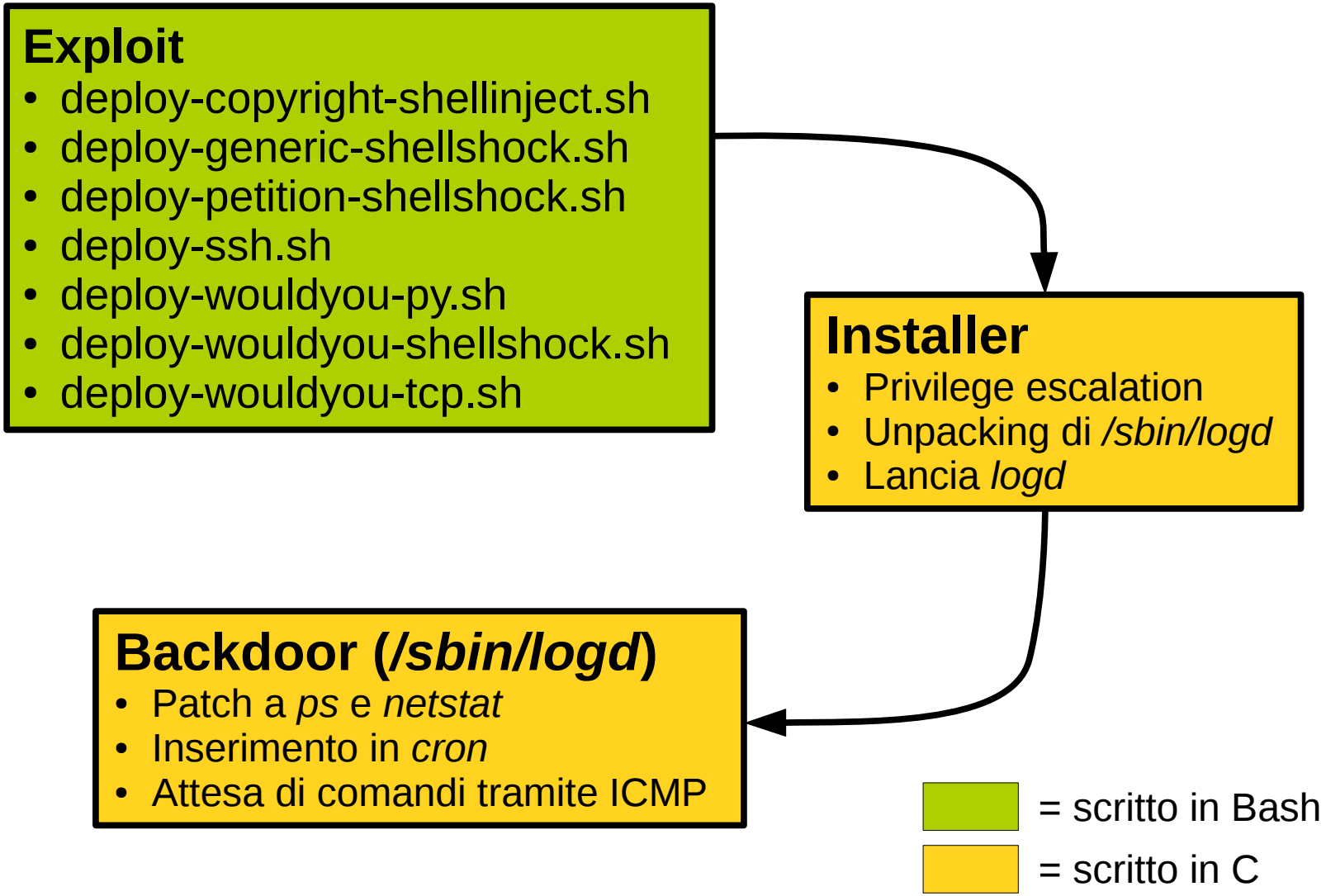
Backdoor


Exploit
• deploy-copyright-shellinject.sh
• deploy-generic-shellshock.sh
• deploy-petition-shellshock.sh
• deploy-ssh.sh
• deploy-wouldyou-py.sh
• deploy-wouldyou-shellshock.sh
• deploy-wouldyou-tcp.sh
Installer
• Privilege escalation
• Unpacking di /sbin/logd
• Lancia logd
Backdoor (/sbin/logd)
• Patch a ps e netstat
• Inserimento in cron
• Attesa di comandi tramite ICMP
= scritto in Bash
= scritto in C

Nascondere processi e persistenza

- Patch a libproc (**ps**, **top**, …) – procps-3.2.7/proc/readproc.c:700-742
  - Nasconde *logd* e relativo sottoalbero dei processi
- Patch a net-tools (**netstat**) – net-tools-1.60/netstat.c:749-753,976-977
  - Nasconde tutte le connessioni TCP verso la subnet Tendermemory (10.10.1.0/24)
  - Nasconde i processi in ascolto su protocollo ICMP

- **Cron** ([ri]attiva backdoor automaticamente ogni minuto)

```
# /etc/cron.d/logd: crontab fragment for system log
# reporting daemon. Flush log every minute
* * * * * root /sbin/logd flush
```

File da sovrascrivere **integrati all'interno della backdoor** (offuscati con XOR per renderli invisibili in caso di analisi di *logd* tramite strings/hexdump).

Azioni **rieseguite automaticamente ad ogni avvio** della backdoor.

I/O con backdoor

- Comandi trasmessi in pacchetti di tipo **ICMP echo request** (i.e. ping)
- Payload cifrato con chiave “T3nd3rM3m0r1” (cifrario XOR con qualche aggiunta per randomizzare l'encryption)
- Solo alcuni valori del campo ICMP ID attivano la backdoor (necessario per scartare pacchetti ping legittimi)

Comandi disponibli:

- **run_interactively:** esegue un comando con redirect dello stdio su socket TCP (anche in questo caso cifrando con chiave “T3nd3rM3m0r1”). Utilizzato dai rastrelli.
- **fix_bootloader**: Comando monouso, v. demo ☺

Demo

- Avviamo wireshark
- Exploit *deploy-wouldyou-tcp.sh*
- Confronto tra *ps* e *netstat* autentici e patchati
  - Variabile d'ambiente NOHIDE=TM
- *run_interactively*
  - Shell di root
  - Demo del rastrello (*)
- *fix_bootloader*

* = ho preavviato l'arbitro, quindi sulla macchina sono già presenti alcuni flag