

Forum:[Hack Forums](#)

Thread: [New Cryptoware, ZeroLocker, with no chances of recovering your files](#)

Aura - August 20, 2014, 8:33 am

Hey guys, Aura here with another [WARNING] thread.

In the last year (or two years), a new kind of malware emerged from the Black Hat Forums, a combinaison of Ransomwares and Encryption malware, that comes together under the name of "Cryptowares". These malwares encrypt files with pre-defined extensions on a system (like .png, .mp3, .docx, etc.) and then totally lock down your computer, and ask you to pay for a ransom in order to decrypt these files. There's no ways to actually decrypt these files, except to pay the ransom, find a flaw in the malware, retrieve the private key used for the encrypted and decrypt the files yourself, or to restore the encrypted files from a back up or Windows Shadow Volume Copy service. These malwares became so popular, that many developpers started creating their own variants, making Cryptowares one of the most efficient malware-related way to make money. However, this Cryptowares method boum attracts a lot of malware developpers, experienced like inexperienced.

[img]<http://www.bleepstatic.com/swr-guides/z/zerolocker/zerolocker.jpg>[img]

ZeroLocker, a new variant of the first Cryptoware, CryptoLocker has been released and is now being spread. ZeroLocker encrypts your files using the AES encryption pattern and once its done, it will display a warning note explaining you the situation and telling you that it can actually "help" you regain your files for a starter price of \$300 in BTC, that will raise to \$600 in 5 days and \$1000 in 10 days (all in USD). A new feature in that Cryptoware is that it will actually encrypt EVERY files on your C: drive, even executable files except if they are in specific "white-listed" folders (the ones that contains the words Windows, WINDOWS, Program Files, ZeroLocker and Desktop) or if they are larger than 20MBs of size. Once a file has been successfully encrypted, ".encrypted" will be appended to its file name . After that, the following command will be ran :

Code C:\Windows\system32\cipher.exe /w:C:\

This command overwrites all the deleted data on your C: drive, which then prevents the user from using data recovery tools (such as EaseUS Data Recovery Wizard, Recuva, GetDataBackNTFS, etc.) in order to recover the data and restore the files. A folder called "ZeroLocker" will be created directly on the C: drive, and it will contain various files and the executable of the decryptor used to decrypt your files if you pay the ransom, called ZeroRescue.exe. This executable is called on Startup via the registry when you login to your computer.

However, here comes the biggest flaw that makes this Cryptoware the most dangerous one to this day. When ZeroLocker uploads the decryption key used to encrypt the files on a system to the Command and Control (C&C) server, it will returns a 404 status error code, which means that the request page on the server doesn't exist on the server. Usually, this upload should return a HTTP 200 status code, which means that the webpage was accessed successfully. In the end, this will result in the loss of the decryption key used for the encryption of the files on a system. Which means that even if you pay the ransom, your private key will not be returned by ZeroLocker in order to be used to decrypt your files. Which means that you'll basically pay the ransom and receive nothing in exchange. The only way to recover that key would be to manually explore the HTTP access logs, if the developper even keeps them or go through them. And this is if they aren't being deleted or rotated (overwritten) already. This is a big coding mistake (flaw) from the developper that released

the product too quickly and didn't test it first. Without the private key, there's no way to decrypt your files as the encryption used is too strong to be broken.

[img]http://www.bleepstatic.com/swr-guides/z/zerolocker/404-error.jpg[/img]

However, there's one solution left for those who would get infected with ZeroLocker. This malware does not delete the Windows System Restore Points, which means that you can restore precedent version of your files using programs like Shadow Explorer or use the in-built "Previous Version" feature in Windows (requires you to have the Windows Shadow Volume Copy service enabled however).

To this day, this Cryptoware is the most dangerous there is, not only because it also encrypt your executable files and have the highest ransom of all the Cryptowares, but because of it's coding flaw, it offers you NO CHANCES AT ALL to recover your encrypted files via the ransom you pay and the only way to get that data back is to restore it from the Previous Versions or a back-up you took.

