threat post

CATEGORIES   FEATURED   PODCASTS   VIDEOS

09/16/14   5:59   . @Adobe Gets Delayed Reader Update Out The Door - http://t.co/MtXh5keHkj

Welcome > Blog Home > Cryptography > Audit Project Releases Verified Repositories of TrueCrypt 7.1a

AUDIT PROJECT RELEASES VERIFIED REPOSITORIES OF TRUECRYPT 7.1A

by Dennis Fisher   🐦 Follow @dennisf   June 10, 2014 , 1:59 pm

As the uncertainty surrounding the end of TrueCrypt continues, members of the security community are working to preserve a known-good archive of the last version of the open source encryption software released before the developers inserted a warning about potential unfixed bugs in the software and ended development.

The team behind the Open Crypto Audit Project, which has undertaken an audit of TrueCrypt, has posted a verified repository of TrueCrypt 7.1a on GitHub. There are versions for Windows, Linux and OS X. When the anonymous developers behind TrueCrypt posted a notice on their Web site and SourceForge page in late May saying that the software was not safe to use because it might contain unfixed security vulnerabilities, speculation arose immediately that perhaps the team had been targeted by a National Security Letter, a la Lavabit, or that maybe the developers were sending a subtle message about a backdoor in the application. No word has been forthcoming from the developers, and speculation has continued, but many seem to have come to the conclusion that the developers simply hit a wall with the project.

The message that the TrueCrypt posted about the security of the software also was included in the release of version 7.2a. The OCAP team decided to focus on version 7.1a and created the verified repository by comparing the SHA2 hashes with files found in other

Many seem to have come to the conclusion that the developers simply hit a wall with the

Top Stories

Citadel Variant Used in Attacks Against Middle Eastern Petrochemical Companies
September 16, 2014 , 11:10 am

Home Depot Urges Credit Monitoring Vigilance
September 3, 2014 , 11:06 am

Robert Hansen on Aviator, Search Revenue and the $250,000 Security Guarantee
August 29, 2014 , 3:43 pm

Flaw in Android Browser Allows Same Origin Policy Bypass
September 15, 2014 , 1:32 pm

Researcher Identifies Hidden Data-Acquisition Services in iOS
July 21, 2014 , 12:22 pm

Comcast Pushes Back Against Allegations it Will Cut Off Tor Users
September 15, 2014 , 2:19 pm

Millions of PCs Affected by Mysterious Computrace Backdoor
August 11, 2014 , 4:58 pm

Critroni Crypto Ransomware Seen Using Tor for Command and Control
July 18, 2014 , 10:37 am

WordPress Sites Seeing Increased Malware, Brute Force Attacks This Week
July 23, 2014 , 3:11 pm

With MAMA, U.S. Air Force Aiming to Raise Cyber Awareness on Networks
September 15, 2014 , 3:35 pm

New Signal App Brings Encrypted Calling to iPhone
July 29, 2014 , 2:56 pm

TrueCrypt repositories. So the files are the same as the ones that were distributed as 7.1a.

project.

"These files were obtained last November in preparation for our audit, and match the hash reported by iSec in their official report from phase I of the audit," said Kenn White, part of the team involved in the TrueCrypt audit.

The provenance and integrity of TrueCrypt has been a subject of much debate in the security community. The developers of the software are anonymous and have proven elusive. It took some doing for the OCAP audit team to get in touch with the developers and get the audit started, a project that was meant to answer longstanding questions about the integrity of the application. The events of the last couple of weeks haven't served to calm any of the fears of those who worried that TrueCrypt might have been backdoored or otherwise compromised, despite the clean bill of health produced by the first phase of the audit.

For some, those questions may never be answered fully, but the OCAP team is continuing with its audit, now looking at the cryptographic functions used in the software.

About Dennis Fisher

Dennis Fisher is a journalist with more than 13 years of experience covering information security.

View all posts by Dennis Fisher →

Latest Tweet from: Dennis Fisher

Follow

DennisF
@DennisF

"Cyber-defense has largely been pick-up game, and I don't think that is going to get us anywhere."
threatpost.com/nsa-director-r...

11:48 AM - 16 Sep 2014

Categories: **Cryptography**, **Web Security**

0

Leave A Comment

Your email address will not be published. Required fields are marked *

Name

Email

Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Recommended Reads

September 16, 2014 , 10:18 am

Categories: **Apple**, **Cloud Security**, **Cryptography**, **Mobile Security**, **Privacy**

Apple CEO Defends iMessage Security

by Dennis Fisher

Despite research published last year that demonstrated that Apple has the ability to decrypt users

Read more...
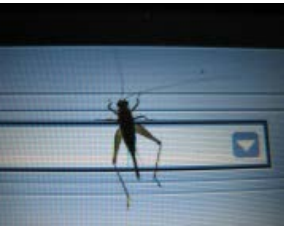
September 15, 2014 , 10:46 am   *Categories:* **Featured**, **Vulnerabilities**, **Web Security**

Big Batch of Bugs Fixed in Various Versions of IDA

by Dennis Fisher

The makers of the popular IDA disassembly and debugging tool have fixed more than a

Read more...

September 12, 2014 , 11:30 am

Categories: **Featured**, **Hacks**, **Vulnerabilities**, **Web Security**

Hacked Brazilian Newspaper Site Targets Router DNS Settings

by Michael Mimoso

A Brazilian political website has been compromised and is injecting iFrames that attempt to change the victim's router DNS settings.

Read more...

The Final Say *From Kaspersky Blogs*

THE KURILS: WHY, WHERE, HOW....

So, where on earth did the idea of a cruise, not around tourist-friendly tropical islands, but around mostly uninhabited – for a reason – polar-esque ones, come from? It's quite simple really… My favo...

Read more…

THEFTS IN REMOTE BANKING SYSTEMS: INCIDENT INVESTI...

An organization recently asked Kaspersky Lab to investigate an incident that had occurred in its corporate remote banking system: a bank asked for confirmation of a payment worth about US$80,000. The ...

Read more…

GOOD GETS BETTER: KIS 2015

Like it or not, your children are going to be on the web. Kaspersky's award-winning parental controls let you monitor their activity and block them from any sites that you choose.

Read more…

WHERE HAVE ALL THOSE MALWARE EPIDEMICS GONE?

It's been years since we've last heard of any large worm epidemics. Does it really mean that malware epidemics have gone away for good?

Read more…

WHY LESS IS MORE...

Many believe that two layers of security will always be better than one. The real-world logic is obvious – if your fortress walls are thick, your enemy can spend an eternity hammering away with little...

Read more…

The Kaspersky Lab Security News Service

AUTHORS

Dennis Fisher

Michael Mimoso

Christopher Brook

Brian Donohue

Anne Saita

CATEGORIES

Apple | **Cloud Security** | **Compliance** | **Critical Infrastructure** | **Cryptography** | **Data Breaches** | **Featured** | **Featured Podcast** | **Featured Video** | **Government** | **Hacks** | **Malware** | **Microsoft** | **Mobile Security** | **Podcasts** | **Privacy** | **Scams** | **Slideshow** | **SMB Security** | **Social Engineering** | **Uncategorized** | **Videos** | **Virtualization** | **Vulnerabilities** | **Web Security**

Newsletter Sign-up | RSS Feeds | Home | About Us | Contact Us