

Hidden Tear Ransomware Developer Blackmailed by Malware Developers using his Code

bleepingcomputer.com/news/security/hidden-tear-ransomware-developer-blackmailed-by-malware-developers-using-his-code/

Lawrence Abrams

By

Lawrence Abrams


- January 25, 2016
- 06:58 PM
- 1

In a post on the BleepingComputer.com forums, the developer of the Magic Ransomware infection is blackmailing the author of the open source Hidden Tear and EDA2 Ransomware Project. The malware developer's demands are simple; take down the Hidden Tear project or the Magic ransomware's victims lose their decryption keys.

This past weekend we reported about the Magic ransomware, which utilized the publicly posted open source EDA2 ransomware project. Unfortunately, the Command and Control servers for the Magic ransomware were hosted on free web hosting sites and were deleted along with the decryption keys. When this happened, Utku Sen, the developer of the open source Hidden Tear and EDA ransomware projects, realized making EDA2 publicly available as an educational project was a mistake and pulled it from github so it couldn't be used in the future.

Today, in our Magic Ransomware Support Topic, a user named jeanclaudevandan, who appears to the ransomware developer, posted that they felt bad for one of the victim's who lost pictures of his newborn baby and would give him his decryption key for free.

jeanclaudevandan #47 <



Posted Today, 11:58 AM

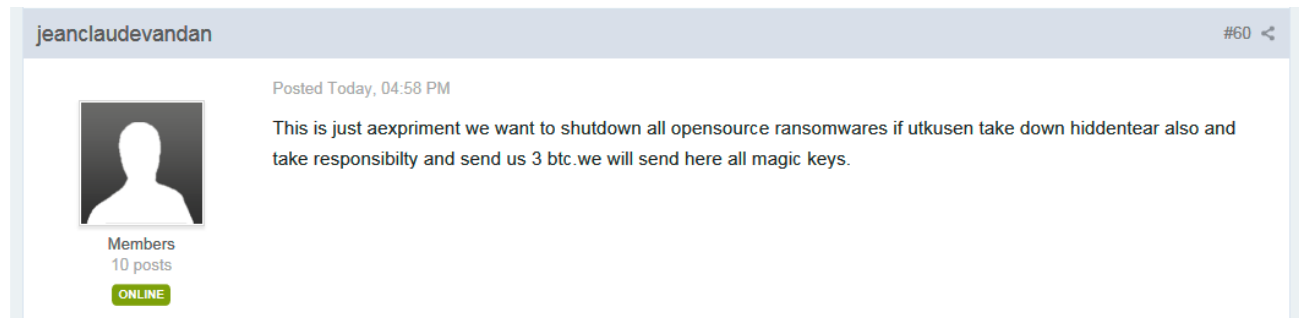
Anyway andriy sent us an email usernameand pname ,we will not publisheddecryptiion prog.this guyz gonna helpyou.Just get the hiddentear decrypter source and change the extension *.locked to *.magic and compile.We will send you your key.

Members
10 posts
ONLINE

Magic Ransomware Developer Offering Key for Free

Soon after, the victim reported that they received the key and we tested that we could indeed use it to decrypt their files. Later in the day, Utku Sen posted in our forum as well stating that he would help as much as possible those who were affected by ransomware

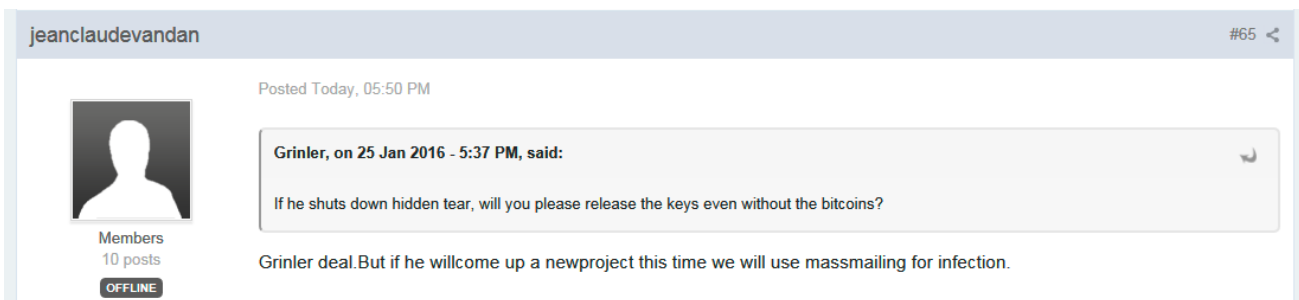
that utilized his project. In response, the user jeanclaudevandan wrote that they would release all the keys if Utku also took down his still visible Hidden Tear ransomware project and paid the malware developer 3 bitcoins.



A screenshot of a forum post by user 'jeanclaudevandan'. The post is titled '#60' and was posted 'Today, 04:58 PM'. The user's profile picture is a silhouette, and their bio indicates they are a member with 10 posts and are currently 'ONLINE'. The post text reads: 'This is just a experiment we want to shutdown all opensource ransomwares if utkusen take down hiddentear also and take responsibilty and send us 3 btc.we will send here all magic keys.'

Second post by the Malware Developer

The reality is that this is a win-win situation. If the victim's could get their keys back and the Hidden Tear project, no matter how vulnerable it is, out of public view, everyone would benefit. After further posting back and forth, the malware developer agreed to release all of the keys if Utku would just take down the Hidden Tear program.



A screenshot of a forum post by user 'jeanclaudevandan'. The post is titled '#65' and was posted 'Today, 05:50 PM'. The user's profile picture is a silhouette, and their bio indicates they are a member with 10 posts and are currently 'OFFLINE'. The post text reads: 'Grinler, on 25 Jan 2016 - 5:37 PM, said: If he shuts down hidden tear, will you please release the keys even without the bitcoins? Grinler deal.But if he willcome up a newproject this time we will use massmailing for infection.'

Third post by the Malware Developer

On one hand, taking down the Hidden Tear project is in the best interests for everyone and the victim's of the magic ransomware get their keys back. On the other hand, giving into the demands of ransomware developers is never a wise policy and may embolden malware developers to make similar threats in the future. At this point we are waiting to hear from Utku Sen about what his next move will be.

Related Articles:

[Cactus ransomware exploiting Qlik Sense flaws to breach networks](#)

[Black Basta ransomware made over \\$100 million from extortion](#)

[Toronto Public Library confirms data stolen in ransomware attack](#)

[Qilin ransomware claims attack on automotive giant Yanfeng](#)

[Police dismantle ransomware group behind attacks in 71 countries](#)

- [EDA2](#)

- [HiddenTear](#)
- [Ransomware](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments

 [Retry2 Photo](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
