MALWARE | THREAT ANALYSIS

VirLocker's comeback; including recovery instructions

Posted January 25, 2017 by nscott

https://blog.malwarebytes.com/threat-analysis/2017/01/virlockers-comeback-including-recovery-instructions/

VirLocker is in no way new, it has been making a mess of victim's machines for quite a few years now. VirLocker was the first example of a mainstream polymorphic ransomware and it left no expense of misery to its victims.

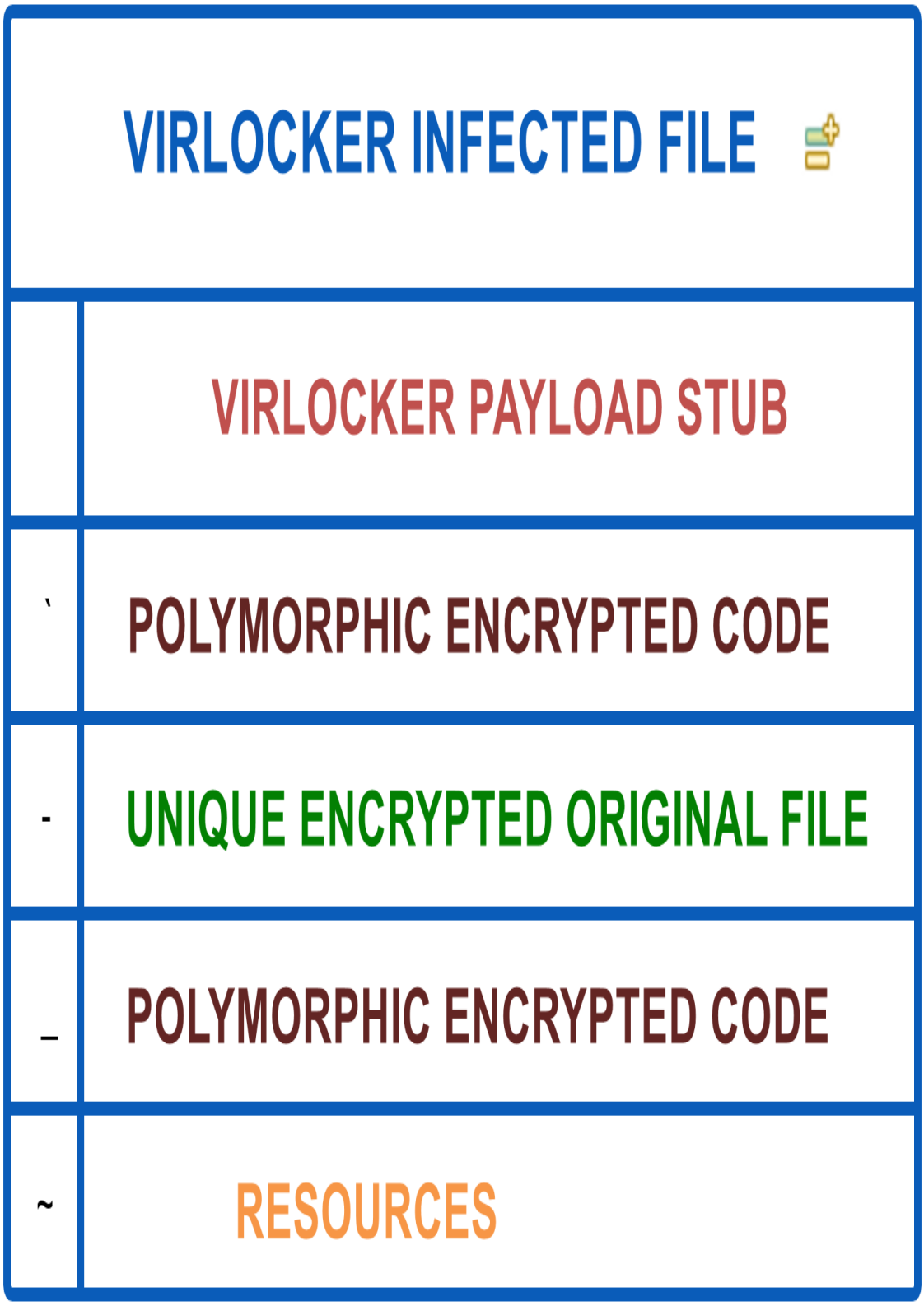
VirLocker can of course be propagated like any other malware from its author, but VirLocker has a trick up its sleeve when it comes to infecting other users. Because every file that VirLocker touches becomes VirLocker itself, so many users will accidentally send an infected version of a file to friends and colleagues, backups become infected, and even applications and EXE's are not safe. Basically, when getting infected by VirLocker, you can no longer trust a single file that is on the affected machine.

This presents a problem when attempting to clean up the machine, because nothing can be trusted and every tool you use is dirty. Even attempting to download a tool to help you can prove a problem, because VirLocker will attempt to infect the new file before it is even opened if VirLocker is running on the machine.

However, if you find yourself infected with this variant DO NOT attempt to remove it yet! Not only does this article discuss the ransomware and how it works, but it will also show you how you can get your files back without paying the ransom.

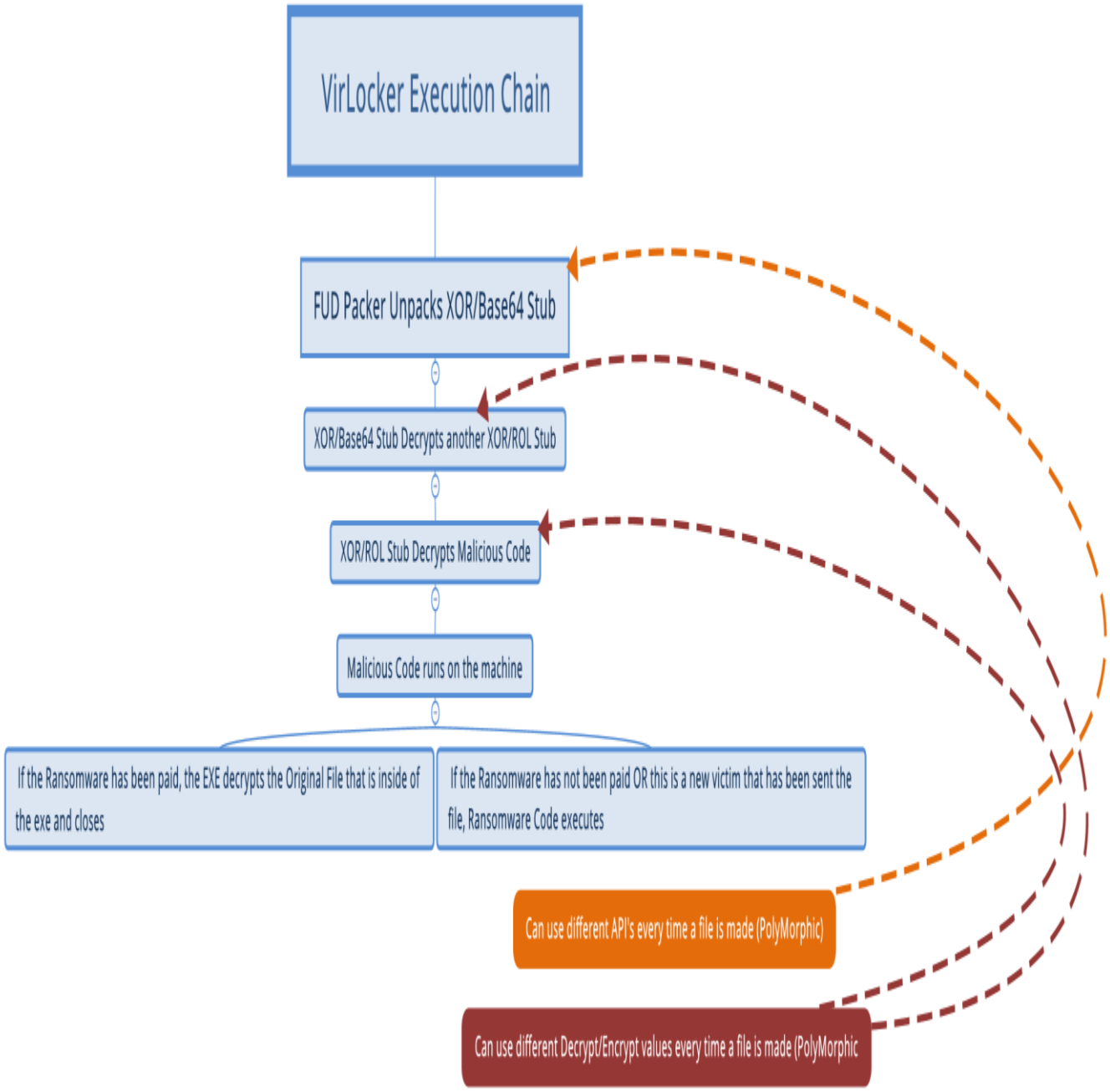
Polymorphic functionality of VirLocker

VirLocker's polymorphic abilities are a headache for everyone involved, researchers, victims, security companies, and more. Every time VirLocker adds itself to a file, the file is practically different in many ways than any other version of itself. VirLocker can add "Fake Code" to itself in certain sections to cause the file to be different, it can use different API's in the main loader of the malware to avoid section fingerprinting, it can use different XOR and ROL seeds to make the encrypted content of the exe entirely different, and more. This level of polymorphic functionalities makes it astonishingly hard to deal with. When even the unpacker stub is different in every file, which could typically be used to fingerprint every variant, it only leaves behavior and heuristics as a possible method of detection.


VIRLOCKER INFECTED FILE
VIRLOCKER PAYLOAD STUB
`
POLYMORPHIC ENCRYPTED CODE
-
UNIQUE ENCRYPTED ORIGINAL FILE
_
POLYMORPHIC ENCRYPTED CODE
~
RESOURCES

As you can see with the above graph of a sample VirLocker infected file, if the payload stub can be different each creation, and the encrypted code is always seeded different, the embedded original file will of course always be different, depending on the file it attacks, and the resources are just a small icon of the original file it attacked. This leaves very little that is suitable for detection.

VirLocker's execution chain



VirLocker's execution is anything but simple and really reflects more of a mix of multiple protection types we have seen in single case ransomware scenarios. When the infection

is executed, the FUD packer (which can be in some ways polymorphic itself) unpacks the first decryption function which is a mixture of Base64 and XOR and is always differently seeded. This new decryption function then decrypts another new decryption function that is a mixture of XOR/ROL and is always differently seeded. This decryption function then finally gets to the malicious code intended to run on the machine.

At this point the ransomware checks if it has already infected the machine, and if so, has it been paid? If it has been paid, the ransomware then becomes benign, and simply decrypts and extracts the original file that it had embedded inside of itself, and closes. If the user has been infected, but hasn't paid, it simply opens the ransomware screen locker again, if it's not open.

If it is a new victim, the ransomware opens the file embedded inside itself to make the user think all is well. For example, if the user B received a picture from their friend, user A, that was infected, once user B opens the file, the ransomware will show them the embedded intended picture, but then continue to infect the machine in the background. This is the background to how this ransomware self-replicates itself.

