Name: Purva Pawaskar

Intern ID:259

Proof of Concept (PoC) Report – ProcDOT

Tool Name:

ProcDOT – Process + Network Visualization Tool for Malware Analysis

History

ProcDOT was created by Christian Wojner (PMA Labs, Austria) around 2012 to simplify malware behavior analysis. It is widely used in DFIR, SOC teams, and malware research labs. The tool gained popularity because it visualizes large and noisy Procmon logs with network data in a clean, interactive graph.

Description – What Is This Tool About?

ProcDOT correlates process/file/registry activity (from Sysinternals Procmon) and network traffic (from Wireshark PCAP) to create a behavior graph. It helps analysts quickly identify persistence techniques, file drops, child processes, and command & control (C2) communication.

Key Characteristics / Features

✅ Combines Procmon + PCAP logs

✅ Generates interactive DOT graphs

✅ Highlights process, registry, file & network relationships

✅ Portable, no installation required

✅ Works well for sandbox & VM malware analysis

Types / Modules Available

• Procmon Log Parser (.PML)

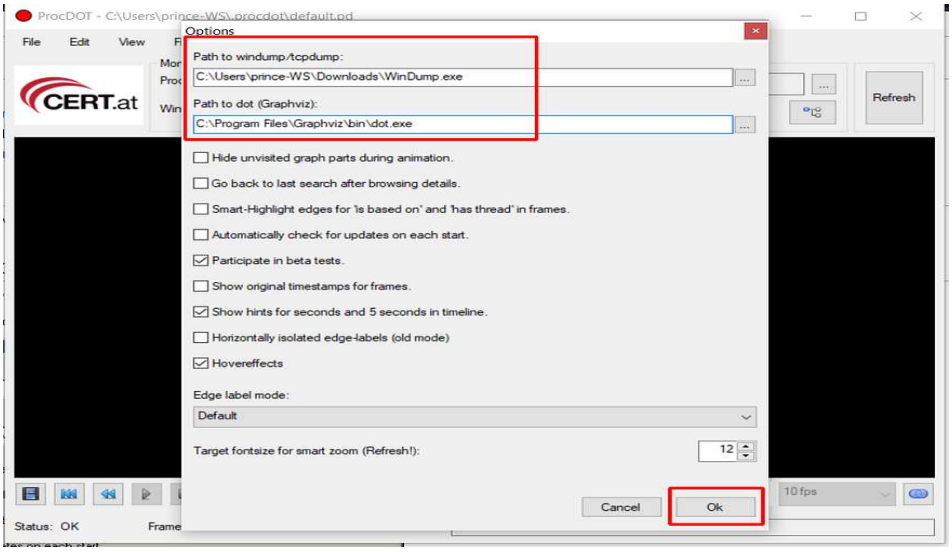
• Wireshark Log Parser (.PCAP)

• DOT/Graphviz Graph Generator

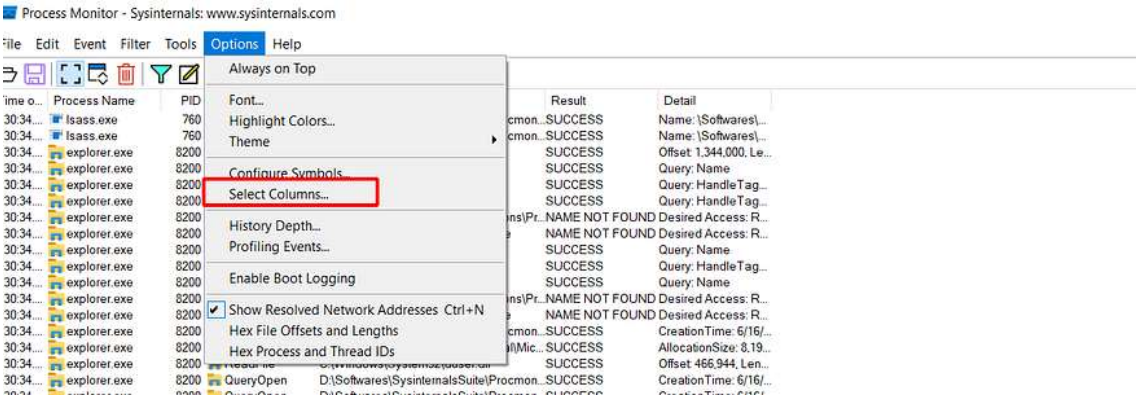
How This Tool Helps

- Speeds up malware triage
- Identifies suspicious behaviors without deep reverse engineering
- Saves hours of manual log reading
- Produces visual PoC reports for management
- Helps SOC/DFIR teams investigate unknown executables

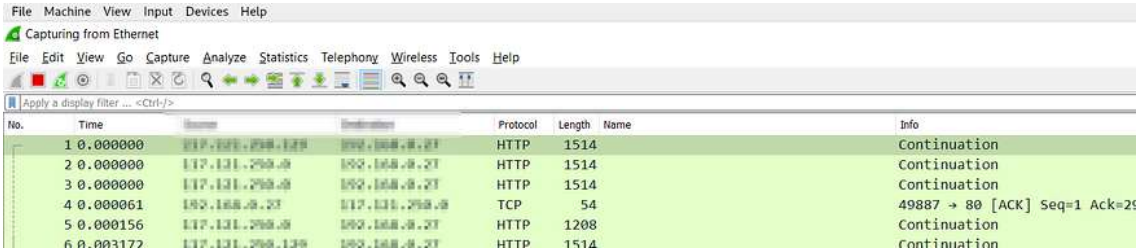
ProcDOT Interface



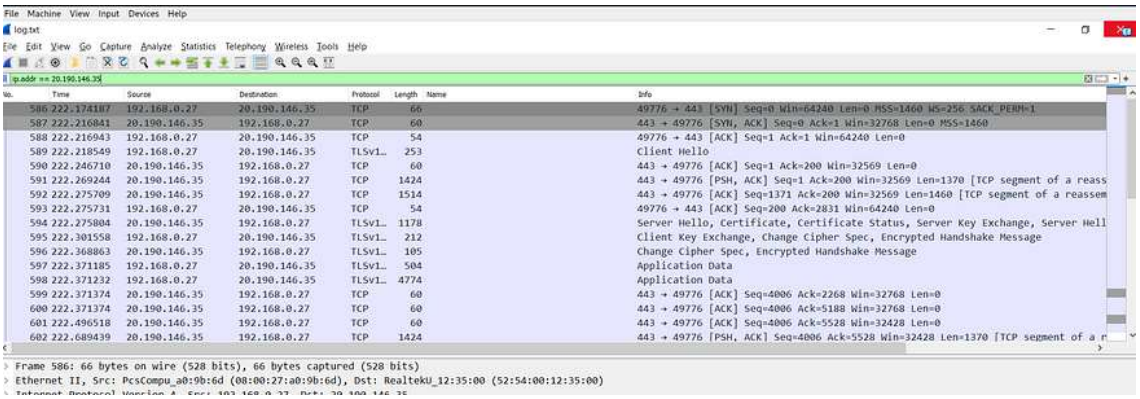
Setup ProcMon:



Wireshark



Graph View:



Summary

1. ProcDOT is a malware analysis visualization tool

2. Developed by PMA Labs for Windows environments

3. Uses Procmon logs for process/registry/file events

4. Uses Wireshark PCAP for network traffic

5. Creates interactive DOT graphs

6. Shows child processes & persistence

7. Helps SOC & DFIR teams triage samples

8. Works best in isolated VM labs

9. Free & portable

10. Useful before reverse engineering malware

11. Helps visualize MITRE ATT&CK TTPs

12. Filters out noise for clarity

13. Ideal for training & incident response

14. Not a prevention tool, analysis only

15. Great for malware PoC reporting

Time to Use / Best Case Scenarios

✅ During sandbox malware execution

✅ In incident response investigations

✅ Before deep reverse engineering

✅ When preparing malware behavior reports

When to Use During Investigation

1. After running a sample in a Windows VM

2. Once you have Procmon + PCAP logs

3. Before moving to IDA/Ghidra analysis

4. To quickly explain behavior to non-technical teams

Best Person to Use & Skills Required

• Best for: Malware Analysts, SOC Engineers, DFIR Experts

• Skills Needed:

- Windows Internals

- Understanding of Procmon & Wireshark

- Networking basics (TCP/IP, HTTP)

- Ability to read DOT graphs

Good About This Tool

✅ Free & easy to use

✅ Saves hours of manual log parsing

✅ Visualizes complex behavior for quick understanding

✅ Works well for PoC & training

✅ Integrates easily with sandbox workflows

Execution Summary

VM Used: Windows 10 (32-bit) VMware VM

Sample Executed: Safe PowerShell script simulating malware (created file, registry, and network request)

Captured Logs:

- capture.pml (Procmon)

- capture.pcap (Wireshark)

ProcDOT Visualization:

- Showed powershell.exe creating a file in %AppData%

- Modified registry key for persistence

- Connected to example.com over HTTP

Conclusion

ProcDOT is an essential malware triage tool. It helps analysts visually correlate system and network behavior, making it easier to explain findings and detect malicious techniques. While it’s not a real-time prevention tool, it saves time during post-infection analysis and improves DFIR workflows.