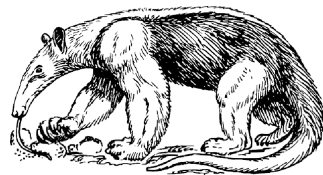


# Anteater CI Gate Security ...



# 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.

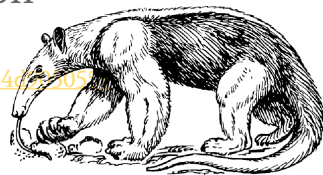


# Why Anteater..?

## Recent Attacks against CI environments

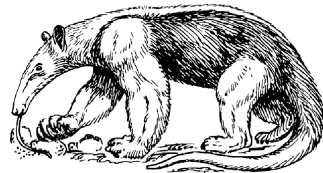
- Ticketing, bug tracking, and git provided secrets (e.g. crypto keys, seeds, hashes, credentials, and source code) provided hacker access to build systems.
- Wikis revealed administrative workflows, IP's and VPN details
- Stolen Engineering credentials (ssh keys) were used to commit backdoors to version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

<https://medium.com/@chrismcnab/alexseys-https-120467205>



# 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
- Lot's of binaries
- Uses of 'eval' and other functions that can be exploited.
- Clones of git repositories outside opnfv.



# What does Anteater do?

Scans git patches for potential malicious strings or binaries.

If a potential malicious object is identified, it is from merging until reviewed.



# How?

Using standard regular expressions to search in scripts / code or any text file:

```
- "-----BEGIN\sRSA\sPRIVATE\sKEY-----"  
- "curl(.*)bash"  
- "git(.*)clone"  
- "sh(.*)curl"  
- "subprocess(.*)shell(.*)=(.*)True"
```



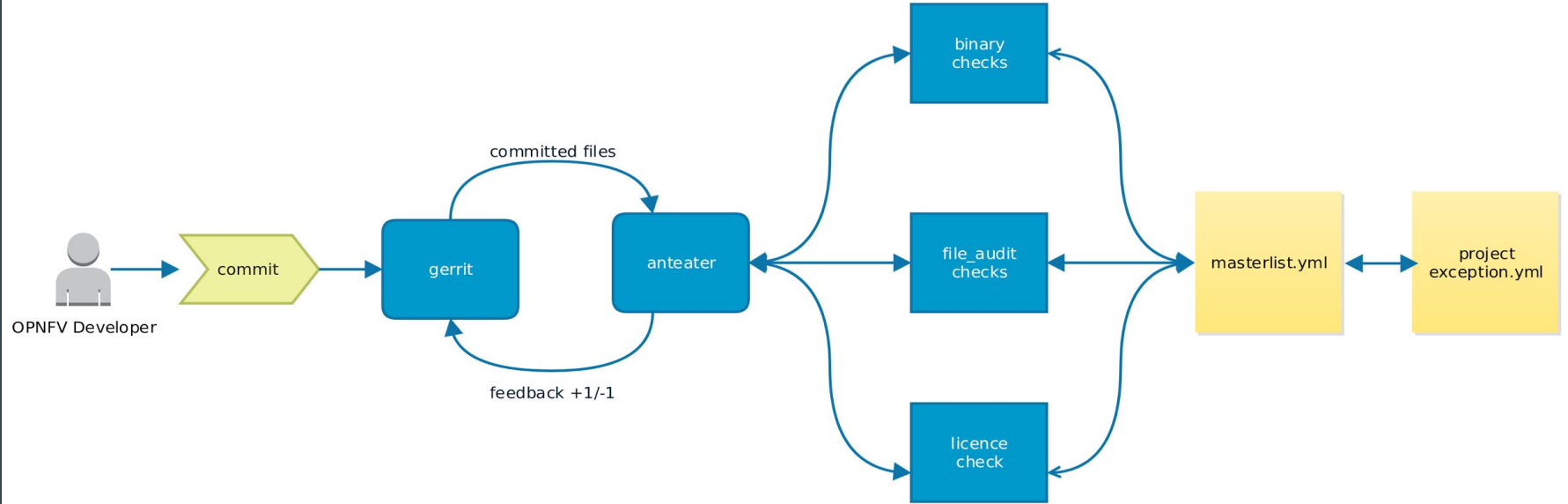
# How?

All binary files are blocked, unless a sha256 checksum of the file is provided.

```
[architecture.jpeg, 407fb352a8b709fa1890f200fee5186455fe815fb6c7808305f210e2f1faf76d]  
[architecture.pdf, 90517f282ed8137978c9a5e8da06450371fa1a7a783423ee28ba7a5d61f2d1e6]
```



# How does this work in CI Gate?





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 has an exception (as below).

