TlsCheck Plugin Manual

Volatility Contest - 2024

Contents

1. Description of How to Use the TlsCheck Plugin

The TlsCheck plugin is a specialized tool designed to detect, analyze, and disassemble Thread Local Storage (TLS) callbacks in memory samples. Below are the detailed usage instructions and commands for all available options:

General Command Syntax:

```
python3 vol.py -f <memory_dump> windows.TlsCheck [OPTIONS]
```

2. Options and Descriptions

a. --disasm-bytes [value]

Sets the maximum number of bytes to disassemble. The plugin stops disassembling by default at the ret instruction or after 64 bytes, whichever comes first.

```
python3 vol.py -f memory.dmp windows.TlsCheck --disasm-bytes 128
```

This disassembles up to 128 bytes per TLS callback, useful for detailed inspection.

b. --scan-suspicious

Enables regex-based instruction scanning to detect suspicious patterns like indirect jumps, anti-debugging techniques, or obfuscation.

```
python3 vol.py -f memory.dmp windows.TlsCheck --scan-suspicious
```

Use this to identify unusual or potentially malicious instructions in callbacks.

c. --regex [pattern]

Allows users to define custom regex patterns for scanning specific instructions or behaviors in disassembled callbacks.

```
python3 vol.py -f memory.dmp windows.TlsCheck --regex "jmp.*eax"
```

This searches for instructions matching the provided pattern.

d. --yara-file [path_to_yara_rules]

Scans disassembled TLS callbacks against custom YARA rules for detecting specific malicious patterns.

```
python3 vol.py -f memory.dmp windows.TlsCheck --yara-file ./rules.yara
```

Use this to identify specific malware signatures or behavior patterns.

3. Output

The plugin generates a user-friendly output with the following columns:

- **PID:** Process ID.
- **PPID:** Parent Process ID.
- **Process Name:** Name of the executable.
- **Offset(V):** Virtual memory offset of the process.
- **TLS RVA(V):** Relative Virtual Address of the TLS.
- **Architecture:** Indicates whether the process is 32-bit (x86) or 64-bit (x64).
- **Path:** Full path of the executable.
- **TLS-Callback Instructions:** Disassembled instructions with:
    - **Hexdump:** Hexadecimal representation.
    - **Address:** Memory address of the instruction.
    - **Instruction:** Operation being performed.
    - **Operands:** Data or registers involved.