Process Monitor を用いたマルウェアの動的解析

山下恭平、塚本覇虎、奥若菜

2022 年 5 月 17 日

1　テーマ

この実験では、擬似マルウェアツール ShinoBot と Process Monitor を用いたマルウェアの動的解析を行う。

2　環境

本実験は以下の県境において実験を行う。

- Virtual Box ・・・ 仮想環境、今回は Windows10 をインストールしている。
- Prosess Monitor ・・・ 動作しているプロセスを監視し、そのログを採取するソフト。
- ShinoBot ・・・ RAT(Random Access Tool) 型のマルウェアを再現したソフト、web 上に設置されたサーバから感染 PC を操作できる。

3　行なったこと

感染 PC の特定のァイルを ShinoBot から命令を送り削除した時のプロセスのログと、通常の削除のログを取り、双方のログを比較しながら、怪しいプロセスの特定を行った。

4　分かったこと

ShinoBot から送られてきた命令は「ShinoBot.exe → cmd.exe → cohost.exe → cmd.exe → powershell」の順にプロセスが遷移し、削除が行われていた。
一方で通常の削除では、「cmd.exe → powershell」の順でプロセスが遷移しているのを確認した。ShinoBot によるものが通常とは異なる挙動を示していたが、cmd.exe および powershell にて作成、実行されるプロセスはほとんどが一致していることも確認できた。

5　予想

- cohost.exe を一度経由することが、外部から操作されているときに見られる特徴である可能性。