Researchers at Kaspersky's Lab analyzed the malware and state that this malware, is inspired by CryptoLocker, borrows a few of it's features but also add its own to make it more dangerous, not even counting the loss of the private key along the process.

I wrote this article by reading Grinler's post on BleepingComputer here : [ZeroLocker - a new destructive encrypting ransomware](#)

The credits for the pictures and information contained in this thread goes to him entirely, good job Grinler.

Another article on ZeroLocker has been published on ZDNet, here : [New ZeroLocker crypto-ransomware offers discount for paying up quickly - or \\$1,000 in Bitcoin](#)

Once again, I cannot stress enough of how backing up your data is important these days with these Cryptowares around, and even with the other malwares. Having an external HDD or Cloud Storage with scheduled back-up operations is a must-have now a day in order to have a rescue plan in case something bad really happens, and not only something caused by malwares.

[CryptoPrevent](#), developped by FoolishIT can also be used to prevent ZeroLocker (and other Cryptowares and even other malwares) from being executed on your system. This tool have both a free and a paid version, however, the free should do a good job by itself.

Once again, be very, very careful of what you do on the web and your computer guys.

Stay safe and secure.

LiveMChief - August 20, 2014, 9:33 am

I wonder what these people would make if they made things that would HELP people and not steal from them.

Meow - August 20, 2014, 9:35 am

Another great share by Aura.

Can you PM me your skype I have some questions?

Thanks. ?

Marky Marky - August 20, 2014, 3:53 pm

Holy shit, that's crazy. I assume this zero locker is disguised as a .exe?

0x03a8 - August 20, 2014, 4:00 pm

(Aug 20, 2014 03:53 PM)Shade Wrote: [\[CITE\]](#) Holy shit, that's crazy. I assume this zero locker is disguised as a .exe?

You can spoof extensions.

I'm creating a system restore point right now -.- just in case.

Aura - August 20, 2014, 4:02 pm

(Aug 20, 2014 09:33 AM)LiveMChief Wrote: [\[CITE\]](#) I wonder what these people would make if they made things that would HELP people and not steal from them.

The designer of this tool would fail to make whatever else.

(Aug 20, 2014 03:53 PM)Shade Wrote: [\[CITE\]](#) Holy shit, that's crazy. I assume this zero locker is disguised as a .exe?

It's launched from an executable file, yes. Maybe not an .exe, but an executable file : .src, .pif, .com, .bat, etc.

(Aug 20, 2014 04:00 PM)0x0b08 Wrote: [\[CITE\]](#) You can spoof extensions.

I'm creating a system restore point right now -.- just in case.

Consider investing in an external HDD and install CryptoPrevent as well.

goinblind - August 20, 2014, 4:06 pm

how can u get infected by this virus

Aura - August 20, 2014, 5:42 pm

(Aug 20, 2014 04:06 PM)goinblind Wrote: [\[CITE\]](#) how can u get infected by this virus

Most likely the standard way, via email with infected attachments.

john12 - August 21, 2014, 12:33 am

Are they the same guys who created cryptolocker?

He must be really stupid,if paying the ransom does not decrypt files,then why would someone pay?

Meow - August 21, 2014, 1:45 am

Huh?

Not sure what is happening but someone copy/pasted thread from other one or it's you Aura with another name?

Spoiler [\(Click to View\)](#)

Is that you Aura on 2 forums or someone copy pasted from your thread?

?

Aura - August 21, 2014, 3:17 am

(Aug 21, 2014 01:45 AM)Meow. Wrote: [\[CITE\]](#) Huh?

Not sure what is happening but someone copy/pasted thread from other one or it's you Aura with another name?

Spoiler [\(Click to View\)](#)

Is that you Aura on 2 forums or someone copy pasted from your thread?
?

PM me the forum name where this was posted, as I'm on multiple forums.

Meow - August 21, 2014, 7:15 am

(Aug 21, 2014 03:17 AM)Aur? Wrote: [\[CITE\]](#) PM me the forum name where this was posted, as I'm on multiple forums.

