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/20161112-OurMine

< Incident documentation

Contents [hide]

Summary

Accounts of Wikimedia Foundation staff and community members were compromised by the hacker group OurMine. The attackers used those accounts to vandalize highly visible pages. An initial response was posted on the Wikimedia Blog. Tim Starling wrote a pretty good summary on wikitech-l and wikimedia-l:

> *Since Friday, we've had a slow but steady stream of admin account compromises on WMF projects. The hacker group OurMine has taken credit for these compromises.*
>
> *We're fairly sure now that their mode of operation involves searching for target admins in previous user/password dumps published by other hackers, such as the 2013 Adobe hack. They're not doing an online brute force attack against WMF. For each target, they try one or two passwords, and if those don't work, they go on to the next target. Their success rate is maybe 10%.*
>
> *When they compromise an account, they usually do a main page defacement or similar, get blocked, and then move on to the next target.*
>
> *Today, they compromised the account of a www.mediawiki.org admin, did a main page defacement there, and then (presumably) used the same password to log in to Gerrit. They took a screenshot, sent it to us, but took no other action.*
>
> *So, I don't think they are truly malicious -- I think they are doing it for fun, fame, perhaps also for their stated goal of bringing attention to poor password security.*
>
> *Indications are that they are familiarising themselves with MediaWiki and with our community. They probably plan on continuing to do this for some time.*
>
> *We're doing what we can to slow them down, but admins and other users with privileged access also need to take some responsibility for the security of their accounts.*

To the best of my knowledge, all of the information in the incident report is public knowledge, though I (Legoktm) did use some of my Phabricator security access to help connect the dots.

Timeline

I'm not going to include a list of users who were compromised here to avoid shaming people.

- 2016-11-11T22:07 UTC: First malicious activity action on foundationwiki.
- More accounts compromised, a private Phabricator task is started to track them all to provide a permanent record in addition to IRC coordination.
- 2016-11-12T14:33 UTC <reedy@tin> Synchronized wmf-config/InitialiseSettings.php: Enable OATHAuth on

fishbowl wikis, bump password requirements (duration: 00m 50s) (SAL)
- 2016-11-12T14:59 UTC <reedy@tin> Synchronized wmf-config/CommonSettings.php: Enable OATHAuth for all sysop, crat, oversight and checkuser (duration: 00m 47s) (SAL)
  - 15:14 UTC Legoktm announces the availability of 2FA on the English Wikipedia's Administrators' noticeboard.
  - 15:38 UTC Bsadowski1 adds the oathauth-enable userright to the ombudsman, global-interface-editor, global-sysop, sysadmin, founder, and steward global groups upon request from the WMF security team
- 2016-11-12T19:53 UTC<tgr> deployed patch for T150554 (SAL)
- 2016-11-13 OurMine claims they have a local copy of the enwiki database (to whom?)
  - 2016-11-14 Tim writes a patch to Fix multiple bugs in EncryptedPassword, and files phab:T150647 about deploying it to counter the value of a SQL injection on leaking password (and other sensitive fields).
- 2016-11-14 Various logging improvements were made to MediaWiki:
  - mediawiki/core: Add extra logging for when user logs in with a temp password
  - mediawiki/core: Add better logging to password reset
- 2016-11-15 A Gerrit account with +2 rights (though not to any Wikimedia-deployed code I think) is compromised, and OurMine sent (who?) a screenshot of it
- 2016-11-16 Non-public, proactive, countermeasures are deployed
- 2016-11-16 Tim sends Update on WMF account compromises to wikitech-l and wikimedia-l

Conclusions

What weakness did we learn about and how can we address them?

- People re-use passwords, usually because of historical reasons from back when reusing passwords wasn't something that was warned against.
- Enabling two-factor authentication (TOTP) would have prevented these account compromises

Some private notes are available for people with security ticket access at T150554#2800564 and T150554#2802376. We should extract some/all of those into a public set of conclusions.

Links to relevant documentation

Where is the documentation that someone responding to this alert should have (cookbook / runbook). If that documentation does not exist, there should be an action item to create it.

Actionables

Explicit next steps to prevent this from happening again as much as possible, with Phabricator tasks linked for every step.

NOTE: Please add the #wikimedia-incident Phabricator project to these follow-up tasks and move them to the "follow-up/actionable" column.

Logging

- Status: **Unresolved** T150300: icinga notification if elevated writing to badpass.log
- Status: **Unresolved** T150903: Alert ops/security on many 2FA failures
- Status: **Done** T151010: Add logging to OATHAuth
- Status: **Done** T151415: Log email changes for all users

Notifications

- Status: **Done** T11838: Send notification to account owner on multiple unsuccessful login attempts
- Status: **Done** T107707: Login alert when user logs in from new machine

Passwords

- Status: **Unresolved** T150576 (private)
- Status: **Unresolved** T32574 Display a password strength bar
- Status: **Unresolved** T150647 Deploy EncryptedPassword to WMF
- Status: **Done** T57420 Remove local wiki password hash when CentralAuth has attached account
- Status: **Unresolved** T112359 (private)

Two factor

- Status: **Unresolved** T150898 Force OATHAuth (2FA) for certain user groups in Wikimedia production
- Status: **Unresolved** T100375 Improve user experience of Two-Factor process
- Status: **Unresolved** T145915 (private)

Other

- Status: **Done** T150930 Remove capture feature from Special:PasswordReset
- Status: **Done** T151015 Deploy EmailAuth extension to the beta cluster

Category: Incident documentation