**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-----  
- "curl(.*)bash"  
- "git(.*)clone"  
- "sh(.*)curl"  
- dual_ec_drbg  
- eval  
- gost  
- md[245]
```

Unless an exception is provided:

## **file\_contents:**

```
- "wget http://repo1\\.maven\\.org"  
- paramiko\\.RSAKey\\.from_private_key_file\\(pkey_file\\)  
- "git clone(.*)\\.openstack\\.org"  
- "git clone(.*)gerrit\\.opnfv\\.org"
```



# Example One

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

[https://github.com/john\\_doe/repo](https://github.com/john_doe/repo)

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

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



# Example Two

A project has the following in script

```
wget https://trusted.com/somepackage.rpm
```

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

**someproject:**

**file\_contents:** "wget(.\*)trusted\\.com/somepackage.rpm"



# Example Patch One

AllMyProjectsPeopleDocumentation

ChangesDraftsDraft CommentsEditsWatched ChangesStarred ChangesGroups

Search term

Change 36075 - Needs Code-Review Label

Test binary file

Change-Id: I3dbeca3ebdc514134158d715b5e018d52a5ec599  
Signed-off-by: lhinds <lhinds@redhat.com>

Owner Luke Hinds  
Reviewers Jenkins Ericsson xjenkins-ci x  
Project sandbox  
Branch master  
Topic binary  
Strategy Merge if Necessary  
Updated 8 days ago

Reply...Cherry PickRebaseAbandonFollow-Up

Code-Review  
Verified

Related Changes (3)

test patch  
Test binary file  
test anteater

Author lhinds <lhinds@redhat.com>  
Committer lhinds <lhinds@redhat.com>  
Commit d1e6cd2438cb198d6c05a06595eb80f15f1d2e04  
Parent(s) afd0a0b9f2218531b9de567d9fe8584066b1f10a  
Change-Id I3dbeca3ebdc514134158d715b5e018d52a5ec599

Jun 14, 2017 4:08 AM  
Jun 14, 2017 4:08 AM  
(gitweb)  
(gitweb)

Files

Open AllDiff against: BaseEdit

File Path	Comments	Size
Commit Message		
A trojanfile		+59.7 KiB
		+59.7 KiB, -0 B

History

Expand All

Luke Hinds	Uploaded patch set 1.	Jun 14 4:10 AM
jenkins-ci	Patch Set 1: Build Started https://build.opnfv.org/ci/job/opnfv-security-audit-verify-master/29/	Jun 14 4:10 AM
Jenkins Ericsson	Patch Set 1: Non Whitelisted Binary file: /home/opnfv/anteater/sandbox/trojanfile Failures registered	Jun 14 4:10 AM
jenkins-ci	Patch Set 1: Build Failed https://build.opnfv.org/ci/job/opnfv-security-audit-verify-master/29/ : FAILURE (skipped)	Jun 14 4:10 AM



# Example Patch Two

All

My

Projects

People

Documentation

Changes

Drafts

Draft Comments

Edits

Watched Changes

Starred Changes

Groups

Search term

Change 36087 - Needs Code-Review Label

test\_patch

testing, binaries, keys, passwords

Change-Id: Ief03a1ec561c77917eead8263d1766651e683725

Signed-off-by: lhinds <lhinds@redhat.com>

Reply...

Owner Luke Hinds

Reviewers Jenkins Ericsson x jenkins-ci x

Project sandbox

Branch master

Topic testpatch

Strategy Merge if Necessary

Updated 8 days ago

Cherry Pick Rebase Abandon Follow-Up

Related Changes (3)

test\_patch

Test binary file

test anteater

Code-Review

Verified

Author lhinds <lhinds@redhat.com>

Committer lhinds <lhinds@redhat.com>

Commit 4f236338a9997f64e16d54f1c888e47cf6828c63

Parent(s) d1e6cd2438cb198d6c05a06595eb80f15f1d2e04

Change-Id Ief03a1ec561c77917eead8263d1766651e683725

Jun 14, 2017 7:02 AM

Jun 14, 2017 7:02 AM

(gitweb)

(gitweb)

Files

Open All

Diff against: Base

Edit

File Path	Comments	Size
Commit Message		
A credentials.txt	2	
A harmless	+59.7 KiB	
A id_key	27	
A id_key.pub	1	
	+30, -0	
	+59.7 KiB, -0 B	

History

Expand All

Luke Hinds

Uploaded patch set 1.

Jun 14 7:03 AM

jenkins-ci

Patch Set 1: Build Started https://build.opnfv.org/ci/job/opnfv-security-audit-verify-master/31/

Jun 14 7:03 AM

Jenkins Ericsson

Patch Set 1:

Non Whitelisted Binary file: /home/opnfv/anteater/sandbox/harmless

File contains violation: /home/opnfv/anteater/sandbox/id\_key

Flagged Content: -----BEGIN RSA PRIVATE KEY-----

Matched String: -----BEGIN RSA PRIVATE KEY----

Failures registered

Jun 14 7:04 AM

jenkins-ci

Patch Set 1: Build Failed https://build.opnfv.org/ci/job/opnfv-security-audit-verify-master/31/ : FAILURE (skipped)

Jun 14 7:04 AM



# 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





# New features planned

ClamAV Scanning of all files

HTML rendered reports

Possible Integration with Black Duck Hub API

Developer tools for generating exception regular expressions

Github integration



# More information

Wiki: <https://wiki.opnfv.org/pages/viewpage.action?pageId=10294496>

Git Mirror: <https://github.com/opnfv/releng-anteater>

