New RegretLocker ransomware targets Windows virtual machines

bleepingcomputer.com/news/security/new-regretlocker-ransomware-targets-windows-virtual-machines/

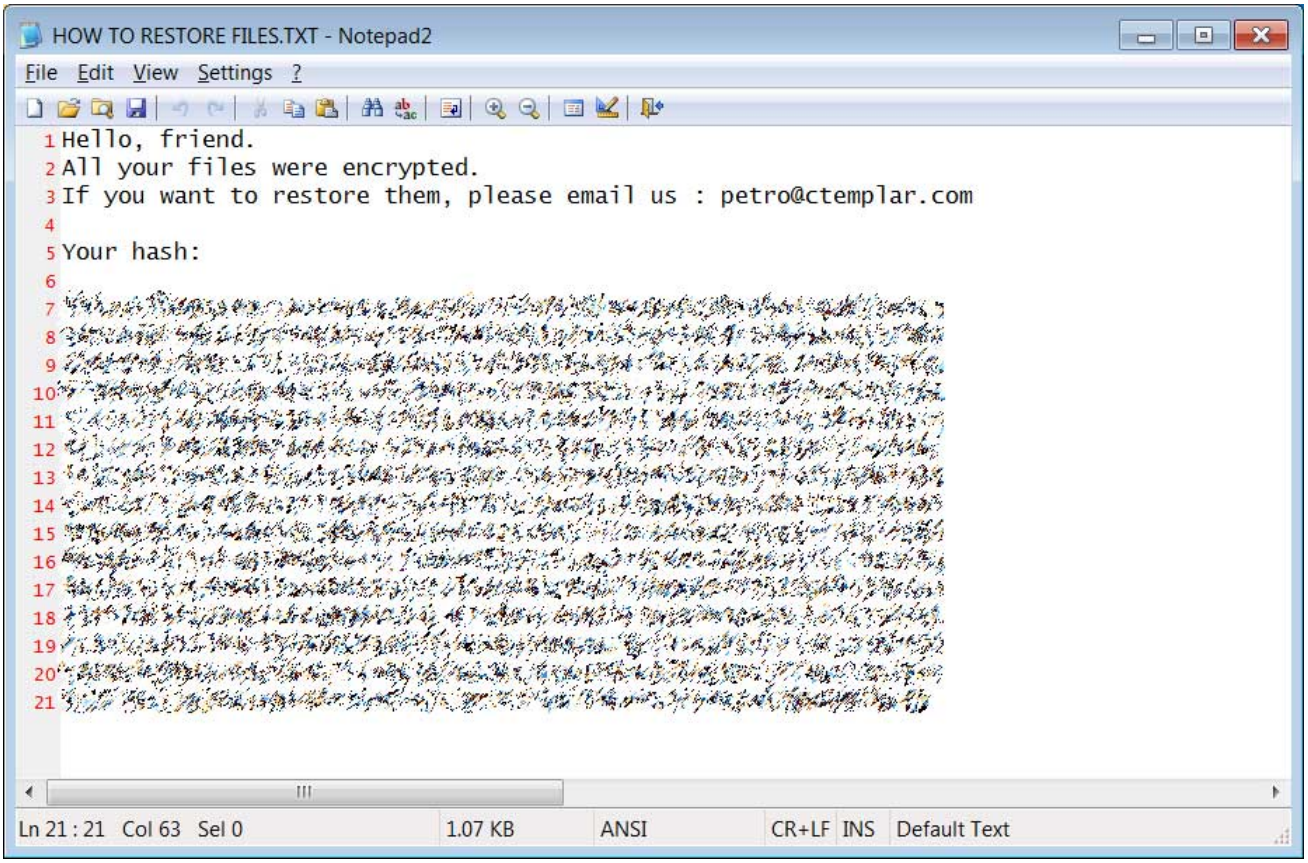
Lawrence Abrams

By
Lawrence Abrams

- November 3, 2020
- 05:31 PM
- 0

A new ransomware called RegretLocker uses a variety of advanced features that allows it to encrypt virtual hard drives and close open files for encryption.

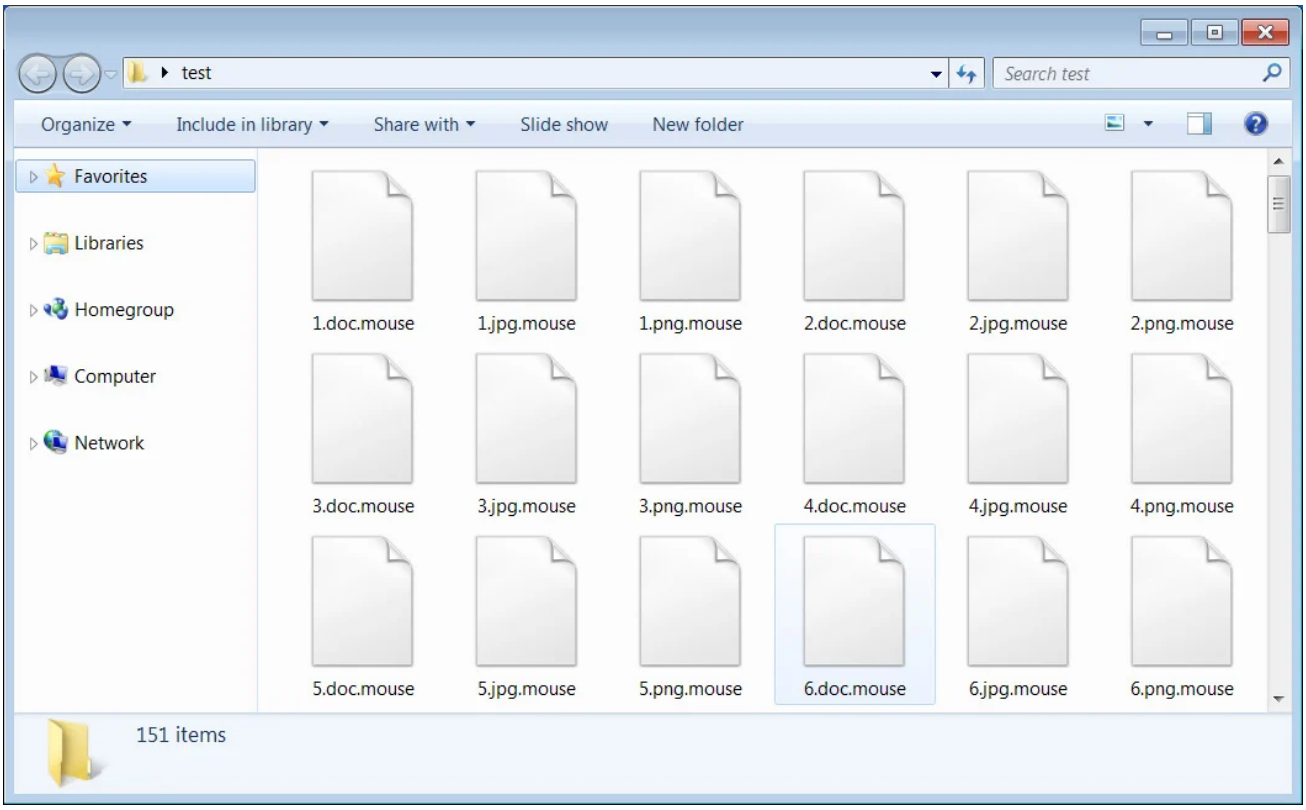
RegretLocker was discovered in October and is a simple ransomware in terms of appearance as it does not contain a long-winded ransom note and uses email for communication rather than a Tor payment site.



RegretLocker ransom note

Source: BleepingComputer

When encrypting files, it will append the innocuous-sounding **.mouse** extension to encrypted file names.



RegretLocker encrypted files

Source: BleepingComputer

What it lacks in appearance, though, it makes up for in advanced features that we do not usually see in ransomware infections, as described below.

RegretLocker mounts virtual hard disks

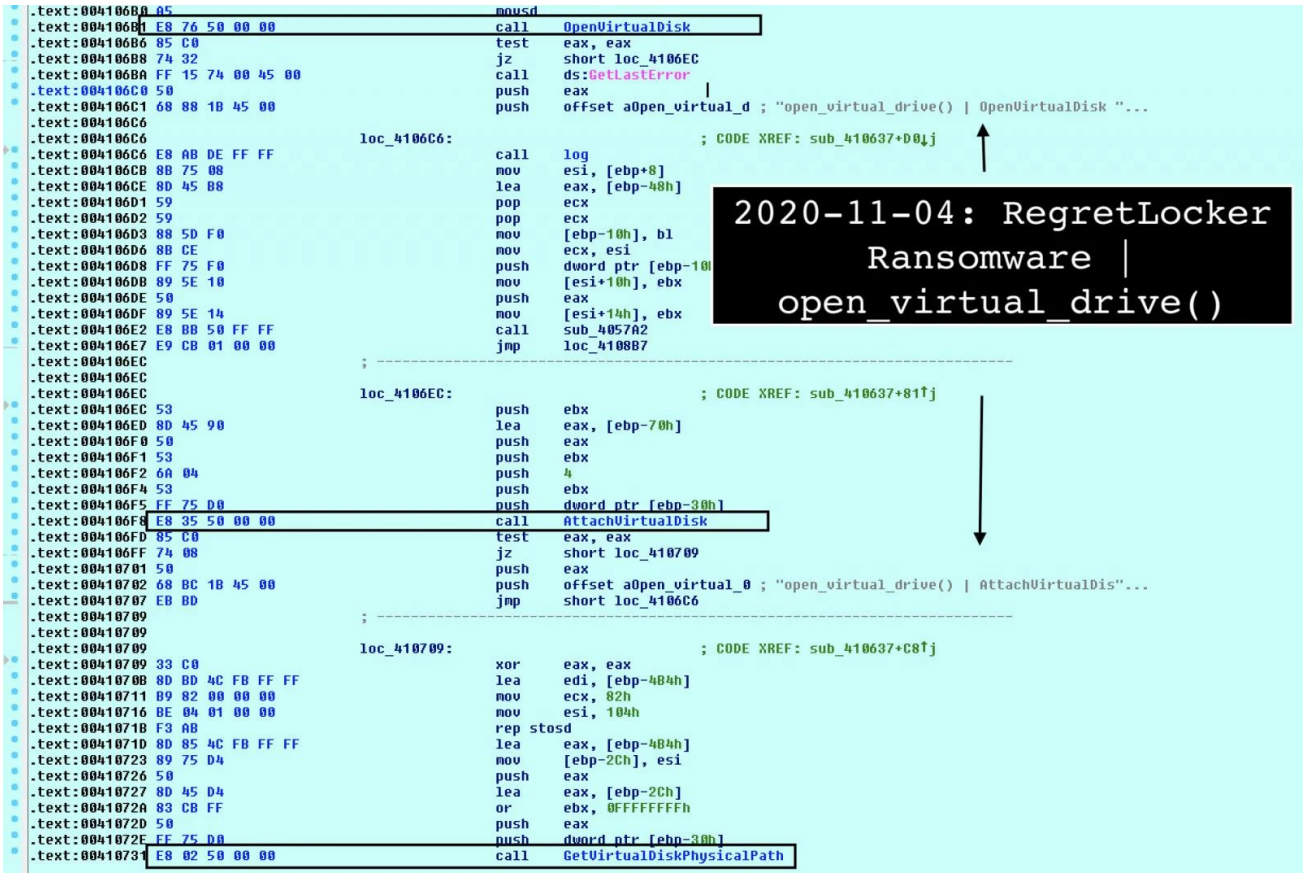
When creating a Windows Hyper-V virtual machine, a virtual hard disk is created and stored in a VHD or VHDX file.

These virtual hard disk files contain a raw disk image, including a drive's partition table and partitions, and like regular disk drives, can range in size from a few gigabytes to terabytes.

When a ransomware encrypts files on a computer, it is not efficient to encrypt a large file as it slows down the entire encryption process's speed.

In a sample of the ransomware discovered by MalwareHunterTeam and analyzed by Advanced Intel's Vitali Kremez, RegretLocker uses an interesting technique of mounting a virtual disk file so each of its files can be encrypted individually.

To do this, RegretLocker uses the Windows Virtual Storage API OpenVirtualDisk, AttachVirtualDisk, and GetVirtualDiskPhysicalPath functions to mount virtual disks.



Mounting a VHD file

As shown by a debug message in the ransomware, it is specifically searching for VHD and mounting them when detected.

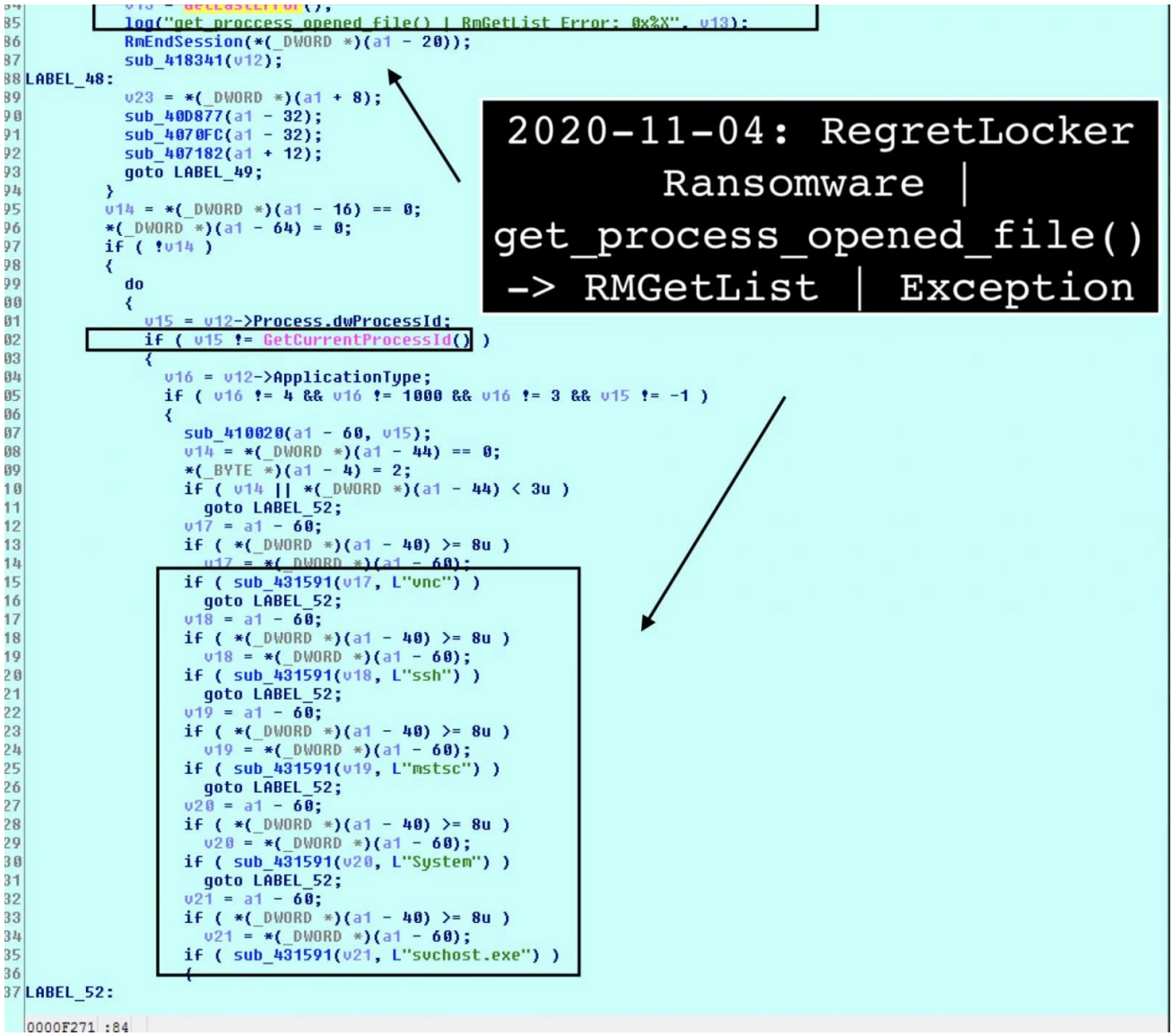
```
parse_files() | Found virtual drive: %ws in path: %s
```

Once the virtual drive is mounted as a physical disk in Windows, the ransomware can encrypt each one individually, which increases the speed of encryption.

The code used by RegretLocker to mount a VHD is believed to have been taken from a recently published research by security researcher smelly__vx.

In addition to using the Virtual Storage API, RegretLocker also utilizes the Windows Restart Manager API to terminate processes or Windows services that keep a file open during encryption.

When using this API, Kremez told BleepingComputer if the name of a process contains 'vnc', 'ssh', 'mstsc', 'System', or 'svchost.exe', the ransomware will not terminate it. This exception list is likely used to prevent the termination of critical programs or those used by the threat actor to access the compromised system.



Windows Restart Manager exception list

The Windows Restart Manager feature is only used by a few ransomware such as REvil (Sodinokibi), Ryuk, Conti, ThunderX/Ako, Medusa Locker, SamSam, and LockerGoga.

RegretLocker is not very active at this point, but it is a new family that we need to keep an eye on.

Related Articles:

Microsoft shares mitigation for Windows KrbRelayUp LPE attacks

Microsoft adds support for WSL2 distros on Windows Server 2022

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Microsoft adds Office subscriptions to Windows 11 account settings

CISA adds 41 vulnerabilities to list of bugs used in cyberattacks

- Hyper-V
- RegretLocker
- VHD
- Virtual Disk
- Virtual Drive
- Virtual Machine
- Virtualization
- Windows

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

You may also like: