Mount Locker ransomware now targets your TurboTax tax returns

bleepingcomputer.com/news/security/mount-locker-ransomware-now-targets-your-turbotax-tax-returns/

Lawrence Abrams

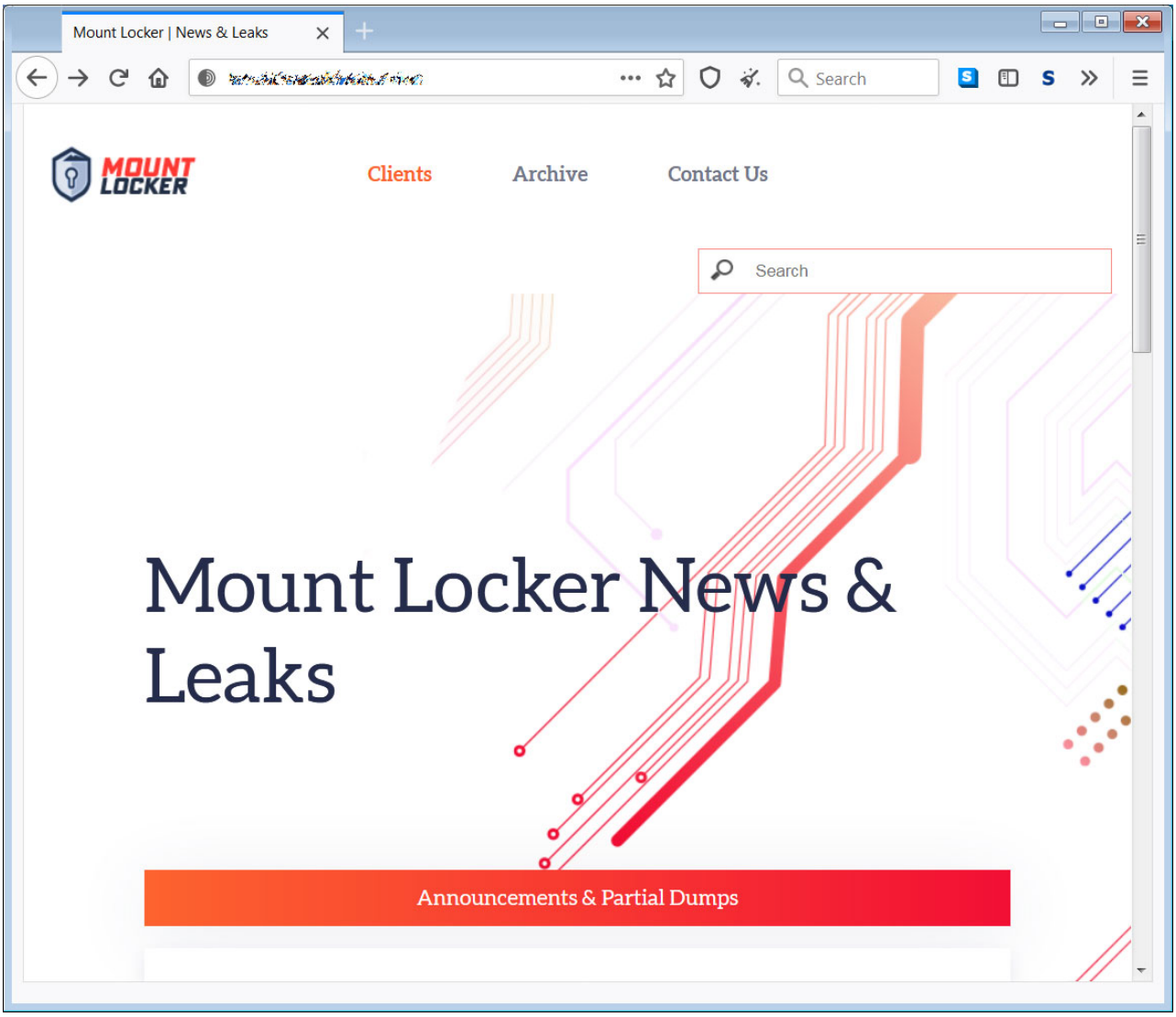
By
Lawrence Abrams

- November 19, 2020
- 04:09 PM
- 0

The Mount Locker ransomware operation is gearing up for the tax season by specifically targeting TurboTax returns for encryption.

Mount Locker is a relatively new ransomware operation that began infecting victims in July 2020. Like other human-operated ransomware gangs, the Mount Locker gang will compromise networks, harvest unencrypted files to be used for blackmail, and then encrypt the devices on the network.

Stolen data and the encrypted files are then used in a double-extortion scheme where victims are warned that their stolen files will be published on a data leak site if a ransom is not paid.



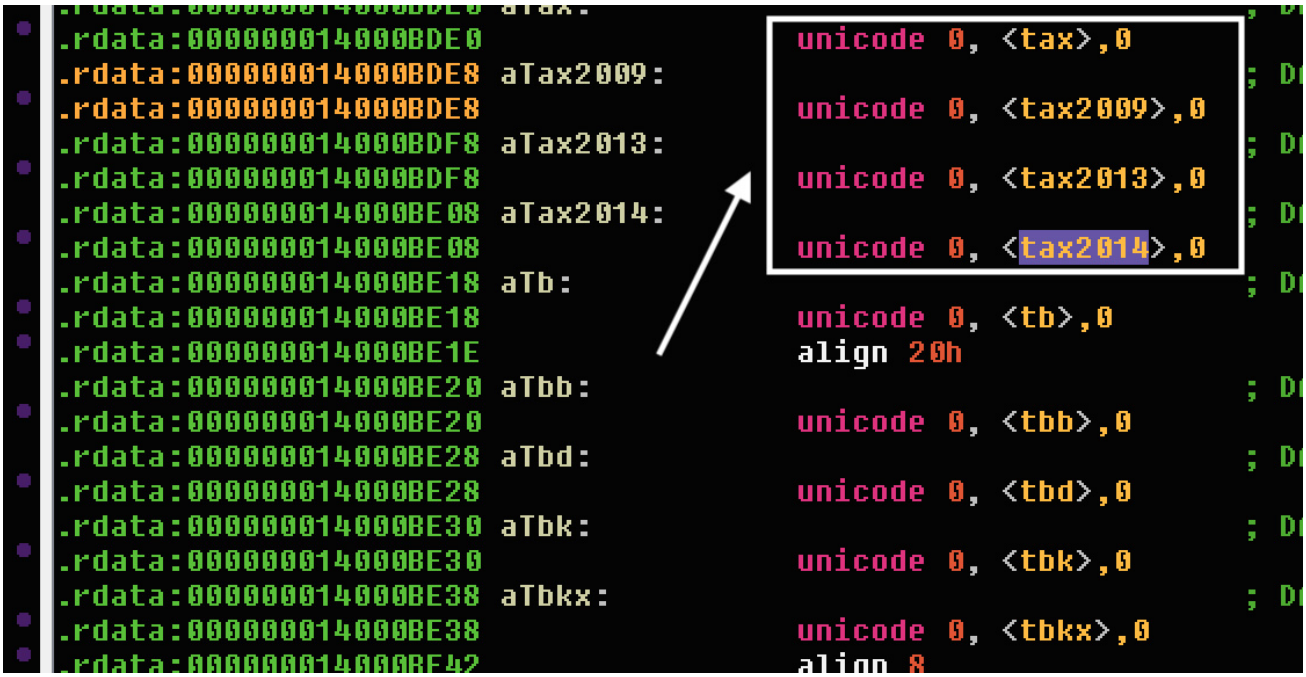
Mount Locker data leak site

New Mount Locker version targets TurboTax

With the tax season fast approaching, some are already gathering their tax information and inputting it into TurboTax to prepare for the April 15th tax deadline.

In a new version of the ransomware analyzed by Advanced Intel's Vitali Kremez, Mount Locker is getting ready for the tax season as well by specifically targeting files used by the TurboTax tax software.

When encrypting a computer, Mount Locker only encrypts files that have certain file extensions. With the latest version, the ransomware developers are now targeting the **.tax**, **.tax2009**, **.tax2013**, and **.tax2014** file extensions associated with the TurboTax tax preparation software.



Malware Locker targeting TurboTax extensions

While Mount Locker is oddly targeting file extensions for specific tax years, Kremez told BleepingComputer that the 'tax' targeting would match all extensions that contain the string.

To be safe from Mount Locker and other ransomware, be sure to make backups of your TurboTax files and other essential documents on detachable media after you make any changes.

Simply backing up your important files to a USB drive every night and then unplugging it will guarantee the safety of your files even if you suffer a ransomware attack.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

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

- Mount Locker
- Ransomware
- Tax Return
- Taxes
- TurboTax

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

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: