Problem 1.3.1

A Dangerous Situation

Initial Reported Issue

You were in your high school cafeteria one morning, planning to meet your friends. You decide to go get something to drink and leave your laptop out on the table. You figure you'll only be away for a minute to two—What's the worst that could happen? You get your drink, come back to the table, and see that your friends arrived while you were away. After chatting with them for a bit, you close your laptop and head off to your classes for the day.

The next time you open your laptop, you notice a suspicious file on your Desktop that you've never seen before. You start to think about all of the information available and at risk on your computer and you begin to worry about how that file might have gotten on your computer.

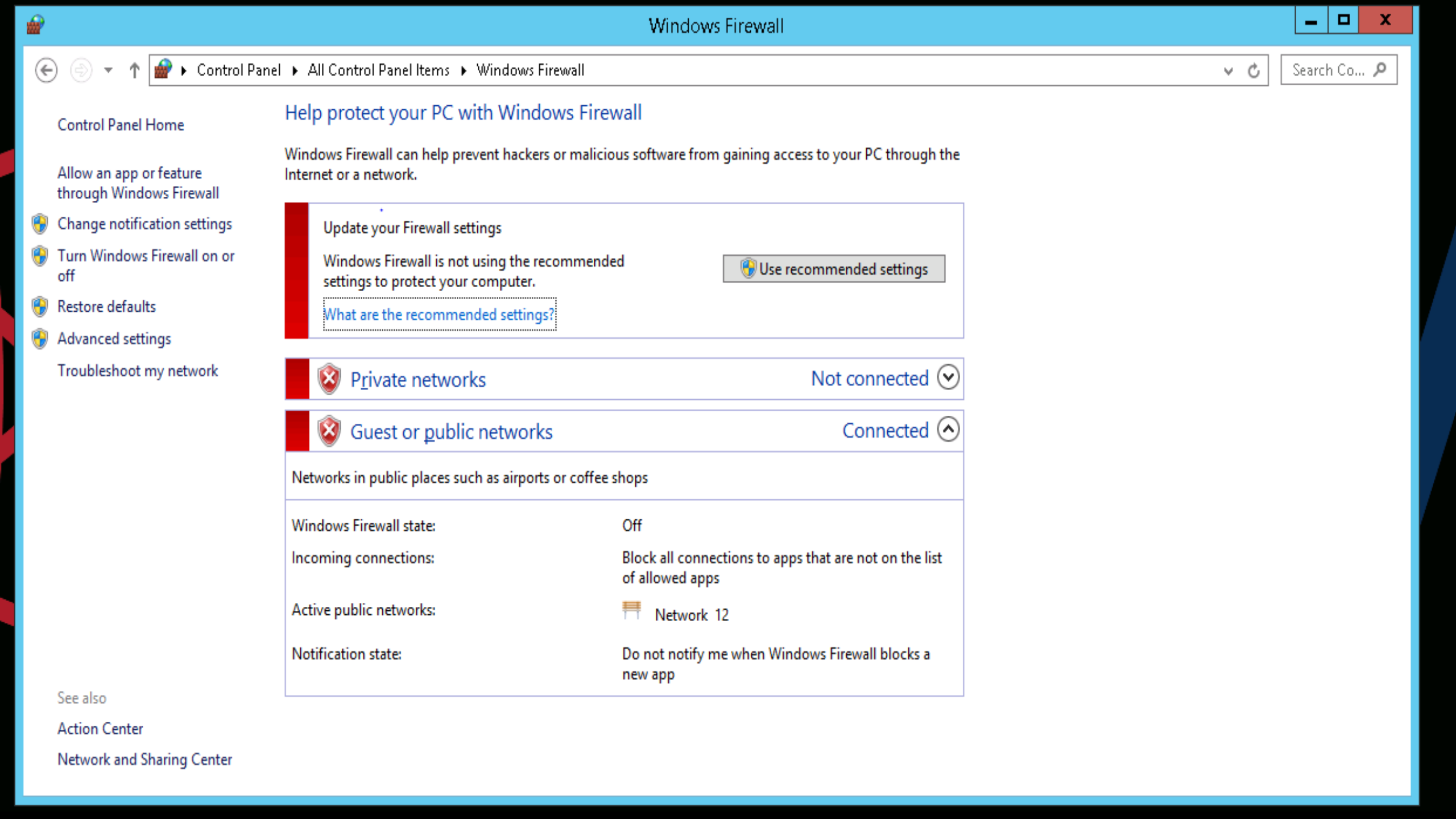
But how can you figure out what might have been touched? How can you fix anything that has been altered? And most importantly, how can you keep this from happening again?

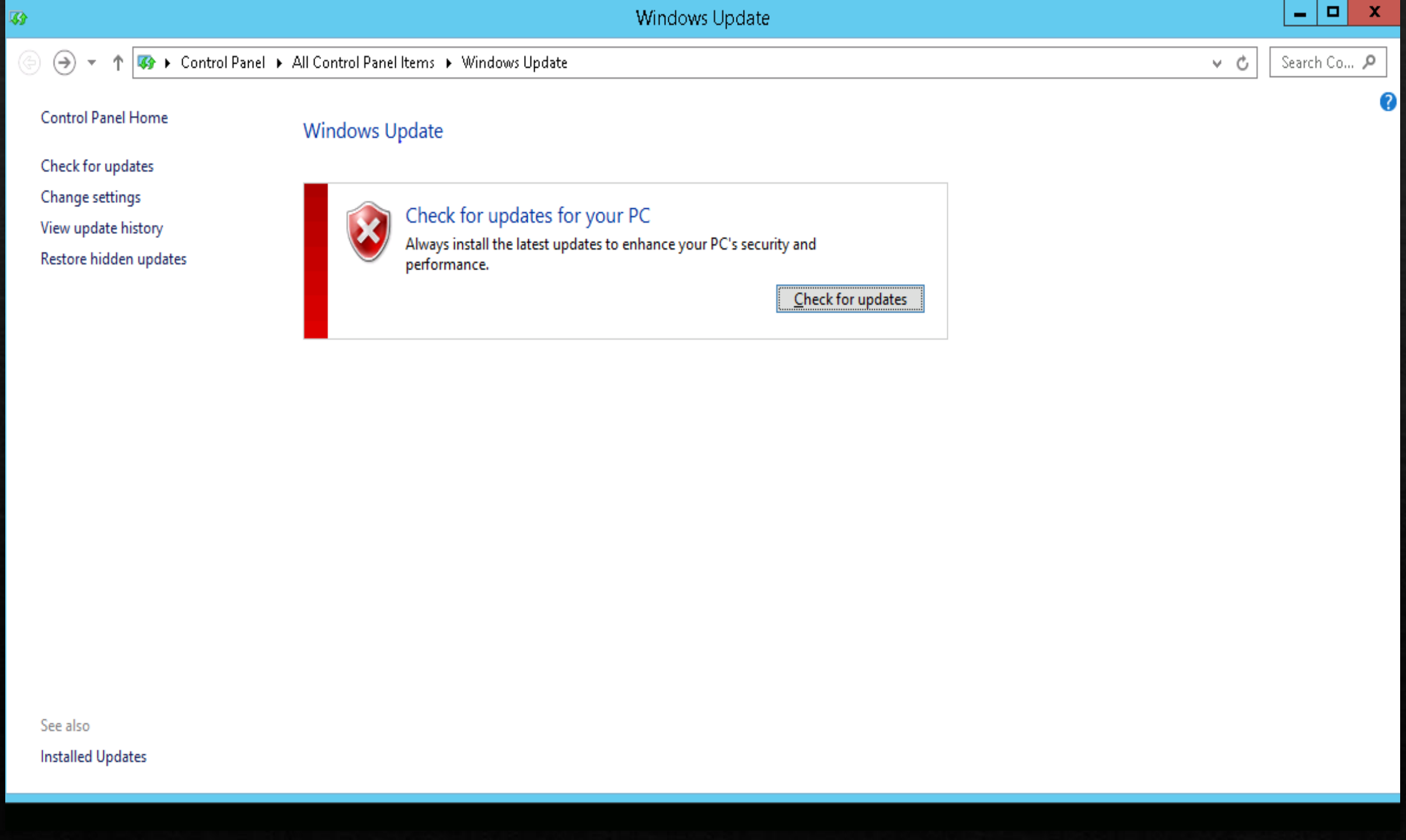
Problems Detected

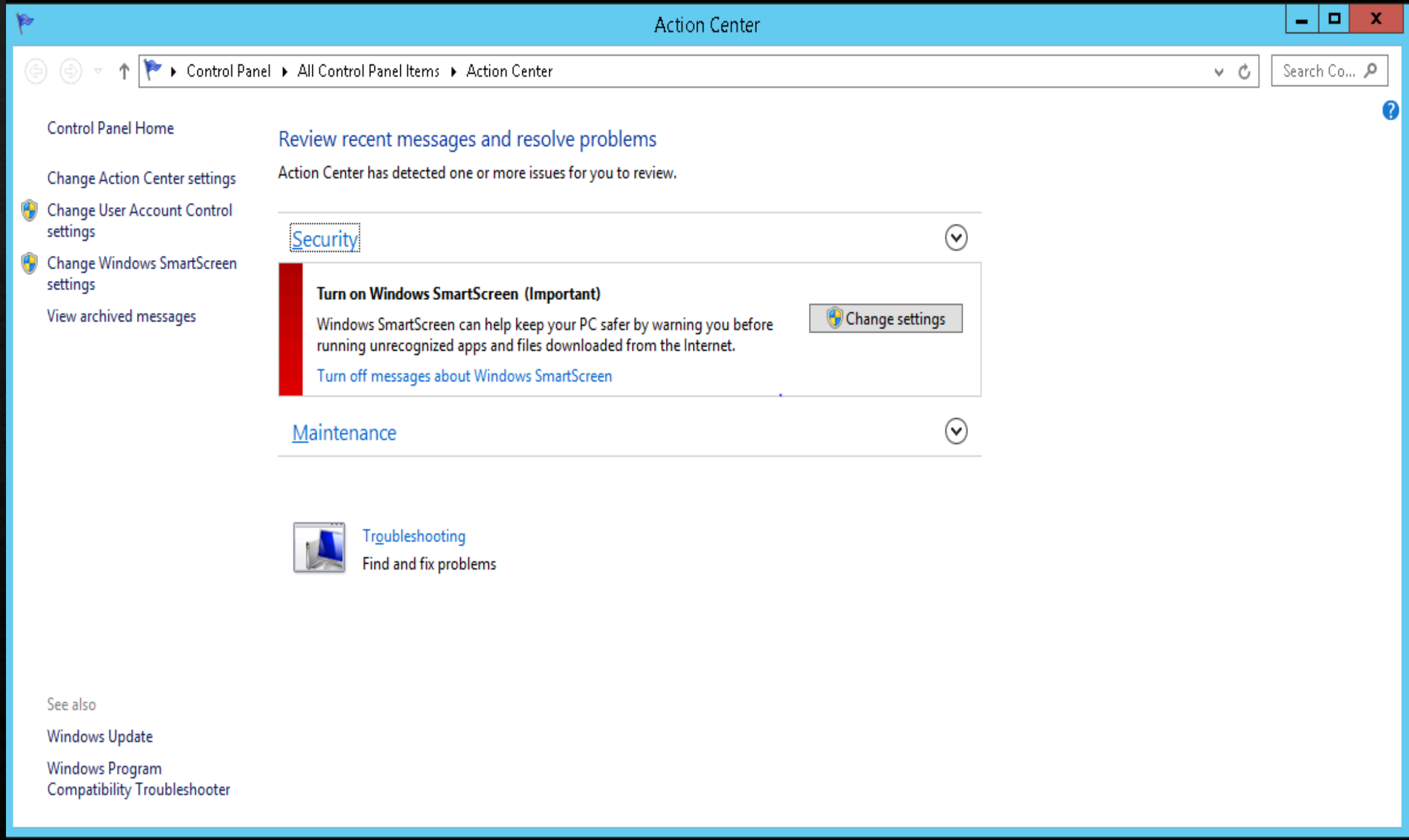
Some of the problems we detected were unrecognized files on the system (Python, .bat, .exe), Hidden bat and exe files, missing files in the recycle bin and Windows Firewall was turned off. These files have strange names and them being hidden adds even more suspicion to them. Windows updates were disabled allowing for very dangerous security issues, and Windows SmartScreen was turned off allowing malware programs to run. One of these programs were found in settings trying to guess user passwords. Lastly files were set to share with everyone on the network allowing anyone to access and modify the users documents and data.

MAJOR ISSUES:

- Windows Firewall Turned OFF
- Windows SmartScreen Turned OFF
- Windows set to NEVER update
- MALICOUS file trying to guess passwords every minute in event viewer
- Files were deleted and needed to be restored


Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Co...
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Network 12
Notification state:
Do not notify me when Windows Firewall blocks a new app
See also
Action Center
Network and Sharing Center


Windows Update
Control Panel ▸ All Control Panel Items ▸ Windows Update
Search Co...
Control Panel Home
Check for updates
Change settings
View update history
Restore hidden updates
Windows Update
Check for updates for your PC
Always install the latest updates to enhance your PC's security and performance.
Check for updates
See also
Installed Updates


Action Center
Control Panel ▸ All Control Panel Items ▸ Action Center
Search Co...
Control Panel Home
Change Action Center settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
Review recent messages and resolve problems
Action Center has detected one or more issues for you to review.
Security
Turn on Windows SmartScreen (Important)
Windows SmartScreen can help keep your PC safer by warning you before running unrecognized apps and files downloaded from the Internet.
Change settings
Turn off messages about Windows SmartScreen
Maintenance
Troubleshooting
Find and fix problems
See also
Windows Update
Windows Program Compatibility Troubleshooter

Response Methods

What we did to combat these issues:

- Set Windows to update always and automatically for improved security
- Permanently Deleted the suspicious files found on the system
- Turned on Windows SmartScreen to protect from malware running
- Turned on Windows Firewall to protect the system from attacks
- Turned off file sharing to the network to keep files more private
- Edited firewall settings to block incoming attacks to the computer through inbound rules

Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

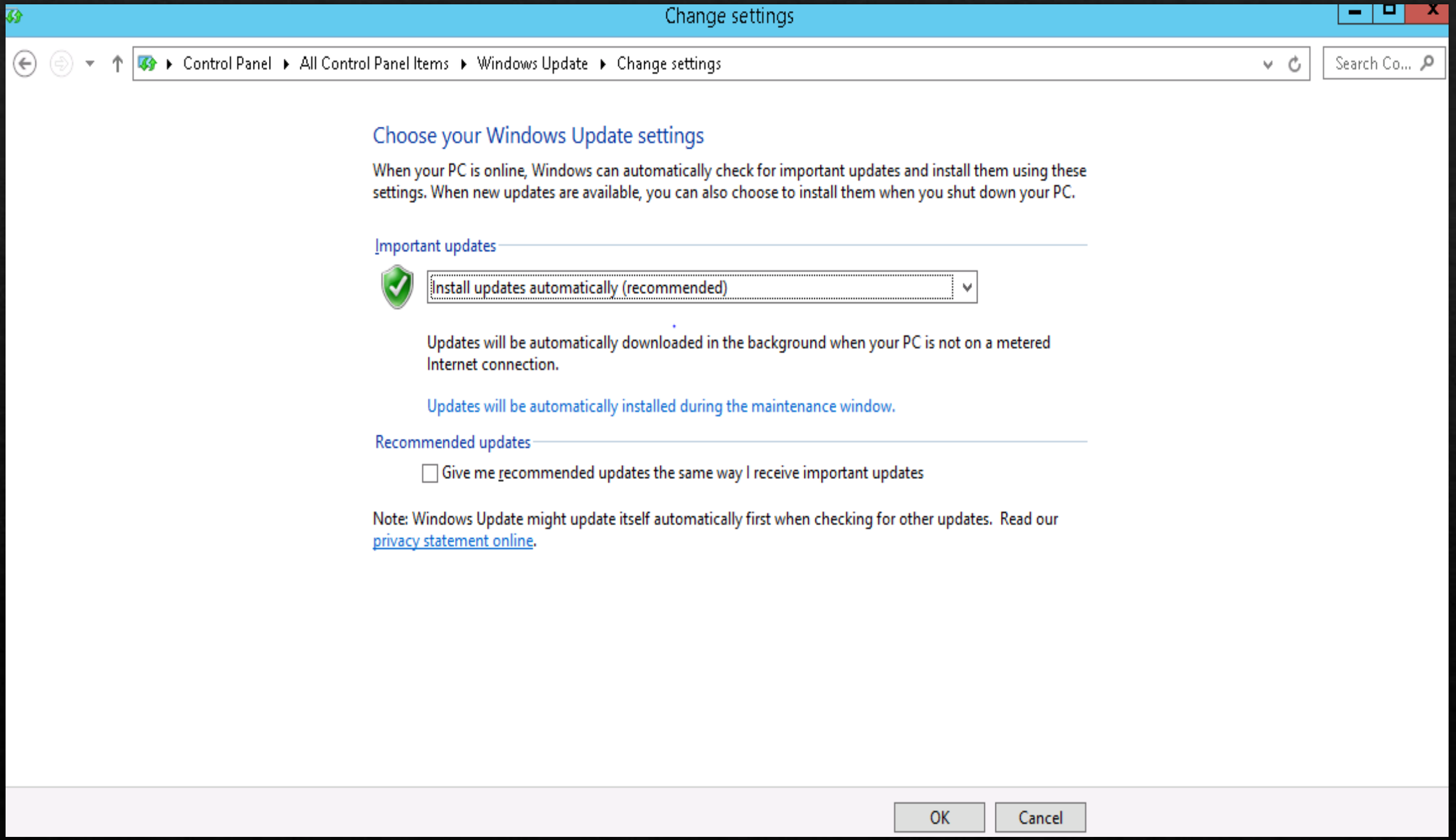
Networks in public places such as airports or coffee shops

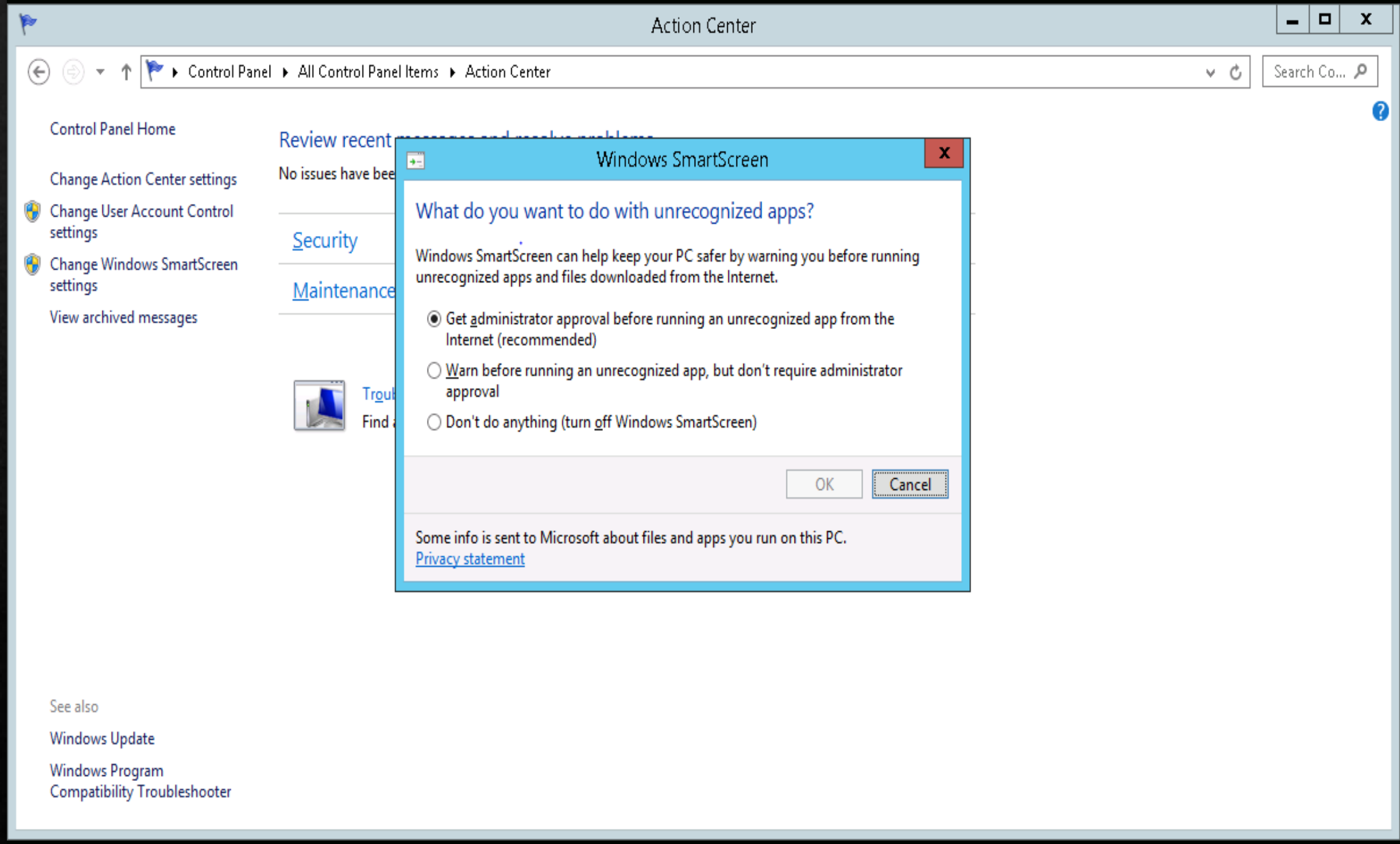
Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network 12
Notification state:	Do not notify me when Windows Firewall blocks a new app

See also

Action Center

Network and Sharing Center


Change settings
Control Panel ▸ All Control Panel Items ▸ Windows Update ▸ Change settings
Search Co...
Choose your Windows Update settings
When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.
Important updates
Install updates automatically (recommended)
Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.
Updates will be automatically installed during the maintenance window.
Recommended updates
Give me recommended updates the same way I receive important updates
Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.
OK
Cancel


Action Center
Control Panel ▸ All Control Panel Items ▸ Action Center
Search Co...
Control Panel Home
Change Action Center settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
Review recent
No issues have bee
Security
Maintenance
Windows SmartScreen
What do you want to do with unrecognized apps?
Windows SmartScreen can help keep your PC safer by warning you before running unrecognized apps and files downloaded from the Internet.
Get administrator approval before running an unrecognized app from the Internet (recommended)
Warn before running an unrecognized app, but don't require administrator approval
Don't do anything (turn off Windows SmartScreen)
OK
Cancel
Some info is sent to Microsoft about files and apps you run on this PC.
Privacy statement
See also
Windows Update
Windows Program Compatibility Troubleshooter

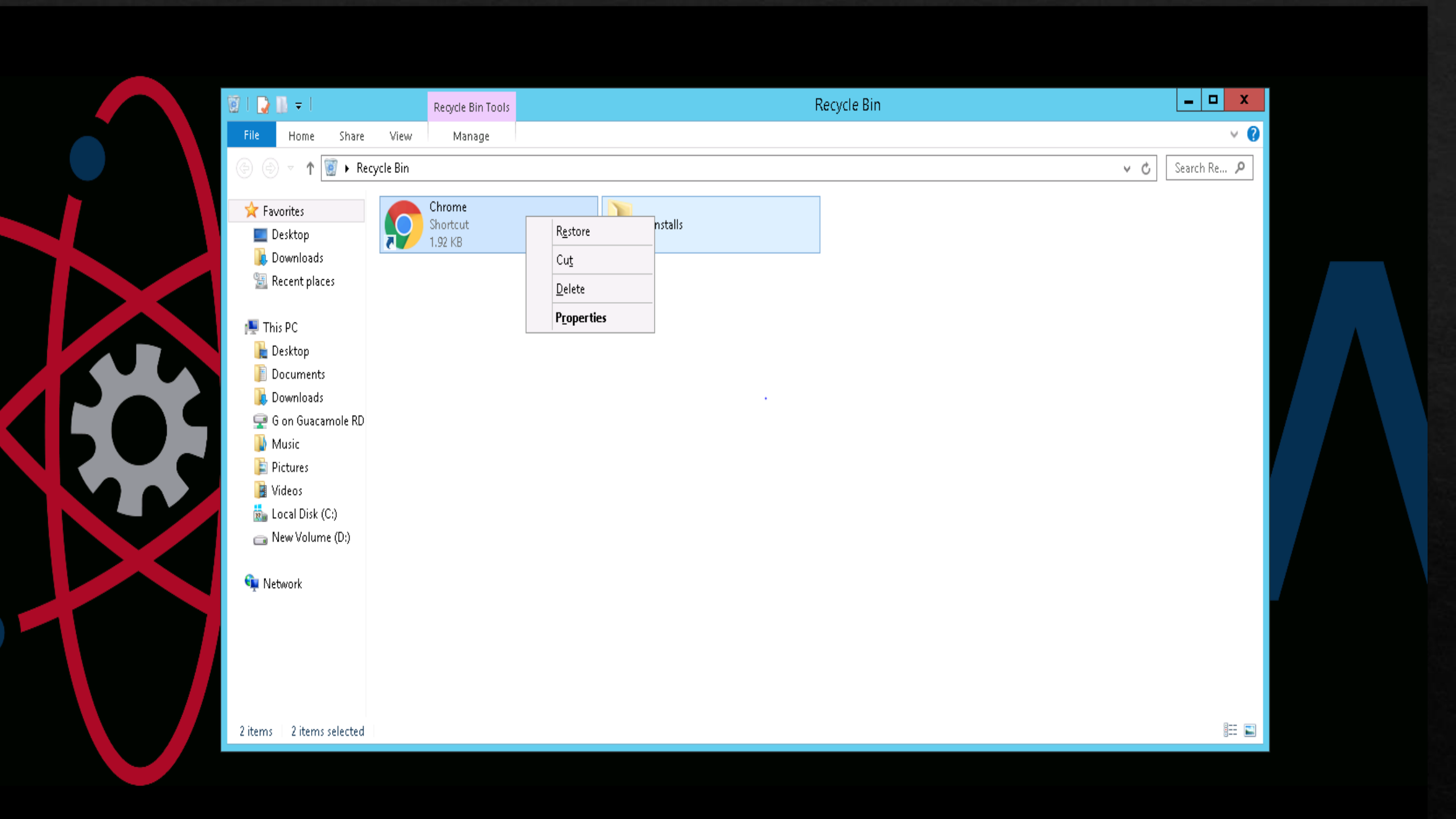
Recovery Methods

Not much information is lost that we know of, but to restore what was lost this is what we did:

- Opened Recycle Bin and searched for files that seem to belong to the user
- Restored those files back to the desktop

(We do not know if any files were permanently deleted by the malware)

- Additionally, you can restore previous files in the file explorer itself by using a System Restore, To use this feature, open a file explorer window and browse to the folder that contained (or still contains) the file or folder you want to recover. Right-click the file/folder and select Restore previous versions. Note * You must have a previous Windows Restore point to use this feature which comes preset on some systems


Recycle Bin
Recycle Bin Tools
File
Home
Share
View
Manage
Recycle Bin
Search Re...
Favorites
Desktop
Downloads
Recent places
This PC
Desktop
Documents
Downloads
G on Guacamole RD
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Network
Chrome
Shortcut
1.92 KB
nstalls
Restore
Cut
Delete
Properties
2 items
2 items selected

Protection/ Recommendations Methods

- Be Weary of suspicious looking emails !
- Do not share your passwords or logins with **anyone**.
- If you leave your computer unattended at ANY time lock it by simply pressing the Windows key and the "L" key at the same time.
- Always have the firewall set on the recommended settings.
- Always have Windows Smart screen turned on.
- When you download something find where it was downloaded in file explorer and make sure nothing else came with it.
- Be able to identify suspicious files you don't remember installing or came in with other legitimate downloads such as files that end in .exe, .bat, and .py
- Remove/uninstall programs that you have determined are malicious by deleting them then emptying the trash bin to ensure they are permanently gone.
- Install an ANTI-Virus software such as Avast or Malware Bytes, their base packages are FREE !

Security Incident Response Report

1. Contact Information for this Incident	
Name(s):	
Date of Report:	

2. Detection

Provide a brief description of what was detected, and the security threat, vulnerability, or breach identified:

Foo1.exe is on the desktop and is an unknown python program, that performs unknown and suspicious action. A hidden file, Foo.exe was found in the C: drive, the placement of the file is suspicious, and is likely was copied or executed to create Foo1.exe, and the other ones we would find later. It seems that Foo.exe might have installed itself to the root of the C: drive, which would explain the mess of files. It also appears to be self-propagating both on the system and perhaps even over the network. The files it appears to be using are .dlls, as well as a batch file that runs netstat (which lists the ports your machine is listening on), then sends the output to a log file, which is then detected by test.py. This is most likely for the foo.exe program to utilize for its own gain.

Foo3.exe was found in the recycling bin, along with other files that were put in there, including the chrome shortcut, chrome installer, and antivirus installer. An added user account was found with the name “suspicious”, and contained several “foo” files on it, which was obviously created by someone else. Foo2.exe was found in “ftproot” meaning it was likely downloaded using FTP. Both computer and web & email protection from the antivirus have been disabled, and there has never been a virus scan. The entirety of namespace_pkgs found in test_importlib which is a part of Python was infected with foo folders. Four other python files were also found to have foo in their name and were deleted. Windows Firewall was found to be turned off.

3. Response

Provide a brief description of the actions you took to contain and eradicate the security threat, vulnerability, or breach:

For all of the files found, the executables were converted into .pngs (harmless image files) and placed into a temporary folder, which was deleted after everything was thought to have been found.
All of the antivirus protections that were off were reenabled, and a deep scan was started and completed.
The “suspicious” user account was deleted in its entirety (which crashed the VM which means we’re doing something right)

4. Recovery

Provide a brief description of the actions you took to recover any affected data:

There was some data stored in the recycling bin, including the chrome shortcut, and an installers folder which contained installers for the antivirus on the system and for Chrome, which were restored.

5. Identify

Provide a brief description of any assets you identified that need to be protected:

The computer and its data.

6. Protect

Provide a brief description of the actions you took to protect your assets from future threats:

Windows defender was reenabled. FTP and its related services were disabled in the input and output rules in the firewall settings, along with the netbios and smb settings also found on there. Any http inbound rules were also disabled.
A screen saver was added to the device so that the laptop would automatically go into sleep mode after 1-3 minute(s) of inactivity. This would display the logon screen upon coming out of sleep mode.
Teach Josh about physical computer security and how to use Win-l to lock your computer (theoretical).

7. Lessons Learned

Please describe two lessons your team learned while solving this problem.

Antivirus is useful, but it certainly isn't the end-all-be-all and won't be able to catch everything.
Physical protection is the first step in defending against digital threats.

8. Other Information
Please provide any additional information you feel important. The public should be further educated on physical security of devices.