Panic Inc.

PANIC BLOG

May 17th, 2017

The Case of the Stolen Source Code

By Steven

Last week, for about three days, the macOS video transcoding app HandBrake was compromised. One of the two download servers for HandBrake was serving up a special malware-infested version of the app, that, when launched, would essentially give hackers remote control of your computer.

In a case of extraordinarily bad luck, even for a guy that has a lot of bad computer luck, I happened to download HandBrake in that three day window, and my work Mac got pwned.

Long story short, **somebody, somewhere, now has quite a bit of source code to several of our apps.**

Before I continue, three important points:

- **There's no indication any customer information was obtained by the attacker.**
- **Furthermore, there's no indication Panic Sync data was accessed.**

- **Finally, our web server was not compromised.**

(As a reminder, we never store credit card numbers since we process them with Stripe, and all Panic Sync data is encrypted in such a way that even we can't see it. Read more.)

The other important fact is that I feel like a monumental idiot for having fallen for this.

How did this happen?

Story

HandBrake had been nagging me for some time to install an update. I finally decided, for whatever reason, to do the update. There was a note in HandBrake's update dialog that the incremental update was not available, and that I'd have to download an entirely fresh copy from their server. I didn't think too much of this, as we've been in a similar situation with a broken Sparkle update channel once before (the worst).

So, I managed to download within the three day window during which the infection was unknown, managed to hit the one download mirror that was compromised, managed to run it and breeze right through an in-retrospect-sketchy authentication dialog, without stopping to wonder why HandBrake would need admin privileges, or why it would suddenly need them when it hadn't before. I also likely bypassed the Gatekeeper warning without even thinking about it, because I run a handful of apps that are still not signed by their developers. And that was that, my Mac was completely, entirely compromised in 3 seconds or less.

By the time news broke of the HandBrake infection, git credentials had already been stolen from my Mac and used to clone several of our source code repositories, according to our logs.

As soon as I discovered the infection on my Mac, I disabled it, took the Mac out of commission, and we began the incredibly lengthy process of changing all of my passwords, rotating the relevant secret keys throughout our infrastructure, and so on, to re-lock our doors and hopefully prevent anything else from being stolen. The vast majority of these things were changed or rolled simply out of an

abundance of caution — again, there's no indication our web servers were compromised — but in this kind of a situation, you change all the locks.

Then, the forensics: we began combing through our logs to try to determine the extent of what was accessed which, to reiterate, we believe is limited to source code and personal data on my Mac. Thanks to good logging (thank you, James) we got a very complete picture. The method the attacker used prevented them from cloning all of our source code — they were making educated guesses at our repo names, one-by-one, which did not expose everything.

The source code theft was confirmed when we received an email from the attacker (with a few source code files attached as proof of the theft) demanding a large bitcoin ransom to prevent the release of the source code, which would "suffocate" our company, in their words. We're working on the assumption that there's no point in paying — the attacker has no reason to keep their end of the bargain.

And that brings us to today.

So...

When the dust settled, we sat down for a company all-hands meeting, and the conclusion was a little different than I originally expected.

Someone has a bunch of our source code. But does it really matter?

There are essentially three "worst case" scenarios we considered with our source being out there in somebody's hands:

- **They build free, cracked version of our apps.**
  Guess what — those already exist. You can already pirate our software if you want to pirate our software — but please don't — so this doesn't really change anything in that regard. Also, whatever "free" version of our apps that would come from this person are virtually guaranteed to be infected with malware.
- **They create malware-infected builds of our apps.**
  This seems likely. Given the person's entire MO was to infect a well-used Mac app with malware, it seems inevitable. But we will find them, and working directly with Apple, shut them down. To minimize your risk, *never* download a

copy of one our apps from a source that is not us or the Mac App Store. We are going to be hyper-vigilant about the authenticity of downloads on our servers.

- **A competitor obtains this source to attempt to use it to their advantage in some way.**
  The many Mac developers we've met over the years are fine, upstanding people. I can't imagine any of them being this unethical, or even being willing to take the risk of us finding fingerprints of our code in theirs. And let's not forget that — you guessed it — there's a good chance any stolen source could have malware slipped into it.

Also, one important thought gave us some comfort:

With every day that passes, that stolen source code is more and more out-of-date.

This hack hasn't slowed us down. That source is already missing a ton of fixes and improvements we committed over the last week alone, and six months from now it will be missing major critical new features. In short: it's old and getting older.

At this point in our discussion, we even half-seriously considered releasing the source code ourselves — and when that idea was floated, and we realized there wouldn't be any fallout (other than a lot of code questions!), that's when we truly felt free.

Assistance

Within 24 hours of the hack, we were on the phone with two important teams: Apple and the FBI.

Apple rallied the right security people quickly to learn all they could about our situation. (They had, of course, already blocked the HandBrake-attached malware for the broader Mac population once it was discovered widely.) They walked us through the best way to roll our Developer ID and invalidate the old one, which we don't think was leaked, but we're being overly cautious. **And more importantly, the right people at Apple are now standing by to quickly shut down any stolen/malware-infested versions of our apps that we may discover.**

The FBI is actively investigating, so I can't say anything more about that.

Together

We'll be working overtime for the foreseeable future to keep an eye on this situation.

But we could also use your help.

If you see any cracked or otherwise unofficial versions of our apps in the wild, it's safest to assume they are infected, and we ask that you please let us know. If you see our source show up somewhere, also let us know. And if you have information that could help with the investigation into this incident, definitely let us know.

The more we know, the more we can use every method available to us — legal, technical, you name it — to fix it.

Feel free to e-mail us or DM us on Twitter anytime — even if you just have questions. We're here.

And as a reminder, never download one of our apps from a source that is not our website or the Mac App Store.

This has been a hard post to write. I hate that this happened. I kick myself every day for not paying attention to what I was doing; the tells were obvious in hindsight. It's a good reminder though — no matter how experienced you might be with computers, you're human, and mistakes are easily made. And even though this doesn't affect our customers directly, we want to apologize that we're even having to have this discussion with you.

We've been doing this 20 years because you keep us going every day — by buying our software, by giving us your good ideas, by telling your friends about us. You are the good in the world. So we're going to do everything we can to rise above this and keep going even further — together.

87 Comments

Frank, S. (2017). 'The Case of the Stolen Source Code'. Panic Blog [Online]. 17 May, 2017. https://panic.com/blog/stolen-source-code/. (Accessed 27 June, 2018). Reprinted with permission.