Anteater
CI Gate Security

•••

June 15, 2017

The Problem

- Approx 1000 Changesets a month / 70+ projects
- No security controls - projects can pull in binaries, scripts, artefacts from anywhere.
- Platform is then deployed into multiple NEP and Operator networks.

Recent Attacks against CI / CD environments

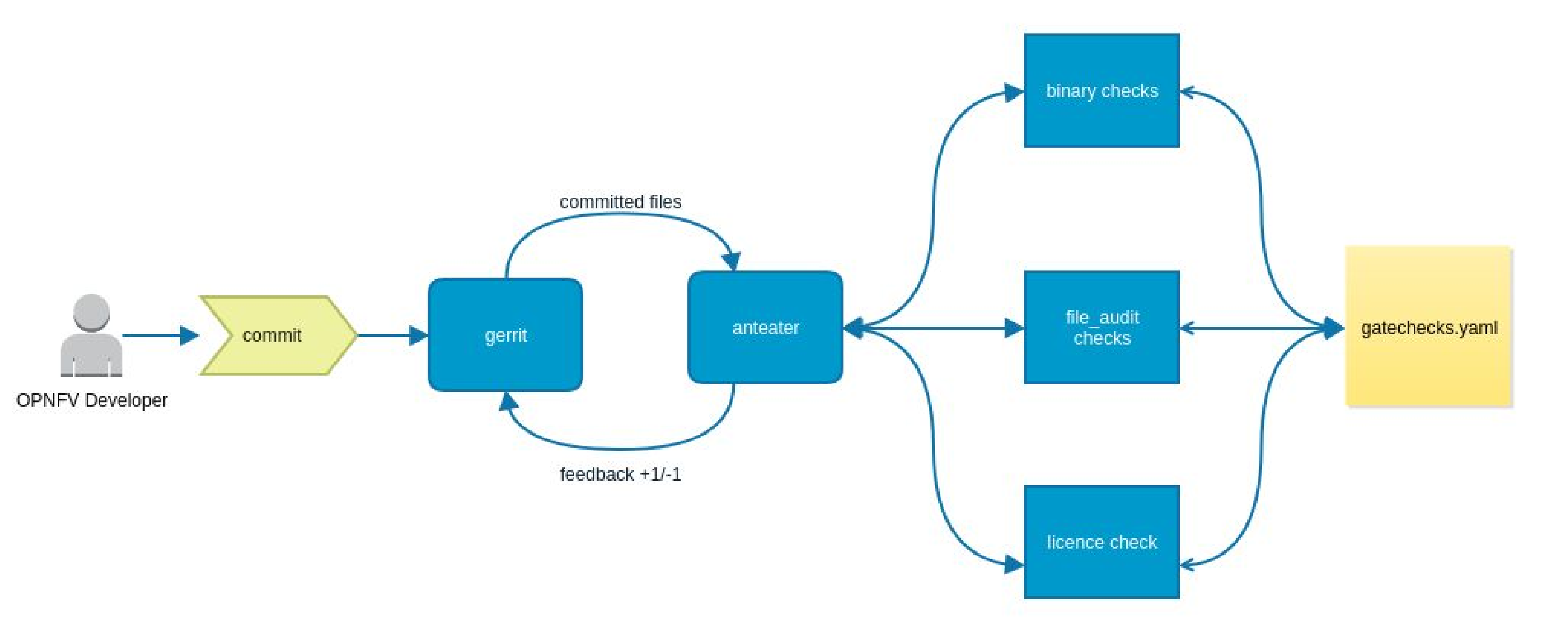
- “Ticketing, bug tracking, and git provided secrets (e.g. crypto keys, seeds, hashes, credentials, and source code)
- Wikis revealed administrative workflows and VPN details”
- “Engineering credentials (ssh keys) were used to commit backdoors to version control which were self-approved and later deployed into production”

https://medium.com/@chrismcnab/alexseys-ttps-1204d9050551

What we have seen in OPNFV..

- Private keys stored in repos (CVE-2016-1000297).
- WGET script downloads from a developer's laptop.
- Lot’s of hard coded passwords
- Uses of ‘eval’ and other functions that can be exploited.
- Clones of git repositories outside opnfv.

What does Anteater do?



A patchset file list is provided by JJB

```
/home/jjb/repo/fileone.py

/home/jjb/repo/somebinary

/home/jjb/somescript.sh
```

If the file is a binary, its blocked or ‘waivered’

```
repo_name:
  binary_ignore:
   [somebinaryfile, 407fb352a8b709fa1890f200fee5186455fe815fb6c7808305f210e2f1faf76d]
   [anotherbinaryfile, 90517f282ed8137978c9a5e8da06450371fa1a7a783423ee28ba7a5d61f2d1e6]
```

- *Blocked means -1 at gate*

If a file is not a binary, the contents are checked

```
file_contents:
[-----BEGIN\sRSA\sPRIVATE\sKEY----,secret,ssh_key,private_key,md5,wget,"curl(.*?)bash",eval
,shell(.*?)true"sh(.*?)curl","git(.*?)clone",gost,md2,md4,md5,rc4,sha0,streebog,dual_ec_drb
g,snefru,panama,ripemd,sslv1,sslv2,tlsv1] <snip>
```

Unless waived:

```
repo_name:
  file_contents:
[self\.local_ssh_key,self\.proxy_ssh_key,jh_ssh_key='/root/\.ssh/id_rsa',fa-user-secret,-s  set secret
key,paramiko\.RSAKey\.from_private_key_file\(pkey_file\),git clone the Openstack-Ansible,secret not
defined,user_secrets\.yml,wget -O,/tmp/get-pip\.py,"PKG_MAP\\[wget\\]",^wget \\,"git
clone(.*)gerrit\\.opnfv\\.org","git clone(.*)\\.openstack\\.org",wget(.*)build.opnfv.org
```

Example One

A project needs to clone the following repo in a script / code file:

https://github.com/john_doe/repo

Developer submits a patch to releng-anteater with the following regex:

```
someproject:
    file_contents: "git (.*)github\\.com\\john_doe/repo"
```

Example Two

A project has the following in script

wget https://example.com/somepackage.rpm

Developer submits a patch to releng-anteater with the following regex:

```
someproject:
   file_contents: "wget(.*)example\\.com/somepackage.rpm"
```

How is this being phased in.

- During E release, non voting. Voting for F release.
- Tool will be available on PyPi for developers to test locally.
- Works against patchset, not entire repo (although repo can be scanned / daily cron)
- Tools are planned to support developers write and test waivers

Come and get involved!

Room Pastel

Tuesday 15:00 to 16:00