Main page
Recent changes
Server admin log (Prod)
Server admin log (RelEng)
Deployments
SRE/Operations Help
Incident status

Cloud VPS & Toolforge
Cloud VPS documentation
Toolforge documentation
Request Cloud VPS project
Server admin log (Cloud VPS)

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Incident documentation/20180615-phabricator-vandalism

< Incident documentation

This page is currently a draft.
More information and discussion about changes to this draft on the talk page.

Contents [hide]

Summary

On Friday, June 15th 2018, Phabricator was vandalized by an attacker who randomly reassigned tasks, dropped members from projects, posted random gibberish comments, altered task priorities, merged tasks, etc.

Timeline

- 2018-06-15 07:50: Vandal creates Phabricator account 238482n375
- 2018-06-15 08:01 to 08:08: 238482n375 starts to edit tasks (edited projects: added Analytics-Kanban, Security, Wikimedia-VE-Campaigns (S2-2018), Scap (Scap3-Adoption-Phase2), AbuseFilter, Data-release, Hashtags, LabsDB-Auditor, Ladies-That-FOSS-MediaWiki, Language-2018-Apr-June, Language-2018-Jan-Mar, HHVM, HAWelcome; edited projects: removed Cloud-Services, Tools; set Priority field to Lowest; removed task assignee; moved task from Next Up to In Code Review on the Analytics-Kanban board; added subscriber 238482n375; removed subscriber Aklapper; and/or: set the Security field to Software security bug to change task visibility)
- 2018-06-15 08:08: Volans and JAlexander disable Phabricator account 238482n375
- 2018-06-15 08:12: Vandal creates Phabricator account Hfewjfjjsjjksa
- 2018-06-15 08:18: Vandal creates Phabricator account Dnvjdvsj
- 2018-06-15 08:30: Hfewjfjjsjjksa creates 161 tasks
- 2018-06-15 08:30: AKlapper disables Phabricator account Hfewjfjjsjjksa
- 2018-06-15 08:33: AKlapper disables Phabricator account Dnvjdvsj
- 2018-06-15 08:50: Discussions about potential conclusions start (phab:T162026#4289748, IRC)
- 2018-06-15: Several people (akosiaris, Ladsgroup, mutante, Volans, AKlapper, etc) revert those actions
- 2018-06-15 14:10: mmodell temporarily enables `auth.require-approval` in the Phabricator configuration
- 2018-06-16 22:47: Vandal creates Phabricator account Ndscnjd (no activity as `auth.require-approval` was enabled; account disabled later)
- 2018-06-17 01:31: Vandal creates Phabricator account Jsdhmvdj (no activity as `auth.require-approval` was enabled; account disabled later)
- 2018-06-19 mmodell locks down the 'Lock as security issue' feature
- 2018-06-20 04:35: Vandal unsuccessfully tries to log into their already disabled older Phabricator account Ahmed123
- 2018-06-27 06:00: tstarling disables `auth.require-approval` - phab:T197550#4318144
- 2018-06-30 02:38: Vandal creates Phabricator account Vvjjkkii
- 2018-07-01 01:01: Vvjjkkii starts to edit tasks
- 2018-07-01 01:05: Paladox files phab:T198547 about blocking the account Vvjjkkii
- 2018-07-01 01:14: bd808 disables Phabricator account Vvjjkkii

- 2018-07-01 01:53: greg reenables `auth.require-approval` and informs the community in https://lists.wikimedia.org/pipermail/wikitech-l/2018-July/090269.html
- 2018-07-01: Many people start to manually revert the edits
- 2018-07-01 05:12: phab:p/Community_Tech_Bot/ (later renamed to phab:p/CommunityTechBot/) starts to revert the edits
- 2018-07-01 06:16: Rate limiting patch by mmodell in https://gerrit.wikimedia.org/r/#/c/operations/puppet/+/441525/ gets merged - phab:T197922
- 2018-07-01 06:28: Jsamwrites files phab:T198552 about reverting the edits
- 2018-07-02 16:58: phab:p/CommunityTechBot/ finishes, Musikanimal summarizes in https://lists.wikimedia.org/pipermail/wikitech-l/2018-July/090283.html

Conclusions

- It's more work than it should be to revert the damage done by a bad actor.
- Phabricator has weak anti-vandalism features, we need to improve them.

Actionables

- ✓ **Done** Short-term: Enable manual approval of new user accounts in Phab - phab:T197550
- ✓ **Done** Lock down the 'Lock as security issue' feature - phab:D1069, phab:rPHEXf951c8bfa70a1d4f561ebd82cdbbcf9a619172fa
- ✓ **Done** Reinstate phabricator request rate limits - phab:T197922
  - ✓ **Done** Exclude offices from rate limits - phab:T198612
- ✓ **Done** Implement rate limiting on edits (AWA) - phab:T199741
- Allow reverting all actions by one single user in a recent timeframe - phab:T198283
- ~~Short-term: Block IPs~~: gerrit:440510
- ✓ **Done** Revert manual approval of new user accounts in Phab - phab:T197550 on 2018-08-09

Category: Incident documentation