Inject #7: Suspicious Program

MAIL FROM: Team 1 “Club Penguin”
RCPT TO: Circle for the Protection of Antarctica
SUBJECT: Suspicious Program

Hello Circle For The Protection of Antarctica,

We found “injectd” on albatross machine. It was located in /usr/bin/injectd. We deleted it and stopped the attached service as shown in the screenshot below. Thank you for the valuable intel, eliminating this binary helped to avoid potential breaches.

```
[rigmanager@albatross-team01-seal-aq /]$ sudo find / -name "*injectd*"
/run/systemd/units/invocation:injectd.service
/etc/systemd/system/multi-user.target.wants/injectd.service
/etc/systemd/system/injectd.service
/sys/fs/cgroup/system.slice/injectd.service
/usr/bin/injectd
[rigmanager@albatross-team01-seal-aq /]$ cat /etc/systemd/system/injectd.service
[Unit]
Description=Inject

[Service]
ExecStart=/usr/bin/injectd

[Install]
WantedBy=multi-user.target[rigmanager@albatross-team01-seal-aq /]$ file /usr/bin/injectd
Bad system call
[rigmanager@albatross-team01-seal-aq /]$ rm /usr/bin/injectd
```

Regards,
Team 1 “Club Penguin”