

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.

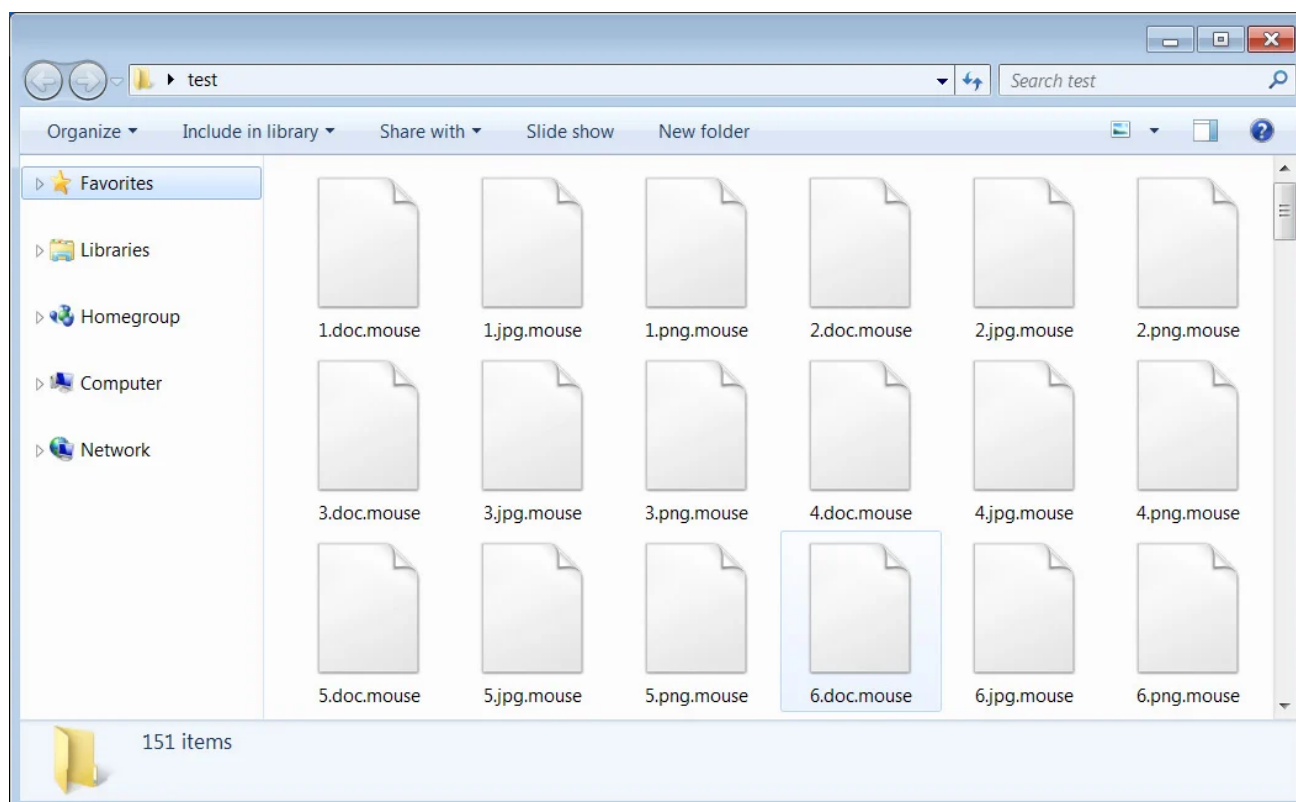
RegretLocker was discovered in October and is a simple ransomware in terms of appearance as it does not contain a long-winded ransom note and uses email for communication rather than a Tor payment site.

```
HOW TO RESTORE FILES.TXT - Notepad2
File Edit View Settings ?
1 Hello, friend.
2 All your files were encrypted.
3 If you want to restore them, please email us : petro@ctemplar.com
4
5 Your hash:
6
7 [Redacted]
8 [Redacted]
9 [Redacted]
10 [Redacted]
11 [Redacted]
12 [Redacted]
13 [Redacted]
14 [Redacted]
15 [Redacted]
16 [Redacted]
17 [Redacted]
18 [Redacted]
19 [Redacted]
20 [Redacted]
21 [Redacted]
Ln 21 : 21 Col 63 Sel 0 1.07 KB ANSI CR+LF INS Default Text
```

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.

```

.text:00410680 05          movsd
.text:00410681 E8 76 50 00 00    call    OpenVirtualDisk
.text:00410686 85 C0          test   eax, eax
.text:00410688 74 32          jz     short loc_4106EC
.text:0041068A FF 15 74 00 45 00    call    ds:GetLastError
.text:004106C0 50          push   eax
.text:004106C1 68 88 1B 45 00    push   offset aOpen_virtual_d ; "open_virtual_drive() | OpenVirtualDisk ..."
.text:004106C6          loc_4106C6:          ; CODE XREF: sub_410637+D0↓j
.text:004106C6 E8 AB DE FF FF    call    log
.text:004106CB 88 75 08       mov    esi, [ebp+8]
.text:004106CE 8D 45 08       lea   eax, [ebp-48h]
.text:004106D1 59          pop    ecx
.text:004106D2 59          pop    ecx
.text:004106D3 88 5D F0       mov    [ebp-10h], bl
.text:004106D6 8B CE       mov    ecx, esi
.text:004106D8 FF 75 F0       push  dword ptr [ebp-10h]
.text:004106DB 89 5E 10       push  [esi+10h], ebx
.text:004106DE 50          push  eax
.text:004106DF 89 5E 14       mov    [esi+14h], ebx
.text:004106E2 E8 BB 50 FF FF    call    sub_4057A2
.text:004106E7 E9 CB 01 00 00    jmp    loc_4108B7
;
.text:004106EC          loc_4106EC:          ; CODE XREF: sub_410637+81↑j
.text:004106EC 53          push   ebx
.text:004106ED 8D 45 90       lea   eax, [ebp-70h]
.text:004106F0 50          push   eax
.text:004106F1 53          push   ebx
.text:004106F2 6A 04         push   4
.text:004106F4 53          push   ebx
.text:004106F5 FF 75 D0       push  dword ptr [ebp-30h]
.text:004106F8 E8 35 50 00 00    call    AttachVirtualDisk
.text:004106FD 85 C0          test   eax, eax
.text:004106FF 74 08          jz     short loc_410709
.text:00410701 50          push   eax
.text:00410702 68 BC 1B 45 00    push   offset aOpen_virtual_0 ; "open_virtual_drive() | AttachVirtualDis..."
.text:00410707 EB BD          jmp    short loc_4106C6
;
.text:00410709          loc_410709:          ; CODE XREF: sub_410637+C8↑j
.text:00410709 33 C0          xor    eax, eax
.text:0041070B 8D BD 4C FB FF FF    lea   edi, [ebp-4B4h]
.text:00410711 B9 82 00 00 00    mov    ecx, 82h
.text:00410716 BE 04 01 00 00    mov    esi, 104h
.text:0041071B F3 AB          rep stosd
.text:0041071D 8D 85 4C FB FF FF    lea   eax, [ebp-4B4h]
.text:00410723 89 75 D4       mov    [ebp-2Ch], esi
.text:00410726 50          push   eax
.text:00410727 8D 45 D4       lea   eax, [ebp-2Ch]
.text:0041072A 83 CB FF       or     ebx, 0FFFFFFFh
.text:0041072D 50          push   eax
.text:0041072E FF 75 D0       push  dword ptr [ebp-30h]
.text:00410731 E8 02 50 00 00    call    GetVirtualDiskPhysicalPath

```

2020-11-04: RegretLocker Ransomware | open_virtual_drive()

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.

```

95 v13 = GetProcAddress(
96 log("get_process_opened_file() | RmGetList Error: 0x%X", v13);
97 RmEndSession(*(DWORD *)(a1 - 20));
98 sub_418341(v12);
99 LABEL_48:
100 v23 = *(DWORD *)(a1 + 8);
101 sub_40D877(a1 - 32);
102 sub_4070FC(a1 - 32);
103 sub_407182(a1 + 12);
104 goto LABEL_49;
105 }
106 v14 = *(DWORD *)(a1 - 16) == 0;
107 *(DWORD *)(a1 - 64) = 0;
108 if ( !v14 )
109 {
110 do
111 {
112 v15 = v12->Process.dwProcessId;
113 if ( v15 != GetCurrentProcessId() )
114 {
115 v16 = v12->ApplicationType;
116 if ( v16 != 4 && v16 != 1000 && v16 != 3 && v15 != -1 )
117 {
118 sub_410020(a1 - 60, v15);
119 v14 = *(DWORD *)(a1 - 44) == 0;
120 *(BYTE *)(a1 - 4) = 2;
121 if ( v14 || *(DWORD *)(a1 - 44) < 3u )
122 goto LABEL_52;
123 v17 = a1 - 60;
124 if ( *(DWORD *)(a1 - 40) >= 8u )
125 v17 = *(DWORD *)(a1 - 60);
126 if ( sub_431591(v17, L"vnc" ) )
127 goto LABEL_52;
128 v18 = a1 - 60;
129 if ( *(DWORD *)(a1 - 40) >= 8u )
130 v18 = *(DWORD *)(a1 - 60);
131 if ( sub_431591(v18, L"ssh" ) )
132 goto LABEL_52;
133 v19 = a1 - 60;
134 if ( *(DWORD *)(a1 - 40) >= 8u )
135 v19 = *(DWORD *)(a1 - 60);
136 if ( sub_431591(v19, L"mstsc" ) )
137 goto LABEL_52;
138 v20 = a1 - 60;
139 if ( *(DWORD *)(a1 - 40) >= 8u )
140 v20 = *(DWORD *)(a1 - 60);
141 if ( sub_431591(v20, L"System" ) )
142 goto LABEL_52;
143 v21 = a1 - 60;
144 if ( *(DWORD *)(a1 - 40) >= 8u )
145 v21 = *(DWORD *)(a1 - 60);
146 if ( sub_431591(v21, L"svchost.exe" ) )
147 {
148 }
149 }
150 }
151 LABEL_52:
152 0000F271 :84

```

2020-11-04: RegretLocker Ransomware | get_process_opened_file() -> RMGetList | Exception

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](#)

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:
