Identity Tracking in Multi-User Pilot Jobs (MUPJ)

Sven Gabriel, sveng@nikhef.nl
Nikhef http://nikhef.nl

Introduction

SSCs and User Traceability

User Traceability Test

Introduction

User traceability in MUPJ,some Remarks:

- User Traceability was not challenged within Security Drills SSC-4/5.
- Identities to operate on are clearly marked (DN=...SSC)
- The User-Traceability Test is not a Security Drill,like SSC-5.
- The User-Traceability Test was unscheduled, simple and intended to provide input for a Discussion.

Test Case

The Situation/Notification to CSIRT

- ”Malicious” Jobs via Panda: write a file in Pilots home (persistent).
- Subsequent jobs also run this file.
- Subsequent jobs modify the time stamps of this file
- The ”malicious” Job was run at 3 sites.
- VO-CSIRT was provided with a lot of information in the ”alarm” (file name, complete host list)

Incident-Response

Find compromised account/DN. Reasonable Time range 4-24h

Case: Unix-IDs not shared

- Check reported WN(s)
- Check ”malicious” processes
- Unix-ID
- Unix-ID is mapped to a DN
- Suspend DN

Incident-Response

Find compromised account/DN. Reasonable Time range 4-24h

Case: Unix-IDs shared, WN shared homes

- Check reported WN(s), single ”malicious” job infects many WNs)
- Check ”malicious” processes
- Unix-ID
- Unix-ID is mapped to a DN (Pilot)
- Unix-ID runs payload from Multiple users
- No possibility connect a activity to one ID with sufficient certainty.
- Containment is very difficult.

Incident-Response

Find compromised account/DN. Reasonable Time range 4-24h

Case: Unix-IDs shared, WN local home dirs

- Check ”malicious” processes
- Unix-ID
- Unix-ID is mapped to a DN (Pilot)
- Unix-ID runs payload from Multiple users
- No possibility connect a activity to one ID with sufficient certainty.
- Containment is very difficult.
- *Heuristics possible, just give hints to users.*

Response

CSIRT-Response

- After one week the ”offending” DN was not yet found (Report from VO-CSIRT).
- Remarkable resources would be needed for a proper response (not available for an unscheduled test)
- Retention times for needed logs are to short (15, resp. 30 days).
- *”It would have taken O(1 week) to scan all input sources for the offending code”*

Response

Severe Security Issue found

- During this activity a severe Vulnerability was found. (Not exploited here!)
- Svg-rat New Vulnerability EGI RT no 3231 concerning Panda.
- This report could not be kept back, it also contained the ”malicious” DN.
- *”After the hint in the new vulnerability report tonight I found the bash_profile hackers jobs:... ”*
- Atlas experts eliminated this vulnerability within 4h!

Summary

Summary

- It is possible to create untraceable jobs in an Unix-Environment with shared IDs.
- Even if heuristics point to some IDs, a proof is difficult.
- Containment of an incident very difficult.
- The amount of data to process for tracing an ID in such a case consumes more resources/time as reasonably available during incident response.
- With shared Unix-IDs sites can not control the access to their resources efficiently.
- Unix-IDs should not be shared.