SecHack365

Linux 向けの機能豊富な RAT

坂上良朗

* 概要

ネットワークやシステムのセキュリティを実践的な観点から評価する際に使用できる RAT を既存のものを流用せずに、一から開発した。

RAT とは？
- Remote Access Tool の略
- サイバー攻撃で頻繁に用いられる遠隔操作ツールのこと。

本 RAT は、悪用のためではなく研究開発のために行った。

* 機能

一般的な RAT が備えている機能はもちろん、
強力なネットワークへの操作、柔軟な情報収集などの機能を備えている。

機能のいくつかを下記に挙げる。

- ファイル管理
- プロセス管理
- リソース管理
- 様々なプロトコルを使用したプロキシ作成
- 様々なプロトコルを使用したネットワークの偵察
- 様々なソフトウェアから興味深い情報の収集

また、下記の工夫により出来るだけ分析を困難にしている。

- 制御側とのやり取りを暗号化
- 内部で使用しているデータの難読化
- VM やデバッガに対する妨害
- メモリ上へ展開したデータの消去
- 様々な方法を使用した自身の隠蔽

* 悪用防止

RAT が動作環境外に漏れた場合に備えて、下記のものを悪用防止の策としている。

- 時間制限
  - RAT が動作する時間を特定の範囲に狭める。
- IP 範囲の制限
  - RAT がコールバックする先の IP や、使用する IP を特定のものに制限。
- 認証
  - 制御側との認証。

* 今後の予定

- 悪用防止策を実装。
- 制御側を Ruby で再実装。

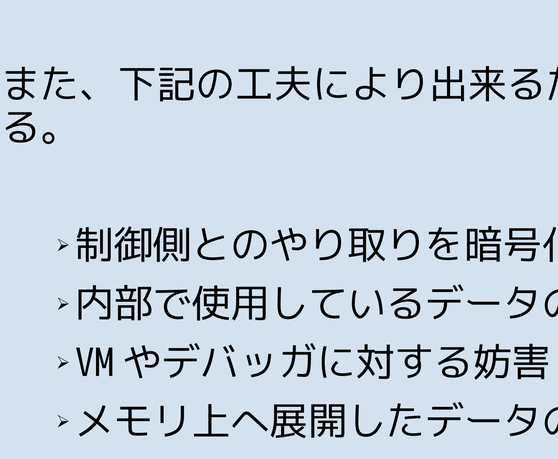
*Sechack365 の感想

- 法律に関する話を聞いて、危ない橋を渡ろうとしていたことに気づけて良かった。
- ハッカソンへの参加は初めてだったが、いい刺激になった。

* 最後に

RAT は今後、ペンテストや攻撃者のシミュレーションなどの正当な目的で使われていけば良い。

制御側



遠隔操作

開発した RAT