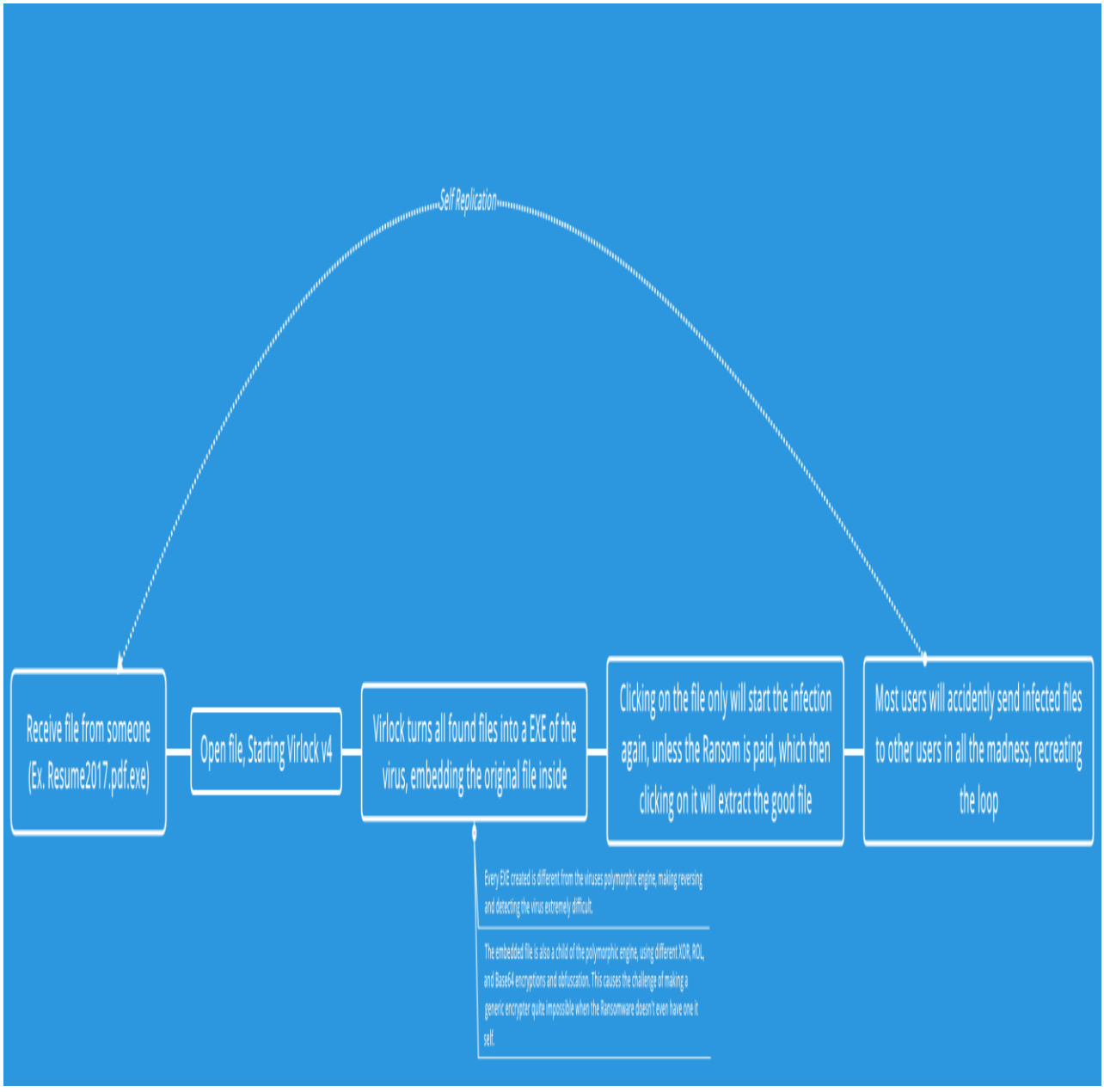
guest.bmp.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000230	00000238	0000023C	00000240	00000244	00000248	0000024C	00000250	00000252	00000254
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0013A000	00001000	0013A000	00000600	00000000	00000000	0000	0000	60000020
.rdata	00002000	0013B000	00002800	0013A600	00000000	00000000	0000	0000	40000040
.data	0014C000	0013D000	0014C000	0013CE00	00000000	00000000	0000	0000	C0000040
.rsrc	00001200	00289000	00001200	00288E00	00000000	00000000	0000	0000	C0040020

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00024630	32	32	75	52	33	70	4C	32	69	64	54	45	4E	43	52	50	22uR3pL2idTENCRP
00024640	51	31	6C	32	79	57	69	51	32	58	63	50	41	47	30	32	Q1l2yWiQ2XcPAG02
00024650	4A	73	61	32	69	50	74	70	63	67	62	32	77	33	62	32	Jsa2iPtpcgb2w3b2
00024660	52	71	67	33	38	70	45	39	33	69	61	32	47	57	48	45	Rqg38pE93ia2GWHE
00024670	71	43	52	39	54	58	55	32	34	62	4B	75	32	49	53	32	qCR9TXU24bKu2IS2
00024680	58	72	55	34	35	66	6E	4C	32	71	49	50	41	55	66	39	XrU45fnL2qIPAUf9
00024690	6F	32	6E	75	4E	7A	63	32	65	52	70	4C	75	66	50	4E	o2nuNzc2eRpLufPN
000246A0	6D	52	6E	68	73	20	64	61	30	52	6E	65	6C	52	6D	38	mRnhs.da0RnelRm8
000246B0	69	77	54	53	50	71	75	76	65	32	50	36	4C	69	23	37	iwTSPquve2P6Li#7
000246C0	44	63	35	51	61	32	32	41	40	32	40	32	56	52	50	6E	Dc5Qa22A@2@2VRPn
000246D0	4C	52	6E	75	32	55	58	72	69	68	4C	77	40	71	78	4E	LRnu2UXrihLw@qxN
000246E0	32	77	78	66	32	52	6D	77	44	47	63	73	32	41	6D	79	2wxf2RmwDGcs2Amy
000246F0	32	58	78	4B	31	52	78	46	32	6D	35	54	32	63	69	35	2XxK1RxF2m5T2ci5
00024700	59	71	59	4C	6E	63	62	54	32	49	43	6B	58	6E	6E	4C	YqYLncbT2ICkXnnL
00024710	55	57	67	5A	32	32	67	67	33	53	50	20	32	4C	76	72	UWgZ22gg3SP 2Lvr
00024720	34	76	4C	32	54	45	71	47	35	6C	38	20	42	4B	35	32	4vL2TEqG518 BK52
00024730	57	6E	33	4B	32	4C	6C	48	41	56	53	32	6F	63	52	32	Wn3K2L1HAVS2ocR2
00024740	37	64	5A	5A	33	45	61	32	55	62	61	32	78	74	63	4C	7dZZ3Ea2Uba2xtcL
00024750	77	66	39	6A	33	5A	52	32	38	50	48	75	77	76	78	6E	wf9j3ZR28PHuwvxn
00024760	54	39	63	32	33	64	75	44	32	23	53	32	57	6D	4A	64	T9c23duD2#S2WmJd
00024770	37	32	32	63	6B	78	6C	70	47	6D	4E	51	43	32	50	4D	722ckxlpGmNQC2PM
00024780	39	20	30	32	4D	4E	63	67	4E	52	6D	53	4A	52	50	39	9 02MNcgNRmSJRP9

Example of what the original good file embedded in the virus looks like.

VirLocker overview



The image above shows the journey and issues that VirLocker presents. Not only is the virus hard to detect, it also has methods to continue existing without the help of the malware author. If anyone ever infected by VirLocker happened to send out any files after they were infected, thinking it was just a screen locker, those files will infect more people. This continuous loop of infection can cause VirLocker to spread like wildfire.

Upon opening VirLocker, it will add itself to nearly every file on the machine, ranging from mere pictures all the way to actual applications. Clicking on these files after the infection will only cause the ransomware to run again, or in the case of a new victim, infect them.

Only after “Paying” the ransom, will these files extract their inner “Good Version” on the machine.

With all the madness that this ransomware causes, it has proven to be an amazing infection spreading method. Imagine you get this infection and think it’s just a screen locker like you have heard about. You somehow manage to remove the infection and think you are in the clear. Because extensions are turned off, you do not see that EVERY file on your machine now has a .exe extension added to it behind its original extension. You send your resume to a company you’re applying to and soon enough that whole business is infected.

VirLocker “Decryption” and clean up

DISCLAIMER: If you are infected with VirLocker, you are dealing with a very live and messy piece of malware. It is extremely easy to accidentally cause it to travel to other machines. It’s highly recommended before performing the steps below, that you isolate the machine from any other hardware or network. We cannot be responsible for anything that may happen to your or others machines while following the below instructions because of the nature of the malware.

If you find yourself infected with VirLocker and want your files back, DON’T REMOVE IT RIGHT AWAY. We need to trick the infection into thinking that you have paid the ransom, so you may get your original files back first. If you have removed the infection, clicking on any of the “encrypted/infected” files will bring up the screen again that VirLocker uses.

IF YOU HAVE ALREADY CLEANED THE MACHINE, CONTACT PROFESSIONAL HELP BEFORE TRYING TO REINFECT IT. DO NOT REINFECT THE MACHINE TO SIMPLY FOLLOW THESE STEPS.

Because of how messy VirLocker is and seeing how it doesn’t even have a cleanup method or decryption method internally, our goal here is to help you get back your important files, and completely reformat the machine afterwards. This post will only focus on helping you get back important files. After this is completed, a complete reformat should be done, since nothing on the machine should be trusted after this infection.

Unauthorized or pirated software has been detected. Your system has been blocked.

Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 250 USD

If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.

You will be charged, fined, convicted for up to 5 years.

There are two ways to pay a fine:

1. You can pay your fine online through BitCoin. BitCoin is available nationwide.

Click the tabs below to find the nearest ATM or exchange.

Your computer will be unlocked after you make your payment.

2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.

Your computer will be unlocked within 4-5 working days.

To regain access now, transfer BitCoin to the following address (click to copy):

1JXum7vGYaUeWZadJrZHGE4tnAQZm8esd3

After the payment is finalized enter Transfer ID below.

Online fine payments are securely processed by Chase Paymentech.

Amount: Transfer ID:

BTC 0.283

PAY FINE

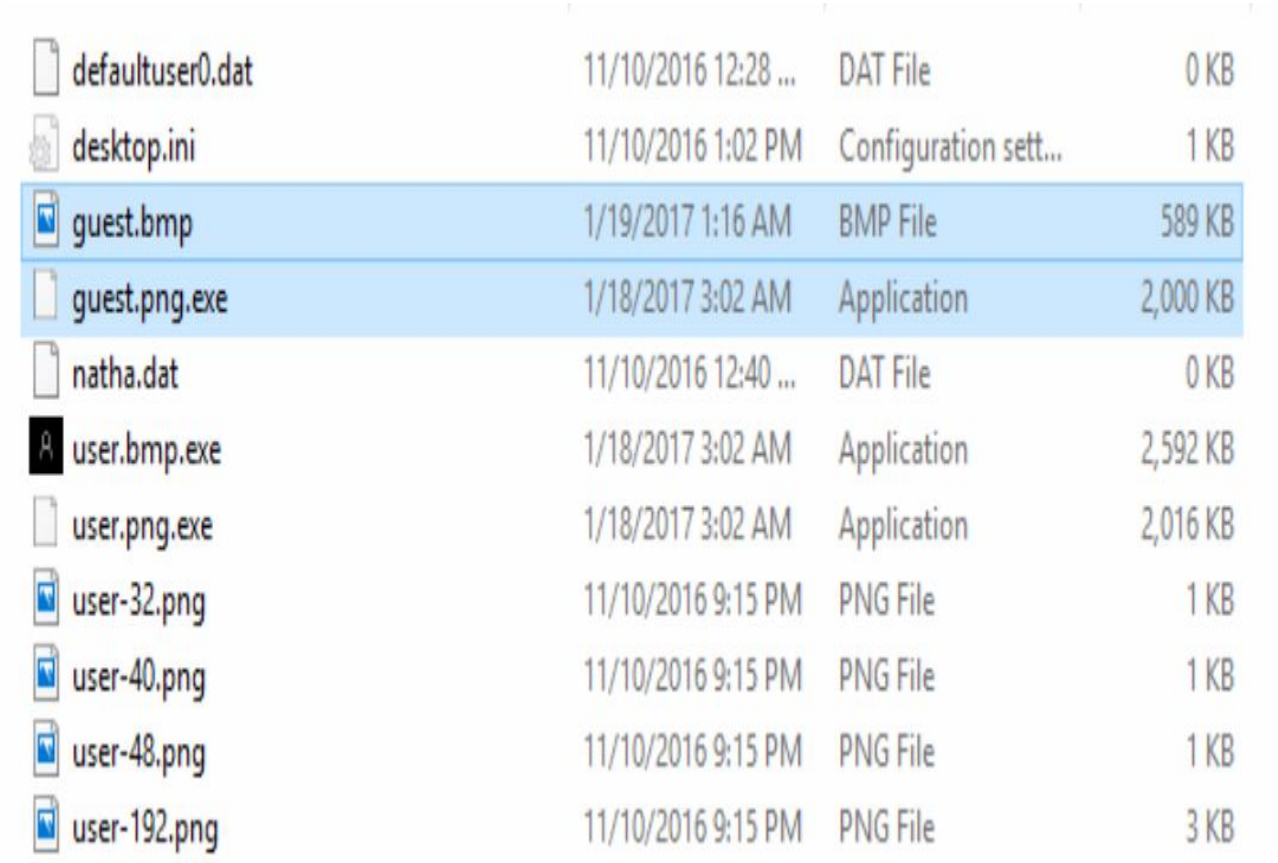
VirLock has screens that look like the above. They seem to always impersonate some type of legal authority. This one claims to be the Office of Criminal Investigation, where past versions called themselves “Operation Global 3” with different legal emblems.

The important part is the “Transfer ID:” text-box. We have found that any 64-length string will be accepted here as a real payment on this latest version of VirLocker. So, on your infected machine type the following into the Textbox:

0000000000000000000000000000000000000000000000000000000000000000

(That is 64 Zero’s.)

After you have done this, hit “Pay Fine”. This will cause the Ransom Lock Screen to disappear. VirLocker now thinks you have paid the ransom. Because of this, any of your infected files, upon double clicking them to open them, will no longer start the ransomware, but instead extract the original file inside of it.

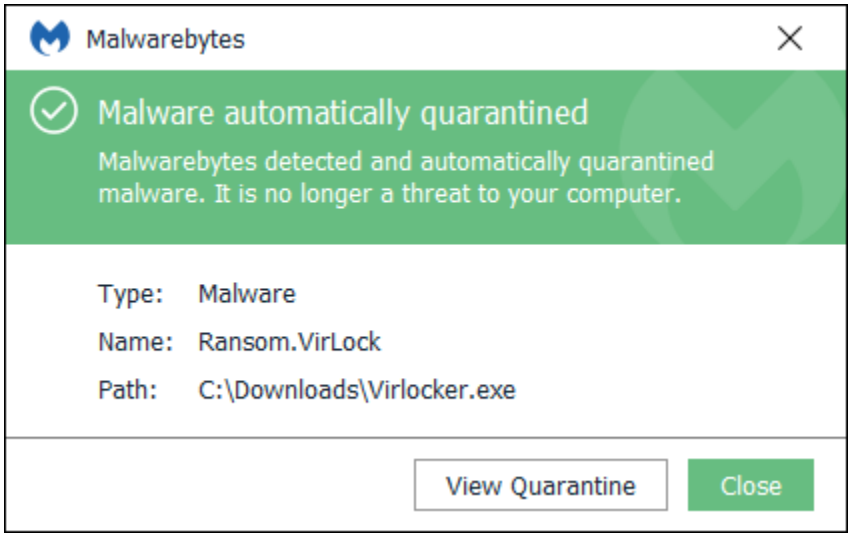


As you can see in the image above, clicking on the infected file “guest.bmp.exe” extracted the “guest.bmp” file, which is the original good version of the file. You may now use a non-important USB drive to back up all the files that are important and that you need recovered from this nasty infection.

ENSURE TO NEVER PUT ANY .EXE FILES ONTO YOUR BACKUP DRIVE WHEN DOING THIS, THIS CAN CAUSE THE INFECTION TO SPREAD. ONLY BACKUP THE EXTRACTED ORIGINAL FILES THE EXE'S SPIT OUT!

ONLY PERFORM THIS ACTION ON THE MACHINE YOU ENTERED THE "0'S" ON THE LOCKSCREEN. OPENING THE EXE FILES ON ANY OTHER MACHINE WILL INFECT THEM!

After you have obtained the files that are important to you, the machine should be completely wiped at this point. To avoid this type of infection in the future, consider using an anti-ransomware solution like Malwarebytes, which has anti-ransomware functionalities built into it!



Hashes used in this analysis:

d438f51fbb56c06c8d910344ceed79504360162c78559254afa7b3fa27eaf763

bfa26552ae53c77a4ff49177e1b27dc318ee4102ca7281aa7dd3afdeccbe58ff

932d7b340cb58cb635b2088421dc73bc1fe079c4b5cee940b2ad8e4dcbfe0f04

a9937f7b85a12f5bc2eda8240c9fa5972275b50bc851aa736402b5f166ef3b03

4d0c238a2cd530b6c9a724af5406dc50cf31988584d34cacf46ac9b2c5f63bcc

ff56e378a221100b160fae0d5cd4f94cb34c14b4e9b932c159c3c95c00526a35

505d86f5181bdd13e473bfa4ab5edbc4d9a6b4ba75f30404ea4966ff7a8ee8da

48abe6cdf1a3f3bc0934abbfaef189938e7ee981f77340cf2ca8b57fdad21a7e

6372a2d90dec71b21fa5991b34289dfd2e8777bca9f51e5991dce03c4e861cd6

https://blog.malwarebytes.com/threat-analysis/2017/01/virlockers-comeback-including-recovery-

instructions/