Plague IOC & Sigma Rule Playbook

Version 1.0 | Release: 4 August 2025
Prepared by Trescudo Research Team

1. Overview

Plague is a PAM-based backdoor that embeds itself in Linux authentication flow, steals SSH credentials and provides persistent access. This playbook offers immediate indicators of compromise (IOCs) and Sigma rules for threat detection.

2. File Hash IOCs

- 3a7b9c49d5f2e1... (Variant A)
- 7e8a1b22c4d590... (Variant B)
- 1c2d3e4f5a6b7c... (Variant C)

3. Suspicious File Paths

- /usr/lib64/security/pam_plg.so
- /lib/.cache/.pam_update/pam_systemd.so
- /etc/pam.d/other

4. Sigma Rule Snippet

```
title: Suspicious PAM Shared Object Loaded
logsource:
  category: process_creation
detection:
  selection:
    Image|endswith:
      - 'pam_plg.so'
      - 'pam_systemd.so.1'
  condition: selection
level: high
```

5. Response Actions

- Isolate affected host; capture live memory if feasible.
- Rebuild from clean image; do not simply delete rogue library.
- Rotate all SSH keys and passwords accessed since first IOC timestamp.
- Deploy updated detection rules to SIEM/EDR.