CompTIA A+ Core 2 Exam 220-1102

Lesson 17

Managing Security Settings

Objectives

- Configure workstation security
- Configure browser security
- Troubleshoot workstation security issues

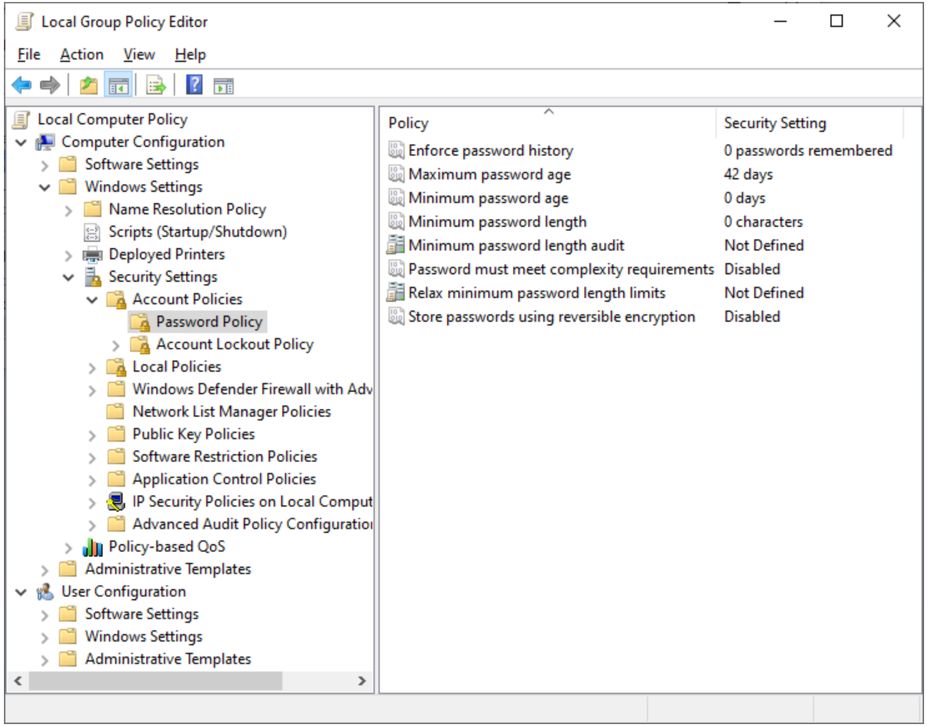
Lesson 17

Topic 17A

Configure Workstation Security

Password Best Practices

- Complexity requirements
  - Length
  - Character types
- Expiration requirements
- Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Screenshot courtesy of Microsoft

End User Best Practices

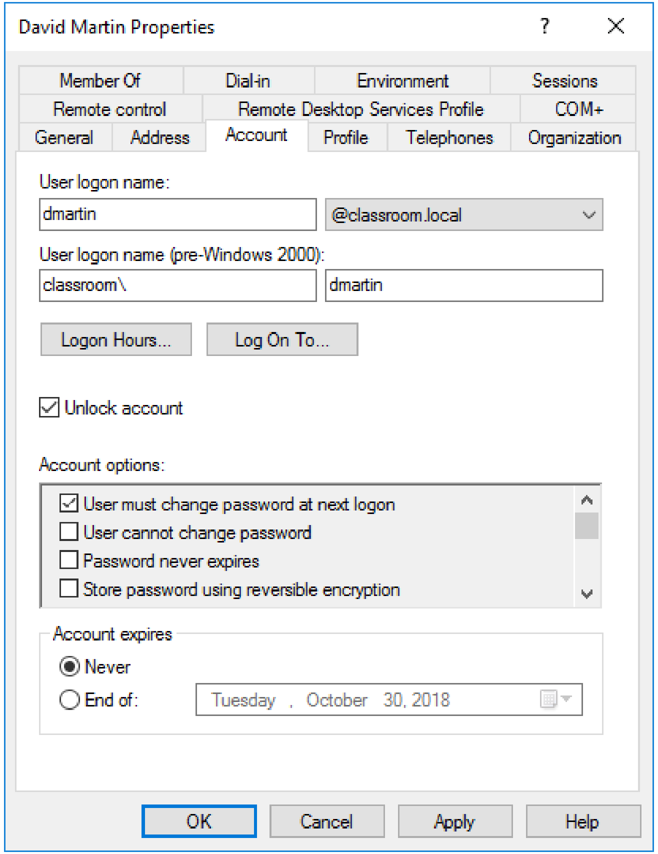
- Log off when not in use
  - Mitigate lunchtime attacks
  - Use screensaver locks
  - Manually lock workstation before leaving unattended
- Secure/protect critical hardware
  - Equipment locks
  - Care in public locations
- Secure personally identifiable information (PII) and passwords
  - Clean desk policy
  - Do not store in unencrypted documents or make unauthorized copies

Account Management

- Restrict user permissions
  - File permissions versus OS rights/privileges
  - Restrict privileges with UAC/sudo
- Change default administrator’s user account/password
  - Default Administrator/root is usually disabled
  - Avoid shared accounts
- Disable guest account

Account Policies

- Policies
  - Restrict login times
  - Failed attempts lockout
  - Concurrent logins
  - Use timeout/screen lock
- Re-enabling accounts
- Resetting passwords



User logon name: dmartin @classroom.local

User logon name (pre-Windows 2000): classroom\ dmartin

☑ Unlock account

Account options:

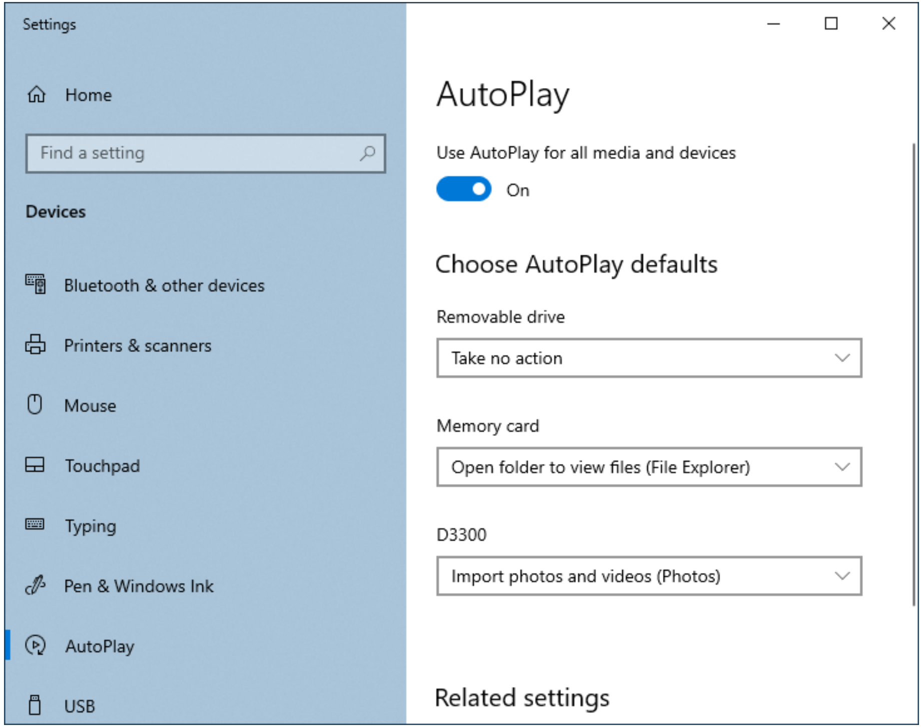
☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption

Account expires

● Never
○ End of: Tuesday , October 30, 2018

Screenshot courtesy of Microsoft

Execution Control



AutoPlay

Use AutoPlay for all media and devices: On

Choose AutoPlay defaults

Removable drive: Take no action

Memory card: Open folder to view files (File Explorer)

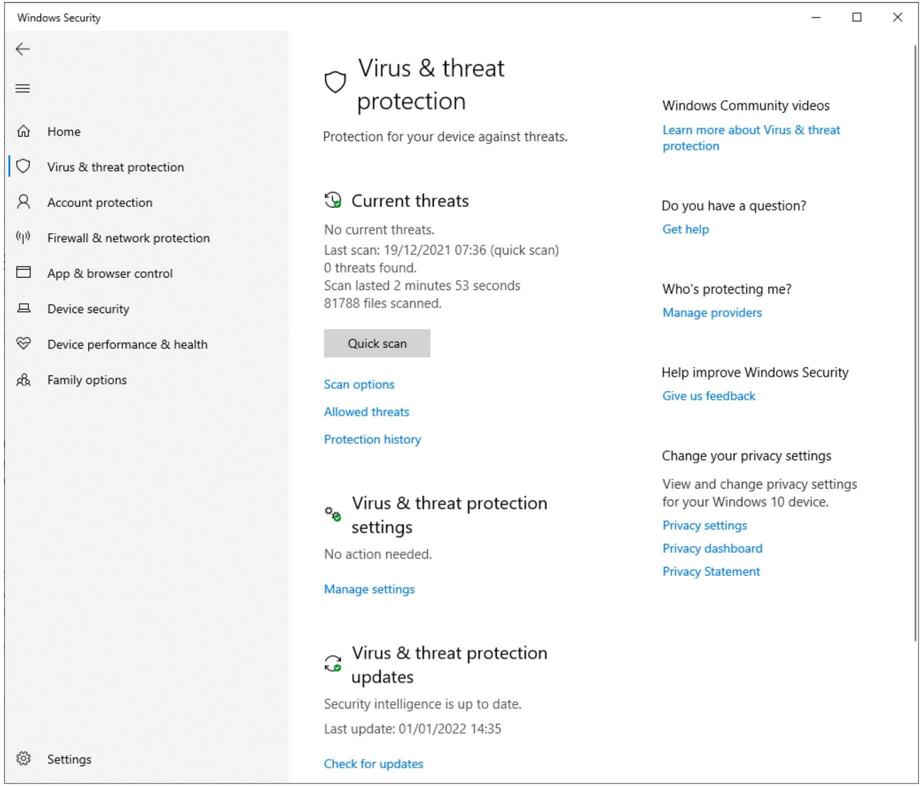
D3300: Import photos and videos (Photos)

Related settings

Screenshot courtesy of Microsoft

- Trusted/untrusted software sources
  - Code signing and hash verification
  - App stores
  - App blocklists
- AutoRun and AutoPlay
  - Configure default action for media attachment
  - Keep UAC enabled to prevent unauthorized code execution

Windows Defender Antivirus



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 19/12/2021 07:36 (quick scan)
0 threats found.
Scan lasted 2 minutes 53 seconds
81788 files scanned.

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Last update: 01/01/2022 14:35

Windows Community videos

Learn more about Virus & threat protection

Do you have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

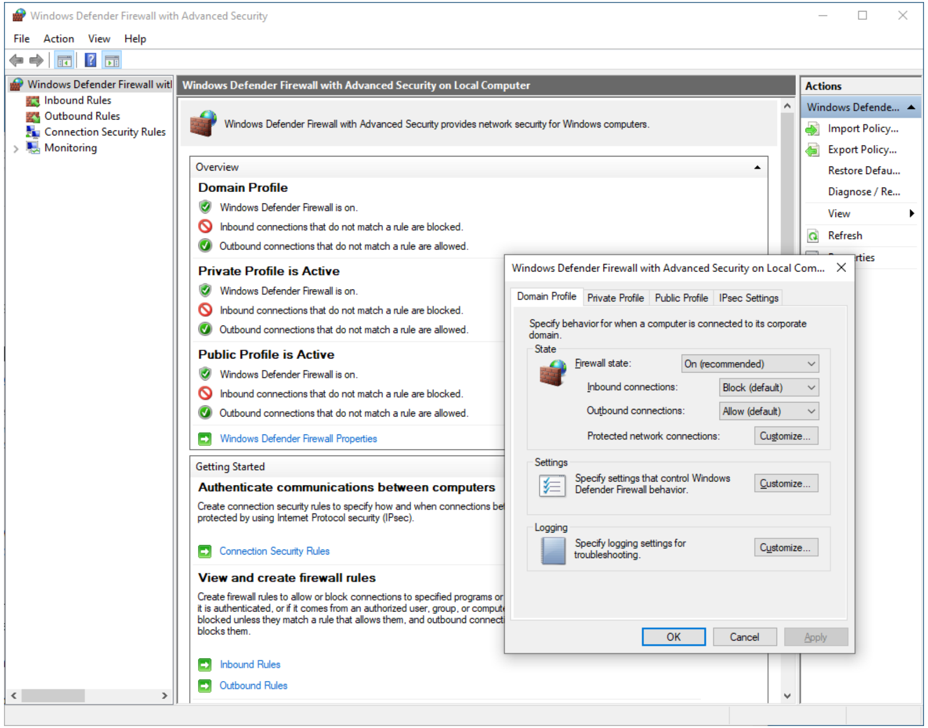
Privacy settings
Privacy dashboard
Privacy Statement

Screenshot courtesy of Microsoft

- Antivirus detection methods
  - Definitions versus heuristic
- Updates
  - Definitions versus scan engine
- Activating and deactivating
  - Temporarily disable online scanning
  - Replace with third-party product
  - Folder exclusions

Windows Defender Firewall

- Activating and deactivating
- Default block/allow policy
- Rule trigger types
    - Port security
    - Application security
    - Address
- Windows Defender Firewall with Advanced Security (wf.msc)



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections be protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or it is authenticated, or if it comes from an authorized user, group, or comput blocked unless they match a rule that allows them, and outbound connect blocks them.

Inbound Rules

Outbound Rules

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

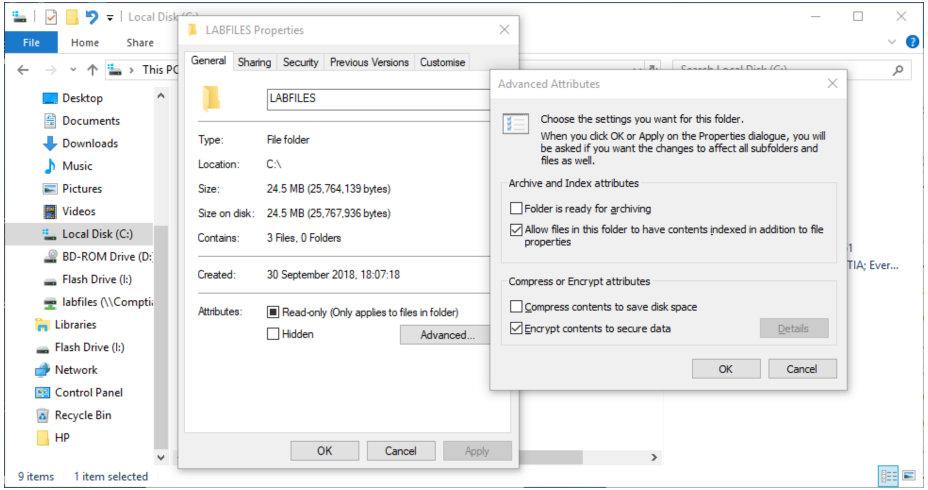
Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

Screenshot courtesy of Microsoft

Encrypting File System

- Data-at-rest encryption
  - Protect data when storage media is lost or stolen
  - Data cannot be read with encryption key
- Encrypting File System (EFS)
  - Encrypts selected folder/files
  - Encryption key stored in account and linked to password



LABFILES Properties

LABFILES

Type: File folder

Location: C:\

Size: 24.5 MB (25,764,139 bytes)

Size on disk: 24.5 MB (25,767,936 bytes)

Contains: 3 Files, 0 Folders

Created: 30 September 2018, 18:07:18

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Advanced...

Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialogue, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

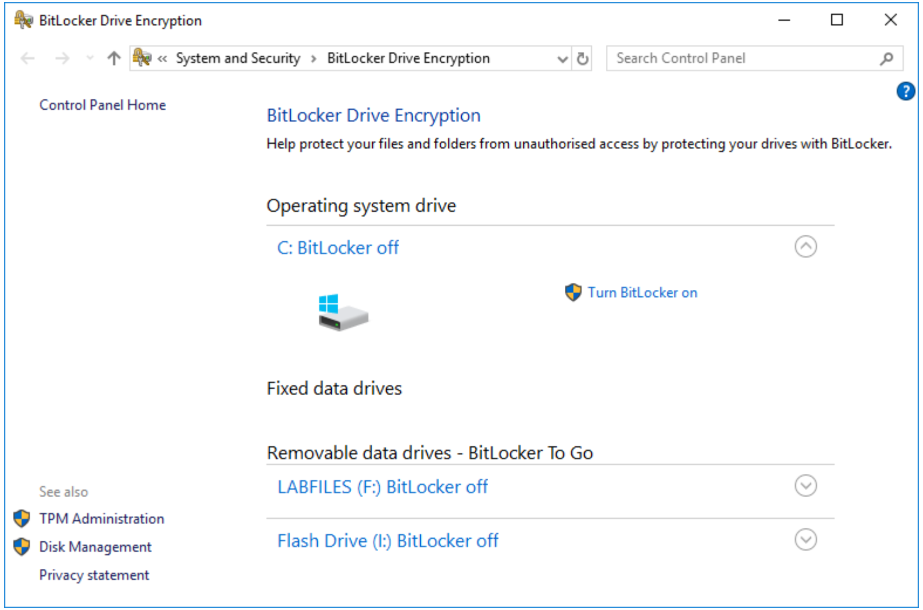
☑ Encrypt contents to secure data

Details

OK Cancel

Screenshot courtesy of Microsoft

Windows BitLocker and BitLocker-to-Go



BitLocker Drive Encryption

« System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

LABFILES (F:) BitLocker off

Flash Drive (I:) BitLocker off

See also

TPM Administration

Disk Management

Privacy statement

Screenshot courtesy of Microsoft

- Encrypts all data on drive
  - BitLocker for fixed disks
  - BitLocker To Go for removable disks
- Startup key stored in Trusted Platform Module (TPM) or on protected USB media
- Recovery key

Review Activity: Workstation Security

- Password and End User Best Practices
- Account Management and Account Policies
- Execution Control
- Windows Defender Antivirus
- Windows Defender Firewall
- Encrypting File System
- Windows BitLocker and BitLocker To Go

Lab Activity

- Assisted Lab: Configure Workstation Security
  - Enforce security settings using Local Security Policy in the Windows operating system

Lesson 17

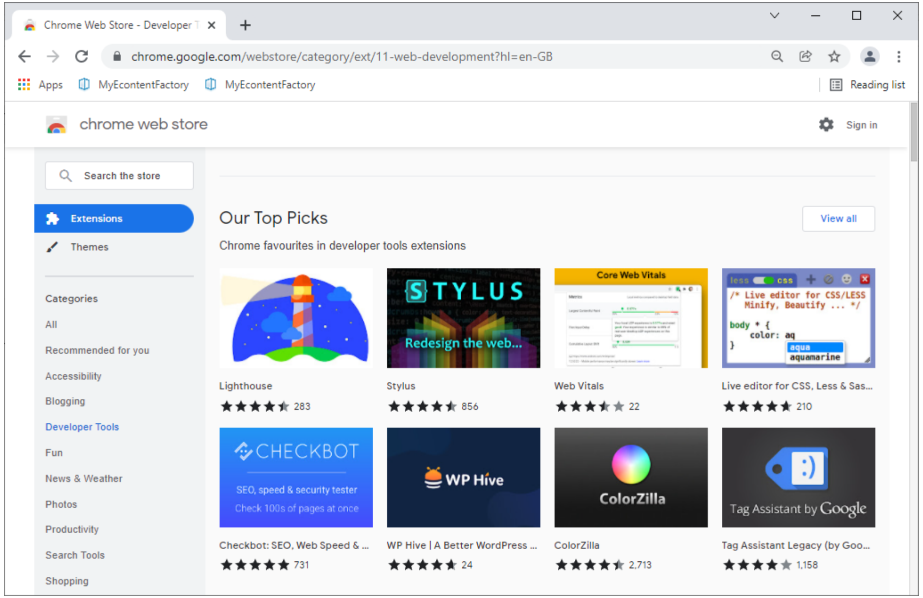
Topic 17B

Configure Browser Security

Browser Selection and Installation

- Trusted sources
  - Major browser vendors (Google Chrome, Opera, Mozilla Firefox, Microsoft Edge, Apple Safari)
  - App stores
  - Hash-based checksums/signatures to validate integrity
- Untrusted sources
  - Adware and bundled software
  - Potentially unwanted applications (PUAs)

Browser Extensions and Plug-ins

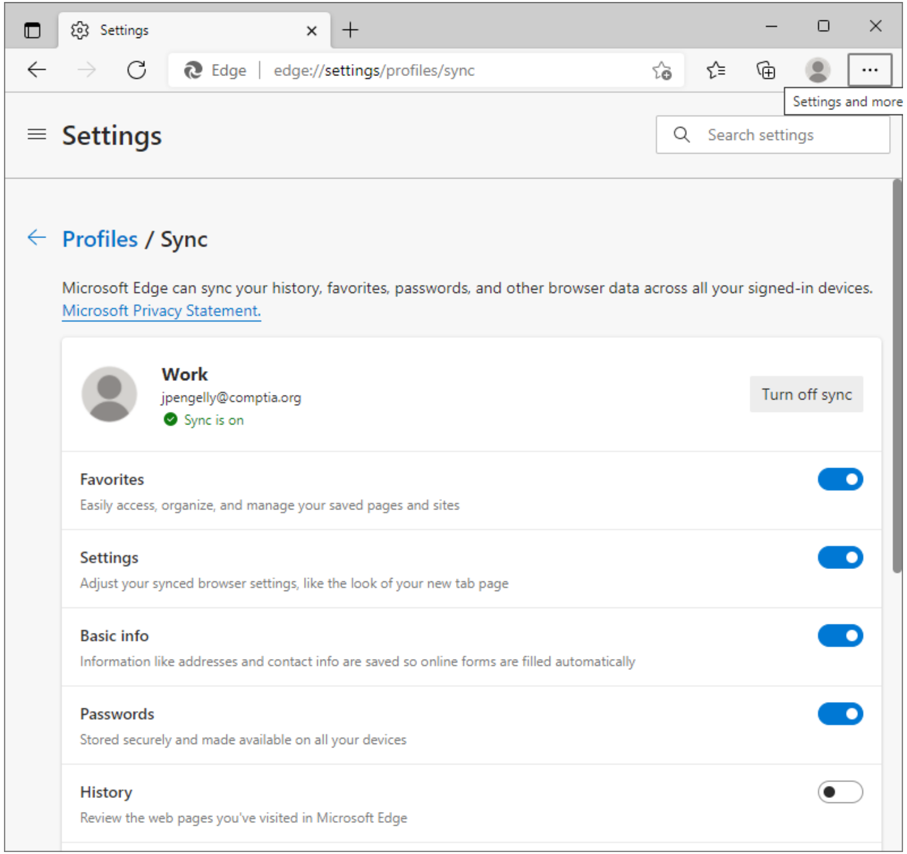


Screenshot courtesy of Google, a trademark of Google LLC.

- Extension
  - Script that uses the browser application programming interface (API) to implement new or modified functionality
- Plug-in
  - Executable designed to handle a specific type of object embedded on a web page
  - Generally deprecated due to risks from vulnerabilities
- Apps, default search provider, and themes
- Trusted versus untrusted sources
  - Browser plug-in store/marketplace

Browser Settings

- Accessing settings page
  - Ellipsis (...) or Hamburger (☰) menu
  - chrome://settings
    edge://settings
    about:preferences
- Sign-in and browser data synchronization
- Password managers



Profiles / Sync

Microsoft Edge can sync your history, favorites, passwords, and other browser data across all your signed-in devices. Microsoft Privacy Statement.

Work
jpengelly@comptia.org
✓ Sync is on

☑ Favorites
Easily access, organize, and manage your saved pages and sites

☑ Settings
Adjust your synced browser settings, like the look of your new tab page

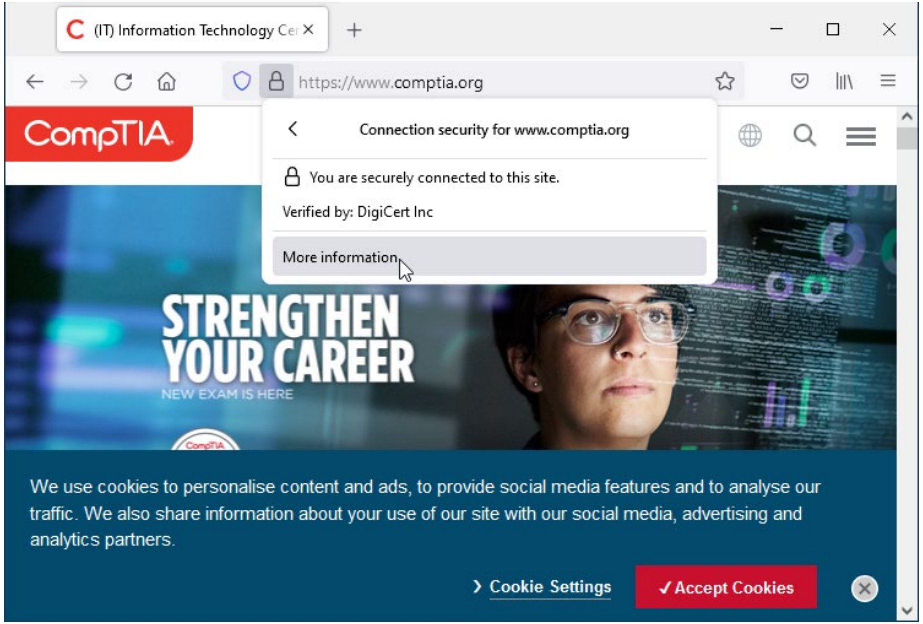
☑ Basic info
Information like addresses and contact info are saved so online forms are filled automatically

☑ Passwords
Stored securely and made available on all your devices

☐ History
Review the web pages you've visited in Microsoft Edge

Screenshot courtesy of Microsoft

Secure Connections and Valid Certificates



Connection security for www.comptia.org

You are securely connected to this site.

Verified by: DigiCert Inc

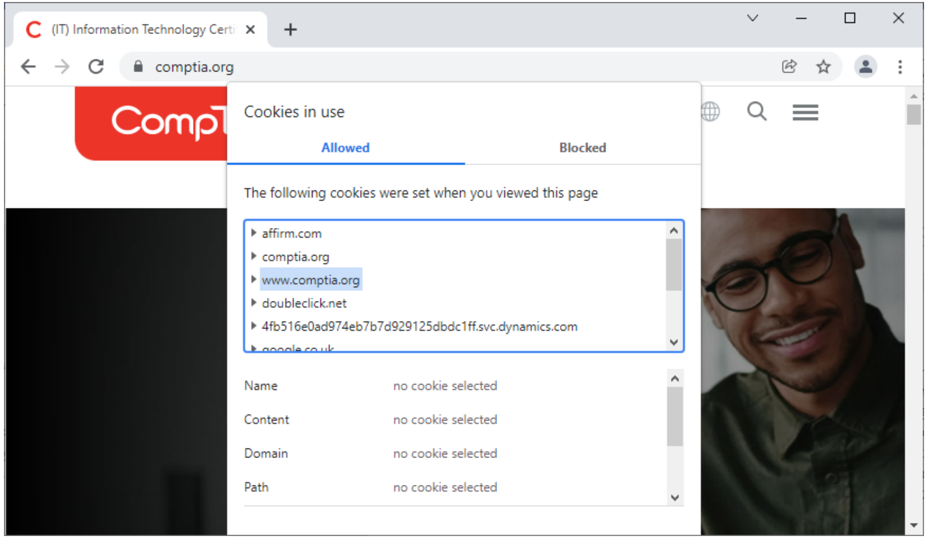
We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

Screenshot courtesy of CompTIA and Mozilla

- Transport Layer Security (TLS) and digital certificates
- HTTPS browser validation
  - Padlock icon
  - High assurance certificates
- Trusted root certificate updates
  - Windows Update
  - Separate per-browser stores

Browser Privacy Settings

- Site privacy and content controls
  - Cookie policy and tracking protection
  - Pop-up blocker
  - Ad blockers
- Browser cache
  - Clearing cache and browsing data
  - Private/incognito browsing mode



Cookies in use

Allowed | Blocked

The following cookies were set when you viewed this page

- affirm.com
- comptia.org
- www.comptia.org
- doubleclick.net
- 4fb516e0ad974eb7b7d929125dbdc1ff.svc.dynamics.com
- google.co.uk

Name	no cookie selected
Content	no cookie selected
Domain	no cookie selected
Path	no cookie selected

Screenshot courtesy of CompTIA and Google, a trademark of Google, LLC.

Review Activity: Browser Security

- Browser Selection and Installation
- Browser Extensions and Plug-ins
- Browser Settings
- Secure Connections and Valid Certificates
- Browser Privacy Settings

Lab Activity

- Assisted Lab: Configure Browser Security
  - Configure privacy settings for Microsoft's Edge browser

Lesson 17

Topic 17C

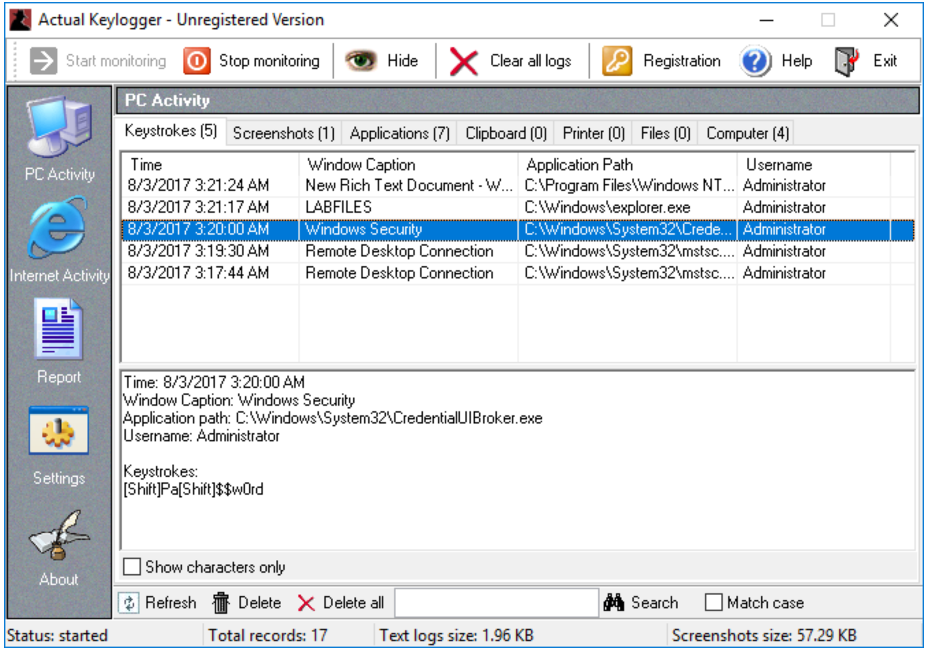
Troubleshoot Workstation Security Issues

Malware Vectors

- Viruses
    - Infects executable image and runs on execution
- Boot sector viruses
    - Infects disk media and runs at boot or on attachment to computer
- Trojans
    - Concealed within installer for legitimate software
- Worms
    - Infects process in system RAM and can spread over network ports
- Fileless malware
    - Uses local scripting technologies (PowerShell or JavaScript) to create malicious processes in memory

Malware Payloads

- Backdoors
  - Remote access Trojans (RATs) and bots
  - Command and control (C&C) network
- Spyware and keyloggers
  - Malware records user and system activity
- Rootkits
  - Malware elevates privileges to run at the highest possible level of trust
  - Makes any local process potentially unreliable



Time	Window Caption	Application Path	Username
8/3/2017 3:21:24 AM	New Rich Text Document - W...	C:\Program Files\Windows NT...	Administrator
8/3/2017 3:21:17 AM	LABFILES	C:\Windows\explorer.exe	Administrator
8/3/2017 3:20:00 AM	Windows Security	C:\Windows\System32\Crede...	Administrator
8/3/2017 3:19:30 AM	Remote Desktop Connection	C:\Windows\System32\mstsc....	Administrator
8/3/2017 3:17:44 AM	Remote Desktop Connection	C:\Windows\System32\mstsc....	Administrator

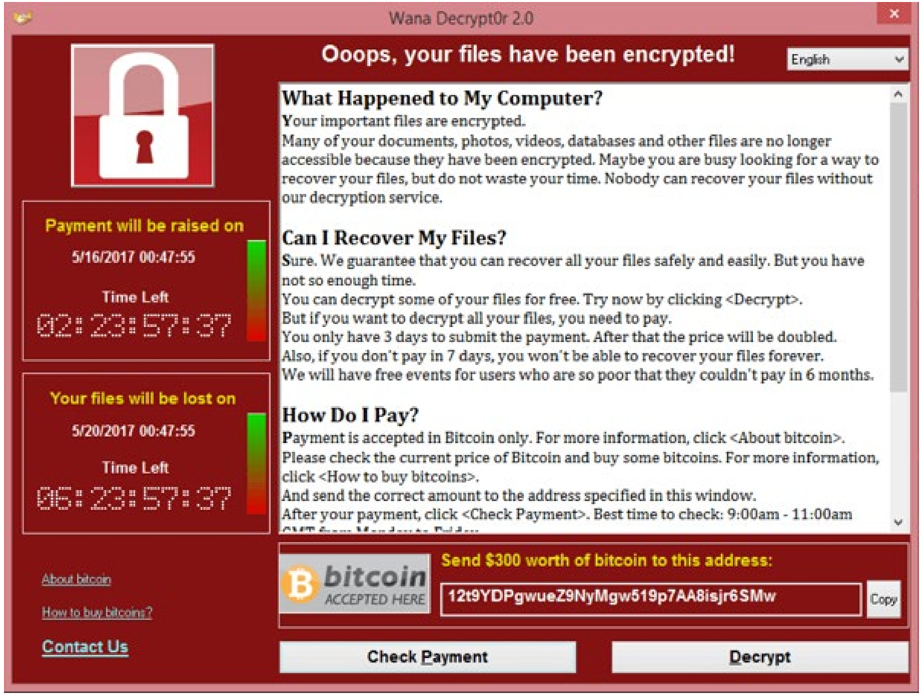
```
Time: 8/3/2017 3:20:00 AM
Window Caption: Windows Security
Application path: C:\Windows\System32\CredentialUIBroker.exe
Username: Administrator

Keystrokes:
[Shift]Pa[Shift]$$w0rd
```

Status: started | Total records: 17 | Text logs size: 1.96 KB | Screenshots size: 57.29 KB

Screenshot courtesy of Microsoft

Ransomware and Cryptominers



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Screenshot courtesy of Wikimedia

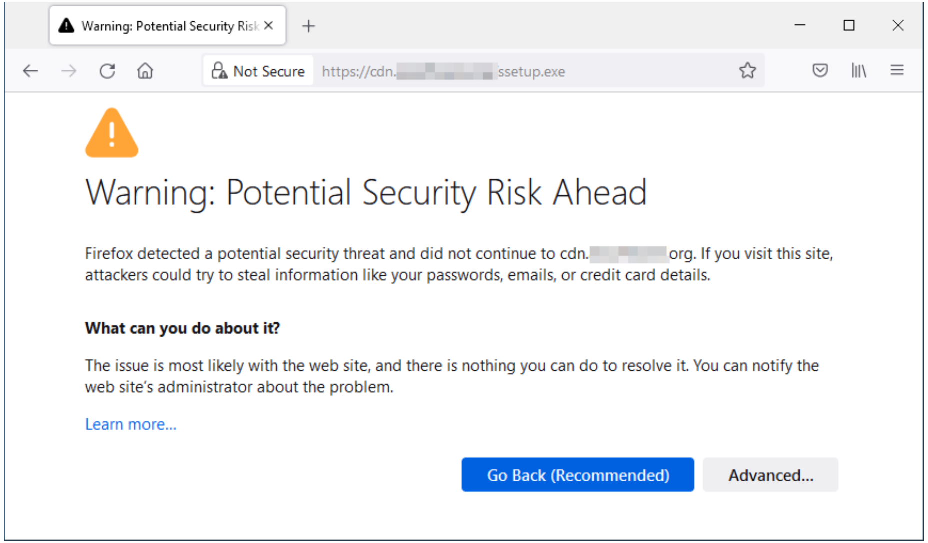
- Ransomware
  - Malware disables access to data files and/or system/shell
  - Often uses encryption
- Cryptominer
  - Malware hijacks computer resources to generate cryptocurrency

Troubleshoot Desktop Symptoms

- Performance symptoms
    - Faulty/slow startup or general performance
    - Unable to access the network
- Application crashes and service problems
    - Security apps stop working
    - OS and definition update failures
- File system errors and anomalies
- Desktop alerts and notifications
    - False alerts regarding antivirus protection

Troubleshoot Browser Symptoms

- Random/frequent pop-ups
- Redirection
  - URL/web address
  - Search engine
- Certificate warnings
  - Self-signed or issuer not trusted
  - Subject does not match host FQDN
  - Expired or revoked
- On-path attacks by malicious proxies


Warning: Potential Security Risk
Not Secure
https://cdn.[redacted]ssetup.exe
Go Back (Recommended)
Advanced...

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to cdn.[redacted]org. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the web site, and there is nothing you can do to resolve it. You can notify the web site's administrator about the problem.

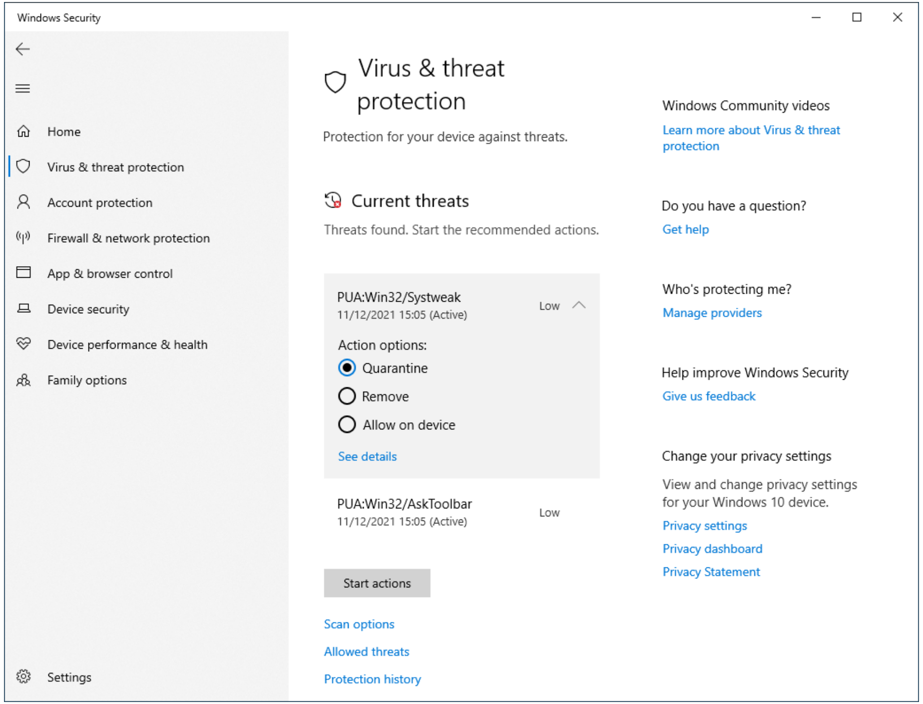
Learn more...

Screenshot courtesy of Microsoft

Best Practices for Malware Removal (Slide 1 of 2)

1. Investigate and verify malware symptoms
2. Quarantine infected systems
3. Disable System Restore in Windows
4. Remediate infected systems
    - Update anti-malware software
    - Scanning and removal techniques (e.g., safe mode, preinstallation environment)
5. Schedule scans and run updates
6. Enable System Restore and create a restore point in Windows
7. Educate the end user

Best Practices for Malware Removal (Slide 2 of 2)



Virus & threat protection

Protection for your device against threats.

Current threats

Threats found. Start the recommended actions.

PUA:Win32/Systweak Low
11/12/2021 15:05 (Active)

Action options:

● Quarantine

○ Remove

○ Allow on device

See details

PUA:Win32/AskToolbar Low
11/12/2021 15:05 (Active)

Start actions

Scan options

Allowed threats

Protection history

Windows Community videos

Learn more about Virus & threat protection

Do you have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

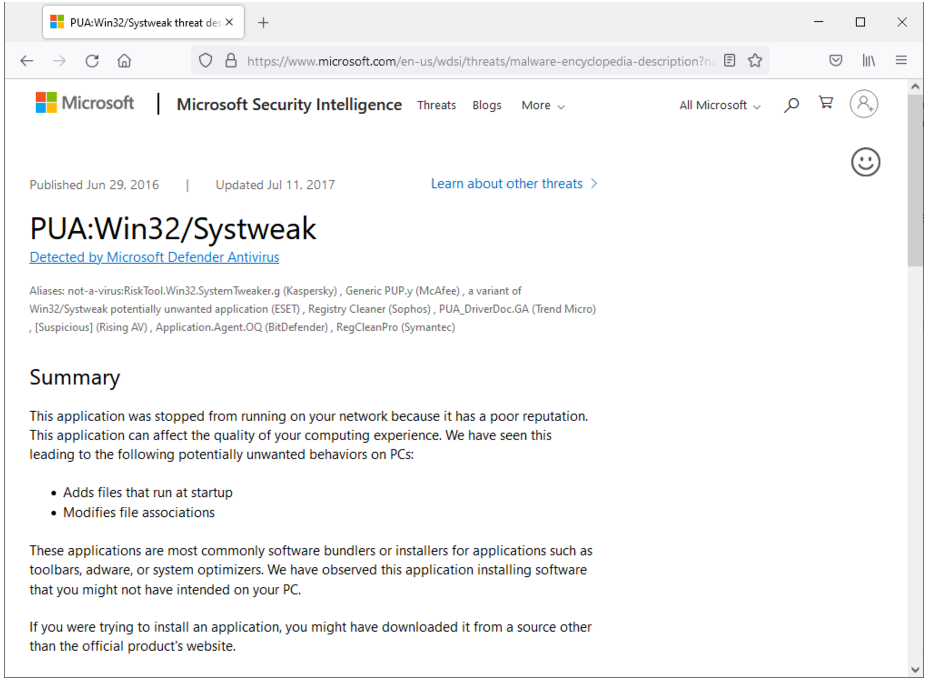
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement


PUA:Win32/Systweak threat des
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?na
Microsoft
Microsoft Security Intelligence
Threats
Blogs
More
All Microsoft

Published Jun 29, 2016 | Updated Jul 11, 2017 Learn about other threats >

PUA:Win32/Systweak

Detected by Microsoft Defender Antivirus

Aliases: not-a-virus:RiskTool.Win32.SystemTweaker.g (Kaspersky) , Generic PUP.y (McAfee) , a variant of Win32/Systweak potentially unwanted application (ESET) , Registry Cleaner (Sophos) , PUA_DriverDoc.GA (Trend Micro) , [Suspicious] (Rising AV) , Application.Agent.OQ (BitDefender) , RegCleanPro (Symantec)

Summary

This application was stopped from running on your network because it has a poor reputation. This application can affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs:

- Adds files that run at startup
- Modifies file associations

These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.

If you were trying to install an application, you might have downloaded it from a source other than the official product's website.

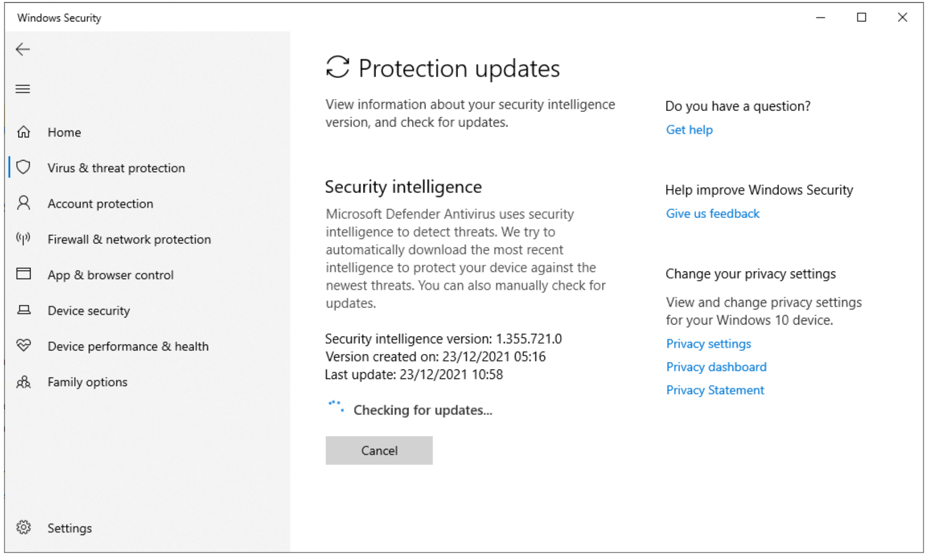
Screenshots courtesy of Microsoft

Infected Systems Quarantine

- Quarantine infected systems
  - Prevent use of privileged accounts
  - Isolate from production network
  - Isolate and scan removable media
- Disable System Restore
  - Turn off backup services that might preserve the malware

Malware Removal Tools and Methods

- Antivirus and anti-malware
  - Range of threat detection
  - Check for latest updates
- Recovery mode
  - Manual removal via antivirus tool or OS tool
  - Safe Mode and Windows Preinstallation Environment (WinPE)
- OS reinstallation



Protection updates

View information about your security intelligence version, and check for updates.

Security intelligence

Microsoft Defender Antivirus uses security intelligence to detect threats. We try to automatically download the most recent intelligence to protect your device against the newest threats. You can also manually check for updates.

Security intelligence version: 1.355.721.0
Version created on: 23/12/2021 05:16
Last update: 23/12/2021 10:58

Checking for updates...

Do you have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Screenshot courtesy of Microsoft

Malware Infection Prevention

- Configure on-access scanning
- Configure scheduled scans
- Re-enable System Restore and services
- Educate the end user
    - General threat awareness
    - Specific anti-phishing training

Review Activity: Workstation Security Issues

- Malware Vectors and Payloads
- Ransonware and Cryptominers
- Troubleshoot Desktop and Browser Symptoms
- Best Practices for Malware Removal
- Infected Systems Quarantine
- Malware Removal Tools and Methods
- Malware Infection Prevention

Lab Activity

- Assisted Lab: Troubleshoot Security Issues Scenario #1
  - Investigate and remediate a host where the security configuration has been compromised
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
  - Work independently to investigate and remediate a host where the security configuration has been compromised

CompTIA A+ Core 2 Exam 220-1102

Lesson 17

Summary