Hidden Tear Ransomware Developer Blackmailed by Malware Developers using his Code

By Lawrence Abrams

Published: 2016-01-25 · Archived: 2026-04-05 21:38:04 UTC

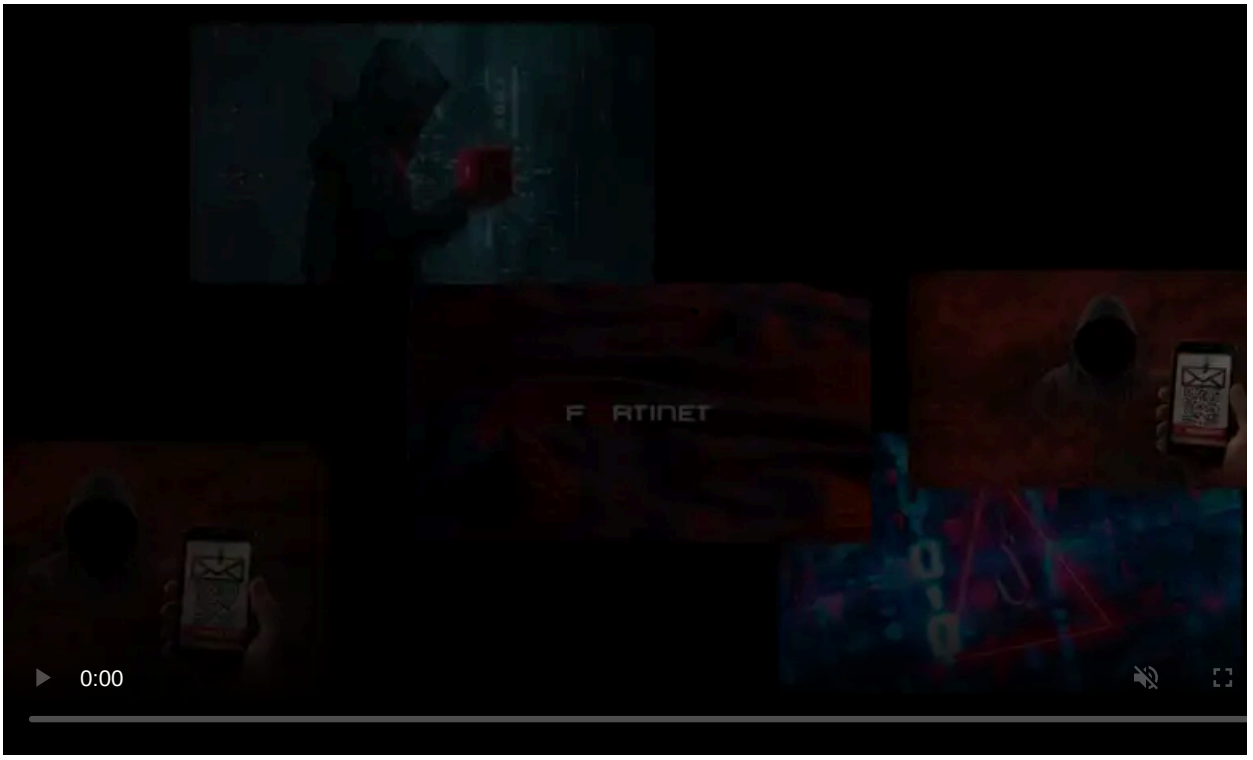
In a post on the BleepingComputer.com forums, the developer of the Magic Ransomware infection is blackmailing the author of the open source Hidden Tear and EDA2 Ransomware Project. The malware developer's demands are simple; take down the Hidden Tear project or the Magic ransomware's victims lose their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

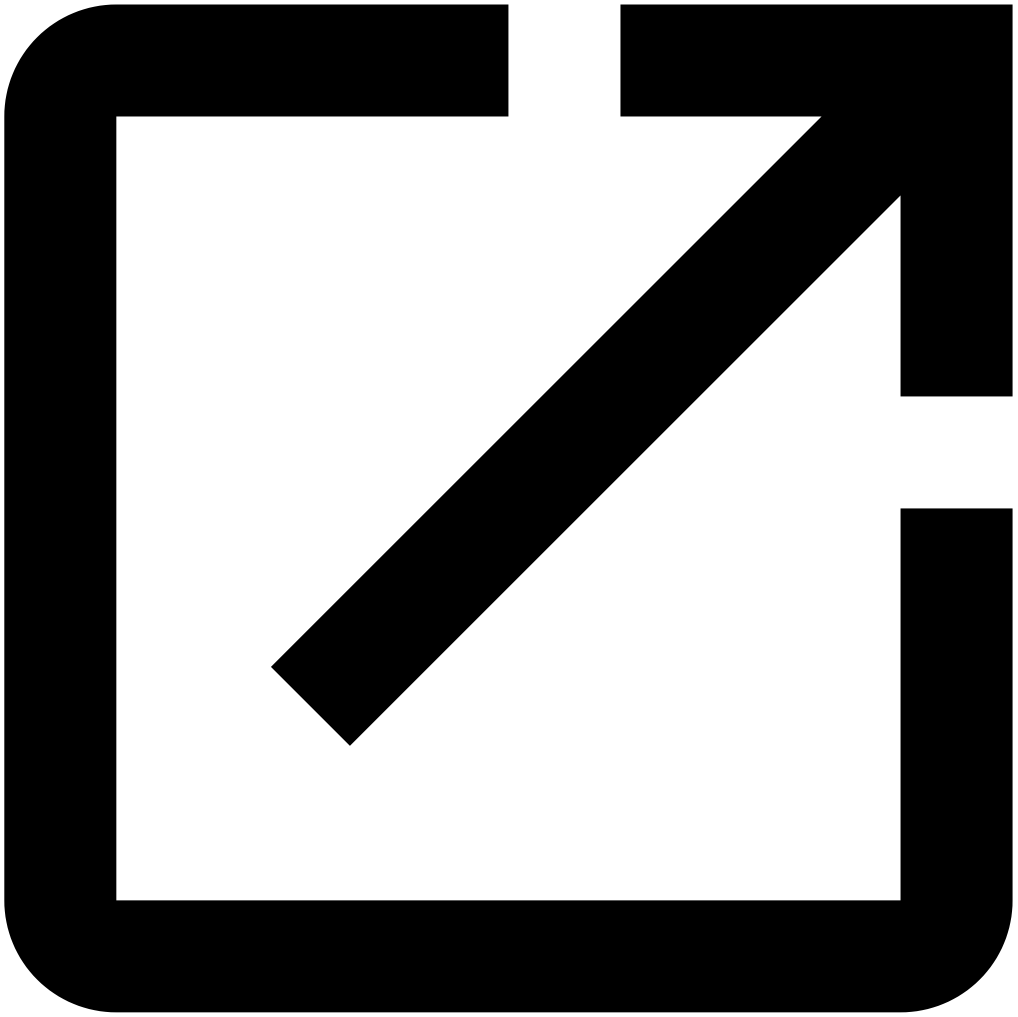
This past weekend we reported about the Magic ransomware, which utilized the publicly posted open source EDA2 ransomware project. Unfortunately, the Command and Control servers for the Magic ransomware were hosted on free web hosting sites and were deleted along with the decryption keys. When this happened, 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.