Sent you PM,it's probably you but eh..?
?

Grindle - August 30, 2014, 5:22 pm

Thanks for the share Aura :). Interesting to see what countermeasures could be used against this sort of threat.

joneh heil - August 31, 2014, 6:57 am

Great share Aura! This is a really interesting topic.

CypherOSINT - August 31, 2014, 4:33 pm

Very good thread ! Thanks aura for sharing.Have you heard about Citroni . That is some well planned ransomware. That is doing some mayor damage and the method it uses makes it difficult to track down the culprit.

Hopsin - August 31, 2014, 4:37 pm

Great share like always. Thanks for the info aura.

xVulnerable - September 1, 2014, 2:27 am

I need to get a copy of this (for analyzing purposes), anybody know where I can get a sample?

Supreme??????? - September 1, 2014, 5:10 am

Thanks for warning us, Aura. Will keep a lookout for this.

sl??g?T of ???D - September 3, 2014, 5:50 am

This happened to one of my business customers. Sales guy opened an email, and it got to Mapped network drives containing almost everything. The customer chose to pay the ransom and we did in fact get data back. Although it took three days to decrypt. (The version we ran into was a copycat - cryptowall)

And... they are also now paying me for data management services to ensure that something like this never happens again.

Here lately I have been preaching back ups like a Southern Baptist Evangelical.

Thanks for this thread man, this is something that everyone should be aware of!

youlded - has1 - September 3, 2014, 6:13 am

(Aug 20, 2014 08:33 AM)Aur? Wrote: [\[CITE\]](#) ZeroLocker, a new variant of the first Cryptoware, CryptoLocker has been released and is now being spread. ZeroLocker encrypts your files using the AES encryption pattern

If this tool uses aes then it should be pretty easy to get the decryption key since its the same as the encryption key, just look up or reverse the malware and get the encryption key they use to encrypt your data....

They only way they could keep the encryption and decryption key seperate is if they used RSA, OP
i am sure they are using RSA and not aes based on your description.

sl??g?T of ???D - September 3, 2014, 6:23 am

(Sep 3, 2014 06:13 AM)youlded1971 Wrote: [\[CITE\]](#) If this tool uses aes then it should be pretty easy to get the decryption key since its the same as the encryption key, just look up or reverse the malware and get the encryption key they use to encrypt your data....

They only way they could keep the encryption and decryption key seperate is if they used RSA, OP
i am sure they are using RSA and not aes based on your description.

The original was AES, but some spin off copycats (like cryptowall) use RSA

gunman2 - September 6, 2014, 11:49 pm

thanks for information.

[img]http://massonlinesolutions.com/banner/clicxabids_468_60.jpg[/img]

<https://bitly.com/1CEk5zl>

Jaatinen - September 7, 2014, 4:55 am

Great post Aura.

Really interesting. Hopefully I ain't getting infected by this cryptoware :S

Tho this "lisence" would be more expensive than my computer, since my computer costs around 200\$ and is from 2007.

PatientZero - September 9, 2014, 2:40 pm

Thnx for the info Aura.

Hopefully and slowly this should fade away.

john12 - September 11, 2014, 12:45 pm

How there have been so many variants and copycats of cryptolocker,its source code was never leaked...

Didn't know it was so easy to create encrypting ransomware

Koffee - September 15, 2014, 11:21 pm

Dam I would expect no less from Aura, helping people educate themselves. Personally, if it was me I would just buy a new hard drive or computer, because if they're asking me to pay \$300-1000 then that would cost more than my actual computer. But I really hope this doesn't get bad and infect innocent people like the elderly and really young kids who have no idea what they're doing on the internet. But anyways, cheers for the post Aura, and stay safe everyone.

OfficialAndroid - September 28, 2014, 4:54 pm

Holllllly sheeeeeeeit... This is long lol, read it all and 10/10!!!

Aura - October 1, 2014, 6:37 pm

Looks like some people still read my [WARNING] threads eh ? Well, I'm glad that you enjoy them ?