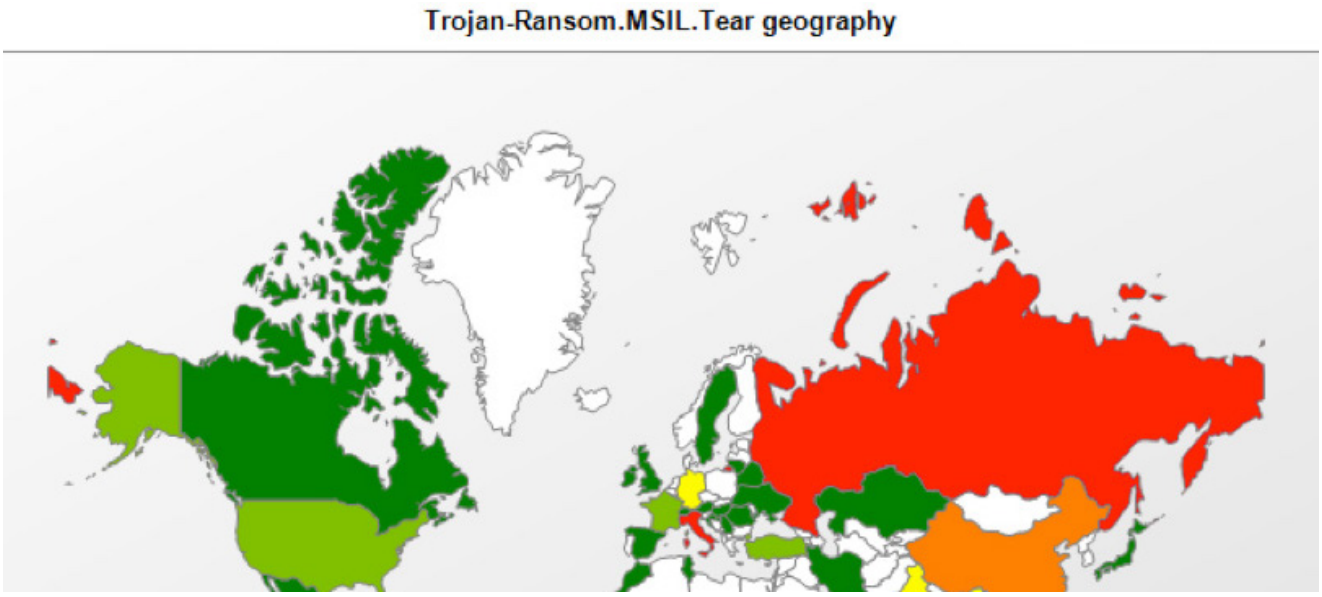
I'm Sorry For Hidden Tear and EDA2

utkusen.com/blog/im-sorry-for-hidden-tear-eda2

Utku Sen - Blog

computer security, programming

Follow @utkusen
21 August 2017



As you all know, I published Hidden Tear's code in August 2015, and EDA2's code in October 2015. I explained the reasons behind these publications several times. To summarise them again:

1. Changing programming language trend to a high level language, so that decompile process will be possible&faster.
2. Destroying the business of ransomware code&service sellers.
3. Using implemented backdoors to decrypt infected files.
4. Providing a ransomware source code for educational purposes

I don't want to talk about them over and over again. Let's just check the outcomes:

1. Yes, trend is slightly changed to a high level language (C#) but it doesn't matter since you can't find a solution for decryption anymore.
2. Their business was slightly broken in 2016, but now it's growing again.
3. Yes we were able to decrypt some cases but the backdoors are fixed by time.
4. That's the only good outcome

Now, we are seeing new Hidden Tear/EDA2 variants appears every day which doesn't have any backdoor. I've already seen this long time ago, and I moved to different things. I want to say that I'm sorry for Hidden Tear/EDA2 experiments, they were total failures. Caused more chaos even my intentation was good.

Note: Some may think that I'm scared after Marcus's case, that's not the thing. I've published Hidden Tear in August 2015, went to Las Vegas in 2016 and 2017. I have no legal problem since I didn't sell this code or used it in criminal activities.

Note 2: I'm seeing some people programmed a variant named EDA3, there is no EDA1 or EDA3 from my side. 2 is not a version number.