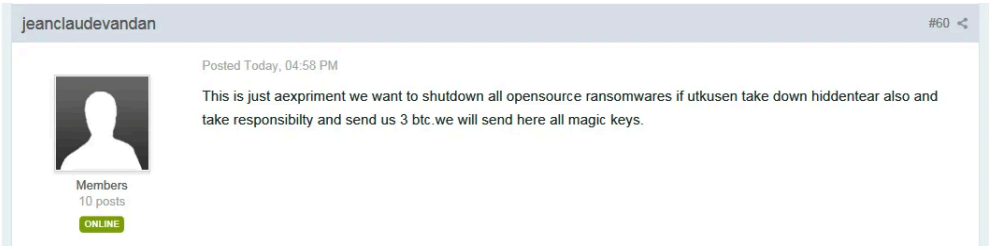
Magic Ransomware Developer Offering Key for Free

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.


F RTINET
0:00

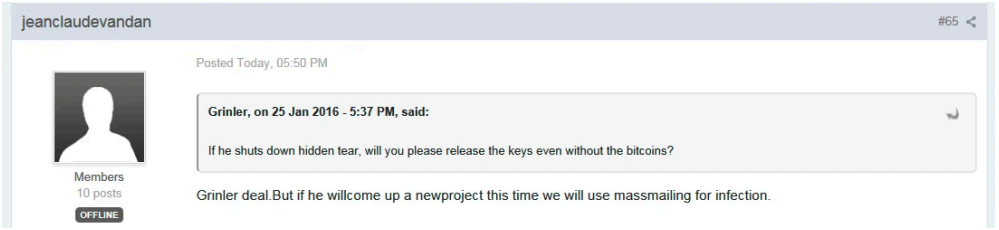


Visit Advertiser websiteGO TO PAGE



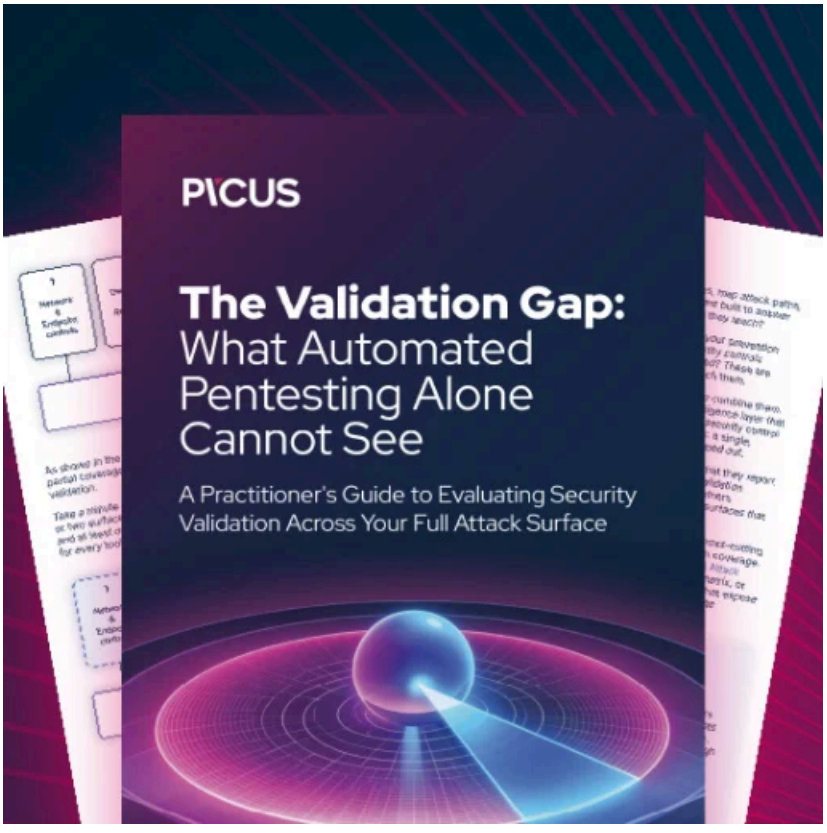
Second post by the Malware Developer

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.



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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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