



## NEWS

# New Ransomware business cashing in on CryptoLocker's name

Program takes a 10 percent cut of the ransom payment



1

CSO | Nov 12, 2015 4:00 AM PT

A new service launched this week is offering a new Ransomware product under the name CryptoLocker to anyone willing to pay ten percent of the collected ransom. In addition to the core Ransomware product, the ultimate goal of the business owner is to implement additional functions to the malware including linking it to recently produced exploits.

Called CryptoLocker Service, the new venture launched this week on a standalone Darknet website. The new venture is being run by a person using the handle Fakben.

The handle isn't new; it's got quite a past on some of the more criminal parts of the Web.

## MORE ON CSO: How to spot a phishing email

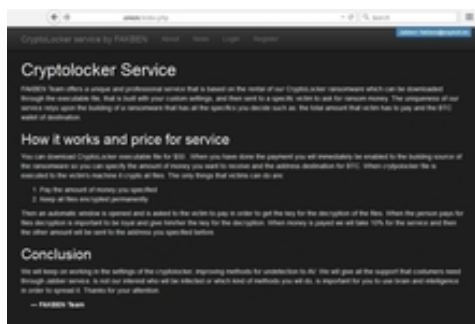
Most recently, Fakben was a former user of the Evolution (Evo) marketplace, a black market that was founded by a known carder (someone who deals with stolen credit card data) after Silk Road was raided and shutdown by law enforcement in 2013.

The owners of Evolution pulled an exit scam and ran off with the money held in escrow for the website's merchants, leading to the eventual shutdown of the site itself. From there, the merchants and customers scattered to the winds, Fakben among them.

Now, a few months later, Evo's former user has launched their own business.

CryptoLocker Service requires a \$50 USD fee, which customers pay in order to get the basic Ransomware payload.

"When you have done the payment you will immediately be enabled to the building source of the ransomware so you can specify the amount of money you want to receive and the address destination for BTC. When cryptolocker file is executed to the victim's machine it crypts all files," the service's website explains.



Once the victim pays the demanded ransom, the payment address will forward the funds – less a ten percent fee – to the Bitcoin wallet designated by the CryptoLocker Service customer. The ransom fee itself can be determined by the customer, but the recommended fee is \$200 USD.

"I prefer to be less expensive, more downloads and more infections," Fakben said during a brief chat with CSO Online.

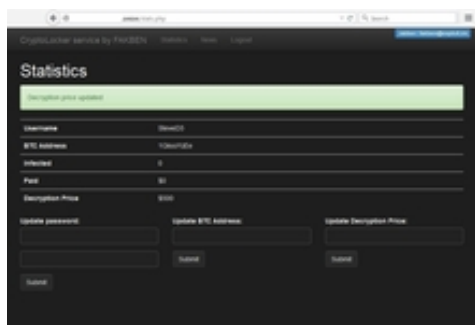
While the new business uses the name CryptoLocker, the code itself is new Fakben said, making it clear that the new code is nothing like the original, which was taken offline by law enforcement in 2014.

However, during the discussion, exact technical details of the malware were not disclosed. For now, the malware only runs on Windows, but there are plans to develop it for other platforms.

In addition to cross-platform and AV avoidance development, Fakben said that by using both internal and outsourced resources, CryptoLocker Service would also move towards internal exploitation.

Depending on what the customer is asking for, and willing to pay, it will be possible to tie the Ransomware payload to a number of exploits targeting vulnerabilities in products such as Adobe and Java.

Those additional services are not part of the core product. If they're used, the customer would still pay the opening \$50 USD fee, plus the exploit cost and development cost, as well as the ten percent commission on each ransom paid.



For now, the customer panel is rather sparse, offering only a basic infection counter and the total amount of ransom paid minus commission. Fakben would not confirm if the new service has gained any customers.

A quick check of their username on a few forms showed no ads for the offering, but Fakben feels there is a market for the service, "people are attracted by [Bitcoin], they feel safe behind this payment, and almost everyone wants to make money in the

deep web."

Depending on the final payload ordered, this new venture will lower the overhead on most campaigns that are reliant on exploit kits pre-configured software, and enable quicker turnarounds on custom development. Both outcomes are bad news to those working to protect users and the Internet at large.

If this business venture sounds familiar, that's because it is. Earlier this year, a service named Tox promised to develop custom Ransomware and asked for 30 percent cut of the final ransom price. Tox folded rather quickly, and most of the payloads were easily detected by basic desktop AV.

Only time will tell if CryptoLocker Service does the same.




Steve Ragan — *Senior Staff Writer*



**Insider: How a good CSO confronts inevitable bad news** ➤

 **View 1 Comment**

## You Might Like

Promoted Links by Taboola 

**This Is What Will Happen When You Eat Avocados Every Day**

AwesomeTips

**The Most Exciting MMORPG You've Ever Played. Don't miss this!**

Sparta Online Game

**Build A Professional Website In Only 10 Minutes !**

Wix.com

**Nords, A Free and Addictive Strategy Game : Turn your Village into an Empire!**

Nords - Online Game

**10 Cars EVERY Man Wants**

Carophile

**The Most Exciting MMORPG You've Ever Played! Don't Miss This!**

Stormfall - Online Game

**The Frederique Constant smartwatch is gorgeous wearable tech**

**Three indicted in JPMorgan hacking case**

**Dow Jones & Co. discloses breach, incident likely related to Scottrade**

**The Multimillion Pound Redesign Of Britain's 2nd Largest City**

**Financial Times**

Copyright © 1994 - 2015 CXO Media, Inc. a subsidiary of IDG Enterprise. All rights reserved.