイロード攻撃のアップロード及び実行します。

Minerva 調査チームが分析した時は、YTD Video ダウンローダーと Video Converter などウエブ上から音楽と映像のソフトウェアに仕掛けられていることが判明しました。

このソフトウェアをダウンロードされると、密かに隠れている悪意の PowerShell が実行され、暗号化された PowerShell スクリプトがドロップされマルウェア感染を引き起こします。このマルウェアが実行されると、スクリプトはアルゴリズムを利用し攻撃の足掛かりをつくります。（この攻撃プロセスの詳細についてはこちら）

Minerva が調査した Jupyter 変種株は侵入後に C&C サーバーへ接続されターゲット PC 情報（暗号化状態で）をフィードバックします。ターゲット PC の認証情報はハードコーディング

された機能を詐取するのではなく、全機能モジュールを C&C サーバーからフィードされてしまいます。

このマルウェア特性の一つとして execute .exe と.ps1 ファイルをターゲット PC へアップロードします。この事象により、多種多様の攻撃手法が実行可能になるだけでなく、全情報を盗み取ることが可能になります。

Jupyter マルウェアが正当なツールを悪意に利用する攻撃に対し、Minerva の自給自足型攻撃防御テクノロジーにより防御することが可能です。下の図は防御した攻撃プロセスのチャートです。

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。