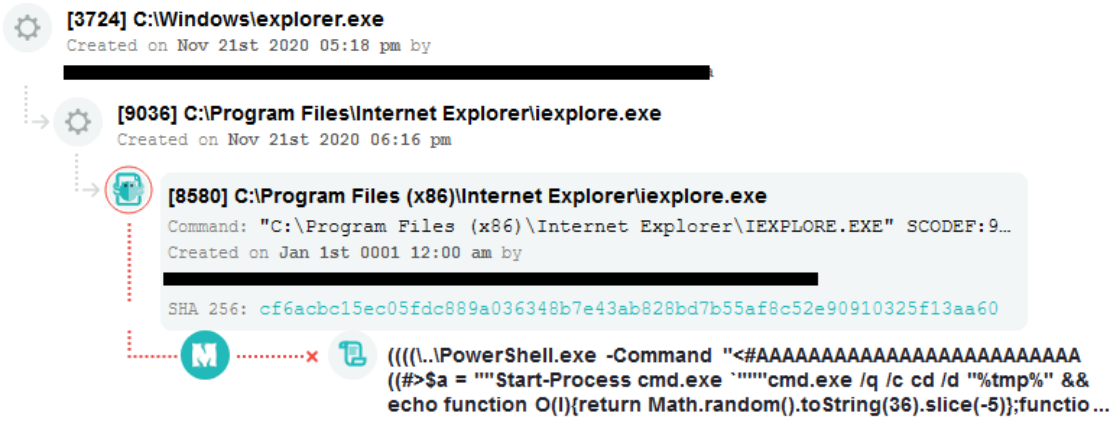

**Rig Exploit Kit 再上陸 - Minerva が攻撃を先制防御する**
**2020 年 12 月 21 日 Minerva のブログから**

Minerva 調査チームは最近 Rig Exploit Kit が再び到来していることを確認しました。この危険なマルウェアは 2015 年に確認され、それ以来セキュリティに脅威を与えています（Trustware の公表）。Minerva が初めてこのマルウェアに出会ったのは、Internet Explorer の脆弱性（version 11.00.9600.19178）による悪意のあるコマンドが実行されることに起因しています。

コマンドは Javascript ファイルをディスクへドロップすることで wscript プロセスによって実行されます。被害者にファイナルペイロードをダウンロードさせると、コマンドラインは C2 アドレスと連携し伝達されます。

Minerva は自給自足型攻撃防御手法でオペレーティングシステム機能を利用する Rig Exploit Kit 攻撃を仕掛けてきましたが、それを先制防御しました。下の図は Minerv ユーザーが実際に攻撃を仕掛けられ先制防御したイベントです。




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。