金融機関を狙うトロイの木馬 Gootkit を防御
2020 年 12 月 14 日 Minerva のブログから

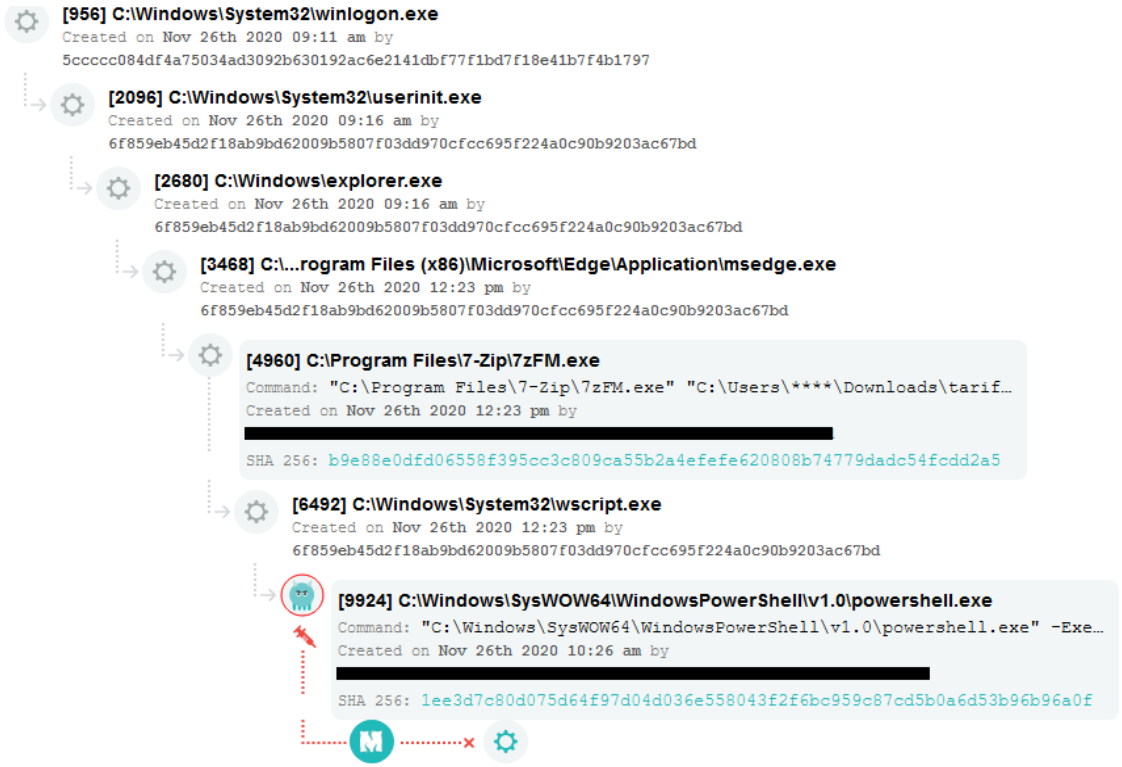
Malwarebytes リサーチチームのレポートによると、ドイツの金融機関を狙った Gootkit というトロイの木馬を利用し攻撃された全容を発表しました。このトロイの木馬は、HTTP を使ってリモートアドレスから追加コードをダウンロードする機能で悪意のある JavaScript を利用します。

その他にもメモリインジェクション攻撃なども実行されていることが確認されています。Malwarebytes はリポートの中で、いくつかの攻撃においてはトロイの最終ペイロード攻撃は REvil のランサムウェアであると結論づけています。

Minerva のあるユーザーは、実際に Gootkit トロイに攻撃を仕掛けられましたが攻撃を防御しました。その実際の攻撃コマンドラインを参照すると、PowerShell 経由でロードされた環境変数内に悪意のあるコードが仕掛けられていました。 下の図を参照ください。

Command Line:	"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -windowstyle hidden -Command "IEX([Environment]::GetEnvironmentVariable('adcadeefceac', 'User'))"

下の図は実際に起こったタイムライン攻撃のプロセスを示しています。



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。