Challenge 1: SillyPutty

Hello Analyst,

The help desk has received a few calls from different IT admins regarding the attached program. They say that they've been using this program with no problems until recently. Now, it's crashing randomly and popping up blue windows when it's run. I don't like the sound of that. Do your thing!

IR Team

Objective

Perform basic static and basic dynamic analysis on this malware sample and extract facts about the malware's behavior. Answer the challenge questions below. If you get stuck, the `answers/` directory has the answers to the challenge.

Tools

Basic Static:

- File hashes

- VirusTotal

- FLOSS

- PEStudio

- PEView

Basic Dynamic Analysis

- Wireshark

- Inetsim

- Netcat

- TCPView

- Procmon

Challenge Questions:

Basic Static Analysis

---

- What is the SHA256 hash of the sample?

- What architecture is this binary?

- Are there any results from submitting the SHA256 hash to VirusTotal?

- Describe the results of pulling the strings from this binary. Record and describe any strings that are potentially interesting. Can any interesting information be extracted from the strings?

- Describe the results of inspecting the IAT for this binary. Are there any imports worth noting?

- Is it likely that this binary is packed?

---

Basic Dynamic Analysis

- Describe initial detonation. Are there any notable occurrences at first detonation? Without internet simulation? With internet simulation?

- From the host-based indicators perspective, what is the main payload that is initiated at detonation? What tool can you use to identify this?

- What is the DNS record that is queried at detonation?

- What is the callback port number at detonation?

- What is the callback protocol at detonation?

- How can you use host-based telemetry to identify the DNS record, port, and protocol?

- Attempt to get the binary to initiate a shell on the localhost. Does a shell spawn? What is needed for a shell to spawn?