Forum:Hack Forums

Thread: [News] 500,000 victims of GameOver ZeuS can recover their files for free !

Aura - *August 6, 2014, 5:14 am*

Hey guys, Aura here ?

So you guys all know about the GameOver ZeuS botnet that was taken down around a month ago by authorities around the world, right (remember that 2 weeks warning before everything goes down) ? Well, not only the botnet got taken down, but also, 500,000 owner of computers that were infected with that botnet (which infected a computer with a Cryptoware) will also be able to decrypt their encrypted files, and this for free !

FireEye and Fox-IT who participated in the botnet takedown managed to retrieve 500,000 private keys used for the encryption of files on the infected computers through different GameOver ZeuS Command and Control centers. Which means that 500,000 infected computers can now have their files decrypted with the private key that is in the lot that FireEye and Fox-IT retrieved.

They created a website called "Decrypt CryptoLocker" that allows you to get your encrypted files by CryptoLocker (from the GameOver ZeuS botnet) decrypted with the help of your private key in the 500,000 they have (if yours' in it). All you have to do is to go on the website, enter your e-mail address as well as upload one of your file that have been encrypted (plus enter the captcha) and send it to the website. Your file will be analyzed to find the private key used for it's encrypted, and you'll be e-mailed a master description key (your private key) along with a download link to the recovery program (this is a direct download link) that you'll be able to use to decrypt all the encrypted files on your computer.

Quote:
Cryptolocker victims to get files back for free
[img]http://news.bbcimg.co.uk/media/images/76753000/jpg/_76753656_497953315.jpg[/img]
Before now Cryptolocker victims had to pay a hefty fee to get the keys to unlock their data

All 500,000 victims of Cryptolocker can now recover files encrypted by the malware without paying a ransom.

The malicious program encrypted files on Windows computers and demanded a substantial fee before handing over the key to the scrambled files.

Thanks to security experts, an online portal has been created where victims can get the key for free.

The portal was created after security researchers grabbed a copy of Cryptolocker's database of victims.

"This time we basically got lucky," said Michael Sandee, principal analyst at Fox-IT - one of the security firms which helped tackle the cyber-crime group behind Cryptolocker.

Cash call

In late May, law enforcement agencies and security companies seized a worldwide network of hijacked home computers that was being used to spread both Cryptolocker and another strain of malware known as Gameover Zeus.

This concerted action seems to have prompted an attempt by the gang to ensure one copy of their database of victims did not fall into police hands, said Mr Sandee.

What the criminals did not know, he said, was that police forces and security firms were already in control of part of the network and were able to grab the data as it was being sent.

Evgeniy Bogachev was believed to be living in Russia, the FBI said
The action also involved the FBI charging a Russian man, Evgeniy Bogachev, aka "lucky12345" and "slavik", who is accused of being the ring leader of the gang behind Gameover Zeus and Cryptolocker.

The Gameover Zeus family of malware targets people who bank online, and is thought to have racked up millions of victims.

Cryptolocker was created by a sub-group inside the larger gang, said Mr Sandee, and first appeared in September 2013, since when it has amassed about 500,000 victims.

Those infected were initially presented with a demand for $400 (£327), 400 euros ($535; £317) or an equivalent amount in the virtual Bitcoin currency. Victims had 72 hours to pay up or face the keys that would unlock their files being destroyed.

Analysis of the back-up database indicates that only 1.3% of all the people hit by the malware paid the ransom.

Despite the low response rate, the gang is believed to have netted about $3m from Cryptolocker. Many of those caught out did not pay because they were able to restore files from back-ups.

However, others are believed to have lost huge amounts of important files and business documents to the cyber-thieves.

"There's a bit of guesswork in that figure because some of it was paid in bitcoins and that does not have a fixed exchange rate," said Mr Sandee.

Now, security firms Fox-IT and FireEye - which aided the effort to shut down the Gameover Zeus group - have created a portal, called Decrypt Cryptolocker, via which any of the 500,000 victims can find out the key to unlock their files.

"All they have to do is submit a file that's been encrypted from that we can figure out which encryption key was used," said Greg Day, chief technology officer at FireEye.

Mr Day said people wishing to use the portal should submit a file that did not contain sensitive information to help it verify which key they needed.

Source : Cryptolocker victims to get files back for free on BBCNews
Also : Get out of jail free card for Cryptolocker victims via betanews
And : FireEye, Fox-IT launch free service to combat Cryptolocker ransomware on ZDNet

It's things like that makes me want to pursue my path into IT Security and ultimately work for a IT

Security for the good of the population and help others ?

FireEye, I love you <3 (you too Fox-IT <3)

?OpDoritos - *August 7, 2014, 2:12 pm*
This is a really interesting report.
Thanks for posting this sort of stuff, I enjoy this type of white hat news.

Aura - *August 7, 2014, 2:21 pm*
(Aug 7, 2014 02:12 PM)?OpDoritos Wrote: *[CITE]* This is a really interesting report.
Thanks for posting this sort of stuff, I enjoy this type of white hat news.
I enjoy them as well, love them ?

Daxe - *August 7, 2014, 3:44 pm*
This is really great news for a lot of people! I'm glad they got those keys