RISK ASSESSMENT / SECURITY & HACKTIVISM

"TrueCrypt is not secure," official SourceForge page abruptly warns

Support for decade-old crypto program pulled, touching off Internet firestorm.

by **Dan Goodin** - May 28 2014, 1:48pm USMST

457

One of the official webpages for the widely used TrueCrypt encryption program says that development has abruptly ended and warns users of the decade-old tool that it isn't safe to use.

"WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues," text in red at the top of TrueCrypt page on SourceForge states. The page continues: "This page exists only to help migrate existing data encrypted by TrueCrypt. The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform."

The advisory, which Ars couldn't immediately confirm was authentic, touched off a tsunami of comments on Twitter and other social media sites. For more than a decade, the open source and freely available TrueCrypt has been the program of choice of many security-minded people for encrypting sensitive files and even entire hard drives. Last year, amid revelations that the NSA can decode large swaths of the Internet's encrypted data, supporters ponied up large sums of money to audit TrueCrypt. Results from phase one of the audit released last month revealed no evidence of any backdoors. Additional audits were pending.

Matthew Green, a professor specializing in cryptography at Johns Hopkins University and one of the people who spearheaded the TrueCrypt audit, told Ars he had no advance notice of the announcement. He said the announcement appears to be authentic, an observation he repeated on Twitter. He told Ars he has privately contacted the largely secretive TrueCrypt developers in an attempt to confirm the site or get more more details.

The SourceForge page, which was delivered to people trying to view truecrypt.org pages, contained a new version of the program that, according to this "diff" analysis, appears to contain changes warning that the program isn't safe to use. Curiously, the new release also appeared to let users decrypt encrypted data but not create new volumes.

Significantly, TrueCrypt version 7.2 was certified with the official TrueCrypt private signing key, suggesting that the page warning that TrueCrypt isn't safe wasn't a hoax posted by hackers who managed to gain unauthorized access. After all, someone with the ability to sign new TrueCrypt releases probably wouldn't squander that hack with a prank. Alternatively, the post suggests that the cryptographic key that certifies the authenticity of the app has been compromised and is no longer in the exclusive control of the official TrueCrypt developers.

In either case, it's a good idea for TrueCrypt users to pay attention and realize that it may be necessary to move to a new crypto app. Ars will continue to cover this unfolding story as more information becomes available.

PROMOTED COMMENTS

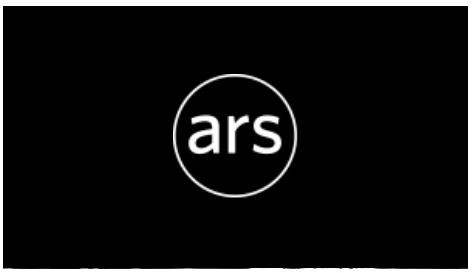
LATEST FEATURE STORY

FEATURE STORY (3 PAGES)

The little-known Soviet mission to rescue a dead space station

How two Cosmonauts battled extreme cold, darkness, and limited resources to save Salyut 7.

WATCH ARS VIDEO



Space Shuttle Enterprise Tour

A mini-documentary on one of NASA's experimental toys, the Enterprise.

STAY IN THE KNOW WITH

cadence | Ars Centurion | et Subscriptor jump to post

I'm stunned.

However, there are too many weird things with this. DNS redirect to sourceforge page, new version with warnings, weird insistence on switching to BitLocker, new keys issued.... it just doesn't add up to a normal project end event. Something is definitely up. I will give it a few more days before I start panic. Let's listen to more explanations from the TrueCrypt developers.

340 posts | registered Mar 26, 2008

---

rodalpho | Ars Centurion jump to post

If this is defacement, it's the most elaborate defacement I've ever seen. They took the time to edit the source so it can only be used to decrypt, not encrypt. Looks likely real to me. Super bizarre.

338 posts | registered Nov 27, 2005

---

k3x | Smack-Fu Master, in training jump to post

Reposting this from Hacker News, not sure if legit:

"Providing some details from SourceForge:

1. We have had no contact with the TrueCrypt project team (and thus no complaints).

2. We see no indicator of account compromise; current usage is consistent with past usage.

3. Our recent SourceForge forced password change was triggered by infrastructure improvements not a compromise. FMI see http://sourceforge.net/blog/forced-password-change/

Thank you,

The SourceForge Team communityteam@sourceforge.net"

9 posts | registered Jan 20, 2010

---

lewax00 | Ars Centurion jump to post

> bbf wrote:
> Why haven't any of the Truecrypt Authors/Maintainers contacted the tech press directly?
>
> Why haven't any *real*(tm) journalists contacted the Authors/Maintainers directly to get the story direct from the source?

From my understanding, the authors of Truecrypt have never spoken publicly, and in fact, no one knows who they are. So that makes the first one unlikely, and the second one impossible.

217 posts | registered Jun 20, 2013

Marlor | Ars Scholae Palatinae jump to post

> bolgerguide wrote:
> This is very strange and I am perplexed. Truecrypt is part of my custom encryption scheme. I'm wondering if all this malarkey is a hijack, extortion, or something more nefarious.

I can't comprehend the conspiracy theories flying around about this.

LATEST NEWS

ACCESS DENIED

Apple’s two-factor authentication now protects iCloud backups

YOUR PRODUCT SUCKS

US law would safeguard free-speech rights to criticize business online

Court upends $368M ruling against Apple for VirnetX patent infringement

20 years, 20 questionable game ratings: A timeline of ESRB oddities

FBI facial recognition system at “full operational capability”

Boeing and SpaceX getting NASA money for manned space launches [Updated]

It's a barely-maintained Open Source project (no updates in the past two years), with an outdated, messy code-base, serious build dependency problems, and lacking in full support for the newest Windows release. It likely only has a small development team - perhaps only one or two people.

The developers are absurdly secretive, and when they do come out of hiding to make a statement, they are confrontational (take, for example, their response to Fedora's queries over the clause in their license that reserves the right to sue for copyright infringement).

If this was any other project, we'd all just assume the developers had decided to call it a day. However, because of the nature of the software, everyone assumes security agencies or reptilians are involved.

> **Quote:**
> Does this have something to do with those Chinese officers the U.S. issued warrants for?

Maybe. Or maybe the developer was a security researcher who has decided to retire to a tropical island. Or maybe there were two developers, and they have had a dispute. Maybe the primary developer took a job offer at a security firm, with a clause prohibiting him from working on external projects. There are an almost infinite range of possibilities... assuming that the cause was the devious acts of state-sponsored actors is leaping to a pretty big conclusion.

> **Quote:**
> How in the hell can an encryption program become unsecure?

If I developed a piece of security software, and wanted to cease development, I'd make a similar statement. *"Don't use this anymore. It's not maintained, and should therefore be considered insecure"*.

Otherwise, if a vulnerability is discovered, everyone will scream: *"Fix it now! Nobody told us to stop using it!"*

1276 posts | registered Oct 3, 2003

READER COMMENTS 457

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE