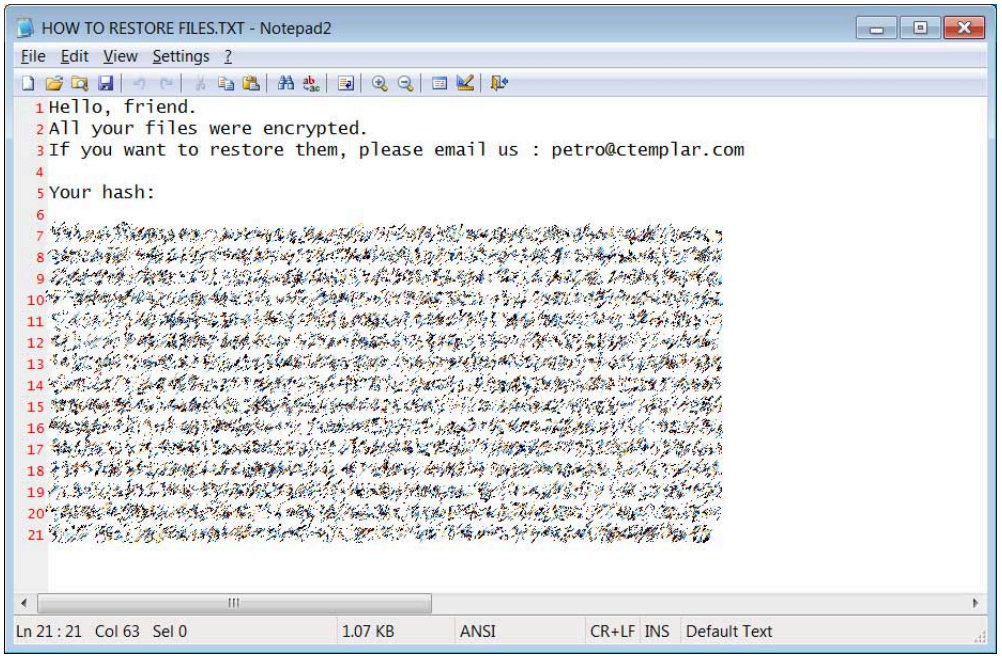
New RegretLocker ransomware targets Windows virtual machines

By Lawrence Abrams

Published: 2020-11-03 · Archived: 2026-04-05 20:06:14 UTC

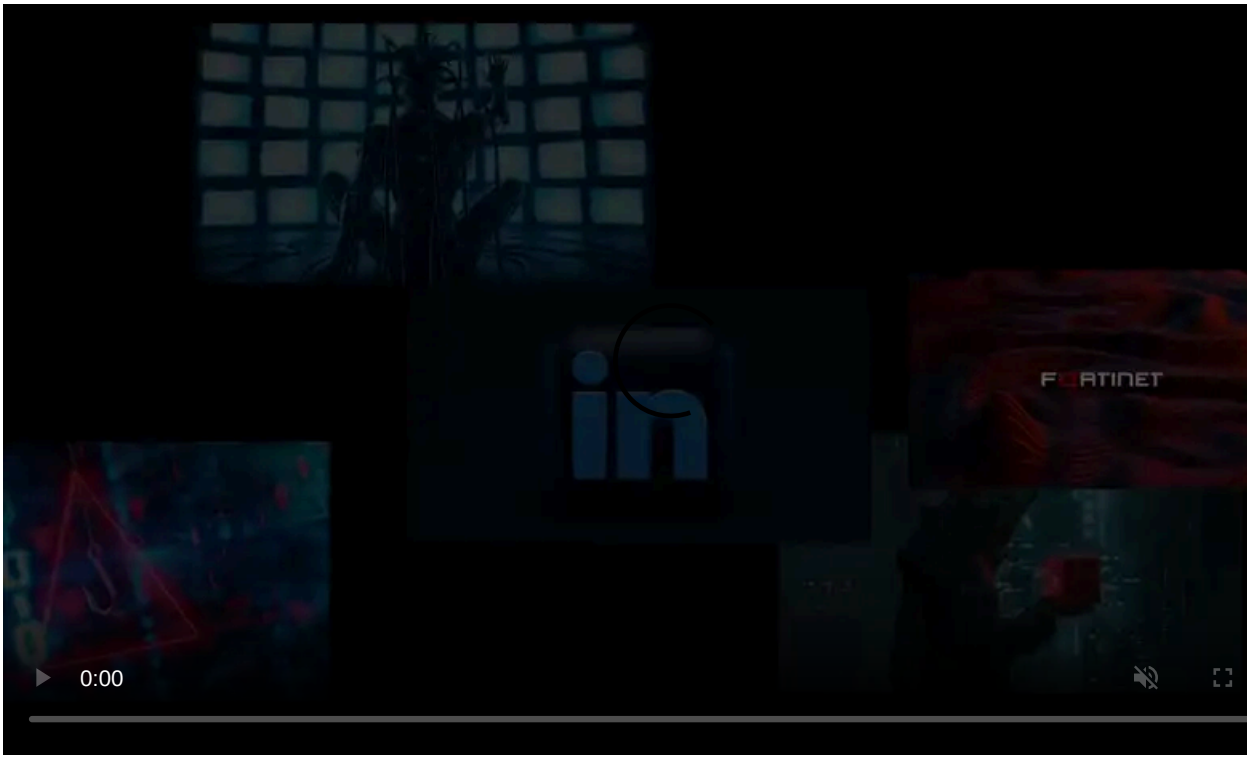
A new ransomware called RegretLocker uses a variety of advanced features that allows it to encrypt virtual hard drives and close open files for encryption.

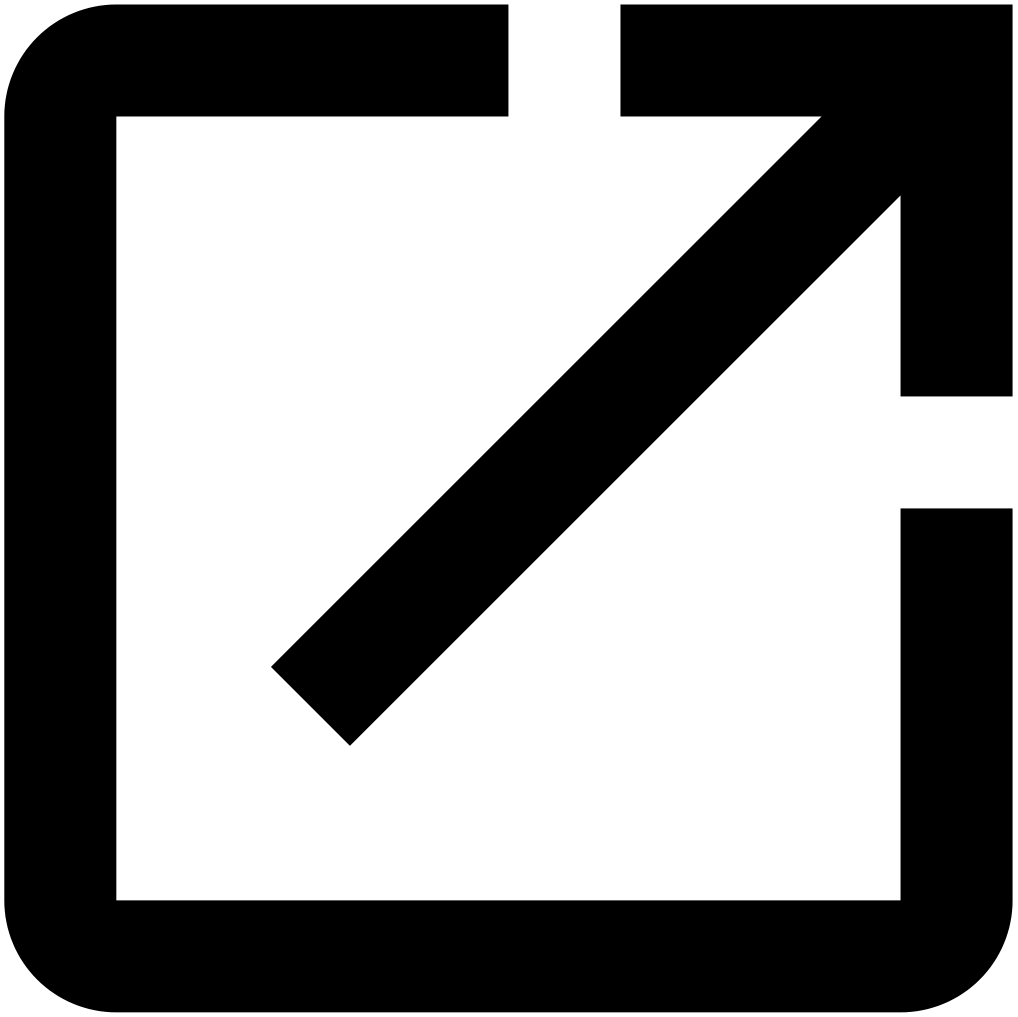
RegretLocker was discovered in October and is a simple ransomware in terms of appearance as it does not contain a long-winded ransom note and uses email for communication rather than a Tor payment site.

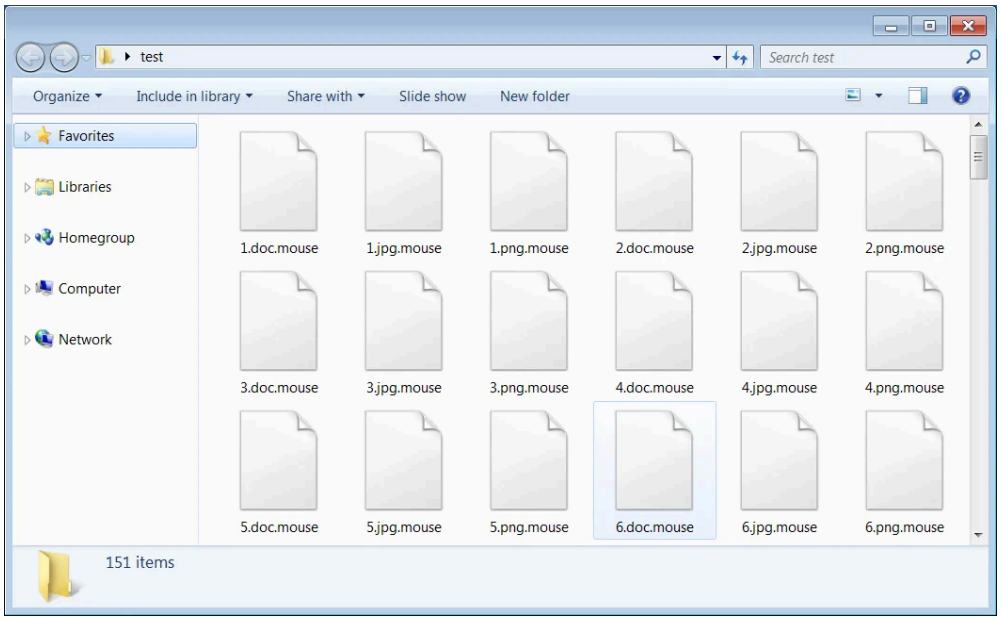


RegretLocker ransom note
Source: BleepingComputer

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


0:00





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

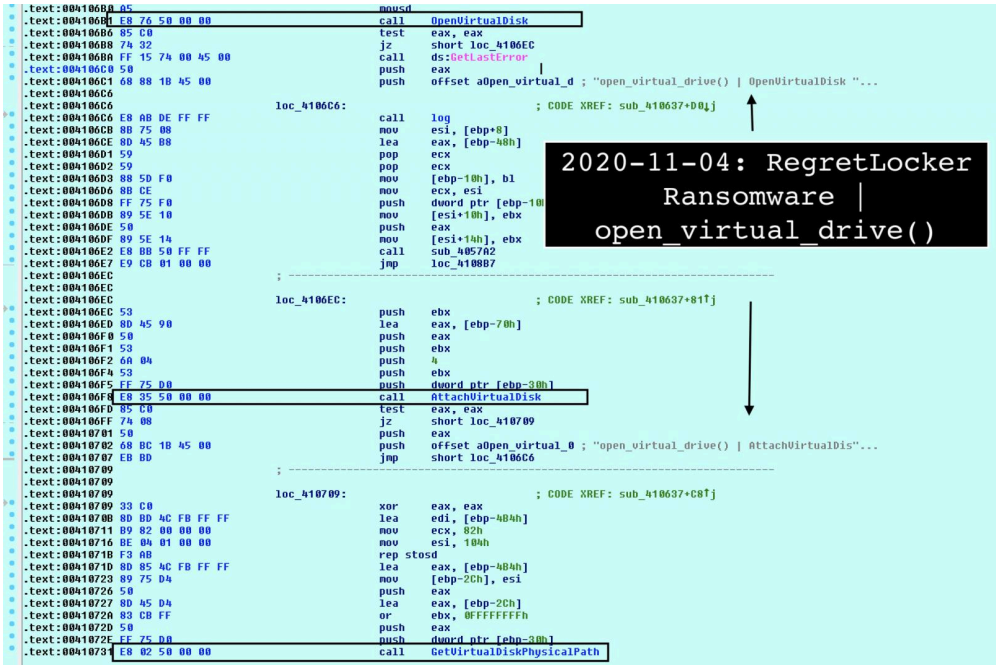
When creating a Windows Hyper-V virtual machine, a virtual hard disk is created and stored in a VHD or VHDX file.

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.

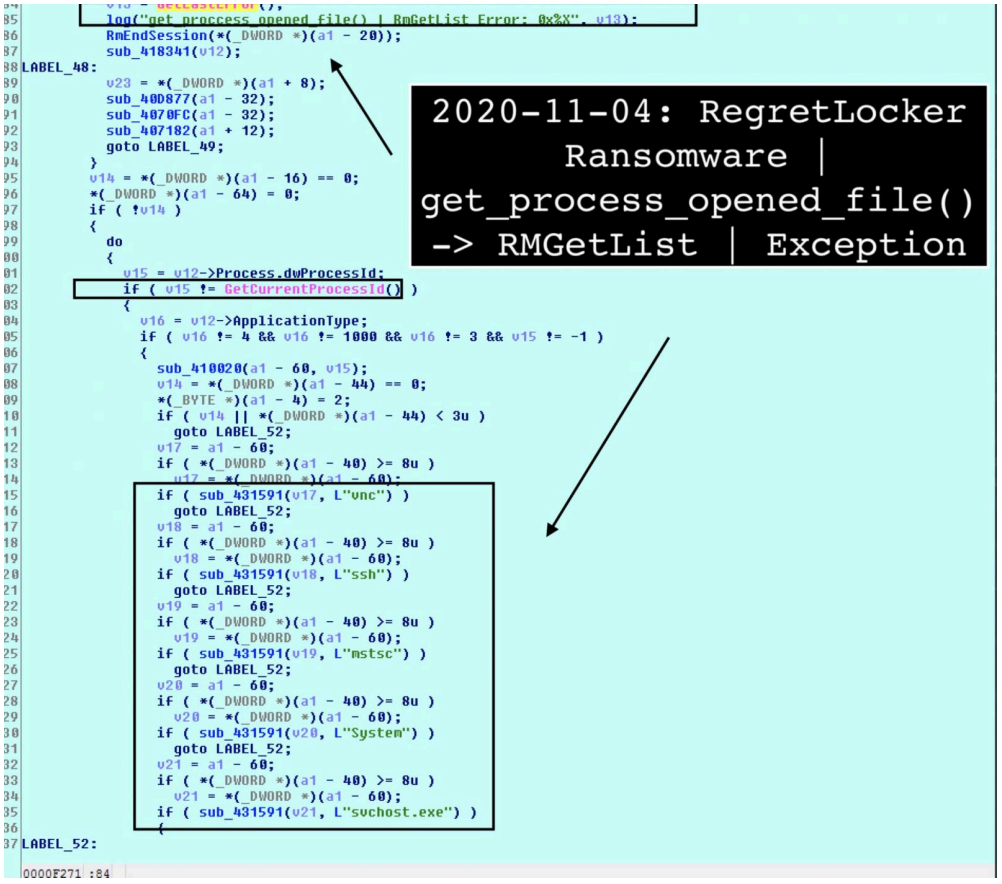
```
parse_files() | Found virtual drive: %ws in path: %s
```

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.

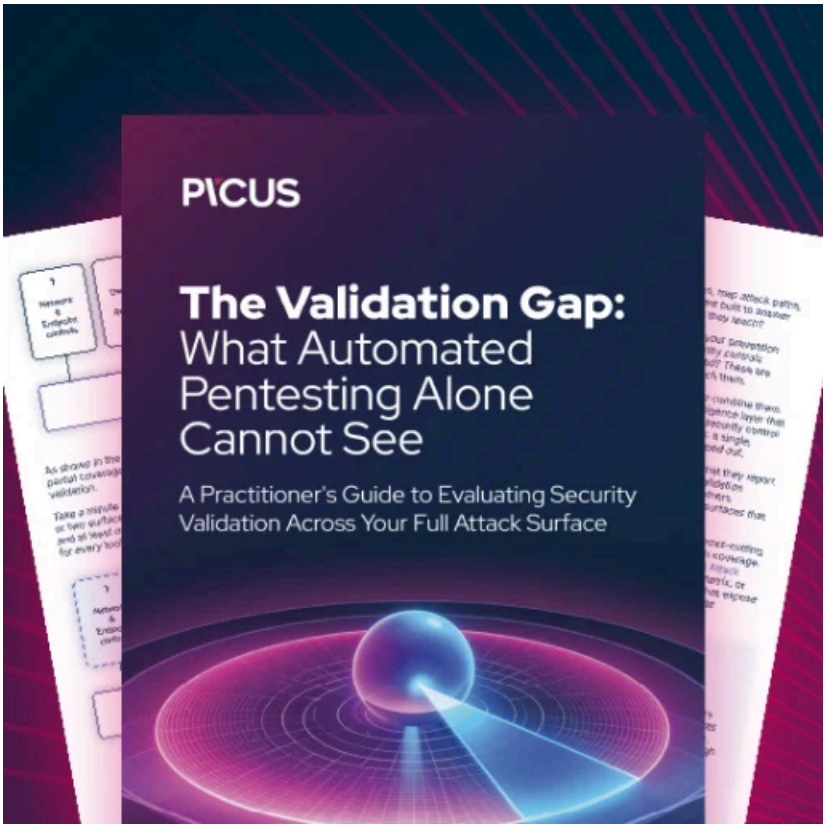
When using this API, Kremez told BleepingComputer if the name of a process contains 'vnc', 'ssh', 'mstsc', 'System', or 'svchost.exe', the ransomware will not terminate it. This exception list is likely used to prevent the termination of critical programs or those used by the threat actor to access the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



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/new-regretlocker-ransomware-targets-windows-virtual-machines/